Timo Mäklin

Keskitetyn haittaohjelmatorjunnan käyttöönoton konfigurointi

Tietojenkäsittelyn koulutusohjelma

Keskitetyn haittaohjelmatorjunnan käyttöönoton konfigurointi

Tietojenkäsittelyn koulutusohjelma

Timo Mäklin
Opinnäytetyö
Kevät 2018
Tietojenkäsittelyn koulutusohjelma
Oulun ammattikorkeakoulu

TIIVISTELMÄ

Oulun ammattikorkeakoulu
Tietojenkäsittelyn perustutkinto, Järjestelmäasiantuntija

Tekijä(t): Timo Mäklin
Opinnäytetyön nimi: Keskitetyn haittaohjelmatorjunnan käyttöönoton konfigurointi
Työn ohjaaja: Jukka Kaisto
Työn valmistumislukukausi- ja vuosi: kevät 2018 Sivumäärä: 34 + 3 liite sivua

---

Tietoturva on tällä hetkellä yrityksillä suurena huolena. Vuonna 2017 haittaohjelmat pääsivät hyvin hyödyntämään tietoturva-aukkoja, koska yritykset eivät olleet päivittäneet järjestelmiään. Siitä aiheutui suuria rahallisia menetyksiä yrityksille. Keskitetyllä hallinnalla voidaan suuresti helpottaa tietoturvaohjelmien ylläpitoa sekä jakelua.

Tämä opinnäytetyö on tehty keskisuureen yritykseen, jossa vanha ennestään asennettu keskitetty hallinta on päivitetty uudempaan sekä otettu käyttöön uusi keskitetty pilvihallinta kannettaville tietokoneille sekä mobiililaitteille. Opinnäytetyö on tehty käytössä olevaan ympäristöön, johon on kuulunut satoja tietokoneita ja päätelaitteita ympäri Suomea. Työn toteuttamiseen meni useita kuukausia ja työ pyrittiin tekemään mahdollisimman paljon automatisoimalla. Teoriaosuudessa on käyty läpi haittaohjelmia sekä kuinka niiltä voidaan suojautua. Työssä on myös haastateltu yrityksessä toimivaa järjestelmäpäällikköä.

Opinnäytetyön toteuttaminen meni suunnitellusti ja kaikki palvelimet, kannettavat sekä Android-käyttöjärjestelmälliset mobiililaitteet saatiin keskitettyjen hallintojen piiriin. Tietoturvaohjelmistojen hallinta sekä jakelu toimivat nyt vaivattomasti ja näin voidaan varmistua, että haittaohjelmat eivät pääse aiheuttamaan haittaa yrityksen verkossa. Jatkokehityksenä yrityksessä voidaan siirtää myös iOS-käyttöjärjestelmällä olevat mobiililaitteet keskitetyn hallinnan piiriin.

Asiasanat: tietoturva haittaohjelmat windows työasemat palvelimet

ABSTRACT

Oulu University of Applied Sciences
Degree Programme of Business Information Systems, System Administration

---

Author: Timo Mäklin
Title of thesis: Configuration of the centralized security management
Supervisor: Jukka Kaisto
Term and year of completion: Spring 2018 Number of pages: 34 + 3 appendices

---

Computer security is a great concern of companies now. In the year of 2017 malware got to take advantage of vulnerabilities because companies hadn't updated their computer systems. With centralized security management companies can greatly improve their management of security programs and be sure that they are safe.

This bachelor thesis was done to a mid-sized company where the old centralized management have been upgraded and the new cloud based centralized management have been configured to managed laptops and mobile devices. Thesis was done in to a working environment where there was hundreds of computers all over Finland. It took several months to complete this thesis because of large environment. Theory part of the thesis tells what malware is and how to protect against them. There is also interview of the of the IT Delivery Manager of the company.

The work of the bachelor thesis went great and all of the computers and mobile devices are now in the centralized security management. Now there are newest security software installed on computers and the future delivery of the newest security software works easily.

Keywords: security malware windows workstations servers

SISÄLLYS

1 JOHDANTO

Maailmassa iski 2017 vuoden kesällä suuri haittaohjelmaepidemia, jossa satojatuhansia tietokoneita joutui haittaohjelmien uhriksi muutaman kuukauden aikana. Tietoturvapäivitykset ja ajantasainen tietoturvaohjelmisto olisivat voineet pelastaa yrityksien tietokoneet. Yrityksen tietoturvaturvan keskitetyllä hallinnalla voidaan varmistaa, että kaikissa yrityksen koneissa ovat oikeat asetukset ja ajantasaiset päivitykset. Lisäksi voidaan tarvittaessa asentaa tietoturvaohjelmistoja tai puhdistaa koneita haittaohjelmista. Keskitetyllä hallinnalla voidaan myös säästää suuria määriä tehokasta työaikaa.

Opinnäytetyössä käydään läpi keskisuuren yrityksen tietoturvaohjelmistojen hallinnan keskittäminen olemassa olevasta ympäristöstä uudempaan sekä lisäämällä siihen älypuhelimet. Työssä on haastateltu yrityksessä toimivaa järjestelmäpäällikköä, jolla on kokemusta IT-alalta jo yli 17 vuotta. Haastattelussa nousi esille henkilöstön kouluttamisen tärkeys tietoturvaan liittyvissä asioissa. Työn toteuttaminen kesti muutamia kuukausia ja tämä johtui koneiden suuresta määrästä, jotka sijaitsivat ympäri Suomea. Siirto vanhasta hallinnasta uuteen haluttiin hoitaa mahdollisimman automaattisesti ilman yksittäisiä käsiasennuksia. Ympäristö yrityksessä oli täysin Windows-käyttöjärjestelmällä toimiva ja keskitynkin käsittelemään aiheita vain Windows-käyttöjärjestelmän näkökulmasta koneissa ja mobiilipuolella keskitytään Android-käyttöjärjestelmään.

Opinnäytetyöni idea syntyi helposti, kun jouduin työni puolesta tekemisiin keskitetyn hallinnan kanssa. Aiheena keskitetty hallinta sekä tietoturva herättivät minussa suurta mielenkiintoa ja aiheena tämä on ajankohtainen haittaohjelmien kasvun takia.

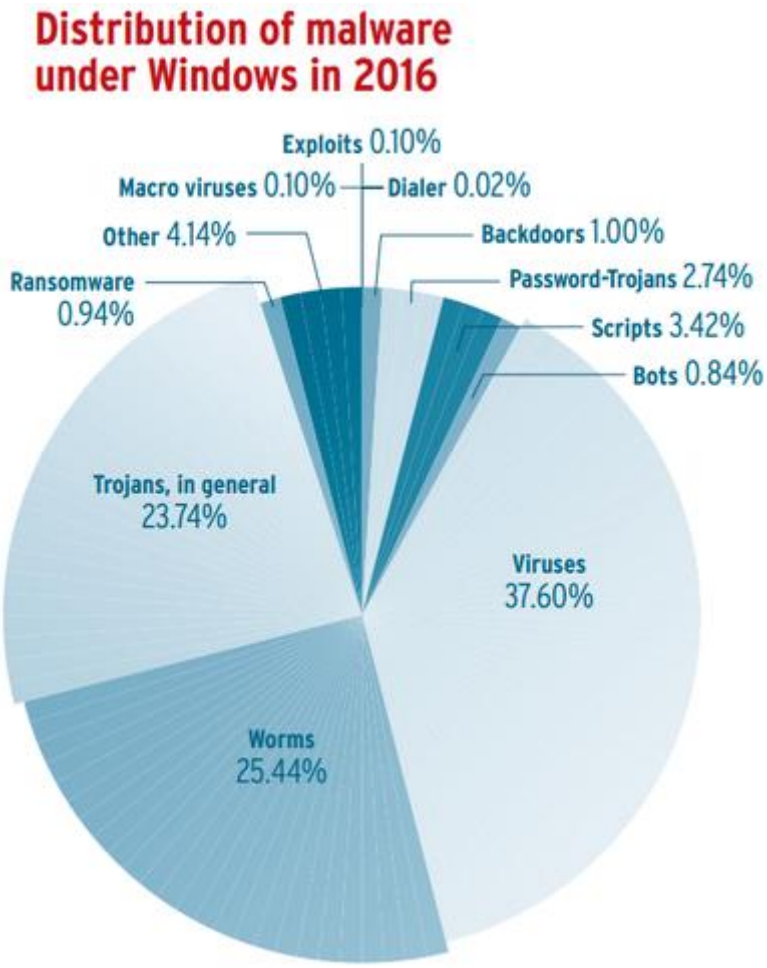
2 HAITTAOHJELMAT

Haittaohjelma on ohjelma, jonka tavoitteena on aiheuttaa tietokoneen käyttäjän kannalta ei-toivottuja tapahtumia tietojärjestelmässä tai sen osassa. Nykyisin haittaohjelmat pyrkivät asentumaan tietokoneelle salaa tai ilman lupaa käyttäjältä ja eri haittaohjelmilla on erilaisia tavoitteita ja voivat toimia hyvin vaihtelevin metodein. Haittaohjelmilla ei pyritä pelkästään aiheuttamaan haittaa vaan niitä käytetään rikollisessa toiminnassa ja niillä pyritään tekemään rahaa. (Oriyano 2016, luku 8, Malware.)

Haittaohjelmat ovat yleiskäsite erilaisille viruksille, madoille, troijalaisille, takaoville, piilohallintaohjelmille sekä kiristyshaittaohjelmille. Haittaohjelma voi toimia taustalla käyttäjän tietämättömänä tai sitten se voi olla myös hyvinkin näkyvä ja haitata tietokoneen käyttöä tai tehdä tuhoja. (Järvinen 2012, 178.)

2.1 Tämän hetken trendit haittaohjelmissa

Yhden itsenäisen tietoturvainstituutin julkaiseman statistiikan mukaan Windows-käyttöjärjestelmä oli selvästi muita käyttöjärjestelmiä suositumpi haittaohjelmissa vuonna 2016, saaden melkein 70% kaikista haittaohjelma havainnoista. Tämä luku on kasvamassa päin ja 2017 vuoden ensimmäisellä kvartaalilla luku on noussut jo yli 77%. Windows-käyttöjärjestelmän yleisimpiä haittaohjelmia vuonna 2016 olivat virukset, madot sekä troijalaiset (katso kuvio 1). (AV-Test 2017, viitattu 18.2.2018.)



KUVIO 1. Haittaohjelmien jakauma Windows-käyttöjärjestelmässä vuonna 2016.

Vuonna 2017 yleistyivät selvästi kiristyshaittaohjelmat, näistä pahimmat tapaukset maailmalla olivat kesällä iskeneet WannaCry sekä NotPetya –haittaohjelmat. Molemmissa tapauksissa haittaohjelman leviäminen oli todella nopeaa yritysten sisäverkossa johtuen haittaohjelman käyttämästä tietoturva-aukosta, joka liittyi Windowsin SMB-verkkolevyprotokollaan. Microsoft oli julkaissut tietoturvapäivityksen pari kuukautta aikaisemmin mutta yritykset eivät olleet asentaneet päivityksiä ajan tasalle. Pelkästään WannaCry kerkesi saastuttamaan maailmanlaajuisesti yli 200 000 tietokonetta yli 150 maassa. (Viestintävirasto 2018, Viitattu 18.2.2018.)

2.2 Mobiililaitteiden haittaohjelmat

Mobiililaitteiden haittaohjelmat ovat saman tyylisiä kuin tietokone puolella. Haittaohjelma pyrkii saamaan aikaan vahinkoa laitteen omistajalle. Tyypillistä käyttäytymistä on varastaa käyttäjän puhelimesta tietoja, sisältäen mm: viestejä, puhelulokeja, yhteystietoja, kuvia, videoita, selaushis-

toriaa sekä laitetunnusta. Haittaohjelmat voivat myös pyrkiä esimerkiksi lähettämään kalliita viestejä palveluihin, asentamaan ei-toivottuja ohjelmia, antaa etäpääsyn rikollisille ja varastamaan pankkitietoja. (Kotipalli, Imran 2016, luku 9, Android Malware.)

