LAMK Lahden ammattikorkeakoulu
Lahti University of Applied Sciences

Yrityksen tietoturvan kehittäminen

Case: Sinuhe Ky

LAHDEN
AMMATTIKORKEAKOULU
Tekniikan ala
Tietotekniikan koulutusohjelma
Tietoliikennetekniikka
Opinnäytetyö
Kevät 2016
Juho Hietanen

Lahden ammattikorkeakoulu
Tietotekniikan koulutusohjelma

HIETANEN, JUHO:

Yrityksen tietoturvan kehittäminen
Case: Sinuhe Ky

Tietoliikennetekniikan opinnäytetyö, 52 sivua, 6 liitesivua

Kevät 2016

TIIVISTELMÄ

Opinnäytetyön tarkoituksena oli yrityksen tietoturvan kehittäminen. Modernin tietoturvan avulla kyetään suojaamaan yritysverkon kohteet, jotka ovat yrityksen toiminnalle välttämättömiä. Opinnäytetyön toimeksiantajana toimi Sinuhe Ky, jonka tietoturvaa pyrittiin kehittämään.

Toimivan yrityksen tietoliikenne toimii korkealla käyttöasteella, mutta suojaa työntekijöidensä yksityisyyttä ja työskentelyä. Hyvin toteutuvan tietoturvan ylläpitämiseksi yrityksen toiminta vaatii myös yrityksen johdolta osaavaa työskentelyä ja valvontaa

Työn tärkein tavoite oli muodostaa tietoturva suunnitelma yrityksen tarpeisiin. Työn tarkoituksena oli analysoida ja kartoittaa yrityksen tietoturvan kehittämiskohteet ja kehottaa yritystä niiden korjaamiseen.

Turvallisen verkon taustalla toimii protokollien ja ohjelmistojen yhteistyö. Tietoturva voidaan jakaa seuraaviin osa-alueisiin: hallinnollinen tietoturva, fyysinen tietoturva, henkilöstöturvallisuus, käyttöturvallisuus ja tietoliikenneturvallisuus.

Keskeisin asia opinnäytetyössä on tietoturvasuunnitelman toteuttaminen. Suunnitelman muodostaminen koostui virusturvan toteuttamisesta, palomuuriohjelmiston valitsemisesta, käyttöjärjestelmien päivittämisestä sekä verkonvalvonnasta.

Asiasanat: tietoturva, verkonvalvonta, virusturva ja palomuuriohjelmisto

Lahti University of Applied Sciences
Degree Programme in Information technology

HIETANEN, JUHO:

Developing the data security of a company
Case: Sinuhe Ky

Bachelor's Thesis in telecommunications technology, 52 pages, 6 pages of appendices

Spring 2016

ABSTRACT

The topic of this thesis is development of the information security of a company. Due to modern security technology it is possible to protect the parts of the company's network which are necessary for the companys operation.

A good telecommunications system runs at a high utilization rate but also protects employees' privacy and work. Good data security also requires knowledge and supervision from the company's management.

The thesis was commissioned by Sinuhe Ky, which wanted its data security to be developed. The most important objective of the thesis was to form a security strategy for the company's needs. The purpose was to analyze and survey the company's security needs and recommend the company to correct subjects which need improvement.

Cooperation of protocols and software form the background of a secure network. Security can be divided to different sections, which are administrative, physical, personnel, utilization and telecommunications security.

The most important subject of the thesis was to implement a security strategy for the company. The strategy consists of accomplishing virus protection, choosing of firewall software, upgrading the operation system, and network monitoring.

Keywords: security, virus protection, network monitoring, firewall software

SISÄLLYS

LYHENNELUETTELO

AES	Advanced Encryption Standard,lohkosalausmenetelmä
CCMP	Counter Chiper Mode Encryption, salausprotokolla
DOS	Denial Of Service, Verkkoliikennettä heikentävä hyökkäys
EAP	Extensible Authentication Protocol, käyttäjien tunnistusprotokolla
IEEE 802.11	Wlan-lähiverkkojen standardi
IGMP	Internet Group Management Protocol, osa TCP-protokollaperhettä
MIC	Message Integrity Check, salausmenetelmän parantamiseen käytetty protokolla
NAT	Network Address Translation, osoitteenmuunnostekniikka
PMK	Pairwise Master Key, salausavainprotokolla
SSL	Secure Sockets Layer, salausprotokolla
TCP	Transmission Control Protocol, tiedonsiirtoon käytetty protokolla
TKIP	Temporal Key Integrity Protocol, salausprotokolla
UDP	User Datagram Protocol, tiedonsiirtoon käytetty protokolla
WEP	Wired Equilevalent Protocol, salausmenetelmä langattomalle verkolle
WPA	Wireless Fidelity Protected Acess (Wi-fi), salausmenetelmä

1 JOHDANTO

Opinnäytetyössä on tarkoituksena kartoittaa Sinuhe Ky yrityksen tietoturvaa sekä kehittää yrityksen tietoturvalle keskeisiä asioita. Opinnäytetyössä käsitellään yrityksen tietoturvaa käyttäjäläheisessä näkökulmassa. Tietoturva suunnitelma auttaisi yrityksen johtoa sekä työntekijöitä tietoturvan aihepiirissä.

Työn tavoitteena on toteuttaa mahdollisimman selkeä tietoturvan kartoitus, jossa yritykselle selvitetään tarpeellisia asioita tietoturvan kannalta sekä ehdotetaan mahdollisia parannusehdotuksia yrityksen tietoturvan toiminnalle ja tulevaisuudelle. Työssä tullaan syventymään sellaisiin aiheisiin, joita hyödyntämällä yrityksellä on mahdollisuus kehittyä sekä parantaa tietoturvallista työskentelyään. Näitä aihepiirejä ovat esimerkiksi tietoliikenteen turvaaminen ja käyttöjärjestelmien heikkoudet.

Tietoturvan kehittämissuunnitelmassa painotetaan tietotekniikan käyttäjän toimivaan käyttökokemukseen sekä yhteyksien kattavaan toimintaan. Lisäksi kehittämissuunitelmassa otetaan huomioon tärkeiden asiakirjojen säilytys- ja tallennusmahdollisuudet, jolloin asiakirjojen käyttämisestä saadaan turvallista ja toiminnaltaan tehokasta.

2 SINUHE KY

Sinuhe Ky on leipomo-alan yritys, jonka toimipisteet sijaitsevat Lahdessa ja Kouvolassa. Näiden leipomoiden lisäksi Sinuhella on kahviloita, joista Lahden alueella osa on lounaskahviloita. Sinuhen päätoimiala on leipomotoiminta sekä suurkeittiötoiminta, joiden toiminta on aloitettu jo 1950-luvulla. Sinuhen toiminta perustuu laajaan tuotevalikoimaan, johon sisältyvät esimerkiksi kahvi- sekä ruokaleivät ja erilaiset leivokset. Yhteensä Sinuhen valikoimiin kuuluvat yli toistasataa erilaista leipomoalan tuotetta.

Sinuhen Lahden-leipomo on perustettu 1970-luvulla, ja yrityksen asiakaskunta muodostuu pääosin erilaisista vähittäismyymälöistä sekä yksityisistä asiakkaista. Sinuhen Vuoripojankadun-toimipiste muodostuu kahdesta osasta: leipomosta sekä toimistotiloista. Leipomoa on sen historian aikana laajennettu useasti, ja sen toiminta laajenee ja uudistuu jatkuvasti. Opinnäytetyön tekeminen toteutetaan pääosin Lahden-toimipisteen tarpeisiin ja kehitykseen.

3 TIETOTURVA

Tietoturvalla otetaan huomioon yrityksen suojauksen ja toiminnan mahdolliset riskit. Tietoja hyödyntämällä voidaan kartoittaa ne osa-alueet tietoturvasta, joita on mahdollista kehittää eteenpäin turvallisemman tietoturvan sekä organisaation toimintaa varten. (Pietikäinen 2013.)

Koulutetun henkilöstön sekä päivitetyn tietoturvallisuuden kartoituksen avulla voidaan varmistaa yrityksen lisäksi myös yrityksen työyhteisön sekä ympärillä elävän yhteiskunnan etuja. Tietoturvallisuudessa on aina otettava huomioon yksilöiden tietoturvakäyttäytyminen, mikä on tietoturvallisen yrittäjyyden toiminnan edellytys tuottavan yrityksen toiminnassa. (Pietikäinen 2013.)

3.1 Tietoturvallisuus

Tietoturvallisuus jaetaan useisiin erilaisiin osa-alueisiin, joista osaltaan merkittävämpänä on hallinnollinen tietoturva. Hallinnollisen tietoturvan tarkoituksena on turvata muiden tietoturvan osa-alueiden toiminta sekä varmistaa, että yritys ymmärtää organisaationsa tietoturvan tason kehityksen sekä lainsäädännön. Hallinnollisen tietoturvan tärkeimpiä huomioitavia asioita ovat riskienhallinnan kartoittaminen, jossa toteutetaan sisäisten- ja ulkoisten riskien arviointia. Hallinnollisen tietoturvan tärkein osa-alue on tietoturvan jatkuvuuden ja ylläpidon turvaaminen. (Tietojesiturvaksi 2016b.)

Seuraavana tietoturvan osa-alueeena määritellään fyysisen tietoturvan merkitys. Fyysinen tietoturva sisältää yrityksen toiminnan kannalta oleellisia asioita. Näitä ovat yrityksen sisäiset toimitilat sekä toimitiloissa sisältävien laitteiden suojaaminen. Yrityksen toimiva fyysinen tietoturva koostuu suojautumiselta mahdollisia sähkö-, vesi- tai palovahingoilta. Fyysisessä tietoturvassa yrityksen on otettava huomioon myös mahdolliset inhimilliset tekijät, kuten vahingot, ilkivalta sekä varkaudet. (Tietojesiturvaksi 2016a.)

Erityisesti tietoturvallisuuden tasoon vaikuttavat henkilöstöturvallisuuden osa-alue. Henkilöstöturvallisuus sisältää yrityksen henkilöstön käyttäytyminen sekä toimiminen. Henkilöstölle on toimiessaan työpaikallaan määrittynyt työkokemuksen myötä erilaisia vastuualueita, joiden tietoturvallinen toteuttaminen on tärkeää tuottavan- ja turvallisen työympäristön luomiseksi. Henkilöstöturvallisuutta voidaan kehittää esimerkiksi huomioimalla varahenkilökäytännöt mahdollisten sairastumisten tai tapaturmien varalta. Tietoturvakouluttamisella ylläpidetään henkilöstön osaamista työskennellä yrityksessään tietoturvallisesti. (Tietojesiturvaksi 2016c.)

Henkilöstöturvallisuuden ala-alueena voidaan pitää käyttöturvallisuutta. Työntekijöiden päivittäisten työalueiden sekä velvollisuuksien koulutuksella ja turvaamisella toteutetaan käyttöturvallisuus. Käyttöturvallisuudessa huomioidaan erilaisten fyysisten laitteiden turvallinen käyttäminen ja tietotekniikassa vahvojen salasanakäytäntöjen toteuttaminen. Käyttöturvallisuuden tavoitteena on minimoida riskejä, jotka aiheutuvat osaamattomasta laitteiden käyttämisestä sekä ohjeiden laiminlyömisestä. (Tietojesiturvaksi 2016d.)

Tietoliikenneturvallisuutta pidetään tietoturvan yhtenä tärkeimmistä osa-alueista. Tietoliikenneturvallisuudella pyritään suojaamaan dataverkoissa liikkuvaa informaatiota. Turvallisia tiedonsiirtokanavia käyttämällä ja tietoliikennettä suojaamalla voidaan vähentää tietoliikenteen sisältämiä riskejä. Verkkolaitteiden sekä dataliikenteen turvaaminen kehittää yritysten tietojen säilyvyyttä sekä liikkuvuutta verkon käyttäjältä toiselle. Turvallisuutta voidaan varmistaa hyvällä verkkodokumentoinnilla, toimivilla verkkosuojausmenetelmillä, kuten esimerkiksi palomuurilla, sekä ajantasalla olevalla virustorjunnalla. (Tietojesiturvaksi 2016e.)

Yrityksessä tietoliikenteenturvallisuutta voidaan ylläpitää selvittämällä taulukossa 1 ilmenevien asioiden toiminta.

TAULUKKO 1. Tietoliikenne turvallisuuden ylläpito (Tietojesiturvaksi 2016e)

1. Tietoliikenteen vastuuhenkilöt sekä vastuualueet.
2. Tietoliikenneverkon dokumentointi ja ylläpitäminen
3. Verkossa liikkuvan informaation suojaaminen.
4. Ylläpitäjien ja käyttäjien ohjeistaminen sekä koulutus.
5. Huolto- ja ylläpitosopimukset ulkoisten toimijoiden kanssa.

Tietoturvan osa-alueista seuraavana käsitellään laitteistotietoturva, joka sisältää yrityksen tekniset laitteet. Teknisiä laitteita voivat olla esimerkiksi tietokoneet, tulostimet ja leipomotekniikaan kuuluvat jauhonannostajat sekä laatikonpesemiseen käytettävä elektroninen laitteisto. Hyvään laitteistoturvallisuuteen päästään henkilökunnan kouluttamisella käytettävää laitetta varten. Laitteistonkäyttöohjeet sekä muut tarvittavat dokumentit kannattaa pitää sellaisessa paikassa, josta tietoja voidaan tarvittaessa tarkistaa. Henkilöstön käyttöongelmaksi saattaa ilmetä esimerkiksi ”hätä seis” painikkeen painamisen jälkeinen laitteen uudelleen käyttöönotto. (Tietojesiturvaksi 2016f.)

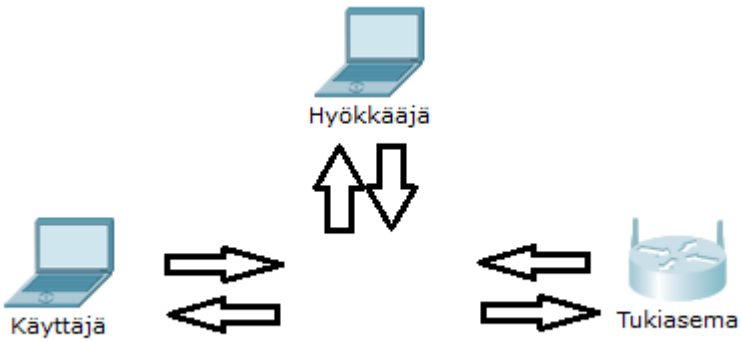
Tietoturvan osa-alueista kannattaa ottaa huomioon vielä ohjelmisto-turvallisuus sekä tietoaineiston turvallisuus. Ohjelmistoturvallisuudessa on tärkeintä ymmärtää käytettävien ohjelmistojen toimintatapa ja lisenssien ylläpitäminen. Virusturvan kannalta esimerkiksi lisenssien käyttöoikeuden päättyminen vaikuttaa virustorjuntaohjelman tai esimerkiksi palomuurisovelluksen toimintaan. Virustorjuntasovelluksen ominaisuudet

lisenssimättömässä käytössä vähenevät radikaalisti verrattuna lisenssin ylläpitämään sovellukseen. Ohjelmistoturvallisuuteen liittyy vahvasti tietoaineiston turvallisuus. Tietoaineiston päämääränä on tarkoituksena määritellä erilaisia käyttöoikeuksia, jotta vain tarvittava henkilöstö pääsee materiaaliin käsiksi. Lisäksi turvallisuutta lisätään aineiston varmuuskopioinnilla ja mahdollisella salaamisella. (Tietojesiturvaksi 2016g.)

3.2 Langaton lähiverkko

Langaton lähiverkko eli WLAN (Wireless Local Area Network) on monissa yrityksissä yleinen tapa toteuttaa yrityksen kiinteistön alueelle verkkoyhteys. WLAN:ia hyödynnetään usein sen helppokäyttöisyyden sekä mahdollisten säätötoimenpiteiden vuoksi. Langatonta lähiverkkoa voidaan käyttää miltei kaikilla tietokoneilla sekä älypuhelimilla, mikä avaa mahdollisuuksia työskennellä yrityksen verkossa myös työpisteen ulkopuolella. WLAN-verkko toimii yleensä IEEE 802.11 -standardeihin perustuen sekä salausmenetelmiä hyödyntäen. (Viestintävirasto 2016a.)

Tietoturvan kannalta langattomien verkkojen käyttäminen avaa mahdollisille hyökkääjille erilaisia mahdollisuuksia verrataessa esimerkiksi kiinteän verkon heikkouksiin. Wlan-verkkojen päätelaitteet kommunikoivat verkossa tukiasemiensa kanssa, mikä aiheuttaa ongelman luotettavuuden kanssa. Päätelaiteet kommunikoivat yleensä vahvimpien signaalien omistavien wlan-verkkojen kanssa, jolloin hyökkääjä voi ohjata signaalia hyödyntämällä omaan wlan verkkoonsa. Tällöin hyökkääjä voi käyttää päätelaitteen lähettämää tietoa omaan käyttöön (kuvio 1).



