KANNETTAVAN LAITTEEN TIETOTURVA

Case:Vulganus Oy

LAHDEN AMMATTIKORKEAKOULU
Liiketalouden laitos
Tietojenkäsittelyn koulutusohjelma
Yritysviestintäjärjestelmät
Opinnäytetyö AMK
Kevät 2009
Janne Laaksonen

Lahden ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma

LAAKSONEN, JANNE: Kannettavan laitteen tietoturva
Case: Vulganus Oy

Yritysviestintäjärjestelmien opinnäytetyö, 38 sivua, 2 liitesivua
Kevät 2009

TIIVISTELMÄ

Opinnäytetyö käsittelee kannettavia laitteita yleisesti ja kannettavien laitteiden tietoturvaa. Opinnäytetyössä selvitetään, mitä Vulganus Oy:n tulisi huomioida suunnitellessaan kannettavien laitteiden tietoturvaratkaisuja. Siinä kartoitetaan yrityksen tämänhetkinen kannettavien laitteiden tietoturvan taso. Lisäksi tehdään selkeä ohjeistus ja tietoturva-analyysi.

Kannettava laite-luvussa kerrotaan, mitä kannettavalla laitteella tarkoitetaan. Kannettavan laitteen tietoturva-osio on opinnäytetyön tärkein luku. Siinä käsitellään muun muassa kannettavien laitteiden tietoturvaa ja sen merkitystä. Työssä selvitetään myös mitkä asiat pitää huomioida, jotta yrityksen tietoturva on kohdallaan.

Luvussa tietoturva-määritykset käsitellään yleisimpiä tietoturvaprotokollia ja salauksia. Kohdeyritys-osiossa käydään läpi lyhyesti case-yrityksen, Vulganus Oy:n, kannettavien laitteiden ja kuljetettavien tallenteiden esittely.

Opinnäytetyön empiirinen osuus toteutettiin Vulganus Oy:lle haastatteluiden avulla. Niiden avulla pyrittiin selvittämään lähemmin, miten nykyinen tietoturvan taso kannettavien laitteiden osalta toimii tällä hetkellä ja mitä kehitettävää siinä on.

Opinnäytetyön keskeisiä tuloksia oli, että kannettavien laitteiden tietoturvan tasoa halutaan parantaa ja hyödyntää paremmin. Analyysin perusteella voidaan päätellä, että Vulganus Oy:n kannettavat laitteet toimivat hyvin, mutta tietoturvassa ja sen hyödyntämisessä on parantamisen varaa.

Avainsanat: kannettava laite, tietoturva, tietoturvaprotokollat

Lahti University of Applied Sciences
Degree Programme in Computing

LAAKSONEN, JANNE: Portable device information security
Case: Vulganus Oy

Bachelor's Thesis in Business Information Systems, 38 pages, 2 appendices

Spring 2009

ABSTRACT

This bachelor's thesis deals with different portable devices and also portable device information security. This study explores what companies should take into consideration when they are planning their portable device information security and investigates Vulganus Oy's present portable device information security level, creates clear directions and a security analysis.

There are three sections in the theory part. First the portable device section explains what a portable device means. The second part on portable device information security is the most important part of this thesis. It discusses among other things portable information security, meaning and also_ what should be taken into consideration in order for the company's information security to be in order.

Third, the security specifications section introduces the most common information security protocols and encryption methods. The target company section contains a brief company presentation of Vulganus Oy, portable device swot-analysis, information security analysis and also information security directions.

The empirical part of the thesis was conducted for Vulganus Oy, via interviews. The interviews attempted to find out more closely how well the existing information security in portable devices was functioning and also what development needs there were.

The survey pointed out_that the level of portable device information security could be improved and also exploited more. On the grounds of the analysis Vulganus Oy's portable devices functioned well, but information security and also its exploitation needed improvement.

Keywords: portable device, information security, information security protocols

SISÄLLYS

SANASTO

Autentikointi= Käyttäjän tunnistus.

DWG = Suunnitteluohjelman tiedostotyyppi.

Defacto-menetelmä = Kun uusia tuotteita halutaan käyttöön nopeammin kuin niitä ehditään standardoida, syntyy yleensä de facto -standardi. Tyypillisiä De Facto -standardien luojia ovat yritykset.

DOC = Document, tiedostopääte, jota esimerkiksi MS-Word käyttää.

DXF = Autocad-ohjelman tiedostotyyppi.

GIF = Graphic Interchange Format, kuvan tallennus muoto.

IPSec-protokolla = Määrittelee tietoliikenneprotokollia, jotka voidaan jakaa kahteen luokkaan: protokollat pakettivirtojen turvaamiseen ja avaintenvaihtoprotokolla turvattujen pakettivirtojen muodostamiseen.

JPG = Joint Photographic Experts Group, kuvan tallennusmuoto.

Mobiilisuus =Liikuteltava sopeutuva muuttuviin käyttötilanteisiin.

Multipleksi = Monistaa saman tiedon useaan eri osoitteisiin.

PDA-laite = Kämmentietokone.

PDF = Portable Document Format, acrobatin käyttämä tiedostotyyppi. PDF-tiedostomuoto soveltuu valmiiden julkaisujen siirtämiseen tietojärjestelmistä toiseen.

PPT = Power Point Table on Microsoftin esitysgrafiikkaa varten kehittämä tiedostomuoto, jota käytetään Microsoft Power Point –ohjelmassa.

Protokolla = Protokolla eli yhteyskäytäntö on käytäntö tai standardi, joka määrittelee tai mahdollistaa laitteiden tai ohjelmien väliset yhteydet.

PSD = Photoshop-ohjelmiston kuvatiedostomuoto.

RAR = Tiedostonpakkaukseen ja arkistointiin tarkoitettu tiedostomuoto.

S-HTTP = Mahdollistaa yleisen tietoturvaprotokollan transaktiosovelluksiin.

SSH2 = Mahdollistaa yhteyksien suojaamisen kaikissa istunnon vaiheissa ja siten sitä voidaan käyttää myös hajautetuissa sovelluksissa tietoturvaratkaisuna.

SSL = Secure Socets Layer-menetelmä mahdollistaa kahden eri sovelluksen välisen turvallisen tiedonsiirron.

Tiedostotyyppi = Ilmoittaa tallennetun tiedostomuodon ja käytetyn ohjelman.

TLS = On IETF:n standardi, joka on kehitetty SSL:n pohjalta. TLS:n koostuu kahdesta tavoitteesta, joita ovat tiedonsiirron yksityisyys ja tiedon eheys.

USB-laite = Universal Serial Bus, sarjaväylä, joka mahdollistaa oheislaitteen liitämisen.

VPN-yhteys = Tarkoittaa kahden intranetin tai etäkäyttäjän ja intranetin turvallista yhdistämistä toisiinsa turvattoman verkon, Internet kautta.

WPA = Wi-Fi Protected Access on välivaiheen tietoturvatekniikka, joka kehitettiin WEP-salauksen ongelmien paljastuttua.

WLAN = Wireless Local Area Network, eli langaton lähiverkko.

XLS = Microsoftin Excelillä luotu taulukkolaskentatiedosto.

ZIP = Tiedonpakkausmenetelmä. Siihen liittyvä tiedostopääte on .ZIP.

1 JOHDANTO

Kannettavan laitteen käyttäminen on osa nykypäivän liiketoimintaa. Suurin osa ihmisistä käyttää kannettavaa laitetta viestimiseen. Tällainen muutos on tapahtunut yhteiskunnassamme hyvin nopeasti viime vuosien aikana. Yrityksien työntekijöistä suurella osalla on käytössään kannettava laite, esimerkiksi tietokone tai jokin mobiililaite.

Välineiden ja tietoturvan kehittyminen on mahdollistanut kannettavien laitteiden ostamisen. Yrityksien päivittäessään ja uudistaessaan laitekantoja kiinnitetään huomiota yhä enemmän myös kannettavien laitteiden tietoturvan merkitykseen ja sen toimivuuteen.

Yrityksien siirtyminen enemmän kannettaviin laitteisiin on tuonut tietoturvan alalle myös uusia uhkia, jotka ovat tyypillisiä vain langattomalle siirtomedialle ja tätä mediaa käyttäville päätelaitteille. Uudet uhkat kohdistuvat esimerkiksi käytettyyn siirtomediaan, laitteiden sisältämään tiedon turvaamiseen, laitteiden luotettavuuteen ja siihen, että laitteet eivät ole fyysisesti yhdessä paikassa.

Yritysten yhtenä haasteena on se, miten yritykset pystyisivät varautumaan kaikkiin uhkiin tulevaisuudessa paremmin. Erilaiset uhkat ovat yrityksille suurimpia tietoturvariskejä, minkä vuoksi yritysten tulisikin ottaa huomioon omat resurssinsa tietoturvaa suunniteltaessa. Tietoturva on olennainen osa yrityksen toimivuutta. Jos yrityksen tiedot päätyvät yrityksen sisältä ulkopuolisille henkilöille, voivat seuraukset olla kohtalokkaita. Pahimmassa tapauksessa tietovuoto voi aiheuttaa suuria taloudellisia haittoja yritykselle.

Hyvänä esimerkkinä on kilpaileva yritys, joka huonon tietoturvan vuoksi pääsee käsiksi toisen kilpailevan yrityksen tuotteiden suunnittelumateriaaliin tai asiakastietokantoihin. Tietoturvariskejä ei tule aliarvioida, koska tietovuodon jo tapahduttua on liian myöhäistä eikä tehtyä saa tekemättömäksi. Näin ollen on tärkeää, että yritys on tietoinen kaikista tietoturvariskeistä ja pitää tietoturvaansa ajan tasalla.

2 TUTKIMUKSEN TAUSTAA

2.1 Tutkimuksen lähtökohdat

Opinnäytetyössäni, Kannettavan laitteen tietoturva, tarkastellaan Vulganus Oy:n tämänhetkisten kannettavien laitteiden tietoturvan tasoa ja niiden merkitystä yrityksessä. Aiheeni tähän opinnäytetyöhöni sain ollessani työharjoittelu-jaksolla kyseisessä yrityksessä, jolloin tein myös projektiopintoja yritykselle. Huomatessani monen Vulganus Oy:n työntekijän käyttävän kannettavia laitteita työpaikalla sekä työmatkoilla heräsi kiinnostukseni kannettavien laitteiden tietoturvaa kohtaan.

Opinnäytetyöni tarkoituksena on tutkia Vulganus Oy-yrityksen kannettavien laitteiden tietoturvatason laatua. Opinnäytetyöhöni keräsin tietoa eri kohderyhmien käyttökokemuksista ja tutkin kannettavan laitteen tietoturvan sisältöä siitä, mitä sen on vähintään sisällettävä. Tutkimuksessa keskityn kannettavan laitteen tietoturvan merkitykseen yrityksessä.