Haittaohjelmat ovat kasvussa mobiililaitteiden Android ja iOs –käyttöjärjestelmissä. Vuonna 2016 tuli pelkästään uusia Android-haittaohjelmatunnisteita yli 4 miljoonaa kappaletta, mikä on tuplasti enemmän mitä vuonna 2015. Selvästi suurin osa haittaohjelmista Android-käyttöjärjestelmässä on troijalaisia. Nykyään kiristyshaittaohjelmat ovat koko ajan yleistymässä ja pelkästään vuoden 2017 ensimmäisellä neljänneksellä kiristyshaittaohjelmien määrä on kasvanut yli 250 prosenttia mobiililaitteissa. (F-Secure 2017, Viitattu 25.4.2018; AV-Test 2018, Viitattu 25.4.2018.)

3 SUOJAUTUMINEN

Haittaohjelmilta suojautuminen on tärkeää, koska nykyään yritykset voivat kärsiä rahallisesti sekä pahimmassa tapauksessa lamaantua, mikäli haittaohjelma pääsee iskemään yrityksen tietokoneisiin. Kaikki yritysten data alkaa olla enemmän ja enemmän ainoastaan digitaalisessa muodossa ja paperisia kopioita tehdään enää vain tarvittaessa. Mikäli tuo digitaalinen tieto salataan tai tuhotaan haittaohjelman toimesta, niin tästä on yritysten enää hankala jatkaa toimintaansa.

Yritysten tarjoamat palvelut voivat olla täysin digitaalisia ja mikäli nämä palvelut ovat poissa käytöstä, niin tästä aiheutuu yrityksen maineelle haittaa sekä tällä voi olla rahallisia vaikutuksia yritykseen asiakkaiden kautta, kun nämä vaativat korvauksia.

Vuoden 2017 laajimmat haittaohjelma hyökkäykset olisi voitu estää, mikäli yrityksillä olisi ollut ajantasaiset päivitykset ohjelmissa ja käyttöjärjestelmissä. Microsoft julkaisi omaan kriittiseen tietoturva-aukkoonsa korjauksen muutamassa tunnissa sen ilmitulon jälkeen ja vielä yli kuukauden jälkeen korjauksen julkaisusta, yrityksistä löytyi satojatuhansia tietokoneita, joista puuttui tuo päivitys. (Viestintävirasto 2018, Viitattu 19.3.2018.)

3.1 Haastattelu järjestelmäpäällikkö

Tein tietoturvaan liittyvän asiahaastattelun, jossa haastattelin keskisuuressa yrityksessä järjestelmäpäällikön tehtävässä toimivaa henkilöä. Yrityksessä on töissä noin 600 henkilöä. Haastattelu toteutettiin palaverin muodossa, jota ennen olin lähettänyt haastattelukysymykset ennakkoon (LIITE 1). Haastattelu oli hyvin onnistunut ja saimme aikaan myös pientä keskustelua, jossa pystyin esittämään tarkentavia lisäkysymyksiä aiheeseen liittyen.

Haastateltavalta löytyy ammatillista kokemusta IT-alan työtehtävistä yli 17 vuotta. Työura on alkanut lähituen tehtävistä ja edennyt asiantuntijapolun kautta tämän hetkiseen tilanteeseen. Tässä yrityksessä hän on ollut töissä seitsemän ja puoli vuotta ja nykyisessä järjestelmäpäällikön tehtävässään hän vastaa yrityksen IT-infrasta, palvelujen toimivuudesta sekä teknisestä tietoturvasta.

Keskitetyn hallinnan tuomat edut haittaohjelmien torjunnassa järjestelmäpäällikkö näkee varsinkin tehokkuudessa. Kun hän tuli seitsemän ja puoli vuotta sitten tähän yritykseen töihin, niin silloin kaikki tietoturvaohjelmistojen asennukset olivat yksittäisiä asennuksia. Nämä muutamat kymmenet asennukset hakivat haittaohjelmatunnisteet keskitetysti, mutta ohjelmien asetukset saattoivat vaihdella hyvinkin paljon asentajasta riippuen. Tämä johtui siitä, että asetuksia ei saatu lukittua ja näin ollen käyttäjä pystyi itse muuttamaan tietoturvaohjelman asetuksia. Nykyään asetusten lukitseminen on vaadittu jopa sertifioinneissa ISAE 3402 sekä ISO 27001, joita yritys noudattaa. Asetusten lukitsemisen avulla voidaan varmistaa, että käyttäjä ei voi omalla toiminnallaan tehdä tietoturvaohjelmistosta toimimatonta.

Haastateltavan työuran aikana haittaohjelmilta suojautuminen on muuttunut varsinkin viime vuosien aikana. Ennen riitti hyvin pitkälle se, että suojauduttiin vain ulkoista uhkaa vastaan vahvoilla palomuureilla ja nyt muutaman vuoden sisään on uhkakuvaan tullut vahvemmin nämä kiristyshaittaohjelmat, jotka salaavat tiedostot päästessään koneelle ja leviävät omatoimisesti verkossa. Haittaohjelman päästessä palomuurista läpi yrityksen verkkoon, haittaohjelma leviää hyvin nopeasti koneesta toiseen salaten kaiken ja näin ollen voi aiheuttaa paljon enemmän haittaa kuin se, että vain yksi kone olisi saastunut. Nykyään täytyy siis suojautua sekä ulkoisia, että sisäisiä uhkia vastaan ja jokaisessa koneessa tulisi olla tietoturvaohjelmisto. Ennen mainetunnisteilla oli suurempi merkitys haittaohjelmien tunnistamisessa, mutta nykyään tulee näitä nollapäivähaavoittuvuuksia koko ajan ilmi, niin käyttäytymiseen perustuva tunnistaminen on tehokkaampaa haittaohjelmien kiinnisaamisessa. Viime vuonna hyvänä esimerkkinä oli WannaCry haittaohjelma, joka käytti hyödykseen nollapäivähaavoittuvuutta. *”Aina on tärkeää tunnistaa poikkeavia tapahtumia, joko verkossa tai koneessa ja näistä pitäisi vähintäänkin nousta lippu pystyyn, että jotain poikkeavaa on tapahtunut ja sitä voidaan katsoa tarkemmin.”*

Mobiililaitteiden haittaohjelmien torjuntaa pitää haastateltava mielenkiintoisena tällä hetkellä. Tässä yritykset ovat ehkä voineet ottaa vähän löysemmän linjan tietoturvan näkökulmasta. Puhelimissa ei välttämättä ole yritykselle kriittistä tietoa ja mikäli puhelin varastettaisiin tai sen suojaus murrettaisiin, niin siinä oletettavasti menetettäisiin enemmänkin henkilökohtaista tietoa kuin yrityksen tietoa. Tämä ei kuitenkaan poista sitä faktaa, että työn tekeminen mobiililaitteilla on koko ajan kasvussa. Mobiililaitteiden tietoturvaan on olemassa jo sovelluksia, joilla voidaan eristää yrityksen tiedostot omaan suojattuun lokeroon ja mikäli puhelin varastetaan, on yrityksen tiedostot turvassa. MDM (Mobile Device Management) on kova juttu tuolla mobiilipuolella haastateltavan mielestä. ”*Tällä hetkellä meillä ei ole vielä kovin suurta tarvetta MDM:lle, mutta on hyvä tiedostaa*

sen tuomat hyödyt, kun tarve tulee. Vaikka puhutaan, että mobiililaitteiden käyttöjärjestelmissä; Android sekä iOS olisi paljon haittaohjelmia, niin täytyy muistaa, että emme ole nähneet vielä yhtään suurta epidemiaa maailmalla. Mobiililaitteiden haittaohjelmat ovat vielä lastenkengissä, kun sitä verrataan esimerkiksi Windows-käyttöjärjestelmään."

Kysyttäessä suurinta uhkaa haittaohjelmissa tällä hetkellä, niin vastauksena tulee kryptolockerit. Mikäli tuollainen haittaohjelma pääsisi iskemään yritykseen ja salamaan sen ensisijaisen tiedon, eikä varmistukset olisi kunnossa, niin sillä voisi aiheuttaa todella suuren haitan yritykselle. Toinen suuri uhka haastateltavan mielestä on haittaohjelmat, jotka varastaisivat tietoa. *"Jos yrityksen ympäristöön pääsee semmoinen haittaohjelma, jonka seurauksena meidän tai asiakkaiden tietoa päätyy yrityksen ulkopuolelle tai pahimmassa tapauksessa julkisuuteen, niin melkein voidaan lyödä lappu luukulle. En kuitenkaan usko, että tällä hetkellä tämä on kovin suuri uhka meidän kokoiselle yritykselle. Kryptolockerit on tällä hetkellä se suurin uhka mihin meidän pitää varautua ja miten niiltä voidaan suojautua niin samalla tavalla kuin muiltakin haittaohjelmilta: kouluttaa henkilöstöä, pitää tietoturvaohjelmistot kunnossa sekä muistaa varmistusten tärkeys, nämäkin erillisessä verkossa.*" Kryptolockereista haastateltava vielä muistuttaa, että ne salaavat myös kaikki verkkokiintolevytkin, mitkä on yhdistetty koneeseen ja maailmalla on ollut tapauksia missä kryptolocker on salannut koneeseen yhdistettyjä Dropbox sekä OneDrive –asemia. Näissä tiedostojen palautus pitäisi kuitenkin onnistua kohtalaisen helposti, esimerkiksi versioinnin kautta.

Ohjelmien ja käyttöjärjestelmien päivittämistä pitää haastateltava hyvin tärkeänä. Haasteen tässä tuo aina yrityksen omat ympäristöt ja niiden tuomat rajoitteet. *"On kuitenkin fakta, että kun tietoon tulee kriittinen tietoturva-aukko sovelluksessa tai käyttöjärjestelmässä ja siihen on päivitys, niin se on pakko päivittää. Tästä loistavana esimerkkinä on tuo WannaCry, tuo SMB-haavoittuvuus mitä tuo haittaohjelma hyödynsi, niin siihen oli tullut Microsoftilta päivitys paria kuukautta aikaisemmin. Samaa haavoittuvuutta hyödynsi myöhemmin myös NotPetya. Tästä taisi tulla FedEx:ille 300 miljoonan dollarin menetykset. Me seurataan viestintäviraston tuottamia tiedotteita tietoturvasta sekä haavoittuvuuksista ja he ovat nostaneet rooliaan tässä tiedottamisessa hyvin. Tällä hetkellä eletäänkin hyvin erilaisessa maailmassa haittaohjelmien suhteen, pitää olla ajan hermolla hyvin. Ennen pystyi menemään vaikka puoli vuotta vanhoilla päivityksillä, mutta ei enää. Tietoturva ei ole nykyään semmoista mikä hoituu itsestään vaan siihen pitää nähdä vaivaa."*

Tietoturvan tärkeimpänä asiana haastateltava näkee kokonaisuuden hahmottamisen. *"Teknisen tietoturvan, palomuurit ja tietoturvaohjelmistot voidaan vetää niin tiukaksi, että ne ovat melkein*

pommin varmoja, mutta nämä täytyy aina suhteuttaa liiketoiminnan kokoon ja siihen kuinka kriittistä se tieto on. Teknisellä tietoturvalla voidaan käytännössä estää yrityksen toiminta, mikäli se on liian tiukkaa. Työntekijöiden kouluttaminen on myös iso osa tietoturvaa, koska vaikka tekninen tietoturva olisi kuinka tiukkaa, niin oletettavasti työntekijä voi jollain tavalla tai toiminnallaan saada vahingossa haittaohjelman järjestelmään. Tämän hetken haittaohjelma trendejä katsellessa, niin aina vaaditaan se työntekijän virhe, että haittaohjelma pääsee järjestelmään. Oli kyse sitten kryptolockerista, joka käyttää hyödykseen tunnettua haavoittuvuutta, niin se olisi meidän IT-järjestelmien ylläpitäjien virhe tai sitten vaikka sähköpostihuijausviestit, niin jonkun käyttäjän pitää niihin reagoida, että niistä on vaaraa. Sopivassa suhteessa teknistä tietoturvaa ja työntekijöiden kouluttamista."

