KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikan koulutusohjelma / tietoverkkotekniikka

Petri Keltanen

TIETOTURVAKOULUTUKSEN SUUNNITTELU KOTKAN KAUPUNGILLE

Opinnäytetyö 2011

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Tietotekniikka

KELTANEN, PETRI	Tietoturvakoulutuksen suunnittelu Kotkan kaupungille
Opinnäytetyö	32 sivua + 12 liitesivua
Työn ohjaaja	Laboratorioinsinööri Marko Oras
Toimeksiantaja	Kotkan kaupunki
Helmikuu 2011	
Avainsanat	tietoturvapolitiikka, koulutus, verkko-oppiminen, tietoturva

Tietokoneilla tehdyt rikokset kasvavat koko ajan. Erityisesti tähän ongelmaan ovat heränneet isot organisaatiot, sillä niillä on eniten suojattavaa omissa verkoissaan. Organisaatiot voivat kyllä määritellä ohjeita ja sääntöjä työntekijöilleen, mutta ne ovat turhia, jos käyttäjät eivät ymmärrä, mistä puhutaan. Siksi koulutus on tärkeää.

Kotkan kaupunki on ottanut asian huomioon ja on siksi aloittamassa tietoturvan koulutusta. Sen tarkoituksena on opettaa työntekijöille tietoturvallista työskentelytapaa, jonka voi siirtää myös kotiin.

Opinnäytetyössä on käyty läpi, millä tavalla koulutus on suunniteltu toteutettavaksi. Koulutuksen pääasialliseksi tavaksi on otettu verkko-oppimisympäristö, jota tuetaan tietoturva-sivustolla, käyttäjien osaamisen kartoituksella ja lähiopetuksella.

Suurimmaksi osaksi opinnäytetyö oli koulutuksen suunnittelua. Käytännön osuus jäi tietoturva-sivuston tekemiseen ja julkaisuun kaupungin työntekijöille.

Koulutuksen tuloksia ja opinnäytetyön lopullista onnistumista on vaikea arvioida, koska varsinaista koulutusta ei ole vielä toteutettu. Alustavasti kuitenkin voidaan sanoa, että työ oli onnistunut, sillä palaute oli positiivista esimiehiltä ja kaupungin johdolta.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Information Technology

KELTANEN, PETRI	IT Security Training for the Employees of the City of Kotka
Bachelor's Thesis	32 pages + 12 pages of appendices
Supervisor	Marko Oras, Laboratory Engineer
Commissioned by	City of Kotka
February 2011	
Keywords	security policy, IT security, training, E-Learning

This thesis deals with a plan for conducting IT security training for the employees of the city of Kotka. The training is based on the security policy that the city of Kotka has adopted. It is also part of the internal security plan of the Kymenlaakso Region.

As no training plan had been used before, the plan had to be created without the support of any existing groundwork. All information was mainly collected from books and various websites. The resulting training plan has four main sections: an E-Learning center, an inquiry conducted among employees concerning their skills of IT security, a website where employees can find more information about the training or IT security, and an actual training event.

As yet, the results of the study are hard to perceive because the training of the employees is incomplete. Nevertheless, the management expressed their satisfaction with the plan.

Because the training is still going on, it is difficult to make any depth analysis about it. So far, all feedback from the participating employees has been positive.

SISÄLLYS

TEKNINEN SANASTO

Tietoturvariski	Tietoon, tietoliikenteeseen tai tietojärjestelmään kohdistuva vahingon vaara
Tietoturva	Tietoturvallisuuden synonyymina erityisesti yhdyssanoissa käytettävä termi
Tietoturvallisuus	Järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus
Tietosuoja	Ihmisen yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä
Tallennusmedia	Väline, johon pystyy tallentamaan tietoa, esimerkiksi CD-levy, DVD- levy, USB -muistitikku
Pilvipalvelu	Pilvipalveluilla tarkoitetaan verkossa tarjottavaa, yleensä selaimella käytettävää ohjelmaa tai sovellusta, joka tuotetaan palveluna yhdestä paikasta monen tahon käyttöön
Audiotiedosto	Äänitiedosto, sisältää puhetta tai musiikkia
Demo-tunnus	Käyttäjätunnus, jolla voidaan ilmaiseksi tutustua tuotteeseen
Referenssi	Viittaus nykyisiin tai entisiin asiakkaisiin
HTML- koodi	Hypertext Markup Language, Internet-sivujen tekemiseen tarkoitettu kuvauskieli
Loppukäyttäjä	Tietojärjestelmäpalvelujen käyttäjä

1 JOHDANTO

Kotkan kaupunginvaltuusto hyväksyi 1.3.2010 kaupungille tietoturvapolitiikan. Tietoturvapolitiikan hyväksyminen oli lähtölaukaus tietoturvakoulutuksen suunnittelulle ja järjestämiselle Kotkan kaupungin henkilökunnalle, koska tietoturvapolitiikassa niin määriteltiin. Opinnäytetyö kertoo, miten tietoturvakoulutus on suunniteltu järjestettäväksi kaupungin henkilöstölle.

Opinnäytetyö on samalla osa Etelä-Kymenlaakson sisäisen turvallisuuden ohjelmaa. Sisäisen turvallisuuden ohjelman periaatteet on määritellyt valtioneuvosto ja sen osa-alueita ovat muun muassa kodin, vapaa-ajan ja liikkumisen turvallisuuden parantamisesta terrorismintorjuntaan. Opinnäytetyö sijoittuu tietoverkkorikollisuuden ja Internetin käyttöön liittyvien riskien torjunnan alle. Sisäisen turvallisuuden ohjelman tarkoitus on tehdä Suomesta Euroopan turvallisin maa vuoteen 2015 mennessä [1,5].

Kotkan kaupungilla on työntekijöitä noin 3500 henkilöä ja erilaisia työasemia noin 2400 kappaletta. Työasemien määrästä johtuen tietoturvallisuus on tärkeä asia, sillä jo yksittäinen päivittämätön työasema voi aiheuttaa tietoturvariskin. Myös Suomen laissa on säädetty määräyksiä tietoturvan hoitamisesta [2,18]. Kotkan kaupungin tietoturvapolitiikka määrittää suuntaviivat, miten tietoturvaa on kehitettävä ja ketkä ovat siitä vastuussa.

Opinnäytetyön tekeminen on ollut mielenkiintoista, koska opinnäytetyö on rakennettu niin sanotusti tyhjän päälle, eli ei ollut mitään valmista mallia mitä olisi käytetty. Alussa työ oli teoreettista, koska tutkittiin ja lisättiin omaa osaamista aiheesta. Tietoa etsittiin Internetistä ja lukemalla alan kirjallisuutta. Jälkikäteen ajatellen oman tiedon lisääminen aiheesta oli onnistunut päätös, aihealueen laajuudesta johtuen. Hyvät perustiedot auttoivat projektin eteenpäin vientiä myöhäisemmässä vaiheessa.

Hyvin nopeasti saatiin kasaan runko, jota lähdettiin kehittämään. Runko koostuu neljästä elementistä: verkko-oppimisympäristöstä, loppukäyttäjien tietoturvan osaamisen kartoittamisesta, Tietoturva-sivustosta ja varsinaisesta käyttäjien koulutustilaisuudesta.

2 MITÄ TIETOTURVA ON?

2.1 Tietoturva yleisesti

Tietoturvalla (joka on sama asia kuin tietoturvallisuus) tarkoitetaan tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaamista. Tietoturvallisuuden uhkina pidetään esimerkiksi erilaisia huijausyrityksiä, henkilökohtaisen yksityisyyden loukkauksia, roskapostia, teollisuusvakoilua, piratismia, tietokoneviruksia, verkkoterrorismia ja elektronista sodankäyntiä. [3]

Eri asioissa tietoturva on erilainen. Esimerkiksi tietoturvallisen word-dokumentin luonti on erilaista kuin tietoturvallisen paperiarkiston teko. Siksi on tärkeää, että ymmärretään, mitä tietoturva isona kokonaisuutena pitää sisällään. Sen jälkeen voidaan miettiä, mitkä tietoturvan osa-alueet osuvat konkreettisesti yhteen tärkeänä pidetyn asian kanssa.

2.2 Saatavuus, luotettavuus, eheys

Perinteisesti tietoturvan kolme perustetta ovat olleet **saatavuus** (vain luvan saaneet henkilöt pääsevät käsiksi tietoihin), **luottamuksellisuus** (tiedot eivät joudu vääriin käsiin) ja **eheys** (tiedot eivät muutu ja niitä ei pysty väärentämään). [4]

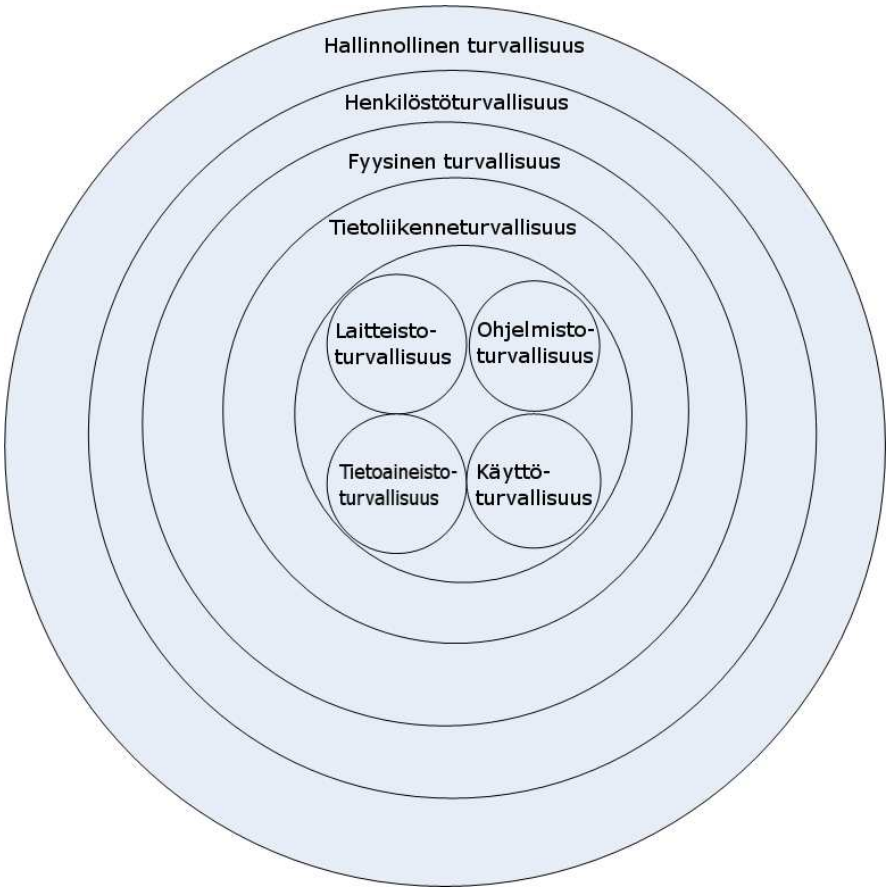
Esimerkiksi jos pitää luoda tietoturvallinen kauppakirja, ensiksi varmistetaan, että kauppakirja tullaan laittamaan paikkaan, jossa se pysyy tallessa, esimerkiksi arkistokaappiin (saatavuus). Seuraavaksi halutaan varmistaa, että kukaan ulkopuolinen ei näe kauppakirjaa, koska se sisältää henkilökohtaisia tietoja. Sen takia hankitaan arkistokaappiin lukko (luottamuksellisuus). Viimeiseksi otetaan kopiot osapuolille kauppakirjasta, todistajien läsnä ollessa, joten kukaan ei voi jälkikäteen väittää, että kauppaa ei ole tehty tai on maksettu väärä rahasumma (eheys).