KUVIO 1. Man in the middle-hyökkäys

Yrityksen langattomien verkkojen hallinta kannattaa toteuttaa huolella. Vuonna 2011 muutetun lainsäädännön mukaan salaamattoman wlan-verkon käyttämistä ei pidetä enää luvattomana käyttämisenä, jolloin verkon käyttäminen ei ole enää rangaistavaa. Langattoman verkon salausavain tulee hyvän tietoturvan toteuttamiseksi muuttaa pois käyttöliittymän oletusavaimesta, jotta ulkopuoliset eivät pääse verkon asetuksiin tai verkon liikenteeseen käsiksi. (Viestintävirasto 2016b.)

3.2.1 IEEE 802.11

IEEE 802.11 on yleisesti käytetty standardi kuvailemaan langattomien yhteyksien omainaisuuksia ja standardin käyttömahdollisuuksia. 802.11-standardien erottamiseksi käytetään yleisesti määriteltyjä kirjain yhdistelmiä (kuvio 2). Historiallisesti ensimmäisenä langattomien yhteyksien standardina otettiin käyttöön 802.11, jonka tarkoituksena oli aloittaa langattomien yhteyksien standardien määritteleminen. 802.11-standardin alkuaikoina ilmestyivät maininnan arvoiset 802.11b ja 802.11a, joiden ominaisuuksien tarkoitus oli päivittää alkuperäistä 802.11-standardia nopeammaksi sekä toimivammaksi kokonaisuudeksi. 802.11a ja b erona ovat niiden käyttämät taajuudet, yhteysnopeus sekä käytössä oleva modulaatiomenetelmä. (Smith 2011.)

Table 1: IEEE 802.11 Standards

Standard	Frequency band	Bandwidth	Modulation	Maximum data rate
802.11	2.4 GHz	20 MHz	DSSS, FHSS	2 Mb/s
802.11b	2.4 GHz	20 MHz	DSSS	11 Mb/s
802.11a	5 GHz	20 MHz	OFDM	54 Mb/s
802.11g	2.4 GHz	20 MHz	DSSS, OFDM	54 Mb/s
802.11n	2.4 GHz, 5 GHz	20 MHz, 40 MHz	OFDM	600 Mb/s
802.11ac	5 GHz	20, 40, 80, 80 + 80, 160 MHz	OFDM	6.93 Gb/s
802.11ad	60 GHz	2.16 GHz	SC, OFDM	6.76 Gb/s

KUVIO 2. IEEE802.11 Standardit (Newton 2015)

Nykyaikaisempia ja käytössäolevia standardeja ovat 802.11g ja 802.11n, joiden nopea yhteys mahdollistaa tiedon lähittämisen langattomia yhteyksiä hyödyntäen edeltäjiään nopeammin. Lisäksi standardien käyttämä taajuus toimii yhteistyössä toistensa kanssa, mikä toteuttaa toimivamman käyttökokemuksen. 802.11n standardi version ominaisuudet ovat kuitenkin 802.11g:tä kehittyneemmät, sillä standardi kykenee toimimaan sekä 2,4 GHz:n, että 5,0 GHz:n taajuudella, mikä tarkoittaa monipuolisempaa toimintaa. Tällä hetkellä yksi uusimmista standardeista on 802.11ac, josta pidetään standardimarkkinoiden johtavana 802.11 standardina. (Smith 2011.)

3.2.2 Salausmenetelmät

Tietoturvaa käsiteltäessä voi verkon käyttäjä pohtia sitä, että onko lähetettävä tieto turvassa ulkopuolisilta esimerkiksi lähetettäessä tietoa langattomien verkkojen kautta. Langattomien verkkojen tietoturvan perusta ovat liikenteen tiedon suojaamiseen kehitetyt salausmentelmät, jotka tekevät verkosta käytettävyydeltään turvallisemman. Kolme yleisintä salausmenetelmää ovat: WEP (Wired Equivalent Privacy), WPA (Wi-Fi Protected Access) sekä WPA 2 (Wi-Fi Protected Access 2). Vanhinta näistä salaumenetelmistä kutsutaan WEP eli ”Wired Equivalent Privacy”, joka otettiin käyttöön 802.11-standardien yhteydessä kehittämään standardin tietoturvan aukkoja. WEP-salausmentelmän toiminta perustuu lähetettävän liikenteen kryptaamiseen eli lähetetyn tiedon luettavuuden sekoittamiseen. (Beal 2007a.)

Tietoturvallisuuden kannalta WEP-salausmenetelmässä löytyi kuitenkin suuria haavoittuvuuksia, mikä vaati salausmenetelmän päivittämisen tarpeelliseksi. WEP-salausmenetelmän heikkoudeksi osoittautui sen suojaukseen käytettävät avaimet. Heikkous johtui siitä, että salauksen avaimet pystyttiin selvittämään, minkä avulla oli mahdollista avata salattu teksti jälleen luettavaan muotoon. WEP-salausavaimen selvittäminen pystyttiin toteuttamaan kuuntelemalla salausmenetelmän liikennettä riittävän pitkään, jotta palasia salausavaimesta pystyttiin selvittämään. Tämän vanhan salausmenetelmän ongelmaa pystytään ehkäisemään vaihtamalla salausmenetelmän avainta mahdollisimman usein. (Beal 2007a.)

WPA-salausmenetelmän tarkoituksena oli korjata WEP-salausmenetelmän sisältämiä heikkouksia. Langattomien yhteyksien tietoturvan kannalta WPA toi kaksi suurempaa parannusta salausmenetelmän käyttöön. Tiedon suojaamista parannettiin kehittelemällä TKIP (Temporal Key Integrity Protocol) -protokolla. TKIP-protokollan tarkoituksena oli lisätä lähetettävään tietoon hash-algoritmi, jonka avulla protokolla pystyy tarkistamaan onko lähetettävä tieto ehjä. WPA-salausmenetelmän toisena parannuksena toteutettiin todennus-toiminto, jonka avulla sallittiin

haluttujen IP-osoitteiden pääsy verkkoon. Tätä protokollaa kutsutaan EAP:ksi. (Beal 2007b.)

WPA-salausmenetelmä päivitettiin, vaikka salausmenetelmä olikin tietoturvallisesti pätevämpi kuin WEP. Modernein ja turvallisin salausmenetelmä sai nimekseen WPA2. Salausmenetelmän päivityksiin kuului esimerkiksi protokolla AES (Advanced Encryption Standard), jonka tarkoituksena oli toimia TKIP-protokollan päivitettynä versiona salausmenetelmässä. Toisena tärkeänä päivityksenä WPA2 protokollaan tuli CCMP-protokolla. CCMP-protokollan ominaisuuksina oli parantaa pakettien tietosuojaa esimerkiksi informaation alkuperän todentamisella sekä informaation eheyden tarkastamisella. Lisäksi WPA2-salausmenetelmää päivitettiin nopeammaksi liittymään jo tunnettuihin verkkoihin PMK (Pairwise Master Key) -protokollan avulla. (Microsoft 2015.)

3.2.3 TKIP ja AES

Salausmenetelmien sisältämien protokollien tärkeimpinä tietoturvan yksikköinä toimivat TKIP (Temporary key integrity) sekä AES (Advanced encryption standard). TKIP-protokollan tietoturvan kohottaminen perustuu sen monimutkaisen salausavaimen toimintaan. Salausavaimen pituus on protokollassa 128 bittiä. TKIPprotokollalla on monia erilaisia ominaisuuksia, jotka toteuttavat protokollan tietoturvan toimintaa. TKIP sisältää esimerkiksi MIC:n (Message integrity check), minkä toiminta estää verkossa liikkuvan datan muokkaamisen. Mikäli verkossa tapahtuu häiriötekijöitä tai mahdollisia hyökkäyksiä, TKIP-protokollan ominaisuus TSC (TKIP sequence counter) pyrkii estämään ongelmien toistumisen tutkimalla ongelmien alkuperää, jolloin esimerkiksi toistuvien hyökkäysten tekeminen on TKIP-protokollaa vastaan hankalampaa. TSC-toiminta perustuu tiedon leimaukseen. Verkossa lähetetään tietopaketti, jonka bitti muutetaan 0 bitistä 1 bitiksi, kun paketti vastaanotetaan. Tämä tarkoittaa sitä, että mahdolliset paketit, joita on jo vastaanotettu, eivät pysty toistamaan lähetettävää pakettia. TKIP-ominaisuuksien yhteis-toiminta tuo langattomalle verkolle toimivan suojan, mutta nykyaikana AES- protokolla on korvannut TKIP-protokollan vielä turvallisempana suojausmenetelmänä. (eTutorials 2016.)

AES (Advanced Encyption Standard) on WPA2-salausmenetelmän käyttämä salausprotokolla. AES on nykyaikaisen langattoman verkon päivitetyin ja turvallisin protokolla tietoturvan takaamiseen. AES protokolla- on ominaisuuksiltaan edeltäjäänsä TKIP:iä turvallisempi, sillä AES-protokollalla on mahdollista käyttää pidempää salausavainta. Salausavaimien pituudet voivat olla 128, 192 ja 256 bittiä pitkiä. Tämä tarkoittaa sitä, että AES-protokollan salausavain voi olla jopa kaksi kertaa pidempi kuin TKIP-salausavain. Salausavaimen pituuden kasvaminen aiheuttaa salausavaimen monimutkaistumista, mikä on tietoturvalle positiivinen ominaisuus, sillä sitä on vaikeampi murtaa. AES-protokollan turvallista toimintaa edistää sen sisältämät ominaisuudet, kuten CCMP-protokolla. CCMP-protokollan toiminta perustuu protokollan kolmeen tärkeään ominaisuuteen. CCMP pyrkii tekemään lähetettävästä tiedosta

mahdollisimman luotettavaa, jolloin se antaa vain määritetyille funktioille mahdollisuuken tiedon käsittelyyn. CCMP:n toinen ominaisuus on tiedon lähettäjien todentaminen, jolloin protokolla pystyy määrittelemään onko tiedon lähettäjä verkossa luotettava. CCMP-protokollan kolmantena ominaisuutena on kulunvalvonta. Kulunvalvonta toteutetaan AES-protokollan salausavainta hyödyntämällä. (eTutorials 2016.)

3.3 Käyttöjärjestelmien heikkoudet

Tietoturvan ylläpitämisessä on tärkeää ymmärtää käytettävän käyttöjärjestelmän heikkoudet, jotta niitä olisi mahdollista ehkäistä tietotekniikkaa käytettäessä. Erilaisissa Windows-käyttöjärjestelmissä on aina olemassa käyttöjärjestelmäkohtaiset heikkoudet. On kuitenkin olemassa heikkouksia, joita esiintyy jokaisessa käyttöjärjestelmässä ja, jotka johtuvat yleensä käyttäjän huolimattomuudesta. Näitä heikkouksia ovat esimerkiksi tietokoneesta puuttuva virusturvasovellus, jonka puuttuminen altistaa koneen erilaisille viruksille ja turvattomuudelle, joita käsitellään myöhemmin opinnäytetyössä. (Beaver 2016.)

Heikkoudeksi voidaan luetella myös kovalevyjen suojaamattomuus. Kovalevyissä voidaan säilyttää yrityksen kannalta tärkeää tietoa, jota ei paperimuodossa kannata säilyttää. Siksi on tärkeää pitää kovalevyjen materiaali mahdollisimman suojattuna, jotta ei olisi riskiä tiedon häviämiseksi. Sähköpostien toiminta saattaa sisältää heikkouden. Tietoturvan kannalta on erittäin tärkeää, että sähköpostien lukeminen sekä lähettäminen suoritetaan SSL-protokollaa tai vastaavaa suojausprotokollaa käyttäen, jolloin ulkopuolisten käyttäjien on miltei mahdotonta näitä sähköposteja saada käsiinsä. Yleinen heikkous on myös liian heikot salasanat. Yleisen vahvan salasanan kriteeri on salasanan pituus sekä monimutkaisuus. Tietoturvan kannalta on myös tärkeää, että niin kutsuttu ”default”-salasana vaihdetaan heti käyttöönottamisen yhteydessä, sillä nämä ”default”-salasanat ovat mahdollisten hyökkääjien tiedossa. (Beaver 2016.)

3.3.1 XP-käyttöjärjestelmä

Windows XP-käyttöjärjestelmän vanheneminen tuottaa käyttöjärjestelmälle tietoturvauhkia. Suurimman tietoturvauhkan aiheuttaa käyttöjärjestelmän päättyneet päivitykset. Päivitysten päättyminen tarkoittaa sitä, että huhtikuun 2014 jälkeen käytössä olevien XP-koneiden käytön turvallisuutta ei enää tueta. Päivitystuen loppuminen aiheuttaa XP-koneiden tulevaisuuden tietoturva uhkien säilymistä siihen asti, kunnes Windows XP-koneiden käyttäminen päättyy lopullisesti. Käyttöjärjestelmän tietoturvauhkia löytyy esimerkiksi Windows XP koneen Internet Explorer-verkkoselaimesta. Internet Explorer 6-11-versioista löytyy ”Zero day vulnerability”. Zero day vulnerabilityksi kutsutaan sellaista heikkoutta, joka sisältyy tietokoneen sovelluksessa ilmenneeseen heikkouteen, jota hyökkääjät voivat hyödyntää. Ongelmana XP-käyttöjärjestelmän kanssa on kuitenkin päivitysten päättymisen aiheuttama uhkatila. (Held 2014.)

Microsoft suosittelee yritysten Windows XP-koneiden korvaamista tuoreemmilla käyttöjärjestelmillä. Yrityksissä saattaa ilmetä ongelmia käyttöjärjestelmän päivittämisessä, koska uudet järjestelmät eivät välttämättä suorita vanhoja yritykselle tärkeitä sovelluksia tai tekniikkaa. Tähän on kuitenkin saatavilla vaihtoehto. Esimerkiksi Windows 7-käyttöjärjestelmässä on mahdollisuutta käyttää osaa Windows XP-tuotettuja ohjelmistoja. Windows XP-tietokoneiden tietoturvan uhkaajaksi on myös noussut XP-koneiden sisältämä vanha laitteisto. Vanhojen laitteistoiden toimivuus ei enää ole tietoturvallisesti käyttäjäystävällistä, sillä iso osa laitteiden päivitys-sovelluksista on vanhentuneita. Vanhojen laitteistoiden korjaaminen voi olla vaikeaa, sillä vanhaa laitteistoa ei välttämättä enää valmisteta. (Prokaza 2015.)

3.3.2 Vista-käyttöjärjestelmä

Windows Vista-käyttöjärjestelmä on Windows XP-käyttöjärjestelmän seuraaja käyttöjärjestelmämarkkinoilla. Windows Vistaa on pidetty Windows XP:n sekä Windows 7-käyttöjärjestelmän välimuotona, mutta sitä pidetään jopa Windows XP:tä epäkäytännöllisempänä. Lisäksi Vistan sovelluksien yhteensopivuutta on pidetty huonona verrattaessa esimerkiksi Windows 7:n ja Windows XP:n väliseen sovellusten toimintaan. (Hiner 2008.)

Windows Vistassa on muutamia kriittisiä tietoturvauhkia, jotka aiheuttivat aikanaan ongelmia verkkojen tietoturvassa. Ensimmäisenä mainittavana tietoturvauhkana oli Windows Vistalle löydetty ongelma vistan ”gadget”-työkalujen yhteydessä.”Gadget”-ohjelmista löytyi heikkous, jonka kautta mahdollinen hyökkääjä pystyi ohjelmoimaan oman ”gadget”-sovelluksensa alkuperäisen oikean sovelluksen päälle ja ohjaamaan käyttäjänsä esimerkiksi urkintasivustoille. (Cluley 2012.)

Toisena esimerkkinä tietoturvauhasta Vistassa löytyi IPv6-verkon käyttämisen yhteydessä. Tässä tietoturvaheikkoudessa hyökkääjä kykeni kuuntelemaan IPv6-verkon käyttäjien verkon käyttöä lähettämällä ICMPv6 echo request-käskyn multicast-osoitteeseen ja tiedustelemaan kuinka verkkoa käytetään. Hyökkääjän oli mahdollista hyödyntää tätä tietoa ja murtautua käyttäjien verkkoon. Tämä saattoi aiheuttaa suojatun verkon tiedon siirtymisen myös hyökkääjän käyttöön. (CVE Details 2016a.)