Vulganus Oy toivoo tämän opinnäytetyön auttavan heitä selventämään nykyisten kannettavien laitteiden tietoturvan tilannetta sekä saamaan lisää tietoa tietoturvan eri mahdollisuuksista. Tutkimuksen tulokset otetaan huomioon erityisesti kannettavien laitteiden tietoturvaa suunniteltaessa ja parannettaessa.

Aihe on tutkimisen arvoinen, koska kannettavien laitteiden tietotekniikan ratkaisut, tietoverkot ja palvelut kehittyvät koko ajan. Tietoturvalla on tällöin suuri merkitys yrityksessä. Yrityksien kannattaa miettiä tarkkaan tietoturvaratkaisujen vaihtoehtoja, jolloin myös mahdolliset virheet tulee huomioitua paremmin. Tietotekniikka ei tule häviämään, vaan kehittyy koko ajan eteenpäin. Tämän vuoksi yrityksien tulee huomioida tietotekniikan jatkuva kehittyminen ja sen vaikutus tietoturvaratkaisuihin.

2.2 Tutkimusongelma ja rajaus

Yrityksen kannettavien laitteiden tietoturvassa havaittiin erilaisia näkemyksiä siitä, kuinka laitteiden tietoturvan tulisi toimia. Yhteisillä kannettavien laitteiden tietoturvaohjeilla koko henkilökunta pystyisi toimimaan samalla tavalla. Opinnäytetyössä tutkin, miten tämän hetken tietoturvan voisi toteuttaa paremmin kannettavien laitteiden osalta. Tutkin myös sitä, miten tietoturvasta olisi kaikille kannettavia laitteita käyttäville mahdollisimman paljon hyötyä. Tutkimustulosten perusteella ja yrityksen mahdollisten tarpeiden mukaan luodaan kannettavien laitteiden tietoturvaohjeistus.

Opinnäytetyö on rajattu niin, että case-tutkimus keskittyy Vulganus Oy:n tämän hetken tietoturvaan kannettavien laitteiden osalta. Tietoturvamääritykset on tärkeää tehdä oikein ja yrityksen tarpeita huomioivalla tavalla, sillä tietoturvan on toimittava joka päivä. Tietoturvan toimiessa yritys pystyy luottamaan siihen, etteivät tiedot pääse palvelimelta ulkopuolisille, jolloin yritys pystyy keskittymään paremmin ydinosaamiseensa eikä siihen, ovatko tiedot oikeassa paikassa.

Tietoturvamääritykset voidaan määrittää tietoturvastandardien ja salauksien avulla. Teoriaosuudesta olen jättänyt pois yleisen tietoturvan selvittämisen. Olen rajannut teoriaosuuden niin, että aihe käsittelee mahdollisimman läheisesti case-tutkimusta eli kannettavan laitteen tietoturvaa. Opinnäytetyöhöni olen valinnut tarkasteltavaksi Vulganus Oy:n kannalta tärkeimmän kannettavan laitteen eli kannettavan tietokoneen. Työssäni tarkastelen myös matkapuhelinta ja PDA-laitetta.

2.3 Tutkimusmenetelmät

Tutkimuksen lähestymistapana on kvalitatiivinen tutkimusmenetelmä. Kvalitatiivisena menetelmänä käytin haastatteluja. Haastateltaviksi valitsin henkilöt, joilla oli käytössä kannettava laite. Haastateltavia oli yhteensä seitsemän henkilöä. Haastattelin kyseiset henkilöt siksi, jotta saisin tarkat tiedot siitä, miten tietoturva on aikaisemmin hoidettu ja siitä, mitä siihen toivottaisiin lisää. Tein haastattelut yksilöhaastatteluina. Haastattelut mahdollistivat myös sen, että pystyin myöhemmin tekemään tarkentavia ja syventäviä jatkokysymyksiä haastateltaville. Lisäksi kartoitin mitä tietoturvaratkaisuja yrityksellä on jo entuudestaan käytössä kannettavissa laitteissaan.

3 KANNETTAVA LAITE

3.1 Kannettavan laitteen määritelmä

Terminä kannettava laite tarkoittaa laitetta, joka ei ole fyysisesti kiinni toimistossa ja jonka voi ottaa mukaan esimerkiksi liikematkalle. Kannettavaa laitetta voi kuvata sanoilla villi, vapaa ja haavoittuva. Tällainen kannettava laite on yleensä sellainen, mikä tyydyttää laitetta käyttävän ihmisen vaatimukset.

Huonon tietoturvan takia kannettava laite voi olla ongelmallinenkin. Nykyään kannettavan laitteen ominaisuudet vastaavat jo kiinteiden pöytäkoneiden ja oheislaitteiden tasoa. Kannettavia laitteita ovat esimerkiksi kannettava tietokone, USB-muistit, ja monet mobiililaitteet, jotka voidaan jakaa erilaisiin älypuhelimiin ja PDA- laitteisiin.

KUVIO 1. Kannettava tietokone

KUVIO 2. USB-muistit

KUVIO 3. PDA-laite, kämmentietokone

Kannettava tietokone (KUVIO1) on helppo kuljettaa paikasta toiseen. Kannettavalla pystytään säästämään tilaa sekä niissä on alhainen virrankulutus. Toisessa kuviossa (KUVIO 2), on USB-muistikortti ja (USB-muistitikku). USB-laitetta on helppo kuljettaa mukana: vie vähän tilaa, soveltuu hyvin tiedon siirtämiseen ja niihin voi tallentaa suuria määriä tietoa.

Kuviossa 3 on esitelty PDA-laite. PDA-laite on kädessä pidettävä kannettava tietokone. USB-laitteiden lisäksi PDA-laitteitakin on helppo kuljettaa mukana, sillä ne vievät vähän tilaa. Laite ei ole kuitenkaan yhtä tehokas kuin kannettava tietokone.

3.2. Kannettavan laitteen SWOT-analyysi

SWOT-analyysiin on kirjoitettu kannettavien laitteiden vahvuudet ja heikkoudet tietoturvan näkökulmasta. Taulukosta näkee sen, mitä yleisellä tasolla voidaan ajatella kannettavista laitteista.

Vahvuudet	**Heikkoudet**
• liikuteltavuus • pieni koko • keveys • monipuolinen yhteys • käyttäjä	• tietoturva • hinta • suorituskyky • toimintavarmuus • käyttäjä
Mahdollisuudet	**Uhat**
• etätyö • siirtomedia	• tietomurrot • kannettavien tallenteiden suojausta ja tietoturvaa vaikea valvoa • varkaudet

TAULUKKO 1. SWOT-analyysi kannettavista laitteista

Taulukon yksi mukaan voidaan havaita kannettavien laitteiden vahvuuksiksi laitteen helppo liikuteltavuus: laite ei ole fyysisesti missään paikassa kiinni. Kannettavan laitteen pieni koko ja keveys mahdollistavat laitteen helpon kuljetettavuuden ja työn tekemisen paikasta riippumatta. Vahvuutena taulukon yksi mukaan on myös kannettavan laitteen helppous muodostaa yhteys Internetiin.

Kannettavan laitteen heikkoutena taulukon yksi mukaan on laitteessa mahdollisesti epäkunnossa oleva tietoturva. Muita heikkouksia kannettavissa laitteissa ovat korkea hintataso sekä mahdollisesti huonompi ja hitaampi suorituskyky verrattaessa tavalliseen pöytäkoneeseen. Toimintavarmuus voidaan lukea mahdolliseksi heikkoudeksi kannettavalle laitteelle. Myös itse laitteen käyttäjä voidaan lukea mahdolliseksi heikkoudeksi tai vahvuudeksi.

Erilaisia kannettavan laitteen mahdollisuuksia taulukon yksi mukaan löytyi muutama. Mahdollisuutena on työskentelyn riippumattomuus tietystä ajasta ja paikasta eli niin sanottu etätyön tekemisen parempi mahdollistaminen. Uhkana kannettavissa laitteissa ovat tietomurrot tietoturvan ollessa epäkunnossa. Uhiksi voidaan lukea myös kannettavan tallenteen suojaamisen ja tietoturvan vaikea valvonta. Tämä uhka johtuu suurimmaksi osaksi käyttäjien unohtelevaisuudesta: usein käyttäjät unohtavat suojata kannettavan laitteensa. Yleisenä kannettavan laitteen uhkana ovat myös erilaiset varkaudet.

4 KANNETTAVAN LAITTEEN TIETOTURVA

4.1 Fyysinen suojaaminen

Kannettavan laitteen fyysinen suojaaminen yleisesti käsittää organisaatioiden tuotanto- ja toimitilojen suojaamisen. Tärkeä asia kannettavien laitteiden fyysisessä suojaamisessa on tietojen kuljettamisjärjestelyjen turvallisuus. Yrityksissä esimerkiksi kannettavat laitteet tulisi suojata yhtä hyvin kuin kiinteätkin laitteet. Kannettavien laitteiden fyysisessä suojaamisessa tulee muistaa myös se, että varas voi viedä laitteesta esimerkiksi pelkän kiintolevyn.

4.1.1 Kannettavan tietokoneen, matkapuhelimen ja PDA-laitteen suojaaminen

Nykyään kannettavien laitteiden fyysisen tietoturvan ongelmia ovat esimerkiksi varastaminen ja tietojen huono tuhoaminen laitteiden poistuessa käytöstä. Tietoturvallisuuden merkitys kannettavien laitteiden kohdalla korostuu entisestään. Kannettavilla laitteilla tulee olla yhtä hyvä tietoturvallisuuden ja suojaamisen taso kuin esimerkiksi toimistossa sijaitsevalla pöytäkoneellakin.

Kannettavan laitteen ollessa suojaamaton, ohjelmiston ollessa pois päältä, tietoturvan puuttuminen tai sen päivittämättömyys ovat suuria uhkia haittaohjelmien leviämiselle. Suojaamattomana kannettavat tietokoneet, matkapuhelimet ja PDA-laitteet voivat aiheuttaa haittaohjelmien leviämisen. (Kannettavien laitteiden tietoturva, 2008.)