Kuten esimerkistä voidaan nähdä, tietoturvallisuus ei liity pelkästään tietokoneisiin tai isojen organisaatioiden sisäisiin asioihin. Se koskettaa meitä jokaista arkipäiväisissä asioissa.

2.3 Tietoturvan osa-alueet

Jotta saavutettaisiin tiedoille tietoturvan kolme perustetta, otetaan avuksi tietoturvan kahdeksan eri osa-aluetta. Nämä osa-alueet auttavat hahmottamaan, mitä tarvitaan saavuttamaan tietoturvan kolme perustetta.

Kuvassa 1 on kuvattu tietoturvan osa-alueet sipulimallina. Voidaan ajatella, että päällimmäinen kerros (hallinnollinen turvallisuus) on se, mikä näkyy eniten työntekijöille yritysmaailmassa. Siihen kuuluu ohjeiden ja määräyksien antaminen. Alemmilla kerroksilla noudatetaan ohjeita, joita on annettu ylimmällä kerroksella.



Kuva 1. Tietoturvan osa-alueet.

Mallin ytimessä olevat osa-alueet (laitteistoturvallisuus, ohjelmistoturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus) ovat niitä, joitten kanssa organisaation työntekijät ovat eniten kosketuksissa, mutta mitä työntekijät eivät välttämättä miellä kuuluvaksi tietoturvaan.

Yritys voi kyllä toimia vaikka ensimmäinen kerros otettaisiin pois, mutta toiminta ei välttämättä olisi yhtä tehokasta, koska yhteiset pelisäännöt puuttuvat. Tämä aiheuttaa helposti sen, että työntekijät tekevät omia päätöksiä ja se voi johtaa toimintaan joka vaarantaa yrityksen tietoturvan.

2.3.1 Hallinnollinen turvallisuus

Hallinnollinen tietoturvallisuus on tietoturvan osa-alueiden perusta. Käytännössä se tarkoittaa esimerkiksi kaupungin tai yrityksen laatimaa tietoturvapolitiikkaa, josta käy ilmi miten organisaatio hoitaa tietoturvan järjestämisen [2,146]. Kauppakirjaesimerkissä hallinnollisena tietoturvana voidaan pitää sitä, että on tehty päätös ostaa lukollinen arkistokaappi, johon talletetaan kaikki tärkeät ja luottamukselliset paperit.

Isoimmissa organisaatioissa tietoturvapolitiikan tarkoitus on myös selkeyttää ja yhtenäistää organisaation tapoja liittyen tietoturvaan. Näin organisaation johto voi hallita luottamuksellisten papereiden käsittelyä ja työntekijöiden ei tarvitse miettiä miten asiat hoidetaan, jos he vaihtavat organisaation sisällä toimipistettä.

Tietoturvapolitiikassa otetaan usein myös huomioon tarve työntekijöiden koulutukseen. Tämä onkin yhteisten pelisääntöjen ohella tärkein asia tietoturvapolitiikassa. Vaikka hyvät ohjeet olisi tehty, eivät ne välttämättä avaudu työntekijöille, joilla ei ole teoreettista osaamista asiasta. Tietoturvan tapauksessa koulutus on erittäin tärkeää, koska aihe on monille vieras teoriatasolla ja jotkin sanat tai termit vaativat selitystä. Yleensä käytännön esimerkit toimivat paremmin kuin pelkkä teoriapohjainen diaesitys [2,255].

2.3.2 Henkilöstöturvallisuus

Henkilöstöturvallisuus keskittyy henkilöstön aiheuttamien riskien torjumiseen. henkilöstön aiheuttamaa riskiä torjutaan yleensä koulutuksella ja tiedonsaanti- ja käyttöoikeuksia rajaamalla [5,41]. Esimerkiksi ei anneta avainta arkistokaappiin epäluotettavalle naapurille. Tällä tavalla estämme mahdollisen kauppakirjan häviämisen tai väärentämisen.

Koulutus taas auttaa työntekijöitä huomaamaan, miten omaa työskentelyä voisi parantaa tietoturvan osalta. On mahdollista, että työntekijä ei itse edes tiedosta tekevänsä jotain asiaa tietoturvattomasti. Tämän takia on suotavaa, että pienillä muistutuksilla palautetaan työntekijän mieleen oikeanlaista työskentelyä. Vanha viisaushan on, että kertaus on opintojen äiti.

Henkilöstön kouluttamiseen liittyy, etenkin julkisella puolella, lainsäädännön osaaminen ja tietäminen. Pahimmassa tapauksessa puutteellinen lainsäädännön osaaminen aiheuttaa julkiselle organisaatiolle joko imagollisia tai jopa rahallisia menetyksiä, esimerkiksi sakkojen muodossa. Esimerkiksi terveydenhuoltopuolella hoitaja saattaa vahingoissa kertoa potilaastaan tietoja ulkopuoliselle, jotka aiheuttavat vahinkoa potilaalle. Potilas saa kuulla tapahtuneesta ja nostaa oikeusjutun kyseistä hoitolaitosta vastaan. Näin julkiselle organisaatiolle aiheutuu sekä rahallista ja imagollista tappiota tapahtumasta.

2.3.3 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan tiettyjen kohteiden suojaamista onnettomuuksilta ja ilkivallalta. Jos käytämme arkistokaappiesimerkkiä: ei pidetä arkistokaappia ulkona, jossa kuka tahansa voi päästä sen luokse, vaan siirretään se työhuoneeseen, jonka ovea pidetään lukossa. Näin ollen arkistokaappi on suojattu ulkopuolisten silmiltä.

Isommassa mittakaavassa fyysiseen turvallisuuteen kuuluu muun muassa toimitilojen kulunvalvonta, murto-, palo- ja vesivahinkohälytysten käyttäminen, ohjeet miten toimitiloihin tulevia vieraita käsitellään ja laitteiden sijoittelu. [5,42]

Toimitilojen kulunvalvonta on tärkeää, koska jos ulkopuoliset saavat kulkea toimitiloissa miten sattuu, he saattavat päästä käsiksi luottamuksellisiin papereihin, esimerkiksi potilastietoihin. Kuluvalvontaa on jo se, että toimitilojen ovet pidetään lukossa.

Erilaisten hälytysjärjestelmien käyttö auttaa myös parantamaan tietoturvallisuutta. Esimerkiksi murtohälyttimillä voidaan vaikuttaa siihen, että tiedot eivät päädy ulkopuolisille murron yhteydessä tai tiedot pelastuvat tulipalolta palohälytyksen johdosta.

Toimitiloihin tulevien vieraiden ohjaaminen ja laitteiden käsittely liittyvät läheisesti yhteen. Ohjeistuksessa on hyvä ottaa huomioon, millä tavalla tuntemattomat henkilöt ohjataan oikean henkilön luokse: jätetäänkö vieras odottamaan taukotilaan, oman työpisteen luokse vai pyydetään seuraamaan oikean henkilön luokse. Jos vierasta pyydetään odottamaan, pitää esimerkiksi oma työasema lukita ja tärkeät paperit laittaa lukittuun kaappiin. Tällä ehkäistään luottamuksellisten tietojen vuotaminen ulkopuoliselle. Etenkin asiakaspalvelutehtävissä olevien kannattaa ottaa huomioon paperien ja näytön sijainti työpöydällä, etteivät näytöllä olevat tiedot näy heti vieraalle, kun hän tulee toimitilan ovesta sisään. Ikinä ei voi tietää, millä asialla vierailija oikeasti on.

2.3.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus tarkoittaa sähköpostin, Internetin ja etäyhteyksien turvallista käyttöä. Turvallinen käyttö määritellään organisaation omilla ohjeilla ja säännöillä. Esimerkiksi ohjeissa määritellään, millä tavalla etäyhteys voidaan ottaa ja millä tavalla se salataan. Myös Internetin ja sähköpostin käyttöön liittyvät ohjeet kuuluvat tietoliikenneturvallisuuteen. [5,43]

Suurin haaste tällä hetkellä on salauksiin liittyvin käytäntöjen puutteet. Puutteet johtuvat vaikeasti käytettävistä ohjelmista ja puutteellisesta koulutuksesta. Myös organisaatioiden väliset erot ohjeissa ja salauksien toteuttamisessa aiheuttavat ongelmia. Salaus on kuitenkin tärkeä asia, sillä esimerkiksi salaamattoman sähköpostin voi periaatteessa kuka tahansa Internetin käyttäjä kaapata ja lukea.

Tässäkin asiassa on korostettava käyttäjien koulutusta ja ohjeistusta. Vaikka organisaatio hankkisi tehokkaimmat ja uusimmat salausohjelmat, ei niistä ole hyötyä, jos henkilöstö ei käytä tai pahimmassa tapauksessa edes tiedä, että organisaatiossa on käytössä salauksen mahdollistamaa teknologiaa.

Etäyhteyksissä tilanne on parempi, sillä suurin osa organisaatiosta vaatii kirjallista sopimusta, jos henkilöstö haluaa ottaa etäyhteyden organisaation palvelimiin. Yleensä etäyhteydet otetaan organisaation tarjoamalla kannettavalla, joten lähtökohtaisesti voidaan olettaa, että kannettavan työaseman tietoturva on samalla tasolla kuin organi-

saation sisällä olevien työasemien. Monesti etäyhteyttä ei edes pysty ottamaan muilla kuin organisaation hyväksymillä työasemilla.

2.3.5 Laitteistoturvallisuus

Laitteistoturvallisuudella tarkoitetaan lähinnä laitteiden sijoittelua niin, että niistä ei tule häiriöitä ja keskeytyksiä työskentelyyn [5,46]. Laitteistoturvallisuudessa kannattaa ottaa huomioon, millä tavalla organisaation henkilöstö ohjeistetaan käyttämään esimerkiksi USB-muistitikkuja. On parempi, jos organisaatio itse ostaa oheislaitteet henkilöstölle, kuin että työntekijät ostavat itse oheislaitteet. Näin organisaation tietohallinto pystyy seuraamaan, mitä laitteita liikkuu organisaatiossa ja kenellä ne ovat käytössä. Samalla myös helpottuu mahdolliset takuuhuoltoon liittyvät asiat. Nyrkkisääntönä voidaan pitää, että kaikki laitteiston hankinnat menevät organisaation tietohallinnan kautta ja omien oheislaitteiden tuonti ja käyttö työpaikalla on kiellettyä.

2.3.6 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus on laaja-alainen osa-alue. Siihen kuuluu muun muassa työasemien käyttöjärjestelmät, käytettävät ohjelmat (esimerkiksi Internet-selain), tietoturvaohjelmistot, organisaation palvelimet ja ohjeiden luominen ohjelmistojen käytölle ja hankkimiselle [5,47].

Ohjeiden luomisessa on otettava erityisesti huomioon, mitä ohjelmia henkilöstö saa asentaa työasemalleen. Suurimmassa osassa organisaatioita on lähtökohtaisesti kielletty omien ohjelmien asentaminen ilman tietohallinnon lupaa. Tämä varmistetaan rajaamalla käyttöoikeuksia käyttöjärjestelmästä niin, että käyttöjärjestelmä ei edes anna lupaa asentaa ohjelmia. Tietohallinto hoitaa kaikki ohjelmistojen asennukset suoraan omilla ylläpito-tunnuksilla. Omien ohjelmien lataus ja asennus on kielletty, koska omista ohjelmista voi tulla haittaohjelmia työasemaan ja lataaminen Internetistä kuormittaa organisaation tietoverkkoa ja näin ollen hidastaa sen käyttöä.