Kouluttamisen suhteen järjestelmäpäällikkö näkee selvän muutoksen aikaisempiin vuosiin. Työntekijöiden kouluttamista tietoturvan suhteen on huomattavasti enemmän kuin vaikka viisi vuotta sitten. *"Meilläkin koulutetaan säännöllisesti työntekijöitä tietoturvan suhteen ja meidän tietoturvapolitiikassakin lukee, että kerran vuodessa on koulutus. Tämä on mielestäni todella hyvä asia. Media on myös nostanut rooliaan tietoturvavalveutuneisuuden ja tietoturvauutisten suhteen. Mikäli maailmalla leviää esimerkiksi Facebook huijauslinkki tai tulee hämäriä soittoja ihmisten puhelimiin, niin tästä yleensä löytyy uutinen melkoisen nopeasti. Meillä yrityksessä tietoturvatietoisuutta lisätään esimerkiksi koulutuksilla, yhden sivun tiivistelmillä ja tietoturvapolitiikalla."*

Järjestelmäpäällikkö kehittää tietoturvaosaamistaan oman työnsä kautta. *"En käy itse missään koulutuksissa, mutta koen että se on iso osa työtäni IT:n päällikkönä. Tässä talossa on tietoturvapäällikkö, mutta hän vastaa enemmänkin hallinnollisesta tietoturvasta ja prosesseista. Laadimme yhdessä tietoturvapolitiikan, mutta tekninen tietoturva ja alan seuraaminen jää minulle. Olen oppinut paljon tietoturvasta vuosien aikana työtä tekemällä ja kun tulin tähän yritykseen töihin, niin ei ollut tietoturvapolitiikkaa, saati sitten tietoturvaohjelmistoja löytyi vain muutamasta palvelimesta. Nyt on sitten tietoturvapäällikköä, tekniseen tietoturvaan panostetaan huikeasti, seurataan alaa tiiviisti, asennetaan päivityksiä vähän väliä ja ollaan koko ajan tosi aktiivisia."*

Tietoturvallisesta näkökulmasta järjestelmäpäällikön päivittäiseen tekemiseen kuuluu viestintäviraston tiedotteiden, sosiaalisten medioiden kuten LinkedIn ja muiden medioiden seuraaminen pitkin päivää. Haastateltava nostaa viestintäviraston tiedotteiden seuraamisen tärkeäksi. *"Viestintävirasto on nostanut profiiliaan hyvin vuoden aikana ja niiden tiedotteiden seuraaminen on todella tärkeää, se on Suomessa todella hyvä organisaatio. Yrityksenä me ollaan jo sen kokoinen, että*

voimme itse panostaa rahallisesti tietoturvaan, mutta jos mennään paljon pienempiin yrityksiin, niin niillä ei ole aikaa tai rahaa panostaa tietoturvaan, silloin on hyvä, että joku muu seuraa ja sieltä tulee päivittäiset tietoturvaan liittyvät tiedotteet. Itsestäni tuo tietoturva on aihepiirinä hyvin kiinnostava ja se että kun ymmärtää enemmän, miten asiat vaikuttavat toisiinsa niin pystyy suojautumaan jo osaltaan ennalta näihin uhkiin."

Haastateltava odottaa tänä vuonna mielenkiintoisia uutisia mediassa tietoturvarikkeistä, jotka täytyy keväästä lähtien ilmoittaa julkisesti EU:n laajuisen GDPR (General Data Protection Regulation) tietosuoja-asetuksen myötä. Hän veikkaa, että tänä vuonna tulee myös sattumaan joku WannaCry:n kaltainen haittaohjelmaepidemia, johon kaikki yritykset eivät ole varautuneet täysin.

Lopussa hän vielä kiteyttää oman näkemyksensä tietoturvasta tähän: "*Tietoturva täytyy aina suhteuttaa liiketoiminnan kokoon ja sen tarpeisiin, unohtamatta henkilöstön kouluttamista. Varmistukset tulee aina olla kunnossa, koskaan ei tiedä milloin niitä voi tarvita. Huolimattomuusvirheitä sattuu meille kaikille ja faktahan on vain se, että tietoturvarikkeitä vaan tulee ja se täytyy hyväksyä."* (Järjestelmäpäällikkö, haastattelu 22.3.2018.)

3.2 Palomuurit sekä tietoturvaohjelmistot

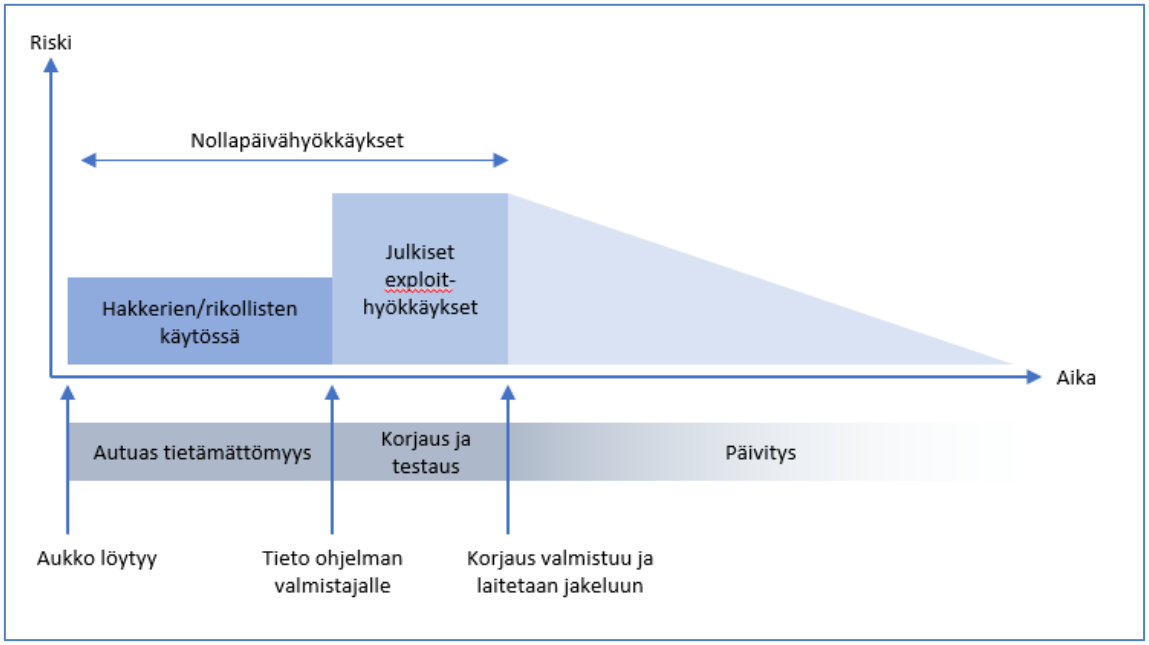
Palomuurilla voidaan hallita tietoliikennettä yrityksen verkon ja muiden verkkojen välillä sekä estää luvatonta tai asiatonta liikennettä verkossa. Palomuuri on yleensä asennettu verkon reunalle, mistä liikennöidään Internettiin. Sinne tehdään sääntöjä sekä avauksia silloin kun niitä tarvitaan ja jos palomuurista ei löydy tarvittavaa sääntöä niin se estää ko. tietoliikenteen ja näin ollen esimerkiksi haittaohjelmat eivät pysty liikennöimään. (Sanastokeskus 2012, Viitattu 18.2.2018.)

Palomuureja on kahdenlaisia. Rautapalomuureja, jotka toimivat erillisissä laitteissa ja sovelluspalomuureja, jotka asennetaan tietokoneeseen. Rautapalomuuri on yritys käytössä paras vaihtoehto, mutta sovelluspalomuureja voidaan käyttää myös yrityksen tietokoneissa. Rautapalomuureja löytyy hyvin monista laitteista ja niillä voidaan suojata monen kokoisia verkkoja. Molempia ratkaisuja voidaan käyttää yhtä aikaa, mutta kahta sovelluspalomuuria ei suositella asennettavan yhtä aikaa. (Järvinen 2006, 109; Dulaney 2018, luku 4, Firewall.)

Tietoturvaohjelmistojen avulla pyritään estämään haittaohjelmien pääsy tietokoneelle. Niiden tarkoituksena on eristää havaitut haittaohjelmat ja mahdollistaa saastuneiden tiedostojen puhdistaminen haitallisista koodeista. Haittaohjelmien tunnistamiseen käytetään useita eri tekniikoita. Perinteisin menetelmä on mainetunnisteisiin perustuva vertaaminen, mutta nykyisin vahinkoja voidaan myös ehkäistä sovelluksen epäolennaista käyttäytymistä tutkimalla. Mikäli mahdollisia uhkia havaitaan, niin sovelluksen suorittaminen keskeytetään. Nollapäivähaavoittuvuus tapauksissa ei ole mainetunnisteiden vertaamisesta apua vaan haittaohjelma saadaan kiinni käyttäytymisanalyysiin perustuen. (Sanastokeskus 2012, Viitattu 10.3.2018; F-Secure 2016, Viitattu 18.2.2018.)

3.3 Sovelluksien päivitys

Tietokoneessa on tärkeää olla ajantasaiset ohjelmistot. Ohjelmistojen päivityksissä yleensä korjaillaan erilaisia ohjelmointivirheitä, sekä huomattuja tietoturvauhkia. Näistä pahimpia ovat ns. nollapäivähaavoittuvuudet yleisesti käytetyissä java ja flash –pohjaisissa sovelluksissa, joita ei ole vielä paikattu nollapäivähaavoittuvuudelta. Näitä haavoittuvuuksia voidaan kuitenkin jo hyödyntää haittaohjelmissa (katso kuvio 2). Löytyneen nollapäivähaavoittuvuuden arvo voi olla pimeillä markkinoilla jopa miljoona dollaria, mutta korjauspäivityksen julkaisun jälkeen haavoittuvuuden rahallinen arvo putoaa nollaan. (Järvinen 2012, 183; Sanastokeskus 2017, Viitattu 18.2.2018.)



KUVIO 2. Nollapäivähaavoittuuden riski ajan mittaan. (Järvinen 2006, 25.)

3.4 Käyttöjärjestelmän päivitys

Päivitysten pitäminen ajan tasalla Windows-käyttöjärjestelmässä on hyvin tärkeää, sillä tietoturvaan liittyviä aukkoja havaitaan nykyistä enemmän. Päivitysten pääasiallinen tehtävä onkin yleensä paikkailla näitä aukkoja eikä niinkään lisätä uusia ominaisuuksia. Windows-käyttöjärjestelmän päivitykseen on muutamia erilaisia mahdollisuuksia, joista yleisimmät ovat joko automaattiset päivitykset suoraan Microsoftilta tai Windows Server Update Service –palvelun (WSUS) asentaminen, jonka avulla voidaan hallita päivitysten jakelua tarkemmin useammille koneille keskitetysti. Yritykset käyttävät hyvin yleisesti WSUS-palvelua, koska sen hyötyihin kuuluu päivitysten testaaminen tietyillä koneilla sekä yritykset voivat tarkemmin päättää mitä päivityksiä halutaan asennettavan. (Järvinen 2006, 16.)

3.4.1 Automaattiset päivitykset

Microsoft Windows –käyttöjärjestelmän perustoimintoja on automaattiset päivitykset. Tämä toiminto lataa ja asentaa uusimmat päivitykset tietokoneeseen oletuksena automaattisesti. Toiminto ottaa yhteyttä ajastetusti Microsoftin Update –palveluun ja saa sieltä uusimmat päivitykset Microsoftin palvelimilta. Yrityksille tämä automaattinen päivitys ei yleensä ole paras ratkaisu. Yritysten käyttämät sovellukset saattavat olla jo sen verran vanhoja, ettei uusien päivitysten yhteensopivuutta ole testattu eri ohjelmistojen välillä. Myöskin joidenkin päivitysten vaatimat uudelleen käynnistämiset sekä tietoliikenne kuormat voivat olla haitaksi toiminnalle. (Järvinen 2006, 20.)