Kannettavan tietokoneen tietoturvassa tulee ottaa huomioon monta asiaa. Työhuoneet tulee olla lukittuina, ellei kukaan henkilöstöön kuuluva ole tilassa. Kannettavat tietokoneet tulee lukita työpöytään kiinni esimerkiksi vaijerilla. Julkisilla paikoilla on hyvä käyttää näytönsuojaa henkilökohtaisia töitä tehdessä, jotta lähellä olevat ulkopuoliset henkilöt eivät saa yritykselle ja sen henkilökunnalle kuuluvia tietoja. Yrityksen on hyvä turvamerkitä kaikki yrityksensä kannettavat tietokoneet. Kannettavien koneiden tiedostot ja

tiedostojärjestelmät tulisi salata, jolloin varkauden sattuessa tiedostojen salaus vaikeuttaa laitteen tiedostojen avaamista. (Pikaopas, 2008.)

Yksi hyvin tärkeä asia on huolehtia kannettavan laiteen tietoturvan minimitasosta. Minimitasoon kuuluvat muun muassa haittaohjelmien poistotyökalu, virustentorjuntaohjelma sekä palomuuri. Käyttöjärjestelmien suojaustoimenpiteet ovat yksi osa minimitason osa-aluetta, johon kuuluu ohjelmistopäivitysten eli käyttöjärjestelmien ja ohjelmistojen säännölliset päivitykset. Varmuuskopiointi tiedostoista tulee tehdä kerran viikossa. (Tietoturvan minimitaso, 2008.)

Kannettavan laitteen tietoturvassa on hyvä huomioida myös arkaluontoisten tietojen tallennus, mikä tulisi tehdä salakirjoitusta käyttäen. Matkalle kannattaa ottaa mukaan vain ja ainoastaan tarpeelliset tiedostot. Laitteen merkki, malli, sarjanumero ja verkkosovitin eli MAC-osoite tulee ottaa itselle muistiin. Käyttäjätunnuksia ja salasanoja ei kannata tallentaa valmiiksi ohjelmien kirjautumisikkunoihin. Kannettavan tietokoneen kiintolevylle kannattaa päähakemistoon tehdä piilotettu ja kirjoitussuojattu tiedosto, josta ilmenee omistajan tiedot. (Pikaopas, 2008.)

Matkapuhelimen tietoturvassa olennaisena osana tulee huomioida se, että käyttäessä eri yhteyksiä pitäisi aina muistaa myös suojata yhteydet. Hyvänä esimerkkinä tästä on puhelimen bluetooth-toiminto. Käytettäessä kyseistä toimintoa tulisi muistaa suojata salasanalla yhteys tai mahdollisesti laittaa puhelimen näkyvyys piilotetuksi. Bluetoothtia käytettäessä voi puhelin vastaanottaa viruksen tai muun haittaohjelman, mikäli puhelimen yhteyttä ei ole asianmukaisesti suojattu.

Edellä mainitut säännöt pätevät matkapuhelimiin samoin kuin isompiinkin mobiililaitteisiin, kuten esimerkiksi PDA-laitteisiin. On olemassa muutamia mobiililaitteiden suojaustapoja, kuten Saferegin-tarrat, joiden avulla pystytään suojaamaan muun muassa matkapuhelimia. Safereg tarjoaa monipuoliset hakumahdollisuudet käyttäjäkohtaisista laitetietokannoista sekä myös tietokannan siirtomahdollisuuden aina yrityksen omiin tietojärjestelmiin asti. Järjestelmään on mahdollista saada organisaatiokohtainen pääkäyttäjätunnus, jolloin organisaation

normaalikäyttäjät hallinnoivat omaa laitetietokantaansa henkilökohtaisesti. Pääkäyttäjä puolestaan hallinnoi organisaation kaikkia laitetietoja ja tiedostoja. (Safereg, 2009.)

Järjestelmä koostuu yksilöllisesti turvamerkityistä tuotteista sekä uudesta teknologiaan perustuvasta Internetin kautta ylläpidettävästä tietokantapohjaisesta hallintajärjestelmästä. Varkauden sattuessa tietokantaan on helppoa ja nopeaa muuttaa laitteen tila varastetuksi. Järjestelmä on siis reaaliaikainen. (Safereg, 2009.)

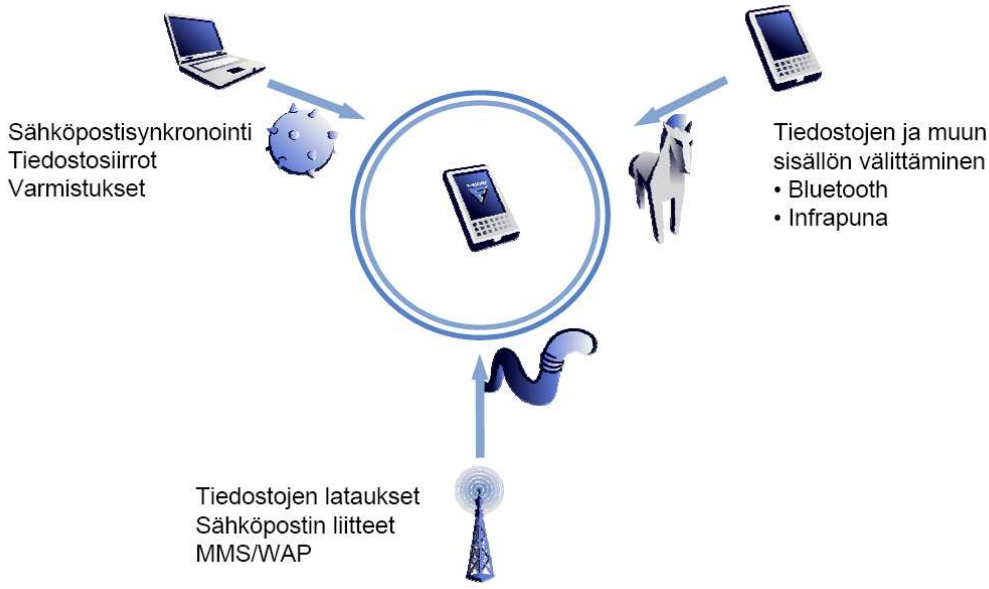
Toinen nykyaikana yleistymään päin oleva suojaustekniikka on sormenjälkitunnistin, jonka voi nähdä uusimmissa mobiililaitteissa. Ideana kyseinen suojaustekniikka on hyvä, mutta asetusten ollessa määritetty liian korkeiksi, ei suojaustekniikka kuitenkaan ole käytännössä kovinkaan toimiva. (Uski, 2008, 46-47.)

Edellä mainitussa suojaustekniikassa sormenjäljelle voi asettaa käyttäjäkohtaisen turvatason, joka määrittää, miten tarkasti jäljen on täsmättävä, jotta suojaustunnisteen saa käyttöönsä. Tämän turvatason asettaminen korkeimmalle tasolle tarkoittaa parhainta tietoturvaa tietoturvan tasoa. Samalla suojaustekniikka lisää myös virheellisten sisäänkirjautumis-yritysten riskiä. (Lisäturvaa sormenjäljellä, 2008.)

PDA-laitteessa tietoturvariski on suurempi, verrattuna normaaliin matkapuhelimeen, koska PDA-laite käyttää monipuolisempia sovelluksia ja sen käytettävyys alkaa vastata normaalia tietokonetta. PDA-laite tulee suojata samanlaisella periaatteella, mitä kannettava tietokonekin. Tietoturvayrityksillä on tarjota myös PDA-laitteisiin tarvittavia tietoturvaratkaisuja. Esimerkiksi F-Securella on tarjota PDA-laitteeseen virus- ja haittaohjelmilta suojaava tietoturvaratkaisu.

Kuviossa neljä on kuvattu PDA-laitteiden käyttömahdollisuuksia. PDA-laite on avainasemassa, sillä siihen pystytään siirtämään erilaisista laitteista tietoa. Kannettavasta tietokoneesta pystytään esimerkiksi synkronisoimaan sähköposteja,

tiedostojensiirtoja ja erilaisia varmistuksia. Matkapuhelimesta tietojen välittäminen PDA-laitteeseen tapahtuu bluetoothin tai infrapunan avulla. Tiedostojen erilaiset lataukset esimerkiksi sähköpostien liitteet voidaan PDA-laitteeseen siirtää mastolinkin avulla.

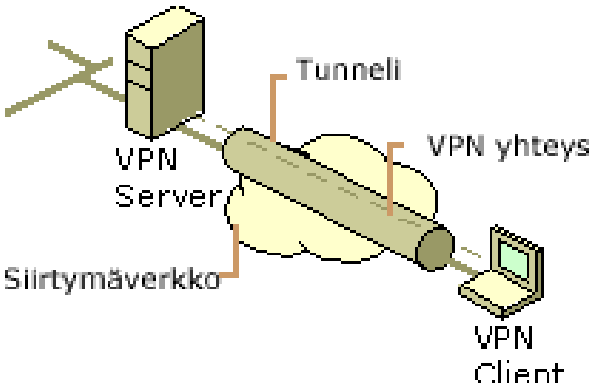


KUVIO 4. Työasemien tietoturvan parhaat käytännöt ja hallinta. (2008.)

4.1.2 Yhteyksien tietoturva ja varautuminen

Yhteyksien tietoturvallisuuteen voi varautua sillä, että tiedostaa riskit ja pyrkii välttämään niitä, esimerkiksi yritysten tulisi suojata kannettavat laitteensa aina salasanoilla tai koodeilla.(Kannettavien laitteiden tietoturva, 2008).

Lisäksi käytettäessä WLAN-yhteyksiä on syytä suojata WLAN-tukiasemat asianmukaisesti esimerkiksi WPA-salauksella sekä valita salasanaksi sellainen, joka vaikeuttaa tiedostoon hakkeroitumista. Yrityksen käyttäessä VPN-yhteyttä on riskinä tietomurto, mikäli laite joutuu ulkopuolisten käsiin. VPN-yhteys koostuu alla olevan (KUVIO 5) osatekijöiden mukaan.



KUVIO 5. VPN yhteyden osatekijät. (VPN 2008.)

VPN-yhteys muodostetaan käyttäjän koneelta eli VPN Clientiltä VPN Serverille. Näin syntyy suojattu yhteys eli tunneli, jota on hyvin vaikea murtaa. Tietomurto on nykyisillä VPN-yhteyksillä vaikeaa, muttei mahdotonta. Tietomurron onnistuessa on yrityksen arka tieto helposti kopioitavissa ja tuhottavissa.

4.1.3 Lisälaitteiden tietoturva ja varautuminen

Lisälaitteiden tietoturvassa pitää kiinnittää huomiota siihen, että laitteet on suojattu asianmukaisesti. Muistitikkua käytettäessä tulisi muistitikku muistaa salata. Muistitikkujen uusimmissa ja tunnetuissa merkeissä tulee mukana nykyään myös salaus, virus tai tietoturvaohjelma. Muistitikun jouduttua vääriin käsiin, on sitä mahdoton käyttää ilman oikeaa salasanaa.

