KYMENLAAKSON AMMATTIKORKEAKOULU
Hoitotyön koulutusohjelma sairaanhoitaja

Antti Tiittanen

TERVEYSALAN OPISKELIJOIDEN KÄSITYKSET TIETOTURVASTA ENSIMMÄISEN OPISKELUVUODEN JÄLKEEN

Opinnäytetyö 2013

TIIVISTELMÄ

KYMENLAAKSON AMMATTIKORKEAKOULU
Hoitotyön koulutusohjelma

TIITTANEN, ANTTI

TERVEYSALAN OPISKELIJOIDEN KÄSITYKSET TIETOTURVASTA ENSIMMÄISEN OPISKELUVUODEN JÄLKEEN

Opinnäytetyö 53 sivua + 15 liitesivua
Työn ohjaaja Lehtori Satu Anttonen
Toimeksiantaja Kymenlaakson ammattikorkeakoulu
Tammikuu 2013
Avainsanat Tietoturva, kyberturvallisuus, pääsynvalvonta, tietosuoja

Tutkimuksen tarkoituksena oli kartoittaa terveysalan opiskelijoiden tietoutta perustason tietoturvasta. Opinnäytetyön aihe syntyi yhteistyössä Kymenlaakson ammattikorkeakoulun kanssa. Työn tarkoituksena oli tietoturvateorian ja kyselyn kanssa etsiä vastauksia siihen, miten terveysalan opiskelijat tiedostavat ja toteuttavat perustason tietoturvaa opiskeluympäristössään ja kotonaan.

Tutkimus on kvantitatiivinen, ja aineisto koottiin strukturoidulla verkkokyselylomakkeella, joka toteutettiin ZEF@ Editori -työkalulla, johon luotiin kysymyspohjat. Kyselylomake saatekirjeineen lähetettiin 164:lle Kymenlaakson ammattikorkeakoulun terveysalan opiskelijalle. Kyselyyn vastasi hyväksytysti (N=59). Tutkimuksen vastausprosentiksi jäi 36 %. Tutkimusaineiston analysointiin käytettiin Excel 2010 -ohjelmaa, jonka avulla tehtiin myös kyselyn graafiset taulukoinnit.

Terveysalan opiskelijoiden perustason tietoturvaosaaminen oli pääsääntöisesti hyvää. Heidän käsityksensä tietoturvaosaamisestaan oli suurempi, kuin mitä kyselyn vastausten perusteella voi olettaa. Tutkimuksesta käy ilmi, että alle puolet vastanneista on varautunut etukäteen varmuuskopioin tietokoneen vioittumiseen. Oppilaitoksen tekemät Käyttäjän tietoturvaohjeet olivat vastanneista 38 %:n tiedossa ja he olivat niihin tutustuneet.

ABSTRACT

KYMENLAAKSON AMMATTIKORKEAKOULU
University of Applied Sciences
Nursing and Health Care

ANTTI TIITTANEN

Health care students' impressions conceptions of information security after the first year of their studies

Bachelor's Thesis
53 pages + 15 pages of appendices
Supervisor
Satu Anttonen, senior lecturer
Commissioned by
Kymenlaakso University of Applied Sciences
January 2013
Keywords
information security, data protection, access control, cybersecurity

The aim of this thesis was to survey health care students' knowledge on basic level information security. The subject of this thesis was developed together with Kymenlaakso University of Applied Sciences. The objective was to collect theoretical knowledge and to execute a survey to find out how health care students were aware of basic level information security and how they put it into practice in their studying environment and at home.

This study was a quantitative one and the material was collected with structured internet questionnaires. It was carried out with ZEF@ Editori –tool where the templates for the questions were created. The questionnaires and the covering letters were sent to 164 health care students in Kymenlaakso University of Applied Sciences. 59 persons filled in the questionnaires acceptably (n=59). The response rate was 39 percent. The research data was analysed and the graphical tabulations were created using Excel 2010 –programme.

The data security know-how of the health care students was mainly good. They seemed to be of the opinion that their data security know-how was better than their answers implied. The study revealed that less than half of the respondents had prepared themselves for computer damages by making backup copies. 38 percent of the respondents knew about and were acquainted with the information security instructions produced by the University of Applied Sciences.

SISÄLLYS

TIIVISTELMÄ

ABSTRACT

1 TAUSTA JA TARKOITUS 6

2 TIETOTURVA 7

2.1 Tieto 7
2.2 Tietoturvan tarkoitus 10
2.3 Tietoturvan perusteet 10
2.4 Tietosuoja 11

3 TIETOTURVAN UHAT JA NIIHIN VARAUTUMINEN 12

3.1 Luottamuksellisuus 12
3.2 Eheys 13
3.3 Saatavuus 17
3.4 Todennus 17
3.5 Pääsynvalvonta 18
3.6 Kiistämättömyys 19
3.7 Perustason tietoturva käytännössä 20
3.8 Terveysalan opiskelijan arkea tietoverkossa 22

4 TUTKIMUSONGELMAT 23

5 TUTKIMUKSEN TOTEUTUS 24

5.1 Kyselytutkimus 24
5.2 Kohderyhmä 25
5.3 Kyselylomake 26
5.4 Aineiston analyysi 27

6 TUTKIMUSTULOKSET 28

6.1 Taustamuuttujat 28
6.2 Opiskelijoiden tietoturvavalmiudet 29
6.3 Opiskelijoiden käsityksiä tietoturvan toteutuksesta ja sen vastuunkannosta. 37
6.4 Tietoturvaopetukseen liittyvät opiskelijoiden toiveet 40
6.5 Yhteenveto tutkimustuloksista 41

7 POHDINTA 43

7.1 Tutkimustulosten tarkastelu 43

7.2 Luotettavuus ja eettisyys 45

7.3 Tulosten hyödynnettävyys 46

LÄHTEET 49

LIITTEET

Liite 1. Sopimus opinnäytetyöstä

Liite 2. Muuttujataulukko

Liite 3. Tutkimustaulukko

Liite 4. Saatekirje

Liite 5. Kyselylomake

1 TAUSTA JA TARKOITUS

Tietoturva ei ole saanut riittävää huomiota osakseen. Huoli siitä on kuitenkin suuri koko maailmassa. Tietoturva ja sen toteutuminen on hyvin ajankohtainen ja tärkeä asia. Media on kertonut viime aikoina useista tietomurroista. Ne ovat tapahtuneet terveydenhoitoalan ulkopuolelta, mutta samanlaiset murrot ovat mahdollisia myös terveydenhoitoalalla, mikäli jokin tietoturvan osa-alue pettää.

Opinnäytetyön aihe syntyi yhteistyössä Kymenlaakson ammattikorkeakoulun kanssa. Tämän opinnäytetyön tarkoituksena on selvittää terveydenhoitoalan opiskelijoiden tietoturvavalmiuksia sekä heidän käsityksiä tietoturvan toteuttamisesta. Opiskelijat ovat saaneet koulutusohjelman mukaisen koulutuksen: tietotekniikan perusteet sekä terveydenhuollon tiedonhallinta- ja dokumentointikurssit, joiden yksi osa-alue on tietoturvan perusteet. Lisäksi kartoitettiin opiskelijoiden toiveita tietoturvaan liittyvän opetuksen sisällöstä.

Tietoturva on kansainvälinen ongelma ja se huolestuttaa suurvaltoja. Esimerkiksi FBI, Yhdysvaltain keskusrikospoliisi (Federal Bureau of Investigation) kertoo sivustollaan, että heillä on satsattu runsaasti kapasiteettia sekä sisäiseen turvallisuuteen että kansainväliseen turvallisuuteen. Järjestön mukaan heillä oli 30.11.2011 listoillaan 35704 työntekijää. Heistä 13864 on erikoisagentteja ja 21840 tukihenkilöitä kuten älykkyysanalyytikkoja, kielen asiantuntijoita, tietotekniikan asiantuntijoita ja muita ammattilaisia. Ryhmän vuosibudjetti vuonna 2011 oli 7,9 miljardia dollaria. Samalla kun maailmalla tekniikka tuodaan verkkoon, huolet lisääntyvät. Infrastruktuuri kuten sähkönsyöttö, vedenjakelu ja lähes kaikki muu tekniikka ovat haavoittuvaisempia ulkoisille uhkatekijöille. (FBI kotisivut 2012.)

Suomessa valtiovarainministeriö hoitaa hallituksen talous- ja finanssipolitiikan sekä valtion talousarvion valmistelun. Valtiovarainministeriö toimii myös veropolitiikan asiantuntijana. (Valtionvarainministeriö 2013a, Ministeriö.)

Muiden tehtävien lisäksi valtiovarainministeriö ohjaa tietohallinnon kehitystä sekä valtion- että kuntahallinnossa. Valtiovarainministeriö vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Se on tehnyt periaatepäätöksen valtion tietoturvallisuuden kehittämisestä. Päätöksessä ohjataan valtionhallintoa kehittämään tietoturvalli-

suutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä hallinnon kehittämistä. (Valtiovarainministeriö 2013a, Ministeriö.)

Valtionhallinnossa tietoturvallisuuden yhteisinä lähtökohtina ovat jokaisen organisaation vastuu oman toimintansa tietoturvallisuudesta, säädöksissä määritellyt tietoturvavelvoitteet, valtioneuvoston periaatepäätös valtion tietoturvallisuuden kehittämisestä sekä valtiovarainministeriön antamat VAHTI:n, eli valtionhallinnon tietoturvallisuuden johtoryhmän antamat tietoturvaohjeet ja muut linjaukset. (Valtiovarainministeriö 2013b, Tietoturvallisuus.)

Tietoturva on merkittävässä osassa nykyajan terveydenhoidossa. Kaikki potilastiedot, ovat pääasiassa nykyään sähköisessä muodossa. Menetelmä on nopea ja mahdollistaa tiedon ajanmukaisen saatavuuden. Samalla tiedon haavoittuvuuden mahdollisuus lisääntyy. Tietoturvateorian ja -käytännön toteuttamisen ymmärtäminen auttaa suojelemaan tietoa. Lainsäädäntö ohjaa Suomessa keskeisesti eri toimijoiden (myös yksityisyyden suojan) tietoturvakäytäntöjä, se määrää tietoturvavelvoitteet kaikille käyttäjäryhmille. (Järvinen 2010, 15; Valtiovarainministeriö 2013d.)

Jokainen organisaatio vastaa omasta tietoturvastaan. Se on niin vahva kuin sen heikoin lenkki, eli mitä tiedon käyttäjä itse on. Tutkimuksen tarkoitus on kartoittaa terveysalan oppilaiden tietoturvan ymmärtämystä ja tietoturvallista käyttäytymistä sen perustasolla. Opiskelijan asenteesta tietoturvaan ja tietoturvan ymmärtämisen ja toteuttamisen tasosta muodostuu laajempi kokonaisuus tietoturvasta. Ilman jatkuvaa koulutusta ja uuden tiedon omaksumista ei käyttäjä voi toteuttaa oikeaa tietoturvallista käyttäytymistä. (Valtiovarainministeriö 2013d.)

2 TIETOTURVA

2.1 Tieto

Tieto on filosofian ja tieteen peruskäsite. Antiikin ajoista tiedon määritelmä on hyvin perusteltu tosiuskomus. Tieto eroaa uskonnosta, luulosta tai arvailusta, koska se on todenperäinen ja tutkittuun tietoon pohjautuva asia. (WSOY Iso Tietosanakirja 9. 1997, 317.)

Nykyään usein samaistetaan informaatio ja tieto keskenään. Ne voidaan erottaa toisistaan siten, että informaatio on laajempi kokonaisuus käsitteenä, joka kattaa kaiken datan esimerkiksi atk-muodossa. Tieto on suppeampi käsite kattaen todellisuuden sekä olennaisuuden vaatimukset. Tietoa voidaan myös käsitellä prosessiluontoisesti. Usein tieto on yksittäinen tosiasia, josta ihminen joutuu muodostamaan kokonaisuuden omalle itsetietoisuudelleen. Tiedon määrittelyä ja kriteereitä sekä tiedon mahdollisuuksia ja rajoja koskeva keskustelu on voimakkaasti korostunut mm. nykyisen informaatioteknologian kehityksen myötä. (WSOY Iso Tietosanakirja 9. 1997, 317.)

Erilainen tiedostojen salaus ja tietoturva rinnastetaan usein toisiinsa. Käsitetään, että tietoturvan tarkoitus on pitää tiedot salassa. Tämä ei kuitenkaan pidä paikkaansa. Tietoturvan tärkeä tavoite on turvata tietojenkäsittelyn toimivuus erilaisten uhkatekijöiden varalta sekä suojata tietoja oikeudettomilta muutoksilta. Osa tietoja mahdollisesti kohtaavista uhkatekijöistä ovat teknisiä uhkia, kuten esimerkiksi palvelimen tai henkilökohtaisen tietokoneen kovalevyn rikkoutuminen. Nämä keskeyttävät palveluiden saatavuuden ja pahimmassa tapauksessa kadottavat tiedot. Suurin uhkakuva aiheutuu kuitenkin palvelun tai tiedon käyttäjän omasta toiminnasta. Mahdollisia ovat myös ulkopuoliset hyökkäykset, joissa pyritään hankkimaan luottamuksellista tietoa ilman oikeutta siihen tai vahingoittamaan tietojärjestelmän toimintaa. (Järvinen 2005, 29.)

