jamk.fi

Tietoturva työmatkoilla

Lassi Markkola

Opinnäytetyö
Toukokuu 2020
Tekniikan ala
Insinööri (AMK), Tieto- ja viestintätekniikka

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Markkola, Lassi	Opinnäytetyö, AMK	Toukokuu 2020
	Sivumäärä 55	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Tietoturva työmatkoilla

Tutkinto-ohjelma
Tieto- ja viestintätekniikka

Työn ohjaaja(t)
Juha Piispanen, Jarmo Viinikanoja

Toimeksiantaja(t)
CYBERDI-projekti/JAMK

Tiivistelmä

CYBERDI on Jyväskylän ammattikorkeakoulun ja Poliisiammattikorkeakoulun yhteistyöprojekti, jonka tavoitteena on lisätä kansalaisten tietoisuutta kyberrikollisuudesta. Opinnäytetyön tavoitteena oli tutkia, mitä uhkia työntekijän ja yrityksen dataan kohdistuu työmatkoilla ja miten näiltä voidaan suojautua.

Opinnäytetyö toteutettiin käyttämällä kvalitatiivista eli laadullista tutkimusmenetelmää. Aineistona käytettiin verkkojulkaisuja, kuten uutisartikkeleita ja blogikirjoituksia. Opinnäytetyössä käytiin läpi monia datan uhkatekijöitä, minkä jälkeen perehdyttiin niiden suojautumiskeinoihin käytännön testejä apuna käyttäen. Opinnäytetyössä käytetyt suojautumiskeinot ovat ohjelmistopohjaisia ratkaisuja. Käytännön testejä varten valittiin yksi ohjelmisto, jonka ominaisuudet esiteltiin ja testattiin.

Tuloksena todettiin työmatkailun lisäävän yrityksen tietoturvariskiä, mutta oikeilla ja hyvin toteutetuilla suojautumiskeinoilla riskien uhka ja niiden vaikutukset voidaan minimoida. Nykyaikaisten suojautumiskeinojen havaittiin olevan helppoja käyttöönottaa kehittyneen pilviteknologian ansiosta.

Yritykset omistavat paljon arkaluontoista dataa, joka kulkiessaan työntekijöiden kannettavissa ympäri maailmaa altistuu useille vaaratilanteille. Lisääntyvien uhkatekijöiden ja tietoturvamurtojen vuoksi toivottavaa olisi saada myös pienemmät yritykset heräämään taisteluun kyberrikollisuutta vastaan ja ryhtymään suojelemaan dataansa asianmukaisilla keinoilla.

Avainsanat (asiasanat)
tietoturva, työmatka, uhkatekijä, salaus, avoin verkko

Muut tiedot (Salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Markkola, Lassi	Bachelor's thesis	May 2020
	Number of pages 55	Language of publication: Finnish
		Permission for web publication: x

Title of publication
Information security on business travels

Degree programme
Information and Communication Technology

Supervisor(s)
Piispanen Juha, Viinikanoja Jarmo

Assigned by
CYBERDI project/JAMK

Abstract

CYBERDI is a collaboration project between JAMK University of Applied Sciences and Police University College. Their mission is to increase citizens' awareness of cybercrimes. The Thesis aims to research what threatens employees' and their company's data on business travels and how to protect the data from these threats.

The Thesis research method was qualitative. The used material consisted of Internet publications such as news articles and blog posts. The thesis covered many different threats to data and ways to be protected from them with the help of hands-on tests. The used protection methods were software-based. One software solution was selected to be tested and reviewed on the hands-on tests.

The result was that business travels increase the risks for company's data; however, with the right tools and implementations the risks can be reduced to minimal. Modern solutions for data protection were found to be easy to use and implement thanks to advanced cloud technology.

Companies own a great amount of sensitive data that travels on employee's laptops across the world while being exposed to countless risks. Due to constantly increasing number of threat factors and ongoing hacking, small businesses are also recommended to join the fight against cybercrimes and protect their own data with appropriate methods.

Keywords (subjects)
information security, business travel, threat, encryption, open network, hacking

Miscellaneous (Confidential information)

Sisältö

Terminologia **6**

1 Johdanto **7**

2 Tutkimusasetelma **7**

2.1 Tutkimuskysymys 7

2.2 Tutkimusmenetelmä 8

3 Taustaa **8**

3.1 Uhkatekijät 8

3.1.1 Yleistä 8

3.1.2 Avoin WiFi 8

3.1.3 Haittaohjelmat 9

3.1.4 Fyysinen uhka 11

3.1.5 Suojautumiskeinot 11

3.2 VPN 12

3.2.1 Yleistä 12

3.2.2 Turvallisuus 12

3.2.3 Yksityisyys 12

3.2.4 Vapaus 13

3.2.5 Miten VPN toimii 13

3.2.6 VPN yrityksessä 14

3.2.7 Yleisimmät VPN-protokollat 14

3.3 VPN-vaihtoehtoja 17

3.3.1 Yleistä 17

3.3.2 NordVPN 19

3.3.3 CyberGhost VPN 21

3.4 Haittaohjelmien torjunta 22

3.4.1 Yleistä 22

3.4.2 Bitdefender 23

3.5 Varmuuskopiointi 25

3.5.1 Yleistä 25

3.5.2 Ulkoinen kiintolevy 25
3.5.3 Pilvipalvelu 26
3.6 Varmuuskopiointikeinoja 27
3.6.1 Yleistä 27
3.6.2 Veeam 28
3.7 Tiedostojen salaus 28
3.7.1 Yleistä 28
3.8 Levyn salausohjelmia 30
3.8.1 Yleistä 30
3.8.2 Bitlocker 30

4 Testaukset 31
4.1 VPN testaukset 31
4.1.1 Yleistä 31
4.1.2 CyberGhost VPN-ohjelmisto 31
4.2 Haittaohjelmasuojauksien testaus 36
4.2.1 Yleistä 36
4.2.2 Bitdefender 37
4.3 Varmuuskopioinnin testit 42
4.3.1 Yleistä 42
4.3.2 Veeam 42
4.4 Levyn salausohjelmistojen testaus 46
4.4.1 Yleistä 46
4.4.2 Bitlocker 46

5 Yhteenveto 48

6 Pohdinta 49

Lähteet 51

Liitteet 55
Liite 1. Bitlockerin käyttöönotto ilman TPM:ää 55

Kuviot

Kuvio 1. CyberGhostin verkkosivujen yläpalkki 32

Kuvio 2. VPN-yhteys muodostettu 32

Kuvio 3. Yhteyden ominaisuuksia 33

Kuvio 4. Yleiset asetukset 34

Kuvio 5. Palvelinluettelo 35

Kuvio 6. Virtuaalikoneella normaalinopeudet 35

Kuvio 7. Bitdefender Central 37

Kuvio 8. Bitdefenderin aloitusnäkymä 38

Kuvio 9. Bitdefenderin suojausvälilehti 39

Kuvio 10. Bitdefenderin yksityisyysvälilehti 41

Kuvio 11. Skannauksien tulokset 42

Kuvio 12. Veeam agentti 43

Kuvio 13. Veeam aikataulutus 44

Kuvio 14. Suoritetut varmuuskopioinnit 45

Kuvio 15. Bitlockerin tila 47

Terminologia

AES	Advanced Encryption Standard, standardoitu salausmenetelmä
FVEY	The Five Eyes, tiedustelutietoja jakava liittouma
GFW	The Great Firewall of China, Kiinan palomuuri
HTTPS	Hypertext Transfer Protocol Secure, suojattu verkkoviestintäprotokolla
IP	Internet Protocol address, verkkolaitteet yksilöivä IP-osoite
MITM	Man-in-the-middle attack, tietoturvahyökkäys
NAS	Network Attached Storage, verkkokiintolevy
RSA	Julkisen avaimen salausmenetelmä
TCP	Transmission Control Protocol, tietoliikenneprotokolla
TLS	Transport Layer Security, salausprotokolla
TPM	Trusted Platform Module, emolevyn turvapiiri
UDP	User Datagram Protocol, yhteydetön tietoliikenneprotokolla
VPN	Virtual Private Network, virtuaalinen erillisverkko
WLAN	Wireless Local Area Network, langaton lähiverkko

1 Johdanto

Monissa työpaikoissa työhön sisältyy paljon matkustelua kuten toimipisteiden välillä liikkumista, asiakkaiden luokse menoa tai jopa ulkomaille matkustamista. Näitä kaikkia matkoja yhdistää yksi asia: mukana oleva kannettava tietokone. Nykyään lähes kaikilla työmatkoilla on tarve käyttää tietokonetta ja päästä käsiksi yrityksen arkaluontoisiin tiedostoihin, mutta moni ei välttämättä ole tietoinen onko omaa tietokonetta turvallista käyttää ja ovatko tiedostot varmasti tallella, jos kone hajoaa tai katoaa työmatkalla.

Opinnäytetyön tavoitteena oli lisätä työntekijöiden ja työnantajien tietoisuutta keinoista, joilla voidaan parantaa kannettavan tietokoneen tietoturvaa työmatkoilla. Opinnäytetyössä tutustutaan yleisimpiin ja helposti toteutettavissa oleviin ratkaisuihin tietoturvan parantamiseksi. Opinnäytetyössä tietoturvan lisäämisellä tarkoitetaan keinoja, joilla parannetaan eritoten kannettavan tietokoneen käytön turvallisuutta. Useimpia esitettyjä keinoja voidaan soveltaa myös muihin mobiililaitteisiin. Opinnäytetyössä ei kuitenkaan perehdytä laitteen omistajan turvallisuuteen työmatkoilla.

Opinnäytetyön toimeksiantajana oli CYBERDI-projekti, joka on Jyväskylän ammattikorkeakoulun ja Poliisiammattikorkeakoulun kanssa toteutettu yhteisprojekti. Projektin tarkoituksena on lisätä kansalaisten tietoisuutta verkossa jatkuvasti tapahtuvista huijauksista. (Cyberdi 2020.)

2 Tutkimusasetelma

2.1 Tutkimuskysymys

Tämän tutkimuksen tutkimusongelmana oli tietoturvallisuus työmatkoilla. Tutkimuksessa selvitettiin, mitkä ovat yleisimpiä tietoturvaan kohdistuvia riskejä työmatkoilla ja miten niiltä voidaan suojautua. Tutkimuksen päälaitteena oli kannettava tietokone. Tutkimuskysymykset olivat seuraavanlaiset:

- Kuinka työntekijä voi käyttää turvallisesti verkkoa työmatkoilla?

- Mitä uhkia kohdistuu työntekijän datalle työmatkoilla?
- Miten suojautua näiltä uhkatekijöiltä?

2.2 Tutkimusmenetelmä

Tutkimuksen menetelmänä oli kvalitatiivinen eli laadullinen tutkimus. Pääsääntöisesti laadullinen tutkimus valitaan, kun lähtökohdassa ilmiöstä tiedetään erittäin vähän. Laadullisessa tutkimuksessa aineistoa kerätään useista lähteistä ja tehdään siitä johtopäätöksiä, eli yritetään ymmärtää ilmiötä. Ymmärryksen kautta voidaan lähteä kehittämään ilmiötä selittäviä teorioita ja hypoteeseja. (Kananen 2015, 70-71.)

Tutkimuksessa lähteinä käytettiin verkosta löytyviä dokumentteja. Dokumentteja ovat tilastot, verkkosivut, blogit tai mikä tahansa tuotos, joka liittyy tutkittavaan ilmiöön ja millä on merkitystä tutkimuksen kannalta. (Kananen 2015, 81.)

3 Taustaa

3.1 Uhkatekijät

3.1.1 Yleistä

Uhkatekijöitä datalle löytyy monenlaisia. Uhka voi olla digitaalinen tai fyysinen. Internetistä voi tulla haittaohjelma tai itse laite voidaan varastaa esimerkiksi hotellihuoneesta, jolloin menetät kaiken sinne tallennetun datan. Nykymaailmassa digitaaliset uhkatekijät ovat kovassa nousussa. Näitä ovat esimerkiksi tietojen kalasteluyritykset huijaussähköposteilla, haittaohjelmien levittäminen ja erilaiset kyberhyökkäykset. Kaikkien näiden takana voi olla yksittäisiä henkilöitä tai valtiollisia toimijoita. Luvuissa 3.1.2–3.1.4 käydään läpi, minkälaisiin datan uhkatekijöihin työmatkoilla voi törmätä.

3.1.2 Avoin WiFi

Voi tulla hetkiä, jolloin ainoa vaihtoehto saada töitä eteenpäin on käyttää avointa ja epäturvallista verkkoa. Näissä tapauksissa edes tietämys avoimen verkon vaaroista voi estää joutumasta kyberrikoksen uhriksi. (Dolly 2018.)

Isoimpia uhkia avoimissa verkoissa on hakkerien kyky sijoittaa itsensä verkon liityntäpisteen ja käyttäjän väliin. Tämä tunnetaan myös man-in-the-middle-hyökkäyksenä (MITM), jossa hyökkääjä tulee kahden laitteen väliin ja kaappaa tai muokkaa dataa näiden välillä ja pystyy esiintymään toisena osapuolena (What is a man-in-the-middle-attack 2020). Tämän jälkeen käyttäjä luulee juttelevansa suoraan päätelaitteelle, mutta kaikki data meneekin hakkerin kautta. Hakkerilla on pääsy kaikkiin tietoihin, mitä käyttäjä on lähettänyt, kuten sähköpostit, puhelinnumerot, luottokortin tiedot ja niin edespäin. Kannattaa lähteä siitä olettamuksesta, että kaikki tieto, mitä jaat tai käytät avoimissa verkoissa, on muiden vapaassa käytössä. (Dolly 2018.)

Tieto mitä syötät avoimen verkon yli ei siis saa olla luottamuksellista. Vältä siis pankkitietojen, henkilötunnusten ja kotiosoitteiden täyttämistä. Yritykset voivat menettää asiakastietoja, liiketoiminnan suunnitelmia, tuotteiden tietoja ja näiden myötä myös oman maineen. Muista myös tarkistaa, että selaimesi käyttää aina HTTPS:ää vähintään sivuilla, joihin syötät omia tietoja. HTTPS eli hypertext transfer protocol secure on protokolla, joka yhdistää HTTP ja salausprotokolla TLS:n salatakseen liikenteen selaimen ja verkkosivun välillä (What is HTTPS 2020). Hyvä vaihtoehto on myös käyttää omaa mobiilidataa, eli jaat esimerkiksi puhelimestasi verkon kannettavalle, jolloin vältät käyttämästä avoimia verkkoja. Pienentääkseen hyökkäysrajapintaa kannattaa lisäksi koneesta ottaa pois päältä tiedostojen jakaminen. Uuteen verkkoon liittyessä Windows kysyy, onko tämä koti vai julkinen verkko ja valitsemalla julkinen menee jakaminen automaattisesti pois päältä. (Dolly 2018.)

3.1.3 Haittaohjelmat

Haittaohjelmat eli malwaret on laaja käsite, joka tarkoittaa kaikkia haittaohjelmia mukaan lukien virukset ja ransomware. Muita malwareja-tyyppejä ovat mm. spywaret, botit ja rootkitit. Nämä antavat hakkerille keinon seurata laitteen toimintaa, liittää laitteen osaksi bottiverkkoa ja suorittaa omia ohjelmiaan uhrin koneella. (Veale 2019.)

Malwaret leviävät monella eri tapaa esimerkiksi sähköpostitiedostoista, ilmaisohjelmistoista ja saastuneilta verkkosivuilta. Muita keinoja ovat niin sanotut ”scarewaret” eli pelotteluohjelmat. Nämä ovat valheellisia antivirusohjelmia, jotka teeskentelevät

suojelevansa sinua viruksilta. Ne ilmoittavat, että koneesi on saastunut ja klikkaa tästä poistaaksesi uhkatekijä. Jos linkkiä painaa, tulee vain ladattua lisää haittaohjelmia. (Veale 2019.)

Malwaren vaikutukset ovat haittaohjelmatyypin mukaan vaihtelevia. Haitallisia vaikutuksia voivat olla laitteen heikentynyt suoritusteho, identiteettivarkaus, luottokorttipetos tai datan menetys. (Veale 2019.)

Virus

Virukset ovat pahantahtoisia ohjelmia, jotka leviävät laitteista toisiin saastuneiden tiedostojen ja verkkosivujen kautta. Laitteen saastuttua virus asentaa ja ajaa itsensä käyttäjän tietämättä. Viruksia tulee monessa muodossa, jotkin poistavat yksittäisiä tiedostoja ja toiset jopa formatoivat kiintolevyjä. (Veale 2019.)

Laite voi saada viruksia monesta eri lähteistä. Näitä ovat esim. saastuneiden sähköpostien liitetiedostojen avaaminen, internetistä ilmaisten ohjelmien lataaminen tai saastuneen USB-tikun käyttäminen. Lisäksi tartunta voi tulla jo aikaisemmin mainittujen saastuneiden verkkosivujen kautta, vaikka sieltä ei lataisikaan mitään. (Veale 2019.)

Virukset voivat vaikuttaa laitteen suorituskykyyn heikentävästi tai lopettaa laitteen toiminnan kokonaan. Ne voivat poistaa tiedostoja, kuten valokuvia ja videoita. Virus voi lähettää ärsyttäviä ilmoituksia omalle näytölle tai jopa lähettää roskapostia kaikille yhteyshenkilöille. (Veale 2019.)

Ransomware

Ransomware on haittaohjelma, joka lukitsee laitteesi tiedostot ja ohjelmat ja vaatii lunnasmaksun niiden avaamiseksi. Lunnasmaksu on yleensä muutamia satoja euroja. Kehittyneempi ransomware, joka tunnetaan myös kryptowarena salaa laitteen tiedostot ja salauksen purkamiseksi tarvitsee juuri oikean purkamisavaimen, mikä luvataan annettavaksi maksun jälkeen. Lunnasmaksu vaaditaan yleensä kryptovaluuttana niiden anonyymisyyden takia. (Veale 2019.)

Yleisin leviämistapa ransomwarelle on roskapostin kautta. Uhrit huijataan avaamaan saastunut sähköpostin liitetiedosto, mikä puolestaan lataa ransomwaren heidän

koneellensa. Usein nämä sähköpostit näyttävät tulevan lähipiiristä, kuten työkavereilta tai perheenjäseniltä. Ransomware leviää myös tiedostojen jakamisen ja saastuneiden verkkosivujen kautta. (Veale 2019.)

Yrityksille ransomwaret aiheuttavat eniten vahinkoa. Jos ransomwaren uhriksi joutunut yritys ei halua maksaa lunnasvaatimuksia, voivat hakkerit käyttää dataa muihin tarkoituksiin. Hakkerit voivat myydä kaapatun yrityksen arkaluontoisen datan muille hakkereille tai julkaista datan kaikkien nähtäväksi. (Mathews 2020.)