Nykyisin tietohallinnon on helppo suodattaa pois ne Internet-sivustot, jotka organisaation johto on katsonut tarpeettomiksi työtehtäviä ajatellen. Tämä myös auttaa pitä-

mään organisaation työasemat viruksista vapaana, koska sisällönsuodatus estää suoraan pääsyn sivustoille, joilta voi saada tartunnan koneelle.

Uutena uhkana ohjelmistoturvallisuudelle ovat nousseet erilaiset matkapuhelimiin tulevat virukset [6]. Onneksi nämä virukset ovat vielä sellaisia, että ne eivät osaa itseään asentaa matkapuhelimeen, eli käyttäjän pitää asentaa ohjelma, jossa virus on. Näin ollen terveellä järjellä ja ajattelulla pystytään vielä toistaiseksi estämään matkapuhelimeen tulevat virukset. Jos haluaa pelata varman päälle, voi asentaa matkapuhelimeensa samankaltaisen virustorjuntaohjelmiston kuin tietokoneessa on.

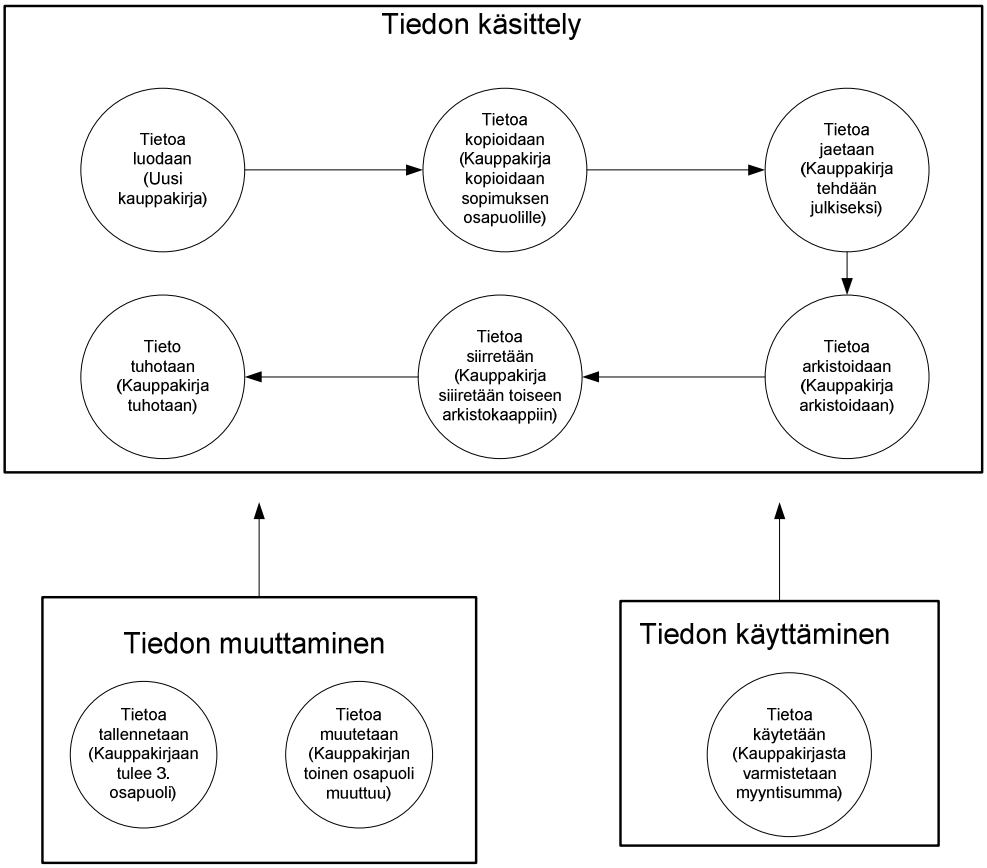
2.3.7 Tietoaineistoturvallisuus

Tietoaineturvallisuus tarkoittaa tiedon ja sen tallennusmedian tunnistusta, luokittelua ja valvontaa tiedon käsittelyn eri vaiheissa. Tavoitteena on, että tiedon sisältö ei muutu tai vuoda ulkopuolisille missään tiedon elinkaaren vaiheessa. Tiedon käsittelyn elinkaari on: tiedon luominen, käyttäminen, muuttaminen, tallettaminen, siirtäminen, jakelu, kopioiminen, arkistointi sekä tuhoaminen. Tärkeimpinä asioina tiedon muuttumattomuuteen vaikuttavat ajan tasalla olevat ohjelmistot, tiedon luokittelu, käsittely ja arkistointi. [5,48]

Kuvassa 2 on kuvattu tiedon käsittelyn elinkaari kauppakirjaesimerkkiä käyttäen. Kuvassa elinkaari on jaettu kolmeen ryhmään. Näin voidaan paremmin havainnollistaa tiedon käsittelyn luonne. Kuva hyvin osoittaa, että tietoa ei pelkästään käsitellä, vaan sitä pitää myös päästä muuttamaan ja käyttämään missä tahansa elinkaaren vaiheessa.

On muistettava, että puutteellinen osaaminen tai tahalliset väärinkäytökset aiheuttavat tiedon vääristymistä, mistä saattaa seurata isoja kaupallisia tai imagollisia tappioita. Pahimmassa tapauksessa organisaatio voi tehdä isojakin päätöksiä väärän tiedon perusteella.

Myös kadonnut tieto voi aiheuttaa ongelmia organisaatiossa. Saatetaan tehdä päätöksiä vanhentuneen tiedon perusteella, koska uudempi tieto samasta asiasta on jostain syystä hävinnyt.



Kuva 2. Tiedon käsittelyn elinkaari.

2.3.8 Tietosuoja

Tietosuoja usein sekoitetaan tietoturvaan, mutta tietosuoja on yksi osa tietoturvallisuutta, tarkemmin tietoaineistoturvallisuutta. Yleisesti tietosuojaa kuitenkin pidetään omana osanaan. Käytännössä tietosuojan perusteet ovat lakipykäliä, joilla määritellään, miten henkilötietoja saa käyttää ja käsitellä. Henkilötiedoksi määritellään mikä tahansa tieto, josta pystyy yksilöimään yksittäisen ihmisen [2,32].

Tietosuojan tarkoitus on suojata henkilön yksityisyys ja henkilötiedot valtuudettomalta tai henkilöä vahingoittavalta käytöltä [5,49]. Tietoturvan tarkoitus on turvata tietosuojan alaisuuteen kuuluvat tiedot.

Lainsäädännössä määritellään tarkasti, miten ihmisten yksityisyyttä suojellaan. Etenkin sosiaali- ja terveysalalla kiinnitetään paljon huomiota tietosuojaan, koska harva asiakas tahtoo, että hänen henkilö- tai potilastietonsa on kaikkien nähtävillä. Tie-

tosuojaan ja tietoturvallisuuteen liittyvä yleislaki on henkilötietolaki (523/1999). Laki määrittelee henkilötiedoksi tiedon, josta pystytään tunnistamaan henkilö. Vaikka lainsäädäntöä on runsaasti, paras ohje henkilötietojen käsittelyyn on: ”Käsittele asiakkaan tietoja siten kuin toivoisit itseäsi koskevia asiakastietoja käsiteltävän.”

Julkisella puolella tietosuojaan liittyy tärkeänä osa-alueena rekisterien suojaus, sillä esimerkiksi kaupungilla on monia erilaisia rekistereitä kaupunkilaisistaan. Esimerkkeinä voidaan ottaa kirjastokortin tiedot, tiedot joita on terveydenhoidon rekistereissä ja tiedot koulujen rekistereissä. Laki määrää suojaamaan rekisterin ulkopuolisten luvattomalta käytöltä, tietojen katoamiselta, muuttumiselta, siirtämiseltä tai luvattomalta kopioinnilta. Suojaamisen velvoite on määritelty henkilötietolaissa. Riittävän suojauksen suunnittelun ja toteutuksen kulmakiviksi kannattaa ottaa tietoturvan osa-alueet. Laissa on myös määritelty se, että henkilö voi pyytää itseään koskevat tiedot rekisteristä.

Viime aikoina tietosuoja ja etenkin tietojen hävitys on noussut puheenaiheeksi. Maaliskuussa 2010 sivullinen löysi Pasilan poliisitalon remonttityömaan roskalavalta salassa pidettävää materiaalia. Ilmeisesti materiaali oli päätynyt epähuomiossa roskalavalle, mutta tapaus on hyvä osoitus, miten paljon valvonta ja työntekijöiden ohjeistus vaikuttaa materiaalin käsittelyyn. Tässä tapauksessa tiedon elinkaaren loppupäässä sattui laiminlyöntejä, jotka vaaransivat kansalaisten tietosuojan. [7]

2.3.9 Käyttöturvallisuus

Käyttöturvallisuuteen liittyy läheisesti organisaation tietohallinnon järjestämä työasemien ylläpito ja huoltotoimet. Näillä on tarkoitus huolehtia siitä, että työasemat ja palvelimet toimivat moitteettomasti, eivätkä aiheuta katkoksia töiden tekemiseen. Työntekijöitä pitää ohjeistaa noudattamaan käyttöturvallisuuteen liittyviä ohjeita. Tärkeää on kertoa, miten esimerkiksi jokin ohjelma toimii, jotta vikatilanteessa tai tietoturvarikkomuksen sattuessa työntekijä osaa informoida tietohallintoa ongelmistaan. [5,51]

Myös organisaation tarjoamien käyttäjätunnusten huolehtiminen kuuluu käyttöturvallisuuteen [5,51]. Yleensä työntekijä saa organisaatioon tullessaan käyttäjätunnuksen ja

salasanan, joilla pääsee organisaation sisäiseen tietoverkkoon. Työntekijöitä pitää opastaa vaihtamaan salasanansa säännöllisesti ja painottaa, että salasanaa ei saa antaa kenellekään muulle. Eli käyttäjätunnus ja muut tunnistautumisvälineet (esimerkiksi kulkukortit, ovien PIN-koodit) ovat henkilökohtaisia, ja niiden käyttöä yleensä valvotaan [5,51]. Valvominen ei ole työntekijöiden jokapäiväisten tekemisten vahtimista, vaan sitä tehdään sen takia, että mahdolliset väärinkäytökset ja tietoturvarikokset (esimerkiksi murtoyritys) saataisiin selville.

3 VERKKO-OPPIMISYMPÄRISTÖ

3.1 Mikä on verkko-oppimisympäristö?

Verkko-oppimisympäristöt ovat www-sivuja, joille on koottu tietoa opittavasta asiasta. Oppimista tehostetaan oppimisympäristöön integroiduilla testeillä. Suurin osa materiaalista on oppimisympäristön tekijän tekemää, mutta siihen voi myös tilaaja lisätä omaa materiaaliansa. Verkko-oppimisympäristöt toimivat yleensä palvelun toimittajan omilla palvelimilla ja niitä käytetään pilvipalveluna Internetin läpi. Kuvassa kolme näkyy hyvin verkko-oppimisympäristön hyvät puolet.

Kuva 3. Navisec-järjestelmän edut [8].

Jotkut verkko-oppimisympäristöt ovat avoimia, mikä tarkoittaa sitä, että tilaaja itse tuottaa kaiken materiaalin oppimisympäristöön. Kotkan kaupungin valitsemassa ratkaisussa oppimisympäristön sisältö on valmiina, ja siihen voidaan lisätä mahdollisuuksien mukaan omaa materiaalia. Lisämateriaali voi olla tekstiä, kuvaa, videoita tai audiotiedostoja.