Turvattava tieto voi olla taloudellista dataa, mittaustuloksista tai tietokoneella tuotettuja dokumentteja. Tietoturvan kohteena on tieto itse. Käsite pitää sisällään yksityisyydensuojan. Suojelemme arkielämässä sekä työelämässä ollessamme omaa yksityisyyttämme. Ei ole hyväksyttävää, että puoliso tai muut perheenjäsenet lukevat henkilökohtaisia sähköposteja luvatta tai että työnantaja saa liian varhain tietää suunnitellusta perheenlisäyksestä. Raha-asiat, seksuaalisuus, terveydentila tai ihmissuhteet kuuluvat myös oleellisesti asioihin, joita halutaan suojella ja pitää omana tietona. Pidemmälle vietynä tietoturvan päämääränä pääsemme kokonaisuuteen, jossa pyritään suojaamaan yhteiskuntamme eri toimijoiden palveluita, sovelluksia ja tietoteknisen infrastruktuurin perusedellytykset. (Järvinen 2010, 15; Valtiovarainministeriö 2013d.)

Tietoturva on 20 % tekniikkaa ja 80 % psykologiaa. Käytännön tietoturva on enimmäkseen jälkimmäistä. Teknisesti on helpompi hallita verkkoja, koneita ja järjestelmiä, mutta tiedon käyttäjän hallinta on jo monimutkaisempaa. Ihminen tekee virheitä, rikkoo annettuja ohjeita sekä sääntöjä. Myös tahallinen halu aiheuttaa vahinkoa on

mahdollista. Suurimmat tietoturvan ongelmat liittyvät yleisesti kiireeseen, huolimattomuuteen, osaamattomuuteen sekä muihin tietoteknisiin käytön ja toteutuksen laadullisiin osatekijöihin. (Järvinen 2002, 47; Valtiovarainministeriö 2013d.)

VAHTI (Valtionhallinnon tietoturvallisuuden johtoryhmä) on laatinut myös ohjeen peruskäyttäjien tietoturvan osalta. Ohje on nimeltään Henkilöstön Tieturvaohje. (Valtiovarainministeriö 2013d.) Johtoryhmältä on tämän jälkeen tullut vuosittain ohjeistuksia tietoturvan kouluttajille, sosiaalisen median käyttäjille sekä ITC-teknologia yrityksille siitä, kuinka rakentaa tietoturvallinen ympäristö. Viimeisin ohjeistus on nimeltään Teknisen ICT-ympäristön tietoturvaohje. (Valtiovarainministeriö 2013c.)

VAHTI:n tekemiä uusia ohjeistuksia on mahdollista tilata sähköpostitse uutiskirjeenä. Ilmoitukset uusista ohjeistuksista lisäävät käyttäjän ajankohtaista tietoa tietoturvasta sekä parantavat tämän tietoisuutta uusista tietoturva käytännöistä. Ohjeistus perustuu lainsäädäntöön ja normiohjeistukseen. Ohjeet on tehty julkishallinnon henkilöstölle, erinäisille palvelun tarjoajille sekä tietojärjestelmiä tai toimitiloja käyttäville henkilöille kuten opiskelijoille ja kotitietokoneen käyttäjille. (Valtiovarainministeriö 2013c.)

VAHTI:n ohjeistuksessa tietoturvajärjestelyt määritellään tarkoituksena pitää tieto, järjestelmät ja palvelut suojattuina siten, että niiden luottamuksellisuus, eheys ja käytettävyys riskeineen olisivat hallinnassa. Tämä tarkoittaa tiedon tai sen osan sekä palveluiden käytön rajoittamista vain niihin henkilöihin, jotka ovat oikeutettuja käyttöön. Näin evätään sivullisten mahdollisuus tiedon tai palvelun käsittelemiseen, muuttamiseen tai poistamiseen. Tietojen sekä järjestelmien käsittelyyn oikeutetut käyttäjät saavat oikeudet näihin asianmukaisesti vain työtehtävänsä mukaan. Tällä pyritään pitämään tieto, järjestelmät sekä palvelut luotettavina, oikeina sekä ajantasaisina. Tarkoituksena on suojella näitä ominaisuuksia paljastumiselta, muuttumiselta tai tuhoutumiselta asiattoman toiminnan, haittaohjelmien, laitteisto- ja ohjelmistovikojen tai muiden vahinkojen ja tapahtumien seurauksena. Tietojen, järjestelmien ja palveluiden on myös oltava saatavilla sekä järjestelmien on pysyttävä toiminnassa aina tarvittaessa. Sähköisen asioinnin lisäännyttyä on korostunut vaatimus tunnistaa luotettavasti asioinnin osapuolet sekä tarvittaessa jälkikäteen todistaa asioinnin tapahtumat sekä sen sisältö luotettavasti. (Valtiovarainministeriö 2013d.)

2.2 Tietoturvan tarkoitus

Edellä mainituilla toiminnoilla pyritään turvaamaan yksilön, yhteisön ja yhteiskunnan etuja. Tietoturvallisuudella turvataan yhteiskuntamme toimintoja, palveluita, sovelluksia ja tietoteknistä infrastruktuuria. Verkottuneessa yhteiskunnassa ollaan yhä enemmän riippuvaisia tietojen käsittelystä ja siirrosta. Sen turvaamisesta eivät enää ole yksinomaan vastuussa yksittäiset organisaatiot, vaan kaikki niissä työskentelevät osapuolet. Puutteellinen tietoturvallisuus vaarantaa valtion, kansalaisen, yhteisöjen ja asiakkaiden etuja aiheuttaen lisätyötä sekä kustannuksia. Tietoturvallisuuden suurimpiin ongelmiin liittyy yleisesti kiire, huolimattomuus, osaamattomuus sekä tietojärjestelmien toteutuksen ja käytön laadulliset tekijät. (Valtiovarainministeriö 2013d.)

Tietoturvan toteuttaminen alkaa jo käyttäjän kotikoneesta, jolla on mahdollisuus liittyä sähköisesti muihin järjestelmiin sekä palveluihin maailmanlaajuisen verkon eli Internetin avustuksella. Tietoturvasta huolehtimisen vastuu on käyttäjällä itsellään henkilökohtaisen tietokoneen osalta. Suojaamaton kotikone tai käyttäjän varomaton toiminta on vaaraksi yhteiskuntamme toiminnoille, palveluille, sovelluksille ja tietotekniselle infrastruktuurille. (Valtiovarainministeriö 2013d.)

2.3 Tietoturvan perusteet

Tietoturvan perusidea on taata tietojenkäsittelylle **luottamuksellisuus** (confidentiality), **tiedostojen eheys** (integrity), **saatavuus** (availability), **todennus** (authentication) **pääsynvalvonta** (access control) sekä **kiistämättömyys** (non-repuditation). Tietoturvajärjestelyjen tarkoituksena on, että tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen liittyvät riskit ovat hallinnassa. (Järvinen 2002, 21 - 27; Valtiovarainministeriö 2013d.)

Tietoturvakäytäntöjen luomisella on tärkeä merkitys myös tietoverkkojen suojaamisessa ja turvaamisessa. Tietoturvakäytäntö määrittelee, mikä on soveliasta käyttäytymistä tietoverkon sisällä sekä sen ulkopuolella. Näillä menettelytavoilla luodaan kaikille käyttäjille heitä koskevia odotuksia, määritellään sovelias käyttäytyminen organisaation verkoissa, määritellään eri ryhmien roolit ja vastuut turvallisuuden takaamiseksi sekä määritellään tietoverkon tietoturvassa tarvittavat käsitteet ja mallit. (Thomas 2005, 47 - 48.)

2.4 Tietosuoja

Tietosuoja käsitetään myös yksityisyyden suojaksi. Halutaan suojella ihmistä hänestä kerättävän henkilötiedon sekä henkilökohtaiseen toimintaan liittyvän tiedon varastoinnin sekä käsittelynosalta siten, ettei henkilön yksityisyys vaarantuisi. Huolta aiheuttaa sellaisen tekniikan kehitys, mikä mahdollistaa tällaisen tiedon keräämisen huomaamattamme todella helposti. (Järvinen 2002, 21; Microsoft Security Response Center 2012.)

Kauppias rekisteröi ostokset, kirjasto lainattavat kirjat, työpaikka seuraa työntekijän kulkua rakennuksessa. Matkapuhelimella soitettaessa operaattori tietää soittajan sijainnin. Myös puhelimella Internetiä tai sähköpostia käyttäessään jättää käyttäjä jälkensä satoihin viranomaisten ja tuhansiin yksityisten ylläpitämiin tietokantoihin. Voidaan sanoa, että pääsy tähän tallennettuun tietoon kiinni mahdollistaisi henkilön yksityisen sekä työelämän läpivalaisun hetkessä. Silloin saataisiin selville, millaisia ihmiset todellisuudessa ovat. (Järvinen 2010, 9.)

Yksityiselämän suoja ja julkisuusperiaate ovat jo perustuslaissa säädeltyjä perusoikeuksia. On olemassa lakeja, jotka pyrkivät suojaamaan ihmisiä työpaikallaan näiltä uhkakuvilta. Keskeisimmät ovat sähköisen viestinnän tietosuojalaki (516/2004) sekä laki yksityisyyden suojasta työelämässä (759/2004). Henkilötietolaki velvoittaa rekistereiden pitäjiä suojaamaan kerätyt tiedot siten, etteivät ulkopuoliset pääse niihin käsiksi. (Järvinen 2005, 29 - 30; Valtiovarainministeriö 2013d.)

Viestintäsalaisuus on käsite, joka pitää sisällään kaiken luottamuksellisen viestinnän muodot. Vuonna 2000 voimaan tulleen perustuslain 10. pykälä määrittelee yksityiselämän suojaa seuraavasti: ”Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton”. Laki on tiukka, pelkkä tiedon hankkiminen viestin lähettämisestä tai vastaanottamisesta on kielletty muilta kuin asianomaiselta itseltään. Viestintäsalaisuus on myös voimassa kotioloissa puolisoiden kesken. (Järvinen 2010, 145 - 148.) Tämä ei aina toteudu, sillä eri kyselytutkimuksissa hieman yli puolet naisista ja vähän alle puolet miehistä myöntää lukeneensa salaa kumppaninsa tekstiviestejä tai tutkineensa heidän puhelimensa puhelutietoja. (Järvinen 2010, 26.) Sähköpostien tai puhelutietojen tutkiminen toisen kännykästä sekä tekstiviestien lukeminen on kiellettyä ja rangaistavaa. Suomessa on annettu tuomioita kotona tapahtuvien viestintäsalaisuuksien loukkauksista. (Järvinen 2010, 148.)

3 TIETOTURVAN UHAT JA NIIHIN VARAUTUMINEN

Suomessa toimii Viestintävirastossa kansainvälinen tietoturvaviranomainen (CERTI-FI), jonka tehtävänä on tietoturvaloukkauksien ennaltaehkäisy, havainnointi, ratkaisu sekä tietoturvauhkauksista tiedottaminen. (CERTI.FI 2012).

Tietojen, järjestelmien ja palveluiden on oltava luotettavia, oikeita ja ajantasaisia. Ne eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muidenkaan vahinkojen ja tapahtumien seurauksena. (Valtiovarainministeriö 2013d.)

Tietoturvauhkia on montaa eri laatua. Kaikissa on pohjalla ihmisen hyväuskoisuuden hyväksikäyttö tai tietoturvakäytäntöjen tietämättömyys. Koneita ja verkkoja pystytään ohjelmoimaan ja luomaan niille sääntöjä, joilla ne toimivat. Ihminen on kuitenkin inhimillinen ja tunteet ohjaavat hänen käyttäytymistään. Käyttäytymiseen on helppoa vaikuttaa ja vedota. Ihminen omalla käyttäytymisellään luo tietoturvan toimintaympäristössään. (Järvinen 2002, 47; Microsoftin Security Intelligence Report 2012.)

Tutkimus listaa tietokoneiden käyttäjien laiminlyöntejä suurimmaksi uhkaksi itse tietoturvalle. Microsoftin Security Intelligence Report (SIR) analysoi raportissaan maailman laajuisesti haavoittuvuuksia ja haittaohjelmia 2012 vuoden ensimmäisen ja toisen vuosineljänneksen aikana, joita esiintyy Windows-käyttöjärjestelmissä. **Tietoja oli kerätty yli 600 miljoonan tietokoneen antamista telemetria-tiedoista ympäri maailmaa.** Tulokset saatiin käyttäjien tehdessä Windows® Malicious Software Removal Tool -työkalulla haittaohjelmien poistoja tietokoneista. Raportissa selvitettiin samalla, miten hyökkääjät hyödyntävät haavoittuvuuksia. Uhkan tietoisuus voi auttaa suojaamaan organisaatiota, ohjelmistoja ja ihmisiä näihin kohdistuvilta hyökkäyksiltä.(Microsoftin Security Intelligence Report 2012.)

