jamk

Tietoturvaohjelmistojen laadullinen vertailu

Juho Hiltunen

Opinnäytetyö, AMK
Maaliskuu 2025
Tieto- ja viestintätekniikan tutkinto-ohjelma

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Kuvailulehti

Hiltunen Juho

Tietoturvaohjelmistojen laadullinen arviointi

Jyväskylä: Jyväskylän ammattikorkeakoulu. **Maaliskuu 2025**, 31 sivua.

Tieto- ja viestintätekniikan tutkinto-ohjelma. Opinnäytetyö AMK.

Julkaisun kieli: suomi

Julkaisulupa avoimessa verkossa: kyllä

Tiivistelmä

Tietoturvaohjelmistojen vertailu keskittyi kolmen ohjelmiston F-Secure Total, Norton 360 Premium ja Acronis True image vertailuun. Tavoitteena oli arvioida ohjelmistojen käytettävyyttä, suorituskykyä ja tehokkuutta haittaohjelmien torjunnassa sekä selvittää kuinka hyvin ne vastaavat käyttäjien tarpeisiin.
Tutkimus toteutettiin laadullisella arvioinnilla, jossa käytettiin heuristista arviointia sekä testattiin ohjelmistoja virtuaalikoneympäristössä. Haittaohjelmatestauksessa hyödynnettiin European Institute for Computer Antivirus Researchin testitiedostoja sekä muita valmiita haittaohjelmia. Käytettävyyttä arvioitiin Jakob Nielsenin heuristiikkojen pohjalta. Tulokset osoittivat, että ohjelmistojen käytettävyydessä, suorituskyvyssä ja haittaohjelmistojen tunnistuksessa oli hieman eroavaisuuksia. F-Secure Total tarjosi yksinkertaisen käyttöliittymän ja kuormitti vähiten järjestelmää, mutta tunnisti haittaohjelmia osittain. Norton 360 Premium oli käytettävyydeltään selkeä ja tehokas haittaohjelmien torjunnassa. Arcronis True Image erottui varmuuskopiointi ominaisuuksillaan, mutta monimutkaiset asetukset vaativat käyttäjältä enemmän perehtymistä.

Johtopäätöksissä todettiin, että ohjelmistojen valintaan vaikuttavat käyttäjän yksilölliset tarpeet kuten käytettävyyden helppous, suojausominaisuuksien laajuus tai lisätoimintojen saatavuus. Tulokset tarjoavat hyödyllistä tietoa niin yksityishenkilöille kuin yrityksille, jotka pyrkivät kehittämään tietoturvakäytäntöjään ja valitsemaan tarpeisiinsa sopivan ratkaisun.

Avainsanat (asiasanat)

Tietoturvallisuus, haittaohjelma, tietoverkkorikokset

Muut tiedot (salassa pidettävät liitteet)

NIL (Not in List)

jamk

Description

Hiltunen Juho

Qualitative Evaluation of Information Security Software

Jyväskylä: JAMK University of Applied Sciences, March 2025, 31 pages

Degree Programme in Information and Communication Technology. Bachelor´s thesis.

Permission for open access publication: Yes

Language of publication: Finnish

Abstract

The comparison of information security software focused on analyzing three programs – F-Secure Total, Norton 360 Premium, and Acronis True Image. The objective was to evaluate their usability, performance, and efficiency in malware protection and to assess how well they meet user needs and adapt to the evolving landscape of cybersecurity threats.
The study was conducted using qualitative methods, including heuristic evaluation and testing in a virtual machine environment. The malware testing utilized European Institute for Computer Antivirus Research test files and additional pre-loaded malware. Usability was assessed based on Jakob Nielsen's heuristics.
The results revealed significant differences in usability, performance, and malware detection capabilities among the software. F-Secure Total provided a straightforward user interface but only partially detected malware. Norton 360 Premium demonstrated clear usability and strong malware protection. Acronis True Image stood out for its backup features but required more user familiarity due to its complex settings.
In conclusion, the choice of software depends on individual user needs, such as ease of use, the comprehensiveness of protection features, and availability of additional functionalities. The findings provide valuable insights for both individuals and organizations aiming to enhance their cybersecurity practices and select the most suitable solution for their needs.

Keywords/tags (subjects)

Information Security, malware, cybercrime

Miscellaneous (Confidential information)

NIL (Not in List)

Sisältö

1 Johdanto 7

2 Tutkimusasetelma 7

2.1 Taustatutkimus ja nykytilan analyysi 7

2.2 Eettisyys 8

2.3 Tutkimusmenetelmä 9

2.4 Tutkimuskysymykset 10

2.5 Laadullinen tutkimus 10

2.6 Käytettävyyden arviointi 11

2.6.1 Järjestelmän ja käyttäjän vuorovaikutus tulisi olla yksinkertaista 12

2.6.2 Järjestelmän tulisi käyttää käyttäjän kieltä 12

2.6.3 Esittää asiat näytöllä niin, että käyttäjän ei tarvitse muistella niitä 12

2.6.4 Järjestelmän tulee olla yhdenmukainen 12

2.6.5 Pyrkiä estämään virheenmahdollisuuksia 12

2.6.6 Tukea oikoteitä, tehokasta työskentelyä ja räätälöintiä 13

2.6.7 Pyrkiä esteettiseen ja minimalistiseen suunnitteluun 13

2.6.8 Auttaa käyttäjää tunnistamaan virheet ja ymmärtämään niitä 13

2.6.9 Tarjolla tulisi olla hyvä opastus ja dokumentaatiot 13

2.6.10 Käyttäjän huomioiminen realiajassa 13

3 Tietoturvallisuus 14

3.1 Yleistä 14

3.2 Tekninen tietoturva 14

3.3 Hallinnollinen tietoturva 15

3.4 Yksityishenkilön tietoturva 15

3.5 Yrityksen tietoturva 16

4 Tietoturvaohjelmat 17

4.1 Yleistä 17

4.2 F-Secure Total 17

4.3 Norton 360 Premium 18

4.4 McAfee Total Protection 18

4.5 Acronis True Image 18

5 Haittaohjelmat 19

5.1 Yleistä 19

5.2 Virus 19

5.3 Troijalainen 19
5.4 Ransomware 20
5.5 Mato 20
5.6 Mainosohjelma 21
5.7 Vakoiluohjelma 21
6 Tietoverkkorikollisuus 22
6.1 Tietoverkkorikollisuuden kehitys 22
6.2 Tietoverkkorikollisuus nyt 23
6.3 Lain kohdat 24
6.3.1 Tietojärjestelmän häirintä 24
6.4 Tietoliikenteen häirintä 25
6.4.1 Tietomurto 25
6.4.2 Tietosuojarikos 26
6.4.3 Viestintäsalaisuuden loukkaus 27
6.4.4 Salassapitorikkomus ja -rikos 27
7 Testaamisen toteutus 28
7.1 Ympäristö 28
8 Vertailu 29
8.1 F-Secure Total 29
8.2 Käytettävyyden arviointi F-Secure Total 29
8.3 Norton 360 Premium 30
8.4 Käytettävyyden arviointi Norton 360 Premium 31
8.5 Acronis True Image 32
8.6 Käytettävyyden arviointi Acronis True Image 33
8.7 Tulokset 34
9 Yhteenveto 36
9.1 Laatu ja luotettavuus 36
9.2 Pohdinta 37
Lähteet 39
Liitteet ..... Virhe. Kirjanmerkkiä ei ole määritetty.
Liite 1. Liitteen otsikko ..... **Virhe. Kirjanmerkkiä ei ole määritetty.**

Kuviot

Kuvio 1 Testaus prosessi kuvattuna 9
Kuvio 2 Testaus ympäristö 28

Taulukot

Taulukko 1. Poliisille ilmoitetut rikokset 24
Taulukko 2. Ohjelmistojen suorituskyky 34
Taulukko 3. Ohjelmistojen ominaisuudet 35
Taulukko 4. Käytettävyyden arvioinnin pisteet 36

1 Johdanto

Tietoturva on digitaalisessa maailmassa yksi keskeisimmistä tekijöistä, jotka vaikuttavat niin yksilöiden kuin organisaatioiden toimintakykyyn ja turvallisuuteen. Nopeasti kehittyvä teknologia ja laajeneva internetin käyttö ovat lisänneet huomattavasti tietoturvariskejä, kuten haittaohjelmien leviämistä ja tietoverkkorikollisuutta. Näiden uhkien torjumiseksi tietoturvaohjelmistot ovat muodostuneet olennaiseksi osaksi digitaalista arkea, tarjoten suojan esimerkiksi viruksia, vakoiluohjelmia ja identiteettivarkauksia vastaan.

Tässä opinnäytetyössä tarkastellaan tietoturvaohjelmistojen kykyä suojata käyttäjiä digitaalisilta uhilta vertailemalla kolmea suosittua ohjelmistoa: F-Secure Total, Norton 360 Premium ja Acronis True Image. Vertailu suoritetaan laadullisen tutkimuksen keinoin, jossa analysoidaan ohjelmistojen ominaisuuksia, käytettävyyttä ja tehokkuutta tietoturvan tarjoajina. Vertailu tarjoaa syvällisen näkemyksen siitä, miten erilaiset tietoturvaratkaisut vastaavat käyttäjien tarpeisiin ja muuttuvan uhkakentän vaatimuksiin. Teoriaosuudessa käsitellään tietoturvan perusteita, haittaohjelmien ja virusten toimintaa sekä tietoverkkorikollisuuden kehitystä historiasta nykypäivään.

Opinnäytetyön tavoitteena on tarjota kokonaisvaltainen käsitys siitä, miten eri tietoturvaohjelmistot toimivat, mitä vahvuuksia ja heikkouksia niillä on ja kuinka ne voivat vastata käyttäjien moninaisiin tarpeisiin. Tutkimus antaa tietoa ohjelmistojen valintaan vaikuttavista tekijöistä ja auttaa ymmärtämään, millaisia ominaisuuksia hyvä tietoturvaohjelmisto sisältää. Näin työ palvelee sekä yksityishenkilöitä että organisaatioita, jotka haluavat kehittää tietoturvakäytäntöjään ja tehdä tietoon perustuvia valintoja suojatakseen digitaalista omaisuuttaan.

2 Tutkimusasetelma

2.1 Taustatutkimus ja nykytilan analyysi

Tietoturvaohjelmistot ovat olleet keskeisessä roolissa digitaalisen turvallisuuden kehittymisessä. Haittaohjelmien ja tietoverkkorikollisuuden yleistyessä yksityishenkilöt ja organisaatiot ovat yhä riippuvaisempia tehokkaista suojausratkaisuista. Tietoturvaohjelmistojen markkina on kasvanut merkittävästi, ja niiden ominaisuudet ovat monipuolistuneet. Perinteisten virustorjuntaohjelmien rinnalle on tullut kattavia tietoturvasovelluksia, jotka sisältävät muun muassa palomuurit, VPN-palvelut, salasanojen hallintatyökalut ja identiteettivarkauksien suojausratkaisut ja monia muita ominaisuuksia. Tietoturvan merkitys on kasvanut

erityisesti hybridityön ja pilvipalveluiden yleistyessä. Monet yritykset ja yksityishenkilöt tallentavat arkaluonteisia tietoja pilvipalveluihin, jolloin kyberhyökkäysten torjunta on entistä kriittisempää. Tämä on lisännyt tarvetta tehokkaille tietoturvaohjelmille, jotka tarjoavat laajaa suojaa eri uhkia vastaan.

Eri ohjelmistojen vahvuudet vaihtelevat käytettävyydessä, haittaohjelmien tunnistuksessa ja järjestelmäkuormituksessa. Ulkopuoliset arvioinnit, kuten esimerkiksi AV-TEST ja AV-Comparatives, tarjoavat säännöllisesti tuloksia ohjelmistojen kyvykkyydestä havaita ja poistaa haittaohjelmia.

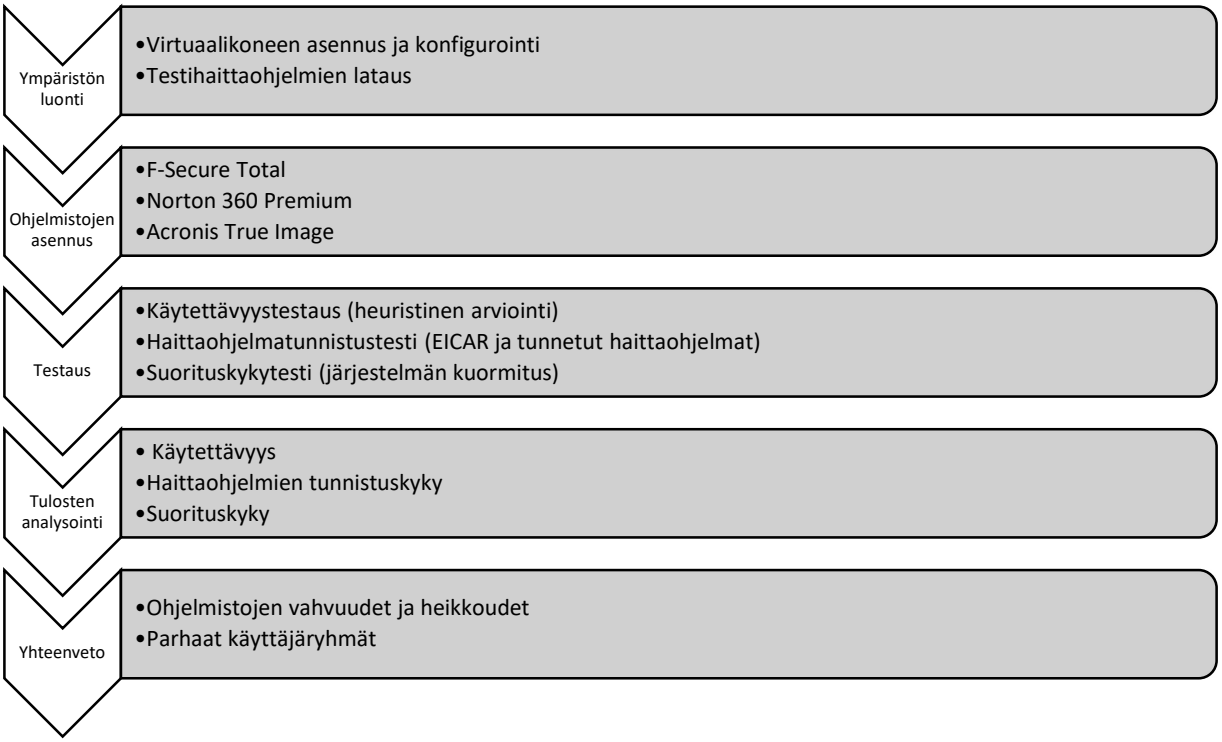
Eettisestä näkökulmasta tietoturvaohjelmistojen käyttäminen voi herättää kysymyksiä datan keräämisestä ja yksityisyyden suojasta. Monet ohjelmistovalmistajat keräävät anonyymisti tietoa ohjelmiston suorituskyvystä ja uhkien havainnoinnista, mutta käyttäjän tulisi tarkastella tietosuojakäytäntöjä ennen ohjelmiston käyttöä. Jotkin tietoturvaohjelmat käyttävät myös käyttäjän tietoja mahdollisten uhkien torjumiseen ja tekoälyavusteiseen analyysiin. Tämä voi parantaa ohjelmiston tehokkuutta, mutta samalla herättää kysymyksiä tietojen turvallisuudesta ja yksityisyyden suojasta. Lisäksi ohjelmistojen sertifioinnit ja ulkopuoliset testaukset lisäävät ohjelmistojen luotettavuutta.

