Opinnäytetyö (AMK)

Tietojenkäsittely

Yrityksen tietoliikenne ja tietoturva

2015

Samuel Héd

TIETOTURVAKARTOITUS CASE: TURUN KAUPUNGINKIRJASTON HENKILÖKUNTA

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Yrityksen tietoliikenne ja tietoturva

2015 | 52 s

Jarkko Paavola

Samuel Héd

TIETOTURVAKARTOITUS CASE: TURUN KAUPUNGINKIRJASTON HENKILÖKUNTA

Opinnäytetyön toimeksianto saatiin Turun kaupunginkirjastosta. Opinnäytetyön tavoitteena oli tutkia kirjaston tietoturvaosaamisen tasoa ja selvittää mahdolliset kehitystarpeet tietoturvan suhteen.

Tietoturvan tärkeys on nykypäivänä erittäin suuri ja sitä suuremmalla syyllä olisi hyvä, että tietoturvan merkitys ymmärrettäisiin jokapäiväisessä toiminnassa. Tietoturvan onnistunut toteutuminen on viime kädessä kiinni organisaation työntekijöiden omasta toiminnasta.

Työn teoriaosuudessa kerrotaan organisaation tietoturvasta, tietoturvauhista, hyvistä salasanakäytännöistä sekä Turun kaupungin tietoturvallisuuden organisoinnista ja hallintapolitiikasta. Lähteinä käytettiin alan kirjallisuutta ja verkkolähteitä.

Työn empiriaosa koostuu tutkimuksesta, joka suoritettiin toteuttamalla verkkokysely koko henkilökunnalle sekä haastattelukysely muutamalle kirjaston henkilökuntaan kuuluvalle henkilölle.

Tämän opinnäytetyön tutkimustuloksia voidaan käyttää apuna suunniteltaessa tietoturvakoulutusta Turun kaupunginkirjastossa tulevaisuudessa.

Jatkossa voidaan suunnitella toimenpiteet, toteutus ja seuranta tutkimuksessa esille tulleisiin kehitystarpeisiin Turun kaupunginkirjaston tietoturvan suhteen.

ASIASANAT:

tietoturva, tietoturvallisuus, kyberturvallisuus, salasana, organisaatio

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Business Data Communications and Information Security

2015 | 52 pages

Jarkko Paavola

Samuel Héd

INFORMATION SECURITY ANALYSIS CASE: TURKU CITY LIBRARY STAFF

Information security is extremely important these days which is why it is vital that the importance of information security is understood by an organisation’s employees when performing their everyday activities. A successful information security system therefore depends on the employees of the organisation.

This thesis was commissioned by Turku City Library. The aim of the thesis was to analyse the level of the library's information security and to identify the possible development requirements regarding information security.

The thesis’ theory section contains information on an organisation's information security, information security threats, secure passwords, as well as how the information security and management policy is handled by the City of Turku to which Turku City Library belongs. The source texts include relevant literature and online resources.

The empirical section of the thesis contains information on the research, which was carried out with an online survey administered to the entire Turku City Library staff and interview questions to selected staff members.

The survey results of this thesis can be used when planning information security training in the Turku City Library in future.

Future developments based on the results of this thesis could include planned actions, implementation and follow up for the development requirements of information security in Turku City Library.

KEYWORDS:

information security, cyber security, password, organisation

SISÄLTÖ

LIITTEET

KUVAT

1 JOHDANTO

Tietoturvalla tarkoitetaan sekä sähköisen tiedon että ei-sähköisen tiedon turvaamista. Sen merkitys on varsinkin tänä päivänä erittäin suuri. Olisi tärkeää, että kaikki kansalaiset ymmärtäisivät tietoturvan tärkeyden jokapäiväisessä toiminnassaan. Organisaatioiden työntekijät ovat avainasemassa tietoturvan toteutumisen suhteen.

Opinnäytetyön toimeksianto saatiin työharjoittelun yhteydessä. Työn teoriaosuudessa kerrotaan organisaation tietoturvasta, tietoturvaohjeista ja uhista, hyvistä salasanakäytännöistä sekä Turun kaupungin tietoturvallisuuden organisoinnista ja hallintapolitiikasta. Lisäksi työssä kerrotaan tietoturva-asiantuntija Petteri Järvisen tietoturvaa käsittelevästä luennosta Turun kaupunginkirjastossa.

Opinnäytetyön empiriaosa koostuu tutkimuksesta, jonka tarkoituksena on kartoittaa kirjaston henkilökunnan nykyinen tietoturvaosaamisen taso ja selvittää mahdolliset kehitystarpeet tietoturvaan liittyen. Kysely toteutettiin kaksiosaisena: koko henkilökunnalle suunnattu Webropol-kysely sekä henkilökohtainen haastattelu yhdeksälle valitulle kirjaston henkilökuntaan kuuluvalle henkilölle.

Kyselyä suunniteltaessa pyrittiin mahdollisimman hyvin ottamaan huomioon kohderyhmä. Tavoitteena oli laatia selkeät ja helposti ymmärrettävät kysymykset. Haastattelukysymykset olivat osittain samanlaiset kuin Webropol-kyselyssä, mutta niitä oli vähemmän ja niihin oli tarkoitus saada monipuolisemmat vastaukset.

2 TIETOTURVALLISUUS

2.1 Organisaation tietoturva

Organisaation kehittymisen edellytyksenä on hyvin hoidettu tietoturva. Kaikkien työntekijöiden olisi hyvä olla tietoisia käsittelemänsä tiedon merkityksestä organisaatiolle ja omasta roolistaan sen suhteen. Tunnettua on, että organisaation tietoturva on juuri niin vahva kuin sen heikoin lenkki. Viestintä ja kouluttaminen ovat tärkeässä asemassa, jotta tietoa käsitellään sen vaatimalla tarkkuudella. (Andreasson & Koivisto 2013, 12.)

Useissa organisaatioissa ollaan siirtymässä asiakaspalvelussa yhä enenevässä määrin tieto- ja viestintätekniikkaa monipuolisesti käyttävään itse- ja yhteispalveluun. Tästä syystä asiakirjojen sähköisen käsittelyn suunnitteluprojektit ja erilaiset verkkopalvelustrategiat ovat nyt juuri monissa organisaatioissa keskeisessä asemassa.

Yhteiskunnan kehittyminen on tehnyt mahdolliseksi sen, että tietoa on voitu kerätä ehkä turhankin paljon; tietojen pääsy väärin käsiin on myös mahdollista. Loppuvuodesta 2011 uutisoitiin 16 000 suomalaisen henkilötietojen vuotaneen verkkoon. (Andreasson & Koivisto 2013, 13-14.) Myös julkishallintoon kohdistui tässä yhteydessä tietomurtoja. Tästä voidaan päätellä kuinka tärkeää on pitää huolta palvelujen tietoturvallisuudesta. Henkilötiedot tulee suojata luvattomalta käytöltä ja käsittelyltä.

Jokin aika sitten tuli julkisuuteen tieto erittäin suuresta tietovuodosta. Suomalaiselle keskustelufoorumille julkaistiin lista, joka sisälsi noin puoli miljoonaa sähköpostiosoitetta. (Andreasson & Koivisto 2013, 13-14.) Se oli saatu murtautumalla yhteen tai useampaan Internetin palveluun. Lista sisälsi useiden yritysten ja kuntien työsähköpostiosoitteita. Tämä lisää organisaatioiden saamaa roskapostia; tietoturva ei todennäköisesti kuitenkaan olisi vaarassa.

Suositeltavaa onkin, että työsähköpostiosoitteita ei käytettäisi Internetin palveluissa. Erityisesti kannattaa välttää verkkopalveluita, joiden avulla tarkastetaan

onko omia tietoja vuodetuilla listoilla. Jotkut näistä palveluista ovat huijausta. Niiden avulla kerätään tietojensa tarkastajien palveluun antamat tiedot ja tämän jälkeen kyseiset sähköpostiosoitteet ovatkin vuodetuilla listoilla. (Andreasson & Koivisto 2013, 13-14.)

Suomen lainsäädännössä määrätään, että tietoturva on pyrittävä hoitamaan asianmukaisesti ja se kuuluu organisaatioiden päivittäiseen toimintaan (Andreasson & Koivisto 2013, 29). Tiedot, palvelut, järjestelmät ja tietoliikenne on suojattava ja niihin kohdistuvat riskit on hallittava sekä normaali- että poikkeusoloissa. Tietojen luottamuksellisuus, eheys ja käytettävyys turvataan laitteisto- ja ohjelmistovikojen, luonnonmullistusten sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta.

Tietoturvallisuustyön tavoitteena on suojata organisaatiolle tärkeiden tietojärjestelmien ja tietoverkkojen jatkuva toiminta, estää tietojen ja tietojärjestelmien asiaton käyttö, tiedon tuhoutuminen tai muuttuminen sekä minimoida aiheutuvat vahingot. Tietoturvallisuuteen pitää erityisesti kiinnittää huomiota silloin kun ulkoistetaan tietojenkäsittelyä ja tietotekniikan ylläpitoa sekä otetaan käyttöön uusia toimintatapoja. (Andreasson & Koivisto 2013, 29.)

On arvioitu, että Suomi olisi toimintakyvytön noin viidessä minuutissa merkittävän kyberuhan toteutuessa (Manninen 2015, 21). Pääesikunnan johtamisjärjestelmäosaston kyberpuolustussektorin johtajan Catharina Candolinin mukaan se lienee kuitenkin liioittelua. Suomella on varautumissuunnitelmat, joiden avulla järjestelmät saataisiin taas toimimaan. Maan johto kykenisi päätöksentekoon ja kansalaisetkin tulisivat toimeen jonkun aikaa ilman suuria vahinkoja, toteaa Candolin. (Manninen 2015, 21.)

2.2 Riskien arviointi ja hallinta

Organisaatioissa on tärkeää huolehtia siitä, että tietoturvariskejä arvioidaan säännönmukaisesti osana organisaation muuta riskienhallintaa. Tietoriskejä ar-

vioidaan suhteessa lainsäädäntöön, toimintaympäristöön ja kustannukset huomioon ottaen. Tietoturvariskejä arvioidaan organisaation perustehtävän ja asetettujen strategioiden ja tavoitteiden mukaan. (Andreasson & Koivisto 2013, 39.)