3.1 Luottamuksellisuus

Tietoturvaan liittyvällä luottamuksellisuudella tarkoitetaan tietoon tai tiedostoihin pääsyä vain heille, joilla on oikeus kyseiseen tietoon. Luottamuksellisuuden motiivina on usein vain organisaatioiden oma etu, mutta nyt myös laki velvoittaa tähän. Pyrkimyksenä on suojata tieto siten, että sitä pystyvät lukemaan tai muokkaamaan vain ne henkilöt, joille on annettu lupa siihen. Käytännössä tämä merkitsee, että osa tiedoista

ja tietojärjestelmistä pidetään vain niiden käyttöön oikeutettujen saatavilla. Tällöin sivullisille ei anneta mahdollisuutta käsitellä, muuttaa tai poistaa tietoja vahingossa tai tahallisesti. Tietojen käsittelyyn oikeutetutkin henkilöt saavat käyttää tietoja ja järjestelmiä vain asianmukaisesti työtehtävissään. Tarvittaessa annetaan vain lukuoikeus tietoon, mikäli tiedon muokkaamiselle ei ole tarvetta (Järvinen 2002, 22; Valtiovarainministeriö 2013d; Microsoftin Security Intelligence Report 2012; Microsoft Top Tips for Online Safety at Home.)

Luottamuksellisuuden uhkana ovat tietomurrot, varkaudet, huijaukset sekä hyökkäykset. Murtautuminen suojatulle tai suojaamattomalle tietokoneelle ja sen käyttäminen ilman lupaa on uhka. Tietokoneelta varastettuja tiedostoja voidaan käyttää myös erilaisiin luvattomiin tarkoituksiin. Esiintyminen vääränä henkilönä sekä huijausyritykset ovat arkipäivää. Tietojärjestelmään hyökkääminen sekä sen heikkojen kohtien etsiminen tarkoituksena vahingoittaa järjestelmää tai käyttää sitä oikeudettomasti on päivittäinen uhka. (KOPPA, Jyväskylän yliopisto.)

Luottamuksellisuus pyritään turvaamaan teknisin ratkaisuin, kuten **tiedon salauksella** (encryption), **todentamisella** (autentication) sekä **pääsynvalvonnalla** (access control). Pääsynvalvontaan kuuluu oleellisesti käytön seuranta. Seuranta tapahtuu erinäisten ohjelmien taikka verkkolaitteiden tekemillä merkinnöillä, eli logi-tiedostoilla (Järvinen 2002, 24 – 27.)

Toimitilojen turvallisuudella varmistetaan, että tietoja, asiakirjoja ja tietokonelaitteita säilytetään ja käsitellään asianmukaisesti turvallisissa tiloissa. Toimitilojen turvallisuus sisältää mm. kulunvalvonnan, teknisen valvonnan ja vartioinnin, palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkojen torjunnan sekä lähettipalvelujen ja tietoaineistoja sisältävien lähetysten turvallisuuden. (Järvinen 2002, 24 - 27; Valtiovarainministeriö 2013d.)

3.2 Eheys

Eheydellä pyritään suojaamaan tietoa siten, että sitä ei pystytä muuttamaan tahallisesti tai tahattomasti. Tällöin tieto säilyy luotettavana ja se on saatavilla tarvittaessa. Eheyden voi rikkoa käyttäjän huolimattomuus hänen käsitellessään tietoa. Käyttäjä voi vahingossa poistaa tiedon tallennuspaikasta. Levyrikko on hyvin mahdollinen, kun kyseessä ovat tekniset laitteet. Nykypäivänä siirrämme tietoa monen eri tiedonsiirto-

kanavan ja laitteen läpi, jolloin tiedon häviäminen, tiedoston eheysvika tai virukset voivat tuhota tiedon tai tehdä siitä käyttökelvotonta. (Järvinen 2002, 22 - 23.)

Eheyden uhkana ovat haittaohjelmat, virukset ja madot, mutta käyttäjä itse on suurin uhka eheydelle. Hän voi vahingossa poistaa tai tuhota tiedostonsa. Järjestelmä saattaa vahingoittua siten, että tiedostot tuhoutuvat tai tiedostojen sijaintipaikka tuhoutuu. Järjestelmään voi päästä haitallisia ohjelmia tai muita käskyjonoja, jotka vaurioittavat tiedostoja. Varmuuskopiointi auttaa palautumaan näistä ongelmista parhaiten tilanteeseen, joka vallitsi ennen tiedostojen vaurioitumista. (KOPPA, Jyväskylän yliopisto.)

Tekniset ratkaisut, joita käytetään turvaamaan tiedon eheyttä, ovat käyttöjärjestelmien ajantasaisuus sekä sen mukana tulevien vakio-ohjelmien päivittäminen. Toimisto-ohjelmistoja ei tule unohtaa tästä listasta. Käyttöjärjestelmien kriittiseksi luokiteltujen korjauspäivityksien ajantasaisuus tulee ylläpitää. Käyttöjärjestelmän kehittäjät sekä valveutuneet käyttäjät tutkivat taustalla käyttöjärjestelmien sekä oheisohjelmistojen haavoittuvuuksia. Maailman johtavalla käyttöjärjestelmän valmistajalla tämä tiimi kantaa nimeä Microsoft Security Response Center. Haavoittuvuuden tullessa ilmi. Taustalla alkaa korjaussuunnittelu sekä huoltopaketin rakentaminen loppukäyttäjille. Toiminto on mahdollista saada automaattiseksi, jolloin käyttöjärjestelmä tarkistaa huoltopakettien saatavuuden itse säännöllisesti sekä asentaa tarvittavat päivitykset koneelle. Tarjolla on myös manuaalinen vaihtoehto, jolloin käyttäjä itse huolehtii asian tarkistamisen ja mahdollisen asentamisen. (Korpela 2005, 35 - 41; Microsoft Security Response Center 2012.)

Erinäiset ”haittaohjelmat” tai ”tuholaisohjelmat”, joita kutsutaan tietokoneviruksiksi, voivat vaurioittaa tiedostoja. Niiden torjumiseksi tarvitaan virusohjelmistoa. Tämä suojaa sekä käyttöjärjestelmää että käyttäjän luomia tiedostoja haittaohjelmien aiheuttamilta tuhoilta. Saatavilla on kaupallisia tuotteita ja ilmaisjakeluversioita. Eroina näillä on niiden kyky puolustautua tai suojata tietojamme. Niiden tarjoamat ominaisuudet sekä tuotteiden valmistajien ylläpitoratkaisut vaihtelevat. (Korpela 2005, 63 - 66.)

Mikä tahansa virustorjuntaohjelma on parempi ratkaisu kuin olla verkkotekniikassa mukana ilman mitään virustorjuntaa. Vain kone, joka ei ole kytketty mihinkään verkkoon tai siihen ei yhdistetä ulkopuolista muuta laitetta, joka voisi koneen saastuttaa, on ainoa ratkaisumalli, jolloin voi harkita virus-torjuntaohjelmiston pois jättämistä. Uskomus, että mikäli käyttää jotain muuta käyttöjärjestelmää kuin Windows-

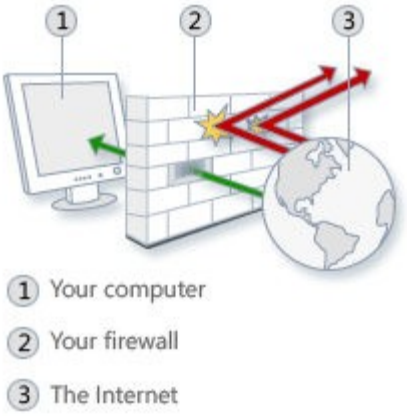
käyttöjärjestelmää, olisi turvassa viruksilta, ei pidä paikkaansa. Kaikille käyttöjärjestelmäalustoille on tehty viruksia, jotka leviävät verkossamme ja lisäksi erinäisten verkkoteknisin menetelmin, latauksien ja tallenteiden mukana. Erona on vain virusten määrä. Windows-käyttöjärjestelmä on maailman levinnein, jolloin sen käyttäjämäärä maailmassa on paljon muita suurempi ja hyötypohja virusten kirjoittajille on siten erittäin laaja. (Korpela 2005, 63 - 66; Microsoftin Security Intelligence Report 2012.)

Microsoftin Security Intelligence Report 2012 paljastaa, että juuri automaattinen toiminto Windowskoneissa, joka aukaisee esim. usb-muistitikun tai cd/dvd-tallenteen ennen virustutkan tarkistusta, levittää mekanismillaan valtaosan haittaohjelmista koneillemme. (Microsoft Security Response Center 2012.)

Mikäli käyttäjä suunnittelee kotiinsa internetyhteyttä, hän tarvitsee palomuurin (firewall). Oli yhteys käytössä työssä tai kotona, hän tarvitsee sen aina. Yhteys mahdollistaa koneen liittymisen maailmanlaajuiseen tietoverkkoon. Internet on avoin kaikille, jotka haluavat siihen liittyä. Maailmanlaajuisessa verkossa ei ole olemassa erillistä organisaatiota, joka valvoo siellä julkaistavaa tietoa tai pitää sen turvallisuudesta huolta, vaan vastuu on aina julkaisijalla itsellään. (Thomas 2005, 157 - 159; Microsoft, Safety & Security Center, What is a firewall?)

Palomuurit ovat tekninen ratkaisu tiedon eheyden saavuttamiseksi verkossa ja tietoturvaa tiedolle. Tietoturvalaite sijaitsee Internet-yhteyden reunalla ja toimii tietoliikenteen seuraajana. Sen tehtävä on huolehtia niin lähtevästä kuin tulevasta tiedosta annettujen määräyksien mukaan. Sen pääsääntöinen tehtävä on suojella sen takana olevia tietoverkkoja tai laitteita luvattomalta käytöltä tai tiedon muuttumiselta tahallisella teolla. (Thomas 2005, 157 - 159; Microsoft, Safety & Security Center, What is a firewall?.)

Palomuureja on ohjelmistopohjaisena sekä erillislaitteina toimivia, joita kutsutaan leikkisästi rautamuureiksi. Ratkaisuna palomuuri ei korvaa virustorjuntaa, vaan täydentää sitä. Virustorjunnan tarkkaillessa koneeseen tulleita tai käynnissä olevia tiedostoja, tarkastaa palomuuri ulkopuolelta tulevaa oliota tai verkkolaitteiden oikeutta tulla verkon sisäpuolelle niille laadittujen sääntöjen mukaisesti. Palomuurin tehtävään kuuluu myös estää verkosta ulospäin pyrkivä sellainen liikenne, joka ei ole tarkoituksenmukaista esimerkkinä liikenne, jota haittaohjelmat lähettävät sen tekijälle. (Korpela 2005, 86 - 92; Microsoft Security Response Center 2012.)



Kuva 1 Palomuuri (firewall), erottaa verkon ja internetin (Microsoft, Safety & Security Center, What is a firewall?)

Ajan myötä Internetin merkitys meille on muuttunut. Aluksi se oli Yhdysvalloissa 1960-luvulla puolustusvoimien kehittämä ARPAnet-tietoverkko. Myöhemmin yliopistot ja tutkimuslaitokset ottivat sen käyttöönsä, kutsuen tätä Internet-verkoksi. Ensimmäiset yritykset liittyivät mukaan tähän tietoverkkoon 1980-luvun tienoilla, niitä kiinnostivat erityisesti sähköposti- ja tiedostonsiirtopalvelut. Valtaväestön käyttöön se saatiin vasta 1990-luvulla. (Salminen 1998.) Aluksi Internet oli mukava etu saada tai levittää tietoa nopeasti, mutta nykyään se on muuttunut meille lähes välttämättömäksi niin kotona kuin työelämässä (Thomas 2005, 158).

Käyttäjät kuitenkin usein mieltävät oman kotikoneensa tietojen olevan niin merkityksettömiä, ettei niiden suojaamiselle ole tarvetta. Tästä ei kuitenkaan ole pelkästään kysymys, vaan tarkoitus on suojata itseään ja kotikonetta joutumasta verkon väärinkäyttäjien kohteeksi. Kotikonetta halutaan hyödyntää niiden tarjoamien resurssien ansiosta vaikkapa laskentakapasiteetin käyttöön salasana-avainten murtamiseksi. Omien jälkien peittäminen onnistuu hyvin, mikäli kuljetaan monen eri kotikoneen kautta. Tällöin reitin alkuperän seuraaminen on lähes mahdotonta. Nykyään kotikoneiden isot levykapasiteetit mahdollistavat piraattitiedostojen tai esimerkiksi pornograafisen tiedon väliaikaisen varastoinnin. (Järvinen 2002, 319 - 320.) Myös internetliikenteen häirintään käytettäviä haittaohjelmia voidaan piilottaa kotikoneille ja ohjaamaan niiden toimintaa tekijän antamasta käskystä. Tätä kutsutaan palvelunestohyökkäykseksi. Edellä mainitun Internetin väärinkäytön estämiseen ovat palomuuri ja virustorjunta yhdessä hyvä ratkaisu ainakin vaikeuttamaan väärinkäyttöä. (Kymen Sanomat 2012a.)