2.2 Eettisyys

Opinnäytetyössä käsitellään tietoturvaohjelmistoja, joiden arviointi ja vertailu perustuvat käytännön testaamiseen ja heuristiseen arviointiin. Työn eettisyyteen liittyy testauksessa käytettyjen haittaohjelmatiedostojen käyttö sekä tietoturvaohjelmistojen käyttöehdot. Opinnäytetyössä käytetään European Institute for Computer Antivirus Research (EICAR) -järjestön laatimia testitiedostoja sekä valmiiksi tunnettuja haittaohjelmia, jotka olivat salasanalla suojattuja eli eivät voi käynnistyä laitteessa ilman salasanan antamista. Testaaminen tapahtui kontrolloidussa virtuaaliympäristössä, jolla varmistettiin, ettei testauksella ollut haitallisia vaikutuksia ulkopuolisiin järjestelmiin tai tietoturvaan. Opinnäytetyössä oli suunnitelman mukaan tarkoitus testata viisi eri tietoturvaohjelmistoa: F-Secure Total, Norton Premium 360, Acronis True Image, McAfee Total Protection sekä Avast Premium. McAfee Total ja Avast Premium jätettiin testauksesta pois, koska heidän käyttöehtonsa kielsivät testaus tulosten julkistamisen.

2.3 Tutkimusmenetelmä

Tutkimuksen tarkoituksena on vertailla kolmea eri tietoturvaohjelmistoa F-Secure Total, Norton 360 Premium ja Acronis True Image. Tietoturvaohjelmista on tarkoitus vertailla suorituskykyä, käytettävyyttä ja haittaohjelmien tunnistusta. Vertailu toteutetaan laadullisena tutkimuksena, joka mahdollistaa ilmiön tarkastelun ilman tilastollista yleistämistä. Tämä lähestymistapa soveltuu hyvin tutkimuksen tavoitteisiin.



Kuvio 1 Testaus prosessi kuvattuna

Tietoturvaohjelmistoja arvioin Jakob Nielsenin heuristisen arvioinnin periaatteiden mukaisesti. Tämä menetelmä perustuu joukkoon käytettävyyden periaatteita, joiden avulla tunnistetaan järjestelmien käyttöliittymien vahvuudet ja heikkoudet. Heuristinen tapa on tehokas suoritettaessa ohjelmiston käyttö testauta ilman massiivista testausjoukkoa.

Ohjelmistojen suorituskykyä ja haittaohjelmien torjuntaominaisuuksien testaus tapahtuu virtuaalisessa ympäristössä. Käytössä on Oracle VirtualBox -ohjelmistoon asennettu Windows 10 -virtuaalikone, joka vastaa keskimääräistä perustason tietokonetta. Tämä lähestymistapa mahdollistaa turvallisen ympäristön haittaohjelmien testaamiselle ilman riskiä fyysiselle laitteistolle. Testaaminen sisältää European Institute for Computer Antivirus Research (EICAR) -testitiedostojen ja ennalta ladatun haittaohjelmapaketin käytön. Näillä testitiedostoilla arvioidaan ohjelmistojen kykyä havaita ja käsitellä tunnettuja ja simuloituja uhkia.

Tutkimusympäristö on vakioitu, jotta ohjelmistojen toimintaa on mahdollista vertailla tasapuolisesti. Esimerkiksi jokaiselle ohjelmistolle on identtiset resurssit, kuten prosessoriteho, keskusmuisti ja tallennustila. Lisäksi testit suoritetaan samassa järjestyksessä ja samoilla menetelmillä, jotta ulkoisten tekijöiden vaikutus on minimoitua.

2.4 Tutkimuskysymykset

Tietoturvaohjelmistojen rooli on keskeinen nykypäivän digitaalisessa ympäristössä, jossa käyttäjät kohtaavat monimutkaisia ja jatkuvasti kehittyviä kyberuhkia. Tämän tutkimuksen tavoitteena on arvioida kolmea tietoturvaohjelmistoa – F-Secure Totalia, Norton 360 Premiumia ja Acronis True Imagea – käytettävyyden, suorituskyvyn ja haittaohjelmien torjunnan näkökulmista. Lisäksi tarkastellaan, miten hyvin nämä ohjelmistot vastaavat käyttäjien erilaisiin tarpeisiin ja mitä kehityssuuntia ohjelmistojen tulevaisuus mahdollisesti pitää sisällään.

Tutkimus perustuu laadulliseen analyysiin, joka tarjoaa syvällistä tietoa ohjelmistojen ominaisuuksista ja niiden soveltuvuudesta erilaisille käyttäjäryhmille. Pohjautuen työn tavoitteisiin, tutkimusta ohjaavat seuraavat kysymykset:

1. Miten F-Secure Total, Norton 360 Premium ja Acronis True Image eroavat toisistaan käytettävyydessä, suorituskyvyssä ja haittaohjelmien torjunnassa?
   Tämän kysymyksen kautta selvitetään ohjelmistojen keskeiset erot ja niiden vaikutus käyttäjäkokemukseen.
2. Kuinka hyvin valitut tietoturvaohjelmistot vastaavat erilaisten käyttäjäryhmien, kuten yksityishenkilöiden ja organisaatioiden tarpeisiin? Tavoitteena on arvioida ohjelmistojen ominaisuuksien ja käyttäjien tarpeiden välistä tasapainoa.
3. Millaisia kehitystarpeita ja -mahdollisuuksia tietoturvaohjelmistoilla on vastaamaan muuttuvaan kyberuhkakenttään? Tämä kysymys avaa näkökulmia tietoturvaohjelmistojen tulevaisuuteen ja niiden rooliin jatkuvasti kehittyvässä teknologiaympäristössä.

Näiden kysymysten kautta tutkimus pyrkii tarjoamaan kattavan kuvan tietoturvaohjelmistojen vahvuuksista, heikkouksista ja kehitysmahdollisuuksista. Tulokset tarjoavat arvokasta tietoa sekä ohjelmistojen käyttäjille ja kehittäjille.

2.5 Laadullinen tutkimus

Tämä opinnäytetyö on tietoturvaohjelmistojen laadullinen vertailu, eli kvantitatiivinen tutkimus. Laadullisen tutkimuksen lähestymistapana pidetään ilmiön kuvaamista ilman numeerista tai tilastoihin perustuvaa yleistystä. Sillä pyritään kuvaamaan jonkinlaista ilmiötä tai toimintaa siihen liittyvien asioiden kautta. (Es-

kola J. & Suoranta J 1998). Laadullinen lähestymistapa asettaa myös tutkijan asemaan, jossa tämän riippuvuus aiheesta on välttämätön. Tämä tarkoittaa sitä, että tutkimus ja siihen liittyvät valinnat voivat muuttua projektin aikana sekä itse tutkijan on asetuttava tutkimuksen keskiöön osallistuvana toimijana. Puolueettomuuden osalta on myös tutkittavaan ilmiöön suhtauduttava objektiivisesti, mutta taustatietojen osalta subjektiivisesti. Laadullisen tutkimuksen tunnuspiirteisiin sisältyy itse tutkimuksessa aihepiirin vähäinen määrä tapauksia, jotka tulisi tutkia perusteellisesti. Laadullisen tutkimuksen aineiston avulla tutkijan tulisi löytää uusia näkökulmia tutkimuksen kohteena olevaan aiheeseen. (Eskola J. & Suoranta J 1998)

Laadullinen tutkimus lähestymistapana ohjelmistokehityksessä mahdollistaa ihmisten kokemusten, näkökulmien ja vuorovaikutusten syvällisen ymmärtämisen. Ohjelmistokehityksen kontekstissa laadullinen tutkimus soveltuu erityisesti tilanteisiin, joissa halutaan tutkia kehitysprosessien dynamiikkaa tai ohjelmiston käyttäjäkokemusta. Tämä tutkimusmenetelmä tarjoaa arvokasta tietoa, jota voidaan hyödyntää prosessien ja ohjelmistotuotteiden parantamiseen. Laadullisen tutkimuksen vahvuutena ohjelmistokehityksessä on sen kyky tarjota syvällistä ja käyttöön perustuvaa tietoa, jota kvantitatiivisilla menetelmillä ei saa. Laadullinen tutkimus tarjoaa ohjelmistokehityksessä näkemyksiä, joita voidaan hyödyntää niin ohjelmistojen käytettävyyden parantamisessa kuin prosessien optimoinnissa.

2.6 Käytettävyyden arviointi

Ohjelmistojen käytettävyyden arviointi on tärkeä osa ohjelmistokehitystä, sillä varmistutaan järjestelmän toimivuudesta ja käyttäjäkokemuksesta. Tässä tutkimuksessa käytettävyyden arviointi toteutettiin heuristisella arvioinnilla, joka on yksi tunnetuimmista ja laajimmin käytetyistä käytettävyysarviointimenetelmistä. (Marjaranta P 2015) Heuristinen arviointi on erityisen tehokas silloin, kun käytettävyyttä halutaan analysoida nopeasti ilman käyttäjätestauksesta aiheutuvia resurssikustannuksia. Heuristinen arviointi perustuu joukkoon ennalta määriteltyjä käytettävyyden periaatteita eli heuristiikkoja. Näitä periaatteita sovelletaan arvioidessa järjestelmän käyttöliittymää ja käyttäjävuorovaikutusta. Tämän tutkimuksen arvioinnissa hyödynnettiin Jakob Nielsenin kehittämää heuristiikkalistaa, joka on yksi yleisimmin käytetyistä viitekehyksistä. Nielsenin heuristiikat tarjoavat systemaattisen lähestymistavan käytettävyysongelmien tunnistamiseen ja auttavat löytämään ratkaisuja järjestelmän käytettävyyden parantamiseksi. (Nielsen J 2024.)

1. Järjestelmän ja käyttäjän vuorovaikutus tulisi olla yksinkertaista
2. Järjestelmän tulisi käyttää käyttäjän kieltä
3. Esittää asiat näytöllä niin, että käyttäjän ei tarvitse muistella niitä
4. Järjestelmän tulee olla yhdenmukainen
5. Pyrkiä estämään virheenmahdollisuuksia
6. Tukea oikoteitä, tehokasta työskentelyä ja räätälöintiä
7. Pyrkiä esteettiseen ja minimalistiseen suunnitteluun
8. Auttaa käyttäjää tunnistamaan virheet ja ymmärtämään niitä

9. Tarjolla tulisi olla hyvä opastus ja dokumentaatiot
10. Järjestelmän tulisi tukea käyttäjän hallintaa ja vapauuta

2.6.1 Järjestelmän ja käyttäjän vuorovaikutus tulisi olla yksinkertaista

Järjestelmän tulisi tarjota käyttäjän tarvitsema tieto oikea aikaisesti ja selkeästi ilmoitettuna. Ylimääräiset asiat näytöllä lisäävät opettelun tarvetta ja mahdollistaa väärin ymmärryksiä. Aiemmin on tutkittu toteen käyväksi 80/20 sääntö. Sääntö tarkoittaa, että 80 prosenttia käyttäjistä ei tarvitse 20 prosenttia ominaisuuksista, mutta 20 prosenttia käyttäjistä tarvitsee 80 prosenttia ominaisuuksista. (Pirinen T 2021.)

2.6.2 Järjestelmän tulisi käyttää käyttäjän kieltä

Sanasto, jota järjestelmä käyttää tulisi olla ymmärrettävissä myös vähemmän aktiivisten tietokoneiden käyttäjille. Sanastona ei tulisi olla ammattisanastoa tai lyhenteitä. Järjestelmässä tulisi asiat esittää niin että käyttäjä on hankkinut tämän tuotteet eikä niin että edustajat ovat myyneet tämän tuotteen. Järjestelmässä olisi myös hyvä käyttää positiivia ilmauksia negatiivisten sijaan. Tutkimusten mukaan positiivinen ilmaisu jää paremmin mieleen. (Pirinen T 2021.)

2.6.3 Esittää asiat näytöllä niin, että käyttäjän ei tarvitse muistella niitä

Järjestelmää käytettäessä käyttäjän muistin käyttö tulisi olla mahdollisimman matalaa. Järjestelmän toiminnot, kohteet ja eri vaihtoehdot tulisi olla selkäesti näkyvillä. Järjestelmän käyttöohjeet tulisi olla vähintään helposti saatavilla käyttöön. (Pirinen T. 2021.)