Resurssien vähyys usein hankaloittaa tietoturvan toteuttamista. Valitettavasti tietoturvatyö tehdään organisaatioissa usein muun työn ohessa, joten kukaan ei huolehdi siitä kokopäiväisesti. Tietoturvan toteutumiseen olisi hyvä tällaisessa tilanteessa osoittaa riittävät resurssit johdon toimesta. Suuremmissa organisaatioissa on yleensä tietoturvapäällikkö tai -vastaava, mutta hänen voi olla vaikea saada organisaation muu henkilöstö noudattamaan tietoturvaohjeistusta. Usein kannattaa nimetä organisaation muista osista yhteyshenkilöt, jotka hoitavat oman toimensa ohella tietoturva-asioita. Voidaan myös hyödyntää esim. riskienhallinnan organisaatiota, johon eri yksiköille on jo valmiiksi nimetty yhteyshenkilöt. Organisaatiolla pitäisi olla myös sisäinen tietoturvaraportointikäytäntö. (Andreasson & Koivisto 2013, 45.)

2.3 Tietoturvauhat

Verizon Data Breach Report 2014-raportin mukaan yksi suosituimmista tietomurtokohteista ovat tietokannat. Tämä johtuu siitä, että ne ovat organisaatioissa avainasemassa. Tietokannat sisältävät asiakastietoja ja muuta luottamuksellista aineistoa. (Imperva 2014.)

Herää kysymys miksi tietokannat ovat niin vahingoille alttiita? Todennäköinen syy lienee se, että organisaatioissa ei panosteta tarpeeksi tietokantojen suojelemiseen tietoturvauhilta.

Silloin kun krakkerit ja muut tietoturvarikolliset pääsevät käsiksi arkaluonteisiin tietoihin seuraa siitä kohteille nopeasti taloudellisia menetyksiä, vahinkoa ja haittaa liiketoiminnalle. Vähäisiä eivät ole myöskään näistä rikoksista aiheutuvat imagonmenetykset kyseisille organisaatioille. Positiivista kuitenkin on se, että Online Trust Alliancen mukaan vuonna 2013 yli 97 % tietomurroista olisi voitu estää panostamalla sisäiseen valvontaan ja toteuttamalla hyviä käytäntöjä sekä noudattamalla yksinkertaisia ohjeita. (Imperva 2014.)

Lähes vaarattomia sähköpostihuijauksia ovat ketjukirjeet, joissa pyydetään levittämään sähköpostiviestiä omille tuttaville. Ikävimpiä ovat tuntemattomilta tulevat viestit joissa huijataan lähettämään rahaa mm. ulkomaille. (Järvinen 2006, 52-53.)

Maalaisjärjen käyttö voi auttaa tunnistamaan epäluotettavan palvelun tai epäilyttävän verkkokaupan. Yleensä onkin niin, että jos jokin kuulostaa liian hyvältä ollakseen totta, se ei olekaan totta. Internet on luonut mahdollisuuden uuteen, edulliseen toimintamalliin. Tällä tavoin hintatasoa on saatu madallutettua. Tästä huolimatta ero normaaliin kauppaan ei voi olla merkittävän suuri. Jos sivusto lupaa tuotteita tai palveluita erittäin halvalla yleiseen hintatasoon nähden, on syytä epäillä sivuston luotettavuutta. (Järvinen 2006, 53-54.)

Luotettavalla nettipalvelulla tulee aina olla fyysinen katuosoite. Epäilykset herää-vät jos sivustolta löytyy ainoastaan sähköpostiosoite ja puhelinnumero. Huomioitavaa on, että sivustolla oleva osoitetietokin saattaa olla keksitty ja osoitteen tarkastaminen esim. ulkomailta on haastavaa.

Verkkosivuston ulkoasusta on vaikea päätellä palvelun luotettavuutta. Kuitenkin sivuston kieliasu on sidoksissa sen luotettavuuden kanssa. Aidon palvelun sivustolla ei ole kirjoitusvirheitä. Varovaisuutta aiheuttaa se, jos suomenkielisellä sivustolla on paljon kielivirheitä. Tämä ei välttämättä merkitse huijausta, vaan kertoo siitä, että on käytetty koneellista käännöstä. (Järvinen 2006, 55.)

2.4 CIA-malli

Tietoturvan pääperiaatteet ovat luottamuksellisuus (Confidentiality), eheys (Integrity) ja saatavuus (Availability). Nämä kolme edellä mainittua periaatetta muodostavat yhdessä tietoturvan toteutumisen tukipilarit.

2.4.1 Luottamuksellisuus

Salassa pidettävät tai luokitellut tiedot voivat saada käyttöönsä vain sellaiset henkilöt, joilla on tiedonsaanti- ja käyttöoikeudet niihin. Luottamuksellisuus toteutetaan yleensä käyttöoikeuksien hallinnalla. Tällöin käyttäjälle annetaan organisaation käytössä oleviin järjestelmiin työtehtävien vaatimat oikeudet. Työpaikalta käyttöön saatujen käyttäjätunnusten ja salasanojen kanssa pitää noudattaa erityistä huolellisuutta - mikäli ne joutuvat rikollisten haltuun, voidaan niiden avulla aiheuttaa esim. tietovuoto ja sitä kautta mittavat vahingot.

Jos rikollinen saa haltuunsa sähköpostiosoitteen, hänellä on pääsy kaikkiin niihin tietoihin, joita siinä sähköpostiosoitteessa on käsitelty. Hän voi nähdä, mitä nettipalveluja on käytetty, joten hän voi helposti vaihtaa näiden palveluiden salasanat "Unohtunut salasana" -toiminnolla ja saada näin palvelut omaan käyttöönsä. Nettikauppa-asioinnissa kannattaa huomioida, että mikäli rikollinen saa tunnukset sinnekin haltuunsa, niin hän voi selvittää helposti esim. luottokorttien tietoja ja tehdä ostoksia niitä käyttäen.

Varmuuskopioiden ottaminen on olennaisen tärkeää silloin, kun kyseessä on kriittiset tietojärjestelmät. Tällöin pystytään säilyttämään tietojen eheys ja palauttamaan hallitsemattomasti muuttuneet tiedot. (Rousku 2014, 47-48.)

Tiedot voidaan luokitella eri ryhmiin sen mukaan minkäasteista vahinkoa organisaatioille aiheutuisi tietojen jouduttua vääriin käsiin. Toimenpiteiden tiukkuus määräytyy sen mukaan mihin kategoriaan kyseessä olevat tiedot kuuluvat.

Normaalikäytäntö luottamuksellisuuden varmistamiseksi on käyttäjätunnuksien ja salasanojen käyttö. Kahdennetusta tunnistautumisesta on tulossa normi. Lisäksi tunnistautumiseen voidaan käyttää muun muassa biometristä todentamista ja henkilökohtaisia tunnistekortteja. Luottamuksellisuutta voidaan myös parantaa minimoimalla tiedonsiirtokerrat ja ne paikat, joissa tiedot näkyvät. (What is techtarget 2014.)

2.4.2 Eheys

Eheydellä tarkoitetaan tietojen tarkkuuden, johdonmukaisuuden ja luettavuuden säilymistä. Data ei saa muuttua tietojen siirron aikana. Myös tietoihin kohdistuvat luvattomat muutokset on estettävä. Lisäksi pitää pystyä estämään ei-inhimillisten tapahtumien, kuten sähkömagneettisten häiriöiden tai palvelimien kaatumisien aiheuttamat muutokset tietojen eheyteen. (What is techtarget 2014.)

Yhteiskunnassa esimerkiksi henkilö- ja väestötiedot, kansalaisten terveydenhoitoon liittyvät tiedot, julkishallinnon johtamisessa tarvittavat järjestelmät, pankkijärjestelmät, verotus, maanomistus- ja kiinteistötiedot, sekä vakuutustiedot ovat sellaisia järjestelmiä ja tietoja, joiden täytyy pysyä muuttumattomina ja jotka pitää kaikissa olosuhteissa pystyä palauttamaan. (Rousku 2014, 49.)

2.4.3 Saatavuus

Tiedon saatavuus on sitä, että tietojen täytyy olla saatavilla käyttäjille palvelussa tai järjestelmässä määritetyn vasteajan sisällä. Yhteiskunnan digitalisoitumisen vuoksi tietojen ja palvelun pitää olla käytettävissä jatkuvasti. Palvelut yritetään pitää toiminnassa nykyään sadan prosentin vasteajalla pakollisia huoltokatkoja lukuun ottamatta.

Nykyään palvelunestohyökkäykset ovat yleistyneet myös Suomessa. Palvelun tarjoajat eivät ole tarpeeksi investoineet tällaisten hyökkäysten torjuntaan, koska sellaiselle ei aikaisemmin ole ollut tarvetta ja siitä koituisi lisäkustannuksia asiakkaille. (Rousku 2014, 50-51.)

2.5 Hyvät salasanakäytännöt

On tärkeää, että eri palveluissa käytetään eri salasanoja. Tästä johtuen salasanojen määrä kasvaa jatkuvasti. Niiden ulkoa muistaminen voi olla hankalaa, joten on järkevää esim. kirjoittaa ne paperille ylös tai tallentaa puhelimeen. Muistiin

merkityt salasanat eivät saa olla selkokielisiä siksi ettei niitä pystyttäisi yhdistämään palveluihin, joissa niitä käytetään. Huonosta salasanasta saa hyvän korvaamalla kirjaimia numeroilla ja erikoismerkeillä. Tutkimuksien mukaan maailman yleisimpiä salasanoja ovat 123456 sekä password. (Rousku 2014, 179-181.)

Salasanojen laatimiseen on useita eri ohjeita joiden tarkoituksena on pyrkiä estämään salasanan murtaminen teknisin keinoin. Seuraavassa luettelossa on hyviä ohjeita salasanojen muodostamiseen:

- Salasanassa on hyvä käyttää sekä isoja että pieniä kirjaimia, numeroita ja erikoismerkkejä, koska tällaisen salasanan murtaminen kestää kauemmin.
- Salasanan minimipituus tulisi olla vähintään 12 merkkiä, koska mitä pitempi salasana on sen kauemmin sen laskennallinen murtaminen kestää.
- Salasana on hyvä vaihtaa aika ajoin esim. kolmen kuukauden välein, koska jos salasana päätyy vääriin käsiin, niin sen säännöllinen vaihtuminen estää väärinkäytön jatkumisen. Jos lisätään salasanan minimipituutta esim. 15–18 merkkiin, niin voidaan samalla pidentää salasanan vaihtoväliä 6-9 kuukauteen. (Rousku 2014, 179-181.)
- Käyttäjätili lukkiutuu määrätyksi ajaksi, kun on syöttänyt salasanan väärin tarpeeksi monta kertaa. Tämä vaikeuttaa käyttäjätunnuksen murtamista, koska salasanan syöttöä ei siten voi yrittää rajattomasti.
- Salasanan ei pidä rakentua minkään kielisestä ymmärrettävästä sanasta, koska se helpottaa salasanan murtamista. Pelkkä erikoismerkkien käyttö salasanan alussa tai lopussa ei auta. (Rousku 2014, 179-181.)