3.2 Toimittajien selvittäminen

Verkko-oppimisympäristö päätettiin hankkia ulkopuoliselta toimittajalta, koska sen katsottiin olevan helpoin tapa järjestää verkkokoulutus. Tärkeä asia oli toimittajien referenssit kunnilta ja kaupungeilta, sillä niillä varmistettiin verkko-oppimisympäristön toimivuus Kotkan kaupungin kokoisessa organisaatiossa. Samalla myös varmistettiin käytettävän materiaalin laatu ja ajanmukaisuus sopivaksi isoon organisaatioon.

Ensimmäiseksi tehtiin esiselvitys, mitkä yritykset tarjoavat tietoturvakoulutusta verkko-opetuksena. Löydettiin kaksi yritystä (Navicre Oy ja Granite Partners Oy), joilla oli valmis verkko-oppimisympäristö ja jotka vastasivat verkko-oppimisympäristölle annettuja vaatimuksia. Tämän jälkeen laitettiin kyseisille yrityksille sähköpostilla tiedustelua heidän verkko-oppimisympäristöistään ja minkälaisia ominaisuuksia ne pitävät sisällään. Pyydettiin myös demo-tunnuksia heidän verkko-oppimisympäristöihinsä, jotta nähtäisiin, miltä koulutusmoduuli näyttää koulutettavan näkökulmasta katsottaen.

Kummankin toimittajan verkko-oppimisympäristö oli sopivanlainen Kotkan kaupungin tarpeisiin ja isompia eroja sisällöistä ei löytynyt. Kummallakin toimittajalla oli referenssejä isoilta kaupungeilta, joten sekin tuki näkemystä, että yritykset ovat tehneet tuotteensa hyvin.

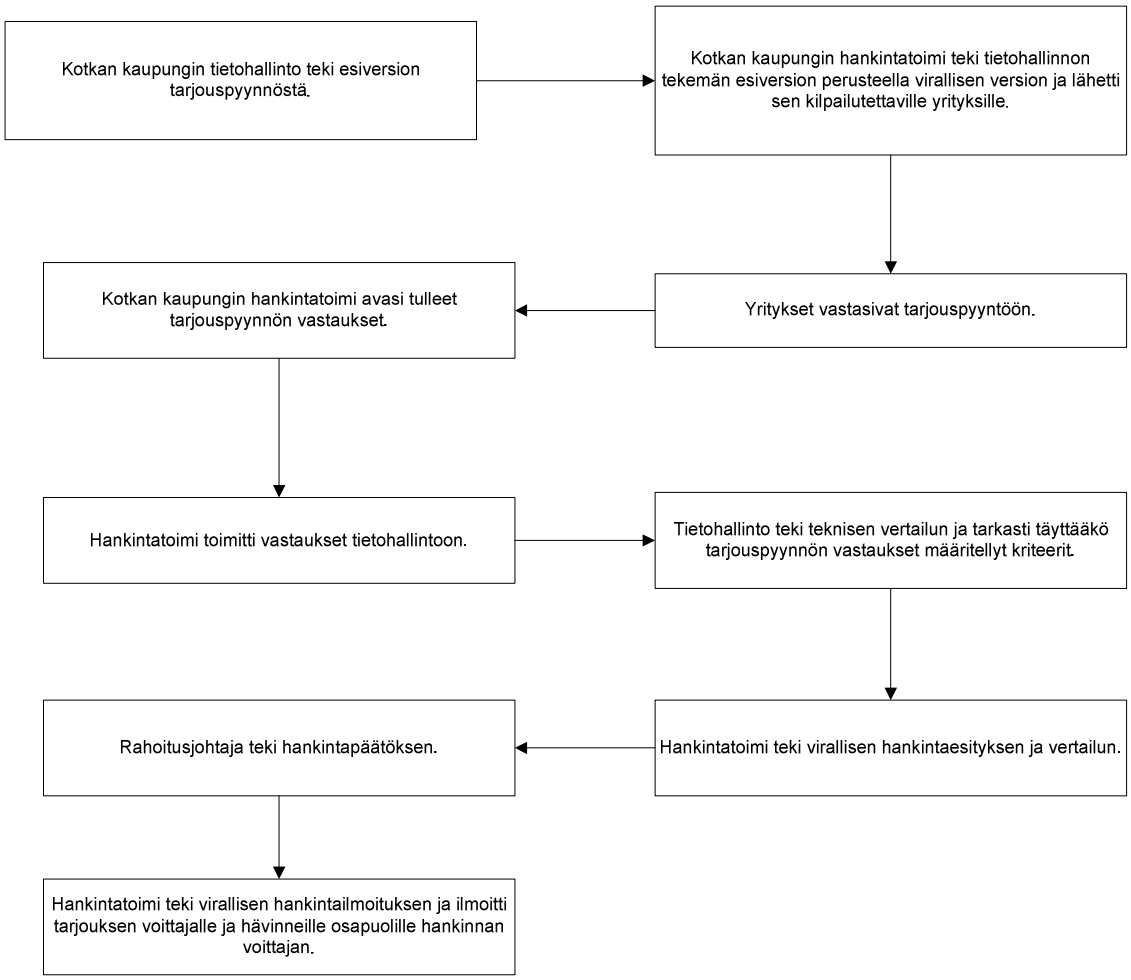
3.3 Tarjouspyynnön tekeminen

Seuraavaksi tehtiin tarjouspyyntö verkko-oppimisympäristön toimittajille. Tarjouspyynnössä kiinnitettiin huomiota erityisesti verkko-oppimisympäristön toimittajien kokemukseen tällaisissa projekteissa, koulutuksen sisällön laadusta, toteutuksesta ja kustannuksista. Tärkeimmäksi valintaperusteeksi valittiin hinta, koska oli jo tutustuttu

kummankin yrityksen oppimisympäristöön ja tiedettiin, että kumpikin niistä vastasi odotuksia.

Tarjouspyynnöstä tehtiin Kotkan kaupungin tietohallinnossa esiversio, joka meni Kotkan kaupungin hankintatoimen käsittelyyn. Hankintatoimi teki tarjouspyynnön suljetun rajoitetun menetelmän mukaan. Suljetussa rajoitetussa menetelmässä tarjouksen pyytäjä valitsee toimittajat, joilta pyytää tarjouksen.

Hankintatoimi teki lopullisen tarjouspyynnön ja hoiti kilpailuttamisen. Tarkemman kuvan tarjouspyynnön prosessista saa kuvasta 4.



Kuva 4. Tarjouspyynnön käsittely.

3.4 Tarjouspyynnön vastauksien käsitteleminen

Kun tarjouspyynnön vastaukset olivat tulleet takaisin hankintatoimeen, se virallisesti avasi vastaukset normaalin menettelymallin mukaan. Hankintalaissa ei ole suoranaisia pykäliä miten tarjouksen vastaukset avataan, mutta Kotkan kaupungin hankintaohjeissa on ohjeistus tarjouspyyntöjen avaamiseen: Järjestetään suljettu tilaisuus, josta tehdään pöytäkirja. Avaustilaisuus on suljettu, jotta mahdolliset yrityssalaisuudet eivät päätyisi ulkopuolisten tietoon. [9,26]

Seuraavaksi hankintatoimi toimitti avatut vastaukset tietohallintoon. Siellä tehtiin tekninen vertailu toimittajien välillä. Käytännössä vertailu tarkoitti sitä, että käytiin läpi kummankin tarjouspyynnön vastaus ja katsottiin, että vastaukset vastaavat tarjouspyyntöä.

Hintavertailu toimittajien välillä oli teknisen vertailun tärkein osio, sillä tuotteen hinta oli tärkein valintakriteeri. Koska toimittajilla ei ollut samanlaista hinnoittelua, jouduttiin tekemään vertailu, jossa oli hinnat 6—24 kuukauden mukaan eri käyttäjämäärillä, kuten liitteestä 1 käy ilmi. Hintaero oli sen verran iso, että tarjouksen voittaja oli selvästi Navicre Oy.

4 HENKILÖSTÖN TIETOTURVAN OSAAMISEN KARTOITUS

4.1 Miksi kartoitetaan?

Loppukäyttäjien tietoturvan osaamisen kartoittamisen suunnittelu oli tärkeä osa projektia, sillä koulutus on kouluttajille ja koulutettaville paljon mielenkiintoisempaa, kun osataan ottaa oikeat asiat esille. Samalla kyselylomakkeella myös kartoitetaan, kuinka monella työntekijällä on mielenkiintoa osallistua koulutukseen, sillä työntekijöiden koulutus perustuu vapaaehtoisuuteen. Kun tiedettäisiin halukkaiden määrä tarkemmin, osattaisiin paremmin suunnitella järjestettävä koulutus: esimerkiksi minkälainen tila tullaan tarvitsemaan.

4.2 Esikartoituksen kyselylomake

Esikartoitus suunnattiin kolmelle ryhmälle: ylin johto, esimiehet ja työntekijät. Jokaiselle ryhmälle laadittiin omanlaisensa kysymyslomakkeet. Kysymyksiä tuli noin 10 per ryhmä. Osa kysymyksistä esiintyi useammassa ryhmässä. Kyselyn lopussa on myös vapaan sanan kohta, johon vastaajat saavat kirjoittaa omia mielipiteitään tietoturvan tilasta ja tulevan koulutuksen painopisteistä. Kysely toteutetaan Digiumin kyselylomakkeella anonyymisti, jotta saadut vastaukset olisivat mahdollisimman todenperäisiä.

Kysymyksien sisältö vaihteli työaseman peruskäyttöön liittyvistä kysymyksistä kaupungin ohjeisiin liittyviin kysymyksiin. Paino kysymyksissä on kuitenkin jokapäiväisessä työskentelyssä ilmi tulevissa asioissa. Näin saadaan kartoitettua, miten hyvin työntekijät noudattavat jo annettuja ohjeita. Esimerkkejä kysymyksistä löytyy liitteessä 2.

Esikartoituslomakkeen teko on helppoa Digiumin tarjoamalla web-sovelluksella. Kyselystä saa tehtyä yksilöllisen ja selkeän helpolla tavalla. Teknistä osaamista ei tarvita, sillä ohjelmaan ei tarvitse syöttää HTML-koodia. Digiumin web-sovelluksella saa myös lomakkeen helposti toimitettua loppukäyttäjien sähköpostiin, sillä web-sovellus hoitaa sähköpostin lähetyksen kyselyn kohderyhmälle.