2.6.4 Järjestelmän tulee olla yhdenmukainen

Käyttäjälle pitäisi olla selkeää mitä eri termit, tilanteet tapahtumat tarkoittavat ohjelmistossa. Ohjelmistossa tulisi noudattaa vakioituneita käytäntöjä esimerkiksi peruuta näppäin aina samalla kodalla ohjelmistossa. Käyttäjän ei pitäisi tarvita opetella ohjelmiston käyttöä ulkoa, vaan sen tulisi toimia johdonmukaisesti. (Pirinen T 2021.)

2.6.5 Pyrkiä estämään virheenmahdollisuuksia

Järjestelmän tulisi antaa virheilmoituksia käyttäjälle. Ohjelman tulisi poistaa väärät arvot automaattisesti tai ilmoittaa vääristä arvoista käyttäjälle. Usein virheet johtuvat käyttäjän huolimattomuudesta. (Pirinen T 2021.)

2.6.6 Tukea oikoteitä, tehokasta työskentelyä ja räätälöintiä

Uudelle käyttäjälle tulisi ohjelman käyttö olla helppoa ja kokenut käyttäjän pitäisi päästä suorittamaan tarvitsemansa toiminnot nopeasti. Tämä tarkoittaa sitä, että ohjelman ympäristö tulisi olla muokattavissa tai tarjota oikoreittejä, että kokeneet käyttäjät voivat tehostaa omaa käyttöään. (Pirinen T 2021.)

2.6.7 Pyrkiä esteettiseen ja minimalistiseen suunnitteluun

Ohjelmassa ei tulisi olla tietoa, jota käyttäjä tarvitsee vain harvoin tai ei ollenkaan. Kaikki ylimääräinen tieto joka näytöllä näkyy, vie huomiota tärkeältä tiedolta ohjelmistosta. Ohjelman sisältö ja teeman tulisi keskittyä olennaiseen ja tukea käyttäjän ohjelmiston käyttöä. (Pirinen T 2021.)

2.6.8 Auttaa käyttäjää tunnistamaan virheet ja ymmärtämään niitä

Ohjelman tulisi ilmoittaa selkeällä ja ymmärrettävällä kielellä käyttäjälle virheilmoitukset. Virheilmoitus ei voi sisältää pelkästään virhekoodeja. Ilmoituksessa olisi hyvä olla ongelma mahdollisimman tarkasti selostettuna ja ongelman ratkaisu ehdotus. (Pirinen T. 2021)

2.6.9 Tarjolla tulisi olla hyvä opastus ja dokumentaatiot

Ohjelmassa olisi hyvä olla ohjattu käyttö ensimmäisellä käynnistys kerralla, jossa käyttäjälle opastetaan ohjelman toiminnot. Käyttöohjeita luetaan harvoin, yleensä ohjelmien kokeileminen tapahtuu yrityksen ja erehdyksen kautta. Ohjelman toiminoissa olisi hyvä olla oikotie käyttöohjeeseen kyseisen toiminnon kohdalle. (Pirinen T 2021.)

2.6.10 Käyttäjän huomioiminen realiajassa

Ohjelman tulisi antaa käyttäjälle reaaliaikaista palautetta esimerkiksi tietojen syöttämisessä välittämöstä mikä tieto on syötetty väärin eikä vasta silloin kun muutettuja tietoja ollaan hyväksymässä. (Pirinen T 2021.)

3 Tietoturvallisuus

3.1 Yleistä

Maailmassa on käynnissä kaksi kilpajuoksua tietoturvallisuuden osalta. Tällä hetkellä käydään jatkuvaa kamppailua kyberpuolustuksen ja -hyökkäyksen välillä. Erityisesti asevoimat ja tietoturvayhtiöt pyrkivät rakentamaan mahdollisimman tehokkaita puolustusmekanismeja, jotta tietojärjestelmät ja erilaiset kybermaailman palvelut olisivat turvallisia. Samanaikaisesti toisella puolella muun muassa kyberrikolliset ja toiset valtiot tekevät jatkuvasti useita hyökkäyksiä puolustajan järjestelmiä vastaan ja pyrkivät löytämään haavoittuvuuksia ja aukkoja puolustuksesta. Hyökkääjän keinot kehittyvät koko ajan monimutkaisemmiksi ja ovelammiksi. Samaan aikaan puolustuksen puolella pyritään tekemään kaikki mahdollinen hyökkääjän onnistumisen estämiseksi (Limnéll, Majewski & Salminen 2014, 36–44.) Tätä taistelua käydään koko ajan, ja jatkuva kilpajuoksu hyökkäyksen ja puolustuksen välillä selittää osaltaan kyberulottuvuuden painoarvon nousua. Kyse on samasta logiikasta kuin on perinteisesti ollut aseiden ja suojien kehityksessä. Esimerkkinä voi käyttää panssarivaunua, joka ensimmäisen kerran ilmestyi taisteluun ensimmäisessä maailmansodassa vuonna 1916. Aluksihan panssarivaunu vaikutti ylivoimaiselta vastustajalta, kunnes keksittiin panssarintorjunta-ase. Tämän jälkeen on käyty jatkuvaa kilpajuoksua panssarivaunun ja panssarintorjunta-aseiden kehityksen välillä edun vaihdellessa molemmin puolin nykypäivään asti.

Tietoturvallisuudessa tavoitellaan kolme pääaihetta, jotka ovat tiedon eheys, luotettavuus ja käytettävyys. Jotta tieto olisi luotettavaa tulee tietoa jakaa vain sitä tarvitsijoille ja tiedon eheys saadaan siitä, kun tietoa pääsee muokkaamaan vain siihen oikeutetut ei kaikki. Käytettävyys edellyttää, että järjestelmiä, ohjelmistoja ja tietoja pääsee oikeudet omaavat hyödyntämään oikea aikaisesti kaikissa mahdollisissa tilanteissa.

3.2 Tekninen tietoturva

Tekninen tietoturva tarkoittaa kaikkia käyttäjän tai järjestelmänvalvojan hankkimia järjestelmiä, ja järjestelmiin tehtyjä ratkaisuja mahdollistan mahdollisimman korkean suojaustason. (Kyberturvallisuusosaamisen perusteita perusopetukseen n.d.) Tekniselle tietoturvalle on asetettu kolme pääaihealuetta laitteisto, ohjelmisto ja toiminta. Laitteisto kategoriaan kuuluvat nimen mukaisesti laitteet eli esimerkiksi palomuuri, salauslaitteet tai vastaavat. Ohjelmisto kategoriaan sisältyy VPN-sovellukset, tietoturvaohjelmistot ja muut vastaavat. Toimintaan sisältyy hallinnollinen tietoturva, jota käsitellään luvussa 2.2. (Jurvanen L 2023.)

3.3 Hallinnollinen tietoturva

Hallinnollinen tietoturva tarkoittaa kaikkia niitä temppuja, joita käyttäjä tekee toteuttaakseen tietoturvaa. Käyttäjä voi esimerkiksi käydä tietoturvallisuuskurssin tai lukea virustorjuntaohjelmiston käyttöohjeet tai tietoturvaohjelmien vertailusta. Kotona yritystä pitävä yrittäjä joka, käyttää työasemaansa yrityksen pyörittämiseen ja perheen vapaa-ajan tarpeisiin on hyvä suunnitella toipuminen, mikäli joutuisi hyökkäyksen kohteeksi. Yrittäjän kannattaa perehtyä työasemansa oikeuksiin ja annettava muille perheen jäsenille vain pienimmät mahdolliset oikeudet. (Hallinnollinen tietoturva – Mitä se on? n.d.)

3.4 Yksityishenkilön tietoturva

Kodeista löytyy nykypäivänä lukuisia laitteita, jotka ovat kytkettynä verkkoon. Toimimalla verkossa huolellisesti ja pitämällä järjestelmät ja sovellukset päivitettynä yksityishenkilö on jo jokseenkin suojassa.

Aina kun käyttää internettiä tai laite on verkossa voi olla tietoverkkorikollisen kohteena. Rikolliset pyrkivät anastamaan kohdehenkilöltä rahaa, identiteettiä tai jotain muuta arvokasta tietoa. Monesti myös kyse on pelkästä häirinnästä. On myös mahdollista, että tietoverkkorikollinen ei ole kiinnostunut yksityishenkilöstä vaan kyseisen henkilön laitteistosta, joita voi hyödyntää esimerkiksi DDoS hyökkäyksessä.

Yksityishenkilö voi nopeasti ajatella, että ei hänellä ole mitään menetettävää. Menetettävää yksityishenkilöllä kuitenkin on esimerkiksi raha, identiteetti, verkkoyhteys, maine tai arkaluontoinen tieto. Rikollinen voi tavoitella rahaa tai luottokortin tietoja, käyttää verkkoyhteyttä rikolliseen toimintaan ja yksityishenkilön nimellä tehdyt rikokset aiheuttavat muita harmeja henkilölle. (Näin pidät huolta tietoturvasta kotona ja työpaikalla 2020.)

Yksityishenkilön kannattaa luoda riittävät pitkiä ja monimutkaisia salasanoja, sekä välttää käyttämästä samoja salasanoja eri palveluissa. Mikäli on mahdollista eri palveluissa niin yksityishenkilön kannatta ottaa käyttöön kaksi- tai monivaiheinen tunnistus. Myös yksityishenkilön kannattaa ottaa varmuuskopiot tärkeimmistä tiedostoistaan esimerkiksi ulkoiselle kovalevylle. Ulkoinen kovalevy, joka sisältää varmuuskopiot on hyvä suojata salasanalla esimerkiksi Windowsin BitLockerilla tai muulla vastaavalla ohjelmistolla ja säilyttää turvallisessa paikassa. Verkossa liikkuminen kannattaa tehdä viisaasti eli mikäli mainos ilmoittaa henkilön voittaneet suuria summia rahaa kyseessä on todennäköisesti huijaus. Erilaisten linkkien ja liitetiedostojen avaamisessa kannattaa edetä harkiten linkit ja tiedostot voivat sisältää haittaohjelmia. (Näin pidät huolta tietoturvasta kotona ja työpaikalla 2020.)

3.5 Yrityksen tietoturva

Niin suurten kuin pienien yritysten tulisi huomioida omassa toiminnassaan tietoturvallisuuden uhkakuva. Yrityksien johto vastaa viime kädessä tietoturvallisuuden toteutuksesta yrityksessä. Tietoturvallisuuden ylläpitämiseen ja varmistamiseen tulisi varata riittävästi resursseja yrityksessä. (Kyberturvallisuus ja yrityksen hallituksen vastuu 2020.)

Yrityksen tulee tarkastella omassa toiminnassaan olevat kriittiset prosessit ja niiden palvelut. Yrityksessä on hyvä olla käytössä ennalta määritelty suunnitelma tietoturvallisuuden häiriötilanteista palautumiseen. Häiriötilanteesta palautumista helpottaa ajantasaiset varmuuskopiot yrityksen kriittisistä materiaaleista ja järjestelmistä. (Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa – Ohje johdolle ja asiantuntijoille 2022.)

Kotikäytössä kuin yrityksessäkin on kannattavaa hyödyntää kaksivaiheista tunnistautumista kirjautumiseen yrityksen palveluihin. Mikäli yritys ei jostain syystä voisi hyödyntää kaksivaiheista tunnistautumista niin yrityksen olisi hyvä pohtia palveluiden eristämistä julkisesta verkosta ainakin niin, ettei sen suora käyttö olisi mahdollista. Tietoturvapäivityksien ja järjestelmäpäivityksien kanssa ei kannata aikaille, mikäli niittä on saatavilla kannattaa ne asentaa välittömästi. Rikolliset hyödyntävät päätelaitteiden haavoittuvuuksia ja haittaohjelmia tietojen anastamiseen tai muuhun haitalliseen toimintaan. (Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa – Ohje johdolle ja asiantuntijoille 2022.)

Yrityksen kannattaa määritellä omassa verkossaan pakollinen ja normaali verkkoliikenne ja estää palomuurilla tarpeeton liikenne. Julkisesta verkosta pääsy yrityksen verkkoon rikollisten hyödyntämillä tiedonsiirtoprotokollilla tulisi estää, eikä tulisi sallia mitään salaamattomia tai haavoittuvaksi tiedostettuja protokollia. (Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa – Ohje johdolle ja asiantuntijoille 2022.)

Yrityksessä kannattaa suojautua haittaohjelmilta ja varautua palvelunestohyökkäyksiin. Haittaohjelmat ovat suuri riski yritykselle, mikäli niihin ei ole valmistauduttu. Yrityksen työasemissa ja palvelimissa olisi syytä olla haittaohjelman torjunta ohjelmistot. Palvelunestohyökkäyksiä on todella usein nykyaikana. Palvelunestohyökkäys luo ruuhkatilanteen yrityksen palvelimelle ja näin ollen estää palvelimen käytön sitä tarvitsevilta. Palvelunestohyökkäyksien torjuminen on haastavaa, koske se usein vaatii runsaasti asiantuntemusta ja laitteistoa, joita ei ole usein käytettävissä. (Pienyritysten kyberturvallisuusopas 2020.)

Huomioitta ei kannata jättää myös yrityksen pilvipalveluita ja etäyhteyksiä. Yleensä suositellut perusasetukset eivät ole yrityksellä riittäviä, joten yrityksen johdon on varmistuttava tietoturvamääräykset toteutuvat

myös pilvipalveluiden ja etäyhteyksien osalta. (Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa – Ohje johdolle ja asiantuntijoille 2022.)

Yksi tärkeimmistä yrityksen toimenpiteistä tietoturvallisuuden osalta on huolehtia ajantasaisista ja toimivista varmuuskopioista. Varmuuskopioiden avulla yrityksen tulisi pystyä palauttamaan koko tekninen ympäristö. Traficom suosittelee varmuuskopioiden osalta 321-sääntöä, jossa numero kolme tarkoittaa, että tieto on tallennettuna kolmeen eri paikkaan. Numero kaksi taas kertoo, että varmuuskopio tulee olla kahdella eri laitteella tai medialla. Viimeinen numero yksi tarkoittaa, että yksi varmuuskopio olisi täysin erillisessä sijainnissa. (Pienyritysten kyberturvallisuusopas 2020.)