3 TURUN KAUPUNGIN TIETOTURVALLISUUS

3.1 Tietoturvallisuuden organisoiminen

Turun kaupunginjohtaja vastaa kaupungin tietoturvasta ja sen kehittämisestä. Kaupungin riskienhallintapäällikön toimenkuvaan kuuluu tietoturvavastaavan tehtävät. Hallintokunnissa ja kaupungin organisaatioissa vastuu tietoturvasta on virastopäälliköllä tai vastaavalla. Tietoturvavastaava hallinnoi tietoturvaan liittyviä tehtäviä ja delegoi käytännön toimia muille, esim. tietoturvakoulutuksen järjestäminen, teknisen tietoturvan toteuttaminen ja kulunvalvonta. Lisäksi hän valvoo, että edellä mainitut tehtävät tehdään.

Esimiehien vastuulla on, että hänen alaisensa ovat selvillä tietoturvan säännöistä ja vaatimuksista sekä myös noudattavat niitä. Esimiehen vastuulla on perehdyttää uudet työntekijät ja sijaiset yksikön tietoturvaperiaatteisiin. Henkilöstöllä on vastuu tietoturvan toteutuksesta omalta osaltaan. Henkilöstön täytyy välittömästi kertoa havaituista rikkomuksista sekä tietoturvallisuuteen liittyvistä aukoista esimiehelleen.

Kaupungin hallintokunnilla ja eri kaupungin organisaatioilla on tietoturvaryhmä. Ryhmän puheenjohtajana toimii organisaation tietoturvavastaava. Ryhmän tärkeimpiä tehtäviä ovat riskianalyysin toteuttaminen, tietoturvallisuuden kehittämissuunnitelman suunnittelu ja seuranta sekä auditoinnista huolehtiminen.

Kaupungin IT-toiminnan tietoturvaosaaminen on kaikkien hallintokuntien käytettävissä. IT-toiminta toteuttaa tietoturvaa koskevia asiantuntija- ja konsultointipalveluja. Koulutusta tietoturva-asioista toteutetaan yhteistyössä henkilöstökoulutuksesta vastaavien kanssa. (Turun kaupunki 2008.)

3.2 Tietoturvallisuuden hallintapolitiikka

Tietoturvatyössä tärkeintä ovat asenteet, toisin sanoen henkilöstö on sisäistänyt tietoturvan merkityksen ja on myös hyvin motivoitunut noudattamaan tietoturvaan

liittyviä määräyksiä ja ohjeita. Hyvä keino tietoturvatietoisuuden lisäämiseen on säännönmukainen tietoturvakoulutus.

Turun kaupunki noudattaa tietoturvallisuuden hallintajärjestelmässään ISO/EIC 27001-standardia. Tietoturvallisuuden hallintajärjestelmään kuuluu riskianalyysi, jota päivitetään säännöllisesti. Tietoturvallisuuden riskianalyysi voi olla laajemman riskianalyysin osa.

Tietoturva-asiat tulee ottaa huomioon henkilöstön työhönotossa ja koulutuksessa. Perustason tietoturvallisuuskoulutus tarjotaan uusille työntekijöille. Pyritään siihen, että jokainen työntekijä voisi osallistua tietoturvakoulutukseen säännöllisesti. (Turun kaupunki 2011.)

4 TIETOTURVA-ASIANTUNTIJA PETTERI JÄRVISEN LUENTO TURUN KAUPUNGIN KIRJASTOSSA

4.1 Tietoturvan merkitys ja käytännön ohjeita

Tietoturva-asiantuntija Petteri Järvinen kävi luennoimassa Turvassa kirjastossa -nimisessä tilaisuudessa 10.12.2014. Järvisen mukaan tietoturva on osa jokaisen arkipäivää. Joudumme tekemisiin sen kanssa työssämme, kotona sekä harrastuksissa. Järvinen herätteli keskustelua siitä, mihin tallennetut tiedot menevät ja kuka näkee nämä tiedot. Hänen mukaansa rutiinit tuovat turvallisuutta tietoturva-asioissa, esimerkiksi siten, että noudatetaan asetettuja sääntöjä.

Hänen mielestään on hyvä varautua odottamattomiin tilanteisiin. Järvinen toteaa, että ei kannata hyväksyä valintaa jos ei ymmärrä mihin pyydetään suostumusta. Lisäksi hän neuvoi, että ei ole hyvä avata tuntemattomia liitteitä ja linkkejä, jättää papereita työpöydälle eikä käyttää toisen tunnusta luvatta. Myöskään ei ole hyvä antaa lasten pelata ja surffata työkoneella. Hän lisäksi muistuttaa välitallennuksien tärkeydestä. Hänen mukaansa vieras kone ei voi olla täysin turvallinen ja kehottaa varomaan vieraita USB-muistitikkuja.

4.2 Nettikäyttäytyminen

Järvisen mukaan kannattaa noudattaa varovaisuutta netissä ja miettiä tarkoin ennen kuin toimii. Esimerkiksi Facebookissa on syytä suhtautua varauksella outoihin kaveripyyntöihin. Hän muistutti myös salasanojen tärkeydestä ja jakoi perustason neuvoja salasanoihin liittyen; muun muassa salasana olisi vaihdettava usein, sitä ei ole hyvä kirjoittaa muistiin, eri palveluihin eri salasanat ja salasanan olisi hyvä olla pitkä ja mutkikas. Hän totesi myös, että kaksiosainen todennus on suositeltavaa.

Hänen mukaansa olisi hyvä peittää koneen web-kamera silloin kun sitä ei käytä, koska sen välityksellä voidaan suorittaa urkintaa. Hän kertoi, että tietojenkalastelu on nykyään erittäin yleistä. Pankkitunnuksia voidaan yrittää urkkia ja huijausviestien avulla voidaan kiristää viestinsaajaa. Järvisen mukaan avoin WLAN-yhteys pitää sisällään aina riskin. Salaamaton liikenne on kaikkien nähtävissä. Tietoliikenne on mahdollista kaapata valepalvelimelle, mutta salasanalla suojattu sisältö pysyy turvassa.

4.3 Mobiililaitteet

Lisäksi hän puhui tämän päivän mobiililaitteista. Laite tietää kaikki käyttäjän salaisuudet ja tiedot tallentuvat myös pilveen. Mobiililaitteissa ei ole juurikaan haittaohjelmia, esimerkiksi IPad on erittäin turvallinen. Mobiililaitteen katoaminen on suurempi riski kuin sen tietoturva. Järvinen suosittelee käyttämään pilvipalveluita ja mobiililaitteisiin saatavilla olevia paikannuspalveluja.

4.4 Johtopäätökset

Luennon anti oli perustason tietoturvainfoa, jonka asiasisältö oli jo useimmille ennestään tuttua. Luennon sanoma oli se, että maalaisjärjen käyttö on suositeltavaa tietoturva-asioissa.

5 KYSELY JA HAASTATTELUT

Kysely toteutettiin kaksiosaisena: koko henkilökunnalle suunnattu Webropol-kysely sekä henkilökohtainen haastattelu yhdeksälle valitulle kirjaston henkilökuntaan kuuluvalle henkilölle. Haastatteluun valittiin henkilöitä, joiden työtehtäviin tietoturva-asiat olennaisesti liittyvät.

Kysely laadittiin käyttäen Webropol-kysely- ja analysointisovellusta. Sovellus oli helppokäyttöinen ja antoi selkeät tutkimustulokset, joista johtopäätösten tekeminen oli vaivatonta.

Tutkimus suoritettiin joulukuussa ja vastausaikaa oli parisen viikkoa. Tutkimuksen toteutuksen aikana osa kirjaston henkilökunnasta oli lomalla, mikä vaikutti vähentävästi vastaajien määrään.

Kyselyä suunniteltaessa pyrittiin mahdollisimman hyvin ottamaan huomioon kohderyhmä. Tavoitteena oli laatia selkeät ja helposti ymmärrettävät kysymykset. Kysymyksiä suunniteltaessa pidettiin mielessä ohje hyvän Webropol-kyselyn tekemiseen:

- ei liian monia vastausvaihtoehtoja
- ei päällekkäisiä vastausvaihtoehtoja
- yhdessä kysymyksessä kysytään vain yhtä asiaa

Kysymysten määrä haluttiin pitää mahdollisimman pienenä, jottei kyselyyn vastaaminen veisi kohtuuttomasti aikaa. Kyselyyn pystyi vastaamaan 5-10 minuutissa. Kysely sisälsi monivalintakysymyksiä sekä kysymyksiä, joihin oli yksinkertaiset vastausvaihtoehdot ”Kyllä” tai ”Ei”. Kyselyssä tiedusteltiin myös henkilökunnan omia ideoita kirjaston tietoturvallisuuden parantamiseksi. Kyselyn lopussa tiedusteltiin vastaajien ajatuksia Petteri Järvisen tietoturvaluennosta sekä annettiin mahdollisuus antaa vapaata palautetta.