Kannettavaa laitetta ja muita lisälaitteita käytettäessä muuallakin kuin työpaikalla, esimerkiksi myös kotona ja työmatkoilla, olisi hyvä tehdä säännöllinen täystarkistus asianmukaisella tietoturvaohjelmistolla. Tietoturvaohjelmisto tutkii laitteen läpikotaisin ja etsii mahdolliset haitta- ja virusohjelmat. Hyvä on myös varautua uusimaan mahdollisuuksien mukaan salasanat ja mahdollisesti käyttää eri salasanoja lisälaitteissa. Riski on aina olemassa, kun lisälaitteita käytetään, mutta hyvillä turvaohjelmilla ja henkilökunnan tietoturvaohjeistuksella tietoturvariskejä pystytään pienentämään. Yrityksen tietoturva on yhtä mitä yrityksen henkilökunnan tieto ja taito.

4.2 Käyttäjätunnukset ja salasanat

Kannettavan laitteen käyttäjätunnuksille on hyvä tietyn määräajan kuluessa antaa uusi salasana umpeutuvan salasanan tilalle ja näin ollen mahdollistaa tietoturvan parempi suojaus. Lisäksi eri käyttäjätunnuksille on hyvä luoda eri oikeuksia. Eri oikeudet on hyvä luoda siksi, ettei eri tasoisilla työntekijöillä voi olla samat oikeudet, esimerkiksi johtajalla ja sihteerillä ei voi olla samoja käyttöoikeuksia, sillä heidän työtoimenkuvansa on erilainen. Jos vain johdon käytössä on jokin yrityksen tieto tai kansio, niihin tiedostoihin ei ole muilla oikeuksia.

Samaa periaatetta kannattaa käyttää yleisesti, eli rajoittaa oikeudet vain niihin, mitä käyttäjätunnuksen omaava henkilö tarvitsee. Jos on suunnittelija, niin ei tarvitse päästä markkinoinnin tietoihin ja niin edelleen. Näillä toimenpiteillä ehkäistään inhimillisiä erehdyksiä ja sitä, ettei tärkeä tieto katoa tai tuhoudu. Ulkopuolisen päästäessä käyttäjätunnuksilla tiedostoihin sisälle, ei hänen olisi mahdollista kuitenkaan saada koko yrityksen tietoja haltuunsa.

4.3 Tiedostojen ja kansioiden jakaminen

Kannettavan laitteen tiedostot ja kansiot voidaan jakaa kiintolevylle tai muistiin, laitteesta riippuen. Tiedon voi salata osittain tai kokonaan. Salattuun tietoon pääsee käsiksi käyttäjän valitsemalla salasanalla, mutta myös ulkoisia, esimerkiksi USB-porttiin kytkettäviä tunnistusmenetelmiä, voidaan käyttää.

Osittain salaamisessa kiintolevylle tai muistikortille luodaan virtuaalinen asema, joka näkyy käyttäjälle kuten normaali asema, mutta todellisuudessa asema on kuitenkin salattu tiedosto. Silloin tiedon salaus tapahtuu yksinkertaisesti siirtämällä tieto salatulle asemalle.

Toinen mahdollisuus on salata koko kiintolevy tai muistikortti, jolloin myös kaikki väliaikaiset tiedostot ja tyhjä tila salataan. Tällöin salaus puretaan laitteen käynnistyksen yhteydessä, jolloin käyttäjältä kysytään käyttäjätunnus ja salasana. Koko levyn salaus ei oleellisesti hidasta laitteen käyttöä tai käynnistymistä, sillä salauksen purku tapahtuu käytön taustalla. (Kannettavan tietokoneen tietoturva, 2008.)

4.4 Tiedonkäsittely

Kannettavan laitteen tiedonkäsittelyssä tulee huomioida tiedon suojaaminen. Tietojen pitää pysyä hyvässä tallessa ja poistetut tiedot pitää pystyä tuhoamaan lopullisesti. Tiedonkäsittelyn ja suojaamisen avulla pystytään varmistamaan se, että tietoon ei pääse käsiksi muut henkilöt kuin sille tiedolle määritetyt henkilöt. Tiedot tulee suojata tiedon tärkeyden perusteella. (Tiedonkäsittely, 2008.)

Todella tärkeää tietoa ei ole välttämättä hyvä säilyttää kannettavassa laitteessa. Yrityksen on hyvä ohjeistaa henkilökuntaansa siitä, mitä tietoja kannettavassa laitteessa saa säilyttää ja tallentaa sekä miten tiedot tulee suojata. Hyvä on salata ainakin kaikki työtiedostot, sovellusohjelmat ja sähköpostit, jotka saattavat sisältää henkilökohtaista tai yrityksen sisäistä tietoa. (Tiedonkäsittely, 2008.)

4.5 Varmuuskopiointi

Olisi hyvä varmuuskopioida kannettavan laitteen kaikki tärkeät tiedostot säännöllisesti. Varmuuskopioinnissa pitää muistaa myös kopioida sähköpostin tiedostot ja selaimen kirjainmerkit, jotka eivät tallennu automaattisesti omiin tiedostoihin. Lisäksi kannattaa varmuuskopioda aina Omat tiedostot-kansio viikoittain. (Korpela, 2005, 98.)

Varmuuskopiointi onnistuu esimerkiksi kopioimalla tiedostot yrityksen verkossa olevalle ulkoiselle kovalevylle. Varmuuskopiointi korostuu nykyään, koska kannettavia laitteita varastetaan enemmän kuin kiinteitä. (Korpela, 2005, 98.)

Varmuuskopiot on hyvä säilyttää eri tilassa kuin itse kannettava laite. Kannettavien laitteiden varmuuskopioinnissa tulee muistaa aina, että varmuuskopiot tarjoavat helpon kohteen tietovarkauksille, sillä murtautuneen henkilön ei tarvitse saada kuin yksi varmuuskopio, jonka jälkeen hänen on käytännössä mahdollista saada kaikki laitteen tiedostot ilman laitteen varastamista. On siis muistettava suojata myös varmuuskopiot salasanalla tai muulla käyttäjäkohtaisella rajoituksella. (Boström, 2003, 101.)

4.6 Langattomat verkot

Matkoilla kannattaa vieraita tietoliikenneyhteyksiä ja langattomia verkkoja käyttää varoen. Langattomat verkot kannattaa sulkea ja poistaa tarpeettomat esimerkiksi ulkoiset levyasemat, kun niitä ei käytä. (Pikaopas, 2008.)

Langattomista verkoista julkisia verkkoja voi käyttää normaaliin tiedonsiirtoon ilman huolta, jos tietokoneen tietoturvasta on huolehdittu ainakin minimitason verran. Palomuuri pitää olla myös oikein säädettynä. Turvallinen tapa lukea esimerkiksi sähköposti langattoman verkon kautta, on käyttää SSHv2-yhteyttä palvelimeen, jolla postit sijaitsevat. On hyvä muistaa myös, että WLAN-verkkoa hitaammat GRPS ja 3G – yhteydet ovat turvallisia, koska niitä on vaikea salakuunnella. (Käyttö langattomissa verkoissa, 2008.)

4.7 Tietoliikenteen salaaminen

Tietoliikenne on hyvä myös salata kannettavassa laitteessa. Suojauskeinoina toimii esimerkiksi suojaaminen murtamattomalla salakirjoituksella. Tämän toiminnon tulee toimia kannettavasta laitteesta aina palvelimelle ja takaisin. (Tietoliikenteen salaaminen, 2008.)

Tietoliikenteen salausprotokollat varmistavat sen, että mikään suojatulla yhteydellä lähetetty viesti ei ole muuttunut matkan varrella lähettäjältä vastaanottajalle. Jotta salausprotokollat toimivat, pitää lähettäjän ja vastaanottajan osata käyttää salausprotokollaa. (Ruohonen, 2002, 207.)

Tietoliikenteen salaaminen pitää tehdä sovelluksien välillä, tällöin asiakas- ja palvelin-ohjelman välinen liikenne kuljetetaan liikenteen salakirjoittavan SSH- tai SSL-tunnelin läpi tai verkkotasolla, jolloin työaseman ja palvelimen tai kahden lähiverkon välinen kaikki liikenne salakirjoitetaan IPSec-protokollan tavalla. (Tietoliikenteen salaaminen, 2008.)

5 TIETOTURVAMÄÄRITYKSET

5.1 Tietoturvaprotokollat

Tietoturvaprotokollamäärityksiä on paljon. Tähän opinnäytetyöhön on kerätty muutama tärkein. On olemassa esimerkiksi SSL, S-HTTP, SSH2 ja TLS. Näistä kerrotaan seuraavassa enemmän. Nämä tietoturvaprotokollat pätevät myös kannettavissa laitteissa.

SSL on Internetin yleisin tietoturvaprotokolla. Tämä protokolla on hyvin yleiskäyttöinen ja se sisältyy automaattisesti Netscapen ja Microsoftin selaimiin. Alun perin SSL:n salausmenetelmän on kehittänyt Netscape. Vähitellen siitä on tullut Internet-istuntojen defacto-menetelmä. SSL on luotettava salausmenetelmä. (Tietoturvaprotokollat, 2008.)

SSL mahdollistaa kahden eri sovelluksen välisen turvallisen tiedonsiirron. Se on sovelluksesta riippumaton ja mahdollistaa kanavan tietoturvan. SSL koostuu kolmesta perusominaisuudesta: luotettavasta siirrosta, olion autenttisuudesta ja tiedon eheydestä. Tärkeimpiä ominaisuuksia ovat myös joustava salaus-, tiivistys- ja autentikointimekanismin valinta. SSL toimii TCP/IP:n ja sovellusten välissä. SLL on riippumaton sovelluksista ja se on myös sovelluksille näkymätön. WWW-selailussa SSL ei ole tehokkain mahdollinen. SSL-liikenteen on käytettävä aina omaa TCP/IP-kanavaa. (Tietoturvaprotokollat, 2008.)

S-HTTP mahdollistaa yleisen tietoturvaprotokollan transaktiosovelluksiin. Näitä sovelluksia ovat luotettavat tapahtuman käsittelyt, autentikoinnit, sanomien eheydet ja alkuperän kiistämättömyydet. S-HTTP perustuu julkisen avaimen RSA-menetelmään ja tavalliseen salaisen avaimen käyttöön. RSA-menetelmä perustuu myös Kerberos-pohjaiseen turvajärjestelmään. S-HTTP perustuu http-protokollaan. Nämä protokollat on integroitu HTTP-protokollaan. (Tietoturvaprotokollat, 2008.)

