LAUREA
AMMATTIKORKEAKOULU
Yhdessä enemmän

Tietoturvaohjeistus käyttäjälle

Ekroth, Henrik

Laurea-ammattikorkeakoulu

Tietoturvaohjeistus käyttäjälle

Henrik Ekroth
Tietojenkäsittelyn Tradenomi
Opinnäytetyö
Joulukuu, 2016

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Tietojenkäsittelyn koulutusohjelma

Henrik Ekroth

Tietoturvaohjeistus käyttäjälle

Vuosi 2016 Sivumäärä 17

Opinnäytetyön tavoitteena oli kehittää päivitetty tietoturva-ohjeistus Finavia Oy:lle. Tietoturvaohjeistuksen avulla yrityksen henkilöstö voisi ylläpitää ja kehittää omia toimia tietoturvan parantamiseksi. Opinnäytetyö on laadittu käytettäväksi Finavia Oy:ssä sisäisesti tukien eri liiketoimintoja ja osastoja.

Työn teoriaperusta pohjautuu vahvasti Valtionvarainministeriön Vahti-ohjeistuksiin, ja siinä on käytetty myös muuta tietoturvaan liittyvää ammattikirjallisuutta. Nykytilannetta kartoitettiin yrityksen intranetistä löytyvästä materiaalista. Tiedonkeruumenetelmistä työssä on käytetty kirjallisuuskatsausta, jonka avulla on hahmoteltu opinnäytetyön aihepiirin kokonaisuutta. Tietoturvan teoria toimii pohjana tietoturvaohjeistukselle. Opinnäytetyössä on käytetty toiminnallisen opinnäytetyön menetelmää, jossa toteutustapana on ollut oheistus. Opinnäytetyö muodostuu prosessin dokumentoinnista ja arvioinnista tutkimusviestinnän keinoin sekä toiminnallisesta osuudesta. Toiminnallinen osuus eli produkti käsittää tietoturvaohjeistuksen.

Työn tavoitteena oli tehdä tietoturvaohjeistus käyttäjille. Tietoturvaohjeistus on tarkoitus ottaa käyttöön kohdeyrityksessä, kun se on testattu käytännössä ja hyväksi todettu. Koska uutta ohjeistusta ei ole vielä voitu testata käytännössä, on lopullisen tuotoksen arvioiminen hankalaa. Opinnäytetyönä tehty tietoturva-ohjeistus vastaa sille annettuja määritelmiä, sekä on saavuttanut sille asetetut tavoitteet. Ohjeistuksen kehittämistä ja päivittämistä tullaa jatkamaan kohdeyrityksessä asiantuntijoiden toimesta.

Asiasanat: Tietoturva, Tietoturvaohjeistus

Laurea University of Applied Sciences
Degree Programme in Information Technology
Bachelor's Thesis

Abstract

Henrik Ekroth

Information Security Guidebook for Uses

Year 2016 Pages 17

The objective on this bachelor's thesis was to develop an updated information security guidebook for Finavia Corporation. This information security guidebook facilitates the company staff's maintenance and development of measures to improve security. The thesis was commissioned by Finavia Corporation for internal use only. The purpose of the guidebook is to support different business departments.

The theoretical framework is based on the Ministry of Finance's VAHTI-guide, and also on other professional information security sources. The present guidance material found in the company's intranet was examined. The main data collection method used was a literature review, which enables outlining the topic of the thesis. Information security is the foundation for the theory of technical documentations. The thesis is functional. This thesis includes the documentation and evaluation of the research process, as well as a functional section. The functional section comprises the established security guidelines.

The objective was to draw up security instructions for users. The security guidebook is scheduled to be operational in the commissioner company, once it has been tested and proven feasible in practice. As the new guidebook has not yet been tested, it is difficult to estimate the final output. The thesis has achieved the set objectives. The guidelines will be updated by experts of the commissioner.

Keywords: **Information Security, Information Security Guidebook**

Sisällys

1 Johdanto

Viestintäviraston kyberturvallisuuskeskus on helmikuussa 2016 varoittanut useista tiedonkalastelukampanjoista, joita on liikkeellä. Huijausviestejä on levitetty tekstiviestitse ja sähköpostitse Poliisin, Postin, Nordean ja Danske Bankin nimissä. Viestin sisältynyt linkki on vienyt huijareiden sivustoille, jotka on esimerkiksi pyritty naamioimaan Nordean sivuiksi. Käyttäjän syöttäessä verkkopankkitunnukset tai luottokorttitiedot ovat ne menneet suoraan huijareiden tietoon. Välittömästi tämän jälkeen on käyttäjien nimissä nostettu pikalainoja. (Viestintävirasto 2016.)