Ransomwaren vaikutukset ovat siis merkittäviä ainakin silloin, kun ei maksa lunnasvaatimuksia. Uhkana on lukitun laitteen kaikkien tiedostojen ja ohjelmien menetys. Vaikka maksaisikin vaaditun summan ei ole mitään takuita, että saisi kaiken tiedon purettua ja takaisin käyttökuntoisena. (Veale 2019.)

3.1.4 Fyysinen uhka

Fyysinen uhka laitteelle voi tulla käyttäjältä itseltään tai ulkopuolisen toimesta. Omistajan oma tahaton vahinko laitteelle on yksi yleisimmistä ongelmista matkustettaessa. Vahinko voi esimerkiksi olla tavallinen, kuten näppäimistön päälle kaatuu kahvia tai laite putoaa ja menee rikki. (Guinness 2016.)

Ulkopuolisella uhalla tarkoitetaan matkoilla tapahtuvaa rikollisuutta. Kannettavat tietokoneet ovat varkaiden suuressa suosiossa. Tärkeintä olisi tiedostaa, että varkauksia tapahtuu ympäri maailmaa ja siksi, pitää oma tietokone koko ajan lähettyvillä ja näkyvissä. Lentokoneissa ja busseissa ei kannata laittaa kannettavaa konetta alaruumaan vaan pitää se lähellä, kuten jalkojen välissä tai yläpuolen säilytystilassa. (Guinness 2016.)

3.1.5 Suojautumiskeinot

Oma verkkokäyttäytyminen on isossa roolissa verkkouhille altistumisessa, mutta tämä lisäksi kaikkiin edellä mainittuihin uhkatekijöihin löytyy myös vastakeinoja ohjelmistojen kautta. Uhkien vasta- ja suojautumiskeinoihin perehdytään tarkemmin otsikoissa 3.2–3.8 kertomalla näistä suojaa antavista ohjelmistoista.

3.2 VPN

3.2.1 Yleistä

Työmatkoilla usein pysähdytään kahviloihin ja otetaan kannettava esille, jotta voidaan jatkaa töitä sen enempää ajattelematta. Pitäisi kuitenkin muistaa, että kahvilat ovat julkisia paikkoja ja ne tarjoavat yleensä ilmaisen langattoman verkon (WLAN) asiakkailleen. Julkisten paikkojen avoimiin verkkoihin kannattaa aina suhtautua skeptisesti. Vaikka kahvilan avoin verkko tarvitsisi salasanan siihen liittyäkseen, ei tämä pidä ketään pahaenteistä henkilöä poissa sieltä, koska henkilökunnalta voi kuka tahansa mennä kysymään verkon salasanaa. Tämän jälkeen kuka vain vähänkin tietoteknisesti taitavampi henkilö voi kuunnella salaamatonta liikennettä kahvilan verkossa. Rikollinen voi myös alkaa jakamaan omaa verkkoaan samalla nimellä kuin kahvilan oikea verkko ja huijata kahvilan asiakkaita liittymään hänen verkkoonsa oikean sijaan. Tätä kautta hän voi saada kalasteltua käyttäjien tunnuksia ohjaamalla heidät aidon näköisille huijaussivustoille.

Välttyäkseen internetliikenteen seurannalta erityisesti julkisissa verkoissa kannattaa käyttää VPN:ää. VPN eli Virtual Private Network on keino, joka tarjoaa internetin selailuun lisää turvallisuutta, yksityisyyttä ja vapautta. (Marks 2020.)

3.2.2 Turvallisuus

VPN tarjoaa turvallisuutta salaamalla lähtevää internetliikennettä. VPN:n ollessa käytössä liikenne kulkee VPN-tunnelin kautta, joka tekee sen liikenteen kaappaamisen erityisen hankalaksi muille osapuolille, kuten valtioille ja hakkereille. On siis erittäin suositeltavaa pitää VPN päällä, kun käyttää avoimia WLAN-verkkoja. (Marks 2020.)

3.2.3 Yksityisyys

Yksityisyyttä internetissä VPN tarjoaa muuttamalla henkilökohtaisen IP-osoitteen VPN-palvelimen osoitteeksi ja tällä tavalla muut internetit käyttäjät eivät saa selville tarkkaa sijaintiasi tai edes oikeaa asuinmaata. Normaalisti muut toimijat voivat yhdistää internetselailusi identiteettiisi ja sijaintiin, mutta tämä kaikki muuttuu, kun käytät

VPN-palvelua. Ellei ole kirjautunut sivustoille yksilöivillä tunnuksilla ei internet aktiviteettia voi jäljittää takaisin kuin VPN-palvelimelle asti. Monet VPN-palveluntarjoajat eivät jaa tai seuraa mitä heidän palvelimiensa kautta tehdään ja näin olet saavuttanut paremman yksityisyyden internetissä, koska tekemisiäsi ei voida jäljittää IP-osoitteesi kautta. (Marks 2020.)

Otetaan esimerkki huonosta VPN-palveluntarjoajasta, joka on kerännyt lokeja eli verkkoliikenteen tapahtumia. Vuonna 2017 VPN-palveluntarjoaja PureVPN tahrasi oman maineensa, koska he auttoivat viranomaisia jäljittämään epäillyn rikollisen, joka oli sillä hetkellä heidän asiakkaanansa. Tuohon aikaan PureVPN väitti, etteivät he seuraa käyttäjiensä toimia tai pidä mitään lokeja tapahtumista. (Taylor 2017.)

3.2.4 Vapaus

Vapaus internetissä lisääntyy mahdollisuudella valita VPN-palvelimen sijainti maailmalla. Yhdistämällä tietyn maan VPN-palvelimeen voi internettiä selata kuin olisi fyysisesti kyseisessä maassa. Tämä on hyödyllistä, koska kaikkialla internet ei ole täysin vapaasti saatavilla. Tietyt maat kuten Kiina, Venäjä ja Iran sensuroivat internetliikennettä maansa rajojen sisäpuolella. Tämä voi tapahtua mm. rajoittamalla sosiaalisen medioiden tai suoratoistopalveluiden käyttöä. Näissä maissa ollessa on VPN-tarjoajasta riippuen mahdollista päästä käsiksi suosikkisivustoille rajoituksista ja sensuurista huolimatta. Tämä toimii myös toiseen suuntaan, eli jos haluaa katsoa muun maan sarjoja, joita ei näytetä kotimaassa, onnistuu se VPN:n avulla. (Marks 2020.)

3.2.5 Miten VPN toimii

Käytännössä kuluttajapuolella hyvän VPN-tarjoajan löydyttyä asennetaan heidän ohjelmistonsa laitteeseen, valitaan mieluiset asetukset ja muodostetaan turvallinen yhteys haluttuun VPN-palvelimeen. Kun yhteys on muodostettu, VPN-ohjelmisto, joka on koneella, salaa lähtevän liikenteen ja lähettää sen tunnelin toisessa päässä olevalle palvelimelle, joka taas purkaa salauksen. Palvelin tekee käyttäjän pyytämät toimenpiteet ja vastaanotettu data tulee takaisin palvelimelle, joka uudelleen salaa liikenteen ja lähettää sen takaisin käyttäjälle. Lopuksi vielä VPN-ohjelmisto purkaa saapuvan datan käyttäjälle ymmärrettävään muotoon. (Marks 2020.)

3.2.6 VPN yrityksessä

Yrityksen oma VPN toimii lähestulkoon samalla lailla kuin kuluttajaluokankin VPN. Erona on, että liikenne kulkee yrityksen verkon kautta, eli VPN-palvelin sijaitsee yrityksen tiloissa (tai pilvessä) ja sitä hallitsee yrityksen IT-osasto. Yhteyden muodostaminen tähän VPN-palvelimeen mahdollistaa pääsyn yrityksen sisäverkon tiedostoihin niin kuin olisi itse paikan päällä toimistolla.

Yhdistettäessä yrityksen VPN-palvelimeen kannattaa olla tietoinen, onko kaikki liikenne salattua vai pelkästään yrityksen sisäverkkoon menevä liikenne. Jos VPN-tunneli muodostuu vain koneen ja yrityksen verkon välille, muualle internetiin lähtevä liikenne ei ole salattua. (Gargiulo 2018.)

Työpaikan VPN-turvallisuuteen liittyen useat yritykset pidättävät oikeuden seurata, suodattaa ja logittaa työntekijöidensä internetliikennettä, kun he ovat yhdistettynä työpaikan VPN-palvelimeen. Jos tekee sellaista internetselailua mitä ei haluaisi työnantajan näkevän, ei sitä kannata tehdä työpaikan VPN:n kautta. (Home vpn vs business vpn 2020.)

VPN:n tehokkaimpia käyttötarkoituksia yrityksessä on tiedon turvallinen jakaminen työkavereiden ja myös organisaation ulkopuolisten henkilöiden kanssa. Yrityksen VPN on korvaamaton työkalu datan jakamiseen turvallisesti, koska uutisistakin nähdään yritysten tietomurtoja tapahtuvan lähes päivittäin. (Gargiulo 2018.)

3.2.7 Yleisimmät VPN-protokollat

Protokollien valinnassa ei ole yhtä oikeaa ratkaisua, vaan valintaan vaikuttaa monta eri asiaa. Vaikuttavia tekijöitä ovat käytettävä laite, verkko, haluttu suorituskyky ja toivottu turvallisuuden taso. Laite voi olla puhelin tai tietokone ja laitteen käyttöjärjestelmä voi vaihdella Windowsista Androidiin. Verkolla tarkoitetaan, kuinka rajatussa ympäristössä verkkoa käytetään. Ollaanko esimerkiksi Kiinassa, koulussa tai työpaikalla verkossa kiinni. Suorituskyvyltään tietyt protokollat ovat toisia parempia erityisesti älypuhelimissa, joissa verkko voi vaihdella liikkumisen myötä. Turvallisuudestakin löytyy eroja, jotkin protokollat ovat parempia turvallisuuden ja yksityisyyden kannalta kuin toiset, mutta se voi näkyä hitaampana nopeutena. (Taylor 2019.)

OpenVPN

OpenVPN on open source eli avoimen lähdekoodin ohjelmisto, joka yhdistelee ja käyttää useita eri teknologioita tarjotakseen vahvan ja luotettavan VPN-ratkaisun. Se on tällä hetkellä alan standardi kaupallisissa VPN-palveluissa ja hyvästä syystä. Se on erittäin turvallinen ja sitä voidaan käyttää melkein kaikissa laitteissa. OpenVPN:n vahvuuksiin kuuluvat myös laajat konfiguraatio mahdollisuudet ja avoimen lähdekoodin kehitysmenetelmä, joka antaa kaikille mahdollisuuden tutkia koodia ja etsiä haavoittuvuuksia. Natiivisti mikään järjestelmä ei tue OpenVPN:ää, mutta se on saatavilla suurimmalle osalle järjestelmiä kolmannen osapuolen ohjelmiston kautta. OpenVPN:n käyttämää porttia voidaan vaihtaa mihin vain, kuten TCP 443:ksi, joka naamioi VPN-liikenteen normaalin HTTPS:n sekaan. Tämä hankaloittaa verkoissa VPN-liikenteen estämistä. (Crawford 2019.)

SSTP

SSTP eli Secure Socket Tunneling Protocol on natiivisti tuettu protokolla Windows-käyttöjärjestelmille, koska sen kehittäjä ja omistaja on Microsoft. Tämän takia koodi ei ole vapaasti julkisesti saatavilla. SSTP:n vahvoja puolia on se, että sen integrointi Windowsiin tekee siitä helposti käytettävän ja toimivan kyseisellä käyttöjärjestelmällä. SSTP voi myös kiertää useat VPN-estot käyttämällä yleistä TCP-porttia 443. Microsoftin yhteistyöhistoria NSA:n kanssa ja spekulaatiot mahdollisista takaovista Windows-käyttöjärjestelmässä eivät kuitenkaan herätä luottamusta standardia kohtaan. (Crawford 2019.)

IPSec

IPSec on lyhenne sanoista Internet Protocol Security ja se on kokonaisuus eri protokollia, joilla varmistetaan turvallinen kommunikointi IP-paketti tasolla. Turvallisen kommunikoinnin muodostamiseen käytetään AH- ja ESP-protokollia, joilla varmistetaan paketin lähettäjä, tarkistetaan sen eheys ja salataan sisältö. (IPSec VPN Overview 2019.)

IPSec-protokollaa käytetään useasti muodostamaan salattu yhteys yrityksen eri toimipisteiden välille. IPSec muodostaa etäyhteyden koko verkkoon, missä on omat hyvät ja huonot puolensa. Tämä antaa käyttäjälle pääsyn kaikkiin verkon resursseihin,

mutta samalla myös mahdollistaa laajemman hyökkäyspinta-alan. IPSec ei myöskään ole nopein protokolla ja se vaatii huomattavaa kaistanleveyttä yhteydeltä. (IPSec 2020.)

IKEv2

Internet Key Exchange version 2 eli IKEv2 on Microsoftin ja Ciscon yhteistyöstä syntynyt protokolla. Se on yksi nopeimmista VPN-protokollista ja paras käytettäväksi mobiililaitteissa, joissa käytettävä verkko voi vaihdella. IKEv2 käyttää MOBIKE-ominaisuutta, mikä varmistaa, ettei VPN-yhteys katkea tai nopeus heikkene verkon vaihduttua. (Mocan 2019.)

IKEv2:ta ei normaalisti käytetä yksinään, vaan se on usein yhdistettynä IPSec protokollan kanssa. Tällöin merkintänä on ”IKEv2/IPSec”, jolloin se yhdistää IPSec:n turvallisuuden IKEv2:n nopeuden kanssa. Heikkona puolena IKEv2:ssa on se, että se toimii vain UDP-portissa 500, mikä on mahdollista estää palomuurin tai verkon ylläpitäjän toimesta. (Mocan 2019.)

SSL-VPN

SSL-VPN mahdollistaa turvallisen etäyhteyden web portaalin kautta ja verkkotason pääsyä SSL-suojatun tunnelin kautta käyttäjän ja yrityksen välille. SSL-VPN mahdollistaa käyttäjälle turvallisen pääsyn yrityksen sisäverkkoon ilman kolmannen osapuolten ohjelmien lataamista. (What is SSL-VPN 2020.)

Kasvavan etätyön takia SSL-VPN on tärkeä pitääkseen työntekijät yhdistettyinä heille tärkeisiin sovelluksiin. Toinen hyvä puoli on, että SSL-VPN antaa IT-osastolle mahdollisuuden rajoittaa pääsy vain valtuutetuille henkilöille ja lisäksi pelkästään tiettyihin resursseihin, kuten vaikka sähköpostiin tai jaettuun verkkoasemaan. (What is SSL-VPN 2020.)

Wireguard

Wireguard on ollut vuosia kehityksessä ja nyt se on ensimmäistä kertaa tulossa osaksi Linux kerneliä, eli ydintä. Tällä on mahdollisuus mullistaa koko VPN maailma, koska pääasiallisesti kaikki VPN-palvelut käyttävät Linux palvelimia. Wireguardin tulo ei heti

lopeta muiden protokollien käyttöä, mutta jos se käyttäytyy odotusten mukaisesti tulevaisuuden VPN tulee pohjautumaan Wireguardiin. (Vaughan-Nichols 2020.)

Wireguard pyrkii olemaan nopeampi, yksinkertaisempi ja hyödyllisempi kuin IPSec ja suorituskyvyltään parempi kuin OpenVPN. Teoriassa Wireguardin pitäisi saavuttaa erittäin hyvä suorituskyky näihin kilpailijoihin verrattuna, mutta sen pitää vielä kehittyä ja testauttaa monia asioita ennen läpimurtoa. Alun perin Linuxille julkaistu, nykyään järjestelmäriippumaton, eli saatavilla myös Windowsille, MacOS ja Androidille. Tällä hetkellä vielä runsaan kehityksen alla, mutta jo nyt sitä pidetään alan turvallisimpana ja yksinkertaisimpana VPN-ratkaisuna. (Wireguard 2019.)

3.3 VPN-vaihtoehtoja

3.3.1 Yleistä

Käyttäjän yksityisyyden näkökulmasta on kahdenlaisia VPN-palveluita. VPN-palvelut, jotka eivät pidä minkäänlaisia lokeja, ja sitten kaikki muut. Niin sanottu ”no-log policy” on VPN-tarjoajan lupaus siitä, ettei mitään yksilöivää tietoa liittyen käyttäjän yhteyteen tai kaistaan kerätä, säilytetä tai jaeta eteenpäin. Tähän vaikuttaa suurelta osalta, minkä maan lainsäädännön alla VPN-palveluntarjoaja operoi. Tämä on yksi tärkeimmistä kriteereistä VPN-palveluntarjoajan valinnassa. (Greenberg 2020.)

VPN-käyttäjien on hyvä tietää, mitä tarkoittaa Five Eyes, Nine Eyes ja Fourteen Eyes. Five Eyes (FVEY) on viiden maan liitto, jonka alkuperäinen tarkoitus oli tiedustelutietojen jakaminen, mutta nykyään se on laajentunut verkkotoiminnan seurantaan. Nine ja Fourteen Eyes ovat käytännössä laajentunut versio alkuperäisestä Five Eyes liitosta. Nämä uudet maat eivät välttämättä jaa niin paljon tietoa kuin alkuperäinen Five Eyes, mutta he kuitenkin vapaaehtoisesti osallistuvat kansainväliseen tietojen jakamiseen. Liittoihin kuuluvat seuraavat maat:

Five Eyes: Yhdysvallat, Iso-Britannia, Kanada, Australia ja Uusi-Seelanti
Nine Eyes: Five Eyes + Tanska, Ranska, Hollanti ja Norja
Fourteen Eyes: Nine Eyes + Saksa, Belgia, Italia, Ruotsi ja Espanja. (Krohn 2019.)

Miten tämä kaikki sitten vaikuttaa VPN-käyttäjään? On turvallista olettaa, että jos jokin näistä maista saa kätensä sinun verkkodataasi, voidaan se jakaa muiden liittoon kuuluvien maiden kanssa. Tärkeää on siis valita sellainen VPN-palveluntarjoaja, minkä liiketoiminta ei sijaitse missään Fourteen Eyes maassa, jos arvostaa omaa yksityisyyttään verkossa. (Krohn 2019.)

VPN:ää voidaan helposti käyttää myös peittämään laittomia toimia verkossa, minkä takia jotkut voivat pitää itse VPN-ohjelmistoja laittomana. Näin ei kuitenkaan ole. VPN:n käyttö on laillista suurimassa osassa maailmaa. VPN:n käyttö on kiellettyä tai rajoitettua seuraavissa maissa:

- Kiina
- Irak
- Iran
- Venäjä
- Valko-Venäjä
- Turkki
- Oman
- Yhdistyneet arabiemiirikunnat (Hochstadt 2020b.)