4 Tietoturvaohjelmat

4.1 Yleistä

Tietoturvaohjelmat ovat yksi työaseman peruspilareista. Tietoturvaohjelmat tarkastavat työaseman tiedostoja sekä ohjelmia etsien jotain mikä olisi mahdollisesti haitallista. Tietoturvaohjelmia on lukuisilta eri valmistajilta. Tietoturvaohjelmia on maksullisia- tai ilmaisversioita. Yleensä maksullisissa tietoturvaohjelmissa on huomattavasti laajempi tarjonta ominaisuuksista. Tietoturvaohjelmalla on kaksi toiminta periaatetta tunnistaessaan haittaohjelmia. Virustorjunta toimii työaseman käynnissä olon aikana taustalla ja suorittaa reaaliaikaista skannausta vertaa tiedostoja tunnettuihin viruksiin ja haittaohjelmiin, sekä tutkii tiedostoa mahdollisten tuntemattomien virusten tai haittaohjelmien osalta. Tietoturvaohjelmistolla voi suorittaa myös koko järjestelmän skannauksen, jossa nimen mukaisesti tietoturvaohjelma tutkii työaseman kaikki tiedostot tutkien tiedostot haittaohjelmien ja viruksien varalta. Tietoturvaohjelmistojen haittaohjelmien ja virusten tunnistaminen perustuu alati kasvavaan tietokantaan, joka sisältää tietoja tunnetuista viruksista ja haitta ohjelmista. Mikäli työaseman tiedostoita löytyy tietokannan tietoja vastaa tiedosto, asettaa tietoturvaohjelmisto sen yleensä automaattisesti karanteeniin, jossa käyttäjä voi itse tehdä päätöksen tiedoston säilyttämisestä tai poistamisesta. Joissain tilanteissa tietoturva ohjelmisto voi automaattisesti poistaa kyseisen tiedoston työasemasta.

4.2 F-Secure Total

F-Secure Total on suomalaisen tietoturvayhtiön F-Securen valmistama ohjelmisto. F-Secure Total on palkittu vuonna 2024 parhaan käytettävyyden palkinnolla Windows-luokassa. Total on myös tunnustettu verkkopankkisuojausten testivoittajaksi AVLab Cybersecurity -säätiön testaamana 2024. Total on saanut AV-TEST sertifioinnin Windowsille, Androidille ja Mac OS:lle.

Totalia mainostetaan tietoturvaohjelmistona, joka sisältää kaiken. (F-Secure Total n.d.). Virustorjuntaohjelma pysäyttää haittaohjelmat, totaalilla on voi suojata henkilötiedot verkossa- Pankkitoimintojen suojauksella voi suojella omia rahojaan. VPN lisää yksityisyyttä verkossa. Lapsille on mahdollista asentaa erinäköisiä sääntöjä, sekä monia muita ominaisuuksia.

4.3 Norton 360 Premium

Norton on yhdysvaltalainen tietoturva-alan yritys, joka on valmistanut tietoturvaohjelmia. Norton 360 on palkittu vuonna 2022 parhaasta suojauksesta kyseisenä vuonna ja vuonna 2023 Norton 360 on palkittu vuoden 2023 parhaana kodin haittaohjelmien torjuntaohjelmana. (Norton 360 Premium n.d.)

Premium tarjoaa kattavan monikerroksisen suojan päätelaitteille, sekä varmistaa yksityisyyden esimerkiksi VPN:n avulla. Norton 360 Premiumissa on virustorjuntaohjelmiston reaaliaikainen suojaus verkkouhkia ja henkilökohtaisia sekä raha-asioita koskien. Secure VPN peittää jäljet verkossa ja Password Managerilla onnistuu salasanojen ja luottokorttien sekä muiden tunnistetietojen ylläpito erittäin helposti. Pilvitallennustilaan saa luotua varmuuskopiot tärkeimmistä tiedostotoista. Lapsilukko estää lapsien pääsyn haitallisille sivustoille. SafeCam hälyttää mikä joku yrittää käyttää web-kameraasi ja auttaa estämään sen luvattoman käytön. Dark Web Monitoring valvoo käyttäjän henkilötietoja mahdollisten vuotojen varalta. (Norton 360 Premium n.d.)

4.4 McAfee Total Protection

McAfee on myös yhdysvaltalainen tietoturvayhtiö, joka tuottaa tietoturva-alan palveluita. McAfee Total Protection on vuonna 2021 palkittu parhaasta haittaohjelma suojauksesta. (McAfee Total Protection n.d.)

Total Protection tarjoaa asiakkailleen WebAdvisor verkkosuojauksen, tietokoneen optimoinnin, jonka avulla saa parhaan teho/hyöty suhteen työaseman ja Total Protectin välillä. McAfee SafeFamilyn avulla voi hallinnoida lasten tekemisiä internetissä. Microsoft Outlookille roskapostisuodatin ja virusten torjuntaan takuu. (McAfee Total Protection n.d.)

4.5 Acronis True Image

Acronis on vuonna 2003 Singaporessa perustettu sveitsiläinen teknologiayritys. Vuonna 2003 Arconis julkaisi jo ensimmäisen ohjelmistonsa Acronis True Image 7.0. Acronis-yritys kasvoi ensimmäisinä vuosinaan merkittävästi ja jo vuonna 2005 heidän tuotteitaan oli saatavilla 18 eri maassa. Seuraavana vuonna Acronis

laajentui Euroopan markkinoille. Tänä päivänä Acronis toimii yli 150-maassa ja palvelut ovat saatavilla yli 25 kielellä. (Acronis Cyber Protect n.d.)

Acronis tietoturvaohjelmistojen valttikortti on yhtiön sanomien mukaan varmuuskopioinnissa pilveen ja sen palauttamisessa pilvestä. Acronis kuitenkin tarjoaa pelkän varmuuskopioinnin lisäksi virus- ja haittaohjelman tennistunnista. Acroniseltä löytyy ohjelmistot työasemille, palvelimille tai virtuaalikoneille. (Acronis Cyber Protect n.d.)

5 Haittaohjelmat

5.1 Yleistä

Haittaohjelma on ohjelma, jonka tarkoituksena on jollaintavalla haitata käyttäjän tekemistä. Haitta, jota ohjelmisto tekee voi olla tiedon varastaminen, tiedostojen lukitseminen tai käyttää osana bottiverkkoa. (Millaisia haittaohjelmia on olemassa? n.d.) Haittaohjelmia jaotellaan eri kategorioihin niiden toimintojen ja tyyppien perusteella. (Mikä on haittaohjelma? 2022.).

Haittaohjelmilla on useita eritapoja levitä verkossa. Haittaohjelmat voivat levitä esimerkiksi sähköpostin liitteinä, kannettavien muistivälineiden kautta, tiedostojen lataamisen seurauksena tai esimerkiksi haavoittuvuuksien kautta. (Millaisia haittaohjelmia on olemassa? n.d.)

5.2 Virus

Virus on ohjelma, joka leviää työasemasta toiseen työasemaan ja hankaloittaa toimintaa työasemassa. Viruksella on mahdollisesti kyky poistaa tiedostoja tai estää työasemaa käynnistymästä. Arkikielessä virus toimii yleiskäsitteenä tarunnalle, josta työasema on saastunut, vaikka kyseessä on täysin omanlainen haitallinen ohjelmisto. (Mikä on tietokonevirus? n.d.)

5.3 Troijalainen

Troijalainen perustuu vahvasti kreikkalaisessa mytologiassa esiintyneeseen Troijan lahjahevoseen, jonka seurauksena kreikkalaiset pääsivät hyökkäämään Troijan kaupunkiin, niin myös troijalainen haittaohjelma naamioituu normaaliksi ohjelmistoksi tai tiedostoksi. Troijalainen haittaohjelma varaa saastuneelta työasemalta henkilökohtaisia tietoja, kaappaa työaseman tai vakoilee työasemaa. (Mikä on troijalainen? n.d.)

Remote Access Trojan (RAT) on etähallittava haittaohjelma, joka päästessään kohteeseensa antaa hyökkääjälle työaseman etäkäytön mahdollisuuden. RAT on usein modulaarinen haittaohjelma, joka sisältää useita eri toimintoja, joita hyökkääjä kykenee suorittamaan etäkäytön avustuksella. Check point. Pankkitroijalaisen tarkoitus on anastaa uhrin pankkitiedot hyödyntämällä näppäintallentimia tai hyökkääjä ohjaa uhrin haitalliselle sivustolle. (Zieniūtė U 2023)

Joitakin Troijalaisia voidaan hyödyntää palvelunestohyökkäyksiin (DDoS) eli tartunnan saanut työasema valjastetaan hyökkääjän armeijaan ja armeija hyökkää jonkin yrityksen sivustoille pyrkien kaatamaan sen ja näin ollen aiheuttamaan myös yrityksille jonkin asteisia vahinkoja. (Zieniūtė U 2023)

5.4 Ransomware

Ransomware haittaohjelma salaa työaseman tiedostot ja yleensä vaati uhrilta lunnaita, että tiedostojen lukitus saadaan poistettua. Ransomware on yksi vaarallisimmasta ja nopeasti yleistyvistä uhkista, joka kohdistuu kotikäyttäjiin ja yrityksiin. Ransomwarekin leviää sähköpostin liitetiedostoina, ohjelmistojen oheistuotteena tai verkosta haitallisilta sivustoilta. (Mikä on ransomware? 2022.)

Ransomware haittaohjelmasta on olemassa erimuotoja. Crypto-ransomware lukitsee tiedostot purkuavaimen taakse. Locker-ransomware lukitsee koko työaseman estäen sen käytön. Leak-ransomware uhkailee käyttäjää arkaluontoisten tietojen julkaisulla, ellei käyttäjä sitoudu maksamaan hyökkääjälle tarvittavaa rahasummaa.

5.5 Mato

Tietokone mato toimii itsenäisesti ja kykenee monistamaan itseään ja leviämään työasemasta toiseen hyödyntäen verkkojen ja ohjelmistojen haavoittuvuuksia. Mato on virukseen verrattuna vaarallisempi, koska mato ei tarvitse isäntää toimiakseen.

Madot leviävät yleensä sähköpostien tai pikaviestien mukana. Mato kykenee hyödyntämään tietojärjestelmien haavoittuvuuksia. Mato on mahdollista tunnistaa mikä työasema hidastuu (resurssien suurikäyttö), verkkojakamisen yhteydessä. (Virusten ja muiden haittaohjelmien estäminen ja poistaminen n.d.)

5.6 Mainosohjelma

Mainoshaittaohjelma on helppo tunnistaa moniin muihin haittaohjelmiin verrattuna, koska mainoshaittaohjelma esittää erilaisia mainoksia tai ponnahdusikkunoita käyttäjän työasemalla näin ollen selkeästi esillä. Mainoshaittaohjelma leviää usein haitallisten ohjelmistojen oheistuotteena tai hyväksyessä käyttöehtoja, joita ei ole lukenut riittävällä tarkkuudella. (Mikä on haittaohjelma? n.d)

Joitakin mainoshaittaohjelmia voidaan verrata luvun 4.2 troijalaisiin, koska mainoshaittaohjelmatkin kykenevät tekeytymään laillisiksi ohjelmistoiksi. Haittaohjelman laatijat kykenevät toimittamaan haittaohjelmia myös haavoituksia hyödyntämällä.

Mainosohjelma ei varsinaisesti ole haittaohjelma, mutta mainosohjelmatkin voivat heikentää tietoturvaa merkittävästi. On esimerkiksi olemassa mainosohjelmia, jotka suorittavat datavarkauksia keräten käyttäjästä ja käyttäjän toiminnasta teettäjä. Mainosohjelmien laillisuus on usein perusteltuna siihen, että käyttäjä on itse hyväksynyt käyttöehdoissa mainosohjelman asentamisen ja sitä myöten mainosten esittämisen. (What is Adware? n.d.)

5.7 Vakoiluohjelma

Vakoiluohjelma on mahdollista asentaa työasemaan käyttäjän huomaamatta. Ohjelmien tarkoituksena on kerätä käyttäjästä henkilökohtaisia ja muita tietoja esimerkiksi verkkovierailut. (Virusten ja muiden haittaohjelmien estäminen ja poistaminen n.d.)

Yleensä vakoiluohjelmien varastamat tiedot ovat pankkitietoja tai käyttäjätunnuksia ja salasanoja, näiden avulla hyökkääjät kykenevät ottamaan käyttäjän tilejä haltuun tai suorittamaan identiteettivarkauksia.

Vakoiluohjelman voi asentaa kaikkiin laitteisiin. Vakoiluohjelma ei välitä onko kyseessä Tietokone, tabletti tai puhelin. Vakoiluohjelmalle ei ole edes merkitystä onko kyseessä Windows tietokone, Android-tabletti tai Apple iOS puhelin. (Kuinka yksityisyyttä uhkaavan vakoiluohjelman voi tunnistaa? n.d.)

6 Tietoverkkorikollisuus

6.1 Tietoverkkorikollisuuden kehitys

Tietoverkkorikollisuuden luonne ja olosuhteet erottuvat monilta osin perinteisempään rikollisuuteen verrattuna. Tietoverkkorikollisuuden muotoja on useita erilaisia esimerkiksi palvelunestohyökkäykset, urkinta, vakoilu, laiton lataaminen, tietojen kalastelu (phishing) ja identiteettivarkaudet (Rousku 2014). Nämä ovat joitakin termejä, joihin törmäämme nykyisin lähes päivittäin uutisoinnissa. Tietotekniikan kehityksen mukana myös rikokset ovat kehittyneet ja monipuolistuneet. Tietoverkkorikosten kehittyminen ja niihin reagoiminen lainsäädännön keinoin voidaan jakaa neljään vaiheeseen.