4.3 Esikartoituksen tulokset

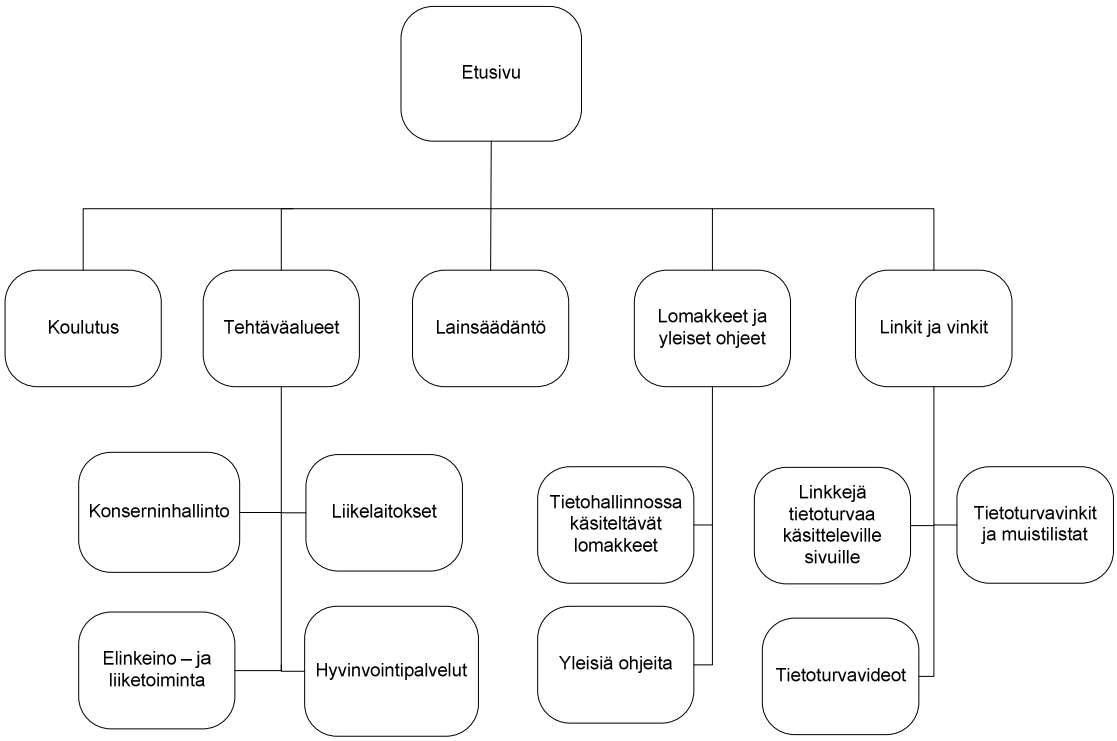
Esikartoituksen tuloksia ei ole saatu, koska varsinainen esikartoitus on vielä kesken. Kyselylomakkeesta tehtiin ensimmäinen versio demo-tunnuksilla, jotta nähtiin mitä kaikkea Digiumin ohjelmalla pystyy tekemään. Varsinaisen kyselylomakkeen teko siirrettiin toiseen yksikköön ja opinnäytetyön valmistumiseen mennessä kyselylomaketta tai kyselyä ei ole tehty.

5 TIETOISKUJEN TOTEUTTAMINEN

5.1 Tietoturva-sivusto

Tietoturva-sivuston tarkoitus on tarjota Kotkan kaupungin työntekijöille materiaalipankki, josta löytyy kaikki tietoturvaan liittyvä aineisto. Näin työntekijöiden on helpompi etsiä tietoturvaan liittyvää materiaalia. Ennen Tietoturva-sivustoa työntekijöiden oli hankala löytää Intranetissä olleita tietoturvaan liittyviä lomakkeita ja ohjeita. Tämä johtui siitä, että työntekijöillä ei välttämättä ollut tietoa, mistä päin Intranetiä olisi kannattanut alkaa etsimään lomakkeita tai ohjeita. Näin ollen myös työaikaa meni hukkaan turhan etsimisen vuoksi. Tietoturva–sivuston rakenne on esitetty kuvassa 5.

Ulkoasun puolesta Tietoturva-sivusto on yksinkertainen mutta toimiva. Ulkoasussa on tähdätty enemmän toimivuuteen kuin hienouteen. Esimerkki sivustosta on kuvassa 6. Sivusto toteutettiin Microsoftin Sharepoint-ympäristössä, joka ei vaatinut web-ohjelmointitaitoja. Tietoturva-sivusto on yksi osa Kotkan kaupungin Intranetiä.

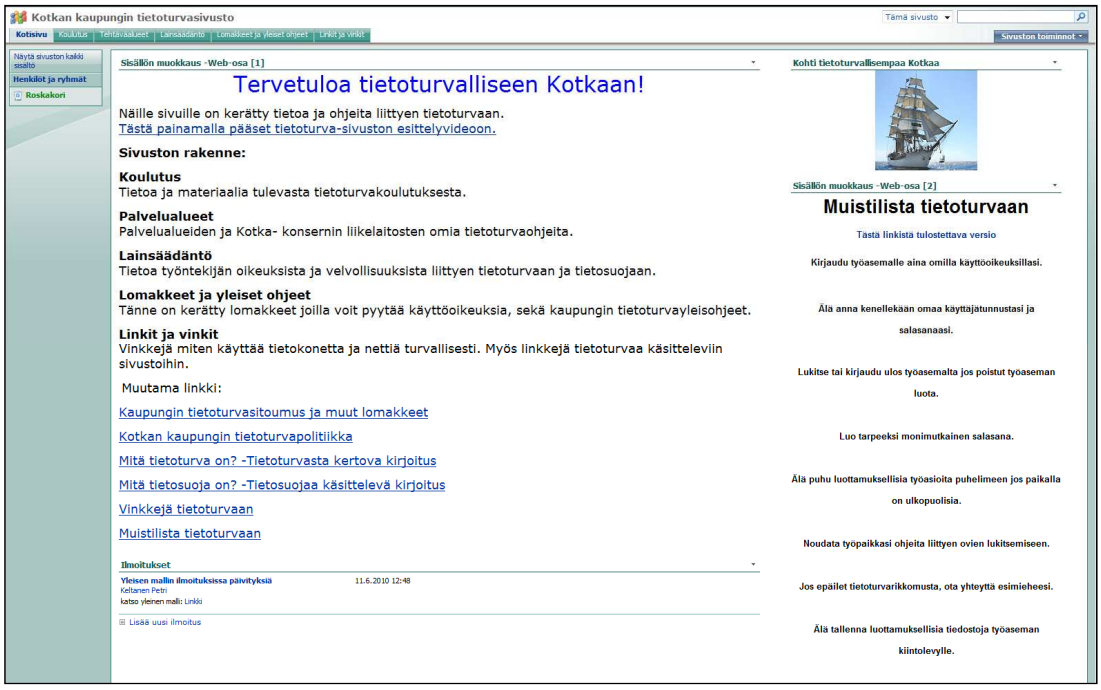


Kuva 5. Tietoturva-sivuston sivukartta.

Tietoturva-sivusto on jaettu kuuteen osaan:

Etusivu

Etusivu on Tietoturva-sivuston ensimmäinen sivu. Siellä on selitettynä sivuston rakennetta ja annettu muutama hyödyllinen linkki tietoturvaan liittyvään materiaaliin. Etusivun tarkoitus on opastaa käyttäjää sivuston käyttöön ja tarjota linkkien ja materiaalien avulla pieni tietopaketti tietoturvaan. Ideana oli se, että etusivulla on koottuna tärkeimmät tietoturvaan liittyvät asiat, joita sitten muut sivut täydentävät. Etusivulla on myös helposti tulostettava muistilista (liite 3), jonka tarkoitus on muistuttaa työntekijöitä tietoturvallisesta työskentelytavasta.



Kuva 6. Kuvankaappaus Tietoturva–sivuston etusivusta.

Koulutus

Koulutus-kohdasta löytyy tiedot alkavista ja olemassa olevista koulutuksista liittyen tietoturvaan. Sinne myös kerätään materiaalia, jota käytetään opetuksessa. Koulutus-osio toimii tärkeänä ohje- ja informaatiokanavana koulutettaville. Sieltä voi myös tarkistaa koulutuksen päivämäärät ja sinne päivitetään mahdolliset muutokset koulutuk-

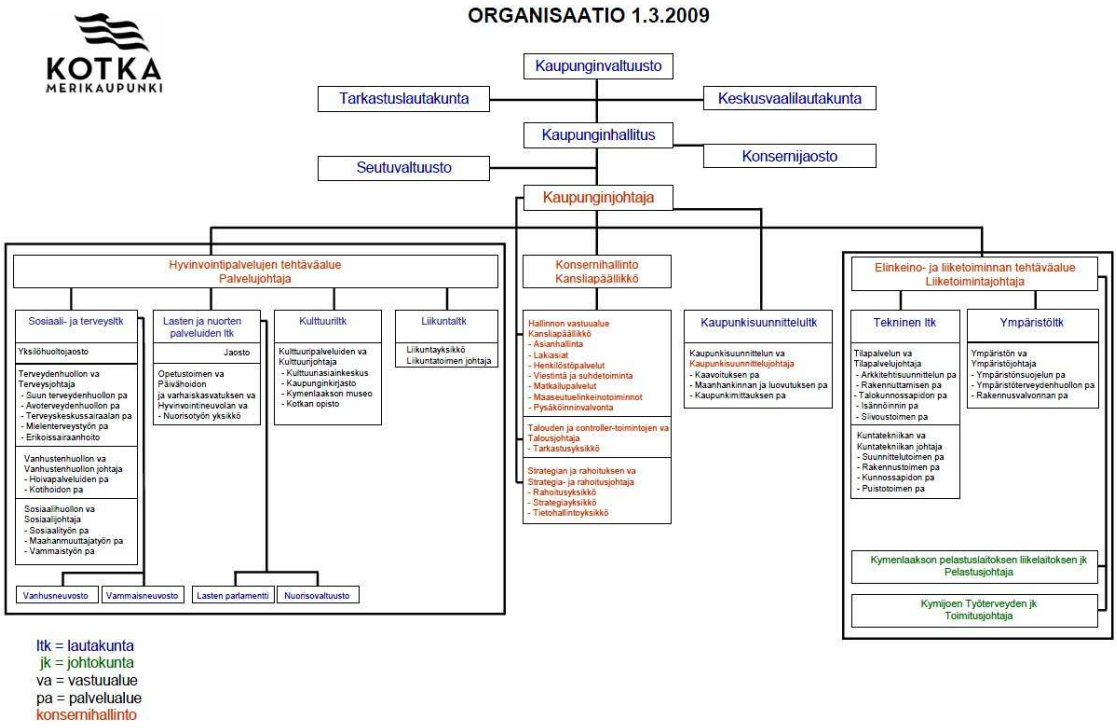
sen päivämäärissä tai sisällössä. Koulutus-kohdasta myös löytyy linkki verkko-oppimisympäristöön.

Tehtäväalueet

Tehtäväalueiden alta löytyy tietoa tietoturvasta koskien eri tehtäväalueita. Kotkan kaupunki on jakanut tehtäväalueet seuraavasti: Hyvinvointipalveluiden tehtäväalue, Konserninhallinto ja Elinkeino- ja liiketoiminnan tehtäväalue. Näiden lisäksi sivulta löytyy omat kohtansa Kotka-konsernin liikelaitoksille. Kotka-konsernin liikelaitoksia ovat muun muassa Kymenlaakson ammattikorkeakoulu Oy ja Kotkan kaupunginteatteri Oy. (Katso kuva 7.) Kotkan kaupungin liikelaitokset eivät osallistu kaupungin järjestämään tietoturvakoulutukseen ainakaan ensi vaiheessa, sillä koulutus on suunnattu niille työntekijöille jotka ovat suoraan Kotkan kaupungin henkilöstöä.

Kuva 7. Kotka-konsernin liikelaitokset [10].

Kotkan kaupungin tehtävät on jaettu toimialueisiin. Alueesta riippuen sen alla on useita lautakuntien johtamia vastuualueita ja palvelualueita. Esimerkiksi Kotkan kaupungin tietohallintoyksikkö kuuluu Strategian ja rahoituksen vastuualueeseen, joka kuuluu konserninhallintoon, kuten kuvasta 8 ilmenee.



Kuva 8. Kotkan kaupungin organisaatio [11].

Lainsäädäntö

Lainsäädännön alle on kerätty tietoja, ohjeita ja linkkejä liittyen lainsäädännön määräämiin asioihin. Erityisesti tärkeässä roolissa on sosiaali- ja terveysalan tietosuoja. Lakikohdat on kerätty Suomen laista ja sivulla on linkki kuntaliiton lainsäädäntösivulle.

Lainsäädäntö luo velvoitteita kaupungin toimintaan. Etenkin uudet sähköiset järjestelmät ovat tärkeässä asemassa. Pelkona on, että puutteellinen tietoturva vaarantaa tietosuojan, mikä johtaa sitten lainsäädännöllisiin ongelmiin.