3.3 Saatavuus

Tiedon saatavuudella halutaan varmistaa tiedostojen tai palveluiden saatavuus sekä estää niiden käyttökatkokset. Tähän vaikuttavat lähinnä pelkästään niiden eteen tehdyt tekniset ratkaisut, joita ovat mm. varmuuskopiointi, turvattu sähkönsyöttö sekä luotettavat verkkoyhteydet. (Järvinen 2005, 31.)

Saatavuuden uhkana ovat samat uhkakuvat kuin eheydellä. Palveluiden saatavuus on turvattavissa ammattitaitoisten palveluidentarjoajien tuotteilla. Teknisin ratkaisuin on varauduttava esimerkiksi sähkönsyöttöongelmiin varavirtaratkaisuin ja etukäteen suunnittelulla toimintamallilla, jossa on varauduttu monipuolisesti erilaisiin tietoa uhkaaviin ongelmatilanteisiin. (Järvinen 2005, 34 - 36.) Tiedon saatavuutta voivat uhata: kiintolevyrikko, tiedostoeheyden häviäminen, käyttäjän vahingossa poistama tieto tai tietomurron yhteydessä vahingoittuneen tiedon palauttaminen alkuperäiseen muotoon. (Järvinen 2002, 95.)

Näihin tilanteisiin tulisi varautua etukäteen. On suunniteltava tiedon palautusratkaisu siltä varalta, että tieto häviää ja on myös testattava sen toimivuus. (Järvinen 2002, 95.) Varmuuskopiointiin annettujen ohjeiden mukaan tulisi kopioida vain välttämättömät tiedot. Siihen tarkoitukseen voi käyttää eri kovalevyä, kuin sitä missä alkuperäinen tieto on. Varmuuskopioinnin voi tehdä cd- tai dvd-levlle tai voi käyttää usb-muistitikkua. Varmuuskopiot tulisi säilyttää fyysisesti eri paikassa, kuin missä alkuperäinen tieto sijaitsee. Tämä tehdään sen vuoksi, että mikäli samassa kiinteistössä tapahtuu esim. tulipalo tai vesivahinko, tuhoutuvat niin kone kuin varmuuskopiot. Varmuuskopioinnin laajuus määräytyy ennalta asetetun suunnitelman pohjalta, jossa on mietitty, kuinka iso osa käyttäjän tekemästä työstä voi tuhoutua vahingon tapahduttua. (Korpela 2005, 95 - 96.)

3.4 Todennus

Todennuksessa varmistetaan, että tietoon tai palveluun pyrkivä olio tai verkkolaite on juuri se, mikä pitääkin (Järvinen 2002, 24 - 25). Yleisin käytetty todennusmuoto tietotekniikassa on salasana. Siinä käyttäjä tunnistetaan käyttäjätunnuksen sekä salasanan perusteella oikeaksi. (Järvinen 2005, 34 - 36.)

Uhkana ovat käyttäjätunnuksien ja salasanojen joutuminen vääriin käsiin. Keskinäisessä todennuksessa käyttäjä ja palvelu todentavat toisilleen, keitä ne ovat. (KOPPA, Jyväskylän yliopisto.)

Käyttäjät omalla käyttäytymisellään usein vaarantavat tietoturvallisuuden toteutumisen. Salasanoina käytetään sellaisia sanoja, jotka ovat helposti arvattavissa ilman tekniikkaa. Esimerkkeinä voidaan todeta tällaisia olevan: oma nimi, puolison nimi, harrastuksiin liittyviä sanoja sekä syntymäaikoja.

Monessa järjestelmässä onkin teknisesti pyritty ratkaisemaan tämä ongelma. Järjestelmään on muodostettu sääntöjä, jotka vahtivat käyttäjän tekemiä salasanoja. Tämä estää tyypillisimmin käyttäjää muodostamasta salasanaa normaaleista merkkijonoista sekä määrää jonon pituuden. Myös vaihtoväli on usein säädetty ennakkoon.

Käyttäjät kirjoittavat usein salasanansa pareille ja säilyttävät sitä paikassa, josta muilla ulkopuolisilla on mahdollisuus löytää ne. Salasanan tulee olla henkilökohtainen eikä sitä tule luovuttaa kenellekään muulle henkilölle. Kirjauduttuaan järjestelmään tai palveluun henkilökohtaisilla tunnuksilla tulisi käyttäjän muistaa kirjautua sieltä myös ulos järjestelmän edellyttämällä tavalla. Mikäli näin ei toimita, voi seuraava koneen käyttäjä esiintyä edellisenä käyttäjänä. Tällöin kaikki hänelle suunnatut palvelut sekä koneen resurssit ovat väärän henkilön hallinnassa ja tietoturva on menettänyt merkityksensä tässä kohden. (Korpela 2005, 122 - 131.)

3.5 Pääsynvalvonta

Pääsynvalvonta varmistaa tunnistamisen jälkeen oliolle tai koneelle pääsyn vain ennalta määrättyihin tietoihin. Usein tiedon käsittelylle on erilaisia tarpeita. Joskus käyttäjän tarvitsee vain päästä lukemaan tietoa ja vain harvoin hänen tarvitsee muokata tätä kyseistä tietoa. Monesti työyhteisössä työnkuvat ovat erilaisia ja tiedon saatavuuden tarve on erilainen. (Järvinen 2005, 31 - 32.) Tiedon tuottajalle sekä sen haltijalle erottelematta, onko tämä yritys vai yksityinen henkilö, on tärkeää estää ulkopuolisen tunkeutuminen heidän tiedostoihinsa ja tiedon käyttäminen omiin tarkoituksiinsa (Hakala, Vainio, Vuorinen 2006, 82 - 86.)

Uhkana on luvaton pääsy tiedostoihin tai tietojärjestelmiin, joita ei ole tarkoitettu vapaaseen tarkasteluun tai tiedon muuttamiseen. Pääsynvalvonta tarkoittaa sitä, että tie-

toa tai tietojärjestelmää voivat käyttää vain valtuutetut henkilöt tai sovellukset. (KOPPA, Jyväskylän yliopisto.)

Esimerkkinä voidaan ottaa palkanlaskija ja tekninen suunnittelija. Palkanlaskija ei tee mitään teknisillä piirustuksilla laskiessaan työntekijöiden palkoja eikä tekninen suunnittelija palkanlaskijalle suunnatuilla tiedostoilla eikä palveluilla. Mikäli kuitenkin esimerkkitapauksessa tämä tietoturvan osa-alue ei toimisikaan, voisi tekninen suunnittelija esimerkiksi tuplata oman palkkansa. Palkanlaskija voisi muuttaa teknistä piirustusta, jolloin koko suunnittelutyö vaarantuisi. (Järvinen 2005, 31 - 32.)

3.6 Kiistämättömyys

Kiistämättömyys tai sen tarve perustuu usein lainsäädäntöön. Organisaation tulee tarvittaessa pystyä todistamaan tiedon alkuperäinen tekijän tai tuottaja. Tällä menetelmällä luodaan myös työntekijälle oikeusturvaa. Kiistatilanteissa tietoturvarikkomuksissa on kyettävä osoittamaan riittävän luotettavalla menetelmällä sekä tekijä että tehty rike. (Hakala, Vainio & Vuorinen 2006, 86.)

Kiistämättömyys tarkoittaa tapahtuneen todistamista jälkeenpäin, jolloin tavoitteena on juridinen sitovuus. Kiistämättömyys varmistaa sen, ettei toinen osapuoli voi kieltää toimintaansa jälkeenpäin. Mikäli tietojärjestelmän haltijalla ei ole riittävää osaamista tai asianmukaista järjestelmää tutkia tapahtumia jälkeenpäin, on oikeusturvan toteutuminen vaarassa (Kymenlaakson ammattikorkeakoulu, Käyttäjän tietoturvaohje.)

Henkilötietolain 7. luvun, §:n 32. mukaan:

”Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä. Toimenpiteiden toteuttamisessa on otettava huomioon käytettävissä olevat tekniset mahdollisuudet, toimenpiteiden aiheuttamat kustannukset, käsiteltävien tietojen laatu, määrä ja ikä sekä käsittelyn merkitys yksityisyyden suojan kannalta.” (Henkilötietolaki, 7. luku 32. §.)

Viranomaisten toiminnan julkisuudesta annetun lain 5. luvun 18. §:n mukaan taas ”Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia

asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muusta tietojen laatuun vaikuttavista tekijöistä…" (Laki viranomaisten toiminnan julkisuudesta 5. luku 18. §.)

3.7 Perustason tietoturva käytännössä

Tietokoneen käyttäjälle ja organisaatioille, joissa he työskentelevät, on laadittu monia ohjeistuksia tietoturvan varmistamiseksi. Tiedon saaminen ei ole ongelma nykypäivänä, sillä Internet tekee sen varsin helpoksi. Ongelmaksi muodostuu tietämättömyys siitä, mistä tätä tietoa etsiä luotettavasti. VAHTI ja Microsoftin ohjelmistotalo ovat listanneet toimenpiteitä, joita toteuttamalla käyttäjät voivat parantaa tietoturvaa. Poimintoja e.m ohjeistuksista.:

1. Jokaiselle käyttäjälle tulee tehdä omat henkilökohtaiset tunnukset, joilla on vain ns. normaalikäyttäjän oikeudet. Käyttäjätilejä Windows-koneissa on kolmenlaisia: normaali, järjestelmänvalvoja sekä vierailija. Ylläpitäjän tunnuksia käytetään (Järjestelmänvalvoja, Administrator) vain ylläpitotehtäviin, mikäli tarvitaan asentaa jonkin uusi sovellus koneelle. Tällä estetään viruksien oikeudet kirjoittaa käyttöjärjestelmän eri osiin omia komentojonojaan tai ainakin vaikeutetaan niiden leviämisestä.

2. Estetään asiaton pääsy tietojärjestelmiin, lukitsemalla työasema (Windows-työasemalla painetaan Ctrl+Alt+Del ja valitaan lukitse tietokone) aina kun poistut työpisteestäsi. Tällä estetään luvaton käyttö käyttäjän tunnuksilla hänen tietämättään.

3. Älä luovuta henkilökohtaisia käyttäjätunnuksiasi, salasanojasi, toimikorttiasi tai PIN-koodejasi toisen henkilön käyttöön, älä edes tietohallinnolle. Suhtaudu epäilevästi kaikkiin tiedusteluihin, jotka liittyvät salasanoihisi tai järjestelmien käyttöoikeuksiisi. Hyvin hoidetussa organisaatiossa ei ylläpito tarvitse käyttäjän henkilökohtaisia tunnuksia tehdessään asennus- tai huoltotoimenpiteitä.

4. Vaihda salasanat riittävän usein ja heti, jos epäilet niiden paljastuneen. Huolehdi, että salasanat ovat riittävän monimutkaisia ja vältä tuttujen jokapäiväisten sanojen käyttöä salasanana. Hyvässä salasanassa voi olla pieniä ja isoja kirjaimia, numeroita ja jopa erikoismerkkejä. Kaikkiin järjestelmiin erikoismerkit eivät kuitenkaan käy. Hyvä salasana on sinun helppo muistaa, mutta vaikea ulkopuolisen arvata.

5. Älä kirjoita salasanoja muistiin ainakaan sellaiseen paikkaan, mistä ne ovat helposti löydettävissä.

6. Asenna vain virallisia, ajan tasalla olevia ohjelmistoja. Mikäli et tiedä, mitä olet tekemässä, jätä se tekemättä kokonaan. Muista pitää käyttöjärjestelmä sekä oheisohjelmistot ajan tasalla sekä tietoturvapäivitettynä.

7. Huolehdi käyttöjärjestelmän ja muun varusohjelmiston jatkuvasta automaattisesta päivittymisestä.

8. Käytä tunnettua ja hyvämaineista tietoturvaohjelmapakettia (sis. mm. virustorjunta, palomuuri, vakoiluohjelmatorjunta, roskapostisuodatus) ja huolehdi sen jatkuvasta automaattisesta päivittymisestä. Microsoft-ohjelmistotalo listaa luotettavat yhteistyökumppanit sivuillaan, niin kaupalliset kuin ilmaisjakelutietoturvaohjelmistotalot, ja ohjaa niiden kotisivuille osoitteessa: http://www.microsoft.com/windows/antivirus-partners/windows-7.aspx. Tarkista virustutkalla aina ennen käyttöäsi ulkopuolinen tallennusmedia, joka voi olla ulkopuolinen kovalevy, usb-muistittikku tai dvd/cd-levy tai jokin muu erillinen tallennusmedia. Poista automaattinen ulkopuolisen medialaitteen avausominaisuus käytöstä. Ohjeistus löytyy Microsoftin tuotetukisivustoilta osoitteesta: http://support.microsoft.com/kb/967715.