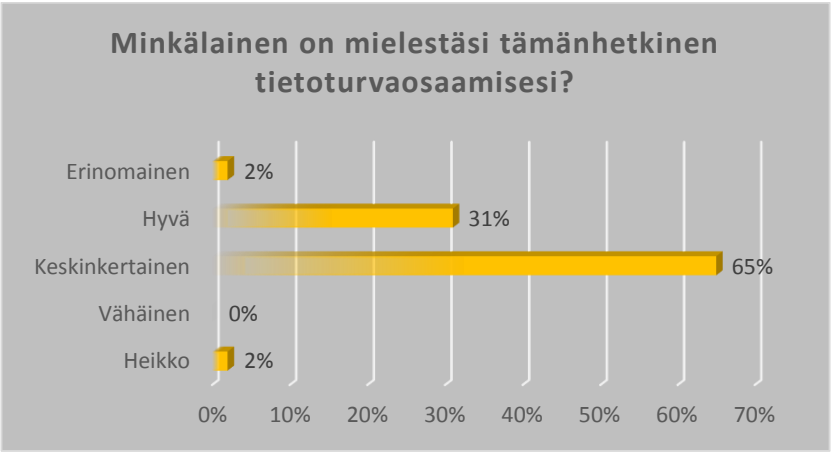
Haastattelukysymykset olivat osittain samanlaiset kuin Webropol-kyselyssä, mutta niitä oli vähemmän ja niihin oli tarkoitus saada monipuolisemmat vastaukset. Kysymykset jaettiin haastateltaville hyvissä ajoin etukäteen siksi, että heillä

oli mahdollisuus miettiä omia vastauksiaan rauhassa. Haastattelujen aikataulu suunniteltiin siten, että yhdelle haastattelulle varattiin aikaa puoli tuntia. Haastattelukysymyksillä pyrittiin selvittämään haastateltujen mielipide siitä, minkälainen on tietoturvan taso Turun kaupunginkirjastossa. Lisäksi tavoitteena oli saada heidän parannusehdotuksiaan kirjaston tietoturvaan liittyen.

5.1 Kysely

Kyselyyn vastasi 46 henkilöä. Joihinkin kysymyksiin olivat muutamat jättäneet vastaamatta.

Kysymys 1: *”Minkälainen on mielestäsi tämänhetkinen tietoturvaosaamisesi?”* Vastausvaihtoehtoina olivat: ”Erinomainen”, ”Hyvä”, ”Keskinkertainen”, ”Vähäinen” vai ”Heikko”.

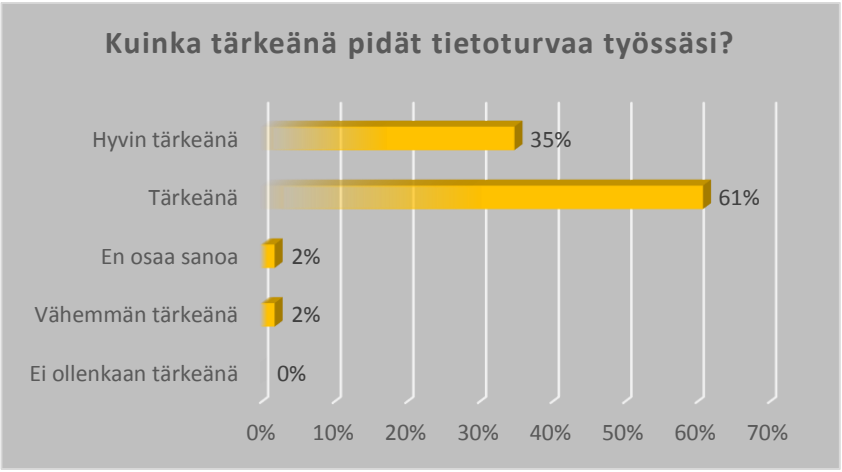


Kuva 1. Tietoturvaosaamisen taso.

Suurin osa vastaajista eli 65 % luokittelee tietoturvaosaamisensa keskinkertaiseksi. Kuitenkin 30 % vastaajista piti tietoturvaosaamistaan hyvänä. Ainoastaan 2 % vastaajista piti tietoturvaosaamistaan joko heikkona tai erinomaisena. Tulosten perusteella voidaan päätellä, että henkilökunnan tietoturvaosaaminen on heidän mielestään tyydyttävällä tasolla, tosin parantamisenkin varaa on.

Kysymys 2: *”Kuinka tärkeänä pidät tietoturvaa työssäsi?”*

Vastausvaihtoehtoina olivat: ”Hyvin tärkeänä”, ”Tärkeänä”, ”En osaa sanoa”, ”Vähemmän tärkeänä” vai ”Ei ollenkaan tärkeänä”.



Kuva 2. Tietoturvan tärkeys.

Suurin osa vastaajista eli 61 % pitää tietoturvaa tärkeänä työssään. Merkille pantavaa on, että niinkin paljon kuin 35 % pitää tietoturvaa hyvin tärkeänä työssään. Ainoastaan 2 % vastaajista piti tietoturvaa vähemmän tärkeänä tai valitsi vaihtoehdon ”En osaa sanoa”. Tulosten perusteella voidaan päätellä, että henkilökunta ymmärtää omasta mielestään hyvin tietoturvan tärkeyden työssään.

Kysymys 3: *”Onko sinulla ideoita tietoturvallisuuden parantamiseksi kirjastossa?”*

Tässä kysymyksessä ei ollut valmiita vastausvaihtoehtoja, vaan jokainen sai mahdollisuuden kertoa omia ideoitaan tietoturvan parantamiseksi.

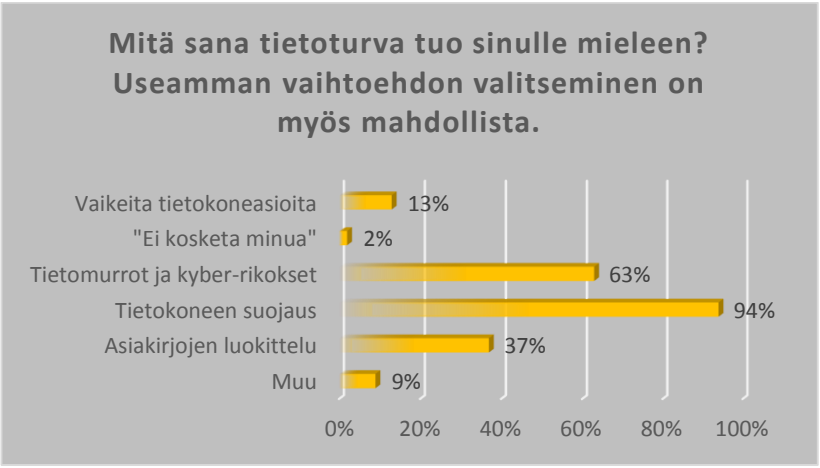
Vastaajat peräänkuuluttavat informaation lisäämistä ja henkilökunta kokee, ettei informaation levittämiselle ole sopivia kanavia. Lisää tietoturvakoulutusta kaivataan. Pidettiin ristiriitaisena sitä, että määrätyt tietojärjestelmät vaativat salasanan vaihtoa verrattain usein, mutta kehotusta Outlookin salasanan vaihtoon ei tule.

Kommenttina kerrotaan, että salasanan säilytys näppäimistön alla ei ole suotavaa. Samoin yhteistunnukset eivät ole tietoturvan näkökulmasta suositeltavia. Oltiin myös sitä mieltä, että koneissa olisi hyvä olla aikakatkaisu esim. jos sosiaalisesta mediasta uloskirjautuminen on jostain syystä unohtunut. Monista vastaajista olisi tärkeää, että salasanat vaihdettaisiin useammin.

Esitettiin toivomus siitä, että verkkokirjastoa ja sen hakumahdollisuuksia parannettaisiin siten, että sitä olisi mahdollisuus käyttää paremmin tiedonhakuun asiakkaiden kanssa. Tämä siksi, että hakuun ei tarvitsisi käyttää tässä yhteydessä Aurora-järjestelmää, jossa asiakkaiden henkilötiedot saattavat tulla näkyviin näytölle ulkopuolisten nähtäviksi.

Kysymys 4: *”Mitä sana tietoturva tuo sinulle mieleen? Useamman vaihtoehdon valitseminen on myös mahdollista.”*

Vastausvaihtoehtoina olivat: ”Vaikeita tietokoneasioita”, ”Ei kosketa minua”, ”Tietomurrot ja kyber-rikokset”, ”Tietokoneen suojaus (virustorjuntaohjelma, palomuuri ym.)”, ”Asiakirjojen luokittelu (salassa pidettävät jne.)” vai ”Muu”.



Kuva 3. Mielikuvat tietoturvasta.

Suurin osa vastaajista on sitä mieltä, että tietoturva tarkoittaa tietokoneen suojaamista, tietomurtoja ja kyberrikoksia. Myös asiakirjojen luokittelun ymmärretään olevan tietoturvan kannalta tärkeää. Positiivista on, että vain muutama vastaajista oli sitä mieltä, että tietoturva tarkoittaa vaikeita tietokoneasioita tai tietoturva ei

kuulu heidän työnkuvaansa. Joidenkin mieleen tietoturva tuo seuraavat asiat: henkilötietoturva, salasanat, henkilötietosuoja, kaikki mitä ei haluta jakaa koko maailmalle ja henkilötietojen käsittely.

Kysymys 5: *”Onko kirjaston tietoturvataso mielestäsi tarpeeksi korkea?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 4. Tietoturvatason korkeus.

Suurin osa vastaajista eli 72 % oli sitä mieltä, että kirjaston tietoturvataso on riittävän korkea. Vastaajista 28 % oli sitä mieltä, että tietoturvassa on parantamisen varaa. Tästä voidaan päätellä, että kirjaston tietoturva on vastaajien mielestä tyydyttävällä tasolla, mutta parannettavaakin löytyy.

Kysymys 6: *”Tiedätkö kuka vastaa kirjaston tietoturva-asioista?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 5. Tietoturvavastaava.

Suurin osa vastaajista eli 72 % ei tiennyt kuka vastaa kirjaston tietoturva-asioista. Vain 28 % vastasi tietävänsä. Tämä osoittaa, että henkilökunnalle olisi syytä informoida paremmin siitä kuka vastaa kirjaston tietoturva-asioista.

Kysymys 7: *”Onko kirjastossa järjestetty aikaisemmin koulutusta tietoturva-asioista?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 6. Tietoturvakoulutukset.

Vähän yli puolet vastaajista kertoi, että tietoturvakoulutuksia on kirjastossa aikaisemmin järjestetty. Kuitenkin koska vastaajista lähes 48 % vastasi ”Ei” näyttää siltä, että kaikki eivät välttämättä ole päässeet osallistumaan näihin koulutuksiin.

Kysymys 8: *”Mitkä seuraavista mahdollisista riskeistä voisivat toteutuessaan aiheuttaa merkittävää vahinkoa kirjastossa? Useamman vaihtoehdon valitseminen on myös mahdollista.”*

Vastausvaihtoehtona olivat: ”Tietojen menetys”, ”Tietomurto”, ”Työntekijöiden tietovuodot”, ”Fyysiset vahinkotapaukset (vesivahinko, tulipalo, murto yms.)”, ”Tietovälineiden häviäminen” vai ”Muu”.