VPN:n käyttäminen on normaalisti turvallista, mutta edellä mainituissa maissa on omat riskinsä VPN:n käytössä. Saatat näissä maissa ottaa riskin, jos käytät VPN:ää, joka ei ole valtion hyväksymä tai sellaista VPN:ää joka pitää lokeja käyttäjistään. (Hochstadt 2020b.)

Ennen valintaa kannattaa VPN-palveluntarjoajaan sivuilta lukea perustietoja, kuten kuinka monta palvelinta he omistavat ja mistä päin maailmaa, sekä moneenko laitteeseen ohjelmisto voidaan asentaa samanaikaisesti. VPN:stä on myös hyvä selvittää, minkä maan lakeja se noudattaa ja onko se missään tekemisissä FVEY-liiton kanssa. Lisäksi on hyvä lukea muiden käyttäjien arvioita palvelusta. Jos työpaikkasi tarjoaa VPN-palvelua, on suositeltavaa käyttää sitä, mutta muussa tapauksessa käydään läpi muutamia VPN-palveluntarjoajia, jotka tarjoavat hyvää henkilökohtaista suojaa internettiä käytettäessä, missä ikinä oletkin.

Valitut kaupalliset VPN:t ovat kaksi hyvin tunnettua ja isoa palveluntarjoajaa NordVPN ja CyberGhost VPN. Käydään läpi syitä valinnalle. Ensimmäisenä kyseiset VPN-palveluntarjoajat ovat useissa ulkopuolisten tekemissä VPN-vertailuissa ja testeissä lähes aina viiden parhaimmiston joukossa (Marshall 2020; Rivington 2020). Pidetään mielessä, että kilpailevia VPN-palveluntarjoajia on satoja. Toisena kumpikaan palveluntarjoaja ei operoi maassa, joka kuuluu aikaisemmin mainittuun Fourteen Eyes liittoon ja kummankaan maan oma lainsäädäntö ei myöskään vaadi datan tai lokitietojen säilyttämistä. Kolmantena niiden eroavaisuudet, Cyberghost VPN sopii yksinkertaisuutensa vuoksi paremmin uusille VPN-käyttäjille, kun NordVPN puolestaan tarjoaa myös yrityskäyttöön sopivaa ja helposti käyttöön otettavaa NordVPN Teams palvelua.

3.3.2 NordVPN

Turvallisuus

NordVPN on rekisteröity Panamaan, mikä ei ole osa aikaisemmin mainittua Fourteen Eyes liittoa. Tämä on tärkeää yksityisyyden kannalta. Panamassa ei ole myöskään tiukkoja datan säilytyslakeja. Normaalisti tämä laki vaatisi internetin ja VPN-palveluntarjoajat säilyttämään käyttäjiensä lokeja määrätyn ajan verran. NordVPN:n ei siis tarvitse noudattaa tällaista lakia, joka tekee siitä yhden ainoista todellakin nolla lokipolitiikan VPN-tarjoajista. NordVPN on tämän lisäksi käynyt läpi ulkopuolisen suorittaman turvallisuusauditoinnin, joka todisti VPN-tarjoajan väitteet turvallisuudesta oikeiksi. (Hochstadt 2020a.)

NordVPN tarjoaa käyttäjilleen myös heidän omaa mainosten ja haittaohjelmien estoa nimellä ”CyberSec suite”. Se on sisäänrakennettuna VPN:ään ja vaatii vain yhden napin painamista aktivoituakseen. Se mahdollistaa mukavan internetin selailun ilman ärsyttäviä ponnahdusikkuna mainoksia. Cybersec on hieno lisäys, mutta se on vain yksi NordVPN:n turvallisuusominaisuuksista. Mahdollisuutena on myös käyttää kaksinkertaista VPN-yhteyttä. Tässä liikenne menee kahden VPN-palvelimen kautta, jonka seurauksena data salataan kahteen kertaan. Peruskäyttäjät eivät tätä ominaisuutta normaalisti tarvitse, mutta lisäsuojaa etsivät henkilöt varmasti arvostavat tätä ominaisuutta. NordVPN:n yksi tärkeistä ominaisuuksista on kill switch (suomeksi

hätä-seis-painike), joka tarkoittaa toimintoa missä VPN-ohjelmisto automaattisesti katkaisee kaiken verkkoliikenteen, jos se havaitsee VPN-yhteydessä jotain häiriötä. (Hochstadt 2020a.)

NordVPN tarjoaa eri protollia eri tarkoituksiin. Vakiona NordVPN tarjoaa erittäin vahvaa salausta käyttämällä AES-256 salausta OpenVPN protokollan kanssa. MacOs ja iOS laitteissa käytetään vakiona AES-256 salausta ja IKEv2/IPsec protokollia. Linux käyttäjien suositellaan käyttävän NordVPN omaa versiota Wireguardista nimeltä NordLynx. (Which protocol should I choose 2020.)

Palvelimet

NordVPN tarjoaa asiakkaidensa käyttöön tällä hetkellä yli 5500 palvelinta, jotka sijaitsevat 59 eri maassa (Servers 2020). NordVPN:n on myös todettu toimivan Kiinassa. Kaikki VPN:ät eivät kykene ohittamaan Kiinan palomuuria (GFW) ja tässä tapauksessa NordVPN on yksi parhaista VPN-vaihtoehdoista Kiinaan matkaileville. Pitää kuitenkin muistaa asentaa VPN-ohjelmisto ennen kuin olet maassa, muuten voi olla hankaluuksia päästä ohjelmiston lataussivulle. Kiinaa ja muita sensuurimaita varten NordVPN tarjoaa erityisiä ”obfuscated servers”, jotka erikoistuvat kiertämään valtioiden asettamia rajoituksia. Hyvä vaihtoehto työmatkailijoille, joiden pitää vierailla tällaisissa maissa. (Hochstadt 2020a.)

Yrityksille

Yrityksille NordVPN tarjoaa heidän omaa NordVPN Teams nimistä VPN-palvelua. Sen tarkoituksena on yhdistää yrityksen kaikki VPN-käyttäjät helposti hallittavaan kokoonpanoon. Pääkäyttäjä voi keskitetystä hallintapaneelista lisätä, poistaa ja hallita muita käyttäjiä ja asettaa heille pääsyrajoituksia yrityksen eri resursseihin. Laskutus on myös keskitetty yhdeksi paketiksi yrityksen käyttäjien ja palvelimien lukumäärän mukaan. NordVPN Teams on helppo skaalata yrityksen kasvun mukana. Käyttäjien lisenssejä, dedikoituja palvelimia ja yrityksen yhdyskäytäviä voidaan lisätä tarpeen mukaan. NordVPN Teams palvelimet ovat erillään kuluttajaluokan VPN:stä ja niitä löytyy tällä hetkellä 31 eri maasta. Hinnat ovat alkaen 7 € per käyttäjä ja 40 € per dedikoitu palvelin kuukaudessa. Enterprise paketin tai lisäominaisuuksia haluavien

yrityksien pitää ottaa yhteyttä NordVPN Teamsiin tarjousta varten. (Remote access VPN 2020.)

Muuta

Ongelmatilanteissa NordVPN tarjoaa 24/7 realiaikaista keskusteluapua ja tikettisysteemin, sekä laajan tietokannan ja usein kysyttyä (FAQ) osion. NordVPN-ohjelmisto voidaan yhdellä käyttäjätilillä asentaa kuudelle eri laitteelle, mikä on tarpeeksi kaikille omille laitteille, pienelle yritykselle tai jopa koko perheelle. Hinta on tällä hetkellä 3 vuoden sopimuksessa noin 111 €, mikä tekee 3,10 € kuukaudessa (NordVPN 2020). NordVPN tarjoaa 30 päivän rahojen palautustakuun. NordVPN on hyvä valinta, mutta se ei ole markkinoiden paras kaikissa osapuolissa. NordVPN ei ole kilpailijoihinsa verrattuna nopein tai halvin vaihtoehto, mutta se on erittäin monipuolinen ja ominaisuuksiltaan hintansa arvoinen. (Hochstadt 2020a.)

3.3.3 CyberGhost VPN

Turvallisuus

CyberGhost VPN operoi Romaniassa, joka on Fourteen Eyes liiton ulkopuolella. Romaniassa ei myöskään lain puolesta ole mitään velvoitteita jakaa tietoa viranomaisten tai muiden tahojen kanssa. CyberGhost VPN tarjoaa myös omaa mainosten ja haittaohjelmien esto-ominaisuutta, jotka saa asetuksista päälle tai pois. Haittaohjelmien eston ollessa päällä, se tarkistaa jokaisen käydyn verkkosivun ja vertaa sitä sen omaan haitallisten sivustojen tietokantaan. Jos haitallinen sivu havaitaan, se estetään ennen kuin se pystyy vahingoittamaan käytettävää laitetta. CyberGhost VPN käyttää alan johtavia turvallisuusominaisuuksia, kuten AES 256-bit salausta, automaattista kill switchia ja tietenkin tiukkaa lokipolitiikka, eli ei tallenna mitään tietoa käyttäjien verkkoaktiviteeteistä. (Veale 2020.)

Palvelimet

CyberGhost VPN tarjoaa laajan yli 5900 palvelimen verkoston, joka sijaitsee 89 eri maassa (CyberGhost VPN servers. 2020). Tällä hetkellä CyberGhost VPN ei pysty ohittamaan Kiinan palomuuria, joten se ei ole paras vaihtoehto, jos haluaa Kiinassa ollessa esteettömän internetin käytön. CyberGhost tarjoaa lisäksi heidän oman

palvelinkeskuksensa ”NoSpy” palvelimiaan, jotka sijaitsevat Romanian pääkonttorissa ja niitä ylläpitää CyberGhostin oma henkilökunta. Näiden tarkoituksena on tarjota käyttäjille lisäsuojaa ja parempia nopeuksia, mikä tekee NoSpy palvelimista ideaalin torrenttien käytölle. (Veale 2020.)

Muuta

CyberGhost VPN on tehty erittäin helppokäyttöiseksi ja käyttöliittymä yksinkertaiseksi, joten se on hyvä vaihtoehto aloittelevalle VPN-käyttäjälle. Kokeneemman käyttäjän ei kuitenkaan tarvitse pettyä. Sovellus on kustomoitavissa mm. käyttämään tiettyä protokollaa tai porttia. Hinta on myös kohtuullinen ainakin kolmen vuoden sopimuksessa, jonka hinnaksi tulee tällä hetkellä 2,7 €/kk, eli kolmen vuoden VPN:n käyttö maksaisi hieman alle 100 euroa (CyberGhost VPN 2020). Tilauksen voi peruuttaa ja rahat on mahdollista saada takaisin 45 päivän sisällä ostosta, jos ei ole tyytyväinen tuotteeseen. CyberGhost VPN voidaan asentaa seitsemään eri laitteeseen samanaikaisesti, mikä on yksi laite enemmän kuin NordVPN:ssä. (Veale 2020.)

3.4 Haittaohjelmien torjunta

3.4.1 Yleistä

Haittaohjelmien suojausohjelmistojen tarkoituksena on suojella tietokonetta malwareilta, eli haittaohjelmilta. Ohjelmisto skannailee järjestelmää mahdollisten saastumisien varalta ja poistaa löydetyt haittaohjelmat. Haittaohjelmien suojausohjelmistolla on samoja piirteitä kuin antiviruksella, mutta ne kuitenkin eroavat toisistaan. Haittaohjelmien suojausohjelmisto on kehittyneempi ohjelmisto, joka käyttää edistyneempiä menetelmiä haittaohjelmien etsintään. Antivirus etsii vain viruksia, kun haittaohjelmien suojausohjelmisto taas käsittelee muutkin malwaren osapuolet, kuten spywaret ja adwaret. (What is anti malware 2020.)

Yksi haittaohjelmien suojausohjelmistojen toimintatavoista on ”behavior monitoring”, eli ohjelmisto etsii haittaohjelmia tarkkailemalla tiedostojen käyttäytymistä ja merkitsemällä epäilyttävät tapaukset uhkatekijöiksi. Tämä toimintatapa on jatkuvaa ja tekee haittaohjelmien havaitsemisesta helpompaa, koska ohjelmiston ei tarvitse

skannata tiedostoa vaan pelkkä käytös koneella paljastaa haittaohjelman. Toinen haittaohjelmien suojausohjelmistojen käyttämä tekniikka on ”sandboxing”. Tämä tarkoittaa tapahtumaa, missä ohjelmisto siirtää epäilyttävän tiedoston eristettyyn hiekkalaatikkoon, jossa sitä voidaan jatko analysoida ilman uhkaa koneen muille tiedostoille. Tämä on hyvä tapa estää malwaren tartunta ja eristää se pois sallittujen sovelluksien joukosta. Viimeisenä haittaohjelmien suojausohjelmisto poistaa havaitun haittaohjelman estääkseen sen suoriutumisen ja koneen saastumisen. Jatkossa jos koneeseen tulee sama haittaohjelma, suojausohjelmisto eliminoi sen saman tien. Haittaohjelman poisto voi kuulostaa isolta hommalta, mutta itseasiassa kaikki tämä on ohi muutamassa sekunnissa. (What is anti malware 2020.)

Yksi syy miksi ihmiset välttävät hankkimasta malwareilta suojaavia ohjelmistoja on se, että niiden luullaan tuntuvasti hidastavan tietokonetta. Enää ei kuitenkaan näin ole. Nykyaikaiset suojausohjelmistot ovat kehittyneet niin paljon, etteivät ne enää käytä kaikkia laitteen resursseja omaan toimintaansa, vaan toimivat huomaamattomasti taustalla. (Best antivirus 2020.)

Windows 10 käyttöjärjestelmää suojaa vakiona Windows Defender. Windows Defenderiin kuuluu palomuuri ja antivirus, joka on kyllä vuosien aikana kehittynyt hyväksi suojausohjelmaksi, mutta se ei riitä yksinään suojaamaan kaikilta malwaren tyypeiltä. Kaveriksi on hyvä asentaa haittaohjelmien suojausohjelmisto, kuten jokin Bitdefenderin tai Kasperskyn tarjoama ratkaisu.

Bitdefender ja Kaspersky valittiin tarkasteluun vuoden 2019 testitulosten perusteella. Testit suorittivat tunnettu AV-TEST, joka on itsenäinen IT-instituutti, joka on erikoistunut IT-laitteiden ja ohjelmistojen turvallisuuden testauksiin (About the AV-TEST Institute 2020). Parhaimman suojauksen tarjoavan ohjelmistojen testien voittajat olivat Kaspersky ja Bitdefender. Kaspersky tarjosi parasta suojaa kuluttajille ja Bitdefender yrityksille (AV-TEST Awards 2019).

3.4.2 Bitdefender

Bitdefender on yksi johtavista globaaleista kyberturvallisuuden alan yrityksistä, joka on toiminut alalla vuodesta 2001 lähtien ja tällä hetkellä suojaa yli 500 miljoonaa

laitetta. Suojausta on saatavilla niin yksityisille henkilöille ja perheille kuin kaiken kokoisille yrityksillekin. (Bitdefender 2020.)

Bitdefender tarjoaa monenlaisia paketteja kotikäyttäjille. Bitdefenderin ”Total Security” niminen paketti tarjoaa yksityishenkilöille parasta suojaa tarjoamalla antivirus ja haittaohjelmien suojausohjelmistot samassa paketissa. Lisäksi pakettiin kuuluu lukuisia muita hyödyllisiä toimintoja, kuten hallintakeskus, mikrofonin ja kameran valvonta, sekä selaimiin lisättävä anti-tracker laajennus. (Bitdefender 2020.)

Ominaisuudet

Jos kone käyttäytyy oudosti ja syyksi epäillään virustartuntaa, voidaan ajaa nopea skannaus. Tämä metodi käy läpi yleisimmät paikat, missä virukset voivat piileskellä ja se ei vie paljoa aikaa. Jos tämä nopea skannaus ei löydä mitään, voidaan suorittaa täysi skannaus, mikä käy kaikki systeemin tiedostot läpi, mutta kestää myös kauemmin. Kustomoituja skannauksia voidaan myös asettaa tarkistamaan haluttuja kansioita tietyin aikavälein, mikä on hyvä keino tarkistaa muilta henkilöiltä saatuja tiedostoja vaaroilta, jotka voisivat vahingoittaa omaa laitetta. (Bitdefender antivirus review 2020.)

Bitdefenderin haavoittuvuusskannaus tarkistaa käyttäjän puolesta onko laitteessa turvallisuusaukkoja, kuten turhia avoimia portteja tai päivittämättömiä sovelluksia. Tämä ominaisuus on hyödyllinen, koska silloin käyttäjän ei itse tarvitse olla teknisesti taitava ja osata sulkea avoimia portteja manuaalisesti, vaan kaikki onnistuu muutamalla hiiren klikkauksella. (Bitdefender antivirus review 2020.)

Reaaliaikainen suojaus hoitaa automaattisesti uhkien tarkistamisen ja estämisen ilman käyttäjän manuaalisia skannauksia. Esimerkiksi tiedoston lataamisen aikana Bitdefender tarkistaa tiedoston ja estää latauksen, jos kyseinen tiedosto havaitaan haitalliseksi. Monissa kilpailevissa ohjelmistoissa haittaohjelmaan reagoidaan vasta kun ne ovat jo ladattuna koneella. Myös koneeseen kiinnitetyt USB-tikut ja muut tallennusvälineet skannataan automaattisesti uhkien varalta. (Bitdefender antivirus review 2020.)

Yrityksille

Bitdefender tarjoaa yrityksille GravityZone nimistä ratkaisua. GravityZonesta on tarjolla erilaisia paketteja kaiken kokoisille yrityksille. Sen tarkoituksena on kattaa kaikki turvallisuustarpeet yhdessä ratkaisussa. GravityZone mahdollistaa fyysisten, virtuaalisten ja mobiililaitteiden turvallisuuden hallinnan yhdestä keskitetystä paikasta. Se on usein luokiteltu parhaimmaksi turvallisuusratkaisuksi ulkopuolisten turvallisuustesteissä. (Business security 2020.)

GravityZonen infrastruktuuri toimii pilvessä ja sen omistaja sekä ylläpitäjä on Bitdefender, mikä poistaa yrityksen tarpeen ostaa omia palvelimia tähän tarkoitukseen. Verkkokonsoli on heti käytettävissä ja sieltä pääsee reaaliaikaisesti hallitsemaan ja monitoroimaan kaikkia käyttäjiä. Verkkokonsolista voi suojausohjelmistot asentaa etänä kaikkiin haluttuihin loppukäyttäjien koneisiin. (Business security 2020.)

3.5 Varmuuskopiointi

3.5.1 Yleistä

Varmuuskopiointi tarkoittaa tapahtumaa, missä tärkeä tieto kopioidaan ja tallennetaan toiseen paikkaan. Tämän seurauksena kopioitu tieto pelastuu, jos alkuperäinen tallennuspaikka tuhoutuu. Nykypäivinä tiedostojen häviämiselle löytyy monia eri syitä, kuten kiintolevyn hajoaminen, varkaus tai ransomware.