3.4.2 Keskitetty päivitysten jakelu

WSUS-palvelu on Microsoftin tarjoama ilmainen päivitystenhallintatyökalu, jonka käyttö soveltuu etenkin yrityksille. Se on päivitetty versio vanhasta Microsoftin Software Update Service –palvelusta (SUS) ja sen uusina ominaisuuksina on mm. tuki muille Microsoftin tuotteiden päivityksille ja päivitysten kohdentaminen ennalta määritetyille ryhmille. WSUS-palvelu asennetaan yrityksessä yleensä yhdelle palvelimelle, josta se määritetään jakelemaan päivityksiä yrityksen sisällä oleville koneille. WSUS-palvelusta voidaan määrittää mitä Microsoftin päivityksiä ladataan ja jaellaan yrityksen sisällä oleville koneille, jotka tarvitsevat ko. päivityksiä. Kun yrityksessä on otettu WSUS-palvelu käyttöön, työasemat tai palvelimet käyttävät Windowsissa olevaa automaattiset päivitykset –toimintoa, mutta eivät yhdistä Microsoftin palvelimelle vaan yrityksen sisällä olevalle

koneelle, joka hoitaa näiden päivitysten jakamisen. WSUS-palvelulla voidaan myös kerätä raportteja yrityksen koneista ja selvittää, mitä päivityksiä näihin koneisiin on asennettu ja mitä niistä puuttuu. (Järvinen 2006, 31–32.)

WSUS-palvelu käyttää päivitysten tiedonsiirrossa samaa taustalataustekniikkaan kuin automaattiset päivitykset –toiminto Windowsissa, BITS (Background Intelligent Transfer Service). BITS taustalähetystekniikka tukee tiedostojen lähetystä myös loppupäätelaitteiden välillä, kunhan nämä kuuluvat samaan toimialueeseen. Näin voidaan päivityksiä jakaa koneiden väliltä toiselle koneelle ja näin saadaan päivityksiä nopeammin jaettua. (Microsoft 2018, Viitattu 10.3.2018.)

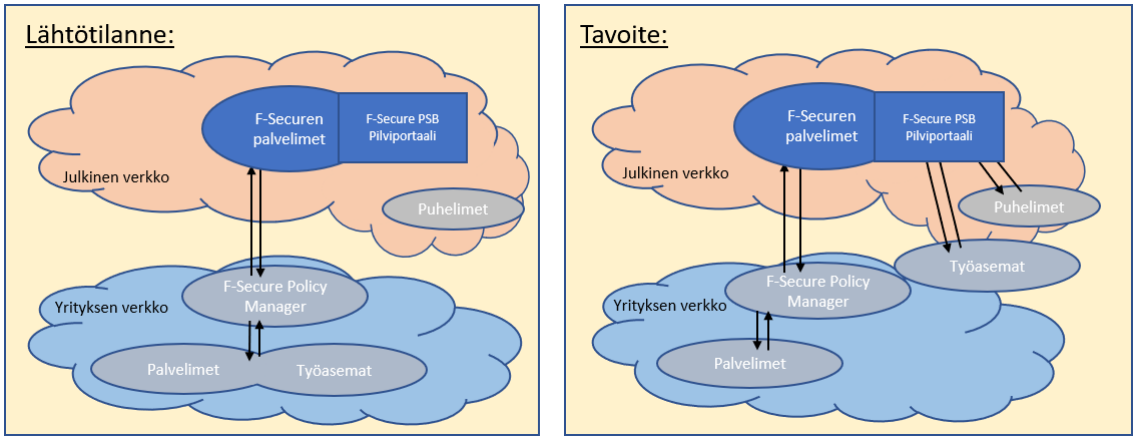
3.5 Käyttäjien kouluttaminen tietoturvatietoisemmiksi

Iso osa tietoturvan vaaroista aiheutuu käyttäjien toimesta, koska he eivät tiedä tekevänsä väärin. Tietämättään he saattavat avata esimerkiksi jonkin epäilyttävän tiedoston tai klikkaamalla linkkiä, josta eivät ole varmoja. Huono kieliasu tai huonot yhteystiedot ovat hyviä merkkejä siitä, että viesti tai verkkosivusto ei ole luotettava. Yleisesti luotettavana pidetyt sivustot ovat myös kieliasultaan hyvin kirjoitettuja eikä sieltä pitäisi löytyä kirjoitusvirheitä ja yhteystiedot ovat yleensä varsin kattavat. (Järvinen, Rousku 2017, 73.)

Vuonna 2017 haittaohjelmat levisivät selvästi eniten sähköpostin liitetiedostojen välityksellä. Tähän on ratkaisuna käyttäjien kouluttaminen tietoturvatietoisemmiksi. Viestintäviraston katsaus vuodesta 2017 tietoturvan kannalta pitää yhtenä TOP5 –ratkaisuna yrityksille tietoturvaan käyttäjäien koulutuksen sekä testaamisen. TOP5 –uhkana yrityksille on huijausviestit sekä tietojen kalastelut. Näiden uhkien tunnistamiseen voidaan työntekijöitä kouluttaa yrityksissä ja pienentää riskiä haittaohjelmien tartuntoihin, tunnuksien joutumista väärälle taholle tai taloudellisten menetysten vaaraa. (Viestintävirasto 2018, Viitattu 10.3.2018.)

4 LÄHTÖTILANNE SEKÄ VAATIMUSMÄÄRITTELY

Yrityksellä on paljon erilaisia palvelimia, jotka ovat suurimmaksi osaksi Windows-käyttöjärjestelmällä varustettuja ja näihin palvelimiin on tarkoitus saada asennettua F-Securen tietoturvaohjelmistot, joita hallitaan F-Securen Policy Managerissa. Yrityksellä on myös kannettavia tietokoneita, jotka sijaitsevat eri puolilla Suomea ja ovat vaihtelevasti kiinni yrityksen verkossa. Näihin liikkuviin koneisiin täytyy saada asennettua F-Securen Computer Security –ohjelmisto, jota hallitaan F-Securen pilviportaalista PSB:stä (Protection Service for Business). Puhelimissa ei ole tällä hetkellä mitään tietoturvaohjelmistoja ja näihin tulee asennettavaksi tietoturvaohjelmisto, jota voidaan valvoa pilviportaalinen kautta (katso kuvio 3).



KUVIO 3. Pelkistetty kuva tietoturvaohjelmistojen hallinoista verkkojen tasolla.

4.1 Nykyinen ympäristö

Yrityksellä on nykyisessä ympäristössä käytössä F-Securen Policy Manager Microsoft Windows 2008R2 –palvelimella. Palvelimille on asennettu F-Securen tietoturvaohjelmistoja, mutta nämä asennukset eivät ole uusimpia versioita. Kannettaville tietokoneille on asennettuna vanhempi F-Securen tietoturvaohjelmisto, joka on yhteydessä F-Securen Policy Manageriin ja tämä asennus tullaan päivittämään uudempaan F-Securen tuotteeseen, jota hallitaan pilven kautta. Mobiililaitteilla ei ole käytössä mitään tietoturvaohjelmistoa.

4.2 Tavoite

Tässä työssä pitää saada siirrettyä kaikki nykyisessä ympäristössä olevat palvelimet uuteen hallinta ympäristöön, sekä päivittää niihin uusimmat saatavilla olevat tietoturvaohjelmistojen versiot. Lisäksi uutena kokonaisuutena tulee F-Securen PSB-portaali (Protection Service for Business), jonka kautta hallitaan liikkuvat työasemat sekä mobiililaitteet. Siirto nykyisestä ympäristöstä täytyy hoitaa rinnakkain nykyisen ja uuden ympäristön kanssa, jotta kaikki koneet saavat uuden tietoturvapalvelimen osoitteen itselleen ja osaavat hakea uudet ohjelmistoversiot, sekä säännöt uudelta palvelimelta. Hallintaohjelmisto tullaan asentamaan uudelle palvelimelle, joka toimii Windows Server 2016 –käyttöjärjestelmällä. Näin voidaan varmistaa pitkäikäinen asennus uudelle kokoonpanolle. Yrityksessä on myös haluttu suojata Android-käyttöjärjestelmäpohjaiset älypuhelimet ja tämä tietoturvaohjelmisto pitää saada jaettua älypuhelimiin, jotka sijaitsevat ympäri Suomea. Microsoftilla olisi tähän sovellus, Intune, jolla mobiililaitteiden asennus voitaisiin automatisoida, mutta yrityksessä ei ole vielä haluttu lähteä tähän mobiililaitteiden hallintaan. Käyttäjien täytyy hoitaa asennukset itse ohjeiden perusteella ja olla yrityksen IT-tukeen yhteydessä, mikäli ongelmia tulee.

4.3 Tietoturvaohjelmiston toimittajan valintaprosessi

Ennen kuin päädyttiin F-Secureen tuotteisiin, tehtiin ominaisuuksien vertailua eri valmistajien tuotteiden kanssa sekä kysyttiin muutamaa tarjousta myyjiltä. Lopullisiksi vaihtoehdoiksi päätyivät F-Securen lisäksi tuotteet Trend Micro:lta sekä McAfee:lta.

Jokainen valmistaja tarjosi lähes samantyylistä pakettia haittaohjelmien torjuntaan. Paketit sisälsivät esimerkiksi keskitettyä hallintaa, erillistä sovellusta palvelimille sekä kannettaville ja sovelluksen mobiililaitteiden suojaukselle, jonka saa yhdistettyä keskitettyyn hallintaan. Tietenkin jokaisella valmistajalla oli oma tekniikkansa sekä lähestymistapansa haittaohjelmien torjuntaan. Lopulta kaikki tuotteet näyttivät tarjoavan hyvän ja nykyaikaisen suojauksen haittaohjelmille, sillä kaikista löytyi käyttäytymisanalyysiin perustuvaa tunnistamista. Tämän avulla tunnistetaan uusia haittaohjelmia, joista ei ole vielä mainetunnisteita.

Internetin riippumattomat testit arvostelivat F-Securen tuotteet parhaimpien joukkoon. Yritys on kotimainen ja näin ollen tukea saa helposti suomeksi. Webinaarien lisäksi vuosittain järjestetään

koulutuksia eri paikkakunnilla. Yrityksellä oli myös ennestään hyviä kokemuksia F-Securen tuotteista nykyisessä ympäristössä. Näiden positiivisten tekijöiden perusteella F-Secure valikoitui yrityksen tietoturvaohjelmistoksi.