3.3.3 Windows 7 -käyttöjärjestelmä

Windows 7 -käyttöjärjestelmän kehittämisessä on opittu edeltävien käyttöjärjestelmien heikkouksista. Kuitenkin myös Windows 7 -käyttöjärjestelmässä on omat turvallisuuteen liittyvä ongelmat, joita huomioimalla voidaan helpottaa turvallista käyttäjäkokemusta. Windows 7 -käyttöjärjestelmän mainittavana heikkoutena on Windowsin oman palomuurin heikkous verrattuna markkinoilla tarjottaviin palomuurisovelluksiin. Lisäksi käyttöjärjestelmän palomuuri käyttää enemmän tietokoneen käyttöön varattuja tehoja, mitä esimerkiksi muiden yrityksen palomuurit käyttävät. Windows 7:n palomuuri ei pysty näkemään verkossa liikkuvan datan uhkaa, jolloin esimerkiksi mahdolliset haittaohjelmat pystyvät saastuttamaan tietokoneen. Siksi on tärkeää, että oli käyttöjärjestelmä mikä tahansa, kannattaa verkkoselauksen yhteydessä varoa lataamasta tietoisesti haittaohjelmia tietokoneelle. (Bradley 2016.)

Windows 7 -käyttöjärjestelmän tietoturvauhkia ovat aiheuttaneet esimerkiksi käyttöjärjestelmän omat tietoturvapäivitykset, joiden kautta käyttöjärjestelmään on asentunut hyödynnettävä heikkous. Näitä heikkouksia on pyritty korjaamaan nopeasti, mutta ovat aiheuttaneet erilaisia ongelmia käyttöjärjestelmän turvallisuuteen. Useasti tietoturvaheikkoudet liittyvät käyttöjärjestelmän kernel driverien päivityksiin, jolloin esimerkiksi heikkous on ilmennyt. Mahdollinen hyökkääjä pystyi aiheuttamaan muistin korruptoitumista rakennetusta datalohkosta, mikä toteutettiin Safari-selaimen avulla. Käyttöjärjestelmässä on myös ilmennyt ongelmia sen Internet Explorer selaimessa, jota ei enää pidetä käyttäjien keskuudessa turvallisena selausmuotona. (CVE Details 2016b.)

3.3.4 Windows 8 ja Windows 10

Windows 8 -käyttöjärjestelmässä on viisi tietoturvaongelmaa, jotka on hyvä ottaa huomioon käyttöjärjestelmää käyttäessä. Ensimmäinen tietoturvaongelma korostuu Windows 8 sopivuudesta Windows 7 käyttöjärjestelmän ominaisuuksien kanssa, mikä aiheuttaa sen, että Windows 7 -ongelmat liittyvät myös vahvasti Windows 8 -käyttöjärjestelmään. Toiseksi Windows 8:lle on olemassa valheellisia virustorjuntaohjelmia, joiden käyttäminen aiheuttaa antivirustulosten vääristymistä, jolloin käyttäjä ei voi tietää, onko käytettävällä koneella mahdollisesti haittaohjelmia. Lisäksi Windows 8 -käyttöjärjestelmä ei pyri ehkäisemään ”Social eningeering”-ongelmia, jotka tarkoittavat yleisesti kaikkia tietokoneenvälityksellä tapahtuvaa sosiaalisen kanssakäymisen yhteydessä tapahtuvaa huijausta. Näitä huijauksia ovat esimerkiksi epärehellinen myynti ja tiedonkalastus. (Phneah 2012.)

Windows 8:n kanssa tuleva tietoturvaohjelmisto ei myöskään ole riittävän tehokas toimiakseen yksin turvatakseen tietokoneen tietoturvan. Siksi on kannattavaa käyttää myös toista ohjelmaa Windowsin oman ”security essentials”-sovelluksen kanssa. Vaikka Windows 8 -käyttöjärjestelmä sisältää myös osaa Windows 7 -käyttöjärjestelmän heikkouksista, on Windows 8 -heikkouksia myös Adoben sekä Microsoftin sovellusten kanssa, joita erilaiset haittaohjelmat voivat hyödyntää. (Phneah 2012.)

Vanhentuneet Windows-käyttöjärjestelmät Windows 7 sekä 8, voidaan tällä hetkellä päivittää ilmaiseksi uuteen Windows 10 -käyttöjärjestelmään. Windows 10 -käyttöjärjestelmä on kuitenkin saannut paljon arvostelua käyttöjärjestelmän yksityisyydensuojan takia. Käyttäjien verkkoselailua sekä toimintaa tarkkaillaan, jotta Microsoft voisi käyttää näitä tietoja markkinoinninsa kehittämiseen sekä mainonnan tarkentamiseen. Tämä siis tarkoittaa sitä, että suurin osa käyttäjän tekemisistä Windows 10 -käyttöjärjestelmän kanssa on sellaista toimintaa, jota Windows 10 voi tarkkailla. Windows 10 -käyttöjärjestelmässä näitä asioita voidaan kuitenkin ottaa pois käytöstä, mutta se ei tarkoita sitä, että kaikki tiedot ovat turvassa Microsoftin tiedonkeräämiseltä. (Forrest 2015.)

Windows 10 -käyttöjärjestelmässä on myös paljon hyvää. Windowsin uusi verkkoselain Microsoft Edge on tullut Firefoxin sekä Chrome -selaimen kilpailija sekä on korvaava tuote vanhalle Internet Explorer-tuotesarjalle. On kuitenkin huomioitava, että Edge selain on vielä suhteellisen uusi selain, joten erilaisia heikkouksia on odotettavissa tulevaisuudessa. Windows 10 - käyttöjärjestelmä on helppo päivittää vanhasta Windows 7 tai 8 -käyttöjärjestelmästä ilmaiseksi, mutta ei ole mahdollista esimerkiksi Windows XP:stä. Lisäksi Windows 10 tukee uutta DirectX 12, jota käytetään tietokoneiden grafiikan kehittämisessä. (Casserly 2016.)

3.4 Virusturva

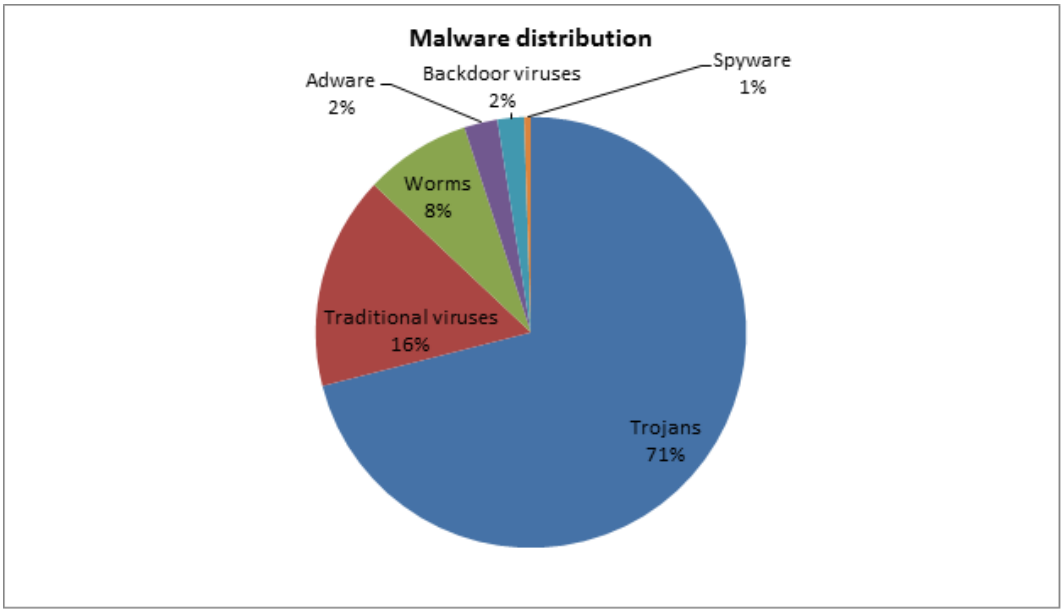
Virusturvan toiminta on tärkeä osa työntekijän sekä yrityksen tietoturvan ylläpitoa sekä työkalu erilaisten ongelmien ratkaisemiseen tietokoneen toimivuudessa. Työasemissa käytössä olevissa virustorjuntasovelluksissa on kaksi ominaisuutta. Ensimmäinen näistä on tietokoneen tilan tarkkailu mahdollisten poikkeuksien huomaamiseksi. Virusturvan toinen ominaisuus on liikkuvien tiedostojen tarkastaminen. Tällä tarkoitetaan sitä, että tiedostot, joita tietokoneelle ladataan tai vastaanotetaan esimerkiksi sähköpostien tai latauslinkkien välityksellä, tarkistetaan virustunnisteiden avulla, jotta käyttäjän työasema olisi turvassa verkossa leviäviä malwareja vastaan. Virusturvan taustana on suojella käyttäjän yksityisyyttä sekä käyttäjän tärkeitä tietoja, kuten luottokorttitietoja sekä esimerkiksi tietokoneelta löytyviä erilaisia muistoja elämästä sekä tärkeistä ihmisistä. (Viljanen 2016a.)

Virusturvan antama suoja ei ole kuitenkaan varma. Verkoissa liikkuvat haittaojelmat muuttuvat, päivittyvät ja uusia Malwareja syntyy päivittäin. Virustorjuntaohjelmistot eivät pysy kaikkien haittaohjelmien perässä, sillä ne tarvitsevat haittaohjelmien tunnistamiseen käytettävät virustunnisteet. Mahdollisten riskien minimoimiseksi kannataa ylläpitää virusturvan tunnistepäivitykset ajan tasalla. Jotkin tietoturvasovellukset päivittävät itsestään virusturvan tunnisteet esimerkiksi käynnistyksen yhteydessä. Virusturvasovelluksen käyttämisessä on myös ongelmia.

Virusturvasovelluksessa itsessään voi ilmetä erilaisia heikkouksia, jotka jälleen altistavat työaseman vaaroille. (Viljanen 2016a.)

3.5 Malwaret ja haittaohjelmat

Viruksia ja erilaisia haittaohjelmia on olemassa modernissa internet-liikenteessä valtavasti. Erilaisia viruksia ja haittaohjelmia kutsutaan Malwareiksi. Tietoturvan kannalta yrityksen tietokoneiden käyttäjien on hyvä pyrkiä erottamaan mahdolliset Malware-tyypit toisistaan. Yleisellä tasolla mahdolliset Malwaret torjutaan päivitetyn virustorjuntasovelluksen avulla, mutta joskus esimerkiksi uusia Malwareita ei ole vielä päivitetty virustorjuntasovelluksen tietokantaan. Kuitenkin suurin osa kaikista virusten saastuttaneista tietokoneista johtuu käyttäjän suorittamasta virheestä, jossa käyttäjä saattaa vahingokseen avata roskapostin tai ladata tarpeelliselta näyttävän sovelluksen, joka osoittautuukin virukseksi. Kuviossa 3 nähdään Malwaretyyppien jako. (Cisco 2016.)



KUVIO 3. Haittaojelmien jaottelu (Bullguard 2016)

Ensimmäinen Malwaren alaluokka ovat virukset. Virukset toteuttavat tietokoneiden saastuttamisen kopioimalla itsensä toisen sovelluksen osaksi. Virukset voivat levitä esimerkiksi sähköpostien ja erilaisten tiedostojen siirtymisen myötä. Koska virukset tulevat yleensä erilaisten sovelluksen kylkiäisenä, ne eivät välttämättä käynnisty heti tietokoneen saastutettuaan. Virukset saattavat käynnistyä vasta sitten, kun saastutettu sovellus käynnistetään. Virukset aiheuttavat tietokoneissa tiedostojen vaurioitumista ja mahdollisia DoS-ongelmia. DoS-ongelmiksi kutsutaan sellaisia hyökkäyksiä, jotka estävät tietyjen tietokoneen ominaisuuksien käyttämisen tai koko tietokoneen käyttämisen estämisen. (Cisco 2016.)

Toinen Malwaren alaluokka ovat madot, joiden toiminta eroaa esimerkiksi virusten toiminnasta siten, että madot voivat hyödyntää tietokoneen mahdollisia tietoturvan heikkouksia ja aukkoja päästäkseen tietokoneeseen sisälle. Madot eivät tarvitse virusten tarvitsemaa emäntäsovellusta. Madot voivat kuitenkin levitä myös tiedostojen lähetysten yhteydessä esimerkiksi yrityksen tärkeässä sähköposti-liikenteessä. Lisäksi madot toimivat itsenäisesti eivätkä tarvitse käyttäjien apua toimintansa aktivoimiseksi. Matojen aiheuttamat ongelmat ovat kuitenkin samankaltaisia esimerkiksi viruksiin verraten. Madot siis aiheuttavat erilaisia käytettävyysongelmia sekä estävät ominaisuuksien käyttöä. (Cisco 2016.)

Malwaren alaluokista kolmantena ovat malwareista yleisimmät eli trojalaiset. Troijalaiset toimivat huijaamisen sovelluksena, jotka näyttävät ensimmäiseksi täysin normaalilta. Kun sovellus aukaistaan, troijalainen aktivoituu ja voi esimerkiksi haitata käyttäjän työskentelyä avaamalla ohjelmia sekä hyppyikkunoita. Lisäksi troijalainen voi aiheuttaa yrityksen tärkeiden tiedostojen poistamista, vaurioitumista tai ryöstämistä. Troijalaiset voivat myös auttaa muiden Malware-tyyppien pääsemisen tietokoneelle, vaikka avamaalla tietokoneesta takaportin, jonka heikkoutta esimerkiksi madot voivat hyödyntää. Toisaalta troijalaisen sovelluksen kanssa voi koneelle siirtyä myös viruksia. Troijalaisten heikkoutena verrattaessa muihin malwaretyyppeihin on se, että troijalaiset eivät kloonaa itseään, kuten madot ja virukset. (Cisco 2016.)

Malwaren neljäntenä suurena alaluokkana ovat botti-prosessit, joiden tarkoitus on tuottaa automaatiota verkossa ja tietokoneissa. Botti-alaluokkaa ei voida suoraan kuvailla haitalliseksi toiminnaksi, sillä botteja voidaan käyttää sekä hyvään että haitalliseen tarkoitukseen. Bottien avulla haitallisen tavoitteen omaava hyökkääjä voi käyttää käyttäjän tietokonetta muiden tietokoneiden käyttäjien toiminnan hidastamiseen tai jopa estämiseen. Botti voi esimerkiksi käynnistää tietokoneella verkkoselaimen ja ruveta häiritsemään verkkosivujen toimintaa. Toisaalta botti voi toimia kuten madotkin eli kloonautua sekä levittäytyä toisiin verkossa oleviin laitteisiin. (Cisco 2016.)

Malware-alaluokkia on olemassa myös muita, mutta ne eivät ole niin merkittäviä alaluokkia harvinaisuutensa vuoksi. Näitä alaluokkia ovat vakoiluohjelmat, pakkomainostusohjelmat ja takaporttivirukset. Vakoiluohjelmien ominaisuus toimii siten, että ne eivät yleensä tee ongelmia tietokoneelle, mutta tutkvat tietokoneen käyttäjän toimintaa ja verkkoliikennettä. Lisäksi spyware saattaa pyrkiä poimimaan käytettyjä salasanoja, jotta niitä voidaan varastaa. Pakkomainostusohjelmat taas toimivat, kuten troijalaiset, mutta niiden päämääränä on verkkoselailun yhteydessä avata erilaisia ponnahdusikkuna mainoksia, jotka häiritsevät työntekoa verkossa. Takaporttivirusten toiminta eroaa normaaleista viruksista siten, että ne pyrkivät avamaan tietokoneen sisältä löytyviä heikkouksia, jotta muut malwaren-alaluokat pääsevät tietokoneeseen hyökkäämään. (Cisco 2016.)

3.6 Tietoliikenteen turvaaminen

Tietoliikenteessä on kyse monista osa-alueista, joiden yhteistoiminta muodostaa kokonaisuuden. Näiden osa-alueiden tietoturvallisuuden ylläpitäminen on tärkeää turvallisen verkkokokonaisuuden ylläpitämiseksi. Tietoliikenteen tietoturvan ylläpitämiseksi ovat esimerkiksi kaapeloinnin suojaus sekä varajärjestelyt tärkeitä (taulukko 2).(Vahti-ylläpito 2016.)

TAULUKKO 2. Verkkokokonaisuuden ylläpito.

Kaapeloinnin suojaus	Kaapelit ovat suojassa fyysisiltä uhilta, kuten katkaisulta ja vaurioitumiselta.
Aktiivilaitteiden suojaus	Aktiivilaitteet ovat turvalliseessa paikassa ja niiden asetukset ovat suojattu.
Ulkoisten yhteyksien Turvaaminen	Verkkoyhteydet ovat vikasietoisia esimerkiksi palomuurin ja virustorjunnan avulla.
Varajärjestelyt	Tietoliikenne yhteyksille on olemassa korvaavia laitteita ja varaosia.
Etäkäyttöyhteydet	Mahdolliset etäkäyttöyhteydet on suojattu esimerkiksi salasanalla.
Verkkosegmentit	Erilaiset tietoverkot ovat eritetty toisistaan.