Varmuuskopiointi on eräs yksinkertaisimmista keinoista parantaa omien tiedostojen tietoturvaa niin työmatkoilla kuin kotonakin. Varmuuskopioita voi ja kannattaa tehdä moneen eri paikkaan. Vaihtoehtoina on esimerkiksi tallentaa tiedostot ulkoiselle kiintolevylle ja lisäksi pilveen. Varmuuskopiointi on hyvä tehdä jo ennen työmatkan alkua, jotta laitteelle matkan aikana tapahtuva mahdollinen onnettomuus ei lopullisesti hävitä tärkeimpiä tiedostoja.

3.5.2 Ulkoinen kiintolevy

Ulkoinen kiintolevy on väline, minne voidaan tallentaa dataa. Se yhdistetään laitteisiin pääasiassa USB-kaapelia käyttäen. Sitä voidaan käyttää datan tallentamiseen,

siirtämiseen laitteesta toiseen ja varmuuskopiointia varten. Ulkoisten kiintolevyjen hinnat ovat tulleet vuosien saatossa alaspäin ja ovat nykyään hyvinkin edullisia. Etu ulkoisella kiintolevyllä pilvipalveluun verrattuna on turvallisuuden näkökulmasta se, että levyllä oleva data pysyy itsellään, eikä siirry kolmannen osapuolen palvelimille. Lisäksi levyn ollessa irti koneesta pääsee dataan käsiksi vain fyysisen kontaktin kautta, ei verkkoja pitkin. Ulkoisen kiintolevyn data voidaan myös erikseen salata, mikä estää tiedon joutumisen vääriin käsiin, jos kiintolevy häviää tai joutuu varkauden kohteeksi.

Ulkoinen kiintolevy on edullinen ja nopea ratkaisu tiedostojen varmuuskopioinnille. Todennäköisesti tämä kiintolevy kuitenkin sijaitsee samassa tilassa kuin itse tietokone, jolloin onnettomuus tai murtovaras voi viedä molemmat mukanaan. Ei kannata myöskään pitää ulkoista levyä jatkuvasti kiinni tietokoneessa, jolloin sama ransomware tai haittaohjelma voisi tuhota molempien tiedostot. Kannattaa siis säännöllisesti laittaa kiintolevy kiinni koneeseen, tehdä tarvittavat varmuuskopiot tiedostoista ja sitten irrottaa ulkoinen kiintolevy koneesta. (Spector 2017.)

3.5.3 Pilvipalvelu

Sana ”pilvi” on nykypäivän muotisana ja sitä käytetäänkin aika löyhästi, kun itse asiassa tarkoitetaan vain etäpalvelinta, jossa sijaitsevat omat tiedostot ja sinne muodostetaan yhteys internetin kautta. Kun joku kertoo lataavansa tiedostoja pilveen, tarkoittavat he oikeasti, että he kopioivat tai siirtävät dataa koneelle, joka sijaitsee jossain muualla, kenties toisella puolella maailmaa. (Encrypted cloud storage 2020.)

Pilveen varmuuskopiointi on helppoa. Siinä ei tarvitse manuaalisesti irrotella kiintolevyjä koneesta, vaan riittää, että on toimiva internet-yhteys. Yhteyden löydyttyä varmuuskopiointi tapahtuu automaattisesti ilman käyttäjän toimenpiteitä alkuasetuksia lukuun ottamatta.

Pilvipalveluntarjoajan ja asiakkaan väliseen sopimukseen kannattaa tutustua ennen valinnan tekoa. On tärkeää selvittää, että omistusoikeus dataan on aina asiakkaalla itsellään, vaikka data tallennetaankin ulkopuoliselle palvelimelle. Hyvänä esimerkkinä on Amazonin, Googlen ja Microsoftin tarjoamat pilvitallennuspalvelut, jotka selvästi kertovat datan omistusoikeuden säilyvän asiakkaalla. (Chima 2016.)

Sopimuksen lisäksi kannattaa varmistua, että pilvipalveluntarjoaja salaa datan sen siirto ja tallennusvaiheessa. Tärkeätä on myös tietää, missä maassa dataa säilytetään ja varmistaa kyseisen maan lainsäädännön datan suhteen olevan kunnossa. Vaikka datasi on pilvessä, ei kannata kuitenkaan lopettaa paikallista varmuuskopiointia. Jos pilvipalveluntarjoaja menee nurin, voit menettää kaiken datan. (Chima 2016.)

Pilvipalvelu tallennuspaikkana on huomattavasti hitaampi kuin ulkoinen kiintolevy. Pilveen tehtävä, ainakin ensimmäinen täysi varmuuskopioi, voi kestää jopa useita päiviä, verrattuna kiintolevyn muutamiin tunteihin. Pilvitallennus tulee myös pitkällä aikavälillä kalliimmaksi, koska niissä on juoksevat kuukausi- tai vuosimaksut. (Spector 2017.)

3.6 Varmuuskopiointikeinoja

3.6.1 Yleistä

Jos dataan haluaa päästä käsiksi monelta laitteelta samanaikaisesti, on helpointa tallentaa varmuuskopiot pilveen, kuten Microsoft Onedriveen, Google Driveen tai Dropboxiin. Pilvipalveluntarjoajia on useita, mutta nämä edellä mainitut ovat tunnetuimpia. Yritysdatan tallentaminen pilveen sellaisenaan voi kuitenkin olla yrityksen sääntöjen vastaista. Yritykset haluavat varmistua, että heidän dataansa eivät muut pääse käsiksi. Lisäturvakerroksena yritykset voivat esimerkiksi siirtää datan salattuihin säiliöihin ennen pilveen tallentamista. Toisena vaihtoehtona on tallentaa varmuuskopiot omille ulkoisille kiintolevyille. Kummatkin vaihtoehdot kuitenkin vaativat hieman manuaalista työtä. Joudut vähintäänkin raahaamaan kansioita edestakaisin tallennussijaintien välillä. Tämän kaiken automatisointiin auttaa erilaiset varmuuskopiointia varten tehdyt ohjelmistot.

Varmuuskopiointia tekeviä ohjelmistoja löytyy monia ja niitä on sekä ilmaisia että maksullisia vaihtoehtoja. Maksullisia ovat esimerkiksi Acronis True Image 2020 ja AOMEI Backupper Professional (Fisher 2020a). Ennen maksullisia vaihtoehtoja kannattaa aina koittaa, voisiko ilmaisen ohjelmiston toiminnot riittää omiin tarpeisiin. Ilmaisia ohjelmistoja ovat esimerkiksi EaseUS Todo Backup ja Cobian Backup (Fisher 2020b).

Testattavaksi varmuuskopiointiohjelmistoksi valittiin Veeam. Veeam valittiin sen tunnettavuuden ja arvioiden perusteella. Esimerkiksi Gartner nimesi Veeam:n jo kolmatta kertaa parhaimpaan johtaja-asemaan datakeskuksien varmuuskopiointi- ja palautusratkaisuissa (Veeam Gartner 2019).

3.6.2 Veeam

Veeam on johtavia varmuuskopioratkaisuja tarjoavia yrityksiä, joka mahdollistaa datan hallinnan yhtenäisen pilvialustan kautta. He suojaavat dataa kaikessa muodossa, joko fyysistä, virtuaalista tai pilvessä olevaa dataa. Heidän ratkaisunsa ovat yksinkertaisia, joustavia ja luotettavia. Yksinkertaisuus tulee yhtenäisestä alustasta, joustavuus tulee mahdollisuudesta mukautua ympäristön mukaan ja luotettavuus tulee jatkuvasta pääsystä dataan ajasta ja paikasta riippumatta. (Veeam 2020.)

Veeam tarjoaa ratkaisuja yrityksille, palveluntarjoajille sekä yksityishenkilöille. Varmuuskopio ohjelmistoja löytyy Windowsille, Linuxille, Office 365:lle, AWS:lle ja Azurelle. Kaikkiin näihin löytyy rajoitetumpi ilmaisversio ja sitten maksullinen versio, joka sisältää runsaasti lisäominaisuuksia. Veeam tarjoaa varmuuskopioinnin lisäksi muitakin tuotteita, kuten Veeam ONE, joka on monitorointi ja analytiikka työkalu IT-ympäristöä varten. (Veeam 2020.)

3.7 Tiedostojen salaus

3.7.1 Yleistä

Täydellinen levyn salaus on ainoa keino suojella dataasi, mikäli kannettavasi häviää tai varastetaan. Jos joku pääsee fyysisesti käsiksi kannettavaasi ja et käytä levyn salausta, niin kaikki tiedostosi on helposti varastettavissa. Ei ole väliä käytätkö vahvaa Windows salasanaa, koska hyökkääjä voi helposti käynnistää Linuxin USB-tikulta, jonka avulla voi ohittaa alkusalasanan ja päästä käsiksi kannettavan kaikkiin tiedostoihin. Toinen hyökkääjän käyttämä keino olisi ruuvata kiintolevy irti uhrin koneesta ja liittää se toiseen koneeseen. (Lee 2015.)

Yleinen harhakäsitys kuitenkin on, että levyn salaaminen tekisi koneesta täysin turvallisen. Levyn salaaminen on hyödyllinen vain sellaista hyökkääjää vastaan, jolla on fyysinen pääsy koneeseesi. Levyn salaus ei siis tee koneestasi yhtään hankalampaa hyökätä verkon kautta. Voit silti vierailla saastuneilla verkkosivuilla tai avata epäilyttävän sähköpostin liitetiedoston ja saada haittaohjelman koneellesi levyn salauksesta huolimatta. (Lee 2015.)

Yksinkertaistettuna salaus on kryptografian digitaalinen muoto, mikä käyttää matemaattisia algoritmeja sekoittaakseen viestit niin, että ainoastaan henkilöt, joilla on lähettäjän avain tai koodi pystyvät lukemaan viestejä. Käytetyimpiä salaustekniikoita ovat symmetrinen- ja asymmetrinen salaus. Symmetrisessä salauksessa käytetään yhtä yksityistä avainta tiedon salaamiseen ja purkamiseen. Asymmetrinen salaus puolestaan käyttää toimintaansa kahta erilaista yksityistä ja julkista avainta. (Rivera 2019.)

Yksi symmetrisen salauksen algoritmeista on Advanced Encryption Standard eli AES. AES voi käyttää 128-bit, 192-bit tai 256-bit pituista avainta, mitä pidempi avain sitä vahvempi. 128-bit avain on itsessään jo erittäin vahva, mutta useimmat valtion ohjeistukset vaativat käyttämään 256-bit avainta täyttääkseen tietyt standardit. AES:ta käytetään esimerkiksi tiedostojen ja levyjen salaamisessa. (Rivera 2019.)

Asymmetristä salausta käyttää RSA algoritmi, jonka nimi tulee sen kehittäjien mukaan Rivest, Shamir ja Adleman. RSA käyttää alkulukuja avaimien luontiin ja luotujen avaimien pituudet ovat esimerkiksi 2048-bit tai 4096-bit. Kansainvälinen standardien ja teknologian instituutti NIST suosittelee käyttämään vähintään 2048-bit pituista avainta. RSA on usein mukana muodostamassa turvallista VPN-yhteyttä käyttäjän ja palvelimen välille. (Lake 2018.)

Laite minkä levy on salattu, kysyy salausavainta ennen kuin edes käyttöjärjestelmä käynnistyy. Oikean salausavaimen syöttämisen jälkeen salaus alkaa purkautumaan, käyttöjärjestelmä käynnistyy ja kaikkiin salattuihin tiedostoihinkin pääsee käsiksi. Tästä syystä salauksen purkava salausavain on yksi mahdollisista heikkouksista. Siitä pitää tehdä tarpeeksi hankala, jottei kukaan pysty sitä arvaamaan, mutta joka on itselle helposti muistettava. Jos oman salausavaimen unohtaa, niin kukaan ei sen jälkeen pääse käsiksi laitteen tiedostoihin ja kadotat datan lopullisesti. (Lee 2015.)

Aina ei kuitenkaan ole pakko salata koko levyä. Salauksen voi tehdä myös yksittäisille kansioille tai tiedostoille. Vaihtoehtona on myös eräänlainen säiliö, joka on täysin salattu. Kaikki tiedostot tai kansiot, jotka luodaan tai tallennetaan säiliöön ovat salattuja. Monissa salausohjelmissa on vaihtoehtoina luoda salattu säiliö koko levyn salaamisen sijaan. (Rivera 2019.)

Sisäänrakennettuja salausohjelmia löytyy moderneista Windows ja Mac käyttöjärjestelmistä, sekä joistakin Linux distribuutioista. Windowsin oma salausohjelma BitLocker on Windows 10 Pro ja Enterprise versioissa, mutta ei Home versiossa. MacOS koneissa salausohjelmana on Apple FileVault. Linuxissa tyypillisesti levy salataan asennuksen aikana käyttämällä työkaluja kuten dm-cryptia. Lukuisia kolmannen osapuolen salausohjelmia löytyy kyllä myöhempääkin salausta varten Linuxille ja muille käyttöjärjestelmille. (Rivera 2019.)

3.8 Levyn salausohjelmia

3.8.1 Yleistä

Turvatakseen laitteen datan koskemattomuuden katoamistilanteissa, pitää datan olla salattuna asianmukaisesti. Avuksi löytyy salaustekniikoita käyttäviä ohjelmistoja. Salausohjelmistoja on kehitelty monille käyttöjärjestelmille ja eri tarkoituksiin. Löytyy salausohjelmistoja, mitkä salaavat koko levyjä, yksittäisiä tiedostoja tai erikoistuvat pilvialustojen salaamiseen. Ohjelmistoja löytyy maksullisia ja ilmaisia, sekä yrityksille ja yksityishenkilölle. Esimerkkejä salausohjelmistoista ovat AxCrypt, Folder Lock ja Veracrypt (Fearn & Turner 2020).

3.8.2 Bitlocker

Bitlocker on Microsoftin oma helppokäyttöinen salausohjelma Windowsille. Bitlocker on saatavilla kaikille Windows käyttäjille, jotka käyttävät Windows 10 Pro, Education tai Enterprise versioita. Bitlocker kuuluu myös joihinkin Windows 8.1, Windows 7 ja Windows Vistan versioihin. Bitlockerin käyttövaatimuksiin kuuluu oikean käyttöjärjestelmän version lisäksi laitteistovaatimuksia. Laitteiston puolelta tarvitaan kahdeksi osioidun kiintolevyn lisäksi Trusted Platform Module eli TPM. TPM on erityinen

mikrosiru, joka ajaa todennustarkastuksia laitteiston raudalle ja ohjelmistolle. Jos TPM havaitsee näissä asioissa muutoksia, käynnistyy kone rajoitetussa tilassa estääkseen laitteen luvattoman käytön. Kaikissa koneissa ei ole asennettuna TPM mikrosirua ja silloin Bitlockerin käyttöönotto vaatii säätämistä Group Policy Editorissa. Käyttäjän ei itse tarvitse tietää, löytyykö koneesta TPM tai kahden osion kiintolevy, koska Bitlocker tarkistaa nämä asiat sen käynnistyessä. (Paul 2016.)

Bitlockerin best practice käytännön mukaista on käyttää kaksivaiheista tunnistautumista. Tämä tarkoittaa, että TPM:n lisäksi vaatii PIN-koodia käynnistyksen yhteydessä. PIN-koodin käyttö lisää merkittävästi järjestelmän turvallisuutta. (Prepare your organization for BitLocker 2019.)

4 Testaukset

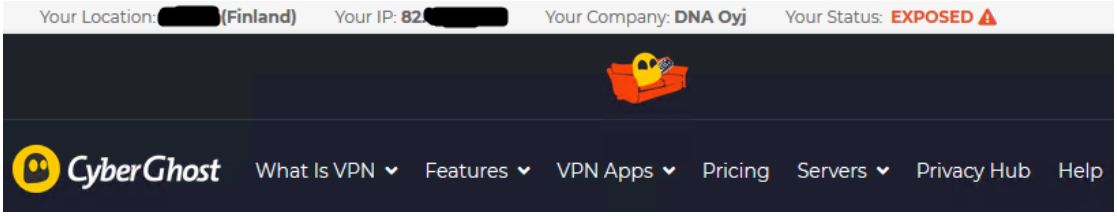
4.1 VPN testaukset

4.1.1 Yleistä

Testaukset hoidettiin virtuaaliympäristössä käyttämällä Oracle VM VirtualBoxia ja siihen ympäristöön Microsoftin tarjoamaa Windows 10 Enterprise Evaluation versiota. Käytetty VirtualBoxin versio oli 6.0 ja Windowsin versio 1909. Testataan valituista palveluntarjoajista CyberGhostin VPN-ohjelmisto, koska Gyberghost tarjoaa 24 tunnin ilmaista kokeiluversiota toisin kuin NordVPN.

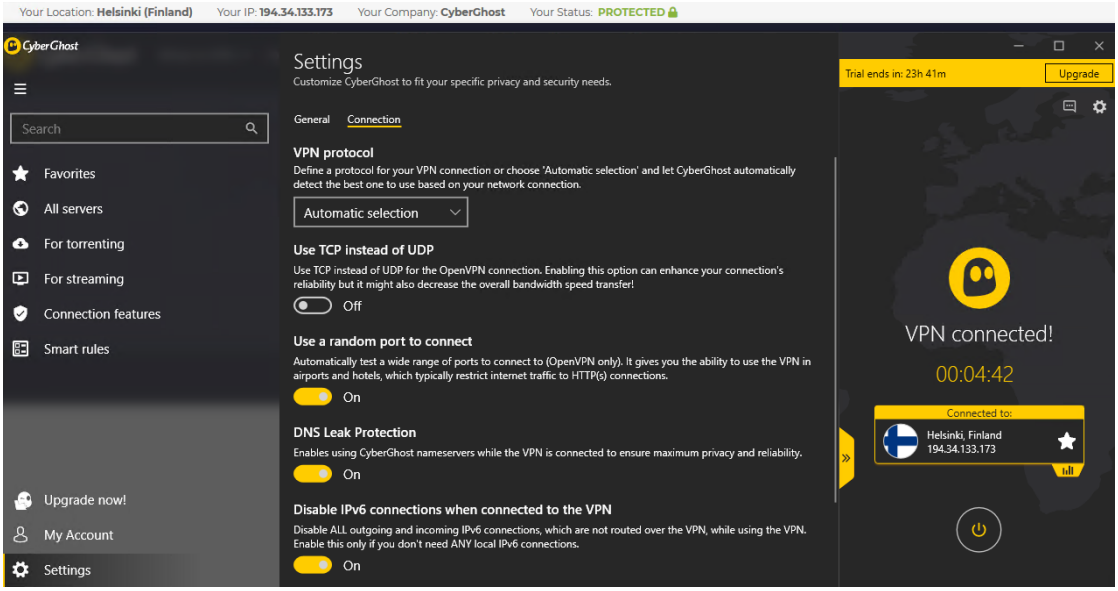
4.1.2 CyberGhost VPN-ohjelmisto

Ennen kuin pääsee edes lataamaan ohjelmistoa, niin heti CyberGhostin verkkosivujen yläkulmassa näkyy palkki, mikä kertoo oman sijainnin, IP-osoitteen ja internetin-palveluntarjoajan sekä ilmoittaa tilan olevan exposed (ks. Kuvio 1) eli yhteys ei ole suojattu VPN:nää käyttämällä.