Opinnäytetyön aiheeksi valikoitui tietoturvaohjeistus, joka on suunnattu Finavian henkilöstölle. Finavia on Lentoasemayhtiö, joka ylläpitää ja kehittää 22 Lentoaseman verkostoa sekä koko maan kattavaa lennonvarmistusjärjestelmää. Ohjeistukselle on tarvetta, koska digitalisaation myötä palvelut ja laitteistot ovat monipuolistuneet ja käyttötarpeet muuttuneet. Tämän myötä käyttäjän tietoturvaosaaminen tulisi vastata nykyisiä haasteita.

Yrityksen tietoturva koostuu monesta osasta, jossa ohjelmistojen ja laitteistojen lisäksi käyttäjän toimet ovat merkittävässä osassa. Markkinoiden paras virustorjuntakaan ei auta, jos saastuneita liitetiedostoja avataan työnantajan tarjoamilla laitteilla. Tietoturvaohjeistus sisältää hyviä tietoturvakäytänteitä. Ohjeistuksen tavoitteena on saada käyttäjä kriittiseksi ja ymmärtämään minkälaisia sähköpostien liitetiedostoja on turvallista avata ja arvioida lähettäjän luotettavuus.

2 Menetelmät

Opinnäytetyön tarkoituksena on tehdä ohjeistus, eli luoda jotain uutta opinnäytetyön toimeksiantajalle. Tällöin menetelmäksi määräytyi toiminnallinen opinnäytetyö. Vilkka ja Airaksinen (2004, 51) toteavat, että selvityksen tekeminen on yksi osa toiminnallisen opinnäytetyön toteuttamistapaa. Toiminnallisen opinnäytetyön lopullisena tuotteena syntyy aina konkreettinen tuote. Tuote voi olla kirja, ohjeistus, opas, tietopaketti tai tapahtuma. Toiminnallisen opinnäytetyön toteutustapaa valittaessa tulee miettiä muoto, jossa lopullinen tuotos viedään kohderyhmälle palvellakseen heitä parhaiten. Tässä opinnäytetyössä ohjeistus luodaan sähköiseen muotoon, ja se viedään yrityksen intranetiin muiden ohjeiden tavoin. Koska pääsääntöisesti opinnäytetyön tekijä maksaa opinnäytetyön tehtävän tuotteen, ei siitä tässä muodossa synny kustannuksia tekijälle. (Airaksinen ym. 2004, 51.). Luotu oheistus viedään käytäntöön ja testaukseen vasta, kun se on hyväksytty valmiina opinnäytetyönä. Kun materiaali tullaan jakamaan sähköisessä muodossa yrityksen intranetissä, on sen päivittäminen jatkossa myös helpompaa.

Tiedonkeruumenetelmistä työssä on käytetty kirjallisuuskatsausta, jonka avulla on hahmoteltu opinnäytetyön aihepiirin kokonaisuutta. Kirjallisuuskatsauksen avulla selvitetään, miten paljon aiheesta on jo olemassa tutkimustietoa sekä näkökulmat ja menetelmät. Lähtökohtaisesti jokaisen opinnäytetyön tulee sisältää teoreettinen viitekehys, joka sisältää opinnäytetyön keskeisimmät käsitteet. Kirjallisuuskatsauksella pyritään selvittämään opinnäytetyön käsitteellistä taustaa ja selvittää, miten työ liittyy jo olemassa oleviin tutkimuksiin. (Hirsjärvi, Remes, Sajavaara 2009, 121.)

Sisällön analysointia tehdään laadullisesta tutkimuksesta. Analysointi sisältää aineiston huolellista lukemista, tekstimateriaalin järjestelyä, sisällön ja materiaalin erittelyä sekä jäsentämistä ja pohtimista. Analyysin tavoitteena on kerätä runsaasta tietomäärästä kiteytettyä tekstiä ymmärrettävästi kohderyhmälle. Analyysin avulla tutkija tiivistää aineistoa, tulkitsee sitä ja käy vuoropuhelua teorian ja oman ajattelun kanssa. (Saaranen-Kauppinen, Puusniekka 2006.)