Näiden osa-alueiden lisäksi on tarpeellista käsitellä yrityksen tietoturvan kannalta kahta oleellista tietoliikenteen aluetta. Nämä alueet ovat tietoliikenteen palomuuri ja varajärjestelyt. (Vahti-ylläpito 2016.)

3.6.1 Palomuuri

Palomuurin tehtävänä on suodattaa tietokoneelle liikkuva liikenne ja informaatio, jotta se pysyisi puhtaana. Palomuuri toimii yrityksen sisäverkon ja ulkoisen internetin välillä suojaten sisäverkkoa ulkoisilta tekijöiltä. Palomuurin toiminta perustuu erilaisten protokollien yhteistoimintaan mahdollisten osoiteenmuutos-protokollien avulla. Proxy-palvelimien avulla palomuuri voi rakentaa ”muurin” sisäverkon sekä ulkoverkon välille. Fyysinen esimerkki tästä on yrityksen toimitilojen seinät, jotka erottavat yrityksen toiminnan ulkomaailmasta. Samanlaisella tavalla toimii palomuuri, mutta vain verkossa. (VirtuaaliAMK 2016.)

Palomuurin tietoturvan edistämiseksi muodostetaan yritysverkkoon usein NAT-verkoitus. NAT (Network Address Translation) -protokokollan tarkoituksena on lyhyesti piilottaa yrityksen sisäverkon tietokoneet ulkoverkon nähtäviltä. Yritykselle muodostetaan NAT-protokollan avulla palomuurille oma IP-osoite, joka toimii koko sisäverkon liikenteen IP-osoitteeena. NAT :n avulla voidaan määritellä, mihin sisäverkon tietokoneelle minkäkin paketin kuuluu liikkua oikein asetetun NAT:n avulla. Tietoturvan kohottamisessa NAT toimii hyvin, koska tunkeilijan on vaikea määritellä tunkeuduttavan sisäverkon koneita, sillä sisäverkosta nähdään ulos vain yksi IP-osoite. (VirtuaaliAMK 2016.)

Palomuuri suodattaa erilaisia paketteja, mitkä liikkuvat verkon yli yrityksen verkkoon. Suodattaminen hyödyntää useita protokollia, joita ovat verkon peruspilarit UDP- (User Datagram Protocol) ja TCP (Transmission Control Protocol) protokollat. Muita välttämättömiä protokollia ovat ICMP (Internet Control Message Protocol) sekä IGMP (Internet Group Management Protocol) -protokollat. Esimerkiksi UDP- sekä TCP -protokollat toimivat informaation lähettämiseen käytettynä protokollina. TCP-protokollan toiminta perustuu lähetettyjen pakettien toimittamiseen käyttäjältä verkkoon. TCP-protokolla numeroi lähettämänsä paketit ja tarkistaa, onko paketit lähetetty sekä vastaanotettu oikein. Mikäli TCP-protokolla huomaa ongelmia pakettien lähetyksessä, lähettää protokolla ne uudelleen. UDP-

protokollan toiminta eroaa TCP-protokollasta hieman. UDP-protokolla ei esimerkiksi tarkista onko paketit lähetetty oikein. (Hoffman 2014.)

3.6.2 Verkonvalvonta

Yrityksen tietoturvassa on hyödyllistä, että yrityksen verkon käyttäytymistä valvotaan, jotta vikatilanteissa on mahdollista nopeasti määrittää verkon laitteidein kunto sekä keskittää resurssit valmiiksi oikealle alueelle verkossa. Verkonvalvonnan lisääminen verkkolaitteille antaa ylläpitotyöntekijöille mahdollisuuden tarkkailla verkosta siirtyvän informaation määrää sekä tutkia, mikä osa verkosta joutuu suurimman käyttöasteen alaisuuteen. Lisäksi hyvin rakennettu verkonvalvonta huomaa automaattisesti, mikäli verkossa tapahtuu häiriöitä. Verkonvalvontaan voidaan myös lisätä monia erilaisia laitteita. Näitä laitteita ovat yksittäiset työasemat, verkon tukiasemat ja jopa verkkotulostimien toiminta. (Zabbix 2016.)

Verkonvalvonta voidaan toteuttaa erilaisten triggereiden avulla. Voidaan esimerkiksi määritellä trigger, joka ilmoittaa häiriön, mikäli tuotannolle tärkeän tietokoneen verkkoyhteys katkeaa. Tällöin verkonvalvonta ilmoittaa tästä sovelluksessaan tai mobiilisovelluksen avulla. Verkonvalvonnan triggerit lähettävät myös viestin, kun häiriö on saatu korjatuksi tai tilanne palautuu normaaliksi. Verkonvalvonnassa voidaan myös tarkailla verkon toimintaa erilaisten graafisten kuvien avulla, millä voidaan tarkailla esimerkiksi yhden tukiaseman toimintaa esimerkiksi leipomon kahvilan ilmaisessa verkossa. (Zabbix 2016.)

3.6.3 Verkon varajärjestelyt

Yrityksissä verkon toiminta perustuu aina fyysisten laitteiden toimintaan, kuten verkon toiminassa yleensä on mahdollisuus siihen, että jokin fyysinen laite hajoaa tai siitä koituu ongelmia. Tietoturvan kannalta on tärkeää, että verkon vikasietoisuus ja varajärjestelmät ovat kunnossa. Mikäli vikasietoisuuden kanssa tulee ongelmia ja esimerkiksi yrityksen verkon kytkimessä tai reitittimessä tulee vikatilanne, voi yrityksen

verkkotoiminta häiriintyä. Siksi on tärkeää, että verkkolaitteita on olemassa myös varalle. Varalaitteet voivat olla esimerkiksi käytetyn laitteen vastaava laite, johon on käytetyn laitteet asetukset sijoitettu, jotta se voidaan ottaa käyttöön häiriötilanteissa. Mikäli verkkoa toteutetaan myös langattomana, on verkon toiminnan takaamiseksi hyvä olla olemassa myös varatukiasemia, joiden asetukset on määritelty kyseiselle verkolle. Varajärjestelyn kannalta on myös tarpeellista, että fyysiset kuiduille tai verkkokaapeille on riittävästi varakappaleita. (Koivunen 2010.)

Varajärjestelmien ylläpitämiseksi on järkevää tarkistaa varalaitteiden toiminta määräajoin. Tällä tavoin yrityksessä on aina toimivia verkkolaitteita sekä vastaavasti tietokoneita, jolloin yrityksen tuottavuus pysyy mahdollisimman täydellisenä. Varajärjestelmät kannattaa optimoida siten, että niiden toiminta on käytännöllinen, jotta niiden käyttöönottaminen olisi mahdollisimman käytännöllistä. Lisäksi yrityksessä kannattaa määritellä henkilöstöstä useampi osaava henkilö, jotka tietävävät kuinka, verkon varajärjestelmä otetaan käyttöön. Yrityksessä voidaan myös ostaa varajärjestelmäpalveluita tietotekniikan yrityksiltä, joiden palvelut ylläpitävät yrityksen verkon toimintaa. (Koivunen 2010.)

3.7 Yksityisyyden suoja

Suomen lainsäädäntö määrää jokaiselle yksityiselle henkilölle oikeuden omaan yksityisyyteen, minkä takana on jokaisen henkilön turvallisuuden takaaminen. Tietokoneen käyttämisen yhteydessä yrityksessä tulee vastaan työntekijöiden sekä asiakkaiden tietoja sekä mahdollisesti sähköisessä muodossa ilmeviä sopimuksia sekä tilauksia. Hyvän tietoturvan omaava yritys pyrkii toteuttamaan mahdollisimman järkevää sekä toiminnaltaan kattavaa yksityisyyden suojaa, jonka avulla kehitetään myös asiakasystävällisyyttä ja toimivaa yritystoimintaa. (Viljanen 2016b.)

Yksityisyyden suojan lainsäädäntöä on määritelty Suomen laissa tarkasti. Yksityisyyden suojan lakina voidaan esimerkkinä ottaa laki yksityisyyden suojasta työelämässä. Laissa määritellään tarkasti työnantajan mahdollisuudet käyttää henkilöstönsä tietoja sekä viitataan, mitä oikeuksia

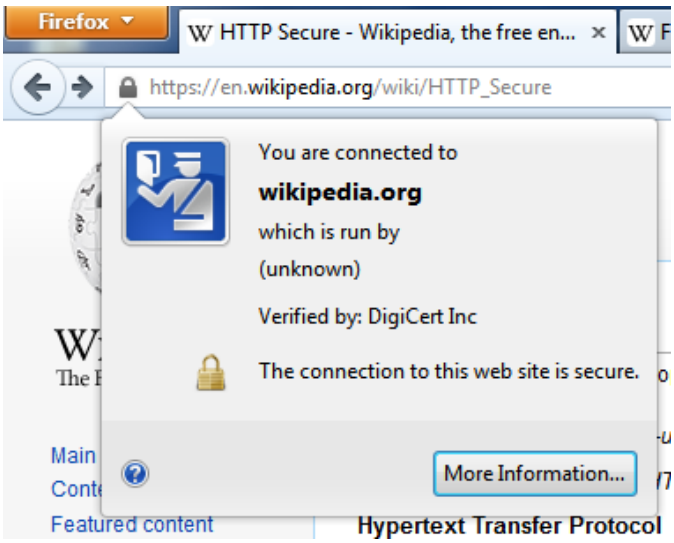
henkilöstöllä on erilaisiin toimenpiteisiin työskentelyn yhteydessä esimerkiksi sähköisten viestien yhteydessä. Tietoturvan kannalta on tärkeää, että yrityksen johto sekä henkilöstö tietävät oikeutensa sekä velvollisuutensa tietojenkäsittelyn osalta. Tällä tavoin yksityisyyden suojan tavoite toteutuu ja yksityisten henkilöiden tiedot ovat turvassa. (Finlex 2004.)

3.8 Tiedon suojaaminen

Yrityksellä on paljon erilaisia asiakirjoja, kuten erilaisia lomakkeita, tilauksia ja sopimuksia. Asiakirjojen pitäisi olla säilytettynä sellaisessa paikassa, jossa niiden säilyminen olisi mahdollisimman pitkäikäistä sekä tietoturvallista. Perinteisen fyysisen säilyttämisen tilalle viimevuosikymmeninä muodostunut erilaisia tapoja säilyttää tietoa verkossa sekä tietokoneella. Näitä säilytysmenetelmiä ovat esimerkiksi kovalevysäilytys sekä pilvipalvelusäilytys. Tiedon suojaamisen kannalta on kuitenkin tärkeää selvittää keinoja, joilla tiedon luottamuksellisuus ja esimerkiksi suojaaminen on mahdollista. (Viestintävirasto 2016c.)

Erilaisten tiedostojen suojaaminen voidaan aloittaa miettimällä,onko kysessä oleva tieto tai tiedosto luottamuksellinen vai julkinen. Mikäli tieto on määritelty asianosaisten kesken luottamukselliseksi, on sen suojaaminen Suomen lain mukaan välttämätöntä. Verkossa sekä sähköpostiliikenteessä liikkuvan tiedon suojaaminen voidaan aloittaa sillä, että onko käytössä oleva verkkopalvelu SSL (Secure Sockets Layer) suojattu, jolloin sen käyttäminen on yleisiä verkkopalveluita suojatumpi. SSL-suojauksen toiminna verkkoselaimessa tunnistaa verkko-osoiteen https:// muodosta sekä graaffisesta lukon kuvasta osoitteen välittömässä läheisyydessä (Kuvio 4). SSL-verkkosuojausta käytetään yleisesti pankkiliikenteen salaamisen yhteydessä sekä erilaisten suojattujen verkkosivujen suojaamiseen. Tietoturvan kannalta on myös tärkeää huomioida sähköpostiliikenteen suojaaminen. Sähköpostisovelluksen asetuksista voidaan määritellä sähköpostin suojauksista. Lisäksi voidaan

käyttää mahdollisia kryptaustyökaluja ja salasanasuojausta. (Viestintävirasto 2016c.)



KUVIO 4. SSL suojaus selauksessa (Wikipedia 2016.)

3.8.1 Tiedon tallentaminen

Tiedon tallentamisen yhteydessä ajatellaan usein, onko tallennettu tieto varmasti tallessa sekä mahdollisesti turvassa ulkopuolisilta käyttäjiltä. Erilaisten tekstitiedostojen tallentaminen voidaan toteuttaa esimerkiksi Office-paketin avulla. Office-paketin valikosta löytyy painike, josta voidaan valita ”valmistele”. Tämän valikon kautta on mahdollista löytää tiedostolle tarpeellisia suojauskeinoja, kuten lukijan käyttöoikeuksia. Käyttöoikeuksien avulla voidaan esimerkiksi valita, voiko tiedoston lukija esimerkiksi muokata tiedostoa vai onko kyseinen tiedosto vain lukijalle luettavassa tilassa. Näitä oikeuksia voidaan varmentaa asettamalla tiedostolle salasana, jonka avulla vain asiankuuluvat henkilöt voivat tiedostoon tehdä muutoksia. Lisäksi valikosta voidaan valita ”Merkitse lopulliseksi”, jolloin käsiteltävä tiedosto muuttuu vain luettavaan muotoon. Valikosta voidaan myös tarkistaa varsin hyödyllinen ”yhteensopivuuden tarkistaminen”, jolla voidaan käsitellä, mitä erilaisia ominaisuuksia eri office-versioissa ei voida käsitellä. Tiedoston suojaaminen voidaan toteuttaa Office Word, Excel ja Powerpoint -tiedostoilla ja näille kaikille voidaan määritellä salasana sekä tarvittaessa myös poistaa se. (Microsoft 2016.)

Windows-käyttöjärjestelmällä voidaan myös varmuuskopioida tärkeitä tiedostoja. Tärkeiden tiedostojen varmuuskopiointi kannattaa toteuttaa silloin kun käyttäjä pitää käsiteltävää tiedostoa tärkeänä. Tiedoston varmuuskopiointi voidaan toteuttaa helposti kolmella tavalla. Ensimmäisenä tapana on tiedoston varmuuskopiointi sille varatun ohjelmiston avulla. Microsoft tarjoaa käyttäjilleee ”Microsoft silverlight”-sovelluksen, jonka avulla voidaan tiedostoja varmuuskopioida. Silverlight-sovellukselle voidaan antaa oikeudet automaattiseen varmuuskopiointiin, mikä helpottaa työskentelyä, mutta saattaa aiheuttaa tietokoneen hidastumista sekä kovalevyjen täyttymistä. (Windows7 2016.)

Toisena tapana on käyttää mahdollista pilvipalvelua tärkeiden tiedostojen säilyttämiseen. Esimerkkinä pilvipalvelusta voidaan käyttää Google Drive-palvelua, johon rekistöröity käyttäjä pystyy säilyttämään tiedostoja. Lisäksi Google Drive-palvelun avulla voidaan jakaa tiedostoja sähköpostiosoitteen avulla. Google Drive-palvelussa on mahdollista uusien tiedostojen luominen. On kuitenkin huomattava, että kirjoitusominaisuudet eivät ole niin kattavia, kuten verrattaessa Microsoftin office-paketteihin. Tärkeästä tiedostosta kannattaa tehdä kopio, jota sitten säilytetään verkko-palvelussa. Kolmantena tapana voidaan pitää erillistä kovalevyä, johon kopiot erilaisista tärkeistä tiedostoista voidaan säilyttää. Turvallisuutta varmuuskopioinissa lisää se, että niiden käyttämät sovellukset mahdollistavat salasanan käyttämisen ja tällöin tiedostot ovat paremmassa turvassa. (Google Drive 2016.)

3.8.2 Tiedon hävittäminen

Tietoa käsiteltäessä tulee ottaa huomioon vanhentuneiden tiedostojen hävittäminen. Tietoturvallinen tiedon hävittäminen toteutetaan siten, että mahdollinen luottamuksellinen tieto hävitetään lopullisesti eikä sitä voida enää palauttaa. Hävitettävän tiedoston poistaminen ei riitä tiedoston lopulliseen poistamiseen, sillä kovalevyltä poistettu tieto ei poista tiedoston sisältöä vaan katkaisee yhteyden kyseiseen tiedostoon. Tiedoston sisältö poistuu vasta sitten, kun kovalevylle laitettu uusi tieto ylikirjoittaa vanhan, jolloin edellinen sisältö korvautuu. Tiedostojen hävittämiseen on olemassa erilaisia sovelluksia, joiden avulla voidaan tiedostoja hävittää. Ohjelmat toimivat siten, että ohjelma tarkoituksen mukaisesti ylikirjoittaa halutun tiedoston päälle uutta koodia. Tiedoston hävittämisen varmistaminen voidaan toteuttaa toistamalla ylikirjoittaminen useamman kerran, jos hävitettävä tiedosto on erittäin arkaluontoinen. (Viljanen 2016c.)