Kuva 7. Mahdolliset toteutuvat riskit.

Suurimpina riskeinä vastaajat pitivät tietojen menetystä ja tietomurtoja. Aika merkittävinä riskeinä pidettiin myös työntekijöiden tietovuotoja, fyysisiä vahinkotapauksia ja tietovälineiden häviämistä. Lisäksi on mahdollista, että henkilökunnan osaamattomuus tietoturvan suhteen voi vaarantaa tietoturvan toteutumista.

Kysymys 9: *”Oletko tutustunut kirjaston tietoturvaohjeisiin?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 8. Tietoturvaohjeet.

63 % vastaajista kertoi tutustuneensa kirjaston tietoturvaohjeisiin, kun taas 37 % vastaajista kertoi, ettei ole tutustunut niihin. Olisi suositeltavaa, että kaikki työntekijät tutustuisivat kirjaston tietoturvaohjeisiin.

Kysymys 10: *”Tiedostatko mitkä ovat omat tietoturvavastuusi?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 9. Tietoturvavastuut.

Suurin osa vastaajista eli 89 % tiedostaa omat tietoturvavastuunsa. 11 % ei tunne omia tietoturvavastuitaan. Olisi hyvä, että kaikki työntekijät ymmärtäisivät oman tietoturvavastuunsa.

Kysymys 11: *”Poistuessasi työpisteeltäsi muistatko lukita työasemasi?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 10. Työaseman lukitseminen.

74 % vastaajista on muistanut lukita työasemansa työpisteeltään poistuessaan, kun taas 26 % vastaajista ei ole näin muistanut toimia. Olisi hyvä, että työasemat aina lukittaisiin silloin kun poistutaan työpisteeltä.

Kysymys 12: *”Jätätkö luottamuksellisia asiakirjoja työpöydällesi muiden nähtäväksi?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 11. Luottamukselliset asiakirjat.

Suuri osa vastaajista eli 87 % kiisti jättäneensä asiakirjoja lojumaan työpöydälleen mikä on hyvä asia, mutta kuitenkin 13 % myönsi jättäneensä niitä työpöydälleen. Olisi hyvä, ettei kukaan jättäisi luottamuksellisia asiakirjoja muiden nähtäville.

Kysymys 13: *”Onko kirjastossa mahdollista säilyttää luottamuksellisia tietoja turvallisesti esim. lukon takana?”*

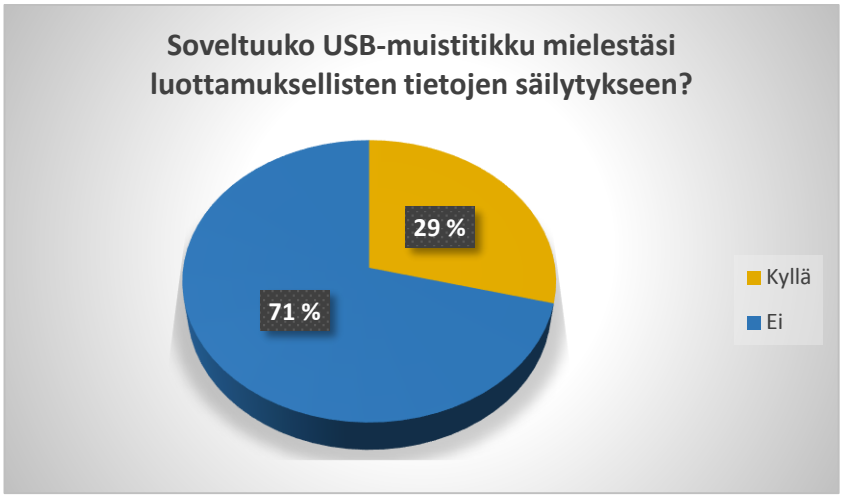
Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 12. Luottamuksellisten tietojen säilytys lukon takana.

Suurin osa vastaajista eli 80 % ovat tietoisia, että kirjastossa on mahdollisuus tehdä näin, mutta muiden vastaajien mielestä se ei ole mahdollista. Tulisi miettiä miten kaikille voitaisiin luoda mahdollisuus säilyttää luottamukselliset tiedot lukkojen takana.

Kysymys 14: *”Soveltuuko USB-muistitikku mielestäsi luottamuksellisten tietojen säilytykseen?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.



Kuva 13. Luottamuksellisten tietojen säilytys muistitikulla.

Enemmistö vastaajista eli 71 % ei pitänyt muistitikkua soveltuvana luottamuksellisten tietojen säilytykseen, kun taas 29 % mielestä muistitikku soveltui tällaiseen tarkoitukseen. Pitäisi lisätä tietoisuutta siitä, että muistitikku ei pääasiassa sovellu luottamuksellisten tietojen säilytykseen.

Kysymys 15: *”Saako vieraasta sähköpostiosoitteesta saatuja liitteitä ja linkkejä avata mielestäsi huoletta?”*

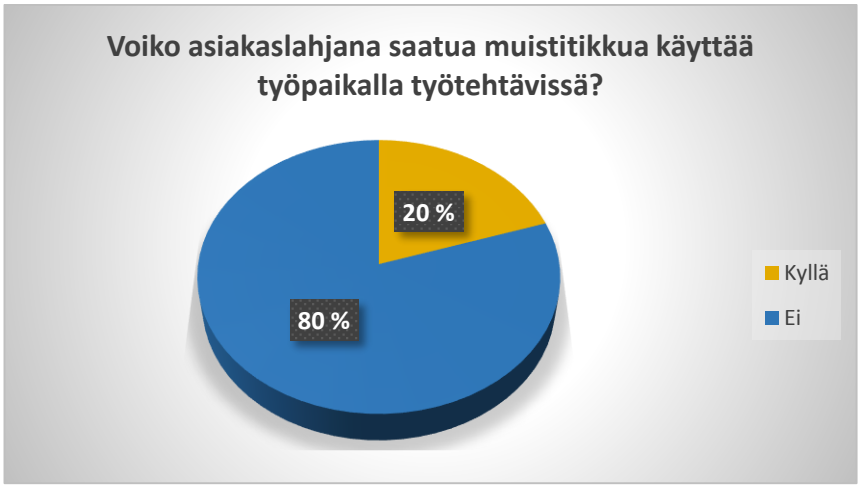
Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 14. Vieraasta sähköpostiosoitteesta saadut liitteet/linkit.

100 % vastaajista tiesi, että vieraasta sähköpostiosoitteesta saatuja liitteitä ja linkkejä ei saa avata. Tämä asia on onneksi kaikkien tiedossa.

Kysymys 16: *”Voiko asiakaslahjana saatua muistitikkua käyttää työpaikalla työtehtävissä?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

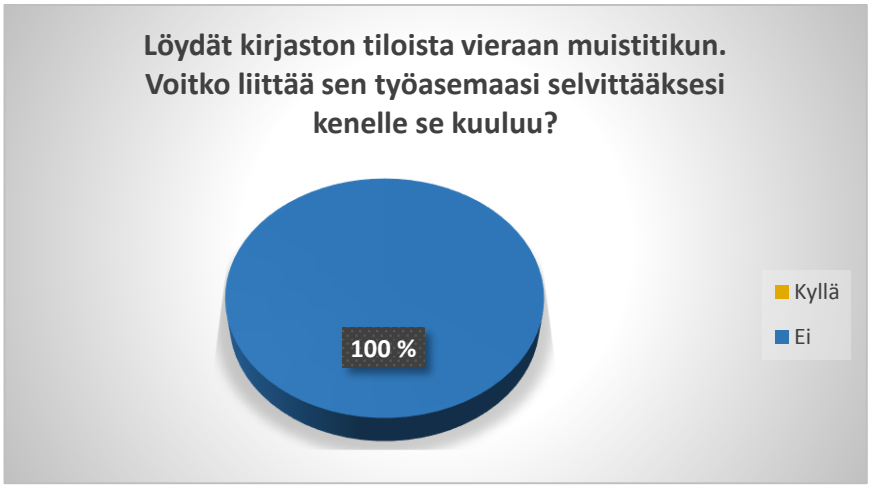


Kuva 15. Asiakaslahjana saadun muistitikun käyttö työssä.

80 % vastaajista oli sitä mieltä, että asiakaslahjana saatua muistitikkua ei ole hyvä käyttää työtehtävien hoitamisessa. Loput 20 % oli toista mieltä. Asiakaslahjana saatuun muistitikkuun voi liittyä merkittävä tietoturvariski, koska se saattaa sisältää vahingollisia haittaohjelmia.

Kysymys 17: *”Löydät kirjaston tiloista vieraan muistitikun. Voitko liittää sen työasemaasi selvittääksesi kenelle se kuuluu?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