3 Tietoturvallisuus

Tietoturvallisuus on toimia, joiden avulla pyritään suojaamaan tieto, järjestelmät ja palvelut luottamuksellisina, eheinä ja saatavilla oltavana. Käytännössä tämä tarkoittaa sitä, että tiedot ja tietojärjestelmät pidetään vain niiden käyttöön oikeutettujen saatavilla. Ulkopuolisille ei tule antaa mahdollisuutta käsitellä, muuttaa tai poistaa tietoa. Tiedot, palvelut ja järjestelmät tulee olla luotettavia ja ajan tasalla sekä saatavilla silloin kuin niitä tarvitaan. Niistä ei saisi löytyä haittaohjelmia eikä laitteisto- ja ohjelmistovikoja. (Valtionvarainministeriö 2013.)

Usein tietokoneelle ja eri järjestelmiin kirjaudutaan käyttäjätunnuksella ja salasanalla. Tämä on ensimmäinen konkreettinen vaihe, missä käyttäjän tulee ottaa tietoturva huomioon. Mikä oli salasana? Missä se säilytetään niin, että se pysyy vain omana tietona? Oliko salasana sama, joka oli jo käytössä jossakin muussa palvelussa? Tässä työssä hyvän ohjeistuksen tulee vastata muun muassa näihin kysymyksiin.

4 Hyvän ohjeistuksen perusteet

Kirjassa Tekniikan Viestintä 2010, (Kauppinen, Nummi & Savola) todetaan ohjeiden turvaavan tuotteiden ja palveluiden tarkoituksenmukaisen käytön. Ohjeita ja oppaita tarvitaan, kun työssä kehitetään uusia toimintatapoja tai käyttäjä perehtyy uuden laitteen käyttöön. Riippumatta ohjeistuksen tekijästä ohjeistuksessa käsiteltävä tieto tulee esittää niin, että jokainen sen käyttäjä ymmärtää sitä. Ohjeistuksen laatiminen missä tahansa työtehtävissä on tavanomaista, eikä siihen tarvita olla aiheeseen perehtynyt asiantuntija. Hyvässä käyttöohjeessa käytännön asiantuntemus yhdistyy täsmälliseen kieleen. Ohjeistuksen alussa tulee selvitä,

mitä ohje koskee ja kenelle se on tarkoitettu. Asiallinen ja selkeä ohje parantaa tuotekuvaa, mutta ei pyri mainostamaan sitä. (Kauppinen, Nummi & Savola 2010, 134-136).

Tässä kohdassa on kuvattu ohjeiden tekoon liittyviä prosesseja. Ennen ohjeen kirjoittamista tulee selvittää tuotteen rakenne ja toiminta. Suunnittelussa tulee ottaa huomioon, kenelle ja mihin tarkoitukseen ohje laaditaan sekä pyrkiä kuvittelemaan tuotteen tyypillinen käyttötilanne. Ohjeessa tyypillisesti kuvataan ensin tuotteen normaalikäyttö. Rajoituksien maininta tulee käydä ilmi, ja esittää niille lyhyet perustelut. Ohjeessa tulee ennakoida tyypillisiä ongelmia, joita käyttäjälle voi tulla vastaan tuotteen käytössä. Ohjeissa tulee noudattaa käyttäjän toimintojen aikajärjestystä, ja rakentaa ohje johdonmukaiseksi kokonaisuudeksi. Ohjeen käytännöllisyyden kannalta mahdollisimman selkeä ja helppo kieli on avainasemassa. Ohjeen käytettävyys helpottuu, kun samasta asiasta käytetään aina samaa ilmaisua. (Kauppinen, Nummi & Savola 2010, 136).