Kuvio 1. CyberGhostin verkkosivujen yläpalkki

CyberGhostVPN tarjoaa 24-tunnin kokeiluversion heidän VPN-ohjelmistollensa ja sitä käytetään tähän testaukseen. Ohjelman latauksen jälkeen pitää luoda käyttäjätunnus antamalla sähköpostitunnus ja asettamalla haluttu salasana. Sähköpostiin saapuneen varmistusviestin jälkeen 24-tunnin kokeilu aktivoitui, joka näkyy myös selkeästi oikeassa alareunassa olevasta CyberGhostin ikkunan juoksevasta ajasta. Keskellä ikkunaa on nappi, joka muodostaa VPN-yhteyden automaattisesti parhaimmaksi havaittuun palvelimeen. Ikkuna laajenee keltaisista nuolista ja sieltä pääsee muokkaamaan asetuksia. Napin painalluksen jälkeen CyberGhost yhdisti minut Helsingissä sijaitsevaan VPN-palvelimeen ja myös heidän verkkosivuillaan olevan yläpalkin tiedot muuttuivat vastaavasti ja tilaksi tuli protected eli suojattu (ks. Kuvio 2). IP-osoitteen ja sijaintitietojen muutos tarkistettiin myös muita sivustoja, kuten ”whatismyipadress.com” käyttämällä ja kaikki näyttivät sijainniksi Helsinki.

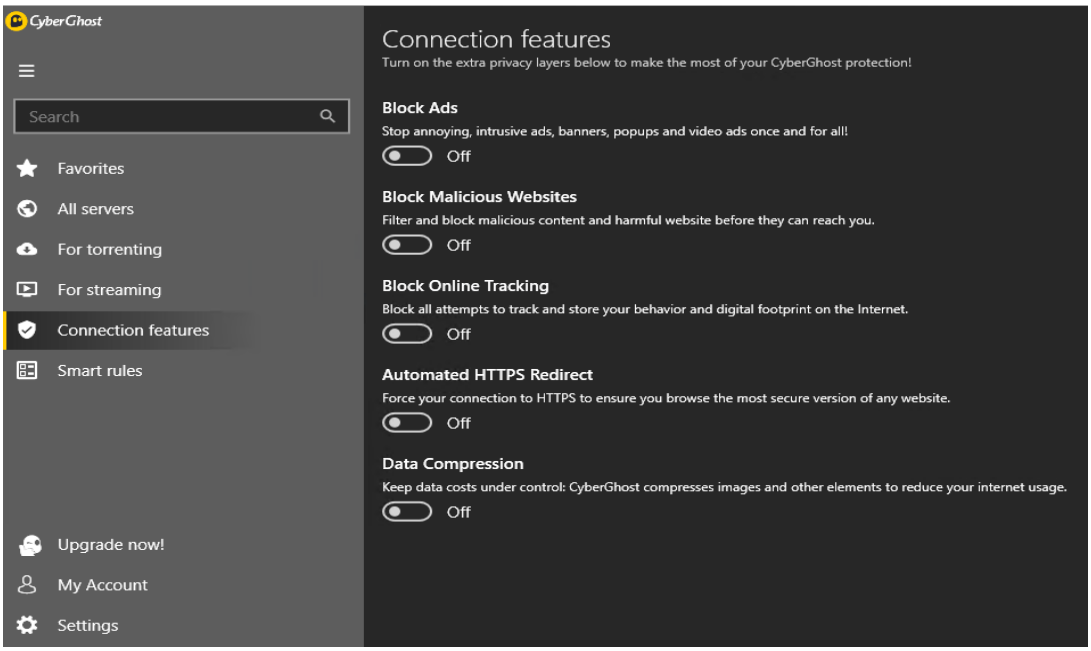


Kuvio 2. VPN-yhteys muodostettu

Kuvio 2 ollaan asetuksien yhteyden välilehdellä ja sieltä voi valita käytettävän VPN-protokollan, jonka voi asettaa automaattisen valinnan lisäksi, joko OpenVPN tai IKEv2. OpenVPN on näistä turvallisin vaihtoehto. Alapuolella olevat neljä nappia ovat

oletuksena hyvissä kohdissa peruskäyttäjälle. Ensimmäisessä kohdassa valitaan käyttääkö OpenVPN UDP vai TCP:tä, vakiona käytössä on UDP mikä tarjoaa parempaa nopeutta. Toinen nappi päättää testaako OpenVPN mikä on paras portti yhteyden muodostamiseen vai käyttääkö vakioporttia, mikä on kylläkin voitu estää verkon palomuurin toimesta. Kolmantena tärkeä turvallisuusvaihtoehto DNS vuodon esto, joka ehdottomasti kannattaa pitää päällä lisätyn yksityisyyden varmistamiseksi. Viimeinen vaihtoehto estää kaiken VPN-yhteyden ulkopuolella tapahtuvan IPv6 liikenteen. Näihin asetuksiin ei siis tarvitse koskea, ellei ole aivan varma mitä tekee.

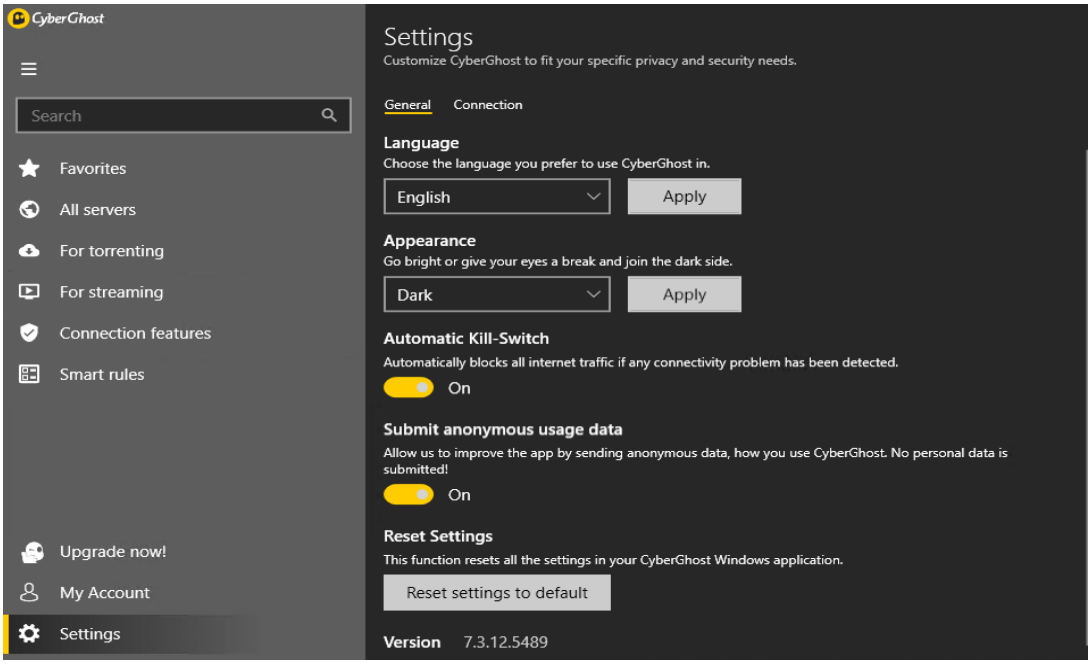
Yhteyden ominaisuudet sivulla (ks. Kuvio 3) nähdään vaihtoehtoja laittaa päälle lisäturvallisuuden ominaisuuksia, kuten mainosten ja haittasivustojen estoja. Nämä asetukset normaalisti kannattaisi pitää päällä, mutta tässä 24-tunnin kokeiluversiossa näitä ei saanut aktivoitua. Viimeinen vaihtoehto on datan kompressointiin liittyvä, mitä ei tarvitse nopealla verkkoyhteydellä tarvitse käyttää. Hidasta verkkoyhteyttä käytettäessä se voi auttaa lataamaan verkkosivuja nopeammin.



Kuvio 3. Yhteyden ominaisuuksia

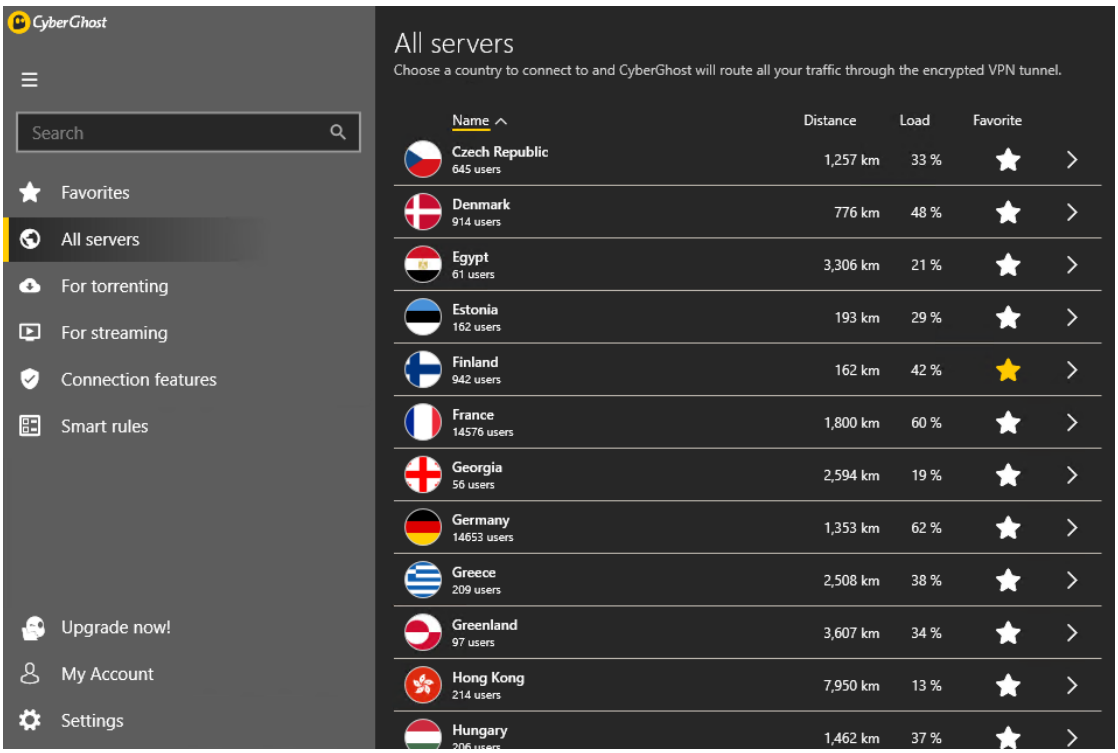
Yleisissä asetuksissa (ks. Kuvio 4) tärkein vaihtoehto on automaattinen kill switch, jonka saa laitettua päälle tai pois. Vakiona se on päällä ja siinä se myös kannattaa pitää. Jos salatussa VPN-yhteydessä ilmenee jotain häiriöitä niin kill switch katkaisee kaiken internetliikenteen välittömästi ja näin estää tiedon vuotamisen vääriin käsiin. Seuraavana valintana on, haluaako lähettää anonyymiä dataa CyberGhostin käytöstä

sen kehittäjille. On se tieto sitten kuinka anonyymiä tahansa niin en itse ainakaan halua turhaan lähetellä mitään dataa minnekään, joten otan sen pois päältä.



Kuvio 4. Yleiset asetukset

CyberGhostin palvelinluettelo (ks. Kuvio 5) on yksinkertainen ja siinä näkyy hyödyllisiä tietoja, kuten etäisyys maan palvelimiin, mikä vaikuttaa yhteyden viiveeseen ja nopeuteen. Esimerkiksi Viron palvelimiin yhdistettynä netin käyttö on sujuvampaa kuin Hong Kongiin yhdistettynä, koska Viroon matkaa on alle 200 km ja Hong Kongiin melkein 8000 km. Toinen hyödyllinen tieto on ”load” eli palvelimien kuormitus, mikä kertoo, kuinka paljon muut ihmiset käyttävät kyseisen maan VPN-palvelimia. Kannattaa yhdistää sellaiseen palvelimeen, minkä kuormitus ei ole lähellä 100% taatakseen itselleen parhaimman käyttökokemuksen.

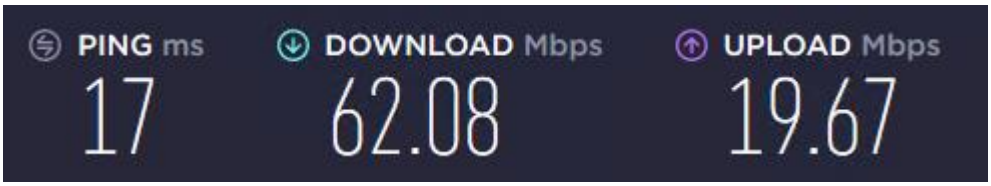


Kuvio 5. Palvelinluettelo

Palvelinluettelon alta löytyy myös erikseen välilehdet palvelimille, jotka ovat optimoitu torrenteille tai striimaamiselle eli suoratoistolle. Suoratoistoa tarjoavia palveluita ovat esimerkiksi Netflix ja Youtube. Suoratoistoon erikoistuvien palvelimien kerrotaan olevan nopeampia kuin normaalipalvelin, mutta näitä ei pääse testaamaan ilmaisversiossa.

Nopeustestit

Nopeustestit suoritettiin ”speedtest.net” sivustoa käyttäen ja yhteyteni normaalinopeudet ovat latauksessa 190 Mbps ja lähetyksessä 19 Mbps. Virtuaalitietokonetta missä testit suoritettiin, käytettiin tietokoneessa, joka oli langattomasti verkossa kiinni ja sen takia latausnopeus näytti vain 62 Mbps. Langatonta verkkoa käyttäen ja VPN-yhteys pois päältä latausnopeuteni näytti 62 Mbps ja lähetys 19 Mbps (ks. Kuvio 6). Käytetään näitä nopeuksia vertailukohteena, kun laitetaan VPN päälle.



Kuvio 6. Virtuaalikoneella normaalinopeudet

VPN-yhteys muodostettiin Ruotsin palvelimiin ja sen jälkeen suoritettiin sama testi, joka näytti latausnopeudeksi 48 Mbps ja lähetys samat 19 Mbps. Hieman kauemmaksi Sveitsiin otettu VPN-yhteyden latausnopeudeksi tuli 30 Mbps ja lähetys hieman alle 19 Mbps. Yhteyden ping eli viive oli tietenkin hieman lisääntynyt kotimaahan verrattuna, koska välimatka oli kasvanut noin 1700 kilometrillä ja Sveitsin yhteydessä se näytti 42 millisekuntia. Kolmas testi tehtiin vielä Yhdysvaltoihin olevalla yhteydellä ja silloin viive näytti 121 ms, latausnopeus enää 11 Mbps ja lähetysnopeus 18 Mbps. Välimatkaa tällä yhteydellä oli jo huimat 7500 km. Testattujen kolmen maan palvelimien kuoritus oli testihetkellä kaikissa alle 50%. Latausnopeus pieneni melkein kuudesosaan Yhdysvaltojen yhteydessä, mutta normaalisti ei tarvitsekaan yhdistää noin kauas maantieteellisesti, ellei halua juuri katsoa esimerkiksi kyseisen maan Netflix sarjoja.

Johtopäätökset

Mielestäni CyberGhost VPN:n käyttöliittymä on erittäin yksinkertainen ja asiat löytyvät helposti, joka on hyvä asia käyttäjän kokemusta ajatellen. Vakiona asetukset olivat myös kohdillaan ja aivan peruskäyttäjän ei tarvitse miettiä muuta, kuin mihin maahan yhdistää palvelinluettelosta. Hyvä valinta siis henkilöille, ketkä eivät ennen ole käyttäneet VPN-palveluja ja haluavat sekä helppokäyttöisen että tyylikkään käyttöliittymän. Lisäksi 24-tunnin testiversio ohjelmisto on helppo tapa testata, sopiiko tämä omiin tarpeisiin ja ilman minkäänlaisia sitoumuksia.

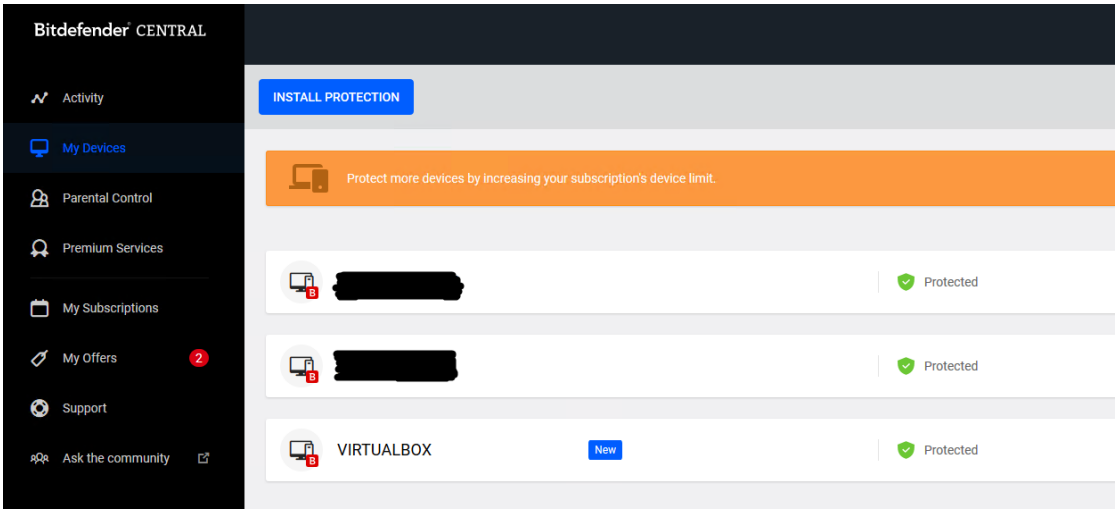
4.2 Haittaohjelmasuojauksien testaus

4.2.1 Yleistä

Testataan Bitdefenderin Internet Security paketti, koska omistan kyseisen paketin. Bitdefenderin lähes kaikkiin paketteihin on saatavilla 30-päivän kokeiluversio, eli kaikki pystyvät testaamaan vaihtoehtoja ennen ostopäätöksiä. Internet Security paketti tarjoaa samat ominaisuudet kuin Total Security, lukuun ottamatta suojausta macOS, iOS ja Android laitteille. Testit suoritettiin samassa virtuaaliympäristössä kuin aikaisemmat VPN testit.