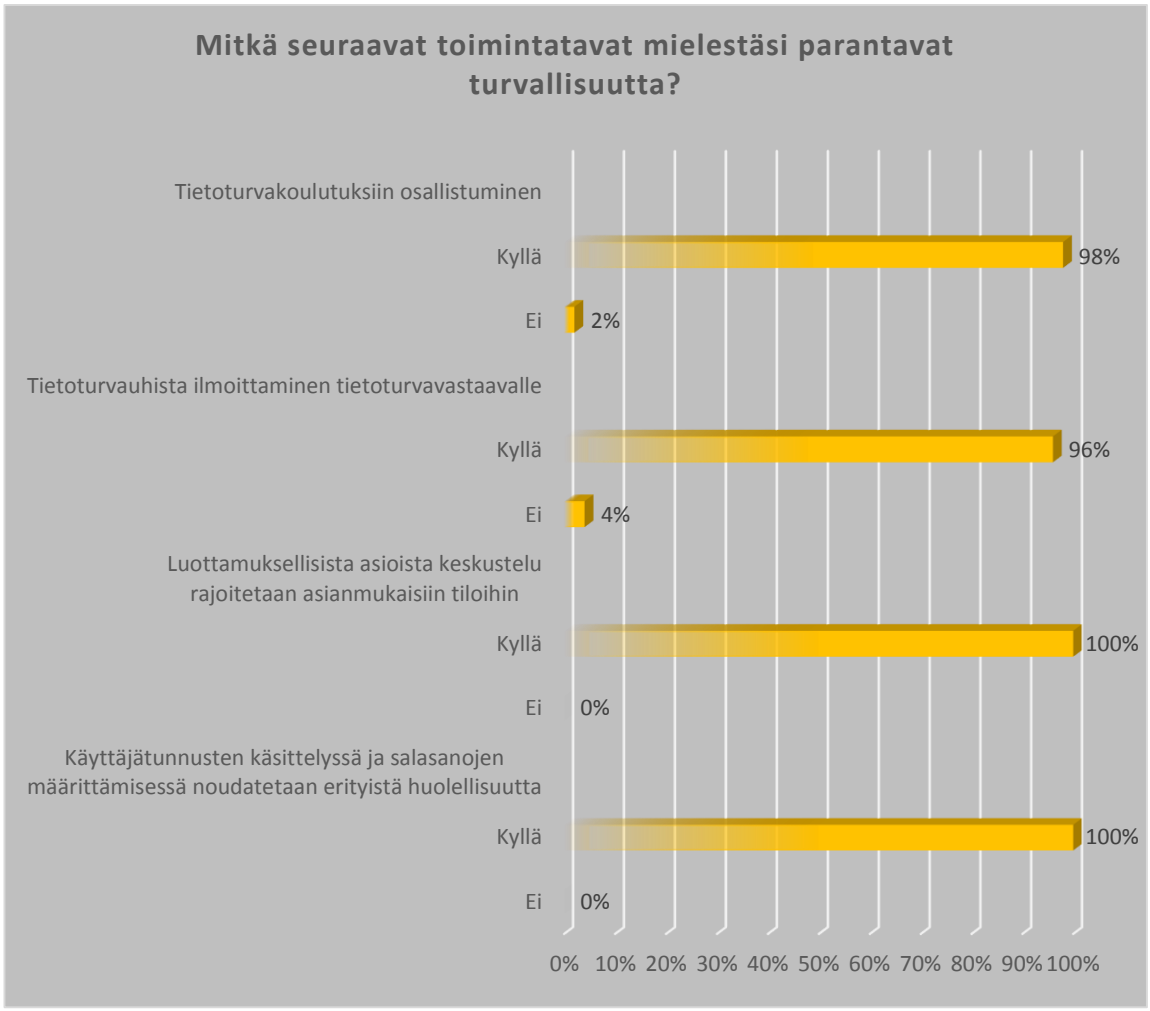


Kuva 16. Vieraan muistitikun liittäminen omaan työasemaan.

Tässä kysymyksessä 100 % vastaajista tiesi, että löydettyä muistitikkua ei saa liittää työpaikan työasemaan. On hyvä, että kaikki vastaajista ovat ymmärtäneet tämän asian.

Kysymys 18: *”Mitkä seuraavat toimintatavat mielestäsi parantavat turvallisuutta?”*

Vastausvaihtoehtoina olivat: ”Tietoturvakoulutuksiin osallistuminen”, ”Tietoturvauhista ilmoittaminen tietoturvavastaavalle”, ”Luottamuksellisista asioista keskustelu rajoitetaan asianmukaisiin tiloihin” ja ”Käyttäjätunnusten käsittelyssä ja salasanojen määrittämisessä noudatetaan erityistä huolellisuutta”.

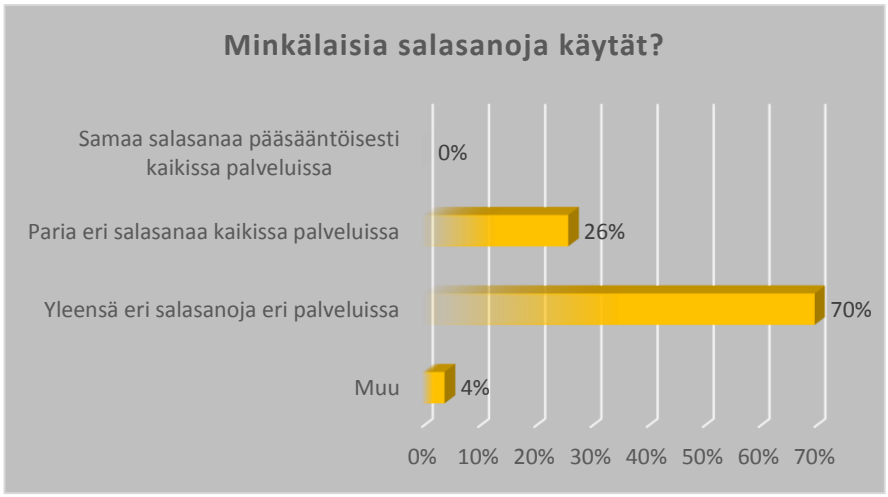


Kuva 17. Turvallisuutta parantavat toimintatavat.

Tässä kysymyksessä vastaajat pitivät kaikkia vastausvaihtoehtoja lähes yhtä tärkeinä asioina. On hienoa, että on ymmärretty hyvin mitkä asiat auttavat tietoturvallisuuden ylläpitämisessä ja parantamisessa.

Kysymys 19: *”Minkälaisia salasanoja käytät?”*

Vastausvaihtoehtoina olivat: ”Samaa salasanaa pääsääntöisesti kaikissa palveluissa”, ”Paria eri salasanaa kaikissa palveluissa”, ”Yleensä eri salasanoja eri palveluissa” vai ”Muu”.



Kuva 18. Käytetyt salasanat.

Suurin osa vastaajista eli 70 % käyttää eri salasanoja eri palveluissa ja 26 % käyttää paria eri salasanaa kaikissa palveluissa. Muutama käyttää vaihtelevasti samoja ja eri salasanojen variantteja eri palveluissa. Suositeltavaa olisi, että koskaan ei käytettäisi samaa salasanaa kuin aikaisemmin vaan muutettaisiin salasanaa ainakin joiltakin osin tai keksittäisiin kokonaan uusi salasana.

Kysymys 20: *”Säilytätkö käyttäjätunnuksiasi ja salasanojasi paperilapulla työaseman läheisyydessä?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 19. Käyttäjätunnuksien/salasanojen säilytys.

Suurin osa vastaajista eli 96 % vastasi, ettei säilytä käyttäjätunnusta ja salasanaa paperilapulla työpisteen läheisyydessä, mutta 4 % kertoi tehneensä niin. Onneksi suurin osa vastaajista tiedostaa sen, että käyttäjätunnusta ja salasanaa ei saa säilyttää paperilapulla työaseman läheisyydessä.

Kysymys 21: *”Käytätkö samoja käyttäjätunnuksia ja salasanoja sekä kirjaston työsovelluksissa että vapaa-ajalla Internetin eri palveluissa?”*

Vastausvaihtoehtoina olivat: ”Kyllä” ja ”Ei”.

Kuva 20. Samojen käyttäjätunnuksien/salasanojen käyttö.

Tähän kysymykseen vastanneista 89 % vastasi, ettei käytä samoja salasanoja ja käyttäjätunnuksia sekä kirjaston työsovelluksissa että vapaa-ajalla Internetin eri palveluissa. 11 % kertoi tehneensä niin. On erittäin suositeltavaa, ettei käytettäisi samoja tunnuksia ja salasanoja sekä kirjaston työsovelluksissa että vapaa-ajan nettipalveluissa.

Kysymys 22: *”Oletko tietoinen seuraavista troijalaisen ominaispiirteistä?”*

Kohta 1: Troijalainen pystyy tyhjentämään koneen kiintolevyn.

Yli puolet vastaajista eli 56 % vastasi ”Kyllä” ja loput 44 % eivät olleet asiasta tietoisia.

Kohta 2: Troijalainen voi kerätä salasanatietoja koneesta.

Lähes kaikki vastanneista eli 80 % tiesivät tämän asian ja 20 % ei tiennyt.

Kohta 3: Troijalainen voi tuoda mukanaan toimintoja jotka aktivoituessaan määrättynä päivänä voivat aiheuttaa suurta tuhoa.

Tämä väittämä oli lähes kaikille eli 91 %:lle tuttu. Vain 9 % ei tuntenut tätä asiaa. Tästä voidaan päätellä, että vastaajat tunsivat troijalaisiin liittyvät asiat kohtalaisesti.

Kysymys 23: *”Oletko tietoinen seuraavista matojen ominaispiirteistä?”*

Kohta 1: Madot hakevat tartuttamastaan järjestelmästä sähköpostiosoitteita ja lähettävät itsensä kaikkiin näihin osoitteisiin.

Suurimmalle osalle vastaajista eli 91 %:lle tämä oli tuttu asia ja vain 9 % vastaajista ei tiennyt tätä.

Kohta 2: Sähköpostimadot tulevat useimmiten liitetiedostojen mukana, mutta joskus niitä on myös suoraan viesteissä.

Tämä asia oli tuttu 80 %:lle vastaajista, mutta 20 % ei ollut perillä tästä asiasta.

Kohta 3: Tietyt sähköpostimadot aktivoituvat pelkällä hiiren kosketuksella ilman että liitetiedostoa lainkaan avataan.

Yli puolella vastaajista eli 67 %:lla tämä asia ei ollut tiedossa. Sentään 33 % tunsi tämän asian. Vastaajat tunsivat matojen ominaispiirteet tyydyttävästi.

Kysymys 24: *”Oletko tietoinen seuraavista tietojenkalastelun ominaispiirteistä?”*

Kohta 1: Pääosa kalasteluviesteistä tulee kansainvälisten pankkien nimissä. Tällöin jollet ole asiakkaana kyseisessä pankissa, niin voit poistaa viestin.

Lähes kaikki vastaajista eli 89 % tiesi tämän asian jo. 11 %:lle vastaajille tämä ei ollut tiedossa.

Kohta 2: Kalastelu-viestit on kirjoitettu useimmiten huonolla suomenkielellä.

Tämänkin asian lähes kaikki vastaajista eli 93 % tunsivat. Vain 7 % ei tiennyt tätä asiaa.

Kohta 3: Oikeassa verkkosivustossa kiinni olevan lukon symboli on sijoitettu aina selaimen osoiteriville.

Suurimmalle osalle vastaajista eli 71 %:lle tämä oli tuttu asia. 29 % vastaajista ei tiennyt tätä asiaa.

Kohta 4: Sähköpostiviestin linkistä ei kannata mennä verkkopankkiin tai muuhun sähköiseen asiointipalveluun.

Tämänkin asian lähes kaikki vastaajista eli 82 % oli tiennyt. Lopuille 18 %:lle tämä oli uutta tietoa.

Kohta 5: On tärkeää muistaa varmistaa, että organisaation domain-nimi on https-alkuinen (salattu yhteys) ennen kuin syöttää luottamuksellisia tietoja. Näin varmistutaan siitä, että ollaan oikean organisaation sivustolla.