Kirjoitetusta ohjeesta tehdään ensin luonnos, josta kerätään palautetta. Palautteen perusteella pyritään tekemään muutoksia puutteellisiin asioihin. Lopullinen ohje tulee testata tositilanteessa aina ennen julkaisua. Ohjeistuksen kirjoittajan tulee pyrkiä ohjaamaan lukijaa ohjeen lukemiseen. Ihmisillä on taipumus ryhtyä heti toimiin luottaen omiin taitoihinsa, ja jättää ohjeet lukematta. Ohjeistuksessa tulee pyrkiä kirjoittamaan ohje oikeaan sävyyn. Pyrkimys on kirjoittaa ohje sellaiseen muotoon, jossa lukijan kykyjä ei yli- eikä aliarvosteta. Hyvässä ohjeistuksessa käyttäjän tulee löytää helposti haluamansa asiakohdat. Lukijalla on mahdollisuus lukea ja käyttää ohjetta eri järjestyksessä kuin se on suunniteltu. Tästä syystä ohjetta tehdessä tulee miettiä eri käyttäjien luku- ja käyttötavat. (Kauppi, Nummi & Savola 2010, 134-136.)

Ohjeissa esiintyvät kuvat ja piirrokset auttavat lukijaa hahmottamaan asian tehokkaammin kuin sanat. Kirjassa Tekniikan Viestintä 2010 todetaan, että esimerkiksi koneen osat ja niiden sijoittuminen kokonaisuuteen voidaan havainnollistaa kuvien kautta paremmin kuin sanoin. Myös kielitaidottomille ohjeistuksen kuvitus on ensiarvoisen tärkeää. Myös ohjeiden testaus on tärkeää ennen julkaisua. Ohjeen tekijä on saattanut jättää mainitsematta sellaista, jota itse pitää itsestään selvänä asiana ja näin lukijalta saattaa jäädä oleellisia asioita tiedostamatta. Ohjeiden testaamisella pystytään välttämään tämä virhe. (Kauppinen, Nummi & Savola 2010, 135).

5 Tietoturvaohjeistus

Tietoturvallisuudella tarkoitetaan tietojen ja palveluiden, järjestelmien ja tietoliikenteen suojaamista ja varmistamista niihin kohdistuvien riskien hallitsemiseksi. Tietoturvallisuuden tavoitteena on tietojen luottamuksellisuuden, eheyden ja käytettävyyden turvaaminen laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisen, tuottamuksellisen tai tapa-

turmaisen tekojen aiheuttamilta uhrilta ja vahingoilta. Tietoturvallisuuden liittyessä yrityksen kaikkeen toimintaan tavalla tai toisella, on henkilöstön sitouttaminen tietoturvaan ja siihen liittyviin toimiin avainasemassa. Henkilöstön tietoturvatietoisuutta tulisi jatkuvasti kehittää. (Valtionvarainministeriö 2007, 13, 52.)

5.1 Laitteet, niiden turvallisuus ja suojaus

Laitteiston turvallisuus käsittää laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niiden hallinnointia. Laitteiden elinkaareen sisältyvät asennukset, takuut, ylläpito ja siihen liittyvät sopimukset sekä poisto muodostavat laitteistoturvallisuuden kokonaisuuden. Kaikkia järjestelmän laitteita on kyettävä seuraamaan, valvomaan ja päivittämään asiaan kuuluvien toimenpitein. (Valtionvarainministeriö 2007, 63.)

Merkittävimmät mobiililaitteisiin kohdistuvat uhat liittyvät fyysiseen turvallisuuteen. Käytännössä tämä tarkoittaa laitteen häviämistä tai varastamista. Fyysisen turvallisuuden parantamiseksi sim-kortille tulee määrittää pin-koodi, jotta liittymän väärinkäyttö toisen henkilön nimissä esiintyminen ei olisi mahdollista. Pin-koodin oletusmerkkisarja tulee vaihtaa heti käyttöönoton yhteydessä. Myös laitteen suojakoodi tulee määrittää, jotta estetään asiattomien henkilöiden pääsy laitteen tietoihin. Suojakoodi tulee muuttaa oletuskoodista, ja puhelimen tulee automaattisesti lukittua kymmenen minuutin aikaviiveellä. (Valtionvarainministeriö 2007, 40, 42.)