Ensimmäinen vaihe sijoittuu 1940-luvun lopusta 1960-luvun loppuun. Tämä ajanjakso on tietoverkkorikollisuuden syntyhetki. Tällä ajan jaksolla oli tyypillistä tietokonekeskuksissa olleiden suurikokoisten tietokoneiden fyysinen vahingoittaminen. Kyseiseen aikaan ei vielä ollut tarvetta säätää omaa, vaan rikoksiin sovellettiin muita rikosnimikkeitä, kuten petosta (Peltomäki & Norppa 2014, 6-23.)

Toinen vaihe alkoi 1970-luvulta ja jatkui 1980-luvun lopulle. Tämä on se ajanjakso, jolloin tietoverkkorikosten katsotaan kehittyneen. Tällä ajan jaksolla alkoivat lainsäätäjätkin säätämään omia lakipykäliä tietoverkkorikollisuuteen. (Peltomäki & Norppa 2014, 6-23.)

Kolmas vaihe sijoittuu 1990-luvulle, jolloin internetin käyttö yleistyi ja oli monessa kotitaloudessakin käytössä. Se mahdollisti entistä monipuolisemmat mahdollisuudet tehdä rikoksia. Alussa kyse oli pääsääntöisesti roskapostiviesteistä ja harrastelijahakkereiden kokeiluista. Tässä vaiheessa tietokonerikoksia ryhdyttiin kriminalisoimaan aiempaa tehokkaammin eli säädettiin lakeja erillisistä tietoverkkorikoksista. Myös Suomessa rikoslakia muutettiin, ja sen 38 luvusta tuli nimeltään tieto- ja viestintärikokset (Peltomäki & Norppa 2014, 6-23.)

Viimeisin vaihe on alkanut vuoden 2000 läheisyydessä, jolloin tietoverkkorikollisuus oli jo jokapäiväistä. Vuosina 2002–2004 ilmestyivät ensimmäiset haittaohjelmat, joilla rikolliset saivat saaliiksi rahaa. Aluksi ne olivat yksinkertaisia sähköposteihin roskapostia lähettäviä ohjelmia, joilla vastaanottajan tietokone saatiin kaapattua haltuun, jotta sitä puolestaan voitiin käyttää roskapostin lähettämiseen edelleen (Peltomäki & Norppa 2014, 6-23.)

6.2 Tietoverkkorikollisuus nyt

Poliisi lajittelee tietoverkkorikokset kahteen eri kategoriaan tietoverkkoympäristöön kohdistuviin ja tietoverkkoja hyödyntäen tehtyihin rikoksiin mitkä kykenevät olemaan minkälaisia rikoksia tahansa, jotka on tehty tietoverkkoja hyödyntämällä.

Vuosien 2019 sekä 2023 välillä tietoverkkorikoksiin kuuluvia rikosnimikkeitä ilmoitettiin poliisille yhteensä 25 586 kappaletta. Lukua suurentaa myös merkittävästi Vastaamon tietomurrosta nostetut törkeän tietomurron syytteet noin 14 000 kappaletta. Vaikka Vastaamon tietomurto nostaa Poliisille ilmoitettujen rikosten määrää niin todellisuudessa luku voisi olla paljon suurempikin, mikäli kaikki rikokset olisivat tulleet poliisin tietoon. Vuosien 2019–2023 välillä erityisesti tietosuojarikoksien määrä on nousussa, ja tietomurtojen määrän nousu on ollut tasaista. (Poliisin tietoon tulleet rikokset rikosryhmittäin ja -nimikkeittäin poliisilaitoksittain 2025)

Tietoverkko rikokset ja -rikollisia eivät maarajat pidättele, usein tietoverkkorikoksia tekevät joukot ovat kansainvälisiä porukoita, joissa esiintyy myös suomalaisia henkilöitä.

Suuressa mittakaavassa tietoverkkorikollisuus on nykypäivänä ammattimaista sekä järjestäytynyttä rikollisuutta. Tästä syystä heidän on mahdollista kehittää rikollista toimintaansa siinä missä hyvien puolen ammattilaiset yrittävät kehittää parempaa tietoturvaa.

Tieto- ja viestintärikoksista Poliisin rekisteröimät henkilöt ovat yleensä noin 30-vuotiaita miehiä. Poliisi on myös rekisteröinyt 12-vuotiaita ja yli 60-vuotiaita rikoksen tekijöitä. (Jämsén C 2020.)

Taulukko 1. Poliisille ilmoitetut rikokset

Poliisille ilmoitetut rikokset	2019	2020	2021	2022	2023
TIETOJÄRJESTELMÄN HÄIRINNÄN YRITYS	0	0	1	1	0
TIETOJÄRJESTELMÄN HÄIRINTÄ	9	16	33	37	59
TIETOLIIKENTEEN HÄIRINNÄN YRITYS	1	3	2	0	1
TIETOLIIKENTEEN HÄIRINTÄ	41	72	116	106	76
TIETOLIIKENTEEN LIEVÄN HÄIRINNÄN YRITYS	0	0	0	1	0
TIETOMURRON YRITYS	16	67	58	37	46
TIETOMURTO	804	1 107	1 525	1 891	2 144
TIETOSUOJARIKOS	58	99	328	139	732
TIETOSUOJARIKOS (Å)	0	0	1	0	0
TIETOVERKKORIKOSVÄLINEEN HALLUSSAPITO	5	2	2	1	2
TÖRKEÄ TIETOJÄRJESTELMÄN HÄIRINTÄ	6	6	4	4	1
TÖRKEÄ TIETOLIIKENTEEN HÄIRINTÄ	8	7	2	1	4
TÖRKEÄ TIETOMURTO	6	16	9	11	14 171
VIESTINTÄSALAISUUDEN LOUKKAUKSEN YRITYS	0	2	2	1	2
VIESTINTÄSALAISUUDEN LOUKKAUS	264	327	240	215	216
SALASSAPITORIKKOMUS	23	25	18	18	21
SALASSAPITORIKOS	57	67	45	63	85

6.3 Lain kohdat

6.3.1 Tietojärjestelmän häirintä

Tietojärjestelmän häirinnällä tarkoitetaan esimerkiksi palvelunestohyökkäyksiä, jotka voivat ilmetä eri tasoisina rikoksina eli tietojärjestelmän häirintänä ja sen törkeänä tekomuotona. Rikoslain 38 luvun 7a pykälässä on säädetty tietojärjestelmän häirintää ja se määrittelee, että jos tietoliikenteen häirinnästä aiheutuva haitta on kokonaisuudessaan vähäinen, voidaan tekijä tuomita lievästä tietoliikenteen häirinnästä sakkoon. Tietojärjestelmän häirinnässä myös häirinnän yritys on rangaistavaa. (Rikoslaki 89/1889 7a §.)

Törkeästä tietojärjestelmän häirinnästä säädetään rikoslain 38 luvun 7b §:ssä, siinä määritellään rikoksen vakavuuden perusteet, joilla teko luokitellaan törkeäksi.

1. Tietojärjestelmän häirintä on törkeä, mikäli aiheutetaan merkittävää haittaa tai taloudellisia tappioita,
2. rikos toteutetaan erityisen suunnitelmallisesti,
3. rikoksen yhteydessä hyödynnetään merkittävää määrää tietojärjestelmiä käyttäen haittaohjelmia tai luvattomia pääsytietoja eli hyödynnetään bottiverkkoa,
4. rikos on osa järjestäytyneen rikollisryhmän toimintaa,
5. rikos kohdistuu kriittiseen tietojärjestelmään, jonka vahingoittaminen vaarantaisi yhteiskunnan keskeisiä toimintoja, kuten energian tuotantoa tai terveydenhuoltoa.

Jos rikos täyttää jonkin näistä tai häirintä on kokonaisuudessaan arvostellen törkeä, voidaan tekijä tuomita törkeästä tietojärjestelmän häirinnästä vankeuteen vähintään neljäksi vuodeksi ja korkeintaan viideksi vuodeksi vankeuteen. Tässäkin yrityskin on rangaistava. (Rikoslaki 89/1889 7b §.)

6.4 Tietoliikenteen häirintä

Tietoliikenteen häirintä tarkoittaa muun muassa sitä, että henkilö oikeudettomasti puuttuu postin, teleliikenteen tai radioviestinnän toimintaan. Tämä voi tapahtua esimerkiksi häiritsemällä viestintälaitteiden toimintaa, lähettämällä tahallaan häiritseviä viestejä televerkon tai radiolaitteen kautta tai muuten estämällä viestintää. Tällaisesta toiminnasta voidaan tuomita sakkoon tai enintään kahden vuoden vankeuteen. (Rikoslaki 89/1889 5 §.)

Mikäli häiriö on kokonaisuudessaan arvioituna vähäinen – esimerkiksi aiheutuneen vahingon laadun tai määrän perusteella – voidaan tekijä tuomita lievästä tietoliikenteen häirinnästä sakkoon.

Törkeä tietoliikenteen häirintä puolestaan toteutuu seuraavissa tilanteissa:

1. Tekijä käyttää rikoksen tekemisessä hyväkseen asemaansa teleyrityksessä, kaapelilähetyksiä tarjoavassa laitoksessa tai yleisradiotoimintaa harjoittavassa yrityksessä, tai hänellä on muuten erityinen luottamusasema.
2. Rikos kohdistuu hätäkutsujen radioviestinnän tai muun ihmishenkiä turvaavan viestinnän estämiseen tai häiritsemiseen.
3. Rikos on osa toimintaa, jossa käytetään laitteita, ohjelmia tai käyttäjätunnuksia vaikuttaen laajasti tietojärjestelmiin
4. rikos tehdään osana järjestäytynyttä rikollisuutta.
5. Rikos aiheuttaa huomattavaa haittaa tai taloudellista vahinkoa.
6. Rikoksen kohteena tietojärjestelmä, viestintä tai laite, jonka vahingoittaminen voisi vaarantaa kriittisiä yhteiskunnallisia toiminta kuten esimerkiksi terveyden huollon tai maanpuolustuksen.

Jos rikos jonkin edellä mainituista kriteereistä ja kokonaisuutta arvioiden törkeä voidaan rikoksen tekijä tuomita törkeästä tietoliikenteen häirinnästä vähintään neljäksi kuukaudeksi ja enintään viideksi vuodeksi vankeuteen. (Rikoslaki 89/1889 6 §.)

6.4.1 **Tietomurto**

Tietomurto on järjestelmään, palveluun tai laitteeseen luvatonta tunkeutumista tai käyttöönottoa. Rikoslain 38 luvun 8 $:ssä säädetään tietomurrosta Se, joka käyttämällä hänelle kuulumatonta käyttäjätunnusta taikka turvajärjestelyn muuten murtamalla oikeudettomasti tunkeutuu tietojärjestelmään, jossa sähköisesti tai muulla vastaavalla teknisellä keinolla käsitellään, varastoidaan tai siirretään tietoja tai dataa, taikka sellaisen järjestelmän erikseen suojattuun osaan, on tuomittava tietomurrosta sakkoon tai vankeuteen. (Rikoslaki 89/1889 8 §.)

Tietomurto tapoja on kahdenlaisia. Tietomurrot on eroteltu tunkeutumalla tehtyyn tietomurtoon, jossa hyökkääjä tunkeutuu kohde järjestelmään hyödyntäen anastettuja käyttäjätunnuksia esimerkiksi. Toinen tietomurto tyyli on tunkeutumatta tehty tietomurto, jossa hyökkääjä anastaa kohde järjestelmästä tiedot, datan vastaavan jollain erikoislaitteella ohittaa tietoturvajärjestelyt (Rikoslaki 89/1889 8 §.)

6.4.2 Tietosuojarikos

Rikoslain luku 38 pykälässä yhdeksän käsitellään tilanteita, joissa rekisterinpitäjänä toimiva yritys tai organisaatio tai muu käsittelijä rikkoo tietosuoja-asetuksen tai siihen liittyvien säännöksiä ja aiheuttaa näin ollen vahinkoa henkilön yksityisyydelle. (Rikoslaki 89/1889 9 §.)

Yleensä tietosuojarikos tapahtuu, jos henkilötietojen käsittelijä toimii tahallisesti tai törkeästä huolimattomuudesta, ja käsittelee henkilötietoja tavalla, joka on vastoin tietosuojasäädöksiä. Tämä tarkoittaa esimerkiksi sitä, että henkilötietoja hankitaan, käytetään, luovutetaan tai siirretään tavalla, joka ei ole yhteensopiva niiden alkuperäisen käyttötarkoituksen kanssa tai on muuten vastoin tietosuojasäädöksiä. (Rikoslaki 89/1889 9 §.)

Lainsäädännössä viitataan neljään keskeiseen säädökseen, joiden rikkominen voi johtaa tietosuojarikokseen

1. Yleinen tietosuoja-asetus (EU 2016/679), joka on Euroopan unionin asettama laaja sääntely henkilötietojen käsittelystä ja yksityisyydensuojan turvaamisesta.
2. Tietosuojalaki (1050/2018), joka täydentää ja tarkentaa EU tietosuoja-asetusta Suomessa.
3. Henkilötietojen käsittelystä rikosasioissa ja kansallisen turvallisuuden ylläpitämisen yhteydessä annettu laki (1054/2018), joka koskee henkilötietojen käsittelyä erityisesti rikosoikeudellisissa ja turvallisuuteen liittyvissä yhteyksissä.
4. Muut henkilötietojen käsittelyä koskevat lait, jotka voivat sisältää erityisiä säädöksiä, esimerkiksi tietyille toimialoille tai tiettyihin tarkoituksiin liittyen

Jos näiden säädösten vastainen toiminta johtaa siihen, että rekisteröidyn (eli henkilön, jonka tietoja käsitellään) yksityisyyttä loukataan, tai hänelle aiheutuu muuta vahinkoa tai olennaista haittaa, kyseessä on tietosuojarikos. Tämä voi tarkoittaa esimerkiksi henkilön tietojen joutumista vääriin käsiin, tai henkilötietojen käyttämistä tavalla, joka vaarantaa hänen oikeutensa. Lisäksi rikos tapahtuu myös silloin, jos henkilötietojen käsittelyn turvallisuudesta ei huolehdita asianmukaisesti. Tietoturvallisuudella tarkoitetaan sitä, että henkilötietojen käsittely tapahtuu suojatussa ympäristössä ja riskejä vastaan suojautuen, jotta tietojen luvaton käyttö tai vuotaminen estetään. Tietosuojarikoksesta voi seurata rangaistus, joka voi olla sakkoa tai enintään vuoden vankeusrangaistus. (Rikoslaki 89/1889 9 §.)