Tässäkin kohdassa lähes kaikki vastaajista eli 87 % sanoivat olevansa tietoisia tästä asiasta. Vain 13 % ilmoitti, että tämä asia ei ollut heillä tiedossa. Tietojenkalastelun ominaispiirteet olivat suhteellisen hyvin vastaajien tiedossa.

Kysymys 25: *”Mitä ajatuksia Petteri Järvisen tietoturvaluento sinussa herätti?”*

Kirjaston henkilökunnan tietoturvaluento oli ollut vastaajien mielestä monipuolinen ja antoisa omien taitojen kehittämisen ja ylläpidon kannalta. Vastaajat kertoivat myös, että osa heistä sai ajatuksen opetella älykännykän paikallistamis- ja etäkomentotoiminnot. Nähtiin myös tärkeäksi kehittää oma systeemi helpottamaan vaikeasti arvattavien salasanojen muistamista. Kuitenkin aika moni kertoi, että ei päässyt valitettavasti osallistumaan luennolle. Henkilökunta toivoisi, että jatkossa kaikilla halukkailla olisi mahdollisuus osallistua tämän tyyppisille luennoille.

Kysymys 26: *”Vapaa palaute”*

Henkilökunnan mielestä on tärkeää muistuttaa kaikkia työntekijöitä arjen tietoturva-asioista. Osa vastaajista kokee turhauttavana sen, että oman työpostin suojaukseen ei voi itse paljonkaan vaikuttaa, koska asiantuntijoiden mukaan sähköpostia ei voi koko kaupungin tasolla paremmin suojata.

5.2 Haastattelut

Henkilökohtaisiin haastatteluihin osallistui 9 henkilöä. Haastatteluun valittiin henkilöitä, joiden työtehtäviin tietoturva-asiat olennaisesti liittyvät. Haastattelukysymykset olivat osittain samanlaiset kuin Webropol-kyselyssä, mutta niitä oli vähemmän ja ne oli muotoiltu siten, että niihin saataisiin monipuolisia vastauksia. Kysymykset jaettiin haastateltaville hyvissä ajoin etukäteen siksi, että heillä oli mahdollisuus miettiä omia vastauksiaan rauhassa.

Haastattelujen aikataulu suunniteltiin siten, että yhdelle haastattelulle varattiin aikaa puoli tuntia. Haastattelukysymyksillä pyrittiin selvittämään haastateltujen mielipide siitä, minkälainen on tietoturvan taso Turun kaupunginkirjastossa. Lisäksi tavoitteena oli saada heidän parannusehdotuksiaan kirjaston tietoturvaan liittyen.

Kysymys 1: *”Minkälaisia mielikuvia tulee mieleesi sanasta tietoturva?”*

Tietoturva tuo vastaajien mieleen seuraavat asiat: palomuuri, Internet, WLAN, salasanat, tietosuoja, virustorjunta, mobiililaitteet, asiakasrekisteri. Edelleen tietoturva käsitetään lähinnä teknisenä asiana. Vastaajien mielestä tietoturvan tärkeyttä ei välttämättä ymmärretä riittävästi.

Kysymys 2: *”Kuinka tärkeänä pidät tietoturvaa työyhteisössäsi?”*

Vastaajat pitävät tietoturvaa erittäin tärkeänä. He tuntuvat olevan huolissaan erityisesti asiakasrekisteriin kerättyjen tietojen joutumisesta ulkopuolisten käsiin. Rekisteri saattaa sisältää mm. yrityssalaisuuksia ja muita luottamuksellisia asiakkaiden tietoja.

Kysymys 3: *”Minkälainen on mielestäsi kirjaston tietoturvataso?”*

Vastaajien mielipide kirjaston tietoturvatasosta vaihtelee melkoisesti. Toisaalta ollaan sitä mieltä, että asia on hyvin hoidettu. Osa taas on sitä mieltä, että tietoturvan taso on jopa heikko.

Päällimmäisinä asioina tietoturvatasosta puhuttaessa nousi esiin yhteistunnusten käyttö (lokitietoja ei kerätä), koneiden lukitsemisen unohtuminen, salasanojen säännönmukainen vaihtaminen ja asianmukainen säilytys sekä asiakaskoneilla unohtunut uloskirjautuminen. Vastaajien mielestä Windows-järjestelmä ei ole kaikkein paras suojauksen suhteen ja käyttöjärjestelmiä pitäisi päivittää useammin.

Kuitenkin todettiin, että tietoturvan taso on selvästi parantunut parin viime vuoden aikana. Ollaan tyytyväisiä siihen, että joka toimialalla on omat mikrotukihenkilöt ja kaupungilla keskitetty it-tuki.

Kysymys 4: *”Miten kirjastossa voitaisiin mielestäsi parantaa tietoturvaa?”*

Vastaajien mielestä pitäisi lisätä koulutusta ja tiedotusta henkilökunnalle ja myös asiakkaille tietoturvan suhteen. Esim. asiakaskoneista pitäisi muistaa poistaa selaimen sivuhistoria. Olisi tärkeää miettiä palvelutiskien ja myös asiakaskoneiden sijoittelua sillä tavoin, että tietojen urkkiminen ei olisi helppoa.

Kaikenlaisten teknisten toimintojen pitäminen ajan tasalla koettiin tärkeäksi, kuten virustorjunta, käyttöjärjestelmät ja selaimet. Lisäksi on hyvä päivittää tietojärjestelmä- ja rekisteriselosteet.

Muistettaisiin lukita työasemat ja luovuttaisiin muistitikkujen käytöstä siirtyen käyttämään mieluimmin pilvipalveluita. Olisi hyvä muistaa vaihtaa salasanat muutaman kuukauden välein eikä tehdä niistä liian yksinkertaisia. Oltiin myös sitä mieltä, että asiakasrekisterin ei tarvitse olla kaikille avoin.

Kysymys 5: *”Minkälainen työympäristö kirjasto mielestäsi on tietoturvan näkökulmasta?”*

Tiedostetaan, että riskejä on paljon: koneiden lukitseminen, muistitikkujen käyttö, ovien hälyporttien ajoittainen toimimattomuus sekä käyttäjätunnusten ja salasanojen säilytys. Ollaan sitä mieltä, että asioita on osattu ottaa huomioon ja parannuksiakin on pyritty tekemään. Esimerkiksi Servicedesk-tukeen on oltu tyytyväisiä.

Vastaajat ovat huolissaan siitä, että kirjastossa on suuri henkilökunnan vaihtuvuus. Tilapäisillä työntekijöillä ei välttämättä ole niin hyvin tiedossa tietoturvaa koskevat säännöt. Joskus toimipisteet saattavat olla tyhjinä mikä aiheuttaa riskejä. Todettiin myös, että tietoturvaennakointi on puutteellista ja WLAN voisi toimia paremmin.

Kysymys 6: *”Minkälaiset tietoturvariskit voisivat mielestäsi realisoitua kirjastossa?”*

Vastaajat toivat esiin tietoturvariskeinä mm. virukset, tietomurrot, ilkivallan teko, esimerkiksi kotisivujen sotkeminen, haittaohjelmat, kalasteluviestit, huijauslinkit sekä käyttäjätunnusten ja salasanojen joutuminen vääriin käsiin. Osa oli huolissaan ns. 15-minuutin asiakaskoneista. Niihin ei vaadita kirjautumista joten käyttäjiä ei voida jäljittää.

Lisäksi keskustelu luottamuksellisista asioista käytävillä aiheuttaa jonkinlaisen riskin. Asiakaspalvelutiskeissä saatetaan unohtaa kone auki, jolloin ulkopuolisilla on pääsy asiakastietoihin. Yhteistunnusten käyttö aiheuttaa omat riskinsä. Lainausautomaateilla olevien asiakkaiden tunnuksia voidaan urkkia ja asiakaskoneilla unohdetaan tyhjentää sivuhistoria mistä aiheutuu tietoturvariski.

Kysymys 7: *”Mitä ajatuksia Petteri Järvisen tietoturvaluento sinussa herätti?”*

Vastaajien mielestä Järvinen osasi herätellä ja korostaa tietoturvan merkitystä. Luento oli mielenkiintoinen ja hyödyllisiä asioita tuli esiin. Hän opetti hyviä muistisääntöjä salasanoista ja kehotti tarkistamaan linkit ennen niiden avaamista. Hänen mukaansa muistitikut voivat sisältää haittaohjelmia ja hän suositteli käyttämään mieluimmin pilvipalveluita tietojen tallentamiseen.

Järvisen mukaan on tärkeää muistaa maalaisjärjen käyttö. Hän kertoi, että älypuhelimissa ja tableteissa ei esiinny niin paljon viruksia kuin esim. tietokoneissa. Hän selitti myös, että virustorjunta ei ehkäise virusten tuloa vaan kertoo vain että koneessa on virus. WLAN-yhteyttä käytettäessä on hyvä ottaa huomioon tietoturva-asiat.

5.3 Suositukset

Kyselystä ja haastatteluista kävi ilmi, että henkilöstön tietoturvaosaaminen sekä kirjaston tietoturvataso ovat vastaajien mielestä tyydyttävällä tasolla. Lisäksi voidaan päätellä, että henkilöstö ymmärtää hyvin tietoturvan merkityksen työssään. On oivallettu erinomaisesti se, mitkä asiat auttavat tietoturvallisuuden ylläpitämisessä ja parantamisessa. Myös vieraiden sähköpostilinkkien ja liitteiden avaamisen vaarat ovat hyvin tiedossa.

Henkilökunnalle ja asiakkaille halutaan lisää koulutusta tietoturvasta, mutta sopivat kanavat tiedonkulkuun puuttuvat. Vastaajat kokevat tietoturvaluennot tarpeelliseksi ja toivovat, että kaikki halukkaat voisivat niihin osallistua.

Asiakasrekisterin käytön jonkinasteista rajoittamista kannattaa tulevaisuudessa harkita. Henkilökuntaa tulisi muistuttaa hyvistä salasanakäytännöistä ja salasanoja pitäisi vaihtaa useammin. Verkkokirjaston toimintoja tulisi kehittää. Lisäksi pitäisi tiedottaa henkilökunnalle kuka vastaa kirjaston tietoturva-asioista.