Windows -käyttöjärjestelmälle on tehty järjestelmänvalvojan tunnuksia murtavia ohjelmistoja, joilla pystytään selvittämään tai jopa vaihtamaan järjestelmänvalvojan salasanat. Murtamisen jälkeen koneelle on pääsy järjestelmänvalvojan oikeuksin ja näin pääsy kaikkiin käyttöjärjestelmän datoihin. Salaamalla työaseman koko kiintolevy voidaan estää ulkopuolisten tahojen pääsy koneelle tallennettuihin tietoihin. Kiintolevyjen salausmenetelmät ovat kehittyneet, eikä kiintolevyn hidastavaa vaikutusta ole havaittavissa, mikä on johtanut salausmenetelmien yleistymiseen. Salausohjelmistoa käytettäessä tulee varmistaa sen keskitetty käyttö esimerkiksi HelpDeskin toimesta. Niin kutsutun recovery -avaimen käytöllä varmistetaan, että salattuun dataan päästään käsiksi riippumatta käyttäjän toimista. (Laaksonen, Nevasalo & Tumula 2006, 196).

Yrityksen tietoturvakäsikirja – ohjeistus, toteutus ja lainsäädäntö kirjassa kirjoittajat kuvaavat haittaohjelmia sovelluksilla, joita käyttäjä ei ole aikonut suorittaa. Haittaohjelmiksi kutsutaan myös ohjelmistoja, jotka aiheuttavat tahallisesti tai tahattomasti haittaa yrityksen tietojärjestelmissä. Lisäksi huijausviestit sekä vakoilu ja mainosohjelmat voidaan luokitella tähän kategoriaan. Haittaohjelmien torjunnassa tulisi ottaa huomioon seuraavia asioita; tulee tehdä selvitys, mitä haittaohjelmat tekevät ja mitä ne näyttävät tekevän. Käyttäjäkunnalle tulee olla ohjeistus siitä, miten voi välttää haittaohjelman tartunnan ja miten toimia mahdol-

lisen tartunnan tapahtuessa. Haittaohjelmien tartunnan välttämiseksi ohjeistuksessa tulee olla selkeät kiellot tiettyjen tiedostojen, liitteiden ja viestien avaamiseksi. (Laaksonen, Nevasalo & Tumula 2006, 163.)

5.2 Sähköpostin ja internetin käytön periaatteet

Sähköpostin käyttöä voidaan vähäisessä määrin sallia työntekijän omien asioiden hoitamiseen. Työntekijää tulisi ohjeistaa hoitamaan henkilökohtaista sähköpostia omien asioiden hoitamiseen. Tällä toimenpiteellä voidaan välttyä henkilökohtaisen työsähköpostiosoitteen päätymistä roskapostilistoille. Sähköpostin käytössä jatkuvasti kasvava roskapostin määrä on merkittävin ongelma. Myös tietojen kalastelu, niin sanottu phishing on lisääntynyt viime aikoina merkittävästi. Tietojen kalastelussa pyritään kalastelemaan tietoja, erityisesti pankkitunnuksia kalasteluviestien uhreilta. (Laaksonen, Nevasalo & Tumula 2006, 164, 206.)

Internetin käyttöä voidaan sallia, rajata tai estää. On järkevää sallia internetin käyttö, mutta laatia sille selkeät käytännöt ja rajoitukset. Yrityksen tulee tiedostaa verkon käyttöön liittyvät tietoturvariskit sekä ottaa huomioon verkon käytöstä aiheutuvat riskit ja haitat. Sopimaton internetin käyttö tulee kieltää yksiselitteisesti. Myös lain kieltämä toiminta, kuten laiton tiedostojen jako ja laittoman materiaalin hallussapito tulee kieltää käyttäjältä. (Laaksonen, Nevasalo & Tumula 2006, 164.)

5.3 Käyttäjätunnus ja salasanaohjeistus

Käyttäjätunnus ja salasana ovat henkilökohtaisia. Käyttäjätunnukseen liitetty salasana tulee olla vain sen käyttöön oikeutetun henkilön tiedossa. Järjestelmän ylläpitäjän tulee määrittää salasana niin, että se on riittävän pitkä ja vaihdettava tarpeeksi usein. Ohjeistuksessa tulee olla maininta työpaikan verkkotunnuksen ja henkilökohtaisten verkkopalveluiden salasanojen eroavaisuuksista. (Laaksonen, Nevasalo & Tumula 2006, 166.)

Valtionvarainministeriön Sisäverkko-ohjeistukessa määritellään salasanalle seuraavat vaatimukset; Salasanan pituus tulee olla vaatimusten pituinen, usein vähintään 10 merkkiä. Salasanassa pitää olla sekä isoja ja pieniä kirjaimia sekä numero, mutta myös useimmat erikoismerkit kelpaavat. Salasanan enimmäisikä saa olla enintään 90 vuorokautta, eikä vaihtaessa saa käyttää jo käytettyjä salasanoja. Yritettäessä kirjautua väärällä salasanalla palveluun tulee tunnuksen lukittua väärinkäytöksien estämiseksi. (Valtionvarainministeriö 2010, 76-77.)