6.4.3 Viestintäsalaisuuden loukkaus

Rikoslain luku 38 pykälässä 3 säädetään rangaistuksesta, kun henkilö oikeudettomasti hankkii tiedon toisen henkilön viestinnästä. Viestintäsalaisuudella tarkoitetaan erityisesti kirjeiden, sähköisten viestien tai muiden vastaavien viestien luottamuksellisuutta. (Rikoslaki 89/1889 3 §.)

Viestintäsalaisuuden loukkaus voi tapahtua kahdella eri tavalla:

1. Kirjeen tai viestin avaaminen eli jos henkilö avaa toisen henkilön kirjeen tai muun suljetun viestin ilman lupaa, se katsotaan viestintäsalaisuuden loukkaukseksi. Tämä koskee myös sähköisiä viestejä, kuten sähköpostia, jos suojauksen murtaen hankitaan tieto viestistä.
2. Tietojen hankkiminen televerkosta eli jos henkilö hankkii luvattomasti tietoja televerkossa tai tietojärjestelmässä välitettävien viestien, kuten puhelujen, tekstiviestien tai datasiirron sisällöstä. Tämä koskee myös tietoja viestin lähettämisestä tai vastaanottamisesta.

Rangaistuksena tästä rikoksesta voi seurata sakkoja tai enintään kahden vuoden vankeus. Tämän lisäksi myös rikoksen yritys on rangaistava, mikä tarkoittaa, että jo pelkkä yritys päästä luvattomasti käsiksi toisen viestintään on rangaistava teko. (Rikoslaki 89/1889 3 §.)

6.4.4 Salassapitorikkomus ja -rikos

Salassapitorikkomus on lievempi muoto salassapitorikoksesta. Siihen syyllistytään silloin, kun salassapitorikos on kokonaisuutena arvioituna vähäinen. Tämä tarkoittaa, että rikoksen vaikutus yksityisyyden tai luottamuksellisuuden suojaan on vähäinen, eikä teko ole yhtä vakava kuin varsinaisessa salassapitorikoksessa. Arvioinnissa otetaan huomioon teon seuraukset ja konteksti: esimerkiksi paljastetun tiedon merkittävyys ja se, kuinka laajalle tietoja on levitetty. (Rikoslaki 89/1889 2 §.)

Salassapitorikkomukseen voi syyllistyä, jos henkilö tahattomasti tai pienellä huolimattomuudella paljastaa salassa pidettävän tiedon, mutta teolla ei ole ollut vakavia seurauksia. Esimerkiksi jos tieto päätyy vahingossa väärään paikkaan, mutta sitä ei käytetä väärin tai se ei aiheuta suurta haittaa, teko saatetaan katsoa salassapitorikkomukseksi. (Rikoslaki 89/1889 2 §.)

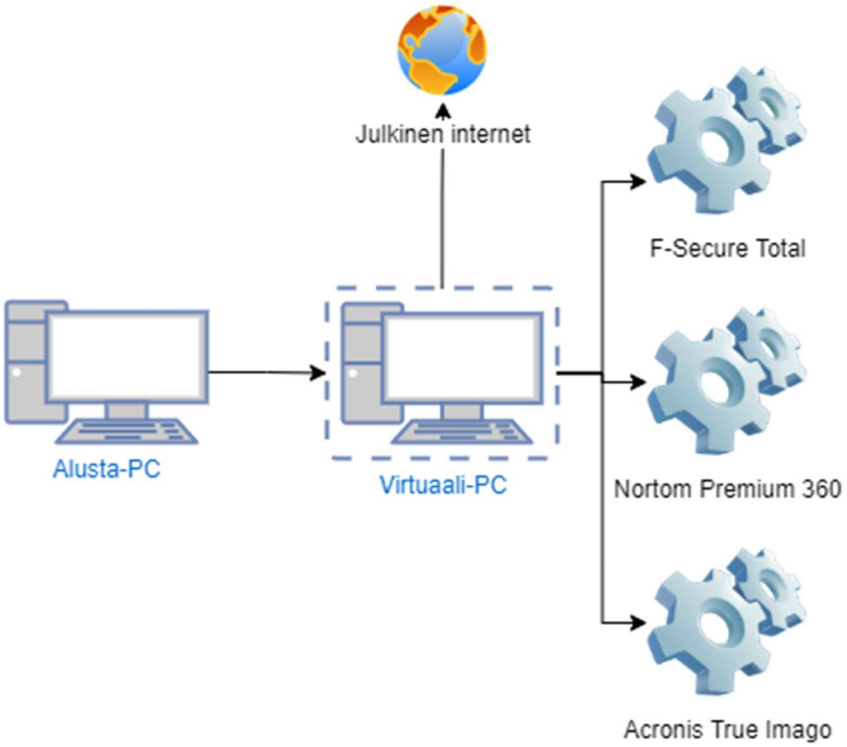
Rikkomus voi olla kyseessä silloin, kun teko on nimenomaisesti säädetty salassapitorikkomuksena rangaistavaksi laissa. Tämä tarkoittaa, että joissakin tapauksissa lainsäädäntö erikseen määrittelee, milloin salassapitovelvollisuuden rikkominen katsotaan rikkomukseksi eikä rikokseksi. Salassapitorikkomuksesta seuraa yleensä sakko, mutta ei vankeusrangaistusta koska teko on lievempi kuin salassapitorikos. (Rikoslaki 89/1889 2 §.)

Salassapitorikoksessa tai -rikkomuksessa on kyse tilanteesta, jossa henkilö rikkoo luottamuksellisten tietojen käsittelyyn liittyviä velvollisuuksia. Rikoksen vakavuus määritellään sen perusteella, kuinka merkittävää tieto on ja miten vakavat seuraukset teolla on ollut. Vakavammasta salassapitorikoksesta voidaan tuomita vankeuteen, kun taas lievemmästä salassapitorikkomuksesta selvitään yleensä sakolla. (Rikoslaki 89/1889 1 §.)

7 Testaamisen toteutus

7.1 Ympäristö

Tietoturvaohjelmistojen testauksen keskeisimpänä tarkoituksena on testata ohjelmistojen käytettävyys, tietokoneen resurssien käyttöä ja sekä se, että havaitseeko tietoturvaohjelmistot testihaittaohjelmia. Haittaohjelmat, joita testauksessa käytetään ovat European Institute for Computer Antivirus Research (EICAR) organisaation valmistamia testitiedostoja, joilla testasin, että tietoturvaohjelmisto toimii oikein. Testauksessa käytin myös ennalta ladattua haittaohjelmia sisältävää tiedostopakettia. Haittaohjelmapaketti sisältää 20 eri haittaohjelmaa esimerkiksi memz, vine memz, wannacry ja petya.



Kuvio 2 Testaus ympäristö

Vertailussa käytettävä tietokone on Oracle VirtualBox virtualisointi ohjelmaan asennettu Windows 10 käyttöjärjestelmällä oleva virtuaalinen tietokone. Virtualisoidulle koneelle on annettu käytettäväksi 80Gt kiintolevy tilaa, 8Gt keskusmuistia ja 4 suoritinta käyttöön prosessorilta. Virtuaalikoneelle vastaa perustietokonetta komponenteiltaan. Virtualisointi ohjelman käyttö tietoturvaohjelmistojen testaamisessa on turvallista suorittaa eikä fyysisen tietokoneen mikä sisältää VirtualBox ohjelmiston pitäisi olla alttiina haittaohjelmatartunnalle.

8 Vertailu

8.1 F-Secure Total

F-Securen ilmaisen testiversion käyttöönotto tapahtui F-Securen verkkosivuilta kokeile ilmaiseksi painiketta painamalla. Ohjelmistoa otettaessa kokeilun tulee henkilötietojen lisäksi ilmoittaa, kuinka mahdollinen tuleva maksu veloitetaan eli mikäli testaaja ei muista perua tilausta veloittaa F-Secure automaattisesti sovitun lisenssin hinnan. Testikappaleen oston jälkeen F-Secure pyytää luoman My F-Secure tilin, jonka kautta voi hallinnoida omia tilauksiaan sekä suojattuja laitteitaan. My F-Securesta löytyy kohta lisää laite, josta pääsee vasta lataamaan F-Securen tietoturvaohjelmiston laitteelle. F-Securen prosessorin käyttö oli hyvin maltillista 0–2 % prosentin välillä testauksen aikana. Muistin käyttö oli F-Securen ohjelmalla 75–80 Mt ja tausta sovelluksilla noin 10 Mt. Skannauksen aikana F-Securen Scan Wizard ohjelmisto käytti prosessoria 2–5 % prosentin verran ja muisti 60–65 Mt. Tarkistuksen kesto F-Securella oli kaksi minuuttia ja 24 sekuntia, jonka aikana F-Secure tarkisti 56544 tiedostoa.

F-Securen toiminta ennen haittaohjelmapaketin latausta todettiin EICAR:in testi haittaohjelmilla. EICAR:ilta testaukseen otettiin kaksi erillistä .zip päätteistä pakattua tiedostoa ja yksi tekstitiedosto, joka sisälsi niin sanotusti haitallista tekstiä. F-Secure ei havainnut pakattuja tiedostoja pikatarkistuksella, mutta laajalla tarkistuksella tunnisti pakatut tiedostot haitallisiksi. Tekstitiedoston F-Securen reaaliaikainen seuranta asetti välittömästi luomisen jälkeen karanteeniin. Haittaohjelmapaketin lataamisen jälkeen suoritettu tarkistus ei havainnut kuin 2 haitallista ohjelmaa 16 ohjelmasta. Haittaohjelmat olivat salasanasuojattuja ja F-Secure jätti ne siitä syystä tarkistamatta. Haittaohjelmien salasanalla avaamisen jälkeen reaaliaikainen suojaus asetti ohjelmat välittömästi karanteeniin.

8.2 Käytettävyyden arviointi F-Secure Total

F-Secure Total pyrkii tarjoamaan yksinkertaisen ja käyttäjäystävällisen käyttöliittymän. Ohjelmiston päänäkymä on selkeä ja keskeiset toiminnot kuten virustarkistus ja VPN:n aktivointi ovat helposti löydettävissä.

Joidenkin lisäominaisuuksien kuten salasanojen hallinnan löytäminen vaatii useamman navigointivaiheen, mikä saattaa hämmentää ensikäyttäjiä.

Ohjelmisto käyttää selkeää ja ymmärrettävää kieltä, joka on tuettuna hyvin eri kielille mukaan lukien suomi. Tekninen terminologia on pääosin vältetty, mutta jotkin termit, kuten "firewall" tai "kill switch" voivat olla vähemmän tuttuja vähemmän kokeneille käyttäjille. Ohjelmiston päänäkymä tarjoaa kaikki keskeiset toiminnot helposti saataville, joten käyttäjän ei tarvitse muistaa monimutkaisia komentoja tai navigointipolkuja. Ohjelma käyttää myös visuaalisia ikoneja, jotka helpottavat toimintojen tunnistamista. Käyttöliittymässä voisi kuitenkin parantaa sitä, miten eri asetusten vaikutukset kuvataan käyttäjälle. F-Secure Total on yhdenmukainen graafisen suunnittelun ja käytettävyyden osalta. Eri ominaisuudet, kuten VPN ja virustorjunta, jakavat samanlaisen visuaalisen ilmeen ja käyttölogiikan. Tämä vähentää oppimiskäyrää, kun käyttäjä tutustuu ohjelman eri osioihin.

Ohjelma estää tehokkaasti virheitä selkeillä vahvistusviesteillä esimerkiksi ennen asetusten tallentamista tai tarkistuksen aloittamista. Käyttäjälle tarjotaan myös oletusasetuksia, jotka minimoivat tarpeen tehdä riskialttiita manuaalisia muutoksia. Ohjelma tukee räätälöintiä hyvin esimerkiksi VPN:n asetusten ja salasanojen hallinnan osalta. Edistyneet käyttäjät voivat säätää tietoturva-asetuksia tarkemmin, mutta oikopolut kuten pikanäppäinten käyttö tai personoidut työtilat eivät ole kovin kattavasti tuettuja. Ohjelma antaa selkeitä ilmoituksia virheistä, kuten internet-yhteyden puuttumisesta VPN:n yhteyden aikana. Virheilmoitukset ovat yleensä informatiivisia ja sisältävät ohjeet ongelman ratkaisemiseksi. Kehitysalueena voisi olla entistä tarkemmat syy-seuraussuhteiden selitykset teknisissä ongelmissa.

F-Secure Total tarjoaa kattavat ohjeet ja tuen verkkosivustonsa ja ohjelmiston sisäisten ohjetoimintojen kautta. Useimmille käyttäjille ohjeet ovat riittävät, mutta osa asetuksista, kuten VPN:n ja virustorjunnan edistyneet toiminnot voisi käyttäjä hyötyä ohjeista suoraan käyttöliittymässä. Ohjelmisto antaa käyttäjälle hallinnan useimmista toiminnoista. Käyttäjä voi esimerkiksi päättää mitä tarkistuksia suoritetaan tai missä VPN-yhteys muodostetaan. Ohjelma tukee myös "peruuta"- ja "muokkaa"-vaihtoehtoja useimmissa asetuksissa, mutta käyttöliittymä ei kaikissa tilanteissa tue toimintojen nopeaa peruuttamista.