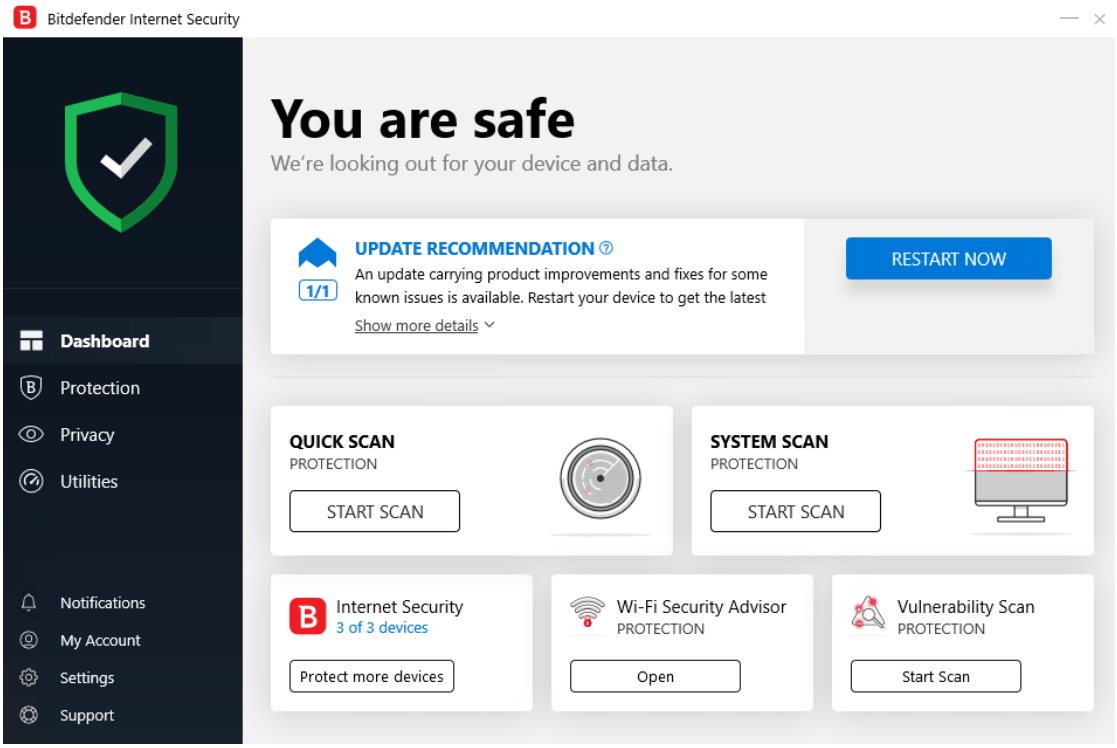
4.2.2 Bitdefender

Virtuaalikoneelle asentaminen oli erityisen helppoa, koska Bitdefender ohjelmisto oli jo asennettu toiselle koneelleni ja sieltä käytiin vain generoimassa latauslinkki, mikä syötettiin virtuaalikoneen selaimeen ja lataus lähti käyntiin. Näin kaikki suojatut laitteet tulevat tililleesi näkyviin Bitdefenderin Centraliin, joka on selaimella mentävä hallintapaneeli. Asennuksen jälkeen virtuaalikone tuli näkyviin Centraliin (ks. Kuvio 7) nimellä virtualbox. Ylhäällä olevasta sinisestä painikkeesta olisi myös voinut generoida latauslinkin, jonka olisi voinut kopioida tai lähettää sähköpostilla eteenpäin.



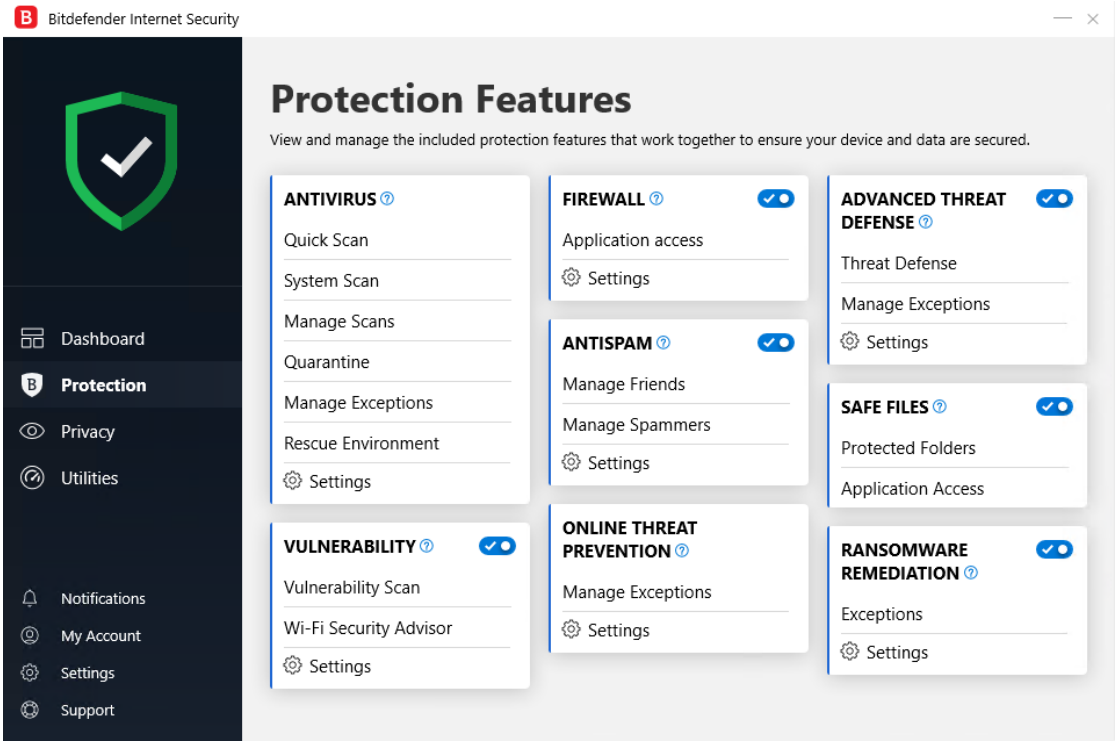
Kuvio 7. Bitdefender Central

Bitdefenderin aloitusikkunassa (ks. Kuvio 8) näkyy mitä toimenpiteitä ohjelmisto ehdottaa tehtävän, sekä pikavalintoja eri toiminnoille kuten skannauksille. Esimerkiksi tälle virtuaalikoneelle Bitdefender ehdottaa uudelleen käynnistämistä, koska on tullut uusia Windows päivityksiä. Kaikki pikavalinnat ovat muokattavissa ja löytyvät myös vasemmassa reunassa sijaitsevien välilehtien alta.



Kuvio 8. Bitdefenderin aloitusnäkymä

Bitdefenderin suojausvälilehdellä pystyy tarkastelemaan ja muokkaamaan kaikkia turvallisuusominaisuuksien asetuksia (ks. Kuvio 9). Kaikki ovat oletuksena päällä. Melkein ainoa asetus mihin itse tarvitsee puuttua, on poikkeuksien hallinta. Poikkeuksiin voidaan laittaa sellaisia sovelluksia tai verkkosivuja, jotka käyttäjä tietää varmasti luotettaviksi, mutta Bitdefender estää niiden toiminnan tiukkojen sääntöjen vuoksi.



Kuvio 9. Bitdefenderin suojausvälilehti

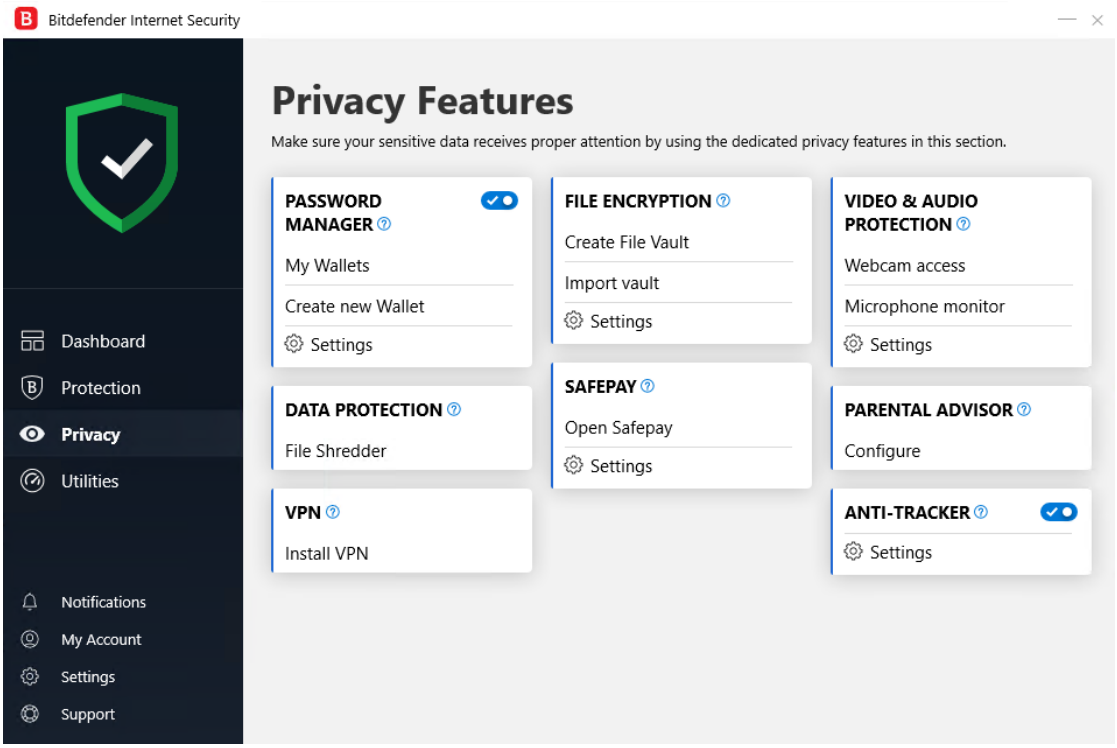
Antiviruksen alta löytyy kaikki tiedostoihin liittyvät skannaukset. Tähän kuuluu mm. laitteen ohjelmistojen, sähköpostien liitetiedostojen ja liitettävien tallennusvälineiden automaattinen skannaus uhkatekijöiden varalta. Asetuksien alta voidaan tarkemmin laittaa päälle tai pois mainittuja yksittäisiä toimintoja. Haavoittuvuuksien alta suoritettava skannaus ei etsi haittaohjelmia, vaan tarkistaa muita uhkia, kuten käyttöjärjestelmään ja ohjelmistoihin saatavia päivityksiä, käyttäjien salasanojen vahvuuksia ja Wi-Fi yhteyden turvallisuutta. Skannauksen päätyttyä samasta ikkunasta saisi myös korjattua löydetyt ongelmat, eli korjaustoimenpiteiden suoritus on tehty erittäin helpoksi käyttäjän kannalta.

Palomuurista voi luoda sääntöjä, mitkä estävät tai sallivat verkkoliikenteen käytetyn protokollan, portin, IP-osoitteen tai suunnan mukaan. Bitdefenderin palomuurin toimintoihin kuuluu lisäksi porttiskannauksien esto. Tämä hankaloittaa kyberrikollisten elämää, jos he haluaisivat hyödyntää laitteessa olevia avoimia portteja. Bitdefenderin palomuurin ja antiviruksen ollessa päällä korvaavat ne Windows Defenderin vastaavat toiminnot. Niiden ollessa päällä voidaan kaikkia suojaustoimintoja hallita helposti Bitdefenderin keskitetystä hallintaikkunasta, eikä tarvitse välillä mennä Windows Defenderin asetuksiin tekemään uusia sääntöjä palomuuriin tai suorittamaan virusskannausta.

Antispam toimii paikallisissa sähköpostisovelluksissa, kuten Outlookissa ja Thunderbirdissä. Sen tarkoituksena on suodattaa roskapostia ja normaalin sähköpostiosoitteiden eston lisäksi asetuksista löytyy vaihtoehto estää automaattisesti sähköpostit, jotka sisältävät aasialaisia tai kyrillisiä kirjaimistoja. Verkkouhkien torjunnan kerrotaan pohjautuvan pilvessä olevaan verkostoon, joka käyttää edistyksellisiä koneoppimisen algoritmeja suojaamaan kalasteluilta ja muilta verkosta tulevilta huijausyrityksiltä. Asetuksien alla kaikki suojausvaihtoehdot ovat päällä, ja niitä ei kannatakaan ottaa pois päältä, vaikka oma luotettava verkkosivu estettäisiin syystä tai toisesta. Tällaisessa tilanteessa kannattaa luotettava verkkosivu lisätä poikkeuksien listalle, eikä siis ottaa suojausta kokonaan pois päältä, jotta seuraava oikea huijausverkkosivusto estetään automaattisesti.

Edistynyt uhkien puolustus on Bitdefenderin behavior monitoring asetus eli se tarkkailee ohjelmistojen toimintaa ja estää epänormaalisti käyttäytyvät sovellukset. Asetuksissa ei ole muita vaihtoehtoja kuin päälle tai pois. Safe Files kohdasta voidaan lukita halutut kansiot niin, ettei mikään ohjelma pysty siellä olevia tiedostoja muokkaamaan tai poistamaan. Tämän on tarkoitus olla suojana myös ransomwareja vastaan. Suojattuina ovat automaattisesti käyttäjän tiedostot, valokuvat ja OneDrive kansiot. Viimeisenä on ransomwaren korjaus, jonka tarkoituksena on automaattisesti palauttaa ransomwaren takia salatut tiedostot. Se luo tiedostoista, mitkä ransomware yrittää salata, automaattisesti varmuuskopioit ja niiden avulla palauttaa alkuperäiset tiedostot ransomwaren estämisen jälkeen.

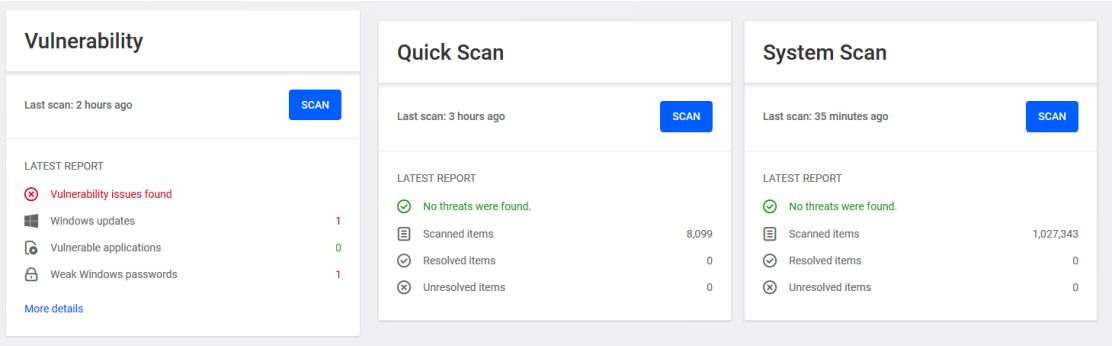
Yksityisyysvälilehdeltä löytyy erilaisia lisätoimintoja, mitkä eivät enää suoraan liity haittaohjelmien tai viruksien torjuntaan (ks. Kuvio 10). Tarjolla on salasanojen hallintaa, tiedostojen täydellistä tuhoamista jälkiä jättämättä, minimaalinen VPN, salasanalla suojattu tiedostosäiliö, eristetty maksuympäristö pankkiasioille, kameran ja mikrofonin suojaus, lapsien valvontatyökalu vanhemmille ja datan keruun esto verkkoselaimille. Hyödylliseksi näistä olen kokenut kameran ja mikrofonin suojauksen, josta saa asetuksen päälle, mikä ilmoittaa aina kun jokin sovellus käyttää näitä. Lisäksi käytössäni on anti-tracker laajennus selaimessa, mikä estää verkkosivuja keräämästä dataa käyttäjistä. Laajennus ilmoittaa sivukohtaisesti, mitä seurantapalvelimia ja analytiikkatyökaluja on estetty. Esimerkiksi Google Analytics on yleinen estettävä kohde verkkosivuilla.



Kuvio 10. Bitdefenderin yksityisyysvälilehti

Skannaus testit

Suoritettiin testikoneella Bitdefenderin tarjoamat haavoittuvuus-, nopea- ja järjestelmäskannaus. Bitdefenderin haavoittuvuusskannaus ei montaa sekuntia kestänyt. Testikoneen haavoittuvuusskannauksessa löytyi heikko Windows käyttäjän salasana ja aikaisemminkin mainittu asentamaton Windows päivitys. Nopeassa skannauksessa meni testikoneella aikaa 3 minuuttia ja skannattuja kohteita oli noin kahdeksan tuhatta. Täydessä järjestelmä skannauksessa meni 1 tunti ja 20 minuuttia ja kohteita tarkastettiin yli miljoona. Kaikki viimeisimmät skannaukset ja niiden tulokset löytyvät myös Bitdefenderin Centralista (ks. Kuvio 11. Skannauksien tuloksetKuvio 11). Centralista pystyy myös suorittamaan suojattujen laitteiden skannaukset etänä, mikä on kätevää, jos on esimerkiksi asentanut kaikkiin perheen laitteisiin Bitdefenderin ja haluaa tarkistaa perheenjäsenen tietokoneen tai puhelimen turvallisuuden.



Kuvio 11. Skannauksien tulokset

Johtopäätökset

Lukuisat konfiguraatio mahdollisuudet voivat saada uuden käyttäjän pään pyörälle, mutta Bitdefenderin tuote toimii ”out of the box” -mallilla eli tuote on heti käytettävissä ja toimintakunnossa asennuksen jälkeen. Kaikki tarvittavat suojausasetukset ovat vakiona päällä ja ainoa mitä käyttäjä itse voi haluta tehdä on suorittaa alkuskannaukset. Bitdefenderin hallintapaneeli Central on kätevä työkalu pitämään tiedossa, mitä laitteita on suojattu, sekä suorittamaan niihin skannauksia helposti samasta näkymästä. Lisäominaisuuksistakin löytyy hyödyllisiä toimintoja. Yhteenvetona Windows koneille suojaa tarjoava Bitdefenderin Internet Security paketti on oikein kattava ja toimiva kokonaisuus.