9. Älä avaa epäilyttäviä sähköpostiviestejä ja -liitteitä. Sähköpostin liitetiedostot voivat sisältää haittaohjelmia (viruksia, matoja tai troijalaisia). Varo kaikkia epätavallisia sähköposteja ja erityisesti liitetiedostoja. Tarkastele viestin otsaketta. Phishing eli suomeksi "kalastus" on eräänlainen identiteettivarkaus verkossa. Sitä käyttävät sähköpostit, jotka on suunniteltu varastamaan henkilökohtaisia tietoja kuten luottokorttinumeroita, salasanoja, tilitietoja tai muita tietoja, mistä voi hyötyä rahallisesti. Roskapostia voivat olla esim. sähköpostiin tilaamatta tulleet mainokset. Roskapostiin ei kannata vastata, vaan se kannattaa tuhota heti. Jos viestiin vastaa, tietää roskapostittaja sähköpostiosoitteesi toimivaksi ja jatkaa roskapostien lähettämistä ja lisäksi välittää osoitteesi myös muille roskapostittajille. Postin automaattinen lukukuittaus kertoo roskapostittajalle saman asian. Tämä automaattinen lukukuittaustoiminto käyttäjän olisi hyvä poistaa sähköpostiohjelmastaan.

10. Tee säännöllisesti varmuuskopiot ja harjoittele niiden käyttöönottoa.

11. Kun kirjaudut Internetin palveluihin ja teet esim. ostoksia, käytä vain luotettavia palveluita ja toimittajia. Älä anna enempää henkilökohtaista tietoa kuin on tarpeen. Sosiaaliset verkot ovat nykyään yleistyneet. Siellä ollessasi huolehdi oman profiilisi turvallisuudesta, tarkista säännöllisesti sivustojen asetuksia lukuoikeuksien osalta, ketkä ovat oikeutettuja näkemään sinun henkilökohtaisia tietojasi. Älä jaa siellä mitään, mikä voisi vahingoittaa sinua myöhemmin. Painaessasi lähetepainiketta on kuva tai tilapäivitys hetkessä laajassa jakelussa. Tilanne on samalla hetkellä poissa sinun hallinnastasi.

12. Jos käytät julkisia päätteitä tai tilapäisesti toisen henkilön hallussa olevaa tietokonetta, muista tyhjentää Internet-selaimen välimuisti ja evästeet (cookies). Pyydä tarvittaessa henkilökunnalta apua, mikäli olet julkisilla paikoilla esim. koulussa, kirjastossa tai muualla vastaavanlaisessa paikassa, jossa on koulutettua henkilökuntaa.

13. Sammuta tietokone yöksi ja silloin, kun työskentelyysi sen kanssa tulee pidempi tauko.

14. Seuraa tietoturvallisuuteen liittyviä tiedotteita, tutustu ohjeisiin ja osallistu sinulle tarjottuun koulutukseen. Toimi saamiesi ohjeiden mukaisesti. (Valtiovarainministeriö 2013d; Microsoft Security Intelligence Report 2012; Microsoft Top Tips for Online Safety at Home; Microsoft Tuotetuki, Automaattisen käynnistyksen poistaminen käytöstä Windowsissa.)

Opiskelija ei pysty suoriutumaan opinnoistaan, mikäli hän ei käytä oppilaitoksen tarjoamaa tietojärjestelmää hyväkseen. Opiskelumateriaali on sähköisessä muodossa mm. Moodle-verkkoympäristössä. Päästäkseen käsiksi tietoon tulee opiskelijalla olla henkilökohtainen käyttäjätunnus sekä salasana Kymenlaakson ammattikorkeakoulun verkkoympäristöön. Tällä menetelmällä käyttäjä tunnistetaan ja hänen käyttäjätunnuksensa mukaiset palvelut avautuvat.

3.8 Terveysalan opiskelijan arkea tietoverkossa

Terveysalan opiskelijan tunnistus tietoverkossa alkaa hänen kirjautuessaan tietoverkkoon. Alkaa edellä mainitut tapahtumat, kuten **todennus** (authentication) ja **pääsynvalvonta** (accesse control). Oppilaitos on aiemmin tehnyt määritelmät **luottamuksel-**

lisuudesta (confidentiality) sekä **saatavuudesta** (availability), joka mahdollistaa opiskelijalle pääsyn tietoon, mikä on hänelle tarkoitettu.

Tiedolle on myös määritetty tiedostojen **eheys** (integrity), mikä takaa sen, että opiskelija ei voi muuttaa tiedon sisältöä esim. luentomateriaaleja. Tieto pysyy muuttumattomana muillekin sitä tarvitseville käyttäjille. **Kiistämättömyydestä** (non-repuditation) huolehditaan järjestelmän keräämien logi-tietojen avulla. Näiden avulla voidaan tarvittaessa jäljittää sekä todistaa tapahtumat tietojärjestelmässä. Oppilaitos painottaa, että tietoturva on kaikkien käyttäjien asia. Tietoturvallisuuden avulla varmistetaan tärkeiden tietojen hallinta ja toiminnan jatkuvuus opetuksessa. (Kymenlaakson ammattikorkeakoulu, Käyttäjän tietoturvaohje.)

Luottamuksellisuus	Todennus
Eheys	Pääsynvalvonta
Saatavuus	Kiistämättömyys

Kuva 2. Tietoturvan kuusi perustaa (Järvinen 2002, 21 - 27.)

4 TUTKIMUSONGELMAT

Tutkimusongelmat nousevat esille tietoturvateoriasta. Siellä määritelty tietoturva on muunnettava käytännöksi. Tutkimuksessa mitataan opiskelijoiden käytännön valmiuksia, tietoturvakäyttäytymistä vapaa-aikana sekä kouluympäristössä perustasolla. Tarkoitus on selvittää mahdolliset riittämättömyydet hyvien tietoturvakäytäntöjen osalta tutkittavassa joukossa. Tutkimus pyrkii myös selvittämään ne osa-alueet, joissa mahdolliset riittämättömyydentunteet tai selkeät virhekäyttäytymiset ilmenisivät.

Työn hyödynnettävyys on terveysalan opiskelijan näkökulmasta tietoturvan merkityksen ymmärtäminen sekä se, että tietoturva toteutuisi kotona ja työelämässä. Ammattikorkeakoululle tulokset antavat suuntaa oppilaiden tietoturvan osaamisesta ja toteutumisesta. Opetussuunnitelmia tehdessä tarkastelupohjan siitä, tarvitseeko tätä osa-aluetta erityisesti korostaa tai lisätä tulevaisuudessa terveydenhuollon opetuksessa.

Tutkimuksen tutkimusongelmat:

1. Millaiset valmiudet tutkittavalla joukolla on toteuttaa perustason tietoturvaa?

2. Millainen käsitys tutkittavalla joukolla on tietoturvan toteutuksesta ja sen vastuunkannosta?

3. Millaisia toiveita tutkittavalla joukolla on koulutusohjelmassaan saamansa tietoturvaopetuksen suhteen?

5 TUTKIMUKSEN TOTEUTUS

Opinnäytetyö on toteutettu kvantitatiivisena kyselytutkimuksena, jossa tutkitaan terveysalan opiskelijoiden tietoturvatietämystä sekä sen toteuttamista perustasolla. Tutkimuskysymykset ryhmiteltiin kahteen pääryhmään, taustamuuttujat sekä tietoturvatietämys.

5.1 Kyselytutkimus

Tutkimussuunnitelma on edellytys onnistuneelle mittaukselle. Kyselylomakkeen tai haastattelun tulisi mitata aidosti sitä, mitä sen tutkimussuunnitelmassa on sanottu mittaavan. Tutkijan tulisi täsmällisesti määritellä asiaongelma. Huolellinen taustatyö aikaisempiin teorioihin sekä aiempiin tutkimusongelmiin on myös välttämätöntä, sillä sen pohjalta tutkija muodostaa aiheesta avainkäsitteet. (Vilkka 2007, 63.)

Kvantitatiivinen eli määrällinen tutkimusote merkitsee sitä, että ilmiötä halutaan ja voidaan kuvata numeroin, määrin. Tutkimustuloksilla saadaan informaatiota siitä, missä määrin jotain ominaisuutta on mitatuissa tai vertailtavissa kohteissa. (Anttila

1996, 133.) Tutkimusmuotoa käytetään yleisesti sosiaali- ja yhteiskuntatieteitä tutkittaessa. Kvantitatiivisen tutkimuksen perustana on aina tutkimusongelma, johon haetaan vastausta. Tutkimuksessa on keskeistä aiempien teorioiden hyödyntäminen ja käsitteiden määrittely. Kyselyn avulla saadaan mitattua tosiasioita, toimintaa, tietoja, arvoja, uskomuksia sekä mielipiteitä. Oleellista on myös hyödyntää aiempien tutkimuksien johtopäätöksiä sekä asettaa hypoteesit, jos se on tarpeen. Tutkimuksen alussa täytyy suunnitella aineiston keruu. (Hirsjärvi 2003, 129,147.)

Määrällinen tutkimus vastaa kysymyksiin, kuinka paljon tai miten usein. Määrällisessä tutkimuksessa tutkittavien määrä on yleensä vähintään 100 silloin kun tutkimuksessa käytetään tilastollisia menetelmiä. Kun vastaajia on paljon, tutkittavat asiat pystytään selvittämään numeerisesti. (Vilkka 2007, 13, 17 - 18.)

Tutkimusta selkeytetään muuttujataulukolla. Tällä menetelmällä pyritään tutkimuksen kokonaiseen hahmottamiseen, tutkimuksen osien keskinäisten suhteiden määrittelemiseen sekä selvittämään ja selittämään tutkimuksen lainalaisuuksia syy-seuraus-suhteen avulla. Tutkimuksen tarkoituksena on saada vastaus seuraaviin kysymyksiin: Kuinka paljon jokin asia vaikuttaa toiseen tai kuinka usein jokin asia ilmenee (Vilkka 2007, 23; Hirsjärvi 2003, 134 - 135)

Saatekirjeestä vastaajalle tulee selvitä, mihin hänen antamiaan tietoja tai mielipiteitä käytetään. Tämän perusteella vastaaja tekee päätöksen osallistumisestaan tutkimukseen. Saatekirjeen pituus tulisi olla korkeintaan yksi sivu. Nykyään yleistynyt saatesanojen käyttö on melko ongelmallista, koska ne ovat informaatioltaan niin vähäisiä, että tutkittavan henkilön on vaikea tehdä sen perusteella päätöstä osallistumisestaan tutkimukseen. Hän ei saa tarvittavaa tietoa lyhyestä selostuksesta aiheen pariin. Hänelle jää kovin hauras käsitys tutkimuksen tärkeydestä. (Vilkka 2007, 81.)

5.2 Kohderyhmä

Opinnäytetyön kohderyhmänä ovat terveysalan opiskelijat. Kohderyhmän opiskelijat olivat vuonna 2011 opintonsa aloittaneita terveysalan opiskelijoita. Kysymykset lähetettiin yhteensä 164 oppilaalle. Kyselyyn vastasi yhteensä 59 opiskelijaa, mikä on 36 % kyselyn saaneista opiskelijoista. Vastaajista naisia oli 83 %.

Sähköisen kyselytutkimuksen yksi ongelma on vastaamattomuus. Kohdejoukkoa ei valmisteltu kyselyyn etukäteen ja vastaaminen oli vapaaehtoista. Verkkokyselyiden vastausprosentti on yleensä 30 - 40 %:n luokkaa. Tämä heikentää kyselytutkimuksen tulosten luotettavuutta. (Luoto 2009.) Tästä tutkimuksesta ei voi tehdä mitään tilastollista yleistystä. Puutteistaan huolimatta tutkimuksesta käy ilmi pienen joukon käsityksiä tietoturvasta sekä tietoturvan toimivuudesta käytännössä.

Tutkimuksen aluksi on tärkeää määritellä tutkimuksen tavoitteet ja tutkimusongelma. Tämän jälkeen päätetään tutkimuksen kohderyhmä eli perusjoukko. Perusjoukolla tarkoitetaan kaikkien havaintoyksiköiden muodostamaa kokonaisuutta. Havaintoyksikkö on siis mittauksen kohde, josta halutaan tietoa. Tämän jälkeen valitaan otantamenetelmä. Seuraavaksi toteutetaan otanta ja tarkistetaan palautuneet vastaukset. Sitten toteutunut otanta arvioidaan. (Vilkka 2007, 52, 60 - 61.) Suppeana otoksena pidetään noin sadan havaintoyksikön kokoa. Tämä edellyttää, että tutkija käyttää joitain analyysiohjelmaa tutkimuksen tuloksien analysoimiseen. (Vilkka 2007, 56 - 57.)

5.3 Kyselylomake

Kyselyn voi toteuttaa jakamalla kyselylomakkeet joko itse henkilöhohkaisesti tai toimittaa kyselyn jokaiselle havaintoyksikölle. Menetelmän valintaan vaikuttaa tutkimuksen aikataulutus sekä se, onko tutkimus yksi- vai monivaiheinen. Käytettävälle menetelmälle on hankittava koulutus. Tutkimuskohde sekä sen tavoitettavuus määrittelee tutkimuksen menetelmiä. Menetelmän valintaan vaikuttavat seuraavat seikat: minkälaista tietoa etsitään ja keneltä tai mistä sitä etsitään. (Hirsjärvi 2003, 170 - 171.) Tässä tutkimuksessa käytetään verkkokyselymenetelmää, koska tutkittava joukko on hajanaisesti sijoittunut tutkijaan nähden. Tällä pyritään lisäämään tutkittavan joukon tavoitettavuutta.