5 TIETOTURVAN TOTEUTTAMINEN

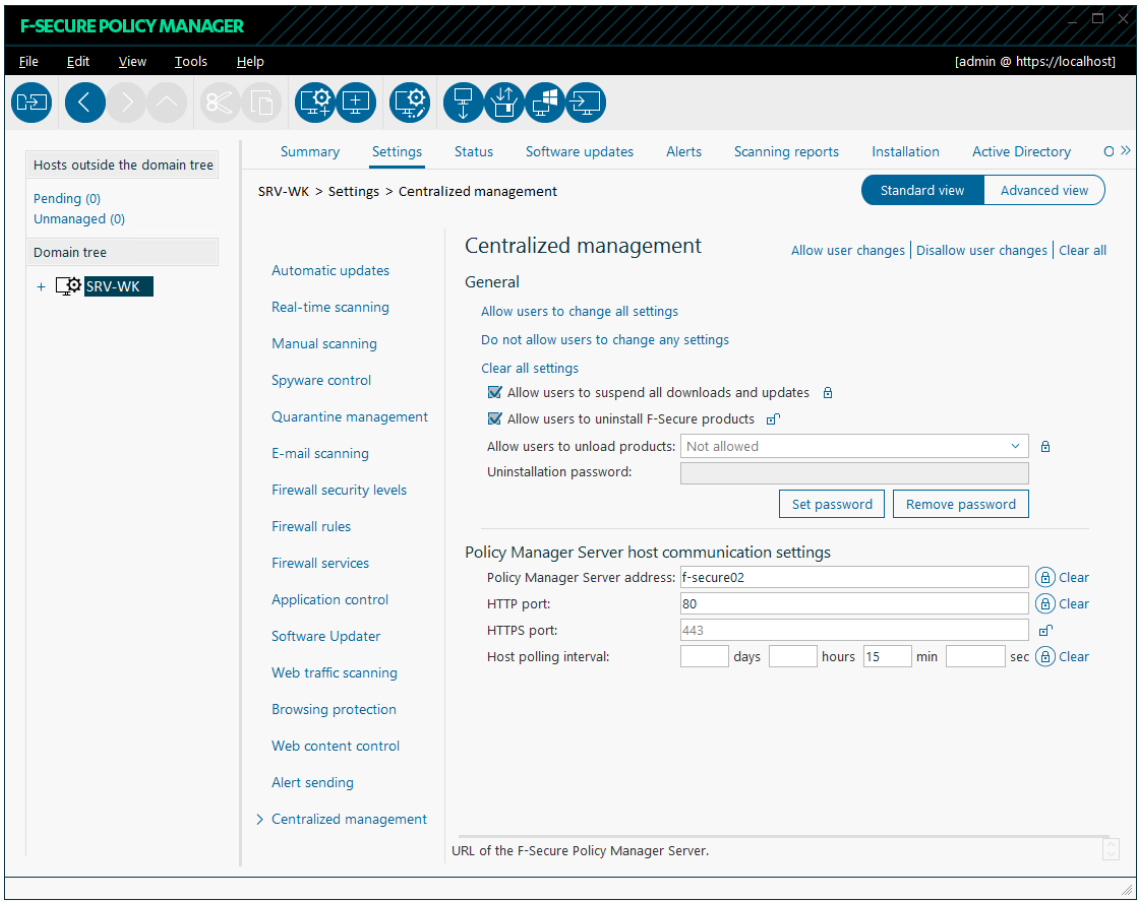
5.1 Mitä on keskitetty hallinta

Keskitetyllä hallinnalla tarkoitetaan yrityksessä paikkaa, jolla voidaan hallita yhdestä paikasta jokaista yrityksessä olevaa konetta. Hallinnan ollessa yhdessä paikassa, säästyy yrityksellä paljon aikaa ja vaivaa, kun jokaista työasemaa tai palvelinta ei tarvitse päivittää yksitellen. Näin voidaan myös varmistua, että työasemien suojaukset ovat ajan tasalla ja suojattuina samalla tavalla, jolloin tietoturvakäytäntöjen tekeminen on helppoa jokaiselle työasemalle yhtä aikaa. Keskitetyssä hallinnassa voidaan tehdä erillisiä ryhmiä, joita voidaan käsitellä eri tavalla ja niissä voi olla erilaisia vaatimuksia ja sääntöjä.

5.2 Keskitetyn hallinnan päivittäminen

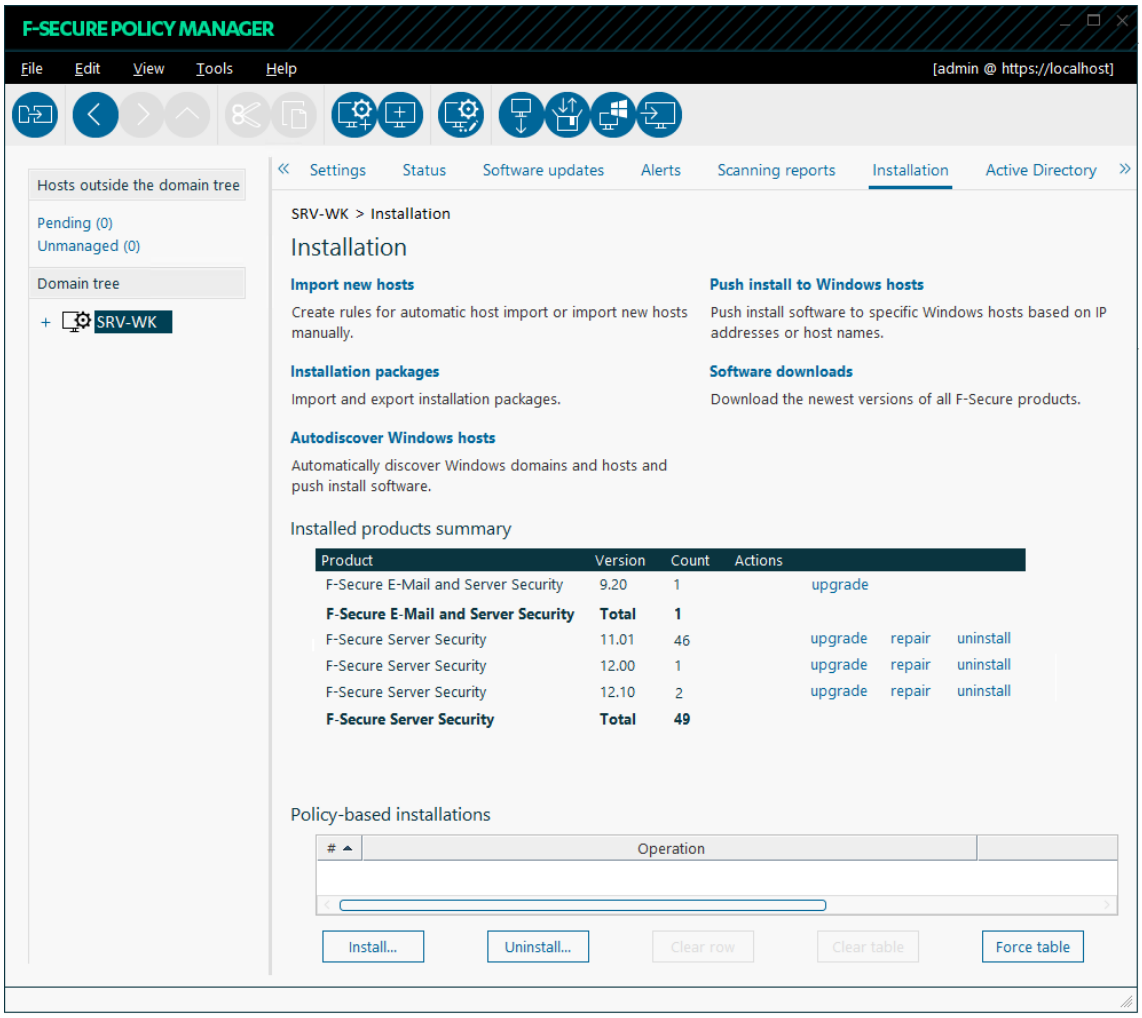
Yrityksellä kun oli jo ennestään F-Securen keskitetty hallinta käytössä, oli ohjelmistojen päivittäminen palvelimiin yksinkertaista. Nykyinen hallinta oli asennettuna Windows Server 2008R2 –käyttöjärjestelmälliselle palvelimelle ja tämä alkoi käydä vanhaksi, niin haluttiin samalla päivittää hallintapalvelin uudempaan. Tähän täytyi rinnalle asentaa uusi palvelin, jotta koneiden hallinta ei missään vaiheessa katkeaisi ja näin ollen jo ennestään hallitut koneet saataisiin siirrettyä uuteen hallintaan hallitusti.

Uuteen palvelimeen valittiin käyttöjärjestelmäksi Windows Server 2016 –käyttöjärjestelmä sekä katsottiin, että palvelin täyttää F-Secure Policy Manager –sovelluksen minimivaatimukset, jotka olivat: 2GHz tuplaydinprosessori, 2GB muistia, 10GB kiintolevy tilaa. Palvelimelle asennettiin F-Securen Policy Manager 12.10 versio, joka oli sillä hetkellä uusin saatavilla oleva versio ja vietiin vanhan palvelimen konetietokanta uudelle palvelimelle. Kun palvelin saatiin asennettua sekä asetettua sinne halutut tietoturvakäytännöt niin täytyi vanhaan hallintaan tehdä muutos, joka muuttaisi koneiden hallintapalvelimen osoitteen osoittamaan uutta palvelinta: f-secure02 (katso kuvio 4).



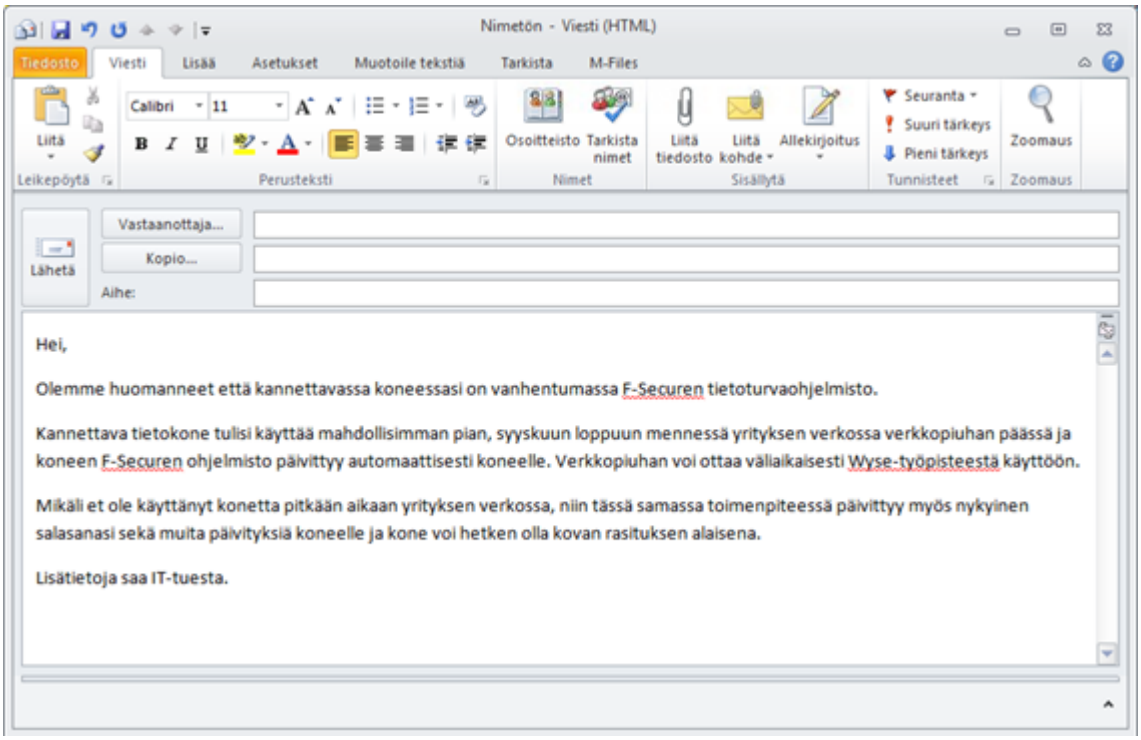
KUVIO 4. F-Secure Policy Manager hallintapalvelimen osoitteen muutos.

Seuraavan kerran kun palvelimet kävivät hakemassa uudet sääntönsä vanhalta hallintapalvelimelta, niin alkoivat ne ilmestyä uuteen hallintaan yksi kerrallaan ja päivän päätteeksi kaikki palvelimet olivat siirtyneet uuden hallinnan piiriin. Suurimmalla osalla palvelimista oli asennettuna vanhempi versio F-Securen Server Security –sovelluksesta ja tämä sovellus piti vielä päivittää uusimpaan saatavilla olevaan ohjelmistoon (katso kuvio 5). Tietoturvaohjelmistojen päivittämiseen meni useita päiviä, kun osa päivityksistä täytyi tehdä ilta aikaan, kun palvelimet tarvitsivat asennuksen yhteydessä uudelleen käynnistämisen ja tätä ei voinut tehdä tuotannollisista syistä kesken päivän.



KUVIO 5. Siirtyneiden palvelinten tietoturvaohjelmistojen eri versioiden määrät.

Nykyiset työasemat olivat hallittuina vanhassa F-Securen Policy Managerissa ja kun työstä oli tullut enemmän liikkuvampaa, niin haluttiin näiden työasemien haittaohjelmatorjunta vaihtaa pilvessä hallittuun, jotta nähdään paremmin tietoturvaohjelmiston tilanne laitteilla. Päätettiin kuitenkin ensin siirtää nykyiset työasemat uuden keskitetyn hallinnan piiriin ja vasta sen jälkeen lähteä vaihtamaan näihin uusi tietoturvaohjelmisto, sekä viemään niitä pilvihallinnan piiriin. Näin päästiin eroon vanhasta hallintapalvelimesta nopeammin, kun saatiin sieltä kaikki koneet pois. Nykyisten työasemien ollessa pääosin kannettavia tietokoneita, koneet eivät olleet kiinni yrityksen verkossa pitkin päivää vaan saattoivat olla useita kuukausia ilman käyntiä yrityksen verkossa. Tällöin koneet eivät saaneet tietoja tietoturvakäytännöistä sekä uudesta hallintapalvelimesta. Tästä meidän piti laittaa koneiden käyttäjille sähköpostiviesti, jossa pyydettiin käyttäjiä tuomaan koneet yrityksen verkkoon kiinni (katso kuvio 6).