4.3 Varmuuskopioinnin testit

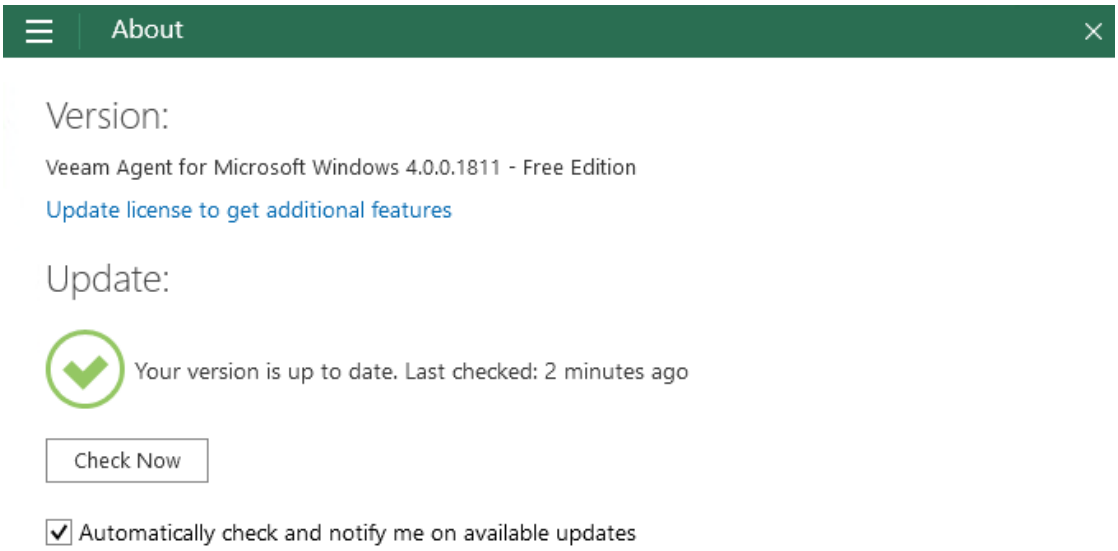
4.3.1 Yleistä

Testattiin Veeam:n tuotetta Veeam Agent for Microsoft Windows FREE, koska se on ilmainen ja siitä löytyy tarpeelliset ominaisuudet. Testit suoritettiin samassa virtuaaliympäristössä kuin aikaisemmatkin testit.

4.3.2 Veeam

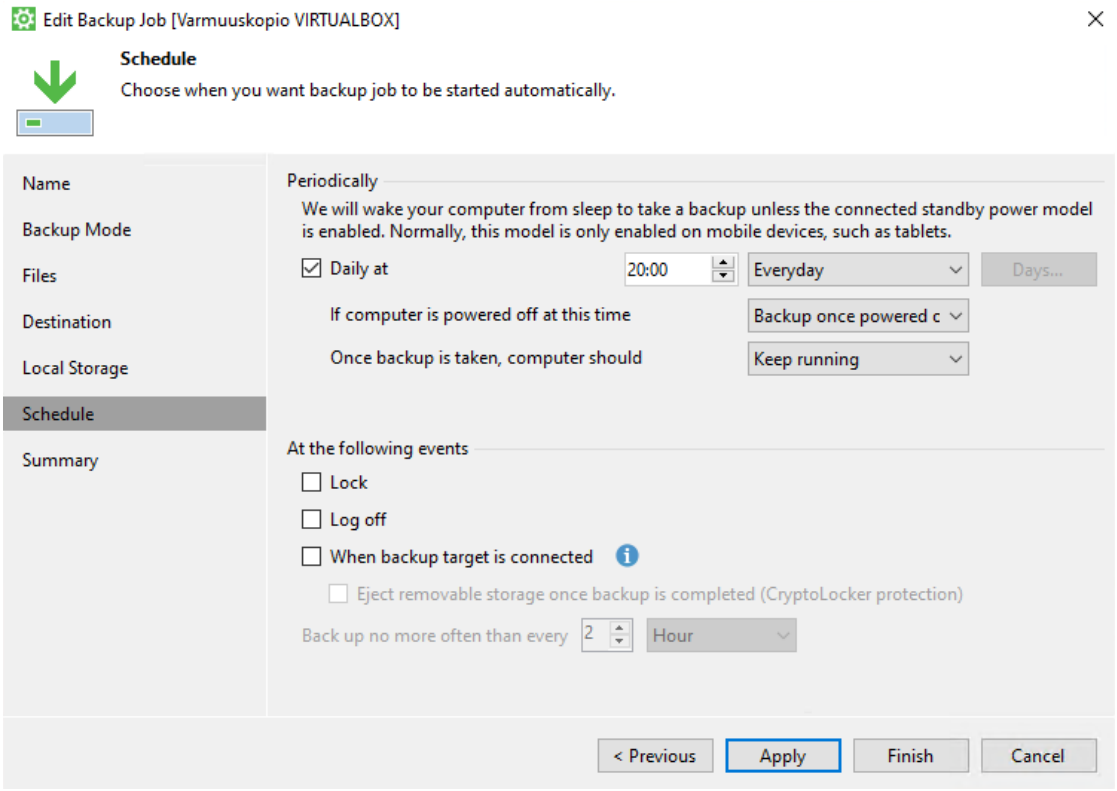
Asennuksen jälkeen avautui yksinkertaisen näköinen Veeam agentin käyttöliittymä (ks. Kuvio 12). Vasemmasta yläkulmasta avautuu sivupalkki, mistä voidaan luoda uusi varmuuskopiointitehtävän. Tehtävä nimetään halutulla tavalla ja sen jälkeen päätetään, halutaanko tehdä varmuuskopio koko tietokoneesta, loogisista levyistä

vai yksittäisistä tiedostoista. Loogiset levyt ovat Windowsissa esimerkiksi C- tai D-asema. Varmuuskopioitavien tiedostojen valinnan jälkeen päätetään tallennussijainti. Sijainti vaihtoehtoina ovat tallennus sisäisiin tai ulkoisiin kiintolevyihin, jaettuihin sijainteihin, Veeam:n omiin palvelimiin tai Microsoftin Onedriveen. Jaettuja sijainteja ovat esimerkiksi NAS eli Network Attached Storage tai tiedostopalvelin.



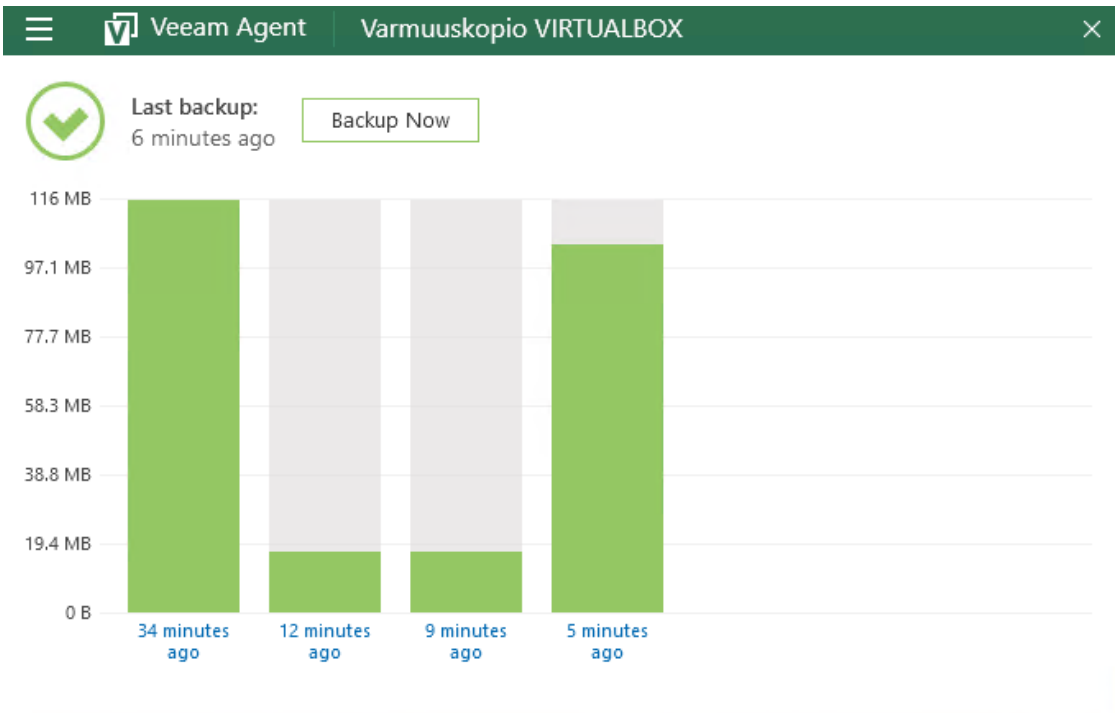
Kuvio 12. Veeam agentti

Testitarkoituksiin valittiin varmuuskopioitavaksi yksittäisiä kansioita ja sijainniksi paikallinen kiintolevy. Normaalisti varmuuskopioiden tallennus tällä tavalla samoihin sisäisiin kiintolevyihin, missä alkuperäisetkin tiedostot sijaitseva ei ole suositeltavaa. Tästä varoittelee myös Veeam agentti. Sijainnin jälkeen valitaan vielä tarkemmin kansio mihin varmuuskopio luodaan. Samasta ikkunasta lisäksi valitaan, kuinka monta päivää varmuuskopioita halutaan säilyttää. Vakiona siinä on seitsemän päivää. Viimeisenä asetuksena tulee varmuuskopioinnin aikataulutus. Aikataulutuksessa automatisoidaan varmuuskopiointi halutuille päiville ja haluttuun kellonaikaan (ks. Kuvio 13). Varmuuskopiointi on myös mahdollista asettaa automaattisesti alkamaan, kun koneen lukitsee, kirjautuu ulos tai kiinnittää ulkoisen kiintolevyn kiinni.



Kuvio 13. Veeam aikataulutus

Asetuksien jälkeen suoritettiin neljä testivarmuuskopiointia (ks. Kuvio 14). Ensimmäinen varmuuskopiointi näkyy vasemmanpuoleisessa palkissa. Y-akseli kertoo datan määrän, kuinka paljon kopioitiin ja x-akselilla näkyy, koska viimeksi suoritettiin varmuuskopiointi. Kaksi seuraavaa varmuuskopiointia näkyy matalina palkkeina, koska niissä ei lisätty mitään uusia tiedostoja varmuuskopioitavaan kansioon. Viimeisessä varmuuskopioinnissa kansioon lisättiin 100 Mt täytedataa ja se näkyy vihreän palkin korkeudessa. Kuten testeistä huomattiin, normaalisti ohjelmisto kopioi vain täysin uudet tiedostot kohdesijainnista. Veeam agentin alkuasetuksista on mahdollista myös laittaa sellainen asetus päälle, mikä kopioisi aina kaiken datan halutusta sijainnista, oli se sitten uutta tai vanhaa. Varmuuskopiointien jälkeen on käyttöliittymästä myös mahdollista palauttaa tiedostojen tila mihin vain aikaisempaan vaiheeseen. Näin voidaan palauttaa esimerkiksi vahingossa poistetut tiedostot tai palautua haittaohjelman tekemistä vaurioista.



Kuvio 14. Suoritetut varmuuskopioinnit

Testatun Veeam agentin ilmaisversion rajoitukset havaitsi, kun yritti luoda toista varmuuskopiointitehtävää. Sovellus ilmoitti, että ilmaisversio tukee vain yhtä tehtävää kerrallaan. Aikaisemmin luodun tehtävän voi poistaa ja luoda uuden, mutta tämä ei ole kovin käytännöllistä, mikäli haluaa päivittäin varmuuskopioida moneen paikkaan. Veeam Ilmaisversio toimii siis käyttäjille, joille riittää yksi varmuuskopiointitehtävä kopioimaan halutut tiedostot yhteen paikkaan.

Johtopäätökset

Veeam agentin hyviä puolia on helppokäyttöinen ja yksinkertainen käyttöliittymä. Yksinkertaiselta näyttävä käyttöliittymä kuitenkin kätkee allensa tarpeelliset asetukset ja vaihtoehdot suoriutuakseen tehtävistään. Heikkona puolena on ilmaisversion rajoitus luoda vain yksi varmuuskopiointitehtävä kerrallaan. Rajoitus voi saada käyttäjiä etsimään vaihtoehtoisia ratkaisuja tai miettimään maksullista versiota.

4.4 Levyn salausohjelmistojen testaus

4.4.1 Yleistä

Testattiin Microsoftin Bitlocker, koska testikoneena toimi Windows 10 Enterprise versio ja Enterprise versioon sisältyy Bitlocker. Testit suoritettiin samalla virtuaalikoneella kuin aikaisemmatkin testit.

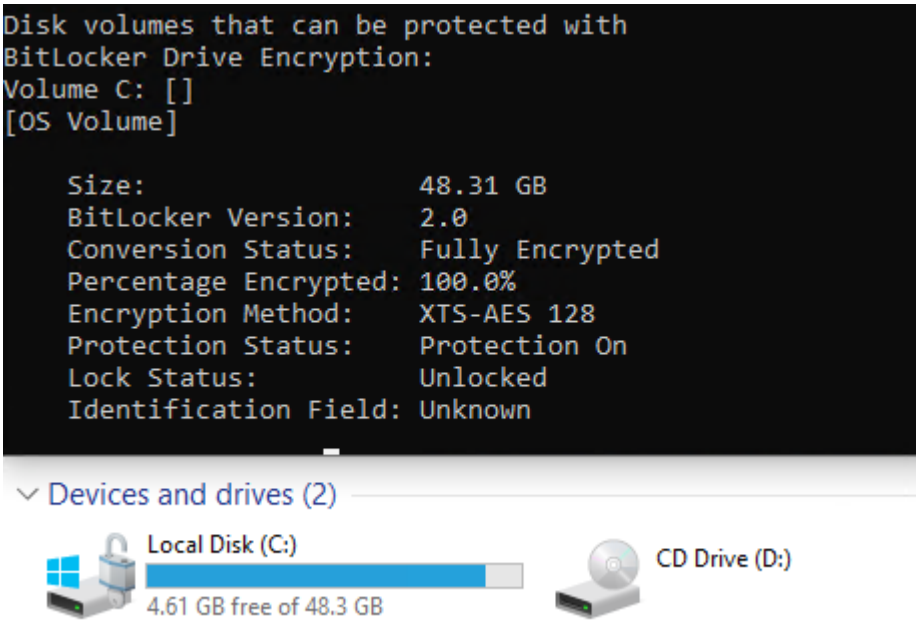
4.4.2 Bitlocker

Virtuaalikoneen resurssienhallinnasta yritettiin suoraan laittaa C-asemalle Bitlocker käyttöön, mutta tuli ilmoitus, että tämä laite ei voi käyttää TPM:ää. Ilmoituksessa luki, että pitäisi laittaa sellainen asetus päälle, mikä sallisi Bitlockerin käytön ilman TPM:ää. Isäntäkoneessa, jossa virtuaalikone pyörii, löytyy TPM, mutta VirtualBoxin kone ei pysty tätä käyttämään. Joudutaan siis käymään Group Policy Editorissa laittamassa tuo asetus päälle (ks. liite 1).

Näiden toimenpiteiden jälkeen yritettiin uudelleen salata C-asema. Päästiin eteenpäin ja ensimmäisenä kysyttiin, avataanko tietokone käynnistyksen jälkeen USB-tikulla vai salasanalla. Nämä vaihtoehdot tulivat käyttöön, koska TPM otettiin aikaisemmin pois käytöstä. Tämän jälkeen valitaan, miten tallennetaan palautusavain. Avaimen voi tallentaa Microsoft tiliin, USB-tikulle, tiedostoon tai tulostaa. Palautusavaimen tallennuksen jälkeen päätetään, salataanko koko levy vai vain käytössä oleva tila. Bitlocker kertoo koko levyn salauksen olevan parempi jo käytössä oleille koneille ja vain käytetyn tilan salauksen olevan parempi uusille koneille. Näiden asetuksien jälkeen alkaa valitun aseman salaaminen. Testikoneella valittiin salasana koneen avaamiseen, palautusavain tallennettiin USB-tikulle ja salatiin koko C-levy. Salatun levyn koko oli 48 GB ja sen salaaminen Bitlockerilla kesti noin puoli tuntia.

Salauksen jälkeen tietokone käynnistettiin uudestaan ja heti käynnistämisen jälkeen kysyttiin salasanaa. Tätä kohtaa ei siis normaalisti tulisi, jos TPM olisi käytössä. Vasta salasanan syötön jälkeen alkoi Windows käyttöjärjestelmä latautua ja seuraavaksi kysyttiin normaalisti käyttäjän salasanaa. Komentokehotteelta nähdään Bitlockerin tila eri asemilla syöttämällä ”manage-bde -status” komento. Testikoneella tämä kertoi C-

aseman olevan täysin salattu (ks. Kuvio 15). Komentokehotteen alapuolella on myös näkymä resurssienhallinnasta ja huomataan, että C-aseman päälle on tullut lukon kuva. Tämä kertoo aseman olevan salattu Bitlockerilla. Lukko on auki, koska asema avattiin syöttämällä avaussalasana koneen käynnistyessä.



Kuvio 15. Bitlockerin tila

Bitlockerin käyttöönotto oli näin helppoa, vaikka ilman TPM:ää se aiheuttikin hieman lisätoimenpiteitä. Tietokoneen avaamisen jälkeen Bitlockerin saa otettua myös kokonaan pois käytöstä, mutta tällöin aseman salaus pitää purkaa ja siinä menee oma aikansa.

Johtopäätökset

Bitlocker on helposti käyttöönotettava yhteensopivissa Windows versioissa. Bitlocker on kuitenkin suunniteltu salaamaan vain kokonaisia levyjä tai osioita, joten yksittäisien tiedostojen tai kansioiden salaamiseen on käytettävä muita työkaluja. Yritysympäristöt koostuvat usein Windows laitteista, joten Bitlocker on hyvä vaihtoehto salaamaan ainakin paljon matkustavien työntekijöiden kannettavat tietokoneet.

5 Yhteenveto

Työmatkustaminen lisää yrityksen ja työntekijän datan riskiä päätyä ulkopuolisten käsiin. Työntekijän astuttua työkoneen kanssa ulos yrityksen tiloista, on koneen datan turvallisuus yrityksen tekemien suojatoimenpiteiden ja käyttäjän toiminnan varassa. Dataan kohdistuva uhka voi tulla melkein mistä tahansa, kuten avoimista verkoista, julkisen kulkuneuvon kanssamatkustajista tai käyttäjältä itseltään. Uhkatekijöitä ovat esimerkiksi haittaohjelmat, laitevarkaudet ja laiterikot. Onneksi näitä uhkia vastaan on olemassa suojautumiskeinoja.

Suojautumiskeinojen kautta löytyi myös vastaukset tutkimuskysymyksiin. Tutkimuskysymykset olivat: miten työntekijä voi käyttää turvallisesti verkkoa työmatkoilla, mitä muita uhkia kohdistuu työntekijän datalle työmatkoilla ja miten näiltä uhkatekijöiltä suojaudutaan. Suojautumiskeinona avoimen verkon seurannalta ja kuuntelulta on käyttää VPN:ää, eli Virtual Private Networkia. Haittaohjelmilta eli malwareilta suojelee antivirus ja haittaohjelmien suojausohjelmistot. Laiterikoilta ja käyttäjien vahinko poistamisilta tiedostoja suojelee varmuuskopioinnit, joista pystyy helposti palauttamaan alkuperäiset tiedostot. Laitehäviämisiltä tai varkauksilta dataa suojelee varmuuskopioiden lisäksi tiedostojen salaaminen eli kryptaus.