Lomakkeet

Lomakkeet-kohdasta löytyy erilaiset hakemukset ja lomakkeet, joilla voidaan hakea esimerkiksi etäkäyttöoikeuksia, joilla voi kotikoneelta ottaa yhteyttä Kotkan kaupungin intranetiin. Kotkan kaupunki on siirtymässä sähköisiin lomakkeisiin, joista tietoturvaan liittyvät sijoitetaan Tietoturva-sivuston lomakkeet-sivulle.

Tulevaisuudessa myös lomakkeiden päivittäminen ja lisääminen helpottuu, koska tietoturvaan liittyvät lomakkeet löytyvät samasta paikkaa. Samalla myös käyttäjien työteho paranee, kun heidän ei tarvitse etsiä lomakkeita monesta paikkaa, vaan voivat suoraan mennä Tietoturva-sivustolle etsimään oikeaa lomaketta.

Linkit ja vinkit

Kaikkea materiaalia ei ollut järkevää laittaa Tietoturva-sivuston kotisivulle, joten tehtiin linkit ja vinkit-kohta, josta löytyy tietoturvaan liittyviä pieniä ohjeita ja linkkejä muille tietoturvaa käsitteleville sivustoille. Linkit ja vinkit löydettiin etsimällä tietoa Googlesta ja seuraamalla sosiaalista mediaa. Etenkin Facebook ja Twitter olivat käteviä työkaluja tietoturvavinkkien etsimiseen. Facebook ja Twitter päivittyvät nopeasti, joten niitä seuraamalla löydettiin ajankohtaisia vinkkejä ja turvallisuusuhkia. Esimerkiksi Twitterin kautta löydettiin hyvä oikeusministeriön tekemä opas sosiaaliseen mediaan [12].

Tietoturva-sivustolle tehtiin myös muutama lyhyt video tietoturvaohjelmien ja Tietoturva-sivuston käytöstä. Kyseiset videot sijoitettiin Linkit ja vinkit-kohdan alle. Videot tallennettiin ja leikattiin Dreambroker-nimisellä ohjelmalla, joka toimii Internetin välityksellä niin sanottuna pilvipalveluna, eli työasemalle ei tarvinnut asentaa mitään Dreambrokerin ohjelmistoa tai videoita, sillä kaikki toimii Internetin läpi Dreambrokerin omalta palvelimelta. Videoiden aiheet vaihtelivat Tietoturva-sivuston esittelystä Spybot-nimisen vakoiluohjelmien poistoon tarkoitetun ohjelmiston välillä.

5.2 Tietoturvavinkit Kotkan kaupungin intranetissä

Tietoturvavinkkien tarkoitus on muistuttaa kaupungin työntekijöitä tietoturvallisesta työskentelystä. Niiden toteutus on seuraavanlainen: Laitetaan varsinaiseen kaupungin intranetiin tietoturvavinkkejä, joissa on lyhyt, ytimekäs ohje työaseman turvalliseen käyttöön. Yksi vinkki on muutaman viikon intranetin etusivulla ja sen jälkeen se vaihtuu uuteen. Samat vinkit löytyvät myös Tietoturva-sivustolta, jotta loppukäyttäjät voivat katsella niitä omassa tahdissaan.

6 KOULUTUSTAPAHTUMA

6.1 Työntekijät

Työntekijöille koulutus järjestetään halukkuuden mukaan. Halukkaiden määrästä riippuen työntekijät jaetaan kahteen koulutusmoduuliin: omien työasemien ja yhteistyöasemien käyttäjät. Koulutus tapahtuu massakoulutuksena auditorioissa ja työntekijöille suunnatun verkko-oppimisympäristön tekemisellä joko kotona tai työpaikalla.

Massakoulutus ei luonnollisesti ole paras mahdollinen tapa kouluttaa, mutta Kotkan kaupungin tapauksessa se on tehokkain tapa. Kotkan kaupungilla on noin 3500 henkilöä töissä, joten massakoulutus saadaan nopeammin päätökseen. On muistettava, että pääpaino koulutuksessa on kuitenkin verkkokoulutuksessa.

Koulutuksen tarkempi sisältö on avoin, koska se riippuu osittain esikartoituksen tuloksista. Ideana on käydä läpi tietoturvan perusteita käytännön esimerkein. Esimerkit ovat niin kotikäytöstä kuin Kotkan kaupungin työympäristöstä. Koulutuksessa on myös mukana ohjeistus verkko-oppimisympäristön käyttöön.

Verkko-oppimisympäristön käyttö antaa koulutettaville mahdollisuuden oman osaamisen testaamisen ja vahvistamiseen. Oppimisympäristö antaa myös esimiehille mahdollisuuden tarkkailla, miten työntekijöiden oppiminen edistyy, ja tuottaa tilastotietoa, kuinka työntekijät ovat pärjänneet testeissä. Tilastotiedoista voidaan sitten päätellä, mihin asioihin tulevaisuuden koulutuksessa pitää panostaa.

Pitää kuitenkin muistaa, että koulutuksesta kieltäytyminen ei vapauta työntekijöitä vastuusta. He ovat samalla tavalla vastuussa omista tunnuksistaan ja toiminnastaan kuin ennen tietoturvapolitiikan hyväksymistä.

6.2 Esimiehet

Esimiehille koulutus järjestetään samaan tapaan massakoulutuksena kuin työntekijöille. Periaatteessa koulutuksen sisältö on sama kuin työntekijöillä, mutta painopiste on enemmän esimiesten vastuussa. Kotkan kaupungin tietoturvapolitiikka määrittelee, että esimiehillä on vastuu alaistensa kouluttamisesta tietoturvalliseen toiminta tapaan [13].

Keskustelua on herättänyt ristiriitaisuus koulutuksen vapaaehtoisuudesta ja esimiesten vastuusta koulutuksen järjestämisestä. Asia on ajateltu niin, että tietohallinto järjestää mahdollisuuden koulutukseen, jonka esimiehet voivat korvata esimerkiksi itse järjestämällään koulutustilaisuudella. Esimiesten järjestämän koulutuksen ei periaatteessa tarvitse olla erikoista: se voi olla muutaman minuutin tilannekatsaus, missä kerrotaan miten työpaikalla toimitaan tietoturvallisesti ja kerrotaan mistä asiasta kiinnostuneet työntekijät saavat lisätietoa aiheesta [2,258].

6.3 Ylin johto

Ylimmälle johdolle koulutus tullaan järjestämään palaverien ja kokousten yhteydessä pienellä infotilaisuudella asiasta. Varsinainen koulutus tapahtuu verkko-oppimisympäristössä.

7 KOULUTUKSESTA TIEDOTTAMINEN

7.1 Tiedotussuunnitelma

Tiedotussuunnitelman tarkoitus on selventää ja olla muistilistana tiedotukseen liittyviin asioihin. Etenkin tämänkaltaisissa isoissa projekteissa on tärkeää, että ihmiset saavat ennakkoon tiedon asioista. Tiedotussuunnitelmassa käy ilmi seuraavat asiat: kenelle tiedotetaan, miten tiedotetaan, milloin tiedotetaan, kuka tiedottaa ja mitä tiedo-

tetaan. Tiedotussuunnitelman teossa ongelmia aiheutti avoin aikataulu, joka johtui lomista ja tarjouspyynnön tekemisen myöhästymisestä.

7.2 Artikkeli henkilöstölehti Tarmoon

Osana tiedotussuunnitelmaa kirjoitettiin artikkeli Kotkan kaupungin henkilöstölehti Tarmoon (liite 4). Kirjoitusprojekti lähti liikkeelle, kun mietittiin tapoja informoida kaupungin työntekijöitä tulevasta koulutuksesta. Ajateltiin, että henkilöstölehti on hyvä tapa kertoa siitä, että kaupunki aloittaa tietoturvakoulutuksen. Haastavinta oli artikkelin rakenne ja hyvän kirjoitustyylin löytäminen, koska kokemusta artikkelien kirjoittamisesta ei ollut ennestään.

Artikkelin kirjoittaminen oli mukavaa vaihtelua koulutuksen suunnittelun ohessa, sillä asioita joutui miettimään loppukäyttäjän näkökulmasta. Ei voinut käyttää monimutkaista ammattisanastoa, vaan piti löytää sanottava asia yleiskielellä. Tämä oli hyvin silmiä avaavaa, sillä helposti unohtaa millä tavalla loppukäyttäjät näkevät tietoturvallisuusasiat.

8 JALKAUTTAMISSUUNNITELMA

Jalkauttamissuunnitelman tarkoitus oli esitellä tietoturvakoulutus Kotkan kaupungin tietotekniikkaryhmälle. Se koostuu toimintayksiköiden valitsemista edustajista ja sitä johtaa tietohallintopäällikkö. Tietotekniikkaryhmän tehtävä on valmistella tietotekniikkaan liittyviä asioita tietohallinnonjohtoryhmälle.

Jalkauttamissuunnitelma (liite 5) otettiin hyvin vastaan tietotekniikkaryhmässä. Eniten keskustelua aiheutti verkko-oppimisympäristön hinta, koska tarkkaa hintaa ei osattu kertoa kokouksen ajankohtana, sillä tarjouspyyntöä verkko-oppimisympäristöstä ei ollut vielä tehty. Jalkauttamissuunnitelman rakenne oli seuraavanlainen: alkusanat, jossa selitettiin, mihin koulutuksen tarve perustuu, miten työntekijät on jaettu ryhmiin, millä tavalla koulutustapahtuma on toteutettu ja missä järjestyksessä koulutuksessa edetään.

9 YHTEENVETO

Tietoturvakoulutuksen suunnittelu onnistui hyvin, mutta harmittamaan jäi käytännön osuuden vähyys. Mukavana poikkeuksena oli Tietoturva-sivusto, joka tehtiin valmiiksi ja julkaistiin Kotkan kaupungin henkilöstölle. Toisaalta käytännön osuuden pieneksi jääminen ei ollut projektissa iso takaisku, sillä kyseessähän oli vasta koulutuksen suunnittelu.

Luonnollisesti käytännön kokemusten puuttuminen vaikuttaa projektin arviointiin. Arvioinnissa on otettu enemmän huomioon esimiesten ja päättävien elinten mielipidettä, joka on ollut poikkeuksetta positiivista.

Isoja teknisiä ongelmia ei tullut suunnittelun aikana vastaan ja ne olivat ohitettavissa kollegoiden avustuksella. Lähinnä ongelmat olivat Sharepointin käytössä ja ne johtuivat siitä, että se oli ympäristönä ennestään tuntematon. Mutta kun Sharepointiin pääsi sisälle, sen käyttö oli helppoa ja yksinkertaista. Sharepointin perusteiden osaamisesta on varmasti etua tulevassa työelämässä, joten siihen tutustuminen oli positiivinen kokemus.

Oli erittäin mielenkiintoista olla tekemässä tällaista isoa projektia. Se opetti hyvin monia eri asioita, aina projektin suunnittelusta projektista tiedottamiseen. Projektin edetessä täytyi myös muistaa, että kunnallisessa päätöksenteossa on isossa roolissa erilaiset lait, tässä tapauksessa hankintalaki, joka määrittelee millä tavalla tuotteet hankitaan kaupungille. Pahimmassa tapauksessa virallisten reittien oikominen on lainvastaista toimintaa ja siitä on oikeudellisia seuraamuksia.

Jatkotoimina suositellaan tietoturvakoulutuksen laajentamista Kotkan kaupungin liikelaitoksiin ja esimerkiksi jonkinlaista tietopakettia tietoturvasta uudelle työntekijälle. Tietohallinto ja Kotkan kaupungin viestintä- ja tiedotusosasto voisivat myös laajentaa tietoiskuja sosiaaliseen mediaan. Näin ne tavoittaisivat enemmän kaupungin työntekijöitä ja asukkaita kuin pelkästään kaupungin suljettu intranet. Myös koulutuksen jälkeen voitaisiin tehdä uusi kysely, jolla mitattaisiin miten koulutetut asiat on opittu.