KUVIO 6. Kannettavien käyttäjille lähetetty sähköpostiviesti.

Suurin osa kannettavista tietokoneista siirtyi näin uuden hallinnan piiriin parin seuraavan kuukauden aikana. Ne koneiden käyttäjät, jotka eivät tuoneet konetta yrityksen verkkoon, oltiin heihin puhelimitse yhteydessä ja saatiin näin kaikki koneet uuden hallinnan piiriin.

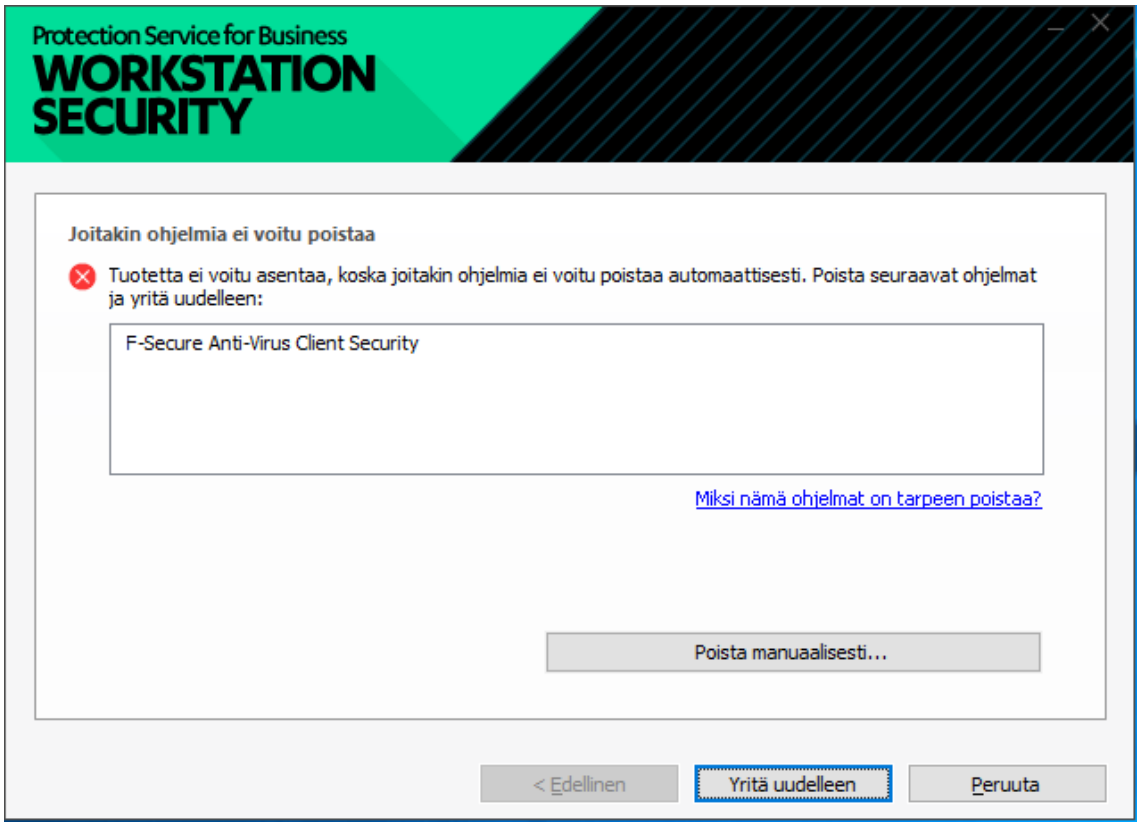
5.3 Pilvipohjainen keskitetty hallinta

F-Securen Protection for Business on pilvipohjainen keskitetty hallinta portaali, josta voidaan ottaa käyttöön, hallita sekä valvoa päätelaitteiden suojausta. Portaaliin voidaan tehdä useita tunnuksia ja tunnuksille voidaan myös asettaa pelkkä lukuoikeus. Kun palvelun hallinta on pilvipohjainen, niin tämä on erityisen sopiva liikkuville työasemille sekä mobiililaitteille vaikkakin myös palvelimet on mahdollista saada tämän hallinnan piiriin. Tässä ympäristössä haluttiin kuitenkin erottaa palvelimet omaan keskitettyyn hallintaan. Pilvipohjainen ratkaisu ei myöskään vaadi yritykselle minkäänlaista asennusta omaan ympäristöönsä vaan hallinnan voi tehdä millä tahansa koneella, jossa on verkkoselain. (F-Secure 2018b, Viitattu 23.4.2018.)

5.3.1 Työasemien tietoturvaohjelmistojen päivittäminen

Yrityksen kannettavat olivat tässä vaiheessa hallittuina uudessa F-Secure Policy Manager –ympäristössä ja niihin oli asennettuina F-Securen Client Security –ohjelmistot, jotka eivät olleet yhteensopivia tämän pilvihallinnan kanssa, vaan niihin täytyi päivittää kokonaan uudet ohjelmistot. Uuden ohjelmiston ohjeen mukaan asennus osasi itse poistaa vanhan tietoturvasovelluksen ja sen jälkeen asentaa uuden tietoturvaohjelmiston rekisteröitymällä pilvihallintaan, kun asennuksessa syötettiin tilauksen yksilöivä avain.

Asennusta aloitettiin testaamaan muutamalla kannettavalla tietokoneella ihan paikallisella asennuksella ja asennus törmäsi aina virheeseen, missä se ei voinut poistaa vanhaa käytössä ollutta sovellusta (katso kuvio 7).

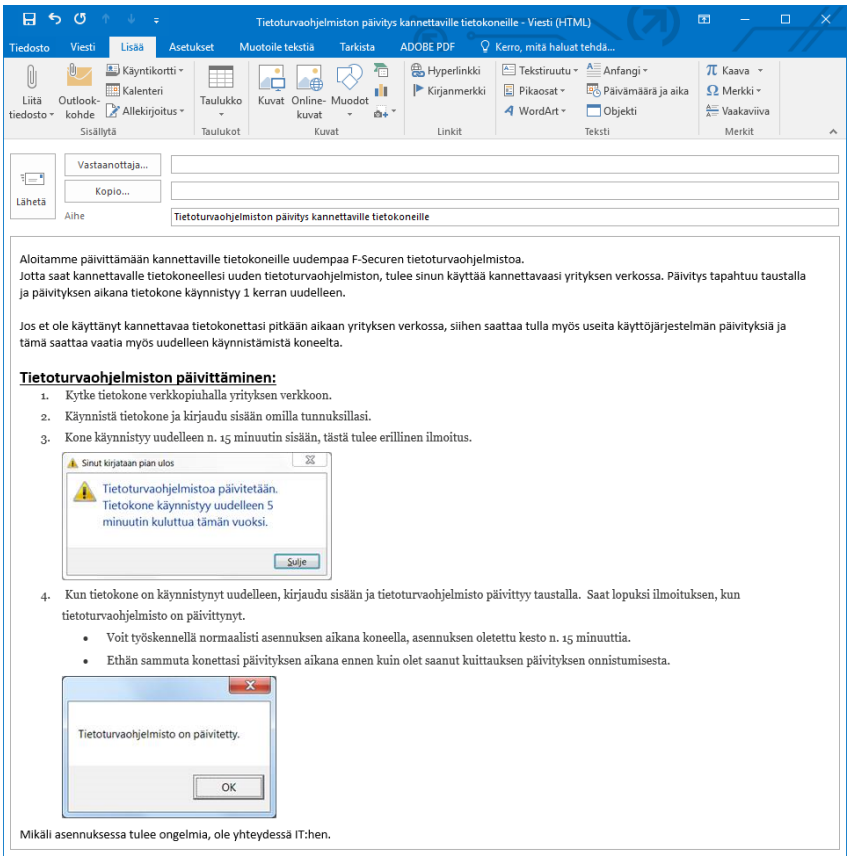


KUVIO 7. Virhe sovelluksen poistossa asennuksen aikana.

Virheeseen ei saatu itse minkäänlaista ratkaisua ja tästä virheestä oltiin yhteydessä F-Securen tukeen, lähetimme muutamia viestejä sekä annoimme heille tarpeen vaatiessa diagnostiikka- sekä lokitiedostoja. Kun suoraa ratkaisua ei F-Securen tuelta saatu, niin keksin itse automatisoida

asennuksen, jossa käyttäjän kirjautuessaan kannettavalle tietokoneelle suoritetaan skripti, mikä hoitaa asennuksen vaiheet oikeassa järjestyksessä (katso liite 2). Skriptissä ensin tarkistetaan, löytyykö ns. ”valmis”-tiedostoa ja löytyessään skriptin suorittaminen loppuu siihen. Tämä ”valmis” -tiedosto luodaan skriptin viimeisenä vaiheena ja näin voitiin varmistua, että tämä kone on saanut asennuksen loppuun asti suoritettua eikä asennusta tarvitse tehdä uudelleen. Skripti suoriutuu täysin koneen taustalla, ilman että käyttäjän tarvitsee tehdä mitään. Tietokone täytyi asennuksen aikana käynnistää uudelleen vanhan tietoturvaohjelman poistossa ja tähän päätettiin laittaa nopea 5 minuutin pakotettu uudelleen käynnistämisen aika. Tietokoneen käynnistyttyä uudelleen skripti jatkoi siitä mihin oli jäänyt tarkistustiedoston avulla ja hoiti asennuksen loppuun. Asennuksen valmistuttua käyttäjälle tulee ruudulle yksinkertainen tekstilaatikko, jossa lukee että ”Tietoturvaohjelmisto on päivitetty”. Käyttäjälle asennus ei näkynyt millään muulla tavalla, kuin pakotettuna uudelleen käynnistämisenä sekä lopussa tulevalla ilmoituksella asennuksen onnistumisesta.

Ennen tietoturvaohjelmistojen päivittämistä, ilmoitimme päivityksestä sähköpostilla yrityksen henkilöille, joilla oli kannettava tietokone. Viestissä kerroimme päällisin puolin, miten asennuksen pitäisi mennä ja kauanko se kestää (katso kuvio 8). Annoimme tämän kirjautumisen yhteydessä suoritettavan skriptin olla käytössä useita viikkoja. Kun suurin osa tietokoneista oli päivittynyt uuteen tietoturvaohjelmaan sekä siirtynyt samalla pilvihallinnan piiriin, niin otimme skriptin pois päältä. Loppuihin käyttäjiin olimme puhelimitse yhteydessä ja hoidimme asennukset käsipelillä etätyökaluilla.

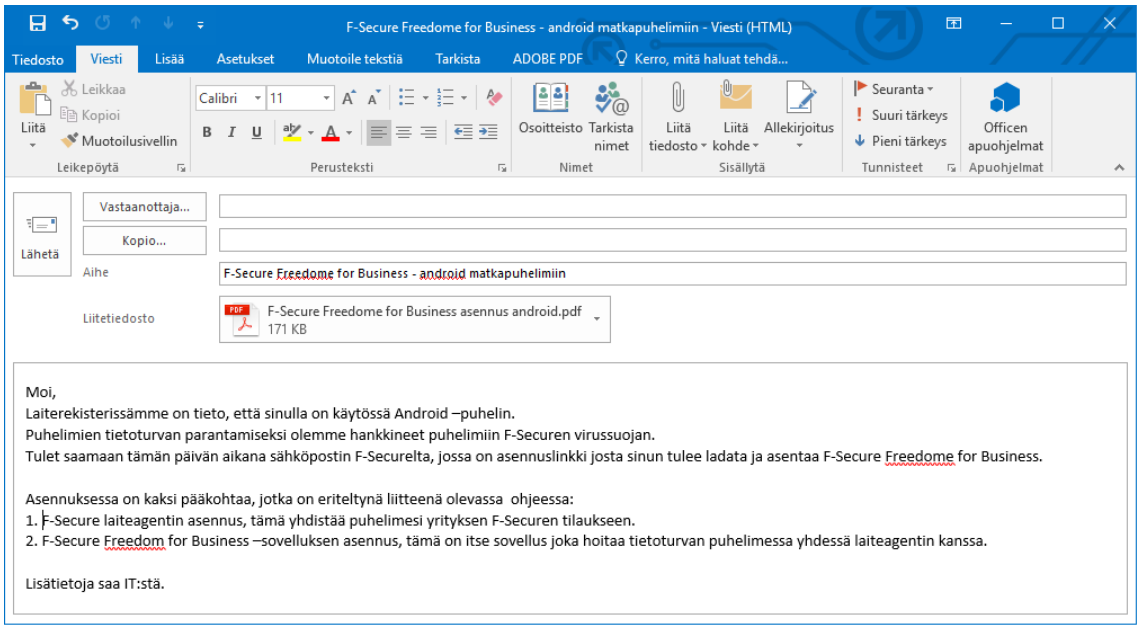


KUVIO 8. Sähköpostiviesti päivityksestä kannettavien käyttäjille.