Kyselylomakkeen selvyys on tärkeintä. Kysymysten tulee merkitä samaa asiaa kaikille vastaajille. Kysymyksien tulee olla spesifisiä, jolloin väärintulkintamahdollisuus jää pieneksi. Kysymyksien pituudella on merkitystä kysymyksen ymmärtämiselle. Lyhyitä ja selkeitä kysymyksiä on helpompi ymmärtää. Kysymyksissä ei saa olla asioiden kaksoismerkityksiä.

Vastaajan on vaikea antaa kahta vastausta yhteen kysymykseen, joka sisältää kaksi erillistä kysymystä yhdellä kertaa. Kysymykseen tulee tarjota vaihtoehto ”ei mielipi-

dettä". Ihmisten on tutkittu vastaavan kysymyksiin vaikka heillä ei olisi asiasta oikeasti käsitystä. Tutkitusti vastaajista 12 – 30 % valitsee vaihtoehdon "ei mielipidettä", mikäli tällainen vaihtoehto on tarjottu ja heillä ei ole käsitystä kysyttävästä asiasta. Kysymyksissä tulisi käyttää mieluimmin monivalintavaihtoehtoja kuin "samaa mieltä / eri mieltä" -väitteitä. Ihmiset tutkitusti vastaavat näihin sillä oletuksella, mitä he olettavat kysymyksen laatijan haluavan vastattavan. Kysymyksien lukumäärällä on merkitystä, kun mitataan vastaajan keskittymistä aiheeseen. Esimerkiksi postikysely tulisi pystyä suorittamaan noin 15 minuutissa. Kysymyksien järjestys on samoin merkitsevässä osassa lomakkeen suunnittelussa. (Hirsjärvi 2003, 188 - 191.)

Ensin on määriteltävä tutkittavan asian käsitteet selkeiksi määritelmiksi, sellaisiksi, joita voidaan mitata. Tutkittavien jokaisen havaintoyksikön on ymmärrettävä käsitteet ja kysymykset samalla tavalla, muutoin tutkimustulos ei ole luotettava eikä yleistettävissä. Tutkijan purkaessa käsitteitä mitattavaan muotoon tulee hänen siirtyä teoreettiselta tasolta arkikielen tasolle. Tutkijan on hahmoteltava ja määriteltävä käyttämänsä käsitteet yleisesti. (Vilkka 2007, 36 - 38.) Kyselylomake esitestattiin havaintoyksiköihin rinnastettavilla henkilöillä. Esitestauksessa esille tulleet virheet korjattiin ennen varsinaista kyselyn toteuttamista.

5.4 Aineiston analyysi

Aineisto kerättiin verkkopohjaisella ZEF@Editor -työkalulla, johon luotiin kysymyspohjat. Kysymyslinkki lähetettiin saatekirjeen mukana 164:lle ennalta valitulle opiskelijaryhmälle. Vastaamiselle annettiin kahden viikon määräaika. Tämän jälkeen vastaukset purettiin Microsoft Excel 2010 -ohjelmistolla.

Oppilaitoksella olisi ollut mahdollisuus tarjota tutkijan käyttöön analysointi PASW Statistics 18 -ohjelma (SPSS). Ohjelmalla olisi pystynyt ristiintaulukoimalla selvittämään esimerkiksi eroja vähemmän tietokonetta käyttävien tietoturvaosaamisen suhteen, taikka koulutustason tuomia eroja. Näitä eroja ei kuitenkaan ilmennyt pienestä vastaajamäärästä. Excel -ohjelmisto oli riittävä tässä tapauksessa. Pohjat luotiin SPSS -ohjelmaan kuitenkin ennen kyselyn umpeutumista. SPSS -ohjelmaa ei käytetty. Kysely oli vakioitu, kysymykset esitettiin kaikille vastaajille samalla tavalla. Vastausvaihtoehdot oli annettu valmiiksi. Useammassa kysymyksessä käytettiin viisiasteista Likert -asteikkoa. Tapa on melko vakioitunut mielipideväittämä kysymyksissä. Muka-

na oli viimeisenä kysymyksenä vastaajan omaa toivetta koskeva kysymys: ”Millaisia tietoturvaan liittyviä asioita toivoisit käsiteltävän lisää opintojesi aikana?”

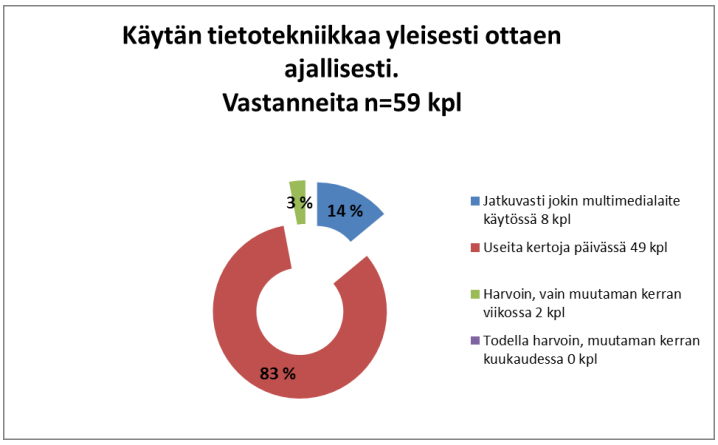
Vastaukset esitettiin seuraavasti: ”täysin samaa mieltä” tai ”jokseenkin samaa mieltä”. Saadut vastaukset käsiteltiin yhtenä tietueena. Myös ”en samaa enkä eri miltä” -vastaukset sekä ”en osaa sanoa” -vastaukset, käsiteltiin myös yhtenä tietueena. ”Jokseenkin eri mieltä” -vastaukset sekä ”täysin eri mieltä” -vastaukset olivat myös yksi tietue. Tämä oli riittävä tarkkuus, josta ilmenee vastanneiden mielipide kysyttävästä asiasta. Tämä myös selkeyttää tulosten purkamista ja esittämistä graafisessa muodossa.

6 TUTKIMUSTULOKSET

6.1 Taustamuuttujat

Tutkimuksessa ei tullut taustamuuttujien osalta esille eroa tietoturvatietämyksessä, kun vertailtiin opiskelijoiden erilaisia koulutustasoja. Vastaajista 42 %:lla oli lukiopohja, 31 %:lla oli lukio ja ammatillinen koulutustausta ja ammatillinen tutkinto oli 22 %:lla vastanneista. Lisäksi 5 %:lla oli ammattikorkeakoulu tai muu ylempi tutkinto. Vastanneista 71 % oli 20 - 29-vuotiaita.

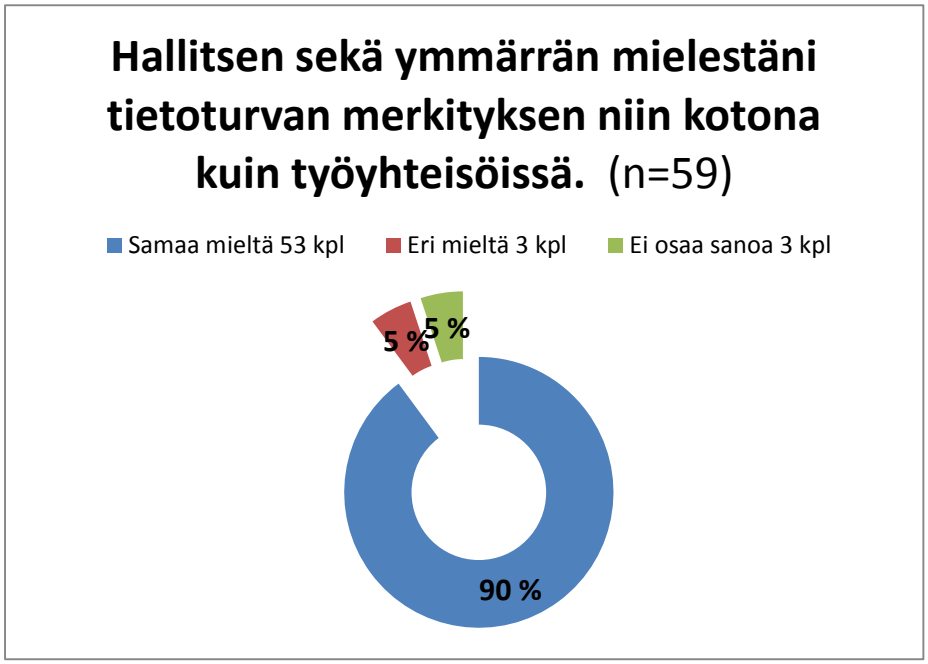
Kysyttäessä tietotekniikan ajallisesta käytöstä (Kuva 3) oli 83 %:n vastaus oli: ”useita kertoja päivässä”, 14 % vastasi että ”jatkuvasti jokin multimedialaite käytössä”. Voidaan todeta, että ajallisesti kaikki vastanneet käyttivät paljon aikaa tietotekniikan parissa. Opiskelu pohjautuu pitkälti itse oppimiseen sekä verkkopohjaiseen opiskeluun.



Kuva 3. Tietotekniikan käyttö

6.2 Opiskelijoiden tietoturvavalmiudet

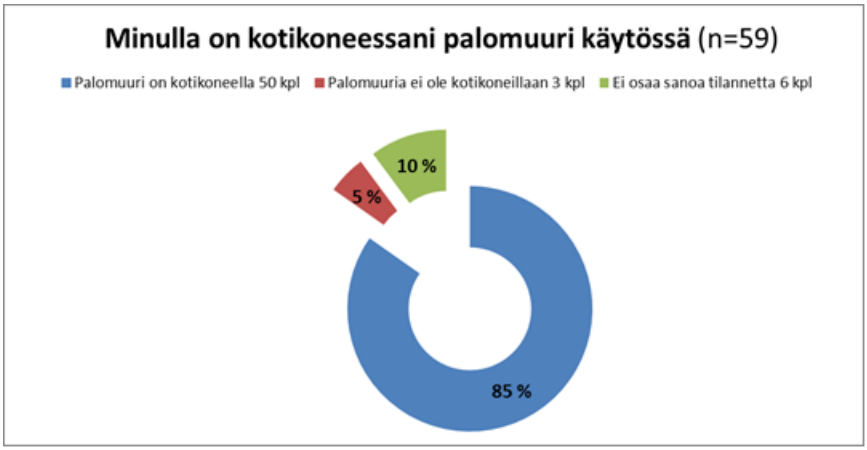
Vastaajien mielestä he ymmärtävät tietoturvan merkityksen hyvin. Vastaus väittämään ”hallitsen sekä ymmärrän mielestäni tietoturvan merkityksen niin kotona kuin työyhteisössä”, 90 %:n enemmistö vastasi myöntävästi.



Kuva 4. Tietoturvan hallinta

Suojausmenetelmät olivat myös suurimmalle osalle tuttuja. Kyselyn väittämä oli ”Tietotekniikassa käytettyjen suojausohjelmien merkitys on minulle selvä asia”. Vastanneista 76 % oli samaa tai jokseenkin samaa mieltä, 7 % oli eri mieltä ja 17 % ei osannut muodostaa mielipidettään. Tietotekniikassa käytettävien suojausohjelmien tuntemus oli erittäin hyvä.

Vastaajista myös valtaosa 85 % ilmoitti omistavansa kotikoneessaan palomuurin. Ainoastaan 10 % ei osannut sanoa tältä osin kotikoneensa tilaa.

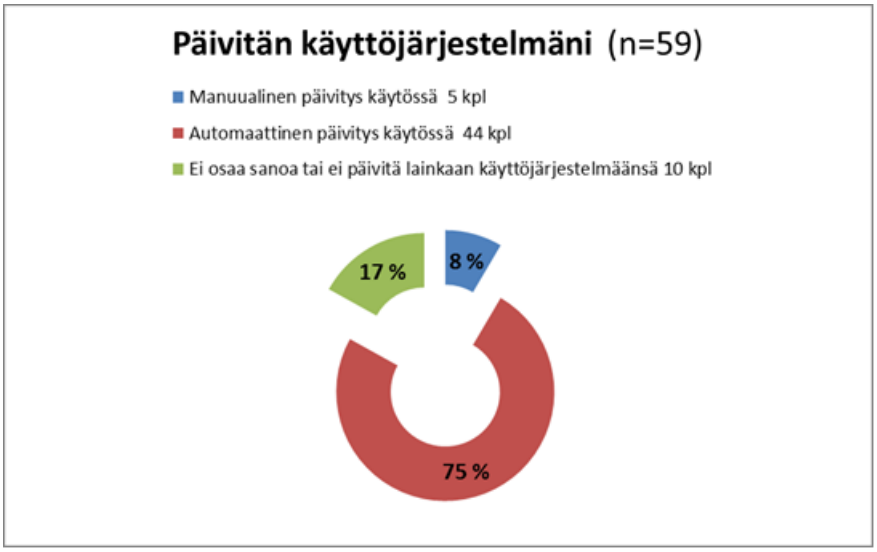


Kuva 5. Palomuurin käyttö

Tutkittavalta joukolta kysyttiin peruskäsitteitä alkaen käyttöjärjestelmän merkityksestä tietokoneessa. Vastausvaihtoehtoina olivat: ”Internet -selaimena, sähköpostiohjelmana, taulukkolaskentaohjelmana, tekstinkäsittelyohjelmana vai tulkkina koneen ja käyttäjän välillä”. 61 % mielsi käyttöjärjestelmän toimivan tulkkina koneen ja käyttäjän välillä. Internet -selaimena puolestaan käyttöjärjestelmää piti 20 % vastanneista. Taulukkolaskentaohjelmana käyttöjärjestelmää piti vain 2 %. Vastaajista 17 % ei osannut sanoa mielipidettään asiaan.