Yrityksen tietokoneiden vanhennettua tietokoneet hävitetään tai myydään. Silloin voi yritykselle olla tärkeää hävittää kovalevyltä kaikki sen sisältämä tieto. Koko kovalevyn tietoturvalliseen hävittämiseen on verkossa olemassa erilaisia sovelluksia. Sovellukset toimivat yleensä siten, että sovellus asennetaan CD- tai DVD-levylle ja sitä käytetään tietokoneessa kovalevyn pyyhkimiseen. Mikäli kovalevy halutaan hävittää esimerkiksi kaatopaikalle, voidaan sen tuhoaminen suorittaa myös fyysisin keinoin tuhoamalla sen virtapiirit. (Viljanen 2016c.)

4 TIETOTURVAN KEHITTÄMISSUUNNITELMA

Kehittämissuunnitelman tarkoituksena on kehittää tapoja sekä ohjeita yrityksen tietoturvan toteuttamiseen sekä kehittämiseen. Suunnitelman päämääräiset aihealueet mukautuvat käyttäjäkokemuksen parantamiseen sekä työskentelyn helpottamiseen samanaikaisesti toteutettavien tietoturvan elementtien tarkastelusta. Kehittämissuunnitelman aihealueet ovat käyttöjärjestelmien päivittäminen, palomuuri, virusturva, verkonvalvonta, asiakirjojen verkkosäilyttäminen.

Näiden aihealueiden huomioiminen on tärkeää turvallisen kokonaissuunnitelman rakentamiseksi. Suunnitelman muodostamisessa käsitellään ensimmäiseksi aihealueita. Näissä aihealueissa vertaillaan sekä toteutetaan päätös tuotteen valinnasta. Ohjeistuksen sekä vertailun jälkeen toteutetaan kahdeksan osainen vaiheittainen suunnitelma, jonka avulla voidaan yrityksen tietoturvaa parantaa ja todeta vaiheiden toiminta toteutuneeksi.

4.1 Käyttöjärjestelmien päivittäminen

Käyttöjärjestelmien päivittämisen lähtökohtana on vanhan tietoturvattoman käyttöjärjestelmän päivittäminen uudempaan tietoturvallisempaan järjestelmään. Vaikka jokaisessa käyttöjärjestelmässä on käyttöjärjestelmäkohtaiset tietoturvaongelmat, ovat uudemmat järjestelmät keskiarvoltaan edeltäjiään turvallisempia. Näiden käyttöjärjestelmien asentaminen on ohjeita noudattamalla yksinkertainen toimenpide, mutta perinteisen pöytäkoneen käyttäjälle nämä asennukset saattavat tuottaa vaikeuksia.

Tämän osuuden tarkoituksena on asentaa pöytäkoneelle sekä Windows 7- että myös Windows 10 -käyttöjärjestelmä asennuksen kohtaan, jossa käyttäjä saa päivitetyn käyttöjärjestelmän työpöydän näkyville. Käyttöjärjestelmien asennusohjeet ovat liitteinä. Windows 7-asennusohje on liitteenä 2 ja Windows 10-asennusohje liitteenä 3.

4.2 Verkonvalvonta

Turvallisen verkon toimintaa valvotaan verkonvalvonnalla. Taulukossa 3 on vertailtu kahta verkonvalvontasovellusta. Vertailtaviksi ominaisuuksiksi on valittu tuotteen hinta, tuotteen päivitettävyys, käyttö sekä käyttökokemus.

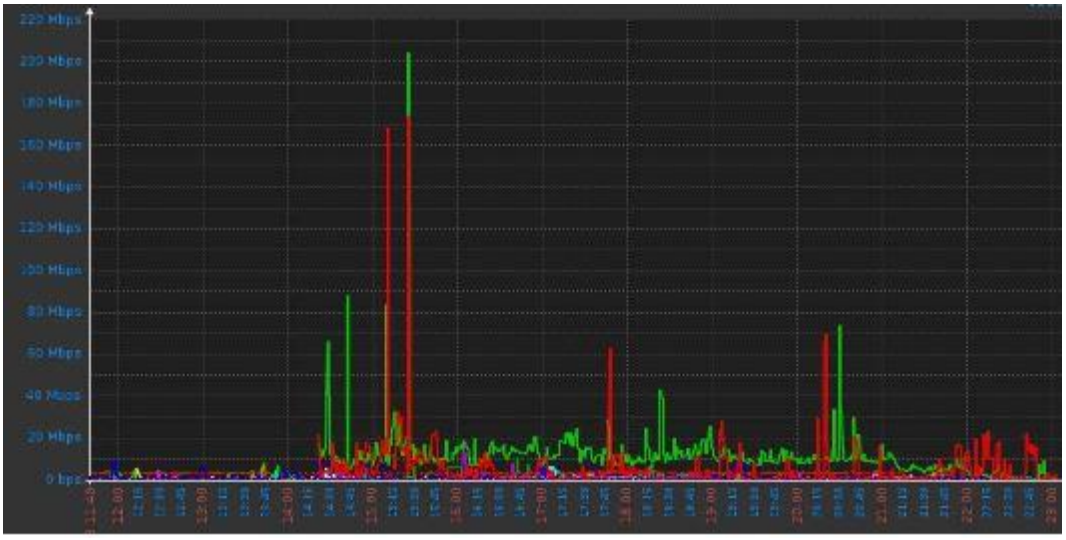
TAULUKKO 3. Verkonvalvonnan ominaisuudet

Ominaisuus	Zabbix	Solarwinds
Hinta:	Open Source, jolloin ohjelmisto on ilmainen.	Hinta alkaen 2275€.
Päivitykset:	Viimeisin päivitys: 2/2016.	Viimeisin suurempi päivitys 4/2014.
Käyttö:	Toimii pienemmilläkin verkoilla.	Tarkoitettu laajemmille verkoille.
Käyttökokemus	Helppokäyttöinen ja käyttämisen opetteleminen ohjeiden kanssa yksinkertaista.	Yksinkertainen käyttöliittymä, mutta pienemmälle verkolle monimutkainen toteuttaa.

Verkonvalvonnan hintavertailussa taloudellisin vaihtoehto on Zabbix. Solarwindsille on olemassa 30 päivän trial-versio, mutta testiversio sopii vain testaukseen. Zabbix-verkonvalvontasovellusta päivitetään jatkuvasti ja sovellus käyttäjälleen ilmainen. Zabbixilla on monimutkaisempi alkuasennus, mutta tämän jälkeen sovelluksen hallinta on helppoa. Solarwinds-verkonvalvontaohjelmisto on tarkoitettu suurille verkoille, joissa laitteiden määrä on suuri ja maailmanlaajuinen. Zabbix-verkonvalvonta-sovellukselle riittää, että valvotaan esimerkiksi muutamien palveluiden toimimista, kuten tukiasemien ja verkkotulostimien toimintaa.

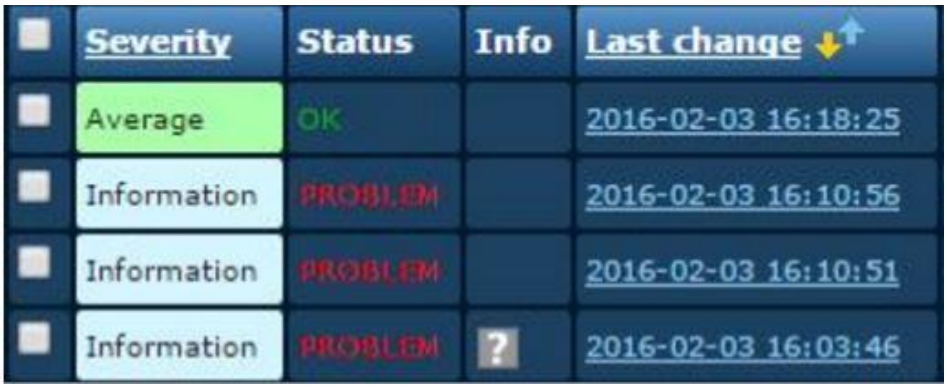
Käyttökokemukseltaan verkonvalvontasovellukset ovat hyvin erilaisen näköisiä, mutta yksinkertaisia. Solarwindsin laitteet saadaan näkyville käyttöliittymän vasemman reunan paneelista. Zabbixissa käyttöliittymää voidaan muokata siten, että käyttöliittymän laatikoita voidaan tuoda etusivulle, siten miten käyttäjälle on käyttäjäystävällisintä.

Zabbix-verkonvalvontaohjelmistossa on muutamia hyödyllisiä ominaisuuksia, joiden avulla verkon tarkkaileminen on käytännöllistä. Verkonvalvontaohjelmisto Zabbixin avulla voidaan seurata erilaisia liikennemääriä, esimerkiksi tukiasemien liikennettä. Kuvio 5 esittää eräitä verkkoliikennemääriä.



KUVIO 5. Liikennemääriä.

Kuviosta 5 nähdään kuinka liikennemäärät vaihtelevat aika-akselilla. Käyttöasteen avulla voidaan esimerkiksi tutkia niitä verkon osia, jotka saattaisivat tarvita lisää resursseja. Verkonvalvontajärjestelmissä on mahdollista myös vastaanottaa erilaisia häiriöilmoituksia, joita voidaan tutkia Zabbixin avulla seuraavassa kuviossa (kuvio 6).



KUVIO 6. Virheilmoitukset

Verkonvalvontasovelluksen häiriöilmoituksen tärkeitä asiakohtia ovat häiriön alkamisajankohta tai muutokset, laite, jota häiriö koskee, sekä tarvittaessa ongelman prioriteettinen kriittisyys. Näiden arvojen avulla voidaan muodostaa kattava valvontaverkko yrityksen tilojen laitteisiin, joiden verkkoliikenteen toimivuutta halutaan valvoa.

Zabbix-verkonvalvonnan valintaan päädyttiin vertailemalla kyseistä ohjelmistoa vastaavaan Solarwinds-verkonvalvonnan kanssa. Solarwinds vaikutti alkuperäiseltä tarkoitukseltaan sopivalta valinnalta, mutta Zabbix-verkonvalvontaan päädyttiin taloudellisuuden perusteella.

4.3 Palomuuri

Palomuuriohjelmistolla voidaan käytännössä antaa verkolle sen tarvitsemaa tietoturvaa erilaiselta liikenteeltä. Tässä käytännön esimerkissä paneudutaan palomuurisääntöjen luomiseen. Palomuuri-ohjelmiston valinta toteuttiin vertailun avulla. Vertailussa PfSensen rinnalla toimi palomuuriohjelmisto Sophos, jota vertaillaan seuraavassa taulukossa.

TAULUKKO 4. Palomuurien ominaisuuksia

Ominaisuus	PfSense	Sophos
Hinta	Ilmainen	Kotikäyttäjälle ilmainen, yritykselle maksullinen
Vaatimukset	Toimii vanhoillakin osilla	Tarvitsee enemmän tehoja toimiakseen
Toiminta	Ilmaiseksi tehokas palomuuri ohjelmisto	Todella suojaava palomuuri ohjelmisto
Käyttöliittymä	Yksinkertainen ja käytännöllinen	Monipuoliset toiminnot ja helposti muokattavissa

Kuten taulukosta 4 nähdään, eroavat palomuuriohjelmistot toisistaan esimerkiksi sillä, että Sophos on yrityskäyttöön maksullinen, mutta tehokkaampi palomuuriohjelmisto. Toisaalta PfSensen toimintaa korostaa ohjelmiston toimiminen pienemmillä vaatimuksilla.
Toimintatarkoitukseltaan kumpikin sovellus toimii tehtävässään ja suorittaa palomuurisovellukselta vaaditut toiminnot.

Palomuurisääntöjen perusteet juurtuvat yksittäisten tai useiden IP-osoitteiden hallintaan sekä erilaisten protokollapakettien hallintaan. Pfsense-sovelluksessa palomuurisääntöjen hallinta toimii Firewall-osiosta, josta valitaan erikseen kohta Rules. Palomuurisääntöjen muokkaaminen ja luominen tapahtuu PFsensessä taulukon vasemmasta reunasta. Sääntöjä voidaan antaa esimerkiksi seuraavan kuvion mukaan. (kuvio 7).

KUVIO 7. Palomuurisääntöjen pohjakaavio

Kuviosta 7 nähdään sääntöjen pohjamuoto, johon valmiit palomuuri-säännöt tulevat näkyville. Sääntöjen luonti tapahtuu kuitenkin kyseisen sivun oikeasta reunasta, josta painetaan painike edit. Painikkeesta avautuu PFsensen sääntöjen muodostamiseen tarkoitettu kuvio. (Kuvio8).

KUVIO 8. Palomuurisääntöjen muodostaminen

Sääntöjä muodostetaan PFsensen avulla seuraavalla tavalla. Action paneelista voidaan valita, onko muodostettavan säännön tarkoitus sallia, estää tai torjua. Seuraavasta Disabled-osiosta sääntö voidaan poistaa käytöstä, mutta säilyttää se kuitenkin palomuurisääntöjen listassa. Säännön muokkauksessa seuraavana kohtana on Interface, josta valitaan, mistä interfacesta halutaan, että liikenne kulkee, jotta ne täyttävät rakenteilla olevan säännön. Tähän sääntöön voidaan valita esimerkiksi WAN-liityntä. Kun jatketaan säännön rakentamisessa eteenpäin, päästään Protocol-osuuteen, josta valitaan, millaisia protocolpaketteja tämä sääntö koskee. Tästä osuudesta voidaan valita esimerkiksi IP-osoitteiden protokollat TCP ja UDP. Source ja destination -valikosta määritellään säännölle lähtö- ja loppupiste. Nämä pisteet voidaan määritellä esimerkiksi IP-osoitteiden ja porttien avulla. Sääntöasetusten lisäksi palomuurisäännölle voidaan kirjoittaa kuvaus, jota luotu palomuurin sääntö yhdistää.

4.4 Virusturvan käyttövertailu

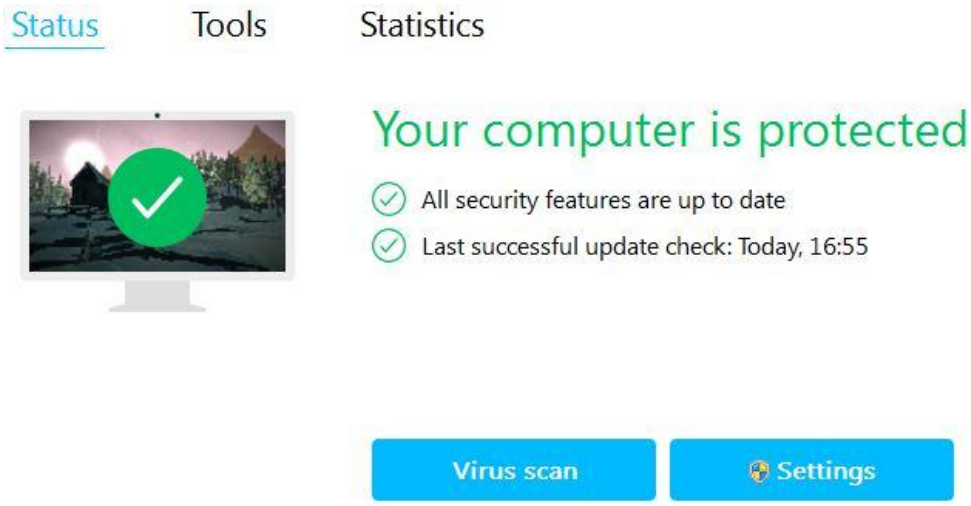
Tietoturvaohjelmisto on jokaisen yrityksen tietokoneiden hyödyllinen suoja. Tämän osuuden tarkoituksena on vertailla kahta virusturvasovellusta. Nämä virustorjuntasovellukset ovat F-Secure Safe sekä Norton Security Premium, jotka nähdään taulukossa 5.

TAULUKKO 5. Virusturvavertailu

Ominaisuus	F-Secure Safe	Norton Security Premium
Hinta	3 Laitetta 59,90€ /vuosi	10 Laitetta 89,95€ / ensimmäinen vuosi
Käyttöliittymä	Yksinkertainen kokonaisuus	Laajempi kokonaisuus
Luotettavuus	Toimi testiajan odotetusti	Toimi testiajan odotetusti
Nopeus	Nopeat tarkistukset Uudet tarkistukset vielä hieman nopeampia.	Ensimmäinen tarkistus hidas, nopeutuvat toistojen yhteydessä.
Asentaminen	Vaatii uudelleen käynnistyksen, poistaa muut virusturva ohjelmat.	Vaatii uudelleen käynnistyksen nopea asennus, poistaa muut viruturvaohjelmat.
Vaatimus	Windows	Windows, Mac , Android.