5.3.2 Mobiililaitteiden tietoturvaohjelmistojen asentaminen

Uuden Protection for Business portaalin avulla voitiin valvoa yrityksen mobiililaitteiden suojausta. Ensin haluttiin lähteä suojamaan Android-käyttöjärjestelmällä olevia mobiililaitteita ja tähän tuotteeksi valikoitui Freedome for Business F-Securelta. Mobiililaitteille ei ollut mitään helppoa tapaa automatisoida asennusta siten, että käyttäjälle ei tarvitsi tehdä mitään vaan päätettiin, että ohjeistetaan käyttäjiä asentamaan sovellus itse. Tähän olikin F-Securella jo saatavilla hyvä ohje (Liite 3). Asennuksessa oli käytännössä kaksi vaihetta: ensin saadusta sähköpostista avattiin yksilöllinen linkki, jonka kautta pystyi lataamaan puhelimeensa hallintasovelluksen, joka liitti puhelimen F-Securen pilvihallintaan. Parin minuutin sisään puhelimen ilmoituskeskukseen tuli ilmoitus, mistä pystyi lataamaan Freedome for Business —sovelluksen, joka hoiti mobiililaitteen suojauksen.

Yrityksen laiterekisterin avulla saatiin helposti tietoon käyttäjät, joilla oli puhelinetu sekä Android-käyttöjärjestelmällinen puhelin käytössä ja näillä käyttäjille lähettiin kohdistettu sähköposti, jossa annettiin ohje asennukseen sekä kerrottiin tulevasta viestistä F-Securelta (katso kuvio 9).



KUVIO 9. Sähköpostiviesti Android-käyttöjärjestelmällisen puhelimen omaaville käyttäjille.

Tietoturvaohjelmiston asentaminen ei aina mennyt täysin ohjeen mukaan, mikä johtui Android-käyttöjärjestelmän versio eroista sekä puhelinvalmistajien itse tekemistä Android-käyttöjärjestelmien muunnoksista. Tämä sekoitti käyttäjiä ja he olivat hyvin usein asennuksesta yhteydessä IT:hen. Ohjeen tekeminen jokaiseen Android-käyttöjärjestelmä versioon sekä puhelinvalmistajien omiin muunnoksiin oli käytännössä mahdotonta, kun testiasennuksiin ei ollut saatavilla kaikkia näitä variantteja sisältäviä laitteita.

6 TESTAUS

Haittaohjelmien torjunnassa on tärkeää saada tieto siitä, kun haittaohjelma on jäänyt kiinni tai kun semmoinen epäilys tulee jostakin sovelluksesta.Työntekijä hyvin usein vain itse sallii sovelluksen tai painaa vain raksista virheen pois, niin suurin osa haittaohjelmien ilmoituksista on otettu työntekijältä pois mutta niistä haluttiin erinäisiä ilmoituksia sekä hälytyksiä IT-järjestelmien ylläpitäjille. Kaikista tietoturvaohjelmiston kiinni saamista haittaohjelmista laitettiin tulemaan hälytys sähköpostilla sekä palvelinympäristöstä laitettiin tulemaan myös perinteinen tekstiviesti lisäksi.

6.1 Hälytykset

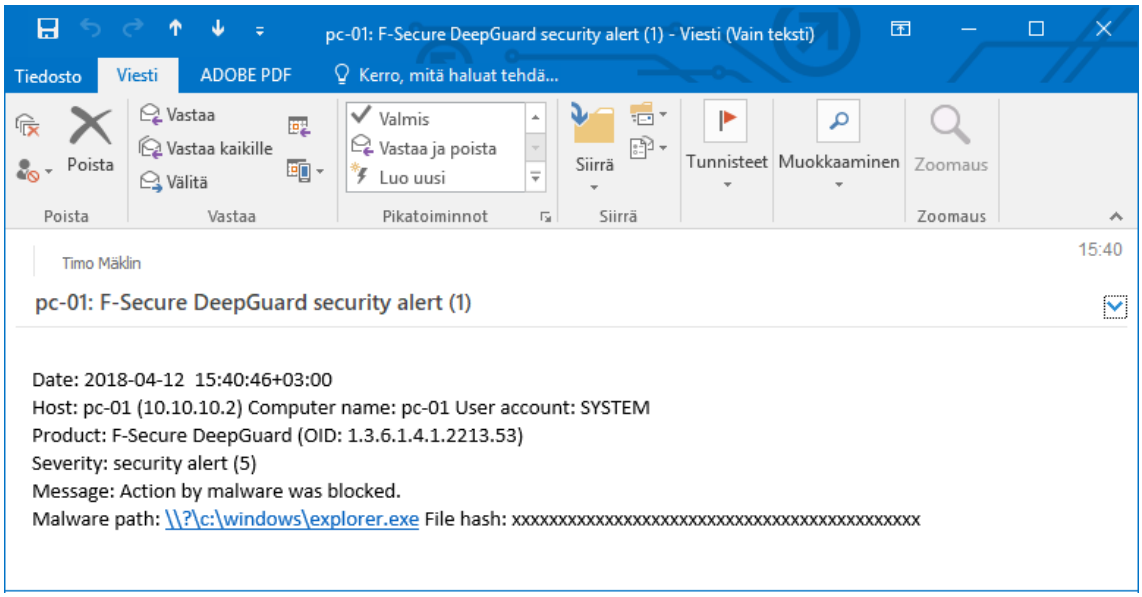
Keskitetyt hallinnat, Policy Manager sekä PSB –portaali täytyi konfiguroida lähettämään sähköpostia aina kun ne havaitsevat haittaohjelman. Sähköpostipalvelimella tehtiin oma jakelulista tätä varten ja listaan lisättiin IT-järjestelmistä vastaavat henkilöt. Järjestelmän testaus tehtiin virallisella EICAR-testihaittaohjelmalla, jonka voi itse tehdä lisäämällä tekstitiedostoon rivin haitallista koodia (katso kuvio 10). Testihaittaohjelma toimii kuten aito DOS-pohjainen haittaohjelma ja sen tavoite on vain tulostaa näytölle teksti: ”EICAR-STANDART-ANTIVIRUS-TEST-FILE”. Yleisimmät tietoturvaohjelmistot tunnistavat tämän EICAR-testihaittaohjelmaksi, mutta käsittelevät sitä kuin oikeaa haittaohjelmaa. (EICAR 2018, Viitattu 24.4.2018.)

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

KUVIO 10. EICAR-testihaittaohjelman koodin pätkä.

6.1.1 Sähköpostilla

Policy Managerin lähettämät sähköpostit ovat hyvin informatiivisia, mutta eivät aina kerro tarkasti onko kyseessä varmasti haittaohjelma. Tässä esimerkissä (katso kuvio 11) kyseessä oli yrityksen oma skripti, joka otti yhteyksiä tietokantoihin yrityksen verkossa, eikä näin ollen ollut oikeasti haittaohjelma, vaikka käyttäytyikin haittaohjelman tavalla. Tämä skripti jäi kiinni F-Securen Deepguardiin, joka on juuri käyttäytymisen analyysin perustuvaa tietoturvaa.



KUVIO 11. Esimerkkiviesti sähköpostilla IT-järjestelmien ylläpitäjille F-Secure Policy Managerista.

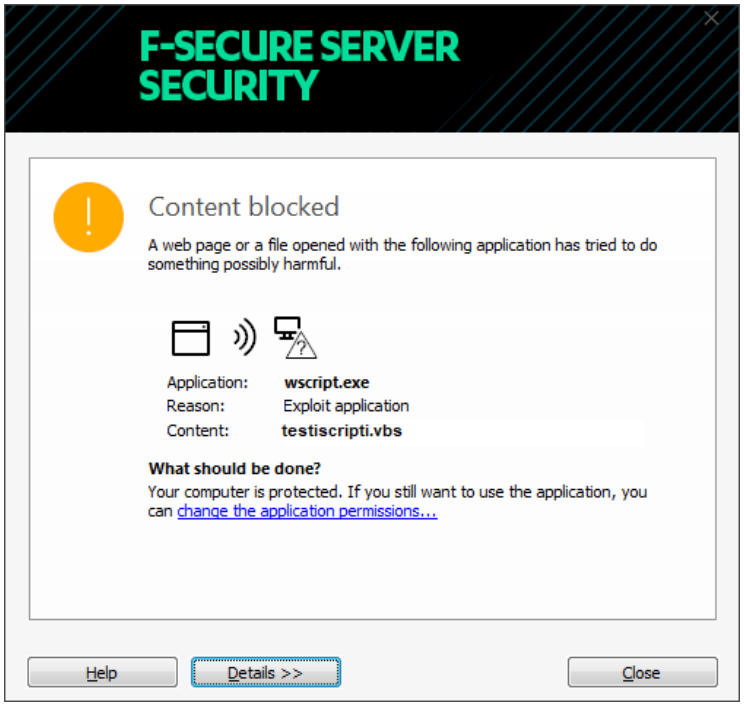
6.1.2 Tekstiviestillä

Yrityksen omista palvelimista haluttiin saada suoraan tekstiviesti IT-järjestelmien ylläpitäjille, koska koettiin että nämä ovat kriittisempiä järjestelmiä kuin yksittäisen käyttäjän kannettava. Matkapuhelimen tekstiviestin myös lukee todennäköisemmin kuin sähköpostin, jos sattuu olemaan esimerkiksi viikonloppu tai ilta-aika. Kumpikaan keskitetyistä hallinnoista ei tukenut suoraan puhelimeen lähetettäviä tekstiviestejä hälytyksen muodossa, niin tämä rakennettiin itse käyttäen hyödyksi jo yrityksen käytössä olevaa PA (Power Admin) Server Monitor –sovellusta. Sovellus skannaa F-Secure Policy Manager –palvelimen tapahtumalokia, poimien sieltä avainsanoja. Mikäli siellä sattuu olemaan F-Securen tapahtuma, jossa on haittaohjelma saatu kiinni, niin siitä lähtee tekstiviesti IT-ylläpitäjille. Tekstiviesti sisältää vain seuraavia tietoja: palvelin, viesti ja haittaohjelmanpolku mutta näiden tietojen valossa voi alkaa tarvittaviin toimiin ja lisätietoja saa sähköpostista sekä keskitetystä hallinnasta.

6.2 Mitä tapahtuu, kun haittaohjelma tartunta tulee.

Käyttäjän suorittaessa haitallista sovellusta, tulee hänen näkyville F-Securen oma ilmoitusikkuna, jossa kerrotaan, että sovelluksen suorittaminen on estetty (katso kuvio 12). Ilmoituksessa lukee, että asetuksista pääsee sallimaan sovelluksen suorituksen, mutta tämä on estetty keskistetyn hallinnan tasolla. Näin voidaan varmistaa, että käyttäjä ei omilla toimillaan pääse suoraan suorit-

tamaan haitallista tiedostoa. Näissä tapauksissa käyttäjiä on opastettu olemaan yhteydessä IT:hen, jossa voidaan tehdä tarvittavat arvioinnit sovelluksen turvallisuudesta.