LÄHTEET

[1] Turvallinen elämä jokaiselle - Sisäisen turvallisuuden ohjelma. 2008. Sisäasiainministeriö. Saatavissa: http://www.intermin.fi/intermin/hankkeet/turva/home.nsf/files/162008/$file/162008.pdf [viitattu 16.2.2011].

[2] Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Oy Nordprint Ab.

[3] Tietoturva. 2010. Wikipedia -artikkeli. Saatavissa: http://fi.wikipedia.org/wiki/Tietoturva [Viitattu 16.2.2011].

[4] Tietoturvan peruskäsitteet. 2011. Internet-artikkeli. Saatavissa: http://gallia.kajak.fi/opmateriaalit/yleinen/ViOl/Tietoturva/Tietoturvan%20perusk%C3%A4sitteit%C3%A4.pdf [viitattu 16.2.2011].

[5] Opas julkishallinnon tietoturvakoulutuksen järjestämisestä. 2003. Valtionvarainministeriö. Saatavissa: http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/53763/53760_fi.pdf [viitattu 16.2.2011].

[6] Matkapuhelimien mahdollisia tietoturvauhkia. Viestintäviraston artikkeli. Saatavissa: http://www.ficora.fi/mobiiliturva/tietoturvauhkia.html [viitattu 16.2.2011].

[7] Poliisi: Pasilan roskalavajupakassa syytä epäillä laiminlyöntiä. Helsingin Sanomat 16.3.2010. Saatavissa: http://www.hs.fi/kaupunki/artikkeli/Poliisi+Pasilan+roskalavajupakassa+syyt%C3%A4+ep%C3%A4ill%C3%A4+laiminly%C3%B6nti%C3%A4/1135254461658 [viitattu 16.2.2011].

[8] Navisec-järjestelmän edut. 2011. Navicre Oy. Saatavissa: http://www.navicre.com/index.php?786 [viitattu 16.2.2011]

[9] Kotkan kaupungin säädöskokoelma 2008 nro 15. Kotkan kaupungin yleiset hankintaohjeet. 2008. Kotkan kaupunki.

[10] Kotka-konserni. 2011. Kotkan kaupunki. Saatavissa: http://www.kotka.fi/general/Uploads_files/asianhallinta/konserni/kotkakonserni-10.3.10.pdf [viitattu 16.2.2011]

[11] Kotkan kaupungin organisaatio. 2009. Kotkan kaupunki. Saatavissa: http://www.kotka.fi/showattachment.asp?ID=14520&DocID=2149 [viitattu 16.2.2011]

[12] Aalto, T. 2010. Sosiaalisen median mahdollisuudet hallinnolle. Oikeusministeriö.

[13] Kotkan kaupungin tietoturvapolitiikka. 2010. Kotkan kaupunki. [Ei yleisessä jakelussa.]

Tarjouspyynnön vastausten hintavertailu

Tietoturvakoulutusympäristöjen hintavertailua

Ensimmäisten 6 kk:n hinnoittelu /kk

Käyttäjämä	1000	1500	2000	3000	ALV 0%
GranitePar	1 390 €	1 560 €	1 720 €	2 040 €	Kuukausihinta (ensimmäiset 6 kk)
Navicre	**466 €**	**550 €**	**633 €**	**767 €**	Kuukausihinta ei muutu 6 kk:n jälkeen

Ensimmäisten 6 kk:n hinnoittelu /kk

Käyttäjämä	1200	1700	2100	3050	ALV 0%
GranitePar	1 510 €	1 660 €	1 760 €	2 055 €	Kuukausihinta (ensimmäiset 6 kk)
Navicre	522 €	598 €	655 €	777 €	Kuukausihinta ei muutu 6 kk:n jälkeen

Kuukausihinta kun 6 kk:ta kulunut (esim 7:s kuukausi)

Käyttäjämä	1000	1500	2000	3000	
GranitePar	640 €	890 €	1 140 €	190 €	kk-hinta 6 kk:n jälkeen hinnoittelu 190€/kk
Navicre	**466 €**	**550 €**	**633 €**	**767 €**	Kuukausihinta ei muutu 6 kk:n jälkeen

Hinta 12 kk

Käyttäjämä	1000	1500	2000	3000	
GranitePar	12 180 €	14 700 €	17 160 €	13 380 €	Hinta laskettu 6:n ensimmäisen ja 6: seuraavan kk:n hinnoittelun mukaan
Navicre	**5 592 €**	**6 600 €**	**7 596 €**	**9 204 €**	Kaikki kuukaudet samanhintaisia

Hinta 12kk -24 kk

Käyttäjämä	1000	1500	2000	3000	
GranitePar	7 680 €	10 680 €	13 680 €	15 660 €	Kaikki kuukaudet samanhintaisia
Navicre	**5 592 €**	**6 600 €**	**7 596 €**	**9 204 €**	Kaikki kuukaudet samanhintaisia

Hinta käyttäjittäin:

Hinta 12 kk

Käyttäjämä	1000	1500	2000	3000	
GranitePar	12,18 €	9,80 €	8,58 €	4,46 €	Hinta laskettu 6:n ensimmäisen ja 6: seuraavan kk:n hinnoittelun mukaan
Navicre	**5,59 €**	**4,40 €**	**3,80 €**	**3,07 €**	Kaikki kuukaudet samanhintaisia

Hinta 12kk -24 kk

Käyttäjämä	1000	1500	2000	3000	
GranitePar	7,68 €	7,12 €	6,84 €	5,22 €	Kaikki kuukaudet samanhintaisia
Navicre	**5,59 €**	**4,40 €**	**3,80 €**	**3,07 €**	Kaikki kuukaudet samanhintaisia

Hinta kun käyttäjiä alle 1000 käyttäjää

Hinta 12 kk

Käyttäjämä	100	200	300	400	
GranitePar	10 200 €	10 500 €	10 800 €	11 100 €	Hinta laskettu 6:n ensimmäisen ja 6: seuraavan kk:n hinnoittelun mukaan
Navicre	**5 592 €**	**5 592 €**	**5 592 €**	**5 592 €**	Kaikki kuukaudet samanhintaisia

Hinta 12kk -24 kk

Käyttäjämä	100	200	300	400	
GranitePar	2 280 €	2 880 €	3 480 €	4 080 €	Kaikki kuukaudet samanhintaisia
Navicre	5 592 €	5 592 €	5 592 €	5 592 €	Kaikki kuukaudet samanhintaisia

Esikartoituskysymykset

Esimiehille:

Hahmotatko mahdolliset tietoturvariskit palvelualueellasi?

kyllä/ei

Osaatko perehdyttää uuden työntekijän tietoturvallisuusasioihin?

kyllä/ei

Osaatko toimia tietoturvallisuuteen liittyvissä ongelmatilanteissa?

kyllä/ei

Onko sinun palvelualueella epäselviä/päällekkäisiä vastuita esim. tietojärjestelmien tietoturvan hoidosta/ylläpidosta?

kyllä/ei

Oletko delegoinut tietoturvavastuuta alaisillesi?

kyllä/ei

Oletko lukenut kaupungin tietoturvapolitiikan?

kyllä/ei

Tiedätkö kenelle pitää raportoida tietoturvarikkomuksista?

kyllä/ei

Jos alaisesi tulee kysymään oikeuksistaan liittyen tietoturvaan/tietosuojaan, osaatko kertoa hänelle asiasta itse tai ohjata jonkun luokse joka tietää asiasta?

kyllä/ei

Onko sinulla halukkuutta osallistua tietoturvakoulutukseen?

kyllä/ei

Mitä haluaisit tietää tietoturvasta?

kommenttikenttä

Minkälaista tietoturvakoulutusta tahdot a) itsellenne b) alaisillenne? (Voit myös kommentoida kyselyä ja muita asiaan liittyviä asioita tähän.)

kommenttikenttä

Työntekijöille:

Kuinka usein käytät työpaikkasi työasemaa?

Monivalinta

Oletko siirtänyt työtiedostoja kotikoneellesi?

kyllä/ei

Tiedätkö, mitä tehdä, jos havaitset puutteita tietoturvassa?

kyllä/ei

Lukitsetko/kirjaudutko ulos työasemalta kun poistut sen luota (pois näköetäisyydeltä)?

kyllä/ei

Onko ulkopuolisilla mahdollisuus tulla toimipaikkanne luo (esim. taukotila, pukuhuone, työpöytä) ilman avainta?

kyllä/ei

Oletko joutunut kertomaan omia tunnuksiasi harjoittelijoille tai työkavereillesi, että he pääsevät kirjautumaan kaupungin verkkoon?

kyllä/ei

Onko esimiehesi perehdyttänyt sinulle tietoturvallista toimintatapaa?

kyllä/ei

Onko salasanasi työasemalle tai johonkin muuhun palveluun jokin seuraavista: vuodenaika/viikonpäivä/kuukausi/syntymäaika /perheenjäsenesi nimi /lemmikkisi nimi?

kyllä/ei

Oletko joutunut puhumaan salassa pidettäviä asioita puhelimeen kun vieressäsi on ollut ulkopuolisia?

kyllä/ei

Tiedätkö eron tietosuojan ja tietoturvan välillä?

kyllä/ei

Onko sinulla halukkuutta osallistua tietoturvakoulutukseen?

kyllä/ei

Mitä haluaisit tietää tietoturvasta? (Voit myös kommentoida kyselyä ja muita asiaan liittyviä asioita tähän.)

kommenttikenttä

Ylin johto:

Oletko delegoinut tietoturvavastuuta alaisillesi?

kyllä/ei

Hahmotatko mahdolliset tietoturvariskit vastuualueellasi?

kyllä/ei

Osaatko perehdyttää uuden työntekijän tietoturvallisuusasioihin?

kyllä/ei

Osaatko toimia tietoturvallisuuteen liittyvissä ongelmatilanteissa?

kyllä/ei

Tiedätkö kenelle pitää raportoida tietoturvarikkomuksista?

kyllä/ei

Tiedätkö minne pitää ilmoittaa mahdollisista tietoturvarikkeistä ja -puutteista?

kyllä/ei

Oletko lukenut Kotkan kaupungin tietoturvapolitiikan?

kyllä/ei

Onko sinun kokemusten perusteella Kotkan kaupungin tietoturva kunnossa?

kyllä/ei

Onko sinulla halukkuutta osallistua tietoturvakoulutukseen?

Kyllä/ei

Onko sinulla tiedossa keinoja joilla voisi parantaa kaupungin tietoturvaa?

kommenttikenttä

Mitä haluaisit tietää tietoturvasta? (Voit myös kommentoida kyselyä ja muita asiaan liittyviä asioita tähän.)

kommenttikenttä

Tietoturvan muistilista

Muistilista tietoturvaan

Kirjaudu työasemalle aina omilla käyttöoikeuksillasi.

Älä anna kenellekään omaa käyttäjätunnustasi ja salasanaasi.

Lukitse tai kirjaudu ulos työasemalta jos poistut työaseman luota.

Luo tarpeeksi monimutkainen salasana.

Älä puhu luottamuksellisia työasioita puhelimeen jos paikalla on ulkopuolisia.

Noudata työpaikkasi ohjeita liittyen ovien lukitsemiseen.

Jos epäilet tietoturvarikkomusta, ota yhteyttä esimieheesi.

Älä tallenna luottamuksellisia tiedostoja työasemasi kiintolevylle.