5.4 Verkot ja yhteydet

Verkkoyhteyden suojaus pyrkii aina siihen, että yhteydellä siirrettävän tiedon luottamuksellisuus ja eheys säilyvät. Yleisien tietoliikenneverkkojen kauppa kulkevat verkkoyhteydet ovat

alttiita erillaisille tietoturvahyökkäyksille. Salakuuntelemalla tiedon luottamuksellisuus, eheys ja saatavuus ovat uhattuna. (Valtionvarainministeriö 2003, 39.)

Verkkoliitännän toteuttamisessa yleistyvät langattomat liitäntätavat kuten wlan ja mobiilidatayhteys parantavat käyttömukavuutta, mutta kasvattavat tietoturvariskejä. Langatonta liitäntää käytettäessä tarvitaan ylimääräisiä varatoimia. Langattomia yhteyksiä käytettäessä tulisi aina käyttää Virtual Private Network- tekniikkaa (VPN), jolla pystytään salaamaan lagattomat tietoliikenneyhteydet. (Valtionvarainministeriö 2003, 38.)

Älypuhelimen wlan ja bluetooth-yhteydet tulee poistaa käytöstä, kun ne eivät ole käytössä. Laiteasetuksista tulee tietoturvan parantamiseksi määrittää siten, että laitteet tila on piiloitettu eikä se mainosta itseään muille laitteille. Laite tulee nimetä myös siten, että käyttäjää ei voida siitä tunnustaa tai päätellä. Matkapuhelimen wlan-yhteyttä käytettäessä suojaamattomissa verkoissa, muodostavat ne samanlaisen vaaran kuin työasemat. Tällöin liikenne tulee muodostaa vpn-yhteyden yli. (Valtionvarainministeriö 2007, 43.)

5.5 Matkakäyttö ja etäyhteydet

Etätöiden suosio ja työnantajan tarjoama mahdollisuus siihen on kasvanut viime aikoina paljon. Kirjassa Syntynyt digiaikaan 2010, todetaan että nettisukupolven edustajia haastatellessa 69 prosenttia haluaa työskennellä missä ja milloin vain. Työajan joustot ja luontaisedut ja ovat tärkeitä tekijöitä työssä viihtymisen kannalta. (Don Tapscott 2010, 177). Etätöitä etäyhteyksiä käyttäen tulee ohjeistaa käyttäjäkuntaa sitä varten laaditulla tietoturvaohjeistuksella. Työntekijöiden ja johdon käyttämät etäyhteydet tulee varmistaa tietoturvallisuuden lisäämisellä, koulutuksella ja motivoinnilla. Etätöissä käytettävien laitteiden tiedot ja niiden välitys asettavat erityisiä haasteita tiedon turvaamiseksi. Laitteille ja järjestelmiin kirjautuminen tulee olla tarpeeksi vahvaa ja näiden sisältämä luottamuksellinen tieto tulee salata. Käyttäjät ohjeistetaan noudattamaan erityistä huolellisuutta laitteiden käsittelyssä, jotta vältyttäisiin laitteiden ja tiedon katoamiselta ja varkauksilta. (Valtiovarainministeriö 2007, 66-67).

Tietojenkäsittelylaitteiden, lähinnä kannettavien tietokoneiden, tablettien ja matkapuhelimien matkakäytön ohjeistus liittyy olennaisesti tietovälineiden käsittelyyn. Bios -salasanat, käynnistyssalasanat ja tietojen salaus eivät takaa laitteen datan tietoturvaa laitteen katoamisen jälkeen. Matkakäytössä turvallisuutta voidaan parantaa vähentämällä mukana kuljetettavan tiedon määrää ja käyttämällä erilaisia etätyöhön liittyviä ratkaisuja, kuten suojattuja etäyhteyksiä. (Laaksonen, Nevasalo & Tumula 2006, 164, 168.)