KUVIO 12. Käyttäjälle tuleva ilmoitus kun haittaohjelma löytyy.

7 POHDINTA

Työntekeminen oli opettavainen prosessi omalle ammatilliselle kehitykselle. Työssä täytyi ottaa huomioon koko ajan käytössä oleva ympäristö, johon ei saanut tulla suuria katkoksia tai hidastuksia työaikana. Työntekijöiden työn jatkuvuus sekä mahdollisimman pienet toimet heidän osalta täytyi ottaa huomioon koko ajan työtä suunnitellessa. Yrityksen sisäinen informointi oli myös erittäin tärkeässä roolissa, varsinkin kun toimipisteitä oli yrityksellä ympäri Suomea sekä työntekijöitä useita satoja.

Työn toteutuksen kannalta työläin prosessi oli suunnitella aina jokainen vaihe mahdollisimman varma toimiseksi. Tämä tarkoitti, että piti miettiä jokaisen työvaiheen mahdollinen lopputulos ja valmistautua siihen. Työn yllättävin kohta tuli kannettavien tietoturvaohjelmistojen päivityksessä uuteen pilvihallintaan, kun tietoturvaohjelmisto ei päivittynytkään valmistajan ohjeiden mukaan. Tämä selvittäminen tuotti haasteita myös valmistajan omassa asiakastuessa ja sieltä en koskaan saanut ratkaisua ongelmaan, vaikka se eteni heidän tuessa usealle asiantuntijalle. Tämän ongelman ratkaiseminen oli itselle työn suurinta antia ja kuvaa hyvin sitä, kuinka luova täytyy työtehtävissä välillä olla.

Testaaminen oikealla testiviruksella sekä hälytysjärjestelmän konfigurointi sähköpostille sekä tekstiviesteille oli yritykselle tärkeää. Näiden avulla voitiin varmistua, että järjestelmä tunnistaa haittaohjelmia oikein ja lähettää tarvittavat hälytykset IT-ylläpitäjille heti havaittuaan haittaohjelman.

Työn tekemisen jälkeen jatkokehitettävää jäi yritykselle vielä ainakin mobiililaitteiden hallinnan ja tietoturvan puolella. Näiden mobiililaitteiden vieminen esimerkiksi Microsoft Intuneen voisi tuoda lisäturvaa yritykselle. Yritys voisi nähdä kattavan kuvan laitteiden käyttöjärjestelmäversioista sekä tarvittaessa päivittää niitä. Keskitetty sovellusten asentaminen Intunen kautta onnistuisi myös jatkossa mobiililaitteisiin. iOs-käyttöjärjestelmälliset mobiililaitteet jäivät nyt myös ilman tietoturvaohjelmistoa ja näihin on tarjolla F-Securella tietoturvaohjelmisto, joka voidaan viedä keskitetyn hallinnan piiriin samalla tavalla kuin Android-käyttöjärjestelmälliset mobiililaitteet.

LÄHTEET

AV-Test 2017. Security report 2016/17. Viitattu 18.2.2018, https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf.

Dulaney, E. 2018. CompTIA Network+ N10-007 Exam Cram. Viitattu 25.4.2018, http://proquest.safaribooksonline.com.ezp.oamk.fi:2048/book/certification/networkplus/9780134866857/common-network-devices/ch04_level2sec1_html?uicode=ouluuas.

EICAR 2018. Anti-malware testfile. Viitattu 24.4.2018, http://www.eicar.org/86-0-Intended-use.html.

F-Secure 2017. Android threats in 2017. Viitattu 25.4.2018, https://business.f-secure.com/android-threats-in-2017.

F-Secure 2016. Deepguard. Viitattu 18.2.2018, https://www.f-secure.com/documents/10192/1656871/deepguard_whitepaper.pdf.

F-Secure 2018a. Freedome for Businessin käytön aloittaminen. Viitattu 23.4.2018, http://mobile.f-secure.com/psb/freedome/android/install_fin.html.

F-Secure 2018b. Protection service for business. Viitattu 23.4.2018, https://www.f-secure.com/fi_FI/web/business_fi/management-portal.

Järjestelmäpäällikkö 2018. Haastattelu 22.3.2018. Tekijän hallussa.

Järvinen, P. 2006. Paranna tietoturvaasi.1.Painos Jyväskylä: Docendo

Järvinen, P. 2012.Arjen tietoturva – vinkit & ratkaisut. Jyväskylä: Docendo

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas. Helsinki: Alma Talent

Kotipalli, S R. & Imran, M A. 2016. Hacking Android. Viitattu 25.4.2018, http://proquest.safaribooksonline.com.ezp.oamk.fi:2048/book/programming/android/9781785883149/9dot-android-malware/ch09lvl2sec99_html?uicode=ouluuas.

Microsoft 2018. About BITS. Viitattu 10.3.2018, https://msdn.microsoft.com/en-us/library/windows/desktop/aa362708(v=vs.85).aspx.

Oriyano, S-P. 2016. CEH v9 – Certified Ethical Hacker Version 9. Viitattu 25.4.2018, http://proquest.safaribooksonline.com.ezp.oamk.fi:2048/book/certification/ceh/9781119252245/chapter-8-malware/c8_2_html?uicode=ouluuas.

Sanastokeskus 2012. Laajakaistasanasto. Viitattu 18.2.2018, http://www.tsk.fi/tiedostot/pdf/Laajakaistasanasto.pdf.

Sanastokeskus 2017. TEPA-termipankki. Viitattu 18.2.2018, http://www.tsk.fi/tepa/fi/haku/nollap%C3%A4iv%C3%A4haavoittuvuus.

Viestintävirasto 2018. Tietoturvan vuosi 2017. Viitattu 18.2.2018, https://www.viestintavirasto.fi/attachments/cert/tietoturvakatsaukset/Tietoturvan-vuosi-2017.pdf.

HAASTATTELU KYSYMYKSET LIITE 1

1. Taustaa
    a. Kauan olet toiminut alalla ja kauan nykyisessä yrityksessä.
2. Mitä etuja keskitetty hallinta tuo haittaohjelmien torjunnassa?
3. Onko haittaohjelmilta suojautuminen muuttunut vuosien aikana?
4. Kuinka tärkeäksi koet mobiililaitteiden haittaohjelmien torjunnan?
    a. Android sekä iOS -käyttöjärjestelmät
5. Mitkä ovat mielestäsi suurimmat uhat haittaohjelmissa tällä hetkellä ja miten niiltä voidaan suojautua?
6. Kuinka tärkeänä näet päivitykset ohjelmissa sekä käyttöjärjestelmissä?
7. Mitkä asiat koet tärkeimmiksi tietoturvassa?
8. Miten tärkeänä näet yrityksen työntekijöiden tietoturvallisuustietoisuuden kouluttamisen ja onko yrityksessä koulutettu työntekijöitä tietoturvan osalta?
    a. Miten tietoturvatietoisuuden lisääminen on hoidettu.
9. Miten huolehdit omasta tietoturvaosaamisestasi?
10. Näkyykö tietoturvallisuus päivittäisessä tekemisessäsi?

F-SECURE PSB WORKSTATION SECURITY ASENNUS.BAT -SKRIPTI LIITE 2

Asennus skripti, joka oli GPO:lla käyttäjäkohtaisesti määritetty suoritettavaksi kirjautumisen yhteydessä.

```
Echo Off
Echo Tarkistetaan loytyyko F-Secure PSB
IF EXIST C:\F-SecureValmis.0 EXIT
Echo Kopioidaan F-Secure PSB WK koneen C:lle tiedostopalvelimelta
XCOPY \\filesrv\F-SecurePSB\* C:\F-SecurePSB\* /D
Echo Tarkistetaan loytyyko F-Secure Client Securitya koneelta
IF EXIST "C:\Program Files (x86)\F-Secure\FSGUI\fsavaui.exe" (
        Echo Poistetaan F-Secure Client Security
        START /WAIT C:\F-SecurePSB\UninstallationTool.exe -s -a --nogui --noreboot
        PRINT > C:\F-SecurePoistoOK.0
        shutdown -r -f -t 360 -c "Tietoturvaohjelmistoa p„ivitet„„n. Tietokone k„ynnistyy uudelleen
5 minuutin kuluttua t„m„n vuoksi."
        EXIT
) ELSE (
        Echo Asennetaan F-Secure PSB WS
        IF EXIST C:\F-SecurePoistoOK.0 START /WAIT C:\F-SecurePSB\fspsbwks.exe /SILENT
/K:XXXX-XXXX-XXXX-XXXX-XXXX /LANG:FIN /REBOOTDELAY:360
                PRINT > C:\F-SecureValmis.0
                EXIT
        )
```

VALMIS.VBS

Käyttäjälle lopussa tuleva ilmoituslaatikko, jossa kerrotaan tietoturvaohjelmiston päivittyneen. Tehty Visual Basic ohjelmointikielellä.

```
msgbox "Tietoturvaohjelmisto on päivitetty."
```

FREEDOME FOR BUSINESSIN KÄYTÖN ALOITTAMINEN

Nämä toimenpiteet tekemällä voit lisätä laitteesi F-Secure Protection Service -palveluun ja asentaa Freedome for Business -sovelluksen.

Freedome for Business tukee Android-versioita 4.0 ja uudempia. Toimenpiteet saattavat vaihdella hieman käytetyn laitteen ja alustaversion mukaan.

Kun saat asennussähköpostin F-Secure Protection Service for Businessilta:

Valitse laitteessa **Asetukset** > **Tietoturva** ja sitten **Tuntemattomat lähteet**.

Tuntemattomat lähteet -asetuksen valinta kannattaa poistaa F-Secure-laiteagenttisovelluksen asennuksen jälkeen.

1. Napauta sähköpostissa saamaasi **asennuslinkkiä**.

   Tämä lataa F-Secure-laiteagenttisovelluksen.

2. Siirry **ilmoitusalueelle** ja napauta ladattua sovellusta.

   Jos sinua pyydetään vahvistamaan F-Secure-laiteagentin edellyttämät oikeudet, jatka napauttamalla **Seuraava**.

3. Napauta **Asenna**.
4. Kun sovellus on asennettu, napauta **Avaa**.

   Jos sinua pyydetään vahvistamaan laitevalmistajan palveluehdot, jatka napauttamalla **Vahvista**.

5. Salli PSB-järjestelmänvalvojan hallita laitettasi napauttamalla **Aktivoi**.

   Laitteesi on nyt muodostanut yhteyden PSB-tiliisi. Freedome for Business -sovellus siirretään laitteeseesi pian.

6. Jos laitteesi ei asenna Freedome for Business -sovellusta automaattisesti:

   a. Etsi -kuvake **ilmoitusalueelta**.

      Tällä alueella näkyy uusi F-Secure-laiteagentin ilmoitus, joka on tässä tapauksessa ilmoitus Freedome for Business -sovelluksen latautumisesta. Sen näkyviin tuleminen saattaa kestää jopa 15 minuuttia sijainnistasi ja verkkoyhteydestä riippuen.

   b. Napauta ja napauta sitten **Asenna sovellus**.
   c. Napauta **Asenna**.
   d. Kun sovellus on asennettu, napauta **Avaa**.

   Jos laitteesi asentaa sovelluksen automaattisesti, avaa sovellus napauttamalla Freedome-kuvaketta.

7. Kun Freedome for Business on avattu:

   - Voit katsoa lyhyen Freedome-opetusohjelman, jos et ole käyttänyt sovellusta aiemmin. Valitse **Aloita opetusohjelma**.
   - Jos tunnet jo ohjelman ja haluat ohittaa opetusohjelman, napauta **Ohita opetusohjelma**.

8. Napauta **Palvelun ehdot** -sivulla **Hyväksy**.
9. Ota suojaus käyttöön napauttamalla valintakiekon keskiosaa.
10. Valitse vahvistusikkunassa **Luotan tähän sovellukseen** ja napauta **OK**, jotta Freedome voi luoda VPN-yhteyden ja käsitellä verkkoliikenteen.

Kun VPN-yhteys on aktiivinen, laitteesi ja tietosuojasi suojaus on käytössä.

(F-Secure 2018a, Viitattu 10.3.2018.)