8.3 Norton 360 Premium

Nortonin ilmaisen testiversion käyttöönotto tapahtui Nortonin verkkosivuilta ”Aloita” painiketta painamalla. Ohjelmistoa otettaessa kokeilun tulee henkilötietojen lisäksi ilmoittaa, kuinka mahdollinen tuleva

maksu veloitetaan eli mikäli testaaja ei muista perua tilausta veloittaa Nortonin automaattisesti sovitun lisenssin hinnan. Nortonin ilmainen kokeilujakso on 14 vuorokautta eli noin puolet F-Securen tarjoamasta 30 päivän kokeilusta. Oston jälkeen varsinaisen asennustiedoston lataaminen alkaa automaattisesti. Nortonin prosessorin käyttö oli kohtalaista 0–24 % prosentin välillä testauksen aikana. Muistin käyttö oli Nortonin ohjelmalla ja taustalla olevilla Nortonin oheissovelluksilla oli 356.2 Mt. Tarkistuksen kesto Nortonilla oli seitsemän minuuttia ja 29 sekuntia, jonka aikana Norton tarkisti 292069 tiedostoa. Nortnilla hyvää oli se, että skannauksen pystyi aloittamaan heti ohjelman etusivulta.

Nortnin toiminta ennen haittaohjelmapaketin latausta todettiin EICAR:in testi haittaohjelmilla. EICAR:ilta testaukseen otettiin kaksi erillistä .zip päätteistä pakattua tiedostoa ja yksi tekstitiedosto, joka sisälsi niin sanotusti haitallista tekstiä. Norton ei havainnut pakattuja tiedostoja älykkäällä tarkistuksellaan eikä myöskään pikatarkistuksella. Haittaohjelmapaketin lataamisen esti Nortnin selaimen suojaus, vastaavaa toimintoa ei ollut F-Securella. Haittaohjelmapaketin lataamisen jälkeen avaamisen jälkeen Nortonin pikatarkistus havaitsi haittaohjelmia 12/16.

8.4 Käytettävyyden arviointi Norton 360 Premium

Norton 360 Premium tarjoaa selkeän ja suoraviivaisen käyttöliittymän, jossa päätoiminnot, kuten virustarkistus ja VPN ovat helposti löydettävissä heti aloitusikkunasta. Ohjelmiston kotinäkymä antaa nopean yleiskuvan suojaustilasta.

Norton 360 käyttää selkeää ja ymmärrettävää kieltä ja ohjelmisto on saatavilla useilla kielillä myös suomeksi. Teknistä terminologiaa on pyritty minimoimaan, mutta osa termistöstä, kuten "karanteeni" tai "VPN-tunneli" voivat olla vaikeasti ymmärrettävissä kokemattomille käyttäjille. Ohjelmiston käyttöliittymä esittää keskeiset tiedot ja asetukset näytöllä siten, että käyttäjän ei tarvitse muistaa aiempia vaiheita.

Toiminnot kuten virustarkistus on yksinkertaistettu niin, että käyttäjä voi suorittaa tarkistuksen yhdellä painikkeella. Joissakin tapauksissa kuten pilvivarmuuskopioinnin asetuksissa käyttäjä joutuu kuitenkin muistamaan tarkempia valintojaan. Norton 360 Premium on yhdenmukainen graafisen käyttöliittymän ja toimintalogiikan osalta. Kaikki ominaisuudet kuten salasanojen hallinta ja palomuuri seuraavat samanlaista käyttölogiikkaa. Ohjelmisto pyrkii tehokkaasti ehkäisemään virheitä tarjoamalla oletusasetuksia, jotka sopivat useimmille käyttäjille. Esimerkiksi automaattiset päivitykset ja haittaohjelmien torjunta ovat oletusarvoisesti päällä, mikä minimoi käyttäjän tekemien virheiden riskin.

Edistyneille käyttäjille Norton 360 tarjoaa mahdollisuuden räätälöidä asetuksia kuten palomuurin sääntöjä ja tarkistusten aikataulutusta. Kuitenkin oikopolut kuten pikanäppäimet tai personoidut työtila, ovat ohjelmistossa melko rajallisia. Ohjelmiston käyttöliittymä on visuaalisesti miellyttävä ja minimalistinen. Näytöllä ei esitetä liikaa tietoa, ja värikoodit kuten vihreä (suojaus kunnossa) ja punainen (ongelma) helpottavat tilan arviointia yhdellä silmäyksellä. Joissakin asetuksissa on kuitenkin runsaasti valintoja mikä saattaa kuormittaa käyttäjää.

Norton 360 Premium tarjoaa selkeitä ilmoituksia, kun suojaus ei ole ajan tasalla tai jokin asetus vaatii käyttäjän huomiota. Virheilmoitukset sisältävät usein ratkaisuja mutta teknisemmät ongelmatilanteet voisivat sisältää vielä enemmän taustatietoa ja ohjeita. Ohjelmiston sisäinen ohje ja Nortonin verkkosivustolla oleva tuki ovat kattavia. Useimpiin ongelmatilanteisiin löytyy ratkaisu ohjedokumentaatiosta. Kohdistetut ohjeet käyttöliittymässä voisi kuitenkin parantaa käyttäjän oppimiskokemusta esimerkiksi asetusten selityksillä suoraan ohjelmistossa. Norton 360 antaa käyttäjälle vapauden hallita ohjelman toimintoja, kuten mitä tiedostoja tarkistetaan tai mitkä ohjelmat saavat yhteyden internetiin. Käyttäjä voi myös helposti peruuttaa tai muokata asetuksia. Joidenkin toimintojen kuten automaattisten toimintojen keskeyttäminen voi kuitenkin vaatia enemmän navigointia.

8.5 Acronis True Image

Acronis True Imagen ilmaisen testiversion käyttöönotto tapahtui Acronisin verkkosivuilta tilaamalla kokeiluversion asennustiedostoon johtava linkki omaan sähköpostiin. Sähköpostissa oli linkin Windows ja Applen Mac OSx asennuksille. Asennuksen valmistuttua Acronis aloittaa ohjatun käytönopastuksen sovelluksessaan. Acronis tarjoaa 30 päivän kokeilun ohjelmistolleen. Acroniksen prosessorin käyttö oli kohtalaista 0–20 % prosentin välillä testauksen aikana. Muistin käyttö oli Acronis ohjelmalla ja taustalla olevill oheissovelluksilla oli 282.3 Mt. Tarkistuksen kesto Acronisilla oli 55 minuuttia ja 27 sekuntia, jonka aikana Acronis tarkisti 230563 tiedostoa. Acronisin valttikortti näiden kolmen ohjelman kesken on varmuuskopiointi. Varmuuskopioinnille on mahdollista asettaa useita eri asetuksia. Tässä opinnäytetyössä ei sen tarkemmin perehdytty varmuuskopiointeihin.

Acronisin toiminta ennen haittaohjelmapaketin latausta todettiin EICAR:in testi haittaohjelmilla. EICAR:ilta testaukseen otettiin kaksi erillistä .zip päätteistä pakattua tiedostoa ja yksi tekstitiedosto, joka sisälsi niin sanotusti haitallista tekstiä. Acronis havaitsitsi pakatut tiedot tarkistuksellaan. Haittaohjelmapaketin lataamisen jälkeen ja salasanalla avaamisen jälkeen Acronisin tarkistus havaitsi haittaohjelmia 15/16.

8.6 Käytettävyyden arviointi Acronis True Image

Acronis True Image tarjoaa selkeän ja hyvin jäsennellyn käyttöliittymän, jossa päätoiminnot kuten varmuuskopiointi, palautus ja synkronointi, ovat helposti löydettävissä. Kuitenkin monimutkaisten ominaisuuksien kuten pilvivarmuuskopioinnin ja edistyneiden aikataulutusasetusten käyttö voi vaatia enemmän opettelua.

Ohjelmisto käyttää selkeää ja helposti ymmärrettävää kieltä, joka sopii sekä teknisesti vähemmän taitaville käyttäjille että asiantuntijoille. Osa termeistä, kuten "cloning" voi olla vaikeasti ymmärrettävä henkilöille, joilla ei ole aikaisempaa kokemusta tietojen suojaamisesta. Ohjelmisto esittää käyttäjälle tärkeät tiedot kuten viimeisimmät varmuuskopiot ja niiden tilan suoraan päänäkymässä. Käyttöliittymä varmistaa, että käyttäjän ei tarvitse muistaa monimutkaisia komentoja. Joissain tilanteissa esimerkiksi asetusten muokkaamisen yhteydessä käyttäjän täytyy kuitenkin siirtyä useamman valikkorakenteen kautta, mikä voi lisätä kognitiivista kuormitusta.

Acronis True Image on visuaalisesti ja toiminnallisesti yhdenmukainen. Sen eri osiot kuten paikallinen varmuuskopiointi ja pilvipalvelut käyttävät samanlaista käyttölogiikan. Tämä parantaa käyttäjäkokemusta sillä eri ominaisuuksiin siirtyminen ei edellytä uuden toimintalogiikan oppimista. Ohjelma sisältää useita toimintoja, jotka ehkäisevät virheitä kuten oletusasetuksia ja automaattisia tarkistuksia ennen varmuuskopioinnin suorittamista. Kuitenkin edistyneiden asetusten käyttö voi johtaa virheisiin, jos käyttäjä ei täysin ymmärrä esimerkiksi varmuuskopiointityypin tai aikataulun vaikutuksia. Ohjelma mahdollistaa monipuoliset räätälöintimahdollisuudet kuten varmuuskopiointien mukauttamisen ja synkronointiasetusten hallinnan.

Acronis True Image hyödyntää modernia ja selkeää käyttöliittymää, joka välttää turhaa informaatiota. Näytöllä esitettävät tiedot ovat relevantteja ja hyvin järjestettyjä. Monimutkaiset valikkorakenteet ja asetukset voivat ajoittain luoda tunteen siitä, että ohjelma on suunnattu enemmän teknisesti edistyneille käyttäjille. Ohjelma antaa selkeitä virheilmoituksia esimerkiksi epäonnistuneista varmuuskopioinneista. Virheilmoitukset sisältävät myös tietoa ongelman mahdollisista syistä ja ratkaisuista. Tietyissä tilanteissa viestit voisivat kuitenkin olla käyttäjäystävällisempiä, erityisesti teknisiä termejä välttämällä. Acronis tarjoaa laajan tuen verkkosivustonsa kautta esimerkiksi ohjeita, usein kysyttyjä kysymyksiä ja käyttäjäfoorumeita. Ohjelmisto sisältää myös ohjetoiminnon, mutta sen tarjoamat tiedot eivät aina ole riittävän kohdistettuja, jolloin käyttäjä saattaa joutua etsimään vastauksia ulkopuolisista lähteistä. Acronis True Image tarjoaa käyttäjälle mahdollisuuden hallita varmuuskopiointiprosesseja ja mukauttaa niitä tarpeidensa mukaan. Esimerkiksi käyttäjä voi valita tiedostot ja kansiot, jotka varmuuskopioidaan, sekä aikatauluttaa prosessit. Ohjelmisto tukee myös useimpien toimintojen perumista, mikä lisää hallinnan tunnetta.

8.7 Tulokset

Testaustoiminnan perusteella resurssien käytön puolesta ehdottomasti F-Secure oli paras. F-Securen ohjelmisto on optimoitu erinomaisesti, jotta vähäisellä muistin ja prosessorin käytöllä onnistuu tietoturvan suojaaminen. Acronisilla oli loistavat varmuuskopiointi ominaisuudet haittaohjelma tunnistusten lisäksi. joten tätä ohjelmistoa tai tämän valmistajan ohjelmistoja voisi suositella yrittäjille, joille ajantasaiset varmuuskopiot ovat elinehto. Kotikäyttöön voi suositella F-Secure vähäisten resurssien käytönpuolesta, jottei tietoturvaohjelmisto haukkaa suurinta osaa käytettävissä olevista resursseista.

Alla oleva taulukko havainnollistaa valittujen tietoturvaohjelmien suorituskykyä eri osa-alueilla testitulosten perusteella:

Taulukko 2. Ohjelmistojen suorituskyky

Ohjelmisto	**Skannausnopeus (min)**	**CPU-käyttö (%)**	**Muistinkulutus (MB)**	**Haittaohjelmien tunnistus (%)**
F-Secure Total	2:24	0–5	75–80	100
Norton 360 Premium	1:45	0–24	100–120	90
Acronis True Image	3:10	0–20	90–110	95

Tiedot perustuvat testauksessa käytettyihin EICAR-tiedostoihin ja valmiiksi ladattuun haittaohjelmapakettiin.

Alla oleva taulukko tiivistää tietoturvaohjelmien ominaisuudet eri näkökulmista:

Taulukko 3. Ohjelmistojen ominaisuudet

Ohjelmisto	Käyttöliittymän selkeys	Suorituskyky	Haittaohjelmien torjunta	Lisäominaisuudet	Hintataso (€)
F-Secure Total	Helppokäyttöinen	Erinomainen	Tehokas	VPN, salasanojen hallinta	69,99/vuosi
Norton 360 Premium	Käyttäjäystävällinen	Hyvä	Tehokas	Pilvivarmuuskopiointi, SafeCam, VPN	89,99/vuosi
Acronis True Image	Monimutkainen	Kohtalainen	Hyvä	Varmuuskopiointi, tietoturvaominaisuudet	79,99/vuosi

Käytettävyyden osalta ohjelmistot olivat suhteellisen samankaltaisia. Erovaisuuksia ohjelmistojen välillä oli esimerkiksi kohdan 6.1.2 mukaisessa heuristiikassa ”Järjestelmän tulisi käyttää käyttäjän kieltä”. Nortonilla oli eniten sanoja, jotka eivät välttämättä heti aukea tietokonetta vähemmän käyttäneelle henkilölle. Toki tässä tulee huomioida, että näistäkin suurin osa sijaitsi ohjelmiston asetuksissa. Seuraavat heuristiikan mukaiset kohdat, joissa tuli erovaisuuksia olivat 6.1.4 ja 6.1.5. Acronis suoriutui näistä kohdista heikoiten, koska vaikka ohjelmistolle oli alussa hyvä käytönopastus alussa nii silti käyttäjälle jää jonkin verran ulkoa muistettavaa sekä painikkeiden paikat vaihtelivat hieman sovelluksen eri ikkunoissa. Virheilmoitukset olisivat voineet olla käyttäjäystävällisempiä välttämällä teknisiä termejä. Kohdassa 6.1.7 heuristiikan ”Pyrkiä esteettiseen ja minimaaliseen suunnitteluun” Acronisilla ohjelmisto sisälsi myös ohjetoiminnon, mutta sen tarjoamat tiedot eivät aina olleet riittävän kohdistettuja, jolloin on mahdollista, että tietoa tullaan etsimään ulkoisista lähteistä.