Artikkeli henkilöstölehti Tarmossa

Kohti tietoturvallista Kotkaa

Tietokoneiden ja internetin lisääntynyt käyttö on lisännyt rikollisuutta, joka kohdistuu tavallisiin tietokoneiden käyttäjiin. Esimerkkinä tästä on Nordean asiakkaisiin alkuvuodesta kohdistunut salasanojen kalastelu. Rikolliset pääsivät käsiksi asiakkaiden tileihin ja saivat nostettua rahaa Nordean ilmoituksen mukaan kymmeniltä tileiltä noin 50 000 euroa.

Edellä mainitunlaiset tapaukset ovat nykyaikana kovin helppoja toteuttaa, joten tietämystä tietoturvasta syytä lisätä. Kun työntekijät osaavat käyttää tietokonetta turvallisesti kotona, he myös osaavat käyttää sitä turvallisesti töissä. Tämän takia Kotkan kaupunki tulee järjestämään työntekijöilleen tietoturvakoulutusta.

Hallinnollisempi syy on Kotkan kaupungin maaliskuussa hyväksytty tietoturvapolitiikka. Se määrittelee että kaupungin on järjestettävä koulutusta työntekijöilleen.

Myös Suomen laissa on pykälät tietoturvan huolehtimisesta sekä valmisteilla oleva tietohallintolaki edellyttävät tietoturvan hallintaa entistä enemmän.

”Olemme laatineet koulutussuunnitelman, joka painottuu internetin välityksellä tapahtuvaan verkkokoulutukseen”, kertoo tietohallintopäällikkö Juha Redsven kaupungin tietohallinnosta.

”Mutta halukkailla kaupungin työntekijöillä on myös mahdollisuus osallistua lähiopetukseen, jotka tullaan järjestämään erillisinä tapahtumina Kotkassa ”.

Koulutus käynnistyy sähköisellä kyselyllä

Koulutuksen ensimmäinen vaihe käynnistyy sähköisellä kyselyllä, jolla kartoitetaan työntekijöiden nykyistä tietoturvan tietämystä sekä kysellään työntekijöiden mielipiteitä tietoturvallisuuteen liittyen.

”Tarkoituksena olisi että työntekijät rohkeasti kertoisivat omia mielipiteitään kaupungin tietoturvan tilasta. Näin osaamme paremmin painottaa koulutuksessa niitä alueita, joissa on parantamisen tarvetta”, Redsven sanoo.

Koulutus on vain yksi osa tietoturvallisuuden parantamista. Muina keinoina ATK-keskus on suunnitellut ja toteuttanut kaupungin intranetissä olevan tietoturvasivuston.

Tietoturva-sivuston tarkoitus on olla informaatiokanavana erilaisissa tietoturvaan ja tietosuojaan liittyvissä kysymyksissä, ohjeistuksissa ja säännöissä.

Sivustolle on myös kerätty vinkkejä oman kotikoneen tietoturvalliseen käyttöön. Myös ohjelmistojen käyttöoikeuslomakkeita uusitaan sähköiseen käyttöön sopivaksi.

Tietoturva:
Tietojen, palvelujen, järjestelmien ja tietoliikenteen suojaaminen.
(http://fi.wikipedia.org/wiki/Tietoturva)

Tietosuoja: ihmisen yksityisyyden suoja ja muut sitä turvaavat oikeudet henkilötietoja käsiteltäessä.
(http://www.tietosuoja.fi)

Tietoturvapolitiikka: Organisaation tasolla johdon hyväksymä näkemys tietoturvallisuuden päämääristä, periaatteista ja toteutuksesta. Tietoturvapolitiikka tai -strategia on kiinteä osa organisaation toiminta- ja tietohallintopolitiikkaa tai -strategiaa.

Tietoturvan jalkauttamissuunnitelma

Tietoturva tavaksi

Tietoturvan jalkauttamisen tarve loppukäyttäjille lähtee kaupungin tietoturvapolitiikasta. Siellä on mm. seuraavanlaiset maininnat:

Tietoturvallisuuden varmistaminen, ja kehittäminen edellyttävät jatkuvaa kehitystyötä ohjeistuksen, toimeenpanon ja henkilöstön osaamisen osalta

sekä

Käyttäjien toimintaa ohjataan käyttöoikeuksilla, säännöillä ja toimintaohjeilla sekä tietojen turvallisen käsittelyn koulutuksella ja tiedotuksella.

Tämä suunnitelma antaa kyseisille lauseille pohjan aloittamalla tietoturvan opettamisen henkilöstölle. Tavoitteena on saada tietoturvasta työntekijöille päivittäistä rutiinia.

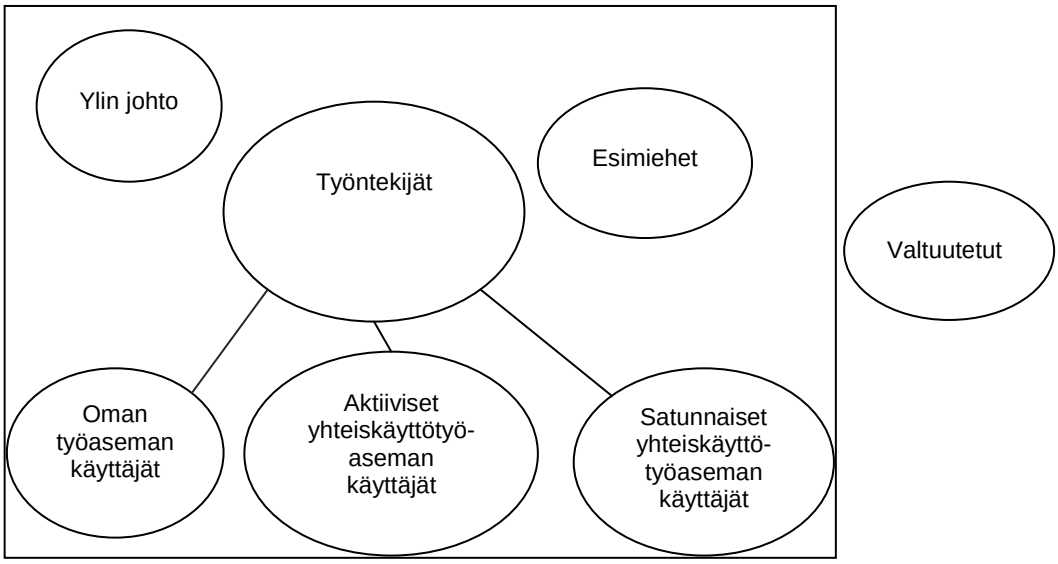
Jotta saamme kaupungin henkilöstön kiinnostumaan asiasta, otamme myös huomioon kaupungin henkilöstön tietoturvan tarpeet kotona. Kun käyttäjä osaa toimia kotona tietoturvallisesti, hän myös välittää tietoa tietoturvasta työpaikalleen omalla esimerkillään ja kahvipöytäkeskusteluissa. Käyttäjien motivointi tietoturvakoulutukseen on helpompaa, kun työpaikalta saadut opit voidaan siirtää myös kotiin.

Käyttäjien jako

Valtuutettujen koulutus?

Olemme jakaneet käyttäjät kolmeen koulutettavaan pääryhmään: *ylimpään johtoon, esimiehiin ja työntekijöihin*. Työntekijät jaetaan kolmeen alaryhmään: oman työaseman käyttäjiin, yhteiskäyttötyöaseman aktiivisiin käyttäjiin ja yhteiskäyttötyöaseman satunnaiskäyttäjiin. (Kuva 1.)

Oman työaseman käyttäjät tarkoittavat työntekijöitä joilla on kaupungin tarjoama kannettava tai työpisteellä kiinteä työasema, jota vain käyttää kyseinen työntekijä.
Aktiiviset yhteiskäyttötyöaseman käyttäjät ovat työntekijöitä jotka käyttävät yhteisiä työasemia päivittäin.
Satunnaiset yhteiskäyttötyöaseman käyttäjät ovat taas työntekijöitä jotka käyttävät työasemaa satunnaisesti. Esim. tarkistavat silloin tällöin työsähköpostinsa.



Kuva 1. Koulutettavien jako

Alkukartoitus

Pyydetään tarjoukset ulkoisesta oppimisympäristöstä (niistä joita Internetistä löytyy). Tietoturvalle tehdään kokonaan oma osion kaupungin intranetiin: tietoturva.kotka.fi. Sinne kerätään tärkeitä asioita ja vinkkejä tietoturvasta. Tarkoitus on, että kaikki tietoturvaan liittyvä materiaali on samassa paikassa, helposti saatavilla ja yksinkertaista päivittää.

Koulutuksen muoto

Ylimmälle johdolle koulutus tullaan järjestämään palaverien ja kokousten yhteydessä pienellä infotilaisuudella asiasta. Varsinainen koulutus tapahtuu ulkopuolisen toimittajan oppimisympäristössä, jossa ensin käydään asiat läpi ja lopuksi on pieni testi. Tällaista oppimisympäristöä voidaan käyttää miltä tahansa työasemalta ja milloin tahansa (liite 1).

Esimiehille koulutus järjestetään pienryhmissä,(Mikä on esimiesten määrä?) joissa ensin kerrotaan koulutuksen tarkoituksesta ja sen jälkeen esimiehet tekevät heille räätälöidyn testin oppimisympäristömoduulissa. Kouluttaja on läsnä tilaisuudessa, jos esim. kesken koulutuksen tulee kysymyksiä.

Työntekijöille koulutus järjestetään halukkuuden mukaan, ja halukkaiden määrästä riippuen työntekijät jaetaan kahteen koulutusmoduuliin: omien työasemien ja yhteistyöasemien käyttäjät. Koulutus tapahtuu massakoulutuksena auditorioissa ja työntekijöille suunnatun oppimisympäristömoduulin tekemisenä joko kotona tai työpaikalla.

Koulutuksen vaiheet

1. Vaihe

Käyttäjille tehdään tietoturvan osaamisen esikartoituskysely (esimiehet, työntekijät, ylin johto). Esikartoituksen ideana on saada tietoa käyttäjien tämän hetken osaamisesta ja painottaa koulutuksessa osia joita käyttäjät eivät hallitse tai itse tahtovat oppia (liitteet 2, 3 ja 4).

2. Vaihe

Aloitetaan kaupungin intranetissä tietoiskujen jakaminen (liite 5). Tällä tavalla saadaan työntekijät kiinnostumaan tärkeistä asioista mikä samalla herättää heidät ajattelemaan tietoturvaa päivittäisenä rutiinina. (Kuva 2) Esikartoituksen pohjalta suunnitellaan tarkemmat koulutustapahtumat erilaisille käyttäjäryhmille.

Kuva 2. Esimerkki mahdollisesta tietoiskun toteutuksesta

3. Vaihe

Aloitetaan koulutus esimiehille ja ylimmälle johdolle. Hierarkkisessa järjestelmässä koulutus on aina aloitettava ylhäältä, koska työntekijät ottavat mallia esimiehistään.

Esimiesten on myös osattava vastata alaistensa kysymyksiin ja tämä ei onnistu jos koulutusta ei ole järjestetty.
Tässä vaiheessa myös kysellään halukkaita työntekijöitä koulutuksiin.

4. Vaihe

Aloitetaan työntekijöiden koulutus.

5. Vaihe

6-12 kuukautta viimeisen koulutuksen jälkeen tehdään uusi kysely tietoturvasta jotta nähtäisiin onko koulutus onnistunut. Tehdään koulutuksen auditointi.

Aikataulu

Alkukartoitus	17.5.—30.6.2010
1. Vaihe	Elokuu 2010
2. Vaihe	Alkaa heinäkuussa
3. vaihe	Syyskuu (Tarvitseeko jakaa kahteen osaan esimiehet, ylin johto/työntekijät?)
4. vaihe	Lokakuu
5. vaihe	Maaliskuu 2011 (opinnäytetyö AMK-opiskelijalle?)