5.6 Turvallinen tietovälineiden käsittely

Yritysten käytössä olevien tietojen käsittely- ja säilytyslaitteiden määrä on kasvanut nopeasti. Lukuiset pieneen kokoon ja suureen tallennuskapasiteettiin kykenevät tallennusvälineet ovat tulleet markkinoille. Tietoturvaohjeistuksen tulee pysyä tekniikan kehityksen mukana. Fyysisen turvallisuuden, tietoliikenne- ja laitteistoturvallisuuden sekä ohjelmistoturvallisuuden tulisi kattaa myös nämä pienet mobiililaitteet ja tallennusvälineet. Tietovälineiden käsittelyssä ja ohjeistuksessa tulee huomioida seuraavia asioita. Käyttäjälle tulee selvitä, mitä tietoja voidaan säilyttää liikuteltavilla tallennusvälineillä. Tietoliikenneyhteydet tulee varmistaa suojatuiksi sekä tehdä varmistuskäytännöt selviksi. Tietovälineiden rikkoutuessa tai hävitessä tulee olla ohjeistus ja ylläpitäjillä tulee olla mahdollisuus rajoittaa ja valvoa tiettyjen tallennusvälineiden käyttöä. (Laaksonen, Nevasalo & Tumula 2006, 164).

5.7 Julkisella paikalla toimiminen

Julkisilla paikoilla toimiessa tietoturvaa voidaan parantaa vähentämällä mukana kuljetettavan tiedon määrää. Tyypillisesti se onnistuu käyttäen suojattuja etäyhteyksiä yrityksen verkkoon, jolloin tiedostot eivät sijaitse fyysisellä levyllä. Ulkoiset tallennuslaitteiden koot ovat pienentyneet merkittävästi, joten niiden mahdollisuus unohtamiseen tai kadottamiseen on suurempi. Julkisilla paikoilla olan yli kuvaaminen tai jopa näytön valokuvaaminen on mahdollista. Verkon valinta tulee miettiä tarkoin, ottaako yhteyden kahvilan suojaamattomaan langattomaan verkkoon tai asiakasyrityksen tarjoamaan lankaverkkoon. Salasanojen tallentaminen laitteen muistiin ei ole tietoturvallinen ratkaisu. Myöskään laitteiden sovellukset eivät saa muistaa käyttäjän salasanoja automaattisesti. Laitteet ja tallennusvälineet on hyvä suojata salasanoilla ja suojakoodeilla, jolla voidaan estää ulkopuolisien pääsy laitteen tietoihin sen kadotessa. (Laaksonen, Nevasalo & Tumula 2006, 164.)

6 Yhteenveto ja johtopäätökset

Työn tekeminen on siirtynyt yhä enemmän pois toimistolta kotiin, mutta myös asiakkaan työtiloihin ja muihin julkisiin tiloihin. Samalla kun työt siirtyvät toimistolta pois, voi työntekoon soveltuvat laitteet ja työkalut muuttua matkapuhelimiin ja taulutietokoneisiin. Laitteiden kulkiessa käyttäjillä mukana, pyrkivät laitevalmistajat tekemään niistä mahdollisimman ohuita ja kevyitä. Tämän myötä laitteiden liittimiä pyritään karsimaan, sekä kehittämään niistä entistä pienempiä. Lukuiset pilvipalvelut ja niiden yleistynyt käyttö ovat osaltaan vähentäneet esimerkiksi fyysisten massamuistien ja muistitikkujen käyttöä. Tarvittava data voidaan tallentaa verkkoyhteyden yli palveluntarjoajan konesaliin, eli pilveen. Kun toimintaympäristömme ja laitteemme muuttuu, tulee meidän kiinnittää entistä enemmän huomiota hyviin tietoturvakäytäntöihin ja päivittää tietomme vastaamaan tämän päivän haasteisiin.

Työn tavoitteena oli tehdä tietoturvaohjeistus käyttäjille. Ohjeistusta tullaan testaamaan hyvän ohjeistuksen kriteerien mukaisesti ennen ohjeistuksen vientiä käytäntöön. Tietoturva koostuu useasta palasista, ja käyttäjät ja niiden toimet ovat vain yksi osa sitä. Ohjeistus antaa käyttäjälle valmiuden ennalta ehkäistä monia tietoturvariskejä.

Lähteet

Kirjalliset lähteet

Airaksinen, T. & Vilkka, H. 2004. Toiminnallinen opinnäytetyö. Helsinki: Tammi.