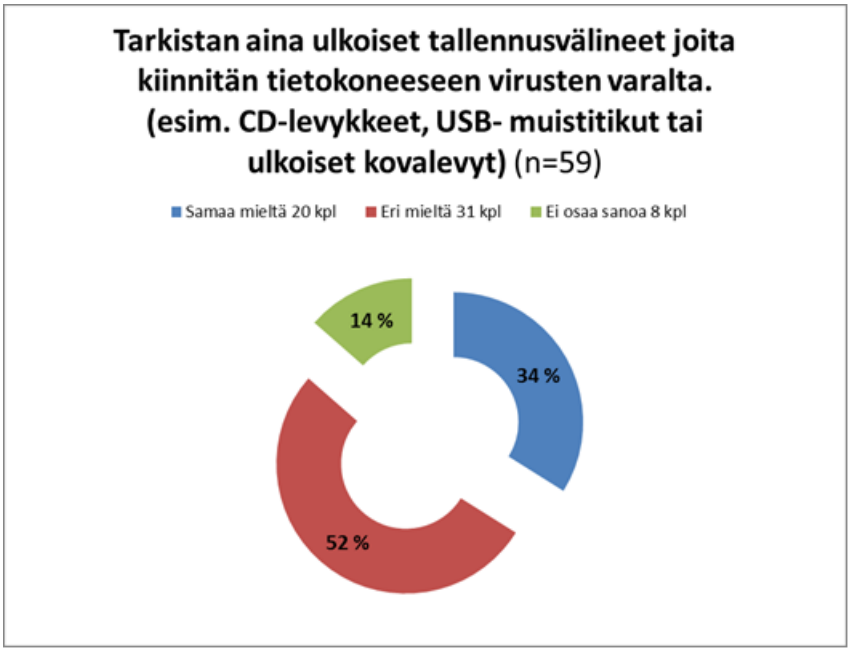
Käyttöjärjestelmän päivityksien ajantasaisuus oli korkeaa luokkaa tutkittavalla joukolla. Vain 17 % ei tiennyt tai osannut sanoa päivitysten ajantasaisuutta. Eli sama määrä vastanneista, jotka eivät tiedostaneet käyttöjärjestelmän merkitystä tietokoneessa, eivät myöskään osanneet kertoa päivitysmenetelmää tai eivät päivittäneet käyttöjärjestelmässään.

Kuva 6. Käyttöjärjestelmän toiminta



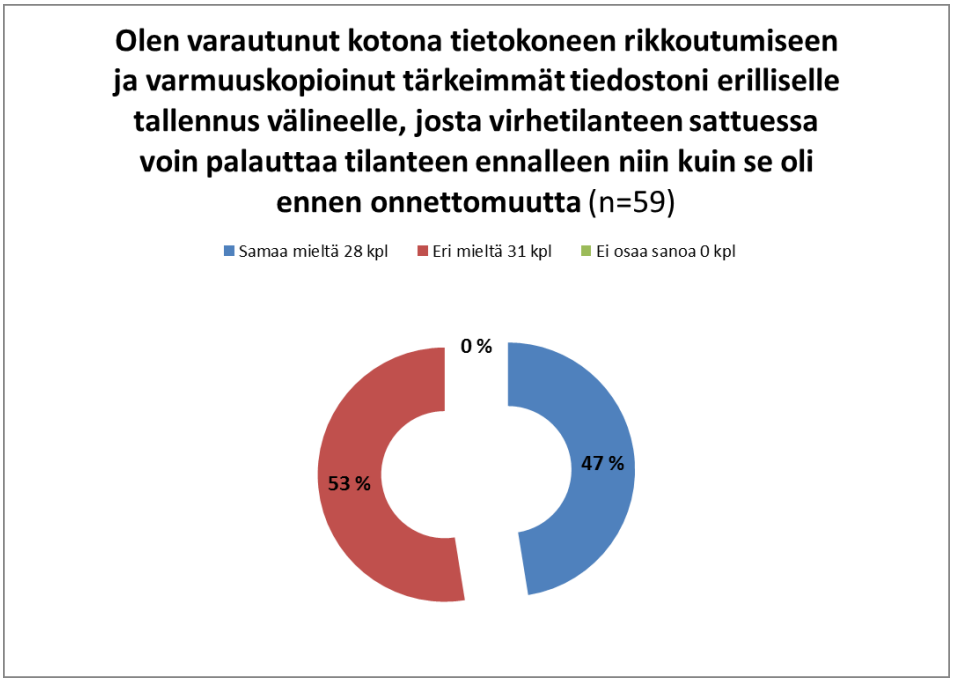
Kuva 7. Käyttöjärjestelmän päivittäminen

Ulkoisien tallennusvälineiden tarkastaminen viruksien varalta, joita kiinnitetään tietokoneeseen, jakoi mielipiteitä melkoisesti. Aina tai melkein aina ulkoiset tallennusvälineet tarkistivat 34 % kyselyyn vastanneista. Yhteenvetona voidaan todeta, että myönteisesti tarkistukseen suhtautui 34 % vastanneista kun taas 52 % suhtautui kielteisesti tarkistukseen.



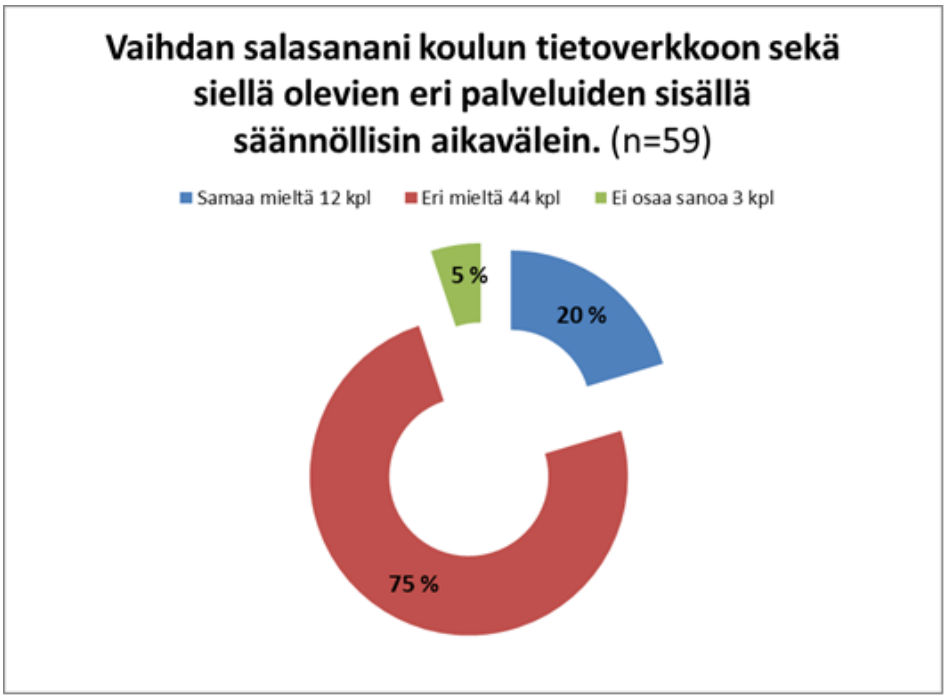
Kuva 8. Ulkoisten tallenteiden tarkistus

Kotikoneen rikkoutuminen tai muu onnettomuus vaatii varautumista. 47 % vastanneista oli tehnyt varmuuskopiot heille tärkeimmistä tiedostoista. Kysymyksessä haluttiin selvittää perusymmärrys varmuuskopioinnin ajatuksesta. Pidemmälle vietynä teknisesti varmuuskopiot tulisi säilyttää vielä fyysisesti eri paikassa kuin oma kotikone. Vain tällöin esimerkiksi vesivahingon tai tulipalon satuttua pystytään varmuuskopioita hyödyntämään jälkeenpäin. Kyselyyn vastanneiden osalta melko suuri joukko eli 53 % ei ollut varautunut koneen ongelmatilanteisiin varmuuskopioin.



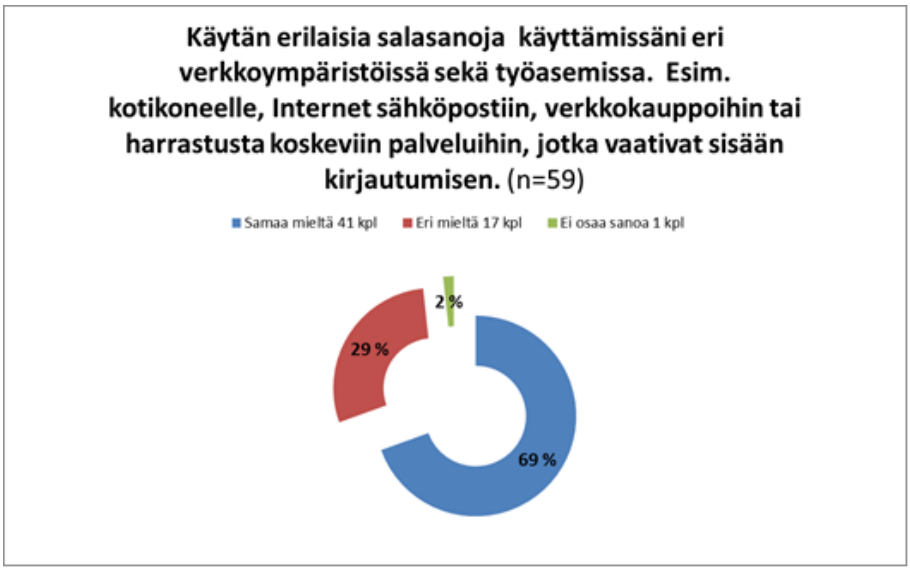
Kuva 9. Varmuuskopiointi

Mielipiteissä salasanan vaihtamisesta koulun tietoverkossa olevien eri palveluiden osalta oli suurta hajontaa. Vain 20 % vastanneista ilmoitti vaihtavansa säännöllisesti salasanansa eri palveluiden osalta. 75 % oli eri mieltä vaihdon suhteen. 5 % ei osannut sanoa salasanan vaihtamisesta mitään.



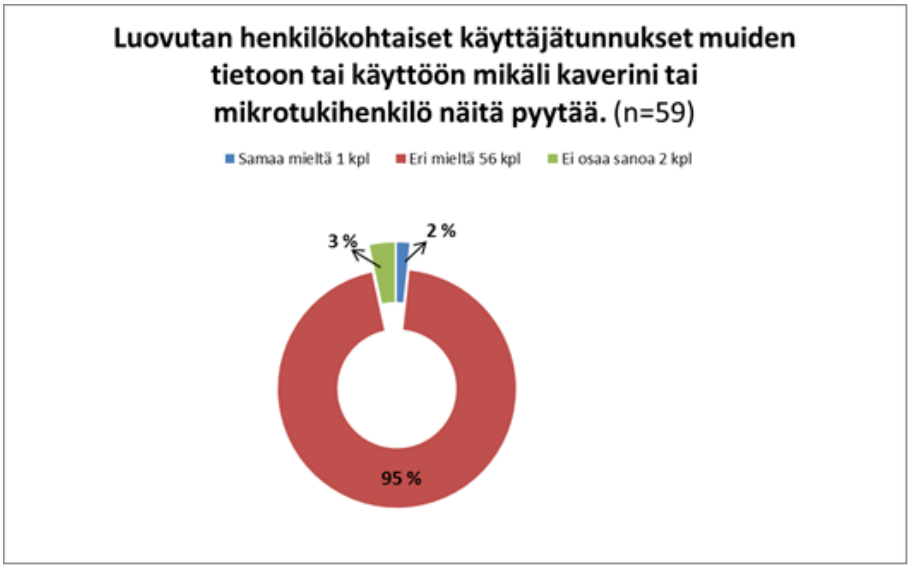
Kuva 10. Salasanan vaihto

Salasanojen käyttö tietoverkkojen eri palveluiden ja työasemien välillä: kyselyyn vastanneista 69 % kertoi myönteisesti käyttävänsä erilaisia salasanoja eri palveluiden kesken, 29 % vastasi eriävästi väittämään, ja 2 % vastanneista ei osannut sanoa mielipidettään.