Taatakseen datalle parhaimman turvallisuuden työmatkoillakin, pitäisi yrityksiltä löytyä valmiiksi mietityt ratkaisut etätyöläisille. Yrityksen koon ja liiketoiminnan mukaan olisi hyvä selvittää sopivat VPN-, varmuuskopiointi-, haittaohjelmasuojaus- ja salausratkaisut yrityksen tarpeisiin. Moni näiden palveluidentarjoaja tarjoaa yrityksille yhtenäistä hallintapistettä, mistä voidaan helposti konfiguroida ja hallita kaikkia yrityksen tietokoneita.

Parasta suojaa kaipaaville ei yksi suojauskeino riitä. Markkinoiden paraskaan haittaohjelmien tunnistustyökalu tai VPN ei 100-prosenttisesti suojaa kaikilta uhkatekijöiltä. Mutta kaikki nämä suojautumiskeinot yhdistämällä saadaan kattava suoja datan uhkatekijöiltä.

Tietokonetta suojaavien ohjelmistojen lisäksi pitää käyttäjän olla tietoinen vaaroista. Yrityksissä olisi hyvä tuoda esille mahdollisia tietoturvariskejä. Tämä voisi tapahtua kouluttamalla työntekijöitä mahdollisista kyberriskeistä ja lisäämällä avointa

keskustelua asiasta. Suojausohjelmistot toimivat eräänlaisena viimeisenä puolustuskeinona, mutta olisi parempi, jos niihin ei tarvitsisi juurikaan turvautua. Tämä vaatisi työntekijöiden kouluttamista, etteivät he tietämättömyyttään jatkuvasti altistaisi omaa ja yrityksen dataa riskeille.

6 Pohdinta

Opinnäytetyön tavoitteena oli lisätä työntekijöiden ja työnantajien tietoisuutta erilaisista vaaroista, jotka voivat olla uhkaksi yrityksen datalle, sekä kertoa keinoja, miten niiltä voitaisiin suojautua. Työn kvalitatiivinen tutkimusmenetelmä tuki työtä hyvin, koska internetistä löytyi paljon materiaalia aiheeseen liittyen. Samoista aiheista löytyi kirjoituksia usein jopa kymmeniltä eri sivustoilta, joista pyrittiin lähteiksi valitsemaan luotettavimmat ja ajankohtaiset. Lähteinä käytettiin paljon ohjelmistojen omia verkkosivuja, erilaisia uutisartikkeleita ja blogikirjoituksia.

Tuloksena saatiin useita ohjelmistopohjaisia ratkaisuja, kutakin uhkaa vastaan löytyi oma ohjelmistonsa. Ohjelmistojen takana on usein isoja yrityksiä, jotka ovat kehittäneet omia tuotteitaan vuosien ajan. Luotettavan yrityksen löydyttyä, jää kuluttajan tehtäväksi vain valita itselleen sopivat ohjelmistopaketit ja hankkia ne. Lisääntyvien tietoturvamurtojen takia toivottavasti ihmiset alkaisivat kiinnittämään enemmän huomiota tietoturvan tärkeyteen ja panostamaan suojautumiskeinoihin. Todennäköisesti helpoin keino yrityksille olisi kilpailuttaa eri suojautumisohjelmistojen palveluntarjoajat ja ostaa kaiken kattavat paketit, joita voisi helposti hallita pilvestä ilman tarvetta hankkia omiin tiloihin lisäpalvelimia. Ei voida enää vedota siihen, että suojautumiskeinojen hankkiminen olisi liian hankalaa. Kysymys onkin, kuinka paljon yritykset ovat taloudellisesti valmiita panostamaan datan suojaamiseen.

Opinnäytetyö ei kuitenkaan kattanut kaikkia suojautumiskeinoja. Opinnäytetyön suojautumiskeinoissa keskityttiin lähinnä ohjelmistoihin, mutta aihetta voisi jatkaa vielä eteenpäin tutkimalla muita kuin ohjelmistopohjaisia ratkaisuja. Muita keinoja voisivat olla esimerkiksi fyysiset suojaratkaisut, ympäristöjen kovennukset, sekä viralliset ohjeistukset ja vaatimukset tietoturvaan liittyen, kuten GDPR.

Opinnäytetyöstä on hyötyä pienyrityksille, joissa ei olla vielä mietitty ratkaisuja datan suojelemiselle ja joiden työntekijöiltä vaaditaan paljon matkustamista. Toimeksiantaja CYBERDI-projekti voi myös hyödyntää opinnäytetyötä jatkaakseen kampanjointiaan tietoturvan tietoisuuden kasvattamisesta.

Lähteet

About the AV-TEST Institute. 2020. AV-TEST:n verkkosivut. Viitattu 23.4.2020. https://www.av-test.org/en/about-the-institute/

AV-TEST Awards 2019. 2019. AV-TEST:n verkkosivut. Viitattu 23.4.2020. https://www.av-test.org/en/news/av-test-awards-2019-products-recognized-for-outstanding-it-protection/

Best antivirus. 2020. Antivirusguiden verkkosivut. Viitattu 16.4.2020. https://www.antivirusguide.com/best-antivirus/

Bitdefender antivirus review. 2020. Antivirusguiden verkkosivut. Viitattu 14.4.2020. https://www.antivirusguide.com/review/bitdefender/

Bitdefender. 2020. Bitdefenderin verkkosivut. Viitattu 7.4.2020. https://www.bitdefender.com/

Business security. 2020. Bitdefenderin verkkosivut. Viitattu 16.4.2020. https://www.bitdefender.com/business/smb-products/business-security.html

Chima, R. 2016. Cloud security - who owns the data. Blogikirjoitus. Viitattu 27.3.2020. https://www.bbconsult.co.uk/blog/cloud-security-who-owns-the-data

Crawford, D. 2019. Ultimate guide to VPN encryption. Viitattu 25.3.2020. https://proprivacy.com/vpn/guides/vpn-encryption-the-complete-guide

Cyberdi. 2020. Cyberdi-projektin esittelysivu. Viitattu 3.3.2020. https://www.jamk.fi/fi/Tutkimus-ja-kehitys/projektit/CYBERDI/Projektiesittely/

CyberGhost VPN servers. 2020. CyberGhost VPN verkkosivut. Viitattu 4.4.2020. https://www.cyberghostvpn.com/en_US/vpn-server

CyberGhost VPN. 2020. CyberGhost VPN verkkosivut. Viitattu 6.4.2020. https://www.cyberghostvpn.com/en_US/

Dolly, J. 2018. Why you should never, ever connect to public WiFi. Viitattu 8.3.2020. https://www.csoonline.com/article/3246984/why-you-should-never-ever-connect-to-public-wifi.html

Encrypted cloud storage. 2020. Acronis artikkeli. Viitattu 16.3.2020. https://www.acronis.com/en-eu/articles/encrypted-cloud-storage/

Fearn, N. & Turner, B. 2020. Best encryption software of 2020: Free, paid and business tools and services. Viitattu 4.5.2020. https://www.techradar.com/best/best-encryption-software

Fisher, T. 2020a. The 8 Best Commercial Backup Software Programs of 2020. Viitattu 28.4.2020. https://www.lifewire.com/best-commercial-backup-software-programs-2624711

Fisher, T. 2020b. 34 Best Free Backup Software Tools. Viitattu 28.4.2020. https://www.lifewire.com/free-backup-software-tools-2617964

Gargiulo, M. 2018. What is a business VPN and how can it secure your company? Viitattu 15.2.2020. https://www.forbes.com/sites/forbestechcoun-cil/2018/11/15/what-is-a-business-vpn-and-how-can-it-secure-your-company/

Greenberg, R. 2020. Different types of VPNs and when to use them. Blogikirjoitus. Viitattu 31.3.2020. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/

Guinness, H. 2016. How to keep your computer safe & secure while traveling. Viitattu 13.3.2020. https://business.tutsplus.com/tutorials/how-to-keep-your-computer-safe-secure-while-traveling--cms-27465

Hochstadt, A. 2020a. NordVPN review & test. Viitattu 2.4.2020. https://www.vpnmentor.com/reviews/nordvpn/

Hochstadt, A. 2020b. VPNmentor verkkosivut. Viitattu 2.4.2020. https://www.vpnmentor.com/

Home vpn vs business vpn. 2020. ExpressVPN verkkosivut. Viitattu 16.2.2020. https://www.expressvpn.com/what-is-vpn/home-vpn-vs-business-vpn

Huculak, M. 2016. How to use Bitlocker Drive Encryption on Windows 10. Viitattu 30.4.2020. https://www.windowscentral.com/how-use-bitlocker-encryption-windows-10

IPSec VPN Overview. 2019. Juniperin verkkosivut. Viitattu 23.2.2020. https://www.juniper.net/documentation/en_US/junos/topics/topic-map/security-ipsec-vpn-overview.html

IPSec. 2020. PureVPN verkkosivut. Viitattu 3.3.2020. https://www.purevpn.com/what-is-vpn/protocols/ipsec

Kananen, J. 2015. Opinnäytetyön kirjoittajan opas: Näin kirjoitan opinnäytetyön tai pro gradun alusta loppuun. Jyväskylä: Jyväskylän ammattikorkeakoulu.

Krohn, D. 2019. Understanding five eyes concept. Blogikirjoitus. Viitattu 31.3.2020. https://www.vpnmentor.com/blog/understanding-five-eyes-concept/

Lake, J. 2018. RSA encryption. Blogikirjoitus. Viitattu 8.4.2020. https://www.comparitech.com/blog/information-security/rsa-encryption/

Lee, M. 2015. Encrypting your laptop like you mean it. The Intercept artikkeli. Viitattu 18.3.2020. https://theintercept.com/2015/04/27/encrypting-laptop-like-mean/

Marks, T. 2020. What is a vpn. Viitattu 8.2.2020. https://vpnoverview.com/vpn-information/what-is-a-vpn/

Marshall, A. 2020. The best VPN service 2020. Viitattu 23.4.2020. https://www.techradar.com/vpn/best-vpn

Mathew, L. 2020. Ransomware Hackers Start Selling Stolen Corporate Data. Viitattu 6.5.2020. https://www.forbes.com/sites/leemathews/2020/03/20/ransomware-hackers-start-selling-stolen-corporate-data/

Mocan, T. 2019. What is IKEv2. Viitattu 23.2.2020 https://www.cactusvpn.com/beginners-guide-to-vpn/what-is-ikev2/

NordVPN. 2020. NordVPN verkkosivut. Viitattu 6.4.2020. https://nordvpn.com/

Paul, I. 2016. A beginner's guide to BitLocker, Windows' built-in encryption tool. Viitattu 1.5.2020. https://www.pcworld.com/article/2308725/a-beginners-guide-to-bitlocker-windows-built-in-encryption-tool.html

Prepare your organization for BitLocker. 2019. Microsoft docs. Viitattu 8.5.2020. https://docs.microsoft.com/en-us/windows/security/information-protection/bitlocker/prepare-your-organization-for-bitlocker-planning-and-policies

Remote access VPN. 2020. NordVPN Teams verkkosivut. Viitattu 3.4.2020. https://nordvpnteams.com/remote-access-vpn/

Rivera, A. 2019. A small business guide to computer encryption. Viitattu 30.3.2020. https://www.businessnewsdaily.com/9391-computer-encryption-guide.html

Rivington, J. 2020. The best VPN service 2020. Viitattu 23.4.2020. https://www.tomsguide.com/best-picks/best-vpn

Servers. 2020. NordVPN verkkosivut. Viitattu 2.4.2020. https://nordvpn.com/servers/

Spector, L. 2017. 3 easy steps anyone can take now to back up a PC. Viitattu 16.3.2020. https://www.pcworld.com/article/2905400/3-easy-steps-anyone-can-take-now-to-back-up-a-pc.html

SSL-VPN. 2020. What is SSL-VPN Viitattu 16.2.2020. https://www.f5.com/services/resources/glossary/ssl-vpn

Taylor, S. 2017. VPNs are lying about logs. Viitattu 25.3.2020. https://restoreprivacy.com/vpn-logs-lies/

Taylor, S. 2019. OpenVPN vs IPSec, WireGuard, L2TP, and IKEv2. Viitattu 18.2.2020. https://restoreprivacy.com/openvpn-ipsec-wireguard-l2tp-ikev2-protocols/

Vaughan-Nichols, S. 2020. VPNs will change forever with the arrival of WireGuard into Linux. Viitattu 22.2.2020. https://www.zdnet.com/article/vpns-will-change-forever-with-the-arrival-of-wireguard-into-linux/

Veale, K. 2019. Difference between malware and ransomware. Viitattu 9.3.2020. https://www.vpnmentor.com/blog/difference-between-malware-ransomware/

Veale, K. 2020. CyberGhost VPN review & test. Viitattu 6.4.2020. https://www.vpnmentor.com/reviews/cyberghost-vpn/

Veeam Gartner. 2019. Gartner Magic Quadrant 2019. Viitattu 5.5.2020.
https://www.veeam.com/2019-gartner-magic-quadrant.html

Veeam. 2020. Why Veeam? Viitattu 28.4.2020.
https://www.veeam.com/why-veeam.html

What is a man in the middle attack. 2020. Cloudflaren verkkosivut. Viitattu 8.4.2020.
https://www.cloudflare.com/learning/security/threats/man-in-the-middle-attack/

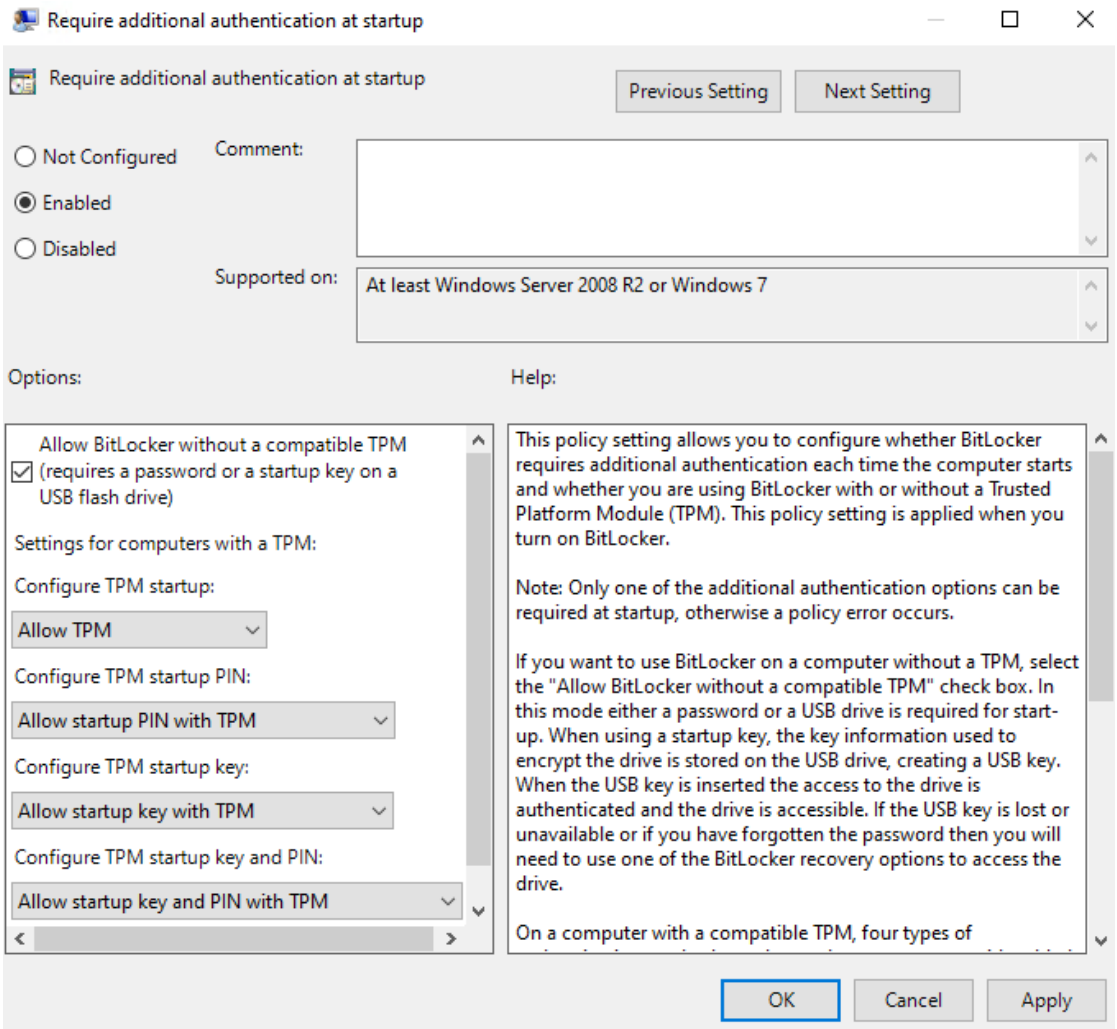
What is anti malware. 2020. Comodo cybersecurity. Viitattu 6.4.2020.
https://enterprise.comodo.com/what-is-anti-malware.php

What is HTTPS. 2020. Cloudflaren verkkosivut. Viitattu 8.4.2020.
https://www.cloudflare.com/learning/ssl/what-is-https/

Which protocol should I choose. 2020. NordVPN FAQ sivut. Viitattu 2.4.2020.
https://support.nordvpn.com/FAQ/1047408592/Which-protocol-should-I-choose.htm

Wireguard. 2019. Wireguardin verkkosivut. Viitattu 22.2.2020.
https://www.wireguard.com/

Liitteet

Liite 1. Bitlockerin käyttöönotto ilman TPM:ää

Group Policy Editoriin mentiin painamalla Windows näppäintä ja R-painiketta samanaikaisesti ja sen jälkeen avautuvaan ikkunaan kirjoitettiin ”gpedit.msc”. Haluttu Bitlockerin asetus löytyi seuraavien kansioiden alta: “Computer Configuration/ Adminstrative Templates/ Windows Components/ Bitlocker Drive Encryption/ Operating System Drivers” ja sieltä asetus “Require additional authentication at startup”, jonka jälkeen avautui alapuolella näkyvä ikkuna. Ikkunasta laitettiin vasemmassa yläkulmassa oleva valinta kohtaan “Enabled” ja alapuolella sallittiin Bitlockerin käyttö ilman yhteensopivaa TPM:ää. Tämän jälkeen painettiin ok ja suljettiin Group Policy Editor. (Huculak 2016.)