Hirsjärvi, S., Remes, P.& Sajavaara, P. 2009. Tutki ja kirjoita. Hämeenlinna: Kariston kirjapaino

Kauppinen, A., Nummi, J. & Savola, T. 2010. Tekniikan Viestintä - Kirjoittamisen ja puhumisen käsikirja. Helsinki: Edita Prima.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing.

Tapscott, D. 2010. Syntynyt digiaikaan; Sosiaalisen median kasvatit. Porvoo: WS Bookwell.

Sähköiset lähteet

Saaranen-Kauppinen, A. & Puusniekka, A. 2006. KvaliMOTV - Menetelmäopetuksen tietovaranto. Viitattu 31.10.2016.
http://www.fsd.uta.fi/menetelmaopetus/

Valtionvarainministeriö. 2003. Turvallinen etäkäyttö turvattomista verkoista. Viitattu 27.11.2016
https://www.vahtiohje.fi/c/document_library/get_file?uuid=370c931e-fe24-4061-b5ac-91f3cc81e28d&groupId=10128

Valtiovarainministeriö. 2007. Tietoturvallisuudella tuloksia: Ohje tietoturvallisuuden johtamiseen ja hallintaan. Viitattu 8.5.2016.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=d0bc6cbd-1626-47aa-99d7-01352f5aede1&groupId=10229

Valtionvarainministeriö. 2007. Älypuhelimien tietoturvallisuus – Hyvät käytännöt. Viitattu 27.11.2016.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=6f3827e9-75bc-4ce8-be73-1166cdee10a5&groupId=10128

Valtionvarainministeriö. 2010. Sisäverkko-ohje. Viitattu 27.11.2016.
https://www.vahtiohje.fi/c/document_library/get_file?uuid=5084ce47-32bf-4025-bcc1-73fc2de4edad&groupId=10229

Valtionvarainministeriö. 2013. Tietoturvallisuus – Mitä se on? Viitattu 31.10.2016.
https://www.vahtiohje.fi/web/guest/691

Liitteet

Liite 1: Ohjeistus

Tämä ohjeistus sisältää keskeisimmät osa-alueet, joiden avulla käyttäjät voivat parantaa omilla toimillaan yrityksen tietoturvaa. Ohjeistus koskee salasanoja, laitesuojausta, sähköpostin käyttöä, verkkoyhteyksiä, massamuistien käyttöä sekä julkisilla paikoilla työskentelyä.

Salasanat

- Vaihda annetut salasanat välittömästi uusiin.
- Pyri käyttämään salasanassa isoja ja pieniä kirjaimia, numeroita ja erikoismerkkejä
- Älä luovuta käyttäjätunnuksia ja salasanoja toisen osapuolen tietoon
- Älä käytä samaa salasanaa toisessa järjestelmässä
- Älä kirjoita salasanoja selkokielisinä talteen laitteeseen muistiin, paperille yms.

Laitesuojaus

- Ota käyttöön suojakoodit ja pin –koodit
- Älä käytä oletuskoodeja ja salasanoja
- Vaihda koodit säännöllisesti uusiin
- Pidä virustorjuntaohjelmistot ajan tasalla

Sähköposti

- Salaa sähköposti tarvittaessa lähettäessä organisaation ulkopuolelle sähköpostia
- Käytä sähköpostin allekirjoitusta
- Älä avaa epäilyttävistä osoitteista tulevien viestien linkkejä tai liitteitä
- Tarkista postin lähettäjän nimen lisäksi oikea sähköpostiosoite, mistä viesti saapunut

Yhteydet

- Sammuta käyttämättömät yhteydet
- Käytä mobiili -yhteyttä aina, kun et voi varmistaa wlan -yhteyksien turvallisuutta
- Avoimissa wlan -verkoissa salaa liikennöinti vpn –yhteyksillä

Massamuistit

- Älä säilytä arkaluontoista materiaalia muistitikulla
- Huolehdi muistitikun materiaalin varmuuskopioinnista
- Älä kytke vieraiden muistitikkuja koneeseen

Työskentely julkisissa tiloissa

- Älä hukkaa laitteita
- Kiinnitä huomiota ympäristöön. Varo olanylikatselua, valokuvausta sekä salakuuntelua
- Kiinnitä huomiota käytettävään verkkoon. Vieraissa verkoissa koneen tietoja voidaan yrittää urkkia.