SSH2 – protokollan avulla pystytään suojaamaan yhteydet kaikissa istunnon vaiheissa ja siten sitä voidaan käyttää myös hajautetuissa sovelluksissa tietoturvaratkaisuna. SSH2 – protokollaa käytetään TCP/IP-yhteyksillä, mutta sitä voidaan käyttää myös proxy-yhteyksien läpi tiedon siirtämiseksi palvelimelle tai palvelimelta. (Tietoturvaprotokollat, 2008.)

SSH2 muodostuu kolmesta pääkomponentista, joita ovat siirtoprotokolla, autentikointiprotokolla ja yhteysprotokolla. Siirtoprotokolla mahdollistaa palvelimen autentikoinnin sekä siirron luottamuksellisuuden ja eheyden. Siirtoyhteys voidaan halutessa siis myös tiivistää. Tätä protokollaa käytetään TCP/IP:n päällä, mutta sitä voidaan käyttää myös muun luotettavan kuljetusprotokollan päällä. Autentikointiprotokolla toimii siirtoprotokollan päällä ja se autentikoi työaseman aina palvelimelle asti. Yhteysprotokolla multipleksaa suojatun tunnelin usealle loogiselle kanavalle ja se toimii autentikointiprotokollan päällä. (Tietoturvaprotokollat, 2008.)

TLS on IETF:n standardi, joka on kehitetty SSL:n pohjalta. TLS:n koostuu kahdesta tavoitteesta, joita ovat tiedonsiirron yksityisyys ja tiedon eheys. TLS:n standardoinnissa on huomioitu yhteensopivuus, laajennettavuus sekä tehokkuus. (Tietoturvaprotokollat, 2008). Tietoturvaprotokollat on hyvä kokonaisuudessaan huomioida myös kannettavissa laitteissa.

5.2 Salaukset

Salauksien avulla pystytään kannettavissa laitteissa myös varmistamaan tietojen luottamuksellisuus, eheys ja kiistämättömyys. Salaus pitää luoda siten, ettei sen murtaminen kohtuullisessa ajassa ja kohtuullisin resurssein ole mahdollista. Salausvaatimukset riippuvat salattavan tiedon tärkeydestä. Salausmenetelmien soveltuvuutta arvioitaessa lähtökohtana tulee olla salausmekanismit, joiden murtaminen ei ole laskennallisesti järkevää. Nämä ovat vahvoja salausmenetelmiä. Suomessa käytettävien salauksien tasoja ei ole rajoitettu lainsäädännössä. (Salaukset, 2008.)

Salausmekanismin turvallisuus pitää perustua käytettyihin salausavaimiin. Salausmekanismin salaisuus ja julkisuus ei saa vaikuttaa mekanismin turvallisuuteen. Hyvin toteutetuissa salausmenetelmissä salauksen purku onnistuu ainoastaan käymällä läpi koko salausmekanismin avainavaruus ja kokeilemalla kaikkia mahdollisia salausavaimia salauksen purkamiseen. Salausavaimen tulisi olla pitkä, mikä tekee sen murtamisesta vaikeampaa. Salausmenetelmät voidaan jakaa kahteen pääluokkaan: jonosalaukseen ja lohkosalaukseen. (Salaukset, 2008.)

Jonosalauksella tarkoitetaan salausta, jossa selväkielinen teksti salataan yleensä merkki kerrallaan. Tätä salausmekanismia käytetään suurta nopeutta vaativissa reaaliaikaisissa sovelluksissa. Lohkosalauksessa selväkielinen teksti salataan ainoastaan lohko kerrallaan. Tätä salausmekanismia käytetään taas yleisimmissä symmetrisissä ja epäsymmetrisissä salausalgoritmeissa. (Salaukset, 2008.)

Salauksiin kuuluu myös salausalgoritmit mitkä voidaan jakaa symmetrisiin ja epäsymmetrisiin salausalgoritmeihin. Symmetrisissä algoritmeissa käytetään salaukseen ja salauksen purkuun samaa salausavainta. Epäsymmetrisissä algoritmeissa käytetään eri avaimia viestin salaamiseen ja salauksen purkuun. Epäsymmetrisiä algoritmeja kutsutaan nimellä julkisen avaimen algoritmi. (Salausalgoritmit, 2008.)

Symmetristen menetelmien etuna voidaan pitää salauksen nopeutta, mutta haittana on avainten hallinta. Avainten hallinnassa viestin lähettäjällä ja vastaanottajalla tulee olla tiedossaan sama salausavain. Symmetrisessä salauksessa viestin ja salauksen purkamiseen tarvittava avain on suoraan johdettavissa salausavaimesta. Ongelmia voi syntyä esimerkiksi kommunikoitaessa maantieteellisesti tai muuten laajoissa verkoissa. (Salausalgoritmit, 2008.)

Epäsymmetrisen menetelmän etuna on taas julkisen avaimen vapaa jakelu, mutta ongelmana on toisaalta salauksen hitaus. Epäsymmetrisessä salauksessa käytetään avainparia, joista toinen avain on aina julkinen ja toinen on yksityinen. Avaimet ovat vaihtokelpoisia siten, että julkisella avaimella salattu viesti voidaan avata kyseessä olevan avainparin yksityisellä avaimella ja päinvastoin. Avaimet ovat yksinkertaisia, mikä on etu symmetrisiin salausalgoritmeihin verrattuna. Parhaiten

toimiva salausjärjestelmä hyödyntää molempien algoritmityyppien parhaita ominaisuuksia. (Salausalgoritmit, 2008.)

Yksi salausmenetelmän muodoista on tiivistefunktiot. Käytettäessä tiivistettä ei ole mahdollista päätellä alkuperäistä viestiä. Hyvä tiivistefunktio ei luo samaa tiivistettä kahdella eri syötetekstillä. Tiivistefunktioita käytetään apuna viestien digitaalisessa allekirjoittamisessa ja käyttöjärjestelmien salasanojen tallentamisessa. (Tiivistefunktiot, 2008.)

Esimerkkinä tiivistefunktiosta on digitaalinen allekirjoitus. Siinä allekirjoituksen lähettäjä laskee lähetettävästä viestistä tiivisteen, jonka hän salaa yksityisellä avaimellaan. Vastaanottaja avaa salatun tiivisteen lähettäjän julkisella avaimella. Samalla hän laskee itse viestistä tiivisteen ja vertaa sitä lähettäjän julkisella avaimella avaamaansa tiivisteeseen. Näiden tiivisteiden ollessa samat, on viesti todistettavasti allekirjoitettu lähettäjän yksityisellä avaimella eikä kukaan ole päässyt muuttamaan viestiä matkalla. (Tiivistefunktiot, 2008.)

6 KOHDEYRITYS

6.1 Case-yrityksen Vulganus Oy:n esittely

Vulganus Oy on vuonna 1977 perustettu perheyritys, jonka pääkonttori ja tuotantotilat sijaitsevat Suomessa, paikkakunnalla nimeltä Nastola. Yrityksessä työskentelee 30 henkilöä ja liikevaihto on noin 8 miljoonaa euroa. Ulkomaisia edustajia ja myyntitoimistoja toimii 20 eri maassa. Yritys on merkittävä alan toimittaja maailmanlaajuisesti ja kotimaassa se on markkinajohtaja. (Lehtinen. L.2008.)

Yritys suunnittelee, valmistaa ja markkinoi elintarviketuotantoa tehostavia spiraalijärjestelmiä tuotettavuuden ja laadun parantamiseksi. Jokainen järjestelmä toteutetaan yksilöllisten tarpeiden mukaisesti kiinteässä yhteistyössä asiakkaan kanssa. Tuotteet jakautuvat seuraaviin kategorioihin: Articline, Tropicline, Cleanline ja Softline. Spiraalijärjestelmien suunnittelussa Vulganus Oy huomioi omalta osaltaan elintarvikealan korkeat hygienia-vaatimukset ja kuluttajien nykyaikaisen tuotetietämyksen. (Lehtinen. L. 2008.)

6.2 Case-yrityksen kannettavien laitteiden ja kuljetettavien tallenteiden esittely

Tässä kappaleessa esitetään Vulganus Oy:n tärkeimmät kannettavat laitteet ja kuljetettavat tallenteet. Yrityksellä on hetkellä käytössä seitsemän kannettavaa, joista yksi ei ole yrityksen verkossa vaan ohjauslogiikkakeskusten ohjelmoinnin käytössä. Lisäksi käytössä on lukuisa määrä muistitikkuja ja DVD-tallenteita. Mobiililaitteita on 20 kappaletta, joista PDA-laitteita on yhdeksän kappaletta.

7 TUTKIMUKSEN TARKOITUS JA SUORITTAMINEN

7.1 Kannettavien laitteiden alustava tietoturvakartoitus ja SWOT-analyysi

Ennen tutkimuksen aloittamista tein case-yrityksen kannettavista laitteista alustavan tietoturvan nykytilan kartoittamisen. Nämä tiedot ovat yrityksen sisäiseen käyttöön. Olen saanut luvan kuitenkin mainita osan niistä tässä opinnäytetyössä. Tietoturvasta selvisi muun muassa seuraavia asioita, joista taulukkoon kaksi on lueteltu hyvät puolet. Taulukkoon kolme on puolestaan lueteltu huonot puolet tämän hetkisestä tietoturvasta.

TAULUKKO 2. Hyvät puolet tietoturvasta

Hyvät puolet
• Kauan käytössä • Halu parantaa ja kehittää tietoturvan tasoa • Tietoturva on toteutettu keskitetysti • Oheislaitteet laadukkaita

Hyviä puolia (TAULUKKO 2) ovat ne, että kannettavat laitteet ovat olleet kauan käytössä sekä tietoturvan osalta ne toimivat kohtalaisen hyvin. Yrityksen henkilöstön halu parantaa ja kehittää tietoturvan tasoa on positiivinen asia. Hyvänä asiana näkisin sen, että tietoturva on toteutettu keskitetysti ja oheislaitteet ovat laadukkaita.

TAULUKKO 3. Huonot puolet tietoturvasta

Huonot puolet
• Päivitykset eivät aina ajan tasalla • Sähköpostin roskapostisuodatus ei ole toimiva

Taulukkoon kolme on kerätty kannettavien laitteiden huonoja puolia, joita ovat huonosti ajan tasalla olevat päivitykset sekä sähköpostissa olevan roskapostisuodatuksen vaihteleva epäkuntoisuus. Kartoituksesta tein myös SWOT-analyysin. Analyysia pystyin hyödyntämään myös lopullisessa tutkimuksessa. Ohessa olevasta SWOT-analyysista selviää kannettavien laitteiden ja kuljetettavien tallenteiden vahvuudet ja heikkoudet sekä niiden mahdollisuudet ja uhat. SWOT-analyysista näkee hyvin missä on vielä parannettavaa.