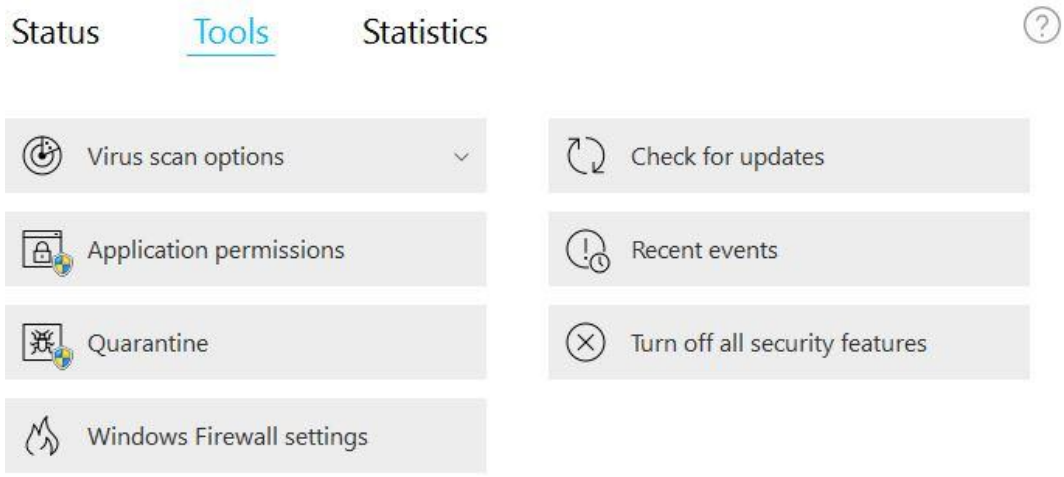
Hintavertailussa F-Securen tuote sopii pienelle laitemäärälle, kun Nortonin vastaava tuote hinnoitellaan suuremmille laitemäärille. Perusnäkymältään sekä F-Secure että Nortonin käyttöliittymä ovat yksinkertaisia, mutta Nortonin vastavaassa on enemmän ominaisuuksia. Ohjelmistot toimivat käyttäjälleen luotettavasti, eikä haittaohjelmia testijaksojen aikana esiintynyt. F-Securen tarkastukset ovat Nortonin tarkastuksiin verrattaessa hieman nopeampia. Asentaminen on nopea sekä yksinkertainen prosessi sekä Nortonin että F-Securen tuotteelle. Asentaminen tarkastaa tietokoneen erilaisilta haittaohjelmilta ja pyytää poistamaan asentamista haittaavat sovellukset. F-securen tuote on tarkoitettu käytettäväksi vain Windows-laitteella. Toisaalta Nortonin vastaava toimii Windowsin, Macin sekä esimerkiksi Android-puhelimissa.

F-Securen uusin tietoturvaohjelmisto F-Secure Safe sisältää helppokäyttöisen tietoturvan ylläpidon verkon tärkeille laitteille. Safe-ohjelmisto on helposti asennettava ohjelmisto, joka sisältää 30 päivän trial-mahdollisuuden. F-Secure Safe:n asentaminen on helppoa ja vaatii ainoastaan rekistöröitymisen sähköpostin avulla. Käytännössä testataan, mitä erilaisia ominaisuuksia F-Secure Safe sisältää. Safe-ohjelmistolla voidaan toteuttaa perinteinen haittaohjelmaskannaus (kuvio 9).



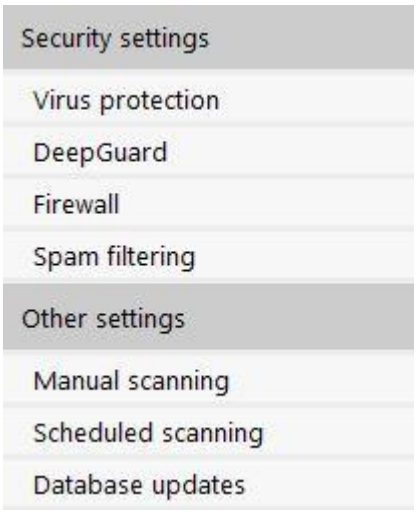
KUVIO 9. F-Secure Safe:n käyttöliittymä

Ohjelmisto sisältää erilaisia työkaluja, joita voidaan käyttää tietoturvatason nostamiseen. Nämä vaihtoehdot löytyy sovelluksen Tools-osiosta (kuvio 10). Tools-osiosta voidaan valita ensimmäiseksi, kuinka haittaohjelma skannaus toteutetaan. Haittaohjelmaskannaus voidaan toteuttaa esimerkiksi kohdistettuna tai tietokoneen kattavana skannauksena. Lisäksi asetuksista voidaan valita luettavaksi edellisen skannauksen raportin, joka sisältää tietoja haittaohjelmatarkistuksesta (Liite 1). Tools-tietokannasta voidaan hallinnoida tietokoneen karanteenista löytyviä haittaohjelmia sekä tutkia sovelluksia, joita ohjelmisto tarkkailee. Lisäksi on mahdollista päivittää ohjelmiston uusimmat päivitykset ja tutkia ohjelmiston tekemiä tapahtumia tietokoneella.



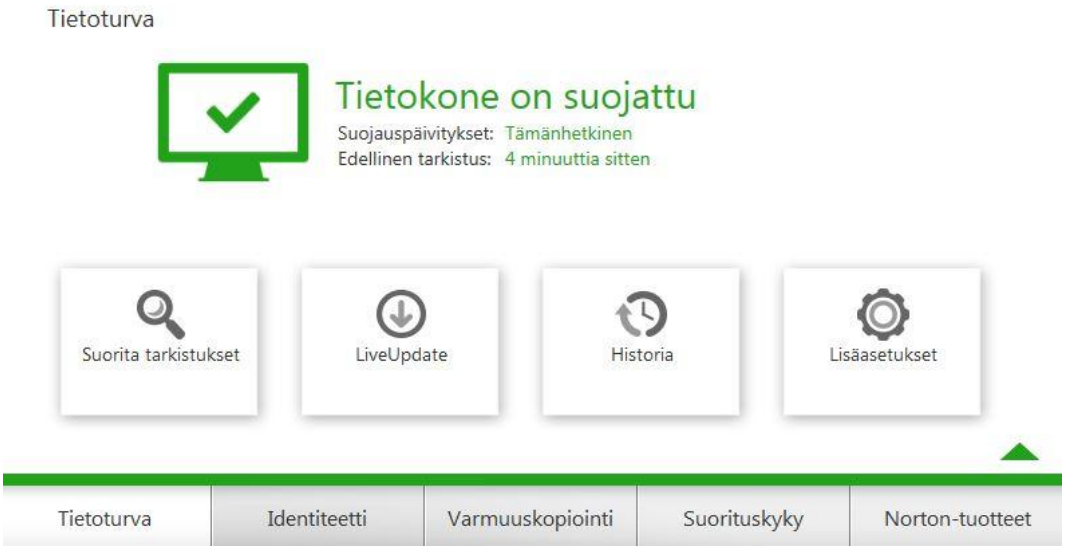
KUVIO 10. Virustorjuntaohjelman asetusvalikko

Työkalujen lisäksi ohjelmistolla on myös perinteisemmät asetukset (kuvio 11). Näitä asetuksia ovat virus-suojauksen asetukset, DeepGuard-asetukset, palomuuriasetukset sekä Spam-filteröinti. Spam filteröintiä voidaan hyödyntää sähköpostiliikenteessä, jossa roskapostiliikenettä halutaan rajoittaa. Lisäksi virustorjuntasovelluksessa on muita asetuksia, joiden avulla voidaan muokata manuaalisesti ohjelmiston skannaus-asetuksia. Näiden ominaisuuksien avulla yksittäisten tietokoneiden suojaaminen onnistuu tehokkaasti.



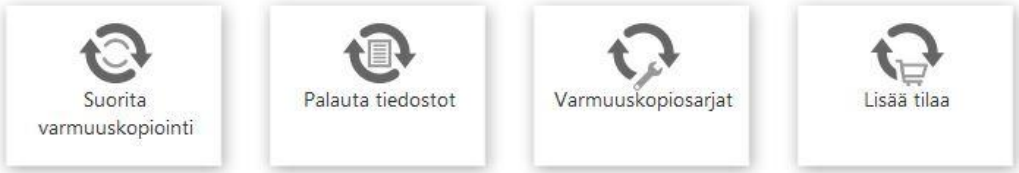
KUVIO 11. Virustorjuntaohjelman erikoisasetukset

Kun vertaillaan FSecure-Safe tuotetta Norton-tietoturvaan, huomataan ensimmäiseksi niiden samankaltaisuus. Nortonin käyttöliittymä näyttää yksinkertaiselta, mutta sisältää samankaltaisia ominaisuuksia kuin Safe-ohjelmisto. Kuviosta 12 nähdään Nortonin käyttöliittymä (kuvio 12).



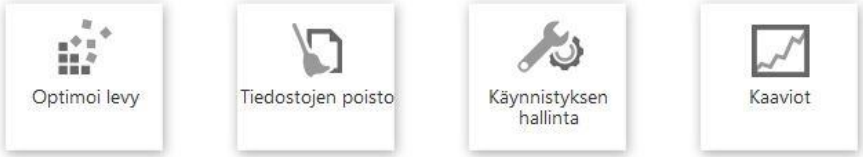
KUVIO 12. Norton-käyttöliittymä

Norton-käyttöliittymästä nähdään ensimmäisenä eroavaisuus, käyttöliittymässä löytyy laajempi tarkistushistoria verrattuna F-Securen vastaavaan. Tarkistuksen toteuttaminen seuraa F-Securen käyttöliittymää ja tarjoaa pikatarkastuksen sekä erilaisia laajempia tarkastuksia. Norton-ohjelmistosta löytyy kiinnostava varmuuskopiointityökalu, jolla erilaiset tärkeät tiedostot voidaan säilyttää turvallisesti (kuvio 13).



KUVIO 13. Nortonin varmuuskopiointi

Varmuuskopiointi näyttää aluksi käytännölliseltä ominaisuudelta, mutta nopeasti voidaan huomata, että varmuuskopiointitila on rajallinen ja tilan lisätilaaminen on maksullista. Nortonin tietoturvassa on olemassa suorituskykyä kohottava toiminto, jonka ominaisuudet on nähtävissä kuviosta 14.



KUVIO 14. Nortonin suorituskyky

Levyn optimoinnissa voidaan kovalevyn rikkoutuneita, sekoittuneita tai hävinneitä tiedonosia palauttaa. Lisäksi on mahdollista hallita tietokoneen tilapäisten tiedostojen määrää sekä selaimen tilapäistiedostoja. Käynnistyksen hallinnassa voidaan hallinoida niitä tietokoneen sovelluksia, joiden käynnistäminen on tietokoneen avaamisen yhteydessä raskasta.

Nortonin ongelmana ovat myös erilaiset hyppyikkunat, jotka saattavat häiritä käyttäjän työskentelyä. Hyppyikkunoita ei ilmene kovin usein, mutta niiden poistaminen on häiritsevää käyttäjäkokemukselle. Kokonaisuutena Norton ei eroa hirveästi F-Securen Safe-tietoturvasta, mutta ohjelmistoissa on erilaisia ominaisuuksia, joten tietoturvasovelluksen valitseminen on tehtävä käyttäjien tarpeita ajatellen ja kokemuksien kautta. Käytettävyyden kannalta valitaan F-Securen Safe-tietoturva. Mutta mikäli tarvitaan varmuuskopiointitilaa ja useampia laitteita, on Norton tähän käytännöllisempi vaihtoehto.

4.5 Asiakirjojen verkkosäilytys

Yrityksen toiminnan pohjana on yleensä erilaisten asiakirjojen liikkuminen sekä säilytys. Verkkosäilytyksestä vertaillaan Box, Google Drive, sekä Windowsin OneDrive-nimisten pilvisäilytyksen toimintaa. Taulukossa 6 esitellään pilvipalveluiden vertailun kokonaiskuva.

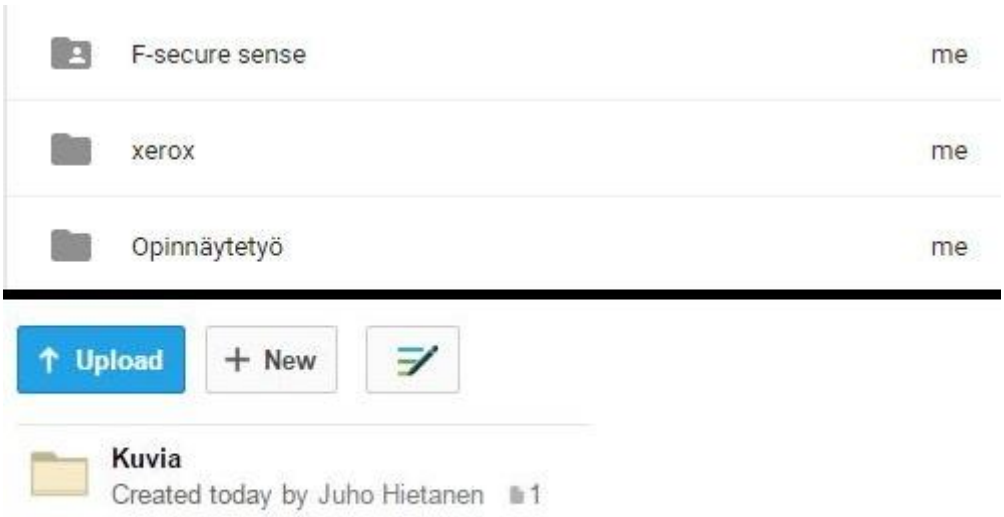
TAULUKKO 6. Säilytyspalveluiden vertailu

Ominaisuus	Box	Google Drive	One Drive
Käyttöönotto	Sähköposti rekisteröinti	Sähköposti rekisteröinti	Sähköposti rekisteröinti
Hinta	Ilmainen, Yrityskäyttöön 15$ / käyttäjä /kk	Ilmainen 10$ /kk/ käyttäjä TB lisää tilaa	Ilmainen Office verkkotuotteet 69 €/ käyttäjä /kk
Tiedostojen luominen	Word, Excel, Powerpoint online.	Google Docs	Office palvelut
Tiedostojen jakaminen	Muiden palvelun käyttäjien kanssa	Muiden palvelun käyttäjien kanssa	Muiden palvelun käyttäjien kanssa
Tiedostojen muokkaaminen	Erillisen ohjelman avulla	Doc tiedostojen muokkaaminen	Yhdistetty office palveluiden kanssa

Kuten taulukosta 6 nähdään, kaikissa säilytyspalveluissa rekisteröinti tapahtuu sähköpostin avulla. Erot palveluille ilmenevät palvelun hinnaston perusteella. Jokaiselle säilytypalvelulle on olemassa ilmainen kokeiluversio, joka sisältää pienen käyttötilan tiedostojen säilytykseen. Mikäli käyttäjä tai yritys haluaa verkkotilan kasvattamisen, sovelluksesta maksetaan kuukausihintaa yhtä käyttäjää kohden. Vertailun hintavoittajaksi nousee Google Drive, jonka kuukausihinta sekä tilan määrä on muita huomattavasti suurempi.

Tiedostojen luominen palveluissa eroaa toisistaan ohjelmiston tarjoaman kirjoituspalvelun muodossa. Box-palvelussa on mahdollista käyttää Officen onlinepalveluita tiedostojen tuottamiseen. Googlella vastaavasti voidaan luoda vain Google Docs-pohjaisia tiedostoja, mutta Office-tiedostoja voidaan kuitenkin säilyttää palvelussa. One Drive on Microsoftin itsenäinen verkkosäilytyspalvelu, joten One Driven avulla voidaan käyttää Office palveluita. Office-palvelut ovat maksuttomassa versiossa onlinekäytössä, mutta viralliset Office-tuotteet voidaan ostaa lisämaksusta. Koska palvelut ovat toisilleen kilpailevia, on tiedostojen jakaminen tehtävä palveluiden sisällä tai väliaikaisia siirtoteitä pitkin. Tiedostojen muokkaaminen on Box-sovelluksen ulkopuolinen palvelu, jonka käyttämiseen tarvitaan erillinen ohjelma. Google Drive-palvelussa on mahdollista doc-muotoisten tiedostojen muokkaaminen, mutta esimerkiksi virallisia Word-tiedostoja on mahdollista vain lukea palvelussa. Palvelussa voi kuitenkin muokata doc tiedostoja samanaikaisesti, jolloin esimerkiksi ryhmätyöskentelystä tulee monipuolista. One Drive-palvelussa voidaan muokata Office-tiedostoja, mikä tekee palvelusta Google Driveä ja Box-palveluita paremman. Mikäli tiedostoja halutaan muokata samanaikaisesti, on Google Drive käytännöllisempi vaihtoehto.