Kaikkien työntekijöiden tulisi tutustua kirjaston tietoturvaohjeisiin ja hahmottaa omat tietoturvavastuunsa. Edelleen pitäisi kiinnittää huomiota seuraaviin asioihin:

työasemien lukitseminen ja aikakatkaisu, luottamuksellisten asiakirjojen käsittely ja säilytys sekä muistitikkujen riskit.

Palvelutiskien ja asiakaskoneiden sijoittelu pitäisi miettiä niin, että tietojen urkinta ei olisi helppoa. Tietojärjestelmä- ja rekisteriselosteet tulisi päivittää. Harkitaan kokonaan luopumista muistitikkujen käytöstä ja siirrytään pilvipalveluihin. Huolehditaan siitä, että myös tilapäiset työntekijät tutustuvat kirjaston tietoturvaohjeisiin. Pohditaan miten voitaisiin pienentää yhteistunnusten ja ns. 15-minuutin asiakaskoneiden käyttöön liittyvää tietoturvariskiä.

6 YHTEENVETO

Aineistoa työn teoriaosaan oli suhteellisen helppo löytää. Mielestäni olen onnistunut rajaamaan melko hyvin opinnäytetyössä olevan teorian sopivaksi työn empiriaosaan.

Vastauksia kyselyyn olisi saatu enemmän, jos vastausaika olisi ollut pitempi. Silloin olisi ollut mahdollista lähettää vastaajille sähköpostitse muistutusviesti kyselystä. Jonkinlaisen arvonnan järjestäminen vastaajien kesken olisi lisännyt vastausten määrää.

Kysely toteutettiin käyttäen Webropol-kysely- ja analysointisovellusta. Pääsin tutustumaan tämän sovelluksen käyttöön jo työharjoitteluni aikana Turun kaupunginkirjastossa, joten sen käyttäminen oli helppoa. Sovellus tuotti selkeät tutkimustulokset, joiden analysointi oli vaivatonta.

Haastateltavat saivat rauhassa tutustua esitettäviin kysymyksiin jo etukäteen, mikä varmasti auttoi niihin vastaamisessa. Vastaukset olivat erittäin monipuolisia, tosin hyvin samanlaisia ajatuksia mahdollisista tietoturvauhista nousi esiin.

Tulevaisuudessa voitaisiin tehdä opinnäytetyö, jossa suunnitellaan toimenpiteet, niiden toteutus ja seuranta tässä tutkimuksessa ilmenneisiin kehitystarpeisiin kirjaston tietoturvan suhteen.

LÄHTEET

Andreasson, A. & Koivisto, J. 2013. Tietoturvaa toteuttamassa. Helsinki: Tietosanoma.

Imperva 2014. Top ten database threats. Viitattu: 25.11.2015 http://www.imperva.com/docs/wp_topten_database_threats.pdf

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

Manninen, O. 2015. Vaara väijyy verkossa. OP Taloudessa 2/2015, 21.

Rousku, K. 2014. Kyberturvaopas Tietoturvaa kotona ja työpaikalla. Helsinki: Talentum.

Turun kaupunki 2008. Tietoturvallisuuden organisoiminen. Viitattu: 4.6.2015 http://ah.turku.fi/kh/2008/0414010x/1852876.htm.

Turun kaupunki 2011. Tietoturvallisuuden hallintapolitiikka. Viitattu: 4.6.2015 http://ah.turku.fi/kh/2011/0523014x/2528257.htm.

What is techtarget 2014. Confidentiality, integrity and availability. Viitattu: 25.11.2015 http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Kyselyn ja haastattelujen kysymykset

Kysely

1) *Minkälainen on mielestäsi tämänhetkinen tietoturvaosaamisesi?*

□ Erinomainen

□ Hyvä

□ Keskinkertainen

□ Vähäinen

□ Heikko

2) *Kuinka tärkeänä pidät tietoturvaa työssäsi?*

□ Hyvin tärkeänä

□ Tärkeänä

□ En osaa sanoa

□ Vähemmän tärkeänä

□ Ei ollenkaan tärkeänä

3) *Onko sinulla ideoita tietoturvallisuuden parantamiseksi kirjastossa?*

4) Mitä sana ”tietoturva” tuo sinulle mieleen?

□ Vaikeita tietokoneasioita

□ ”Ei kosketa minua”

□ Tietomurrot ja kyber-rikokset

□ Tietokoneen suojaus (virustorjuntaohjelma, palomuuri ym.)

□ Asiakirjojen luokittelu (salassa pidettävät jne.)

□ Muu:

5) Onko kirjaston tietoturvataso mielestäsi tarpeeksi korkea?

□ Kyllä

□ Ei

6) Tiedätkö kuka vastaa kirjaston tietoturva-asioista?

□ Kyllä

□ Ei

7) *Onko kirjastossa järjestetty aikaisemmin koulutusta tietoturva-asioista?*

□ Kyllä

□ Ei

8) *Mitkä seuraavista mahdollisista riskeistä voisivat toteutuessaan aiheuttaa merkittävää vahinkoa kirjastossa?*
Useamman vaihtoehdon valitseminen on myös mahdollista.

□ Tietojen menetys

□ Tietomurto

□ Työntekijöiden tietovuodot

□ Fyysiset vahinkotapaukset (vesivahinko, tulipalo, murto yms.)

□ Tietovälineiden häviäminen

□ Muu:

9) *Oletko tutustunut kirjaston tietoturvaohjeisiin?*

□ Kyllä

□ Ei

10) Tiedostatko mitkä ovat omat tietoturvavastuusi?

□ Kyllä

□ Ei

11) Poistuessasi työpisteeltäsi muistatko lukita työasemasi?

□ Kyllä

□ Ei

12) Jätätkö luottamuksellisia asiakirjoja työpöydällesi muiden nähtäväksi?

□ Kyllä

□ Ei

13) Onko kirjastossa mahdollista säilyttää luottamuksellisia tietoja turvallisesti esim. lukon takana?

□ Kyllä

□ Ei

14) Soveltuuko USB-muistitikku mielestäsi luottamuksellisten tietojen säilytykseen?

□ Kyllä

□ Ei

15) Saako vieraasta sähköpostiosoitteesta saatuja liitteitä ja linkkejä avata mielestäsi huoletta?

□ Kyllä

□ Ei

16) Voiko asiakaslahjana saatua muistitikkua käyttää työpaikalla työtehtävissä?

□ Kyllä

□ Ei

17) Löydät kirjaston tiloista vieraan muistitikun. Voitko liittää sen työasemaasi selvittääksesi kenelle se kuuluu?

□ Kyllä

□ Ei

18)Mitkä seuraavat toimintatavat mielestäsi parantavat turvallisuutta?

Tietoturvakoulutuksiin osallistuminen	□ Kyllä □ Ei
Tietoturvauhista ilmoittaminen tietoturvavastaavalle	□ Kyllä □ Ei
Luottamuksellisista asioista keskustelu rajoitetaan asianmukaisiin tiloihin	□ Kyllä □ Ei
Käyttäjätunnusten käsittelyssä ja salasanojen määrittämisessä noudatetaan erityistä huolellisuutta	□ Kyllä □ Ei

19)Minkälaisia salasanoja käytät?

□ Samaa salasanaa pääsääntöisesti kaikissa palveluissa

□ Paria eri salasanaa kaikissa palveluissa

□ Yleensä eri salasanoja eri palveluissa

□ Muu:

20) Säilytätkö käyttäjätunnuksiasi ja salasanojasi paperilapulla työaseman läheisyydessä?

□ Kyllä

□ Ei

21) Käytätkö samoja käyttäjätunnuksia ja salasanoja sekä kirjaston työsovelluksissa että vapaa-ajalla Internetin eri palveluissa?

□ Kyllä

□ Ei

22) Oletko tietoinen seuraavista troijalaisen ominaispiireistä?

Troijalainen pystyy tyhjentämään koneen kiintolevyn. □ Kyllä

□ Ei

Troijalainen voi kerätä salasanatietoja koneesta. □ Kyllä

□ Ei

Troijalainen voi tuoda mukanaan toimintoja jotka aktivoituessaan määrättynä päivänä voivat aiheuttaa suurta tuhoa. □ Kyllä

□ Ei

23)Oletko tietoinen seuraavista matojen ominaispiirteistä?

Madot hakevat tartuttamastaan järjestelmästä sähköpostiosoitteita ja lähettävät itsensä kaikkiin näihin osoitteisiin.

□ Kyllä

□ Ei

Sähköpostimadot tulevat useimmiten liitetiedostojen mukana, mutta joskus niitä on myös suoraan viesteissä.

□ Kyllä

□ Ei

Tietyt sähköpostimadot aktivoituvat pelkällä hiiren kosketuksella ilman että liitetiedostoa lainkaan avataan.

□ Kyllä

□ Ei

24)Oletko tietoinen seuraavista tietojenkalastelun ominaispiirteistä?

Pääosa kalasteluviesteistä tulee kansainvälisten pankkien nimissä. Tällöin jollet ole asiakkaana kyseisessä pankissa, niin voit poistaa viestin.

□ Kyllä

□ Ei

Kalastelu-viestit on kirjoitettu useimmiten huonolla suomenkielellä.

□ Kyllä

□ Ei

Oikeassa verkkosivustossa kiinni olevan lukon symboli on sijoitettu aina selaimen osoiteriville.

□ Kyllä

□ Ei

Sähköpostiviestin linkistä ei kannata mennä verkkopankkiin tai muuhun sähköiseen asiointipalveluun.

□ Kyllä

□ Ei

On tärkeää muistaa varmistaa, että organisaation domain-nimi on https-alkuinen (salattu yhteys) ennen kuin syöttää luottamuksellisia tietoja. Näin varmistutaan siitä, että ollaan oikean organisaation sivustolla.

□ Kyllä

□ Ei

25) Mitä ajatuksia Petteri Järvisen tietoturvaluento sinussa herätti?

26) Vapaa palaute

Haastattelut

1) *Minkälaisia mielikuvia tulee mieleesi sanasta tietoturva?*

2) *Kuinka tärkeänä pidät tietoturvaa työyhteisössäsi?*

3) *Minkälainen on mielestäsi kirjaston tietoturvataso?*

4) *Miten kirjastossa voitaisiin mielestäsi parantaa tietoturvaa?*

5) *Minkälainen työympäristö kirjasto mielestäsi on tietoturvan näkökulmasta?*

6) *Minkälaiset tietoturvariskit voisivat mielestäsi realisoitua kirjastossa?*

7) *Mitä ajatuksia Petteri Järvisen tietoturvaluento sinussa herätti?*