TAULUKKO 4. SWOT-analyysi kannettavista laitteista ja kuljetettavista tallenteista

Vahvuudet	**Heikkoudet**
• keskitetty tietoturva • tietoturvaohjelmisto sopiva ko. yritykselle • liikuteltavuus • koko • keveys • yhteys • mobiliisuus	• päivitettävyys • suojaus • inhimillinen tekijä • huolimattomuus
Mahdollisuudet	**Uhat**
• vpn-yhteyden hyödyntäminen • synkronointi • rajattomat yhteydet	• varkaudet • tietomurto • laitteen katoaminen • siirtomedioiden joutuminen ulkopuolisille

Vahvuuksiksi voidaan lukea keskitetty tietoturva, mitä ohjataan yhdestä paikasta. Tietoturvan ohjelmistopaketti on juuri Vulganus Oy:lle sopivaksi muokattu. Kannettavien laitteiden ja tallenteiden etuihin voidaan lukea liikuteltavuus, koko ja keveys, sillä henkilökunta matkustaa paljon. Yhteys ja mobiilisuus luetaan myös vahvuuksiksi.

Päivitettävyys ja suojaus voivat olla heikkouksia, jos käyttäjä esimerkiksi unohtaa päivittää viimeisimmät tietoturva varmenteet. Yhtenä heikkoutena on myös inhimillinen tekijä, sillä käsiteltävien laitteiden pienen koon vuoksi laitteet voivat helposti vahingoittua tai kadota, verrattaessa esimerkiksi vastaaviin toimistomalleihin. Käyttäjän huolimattomuus voidaan myös luokitella osaksi inhimillistä tekijää.

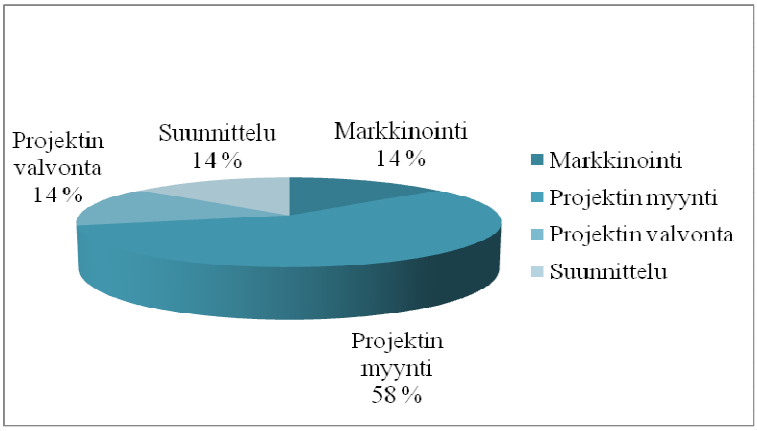
Mahdollisuuksia ovat taas VPN-yhteyden hyödyntäminen eri laitteiden keskinäinen synkronointi sekä rajattomien yhteyksien käyttäminen. Uhkana voi olla mahdolliset varkaudet tai katoamiset, koska matkustetaan paljon. Siirtomedioiden joutuminen ulkopuolisille henkilöille on myös eräs kannettavien laitteiden ja kuljetettavien tallenteiden uhka.

7.2 Tutkimuksen toteutus

Toteutin tutkimukseni kartoituksen jälkeen Vulganus Oy:ssä vuoden 2008 kesän ja syksyn välisenä aikana. Tutkimus oli kvalitatiivinen ja toteutettiin yksilöhaastatteluina, mikä mahdollisti myös syventävät jatkokysymykset tutkimukseni myöhemmässä vaiheessa. Haastattelututkimukseen valitsin mukaan henkilöitä, joilla on käytössä kannettava laite.

Haastateltavia oli seitsemän henkilöä. Haastateltavat voidaan jakaa markkinointiin, projektin myyntiin, projektin valvontaan ja suunnitteluun. Markkinointiin kuului yksi henkilö ja projektin myyntiin kuului haastateltavista neljä henkilöä. Projektin valvonnasta vastaa yksi henkilö samoin kuin suunnittelustakin vastaa yksi henkilö. Katso kuvio 6.

Haastatteluiden lisäksi analysoin ja tutkin kannettavien laitteiden tietoturvaa tarkemmin. Tutkimuksen materiaalipohjana olen käyttänyt myös aikaisemmin tekemieni projektiopintojen materiaaleja.



KUVIO 6. Haastateltavien henkilöiden jakautuminen.

7.3 Tutkimustulokset

Haastattelut onnistuivat hyvin, joten minun oli helppo koota vastauksista yhteenveto. Uskon, että seitsemän vastausta antoi minulle hyvän ja kattavan kokonaiskuvan kannettavan laitteen tietoturvasta ja uhista Vulganus Oy:ssä, sillä kyseiset henkilöt käyttävät työssään kannettavia laitteita päivittäin.

Kysymys yksi ”**Millainen on työnkuvasi?**” on haastatteluissa otettu esiin siksi, että sen kautta sain tutkimukseeni käsityksen siitä, kuinka paljon eri henkilöt työssään ovat tekemisissä eri tietoturvaratkaisujen kanssa. Edellä mainittuun kysymykseen sain seuraavanlaisia vastauksia (TAULUKKO 5).

TAULUKKO 5. Työkuvat eri työtehtävissä.

Markkinointi • markkinointimateriaalien tekeminen • tarjous-layoutin päivittäminen • asiakaskontaktit	**Projektin myynti** • tarjouksien tekeminen • sopimusten laadinta • projektiaikataulun suunnittelu • asiakaskontaktit
Projektin valvonta • projektin valvonta asennuspaikalla • yhteyshenkilö asiakkaan tehtaan huoltohenkilökunnan kanssa	**Suunnittelu** • suunnittelun aikatauluttaminen • tutkimusmittaukset • kehitystyö

Taulukosta viisi pystytään toteamaan, että eri henkilöillä on hyvin erilaiset ja monipuoliset työnkuvat. Tämä myös tulee huomioida tietoturvassa ja sen ratkaisuissa.

TAULUKKO 6. Käytetyt ohjelmat ja käsiteltävät dokumentit kannettavalla laitteella.

Käytetyt ohjelmat	**Käsiteltävät dokumenttimuodot**
• Microsoft Office -ohjelmat • Autocad • Acrobat Reader • Photoshop • WinZip • WinRar	• DOC, XLS, PPT • DWG, DXF • PDF • PSD, JPG, GIF • ZIP • RAR

Toisessa kysymyksessä kysyttiin **”Millaisia dokumentteja käsittelet ja tallennat kannettavalla laitteella?”** Vastaukseksi sain (TAULUKKO 6) listauksen. Tämä kysymys on kysytty siksi, jotta saisin selville kuinka paljon erilaisia tiedostoja, ohjelmistoja ja sovelluksia pitää tietoturvassa kannettavan laitteen osalta huomioida. Kysymyksestä kolme selvisi dokumenttien jakautuminen.

Seuraava haastattelu kysymys (KYSYMYS 3) oli: ”**Minkälaisessa muodossa dokumentit tulevat sinulle?”** Tähän kysymykseen markkinoinnista vastaava vastasi, että hänelle dokumentit tulevat DOC-, XLS-, PPT- ja PDF-muodoissa. Projekti myynnistä vastaaville ja projektin valvonnasta vastaavalle henkilöille sekä suunnittelijalla tiedostot tulevat DOC-, XLS-, PPT-, DWG-, DXF-, PDF-, JPG- ja GIF-muodoissa. Kaikki haastateltavat sanoivat myös, että yleensä tiedostot tulevat pakattuina eli ZIP- tai RAR- paketeissa.

Kysyttäessä **kannettavan laitteen päivittäisestä ajankäytöstä** (KYSYMYS 4) sain kaikilta seitsemältä vastaajalta saman vastauksen: kannettavaa laitetta käytetään päivittäin lähes kahdeksan tunnin ajan. Käyttöään he perustelivat sillä, että kannettava laite on nykypäivän toimistotyöskentelyssä korvannut lähes kokonaan tavallisen pöytäkoneen.

Viidennessä kysymyksessä kysyttiin **kannettavan laitteen suojaamisesta**. Vastaukseksi sain kannettavien laitteiden olevan suojattu jokaisen henkilökohtaisilla käyttäjätunnuksilla ja niiden salasanoilla. Tiedostot ja eri kansiot ovat myös suojattuja salasanoin sekä eri kansiot ovat jaettu eri käyttäjäryhmiin. Tietyt tiedot näkyvät vain henkilöille, joilla on oikeus kyseiseen kansioon. Esimerkiksi markkinointi-kansion tietoihin pääsevät vain henkilöt, jotka on määritelty käyttäjiksi. Näillä toimenpiteillä pystytään ehkäisemään inhimillisiä erehdyksiä eikä kannettavan joutuessa ulkopuolisten käsiin ole mahdollista tuhota tai kopioida kaikkea tärkeää tietoa laitteesta. Tutkimukseni myötä selvisi myös se, että käyttäjät ottavat oman harkintansa mukaan varmuuskopiointeja omista tiedostoistaan.

Kuudes haastattelukysymys oli: ”**Miten koneen kovalevysi on salattu?**” Tähän kysymykseen kaikki vastaajat vastasivat, ettei heidän koneiden kovalevyjä ole mitenkään salattu. Tämä on tietoturvariski.

Kysyttäessä henkilöiltä heidän matkapäiviensä lukumäärää vuodessa (KYSYMYS 7) sain tulokseksi seuraavanlaisia vastauksia: Markkinoinnista vastaava henkilö vastasi matkustavansa alle 10 päivää vuoden aikana, kun taas projektimyynnistä vastaavat henkilöt kertoivat matkustavansa yli 150 päivää vuodessa. Suunnittelijat kertoivat matkustavansa vain noin 30 päivää vuoden aikana. Projektivastaava matkustaa vastausten perusteella kaikista eniten: yli 200 päivää vuodessa. Kysyin kyseisen kysymyksen siksi, että saisin selvyyden kannettavan laitteen riskeistä joutua esimerkiksi varkauden tai tietoturvahyökkäyksen kohteeksi muualla kuin työpaikalla.

Kysymyksessä kahdeksan kysyttiin ”**Kuinka usein käytät langatonta verkkoa, ulkoista siirtomediaa tai eri yhteyttä kuin yrityksen verkkoa?**” Kysymyksen esitin, koska tietoturvariskit ovat aina suuremmat yrityksen verkon ulkopuolella. Kysymys kuusi vastaa osaltaan tähän kysymykseen. Kannettavaa laitetta käyttävät henkilöt käyttävät työmatkoilla useasti hotellin langatonta verkkoa tai työmailla olevia kantoasemia. Ulkoisten siirtomedioiden, esimerkiksi muistitikun, ulkoisen kovalevyn ja DVD-levyn, avulla voi siirtyä viruksia ja vakoiluohjelmia kannettavaan laitteeseen. Edellä mainitut siirtomediat ovat kuitenkin välttämättömiä kannettavaa laitetta käytettäessä.