Palveluiden käyttöliittymää tarkasteltaessa on todettava esimerkiksi kuviossa 14 nähtävät Google Driven sekä Box-sovelluksen käyttöliittymät ovat näkymältään samankaltaisia.



KUVIO 14. Google Drive- ja Box-käyttöliittymä

Sovellusten toiminnan edistämiseksi sovelluksissa on aktiivinen drag and drop-toiminto, jolla voidaan siirtää tiedostoja työpöydältä säilytettäväksi pilvisäilytykseen. Verkkosäilytystä rakentaessa kannattaa tiedostoiden lajittelu toteuttaa seuraavia tapoja huomioiden. Pilvisäilytys-sovelluksesta huomioimatta rakennettavat kansiot kannattaa nimetä kuvaavalla nimellä sekä eritellä erilaisten aihepiirien tiedostot omiin kansioihinsa. Kansioiden luominen tehdään yleisesti painikkeesta New ja valitaan listasta folder. Tästä esimerkkinä seuraava kuvio kansiopohjasta (kuvio 15).

KUVIO 15. Kansiopohjat pilvipalvelussa.

4.6 Tietoturvan kokonaissuunnitelma

Kehitysuunnitelman tarkoituksena on kertoa yritykselle vaiheittainkuinka yrityksen tietoturvaa sekä turvallisuutta kehitetään. Suunnitelma on seuraavan taulukon 7 mukainen.

TAULUKKO 7. Kokonaissuunnitelma

Suunnitelma	Tarve	Ratkaisu
VAIHE 1	Tietoturvan osa-alueiden toteutuminen.	Tarkistetaan tietoturvan osa-alueiden laatu.
VAIHE 2	Turvataan verkon liikenne.	Toteutetaan verkonvalvonta sekä palomuuri suodattaminen.
VAIHE 3	Langattomien verkkojen suojausmenetelmät	Määritellään suojausmenetelmät.
VAIHE 4	Käyttöjärjestelmät	Päivitetään vanhentuneet käyttöjärjestelmät turvallisempaan.

(jatkuu)

TAULUKKO 7. (jatkuu)

VAIHE 5	Työntekijöiden työskentely	Turvataan työntekijöiden työskentely kehittyneellä virusturvalla.
VAIHE 6	Kouluttaminen	Koulutetaan työntekijöitä tarpeellisissa asioissa.
VAIHE 7	Dokumentointi	Dokumentoidaan verkkototeutus sekä tehdyt muutokset.
VAIHE 8	Tulevaisuus	Varaudutaan tulevaisuuden muutoksiin ja kehitetään järjestelmää.

Taulukosta 7 nähdään kokonaissuunitelman muototuvan kahdeksaan erilaiseen vaiheeseen.

VAIHE 1.

Tarkistetaan tietoturvan osa-alueiden toteutuminen yrityksessä. Vaiheella tarkoitetaan sitä, että todetaan yrityksen tietoturvan toteutuminen työssä aikaisemmin käsitellyn tietoturvallisuusosuuden sisällön avulla. Tietoturvallisuuden osa-alueet ovat tärkeitä tukipilareita tietoturvan toteutumiseksi, joten niiden toiminnan tulee olla kunnossa. Osa-alueiden toiminnan taso kartoitetaan tutkimalla, miten erilaiset yrityksen tavat auttavat tai heikentävät yrityksen tietoturvaa.

VAIHE 2.

Pyritään muodostamaan yrityksen verkolle verkonvalvonta sekä palomuurin suodattaminen. Verkonvalvonnan toteuttaminen edesauttaa verkon toimivuusongelmien ratkaisemisessa sekä edesauttaa vikasietoisen yritysverkon ylläpitämisessä. Palomuurin avulla voidaan turvata yrityksen tietoliikenne tarpeettomalta ja turvattomalta liikenteeltä.

VAIHE 3.

Todetaan langattomien verkkojen suojausmenetelmien toiminta. Tarkastellaan, että verkon tukiasemat ovat vahvojen salasanojen takana ja käyttävät tuoreimpia kryptausmenetelmiä, jotta langattomien verkkojen käyttäjät ovat tietoturvallisuuden ytimessä.

VAIHE 4.

Tutkitaan yrityksen pöytäkoneiden sekä kannettavien tietokoneiden käyttöjärjestelmien päivittäminen. Pyritään vähentämään vanhoja käyttöjärjestelmiä, kuten Windows XP-koneita. Varmistetaan vanhojen laitteiden sovellusten toiminta, jotta ne toimivat myös uudemmilla järjestelmillä.

VAIHE 5.

Tarkistetaan pöytäkoneiden sekä kannettavien tietokoneiden virusturvan toiminta. Mikäli virusturvaohjelmisto on vanhentunut tai halutaan vaihtaa sovellus kokonaisuutena uuteen, voidaan harkita työssä käytettyjä F-Secure Safe-tai Nortonin tietoturvasovelluksen käyttöönottoa. Tietoturvasovelluksen vaihtaminen voidaan toteuttaa yksittäisille koneille tai koko yrityksen järjestelmille.

VAIHE 6.

Koulutetaan työntekijöitä asiakirjojen suojaamisessa sekä säilyttämisessä. Todennetaan tietokonetta käyttävien työntekijöiden osaaminen asiakirjojen ja säilytettävän materiaalin kanssa. Pyritään säilyttämään tärkeät asiakirjat useassa paikassa, jotta asiakirjojen häviämiseltä vältyttään. Työssä on esitelty vaihtoehtoja pilvipalvelusäilytykselle.

VAIHE 7.

Mikäli verkossa sekä muissa käytännöissä tehdään erilaisia muutoksia, niitä tulee dokumentoida tai päivittää kattavasti. Kun dokumentit ovat ajantasaisesti päivitettyjä, on dokumentteja yksinkertaisempi ylläpitää. Dokumenttien avulla voidaan työntekijöitä kouluttaa verkon toiminnan ylläpitämiseen sekä turvalliseen käyttämiseen.

VAIHE 8.

Verkon ylläpitäminen muutosten jälkeen on tärkeää tulevaisuuden kannalta. Hyvin ylläpidetyssä verkossa tulevaisuuden muutokset on helpommin muutettavissa sekä mahdollisesti päivitettävissä uusien innovaatioiden myötä.

Verkon ylläpitäminen on verkon käyttöä ja turvaamista helpottava toimenpide. Taulukossa 8 ratkaistaan verkon ylläpidon elementtejä.

TAULUKKO 8. Verkon ylläpitäminen

Tehtävä	Ratkaisu
Tietoliikenteen vastuuhenkilöt sekä vastuualueet	Vastuuhenkilöiden nimittäminen ja vastuualueiden määrittely
Tietoliikenneverkon dokumentointi ja ylläpitäminen	Dokumentointi ylläpidon valitseminen
Verkossa liikkuvan informaation suojaaminen	Verkonvalvonta, palomuuri ja virusturva otetaan käyttöön
Ylläpitäjien ja käyttäjien ohjeistaminen sekä koulutus	Koulutetaan ylläpitäjät, jotka kouluttavat verkon käyttäjät
Huolto- ja ylläpitosopimukset ulkoisten toimijoiden kanssa	Määritellään päivitetyt sopimukset ulkoisten toimijoiden kanssa

Ratkaistaan tietoliikenteen vastuuhenkilöt ja vastuualueet siten, että nimetään yrityksestä asiantuntevat henkilöt näihin työtehtäviin sekä määritellään vastuualueet henkilöiden vahvuuksiin perustuen. Verkon dokumentointi ja ylläpito järjestetään vastuuhenkilöiden työnkuvan yhteyteen verkon asiantuntijuuden avulla. Dokumentointia päivitetään muutosten sekä väliaikatarkastusten yhteydessä. Verkossa liikkuvan informaation suojaaminen toteutetaan verkonvalvonnan, palomuurin ja virustorjunnan avulla.

Ylläpitäjien ja käyttäjien kouluttaminen ratkaistaan uusien verkkotoimintojen käyttöönottamisen yhteydessä perehdytykenä, jolloin perehdytetty ylläpito voi jakaa koulutustaan edelleen palveluiden käyttäjille. Ylläpitosopimukset neuvotellaan uudelleen vastaamaan yrityksen päivitettyä verkkototeutusta.

Kokonaissuunnitelman jatkuessa avataan ratkaisut suojakäytännöille taulukossa 9.

TAULUKKO 9. Suojakäytännöt

Tehtävä	Tarve	Ratkaisu
Kaapeloinnin suojaus	Kaapelit ovat suojassa fyysisiltä uhilta, kuten katkaisulta ja vaurioitumiselta.	Kaapelointi väliseinässä tai seinää myötäillen.
Aktiivilaitteiden suojaus	Aktiivilaitteet ovat turvalliseessa paikassa ja niiden asetukset ovat suojattu.	Eristetään laitteet erillisiin tiloihin tai kaappeihin. Suojataan laitteet salasanalla.
Ulkoisten yhteyksien Turvaaminen	Verkkoyhteydet ovat vikasietoisia esimerkiksi palomuurin ja virustorjunnan avulla.	Palomuurin sekä virusturvan toteuttaminen.
Varajärjestelyt	Tietoliikenne yhteyksille on olemassa korvaavia laitteita ja varaosia.	Pidetään varastossa varalaitteita sekä varaosia.
Etäkäyttöyhteydet	Mahdolliset etäkäyttöyhteydet on suojattu esimerkiksi salasanalla.	Toteutetaan käyttäjätunnistautumine n tai salasanasuojaus verkoille.
Verkkosegmentit	Erilaiset tietoverkot ovat eristetty toisistaan.	Muodostetaan verkot leipomolle ja toimistolle.

Kaapeloinnin suojaaminen on kaapelointirakentamisen yhteydessä toteutettu asentamalla kaapelointi rakennuksen väliseinien tai välikaton sisään. Suojaamista voidaan sisätiloissa korostaa vetämällä tulevat sisäseinien ulkoiset kaapelit seinänmyöteisesti sekä riittävällä mittauksella. Mahdolliset rakennuksen ulkoiset kaapeloinnit on turvallisessa ympäristössä rakennettu säältäsuojattuun kaapelointiin ja sääolosuhteet huomioiden.

Aktiivilaitteiden suojaaminen eli erilaisten verkkolaitteiden suojaus ratkaistaan huomioiden leipomotilojen jauhopölypitoisuudet. Leipomotiloissa laitteet säilytetään, mikäli mahdollista, erillisissä tiloissa tai vaihtoehtoisesti eristetyissä kaapeissa. Eristämisessä pitää kuitenkin huomioida verkkolaitteen mahdolliset ominaisuudet esimerkiksi langattoman signaalin lähetyksessä, jolloin eristämistä ei suositella signaalin heikkenemisen vuoksi. Aktiivilaitteiden asetusten suojaaminen toteutetaan laitteissa salasanasuojauksen avulla. Ulkoisten yhteyksien turvaaminen ratkaistaan verkon suodattamisen avulla palomuurisovelluksen sekä ehkäisevän virustorjunnan yhteistyönä.

Varajärjestelyjen ratkaiseminen toteutetaan hankkimalla laitteille varalaitteet siten, että varalaitteiden asetukset on asetettu valmiiksi korvaamaan mahdollisesti vikautuvien laitteiden tehtävät yrityksen verkossa. Varaosilla tarkoitetaan erilaisten kaapeleiden sekä vastakappaleiden varastoa esimerkiksi kaapeleiden tai osien vikaantumisen tapahtuessa. Vikajärjestelyjen avulla ehkäistään tuotannon häiriintymistä, jolloin ehkäistään myös tappiollisen tuotannon toteuttamista.

Mikäli verkkojärjestelmää on laajennettu käytettäväksi etäyhteyden välityksellä, on tärkeää, että kyseinen verkko on suojattu. Suojaaminen järjestetään esimerkiksi käyttäjätunnistautumisen ja salasanan avulla riippuen etäkäyttäjien määrästä verkossa. Verkkosegmentointi kannattaa liittää käyttäjätunnistautumiseen huomioiden käyttäjien tarpeet verkossa. Käyttäjille annetaan valtuuksia verkkoihin, mikäli verkko on tarpeellinen käyttäjän työhön. Kokonaisuutena verkko segmentointia kehotetaan jakamaan työalueen perusteella. Esimerkiksi voidaan erotella leipomon alue omaksi verkkokokonaisuudeksi ja toisaalta pitää toimistotilat erillisessä verkossa. Laajennetussa verkkosegmentoinnissa voidaan yrityksen toimipisteet jaoitella omiin verkko-osuuksiin, jolloin ylläpidon on yksinkertaisempaa hallita kokonaisuutta.

5 YHTEENVETO

Opinnäytetyön tavoitteena oli muodostaa Sinuhe Ky-yritykselle tietoturvan kehittämissuunnitelma, jossa käsitellään yritykselle tärkeitä tietoturvan osa-alueita. Tavoitteeseen pääsemiseksi opinnäytetyössä selvitettiin tietoturvan sisältö. Tietoturvan sisältö muodostui palomuurista, verkonvalvonnasta, käyttöjärjestelmistä, virustorjunnasta ja pilvipalveluista.

Opinnäytetyössä vertailtiin erilaisia ohjelmistoja, palveluita ja sovelluksia. Vertailun toteutuksesta päädyttiin seuraaviin tuloksiin. Sophos- sekä PFSense-palomuuriohjelmistojen vertailussa päädyttiin PFSensen valintaan taloudellisuuden sekä vaatimusten vuoksi. Verkonvalvontasovellusten Zabbix- sekä Solarwinds vertailussa päädyttiin Zabbix:iin, koska Zabbix oli käytännöllisempi vaihtoehto Sinuhe Ky-yrityksen toimintaa ajatellen. Virustorjuntasovelluksen valinnassa vertailtiin F-Secure Safe ja Norton Security premium virustorjuntasovelluksia. F-Secure Safe oli vertailussa käytännöllisempi vaihtoehto nopeutensa ja helppokäyttöisyytensä takia pilvipalveluiden verkkosäilytysvertailussa vertailtiin kolmea sovellusta. Nämä sovellukset olivat Box, Google Drive ja One Drive. One Drive-sovelluksen valintaan päädyttiin Office-yhteensopivuus huomioiden.

Työtä ja kehitystyötä olisi mahdollista kehittää eteenpäin käytännön järjestelyillä sekä testamaalla opinnäytetyön aiheita käytännössä leipomon virallisessa verkkoliikenteessä ja toiminnassa. Tulevaisuuden kehittelyssä voitaisiin myös toteuttaa erilaista vikasietoisuuden toteuttamista fyysisen varajärjestelmän muodossa. Kokonaisuutena opinnäytetyö pääsi tavoitteeseensa analyyttisenä työnä kartoittaessaan tietoturvan kokonaisuutta ja toteutti erilaisia vaihtoehtoja tietoturvan kehittämisessä ja tulkitsemisessa.

LÄHTEET

Beal. 2007a. The Differences Between WEP and WPA [viitattu 4.3.2016]. Webopedia. Saatavissa: http://www.webopedia.com/DidYouKnow/Computer_Science/WEP_WPA_wireless_security.asp

Beal. 2007b. WPA- Wi-Fi Protected Access [viitattu 4.3.2016]. Webopedia. Saatavissa: http://www.webopedia.com/TERM/W/WPA.html

Beaver. 2016. The 10 most common Windows security vulnerabilities. [viitattu 4.3.2016]. TechTarget. Saatavissa http://searchenterprisedesktop.techtarget.com/tip/The-10-most-common-Windows-security-vulnerabilities

Bradley. 2016. Pros and Cons of Windows 7 Security [viitattu 4.3.2016]. Pcworld. Saatavissa: http://www.pcworld.com/article/182917/pros_cons_windows_7_security.html?page=2

Bullguard. 2016. Malware - definition, history and classification [viitattu 10.3.2016]. Bullguard.com. Saatavissa: http://www.bullguard.com/bullguard-security-center/pc-security/computer-threats/malware-definition,-history-and-classification.aspx

Casserly. 2016. Should I upgrade to Windows 10? Is Windows 10 better than Windows 7 or 8.1? The pros and cons of upgrading [viitattu 4.3.2016]. Pc Advisor. Saatavissa: http://www.pcadvisor.co.uk/feature/windows/should-i-upgrade-windows-10-advice-win7-win8-chrome-3618139/

Cisco. 2016. What Is the Difference: Viruses, Worms, Trojans, and Bots?. [viitattu 4.3.2016]. Cisco Systems, Inc. Saatavissa: http://www.cisco.com/c/en/us/about/security-center/virus-differences.html

Cluley. 2012. Disable Windows Sidebar and Gadgets [viitattu 4.3.2016]. Naked security. Saatavissa: https://nakedsecurity.sophos.com/2012/07/12/disable-windows-sidebar-gadgets/

CVE Details. 2016a. Security Vulnerabilities [viitattu 4.3.2016] CVE Details Saatavissa: https://www.cvedetails.com/cve/CVE-2010-4562

CVE Details. 2016b. Security Vulnerabilities [viitattu 4.3.2016]. CVE Details. Saatavissa: https://www.cvedetails.com/vulnerability-list/vendor_id-26/product_id-17153/hasexp-1/Microsoft-Windows-7.html

ETutorials. 2016. Encryption Protocols [viitattu 4.3.2016]. eTutorials.org. Saatavissa: http://etutorials.org/Networking/Wireless+lan+security/Chapter+8.+WLAN+Encryption+and+Data+Integrity+Protocols/Encryption+Protocols/

Finlex. 2004. Laki yksityisyyden suojasta työelämässä [viitattu 5.3.2016]. Lainsäädäntö. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/2004/20040759.