Taulukko 4. Käytettävyyden arvioinnin pisteet

Nimi	Heuristiikka										
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**Pisteet KA**
	F-Secure	4	5	5	5	5	3	5	4	4	4	4,4
	Norton	4	4	5	5	5	3	5	4	4	4	4,3
	Acronis	4	5	5	4	4	3	4	4	4	4	4,1

Analyysin perusteella **Norton 360 Premium** tarjoaa parhaan suojan haittaohjelmia vastaan ja kattavat lisäominaisuudet, mutta sen resurssikulutus on suurempi. **F-Secure Total** on kevyt ja helppokäyttöinen, mutta sen haittaohjelmien torjuntakyky on hieman heikompi. **Acronis True Image** sopii parhaiten käyttäjille, jotka arvostavat varmuuskopiointia tietoturvan rinnalla.

Käyttäjäprofiilien suositukset testauksen perusteella:

- **Peruskäyttäjä**: F-Secure Total (yksinkertainen ja kevyt)
- **Tehokäyttäjä/yritykset**: Norton 360 Premium (laajin suojaus)
- **Yrittäjät ja yritykset**: Acronis True Image (parhaat varmuuskopiointiominaisuudet)

9 Yhteenveto

9.1 Laatu ja luotettavuus

Tulosten laatu ja luotettavuus perustuvat systemaattiseen testaamiseen, jossa ohjelmisto testattiin samoissa olosuhteissa ja samoilla menetelmillä. Testauksen suoritusympäristö oli vakio, jotta ulkoiset muuttujat eivät päässeet vaikuttamaan tuloksiin.

Työn tuloksia voi hyödyntää yksityishenkilöt, IT-alan ammattilaiset sekä pienet yritykset. Opinnäytetyön perusteella he voivat suoraan valita itselleen sopivan ohjelmiston tai suorittaa oman testaamisen eri tietoturvaohjelmistoilla, että löytyisi heille paras mahdollinen ohjelmisto.

Tietoturvaohjelmistojen suurin testaaja on AV-TEST, joka arvioi tietoturvaohjelmistoja eri käyttöjärjestelmille. Viimeisin AV-TEST-raportti osoitti, että Norton 360 sai hieman korkeammat pisteet järjestelmän suorituskyvyn kuormittamisesta ja haittaohjelmien havaitsemisessa. Käytettävyydessä AV-TEST oli arvioinut molemmat F-Secure Totalin ja Norton 360 saman tasoisiksi. (The best Windows antivirus software for home users).

Opinnäytetyön tulokset vahvistavat AV-TEST:in havainnot. F-Secure Total on kevyt ohjelmisto, joka tarjoaa kattavan suojan, sekä Norton 360 Premium tarjoaa vahvan suojauksen mutta saattaa hidastaa järjestelmän toimintaa. Acronis True Imagen testaus tulosta ei löytynyt AV-TEST:iltä, mutta F-Securen ja Nortonin samankaltaisuuksien osalta voi luottaa myös Acroniksen testauksen onnistuneen.

Heuristisen arvioinnin etuna oli sen tehokkuus ja resurssien vähäinen tarve, koska menetelmä ei vaadi käyttäjätestausta. Tämä tekee siitä nopean ja kustannustehokkaan vaihtoehdon käytettävyyden arviointiin. Nielsenin heuristiikat tarjosivat laajan ja kattavan viitekehyksen, joka soveltui tietoruvaohjelmistoihin kohtalaisesti. Menetelmän rajoituksena oli kuitenkin se, että arviointi perustuu yksittäisen tekijän näkemykseen. Se voi johtaa siihen, että osa todellisista käytettävyysongelmista jäi huomaamatta. Käyttäjien todellisten kokemusten ja ongelmien syvälliseen ymmärtämiseen heuristinen arviointi ei yksin riitä vaan sitä voisi täydentää esimerkiksi käyttäjätestauksella tai käyttäjähaastatteluilla. Tässä tutkimuksessa heuristinen arviointi osoittautui riittävän toimivaksi keinoksi tunnistaa ohjelmiston käytettävyyden vahvuuksia ja heikkouksia. Tulosten perusteella olisi mahdollista antaa suosituksia järjestelmän jatkokehitykseen, jotka tukevat käyttäjäkokemuksen parantamista ja käytettävyyden optimointia.

9.2 Pohdinta

Tämä opinnäytetyö osoitti, tietoturvaohjelmistojen välillä on eroja käytettävyyden, suorituskyvyn ja haittaohjelmien tunnistuksen tehokkuuden osalta. Vaikka kaikki kolme testattavaa tarjosivat kattavan suojan ja paljon ominaisuuksia niin suurelta osin käyttäjän tarpeet vaikuttavat siihen mikä ohjelmisto on sopivin.

Testauksen toteutustapa oli onnistunut, sillä käytetty heuristinen arviointi ja tunnetut haittohjelmat mahdollistivat testauksen samankaltaisuuden jokaisella ohjelmalla. Virtuaalikoneen hyödyntäminen varmisti, että testitulokset ovat toistettavissa ja suorituskykyä oli mahdollista arvioida tasapuolisesti.

Työn rajoituksena voisi pitää testattavien ohjelmistojen vähäistä määrää. Markkinoilla on kymmeniä muita tietoturvaohjelmistoja, mutta ennen testausta tulisi selvittää lisenssitiedot ja käyttöehdot. Useammalla testattavalla ohjelmalla olisi mahdollista saada laajempi käsitys ohjelmistojen vahvuuksista ja heikkouksista sekä eroavaisuuksista. Testausta olisi mahdollista laajentaa tietoturvaohjelmistojen reaktiokykyyn reaaliaikaisissa uhkatilanteissa sekä reagointia uusiin uhkiin.

Jatkossa tutkimusta voisi laajentaa esimerkiksi enemmän yritysmaailmaan suunnatulla tietoturvatutkimuksella tai mobiililaitteiden tietoturvaohjelmistojen vertailulla. Mahdollista olisi lisätä tutkimiskohteeksi koneoppimiseen ja tekoälyyn perustuvien tietoturvaratkaisujen vaikutus tietoturvallisuuteen.

Lähteet

Acronis Cyber Protect. N.d. Ohjelmiston esittely Acronisin verkkosivustolla. Viitattu 27.8.2024. https://www.acronis.com/en-eu/products/cyber-protect/

Eskola, J & Suoranta J. 1998. Johdatus laadulliseen tutkimukseen. Tampere: Vastapaino Oy.

F-Secure Total. N.d. Ohjelmiston esittely F-Securen verkkosivustolla. Viitattu 27.8.2024. https://www.f-secure.com/fi/total

Hallinnollinen tietoturva – Mitä se on? N.d. Artikkeli 2NS verkkosivustolla. Viitattu 22.8.2024. https://www.2ns.fi/hallinnollinen-tietoturva-mita-se-on/

Huijarit kaappaavat pankkitunnuksia Omakannan ja Suomi.fi-palvelun nimissä. 2021. Varoitus kyberturvallisuuskeskuksen sivustolla. Viitattu 30.8.2024. https://www.kyberturvallisuuskeskus.fi/fi/huijarit-kaappaavat-pankkitunnuksia-omakannan-ja-suomifi-palvelun-nimissa

Jurvanen L. 2023. Mitä tarkoittaa tekninen tietoturva? Savelan 29.12.2023. Viitattu 22.8.2024 https://www.savelan.fi/mita-tarkoittaa-tekninen-tietoturva/

Jämsén C. 2020. Tietoverkkorikollisuus poliisin silmin. Viitattu 9.2.2025. https://poliisi.fi/-/tietoverkkorikollisuus-poliisin-silmin

Kuinka yksityisyyttä uhkaavan vakoiluohjelman voi tunnistaa? N.d. Artikkeli Kaspersky sivustolla. Viitattu 2.9.2024. https://www.kaspersky.fi/resource-center/threats/how-to-detect-spyware

Kyberturvallisuuden vahvistaminen suomalaisissa organisaatioissa – Ohje johdolle ja asiantuntijoille. 2022. Julkaisu Kyberturvallisuuskeskuksen sivustolla. Viitattu 10.9.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Kyberturvallisuuden_vahvistaminen_suomalaisissa_organisaatiossa_-_ohje_johdolle_ja_asiantuntijoille.pdf

Kyberturvallisuus ja yrityksen hallituksen vastuu. 2020. Julkaisu Kyberturvallisuuskeskuksen sivustolla. Viitattu 10.9.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Kyberturvallisuusosaamisen perusteita perusopetukseen. N.d. Opetushallituksen verkkosivusto. Viitattu 20.8.2024. https://www.oph.fi/fi/digiosaaminen/kyberturvallisuusosaamisen-perusteita-perusopetukseen/tekninen-tietoturva

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo.

Marjaranta P. 2015. Heuristinen arviointi. Viitattu 11.12.2024. https://kurssit.it.jyu.fi/TJTA104/kalvot/tjta104_majaranta_heuristinen_evaluointi.pdf

McAfee Total Protection. N.d. Ohjelmiston esittely McAfeen verkkosivustolla. Viitattu 25.8.2024. https://www.mcafee.com/fi-fi/antivirus/mcafee-total-protection.html

Mikä on haittaohjelma? 2022. Artikkeli F-Securen sivustolla. Viitattu 2.10.2024. https://www.f-secure.com/fi/articles/what-is-malware

Mikä on ransomware? 2022. Artikkeli F-Secure sivustolla. F-Secure 28.3.2022. Viitattu 5.10.2024. https://www.f-secure.com/fi/articles/what-is-a-ransomware-attack

Mikä on tietokonevirus? N.d. Artikkeli F-Securen sivustolla. Viitattu 16.9.2024. https://www.f-secure.com/fi/articles/what-is-a-computer-virus

Mikä on troijalainen? N.d. Artikkeli F-Securen sivustolla. Viitattu 4.9.2024. https://www.f-secure.com/fi/articles/what-is-a-trojan

Millaisia haittaohjelmia on olemassa? N.d. Julkaisu Kasperskyn verkkosivustolla. Viitattu 2.10.2024. https://www.kaspersky.fi/resource-center/threats/types-of-malware

Nielsen J. 2024. 10 Usability Heuristics for User Interface Design. Viitattu 11.12.2024. https://www.nngroup.com/articles/ten-usability-heuristics/

Norton 360 Premium. N.d. Ohjelmiston esittely Nortonin verkkosivustolla. Viitattu 28.8.2024. https://fi.norton.com/products/norton-360-premium#

Näin pidät huolta tietoturvasta kotona ja työpaikalla. 2020. Artikkeli Kyberturvallisuuskeskuksen verkkosivustolla. Viitattu 26.8.2024. https://www.kyberturvallisuuskeskus.fi/fi/ajankohtaista/ohjeet-ja-oppaat/nain-pidat-huolta-tietoturvasta-kotona-ja-tyopaikalla

Peltomäki, J & Norppa, K. 2015. Rikos meni verkkoon. Helsinki: Talentum.

Pienyritysten kyberturvallisuusopas. 2020. Julkaisu Kyberturvallisuuskeskuksen sivustolla. Viitattu 11.9.2024. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf

Pirinen T. 2021. Nielsenin 10 heuristiikkaa avattuna. Viitattu 10.12.2024. https://teemupirinen.wordpress.com/2021/04/10/nielsenin-10-heuristiikkaa-avattuna-2/

Poliisin tietoon tulleet rikokset rikosryhmittäin ja -nimikkeittäin poliisilaitoksittain. 2025. Viitattu 9.2.2025. https://poliisi.fi/documents/25235045/31329635/Rikostilasto-nimikkeet-fi.xlsx/c851f983-0f65-fe68-fcff-4678e5b5545d?t=1737041449577

Rikoslaki 89/1889. Rikoslaki. Annettu 1.1.1889. Viim. muutos 1.1.2025. Viitattu 2.11.2024. https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001?search%5Btype%5D=pika&search%5Bpika%5D=Rikoslaki

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

The best Windows antivirus software for home users. 2024. AV-TEST julkaisu tietoturvaohjelmistojen vertailusta. Viitattu 12.3.2025. https://www.av-test.org/en/antivirus/home-windows/

Virusten ja muiden haittaohjelmien estäminen ja poistaminen. N.d. Ohje Microsoftin sivustolla. Viitattu 1.10.2024. https://support.microsoft.com/fi-fi/topic/virusten-ja-muiden-haittaohjelmien-est%C3%A4minen-ja-poistaminen-53dc9904-0baf-5150-6e9a-e6a8d6fa0cb5

What is A Trojan Horse?. N.d. Artikkeli Check Point verkkosivustolla. 7.9.2024. https://www.check-point.com/cyber-hub/cyber-security/what-is-trojan/

What is Adware?. N.d. Artikkeli Check Point sivustolla. Viitattu 10.9.2024. https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-adware/

Zieniūtė U. 2023. Mikä on troijalainen virus?. NordVPN 3.9.2023. Viitattu 11.9.2024. https://nordvpn.com/fi/blog/troijalainen-virus/?srsltid=AfmBOoqyXrfgoseD4qGTWd1iPd4HP1rpJaBKsE9PJcZq0ZTsi1zVKCU0