Haastateltavilta kysyttäessä **miten he kokevat nykyisen tietoturvan** (KYSYMYS 9), sain kaikilta vastaajilta vastaukseksi, että nykyinen tietoturva on toimiva, mutta liiallinen roskapostin määrä häiritsee käyttäjiä ja hidastaa työntekoa. Myös virustentorjunta ohjelman F-Secure päivitykset häiritsevät välillä työntekijöitä.

Jatkokysymyksessä kymmenen kysyin: ”**Millainen tietoturvan pitäisi työntekijöiden mielestä olla?**” Yleisesti vastaajat olivat sitä mieltä, että tietoturvan tulisi olla huomaamaton ja toimiva. Eli käyttäjän työn tekeminen ei saisi häiriintyä tietoturvan vuoksi. Tietoturvan tulisi kuitenkin automaattisesti hoitaa suojaukset.

Kysyessäni henkilöiltä kokemuksia kannettavan laitteen varastamisesta tai laitteen joutumisesta virusten kohteeksi (KYSYMYS 11) sain vastaukseksi, ettei kannettavaa laitetta ole varastettu markkinoinnista vastaavalta. Projektimyynnin ihmisiltä yhdeltä on varastettu kannettava tietokone sekä kahdessa muussa laitteessa on ollut viruksia ja haittaohjelmia. Projektivastaavan ja suunnittelijan koneita ei ole varastettu eikä niissä myöskään ole ollut viruksia. Fyysinen suojaaminen on toiminut kohtalaisen hyvin.

Kysymyksessä kaksitoista ”**Tarvitseeko tietoturvaa kehittää?**” kaikki seitsemän haastateltavaa olivat yleisesti sitä mieltä, että roskapostisuodatuksen ja kannettavien laitteiden suojaus pitää saada paremmaksi. Kannettavat tallenteet on myös tehtävä tietoturvallisemmiksi. Tietoturvaohjeita toivottiin koko henkilökunnan käytettäväksi.

7.3 Loppupäätelmät tutkimuksesta

Tutkimuksen tarkoituksena oli selvittää tämän hetken tietoturvan taso ja miten sen voi toteuttaa paremmin kannettavien laitteiden osalta Vulganus Oy:ssä. Tarkoituksena oli myös löytää ratkaisu siihen, miten tietoturvasta olisi kaikille kannettavia laitteita käyttäville hyötyä. Haastateltavat vastasivat kiitettävästi kaikkiin alustaviin kysymyksiin sekä jatkokysymyksiin. Tästä voidaan päätellä, että kiinnostusta yritystä kohtaan löytyy ja sen kehittämisessä halutaan olla osallisina. Kysymyksien vastauksista sai selvyyden siihen, mitä tulee huomioida ja parantaa tietoturvan kehityksessä.

Tutkimuksesta ja kannettavien laitteiden alustavasta tietoturvakartoituksesta ja SWOT-analyysista selvisi hyvin nykyisten kannettavien laitteiden (TAULUKKO 2., 3., 4.) vahvuudet ja heikkoudet sekä mahdollisuudet ja uhat. Nämä tiedot on hyvä huomioida yrityksen kannettavien laitteiden tietoturvan kehittämissuunnitelmassa.

Tutkimuksesta selvisi myös se, että kannettavia laitteita käytetään monessa eri työtehtävässä erilailla, mikä kertoo kannettaviin laitteisiin eri henkilöiltä saapuvien tiedostojen moninaisuudesta. Nämä erilaiset tiedostomuodot on hyvä ottaa huomioon tietoturvaa parannettaessa.

Kuten tutkimuksesta voidaan todeta, tietoturva ei ole kannettavien laitteiden osalta vielä paras mahdollinen. Tämä selvisi kysymyksestä viisi: ” Miten kannettava laitteesi on suojattu?”. Kenenkään kannettavan laitteen käyttäjän koneen kovalevyä ei ole esimerkiksi suojattu. Tämä on suurena riskinä sille, että kannettava laite voi joutua ulkopuolisten käsiin, sillä työntekijät matkustat paljon.

Yrityksen verkon ulkopuolella olevia verkkoja käyttävät eniten matkustavat henkilöt ja he onneksi ovat tietoisia ulkopuolisten verkkojen uhkista. Kannettavien laitteiden kanssa työskentelevät henkilöt pitivät tämän hetkistä tietoturvan tasoa toimivana, mutta toivoivat parempaa roskapostisuodatinta. sähköposteihinsa. Heidän mielestä myös tietoturvan tulisi olla huomaamattomampi ja toimivampi kokonaisuus.

Tietoturvan toteutukseen kannettavien laitteiden tallenteiden osalta toivottiin parannusta samoin kuin tietoturvaa koskevia ohjeistuksia koko henkilökunnalle. Kysymyksestä kymmenen selvisi, että tämän hetkinen tietoturva on toiminut, sillä kannettaviin laitteisiin ei ole päässyt viruksia eikä laitteita ole varastettu.

Edellä olevista tuloksista voidaan lyhyesti todeta kannettavan laitteen olevan kyseisessä yrityksessä kohtalaisen hyvin suojattu, mutta kannettavat tallenteet ja siirtolaitteet ovat suojaamatta kokonaan. Tämä on yrityksen kannalta iso turvallisuusriski, johon tulisi kiinnittää huomiota tietoturvaa parannettaessa. Tietoturvan nykyinen taso on työntekijöiden mielestä kohtalaisen hyvä.

Tutkimuksesta voidaan päätellä kannettavien laitteiden tietoturvan olevan jatkuvan kehityksen ja päivityksien vallassa myös Vulganus Oy:ssä. Yrityksen tulee myös muistaa, että uuden esimerkiksi kannettavan laitteen hankinnassa on heti huomioitava tietoturva ja tietoturvaohjeet (LIITE 2). Tietoturvaohjeiden avulla koko henkilökunta voi toimia samalla tavalla. Liite 2. sisältää lyhyesti sen, mitä kannettavan laitteen tietoturvassa olisi hyvä ottaa huomioon.

Kannettavien laitteiden osalta Vulganus Oy:n tietoturvan voi toteuttaa paremmin toimimalla yhteisesti sovittujen sääntöjen ja tietoturvaohjeistuksen mukaisesti (LIITE 2). Jokainen huolehtii omasta kannettavasta laitteestaan parhaalla mahdollisella tavalla. Kannettavien laitteiden tietoturvan tason jatkotutkimuksen voisi tehdä muutaman vuoden kuluttua, kun laitteet ja ratkaisut ovat kehittyneet. Kun yritys on alkanut toteuttaa tietoturvaohjeistusta käytännössä. Silloin pystyttäisiin arvioimaan onko tietoturva ja sen taso toteutunut toivotulla tavalla.

8 PÄÄTELMÄT

Kannettavan laitteen tietoturva on koko ajan kehityksen pyörissä ja lisäksi kannettavalla laitteella on suurempi riski tietoturvaongelmiin, kun vastaavasti normaalilla pöytäkoneella.

Näin ollen PK-yrityksen IT-tuen ja asiantuntijan on oltava koko ajan tasalla tietoturvan tasosta ja varautua tuleviin tietoturvaongelmiin kehittämällä koko ajan tasoa ja ratkaisuja tietoturvaongelmien vuoksi. Valittaessa tietoturvaratkaisuja pitää muistaa se, ettei tietoturva ole tuote, jonka voit ostaa kaupasta tai asentaa valmiina pakettina. Tietoturvassa on kyse jatkuvasta ylläpidosta. Täydellistä tietoturvaa ei ole olemassa kannettavassa laitteessa ja tietoturva on niin hyvä, kun sen heikoin lenkki.

Tietoturvamäärityksissä on hyvä huomioida aina tietoturvaprotokollat ja salaukset yrityksen tarpeista riippuen. Laitteistokohtaiset vaatimukset on hyvä ottaa huomioon myös, sillä monissa eri merkkisissä laitteissa on tietyt sallitut protokollat. Tietoturva on aina kompromissi laitteen suojaamisen ja käytön helppouden välillä. Jokainen käyttäjä, jolla on pääsy laitteelle ja sen resursseihin tai käyttöympäristöön, on todennäköinen tietoturvariski. Tulevaisuuden teknologiset ratkaisut tuovat lisähaastetta kannettavien laitteiden tietoturvalle.

Lisäksi yrityksen on tärkeää tehdä tietoturvaohjeistus, jossa on tarkka ohje kannettavan laitteen käyttöä silmälläpitäen. Yrityksen on hyvä ohjeistaa henkilökuntaansa siitä, mitä tietoja kannettavassa laitteessa saa säilyttää ja tallentaa sekä miten tiedot tulee suojata. Olisi hyvä salata ainakin kaikki työtiedostot, sovellusohjelmat ja sähköpostit, mitkä saattavat sisältää henkilökohtaista tai yrityksen sisäistä tietoa. Käyttäjätunnuksien avulla pystytään tukemaan tietoturvaa erinomaisesti.

9 YHTEENVETO

Kannettava laite on nykyajan trendi ja se löytyy jokaisesta yrityksestä. Viestintä on nykypäivänä vaivatonta ajasta ja paikasta riippumatonta. Tämä asettaa kannettavien laitteiden tietoturvalle tietyt vaatimukset. Tietoturva pitää huomioida ja hoitaa hyvin myös kannettavaan laitteeseen. Hyvin hoidettuna tietoturva säästää yritykseltä monien miljoonien eurojen tappiot. Kannettavaa laitetta valittaessa tulee ensisijaisesti muistaa myös huomioida tietoturva.

Tietoturvalle luo haasteita kannettavien laitteiden kehittyminen ja käyttäjien lisääntyminen. Kannettavia laitteita ovat esimerkiksi kannettavat tietokoneet, matkapuhelimet ja erilaiset PDA-laitteet. Fyysinen suojaaminen on yhtä tärkeä asia kuin yhteyksien ja lisälaitteiden tietoturvaan varautuminen.

Vähintä mitä voi tehdä niin on suojata tiedot salasanalla tai koodilla. Varkaustapauksissa pystytään oikeanlaisella tiedostojen ja kansioiden suojauksella suojaamaan laitteen tietoja. Tiedonkäsittelystä on hyvä muistaa se, että poistettaessa kannettava laite käytöstä lopullisesti pitää myös tiedot pystyä tuhoamaan laitteesta lopullisesti. Kannettavan laitteen tiedostoista on hyvä muistaa ottaa varmuuskopioita viikoittain.