Forrest. 2015. Windows 10 violates your privacy by default, here's how you can protect yourself. [viitattu 4.3.2016]. TechRepublic. Saatavissa: http://www.techrepublic.com/article/windows-10-violates-your-privacy-by-default-heres-how-you-can-protect-yourself/.

Google Drive. 2016. Tutustu Driven tallennusominaisuuksiin [viitattu 5.3.2016]. Google. Saatavissa: https://www.google.com/intl/fi/drive/using-drive/.

Held.M. 2014. If You're Still Using Windows XP Your Company Is at Risk. [viitattu 4.3.2016]. Huffington post. Saatavissa: http://www.huffingtonpost.ca/matthew-held/windows-xp-no-support_b_5481600.html

Hiner.J. 2008. The top five reasons why Windows Vista failed? [viitattu 4.3.2016]. Zdnet.com Saatavissa: http://www.zdnet.com/article/the-top-five-reasons-why-windows-vista-failed/

Hoffman.C. 2014. What is the Difference Between TCP and UDP? [viitattu 5.3.2016]. How-To Geek. Saatavissa: http://www.howtogeek.com/190014/htg-explains-what-is-the-difference-between-tcp-and-udp/

Koivunen.E. 2010. Vahti-ohje: Verkon aktiivilaitteet [viitattu 5.3.2016]. Valtiovarainministeriö. Saatavissa: https://www.vahtiohje.fi/web/guest/verkon-aktiivilaitteet

Microsoft. 2015. The Wi-Fi Protected Access 2 [viitattu 4.3.2016]. Microsoft Support. Saatavissa: https://support.microsoft.com/en-us/kb/893357

Microsoft. 2016. Asiakirjojen, työkirjojen ja esitysten suojaaminen salasanalla [viitattu 5.3.2016]. Microsoft Support. Saatavissa: https://support.office.com/fi-fi/article/Asiakirjojen-ty%C3%B6kirjojen-ja-esitysten-suojaaminen-salasanalla-ef163677-3195-40ba-885a-d50fa2bb6b68

Newton.G. 2015 Wireless LANs [viitattu 5.3.2016] Electronic and Computer Information. Saatavissa: http://electroniccomputerinformation.blogspot.fi/2015/09/wireless-lans.html

Pheneah. 2012. 5 security issues to watch in Win 8 [viitattu 4.3.2016]. ZDnet. Saatavissa: http://www.zdnet.com/article/5-security-issues-to-watch-in-win-8/

Pietikäinen. 2013. Vahtiohje: Tietoturvallisuus – mitä se on? [viitattu 4.3.2016]. Valtiovarainministeriö. Saatavissa: https://www.vahtiohje.fi/web/guest/691

Prokaza. 2015. Is it still safe to use Windows XP? Security tips for Microsoft’s most popular OS [viitattu 4.3.2016]. BT. Saatavilla:

http://home.bt.com/tech-gadgets/computing/is-it-still-safe-to-use-windows-xp-security-tips-for-microsofts-most-popular-os-11363958273351

Smith. 2011. Understanding The Common WiFi Standards [viitattu 4.3.2016]. Makeuseof.com. Saatavissa: http://www.makeuseof.com/tag/understanding-common-wifi-standards-technology-explained/

Tietojesiturvaksi. 2016b. Hallinnollinen tietoturva [viitattu 4.3.2016]. Tietojesiturvaksi.fi. Saatavissa: http://tietojesiturvaksi.fi/tietoturvasuunnitelma/hallinnollinen-tietoturva

Tietojesiturvaksi. 2016a. Fyysinen tietoturva [viitattu 4.3.2016]. Tietojesiturvaksi.fi. Saatavissa: http://tietojesiturvaksi.fi/tietoturvasuunnitelma/fyysinen-tietoturva

Tietojesiturvaksi. 2016c. Henkilöstöturvallisuus [viitattu 4.3.2016]. Tietojesiturvaksi.fi. Saatavissa: http://tietojesiturvaksi.fi/tietoturvasuunnitelma/henkilostoturvallisuus

Tietojesiturvaksi. 2016d. Käyttöturvallisuus [viitattu 4.3.2016]. Tietojesiturvaksi.fi. Saatavissa: http://tietojesiturvaksi.fi/tietoturvasuunnitelma/kayttoturvallisuus

Tietojesiturvaksi. 2016j. Tietoliikenneturvallisuus [viitattu 4.3.2016]. Tietojesiturvaksi.fi. Saatavissa: http://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoliikenneturvallisuus.

Tietojesiturvaksi. 2016e. Laitteistoturvallisuus [viitattu 4.3.2016]. Tietojesiturvaksi.fi. Saatavissa: http://tietojesiturvaksi.fi/tietoturvasuunnitelma/laitteistoturvallisuus.

Tietojesiturvaksi. 2016f. Tietoaineiston turvallisuus [viitattu 4.3.2016]. Tietojesiturvaksi.fi. Saatavissa: http://tietojesiturvaksi.fi/tietoturvasuunnitelma/tietoaineiston-turvallisuus

Vahti-Ylläpito. 2016. Vahtiohje:Tietoliikenneturvallisuus [viitattu 5.3.2016]. Valtiovarainministeriö. Saatavissa: https://www.vahtiohje.fi/web/guest/tietoliikenneturvallisuus

Viestintävirasto. 2016a. Langattomasti, mutta turvallisesti [viitattu 4.3.2016]. Kyberturvallisuuskeskus. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Langattomasti_mutta_turvallisesti._Langattomien_lahiverkkojen_tietoturvallisuudesta.pdf

Viestintävirasto. 2016c. Pilvipalveluiden turvallisuus [viitattu 5.3.2016] Kyberturvallisuuskeskus. Saatavissa: https://www.viestintavirasto.fi/attachments/tietoturva/Pilvipalveluiden_tietoturva_organisaatioille.pdf

Viestintävirasto. 2016b. Luottamuksellisen viestinnän suojaaminen [viitattu 5.3.2016]. Kyberturvallisuus. Saatavissa: https://www.viestintavirasto.fi/viestintavirasto/ajankohtaista/2013/luottamuksellisenviestinnansuojaaminen.html

Viljanen. 2016v. Virusturva ja palomuuri [viitattu 4.3.2016]. Yksityisyydensuoja. Saatavissa: https://www.yksityisyydensuoja.fi/virusturva-ja-palomuuri

Viljanen. 2016a. Lainsäädäntö [viitattu 5.3.2016]. Yksityisyydensuoja. Saatavissa: https://www.yksityisyydensuoja.fi/lainsaadanto

Viljanen 2016b. Turvallinen tiedonhävitys [viitattu 5.3.2016]. Yksityisyydensuoja. Saatavissa: https://www.yksityisyydensuoja.fi/content/turvallinen-tiedonh%C3%A4vitys

VirtuaaliAMK. 2016. Palomuuri [viitattu 5.3.2016]. Virtuaali Ammattikorkeakoulu. Saatavissa: http://www2.amk.fi/mater/tietotekniikka/palomuuri/files/Palomuuri.htm

Zabbix. 2016. Problem Detection [viitattu 5.3.2016]. Zabbix. Saatavissa: http://www.zabbix.com/problem_detection.php

Wikipedia. 2016. SSL Certificate Info Box In Firefox [viitattu 10.3.2016]. The Free Encylopedia. Saatavissa: https://en.wikipedia.org/wiki/File:SSL_Certificate_Info_Box_In_Firefox.png

Windows7. 2016. Tiedostojen varmuuskopioiminen [viitattu 5.3.2016]. Microsoft. Saatavissa: http://windows.microsoft.com/fi-fi/windows/back-up-files#1TC=windows-7

Wireless LANs [viitattu 10.3.2016]. Electronic and Computer Information. Saatavissa: http://electroniccomputerinformation.blogspot.fi/2015/09/wireless-lans.html

LIITTEET

Liite 1. Haittaohjelmaraportti

SCANNING REPORT

22. helmikuuta 2016 10:22:31 - 10:26:36

Scan type: Virus and spyware scan

Results

Items scanned: 6816
No harmful items found

Details

No harmful items found

Version information

Virus definition database:

- 2016-02-22_04

Scanning engines:

- F-Secure Aquarius: 11.00.01, 2016-02-22
- F-Secure Gemini: 3.02.328, 2016-02-19
- F-Secure Hydra: 5.15.21, 2016-02-22
- F-Secure Online: 15.10.229
- F-Secure USS: 5.08.131, 2016-01-27

Liite 2. Windows 7 asennusohje

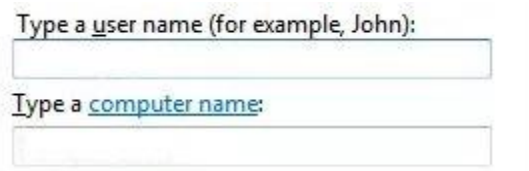
Windows 7 käyttöjärjestelmä asennetaan yleensä USB tai DVD:llä olevasta asennuspaketista. Windows käyttöjärjestelmät ovat joko 32 bit tai 64 bittisiä. Ennen käyttöjärjestelmän asennusta on tietojesi turvaksi tärkeää siirtää tärkeät tiedostot sekä sovellukset toiseen säilytyspaikkaan.

1. DVD:llä asentaminen aloitetaan käynnistämällä tietokone uudelleen ja valitsemalla bootdevice painamalla F12-näppäintä.
2. Kun bootdevice on valittu, windows asennuskuvake aukeaa ja aloittaa asentamiseen tarkoitettujen tiedostojen lataamisen DVD:ltä (Kuvio 16).

KUVIO 16. Windows asennusikkuna

3. Seuraavassa kuvassa näemmä windows käyttöjärjestelmistä tutun kuvakkeen, jossa lukee ”Starting Windows”.
4. Seuraavassa kuvassa aloitetaan ensimmäisten asetusten antaminen asennusta varten. Valitaan haluttu käyttöjärjestelmän kieli, aikavyöhyke sekä näppäimistön kieliasetukset. Valittuasi asetukset, paina next.
5. Seuraavassa ikkunassa tulee esille ikkuna, jossa lukee ”Install now”. Painamalla tästä painikkeesta virallinen asennus aloitetaan.
6. Seuraavassa kuvakkeessa windows pyytää lukemaan license agreement tiedot. Painetaan ”I accept the license terms” ja jatketaan seuraavalle sivulle, painamalla next.
7. Seuraavaksi valitaan ”Custom Advanced” mikäli halutaan tyhjä asennus. Painettuasi painiketta päädyt seuraavaan näkymään.

8. Seuraavassa näkymässä valitaan kovalevy, jolle windows 7 asennus suoritetaan. Lisäksi tässä näkymässä painetaan ”Load Driver”, mikäli tietokoneessa on käytössä ACPI/RAID/SATA-kovalevyjä. Kun mahdolliset driverit on ladattu, painetaan next.
9. Seuraavaksi Windows 7 käyttöjärjestelmän automaattinen asentuminen alkaa. Asentaminen vie tietokoneesta riippuen 10 minuutista 60 minuuttia aikaa, jolloin tietokone käynnistää itseään uudelleen sekä asentaa käyttöjärjestelmää.
10. Kun asentuminen on edennyt seuraavaan vaiheeseen, avautuu käyttäjä valikko, jossa määritellään käyttäjän nimi sekä tietokoneen nimi (Kuvio17). Seuraavaan näkymään päästään, painamalla next.



KUVIO 17. Käyttäjän määritteleminen.

11. Seuraavaksi määritellään juuri luodulle käyttäjälle salasana. Salasanan tulisi olla mahdollisimman monimutkainen, mutta sellainen, mikä on käyttäjän muistettavissa. Kirjoitetaan salasana kahdesti ja lisätään salasanalle vinkki, mikäli salasanan unohtaminen tapahtuu. Seuraavaksi paina next.
12. Seuraavassa näkymässä kirjoitetaan Windowsin ”product key” ja painetaan next.
13. Seuraavassa näkymässä valitaan ”Use recomended settings”, jotta Windows 7 tekee automaattisesti erilaiset päivitysten haut ja asennukset. Näitä asetuksia on mahdollista muokata myös jälkikäteen.
14. Painettuasi recomended settings painiketta, avautuu aikavyöhykkeen sekä päivämäärän asettamisen ikkuna. Valitaan oikea aikavyöhyke sekä päivämäärä. tarkistetaan myös, että kello on oikea. Seuraavaksi painetaan next.

15. Seuraavassa ikkunassa valitaan ”Network profile”. Tässä kuvakkeessa valitaan yrityksessä sijaitseva profiili eli ”Work network”.
16. Seuraavassa kuvassa Windows 7 pyrkii asentamaan verkkoyhteyden uudelle käyttöjärjestelmälle ja antamaan tietokoneelle ip-osoitteen. Verkkoyhteyden muodostettua painetaan next.
17. Seuraavaksi Windows 7 viimeistelee asennuksen ja asennus on valmis.

Liite 3. Windows 10 asennusohje

Windows 10 asentamiselle on kaksi mahdollisuutta. Ensimmäinen mahdollisuus asentamiseen on päivittää ilmainen päivitys Windows 7 sekä Windows 8.1 versioiden päälle. Käyttöjärjestelmän päivittäminen ilmainen päivittäminen on mahdollista vuoden 2016 heinäkuun loppuun menessä. Toinen mahdollisuus on ladata asennustiedosto USB, DVD tai ISO-tiedostona. Asennus voidaan suorittaa joko päivityksenä tai puhtaana asennuksena. Asentaminen aloitetaan Windows käyttöjärjestelmän päälle päivittämällä kaikki Windowsin kehottamat päivitykset Windows updaten avulla (Kuvio18).

KUVIO 18. Päivitys Windows 10.

1. Kun asennusmedia aloittaa toimintansa, valitaan esimmäisestä kuvasta kieli, millä asentaminen toteutetaan. Lisäksi ensimmäisellä sivulla valitaan aikavyöhyke sekä näppäimistön kieli.
2. Seuraavalla sivulla painetaan painike Install now.
3. Seuraavaksi asennus kysyy halutaanko kyseinen tietokone päivittää vai asentaa Windows 10 tyhjälle alustalle. Mikäli tietokoneellasi on säilytettäviä tiedostoja valitse Upgrade ja tämän lisäksi siirrä tärkeimmät tiedostosi varmuudenvuoksi myös toiselle säilytysalustalle esimerkiksi USB-muisti tai pilvipalvelu.

4. Seuraavalla asennussivulla valitaan kiintolevy, jonne asennettu Windows 10 asentuu. Asennuksen tässävaiheessa huomioidaan myös, että asennettavalla kiintölevyllä on riittävästi tyhjää tilaa eli 20GB tai enemmän.
5. Seuraavaksi painetaan next ja asennusaloitetaan.
6. Perusasennuksen jälkeen tietokone käynnistää itsensä uudelleen.
7. Seuraavassa kuvassa voidaan muokata erilaisia käyttöjärjestelmän asetuklsia painamalla Customize tai valitsemalla Use expresss settings, mikä tarkoittaa oletusasetusten käyttöä.
8. Seuraavaksi Windows pyytää käyttäjää kirjautumaan Microsoft käyttäjällä, jotta Windows voi ottaa Windows 10 käyttöjärjestelmän mukana tulevat palvelut käyttöönsä. Tämä ei ole pakollista, mutta vähentää käyttöjärjestelmän palveluidenmäärää, mikäli et tätä kirjautumista toteuta. Seuraavaksi painetaan next.
9. Seuraavaksi käyttöjärjestelmä kysyy käytetäänkö käyttöjärjestelmän kovalevyltä löytyviä tiedostoja. Toinen vaihtoehto on kovalevyntyhjentäminen, jolloin tiedostot häviävät ja aloita puhtaalta pöydältä. Seuraavaksi sivulla painetaan next.
10. Viimeiseksi käyttöjärjestelmä kysyy haluaako käyttäjä käyttää OneDrive pilvipalvelua.
11. Asennuspäättyy, kun olet päässyt takaisin työpöydälle.