Käytettäessä langattomia verkkoja kannettavalla laitteella, on hyvä huomioida mitä verkkoja kannattaa käyttää ja mitä ei. Pääasiassa langattomista verkoista julkisia verkkoja voi käyttää normaalissa tiedonsiirrossa ilman huolta. Mutta tällöinkin tietokoneen tietoturva pitää olla vähintään minimitasolla kunnossa. Tietoliikenteen suojaus kannettavassa laitteessa voidaan hoitaa esimerkiksi murtamattomalla salakirjoituksella. Sen pitää toimia aina laitteesta palvelimelle ja takaisin.

Tietoturvaprotokollat on hyvä huomioida kannettavissa laitteissa. Seuraavat protokollat on hyvä huomioida: SSL, S-HTTP, SSH2 ja TLS. Nämä salausmekanismit voidaan jakaa jonosalaukseen tai lohkosalaukseen. Jonosalaus on hyvä suurta nopeutta vaativissa reaaliaikaisissa sovelluksissa. Lohkosalaus on taas hyvä symmetrisissä ja epäsymmetrisissä salausalgoritmeissa.

Case-yrityksessä, Vulganus Oy:ssä tietoturva on hoidettu kannettavien laitteiden osalta kohtalaisen hyvin. Tietoturva on keskitetty yhteen paikkaan. Vulganus Oy on hoitanut hyvin esimerkiksi kannettavien laitteiden käyttäjätunnukset ja salasanat. Hyvää on se, että käyttäjien tiedostot on jaettu tiettyihin käyttäjäryhmiin. Halu parantaa ja pysyä tietoturvan ajan tasalla ovat myös hyviä asioita. Yleiset tietoturvaprotokolla määritykset on huomioitu Vulganus Oy:ssä hyvin.

Käyttäjien kokemukset ovat suurimmaksi osaksi olleet positiivisia. Ainoa toive oli tietoturvaohjeistus ja parempi roskapostisuodatin-järjestelmä sähköpostiin. Tietoturvan voi paremmin toteuttaa kannettavien laitteiden osalta tietoturvaohjeistuksen avulla. Tutkimustulosten perusteella olen tehnyt case-yritykselle tietoturvaohjeistuksen (LIITE 2). Haittaohjelmien leviäminen voidaan välttää kouluttamalla henkilökuntaa ja tiedottamalla heille mahdollisista tietoturvauhkista.

Paremmin tietoturvan voi myös toteuttaa siten, että yritys valitsee omaan yritykseen sopivan tietoturvaratkaisu-ohjelmiston. Päivitykset on myös hyvä muistaa, vaikka järjestelmä onkin jo olemassa. Tietoturvaratkaisuissa kannattaa aina miettiä järjestelmän hinta-laatu -suhdetta. Hyvä tietoturva lähtee aina käyttäjän luomista tietoturvallisista ratkaisuista ja käyttäjän tarpeista. Hyväkään ohjelma ei pysty takaamaan sataprosenttista tietoturvaa.

LÄHTEET

Painetut lähteet

Uski, J, 2008, Kannettava kahleisiin, MikroPc 12/2008

Boström, M, 2003, Kotimikron tietoturva, Jyväskylä, Gummerus Kirjapaino Oy

Korpela, J. 2005. Turvallisesti netissä, Saarijärven Offset Oy 2005

Ruohonen, M. 2002. Tietoturva, Porvoo: WS Bookwell.

Sähköiset lähteet

Kannettavan laitteen tietoturva, 2008, [Oulun yliopisto], [viitattu 10.8.2008] Saatavissa: http://www.oulu.fi/atkk/tiedotus/sessio/sess218/kannettavan_tietoturva.htm

Kannettavien laitteiden tietoturva, 2008, [Oulun yliopisto], [viitattu 13.8.2008] Saatavissa: http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/laitteet.html

Käyttö langattomissa verkoissa, 2008, [Oulun yliopisto], [viitattu 11.7.2008] Saatavissa: http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/tietoa_kannettavat.html#kaytwlan

Lisäturvaa sormenjäljellä, 2008, [Tietokone], [viitattu 25.2.2009] Saatavissa: http://www.tietokone.fi/lukusali/artikkelit/2003tk04/pikis_bio.htm

Pikaopas, 2008, [Oulun yliopisto], [viitattu 11.7.2008] Saatavissa: http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/index.html

Safereg [Safereg], 2009, [viitattu 30.3.2009] Saatavissa: https://www.safereg.com/

Salaukset, 2008, [Viestintävirasto], [viitattu 12.11.2008.] Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat.html

Salausalgoritmit, 2008, [Viestintävirasto], [viitattu 10.10.2008] Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/salausalgoritmit.html

Suojaa sylimikrosi, 2008, [digitoday], [viitattu 15.8.2008] Saatavissa: http://www.digitoday.fi/tietoturva/2004/02/04/Suojaa+sylimikrosi/20047227/66

Tiedonkäsittely [Oulun yliopisto], [viitattu 11.12.2008], Saatavissa: http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/tietoa_kannettavat.html

Tietoliikenteen salaaminen, 2008, [Oulun yliopisto], [viitattu 10.12.2008], Saatavissa: http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/tietoa_kannettavat.html

Tietoturvan minimitaso, 2008, [Oulun yliopisto], [viitattu 10.7.2008] Saatavissa: http://www.oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/tietoa_kannettavat.html#mintaso

Tietoturvaprotokollat, 2008, [Jyväskylän yliopisto], [viitattu 12.12.2008] Saatavissa: http://www.mit.jyu.fi/opetus/opinnayte/LuK/TietoturvaHajautetuissa/#_Toc523271616

Tiivistefunktiot, 2008, [Viestintävirasto], [viitattu 19.12.2008] Saatavissa: http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva/salausmenetelmat/tiivistefunktiot.html

Työasemien tietoturvan parhaat käytännöt ja hallinta, 2008, [f-secure], [viitattu 1.6.2008] Saatavissa: http://www.mspost.fi/microsoft/Erkki_Mustonen_Hkisali_klo1030.pdf

VPN, 2008, [Koulutus- ja konsultointipalvelu KK Mediat], [viitattu 10.7.2008] Saatavissa: http://www.2kmediat.com/vpn/elementit.asp

Haastattelut

Kulonen. A. 2008. Tuotekehityspäällikkö. Vulganus Oy. Haastattelu 21.5.2008

Kuparinen. J. 2008. Projektipäällikkö. Vulganus Oy. Haastattelu 21.5.2008

Lehtinen, L. 2008. Toimitusjohtaja. Vulganus Oy. Haastattelu. 20.5.2008

Lehtinen, M. 2008. Myynti-ja markkinointijohtaja. Vulganus Oy. Haastattelu. 20.5.2008

Mustonen. A. 2008. Projektipäällikkö. Vulganus Oy. Haastattelu 22.5.2008

Rajasaari. E. 2008. Myynti-ja markkinointipäällikkö. Vulganus Oy. Haastattelu 19.5.2008

Siitari. K. 2008. Avainasiakaspäällikkö. Vulganus Oy. Haastattelu 19.5.2008

LIITE 1

KYSYMYKSET

Kysymykset koskevat Vulganus Oy:n kannettavien laitteiden tietoturvaa. Kysymyksiä on käytetty haastatteluiden runkona.

1. Millainen on työnkuvasi?

2. Millaisia dokumentteja käsittelet ja tallennat kannettavalla laitteellasi?

3. Minkälaisessa muodossa dokumentit tulevat sinulle?

4. Miten paljon aikaa käytät päivässä kannettavalla laitteella?

5. Miten kannettava laitteesi on suojattu?

6. Miten koneen kovalevysi on salattu?

7. Miten paljon sinulla on matkapäiviä vuodessa?

8. Kuinka usein käytät langatonta verkkoa, ulkoista siirtomediaa tai eri yhteyttä kuin yrityksen verkkoa?

9. Miten koet nykyisen tietoturvan?

10. Millainen tietoturvan pitäisi olla sinun mielestäsi?

11. Onko kannettava laitteesi joskus varastettu tai joutunut virusten kohteeksi?

12. Tarvitseeko tietoturvaa kehittää?

LIITE 2

CASE-YRITYKSEN TIETOTURVAOHJEET KANNETTAVALLE LAITTEELLE

Ohjeet ovat yrityksen sisäiseen käyttöön. Olen saanut luvan kuitenkin mainita tässä opinnäytetyössä muutaman tärkeimmän kohdan ohjeistuksista.

- Käytä aina asianmukaista salausta, mikäli sinun on siirrettävä Internetin kautta salassa pidettävää tietoa.
- Mikäli joudut lähettämään salassa pidettävää aineistoa, lähetä se salattuna. Varmistu, että vastaanottaja on oikeutettu sen saamaan ja että lähetys on mennyt perille.
- Tallenna kaikki tärkeä tieto sellaisen verkkopalvelimen / työaseman levylle, josta tiedot tallennetaan säännöllisesti varmuuskopioimalla.
- Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä salasanana. Hyvässä salasanassa voi olla pieniä ja isoja kirjaimia, numeroita.
- Sähköpostin liitetiedostot voivat sisältää haittaohjelmia esimerkiksi viruksia, matoja tai troijalaisia. Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Älä avaa epäilyttäviä viestejä, vaan toimi ohjeistuksen mukaisesti.
- Älä jätä kannettavaa tietokonetta tai matkapuhelinta ilman valvontaa. Säilytä laitteita lukitussa tilassa. Huolehdi myös muistitikkujen ja DVD-levyjen asianmukaisesta säilyttämisestä.
- Vältä datapakettien lataamista ulkomailla pelkällä mobiliiyhteydellä, sillä ulkomailla yhteydet ovat usein hinnakkaampia verrattuna kotimaahamme. Suosi ja käytä ulkomailla matkustaessasi useissa hotelleissa olevia mahdollisia wlan-yhteyksiä.)
- Kuljeta mukanasi vain välttämätön määrä tietoaineistoa ja varmistu aina aineiston asianmukaisesta suojauksesta.
- On hyvä muistaa, että kannettava siirtomedia on yhtä tärkeää suojata ja pitää turvassa kuin itse kannettava laitekin.

- Älä anna asiakkaalle käyttöön siirtomediaa, mikä sisältää yrityksen sisäisiä tietoja ja tiedostoja.
- Ilmoita aina haittaohjelmista esimerkiksi viruksista, madoista tai troijalaisista ja muista tietoturvallisuuteen liittyvistä ongelmista välittömästi atk-vastaavalle.