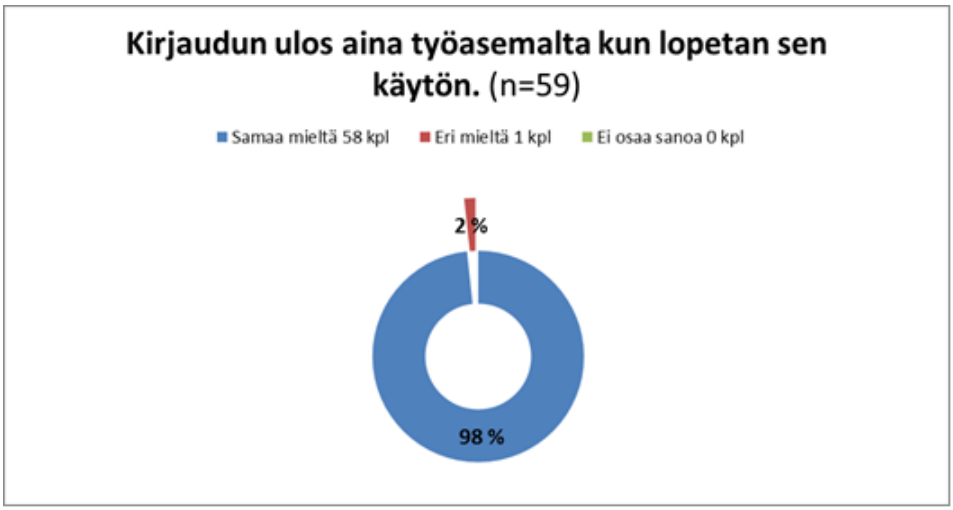
Kuva11. Salasana ja erilaiset verkkoympäristöt

95 % vastanneista ei luovuttaisi henkilökohtaista käyttäjätunnusta ystävän tai edes mikrotukihenkilön käyttöön näiden niitä pyydettäessä.

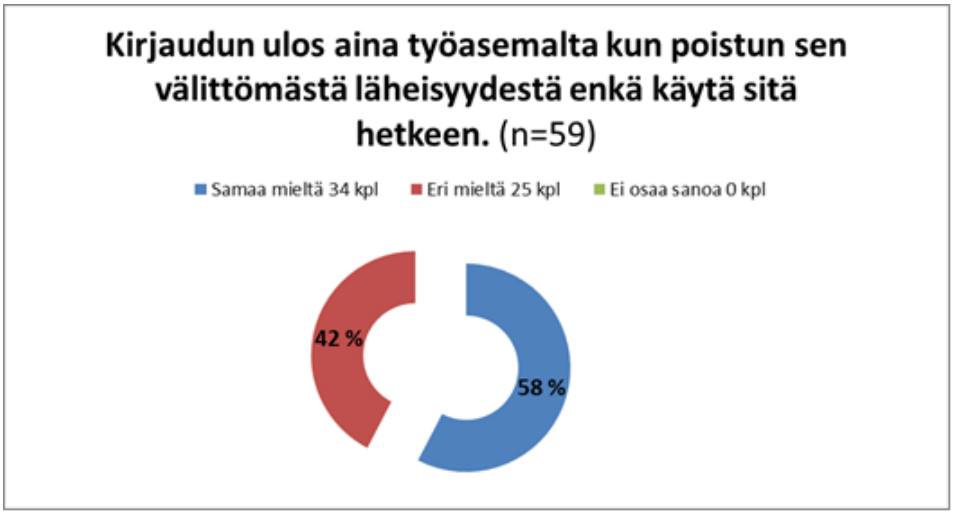


Kuva 12. Käyttäjätunnuksen luovutus

Käyttäjistä 98 % kirjautuu aina ulos työasemilta käytön loputtua. Mikäli poistuttiin työaseman välittömästä läheisyydestä, enää 58 % vastanneista kirjautui ulos työasemalta ja 42 % vastanneista ei kirjautunut ulos tietokoneeltaan.



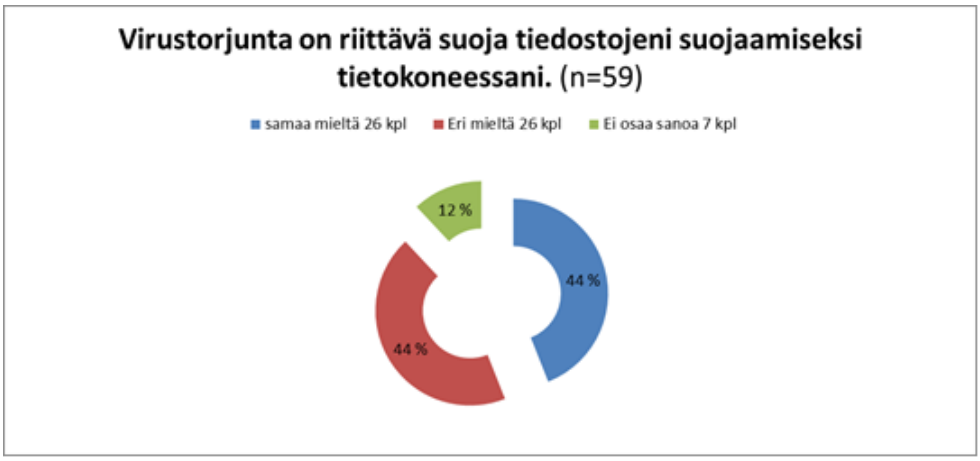
Kuva 13. Työasemalta uloskirjautuminen tietokoneen käytön loputtua



Kuva 14. Työasemalta uloskirjautuminen kun sen läheisyydestä poistutaan

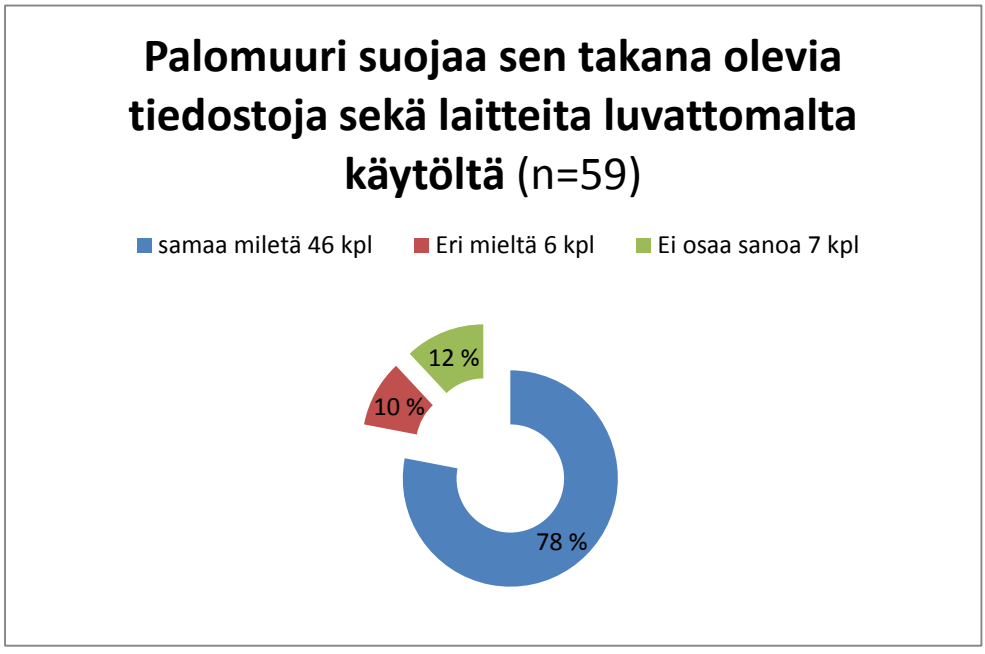
6.3 Opiskelijoiden käsityksiä tietoturvan toteutuksesta ja sen vastuunkannosta.

Kyselylomakkeen väittämä nro 7: ”Virustorjunta on riittävä suoja tiedostojeni suojaamiseksi tietokoneessani” vastaukset jakautuivat tasaisesti kahtia: 44 % oli väittämän kanssa samaa mieltä, 44 % olivat eri mieltä. Vastaajista 12 %:lla ei ollut mielipidettä.



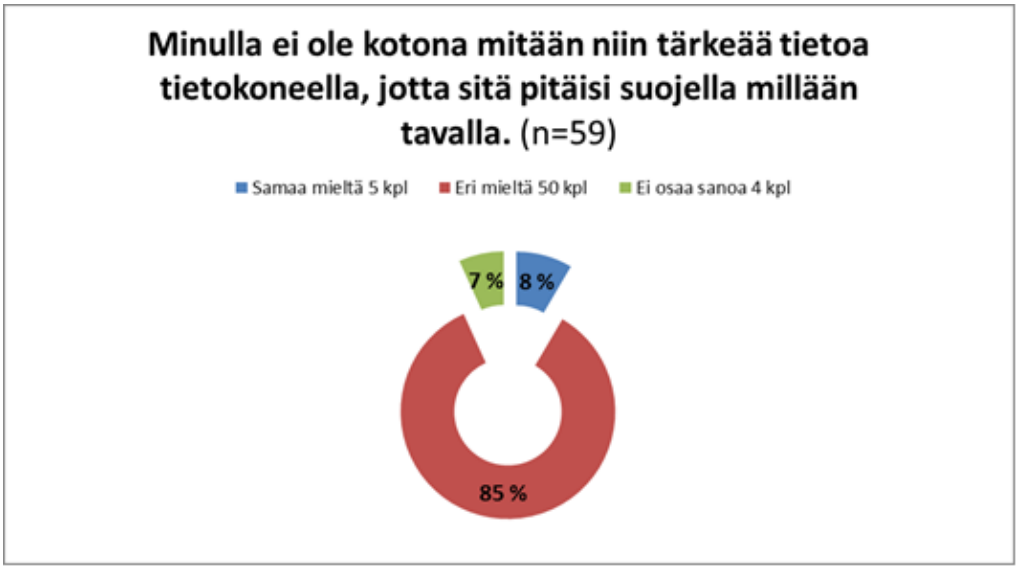
Kuva 15. Virustorjunta

Palomuurin merkitys tiedettiin hyvin, 78 % oli väittämän ”Palomuuri suojaa sen takana olevia tiedostoja sekä laitteita luvattomalta käytöltä” kanssa samaa tai jokseenkin samaa mieltä.



Kuva 16. Palomuurin merkitys

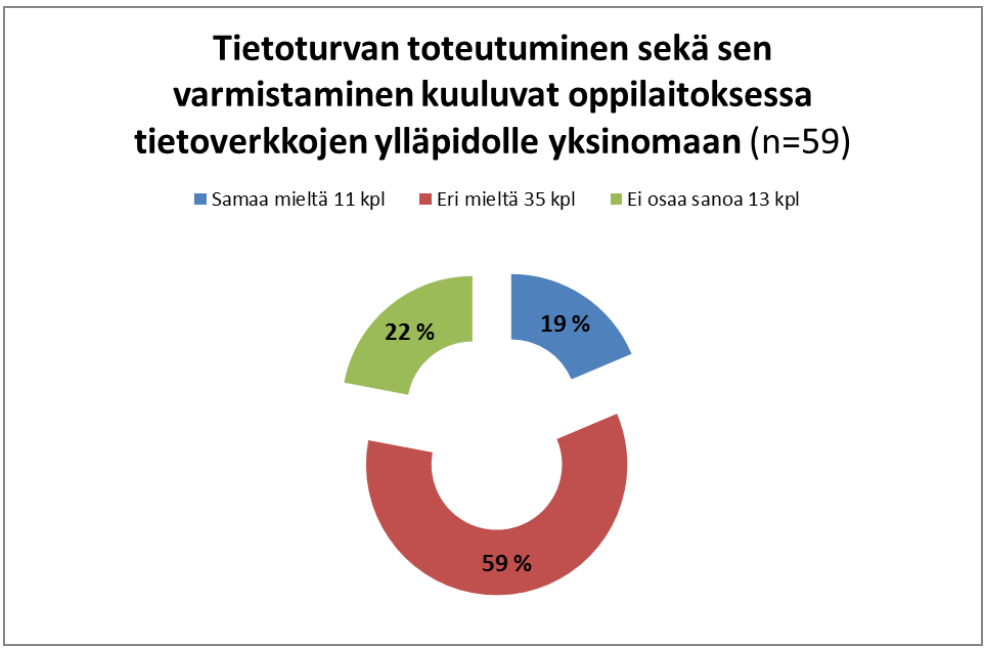
Oman koneen sisältämiä tiedostoja pidettiin hyvin arvossa. Kysymyksessä ei eroteltu tärkeiden tiedostojen laatua tai verrattu niiden tärkeysjärjestystä käyttäjälle. Kotikoneen luvaton käyttöönotto tai sen hyväksikäyttö ulkopuolisten tahojen käyttötarkoituksiin huoletti 85 %:a vastanneista. Vain 8 % vastanneista oli samaa mieltä väittämän kanssa. 7 % ei osannut sanoa mielipidettään.



Kuva 17. Kotikoneen suojeleminen ulkopuolisilta tahoilta

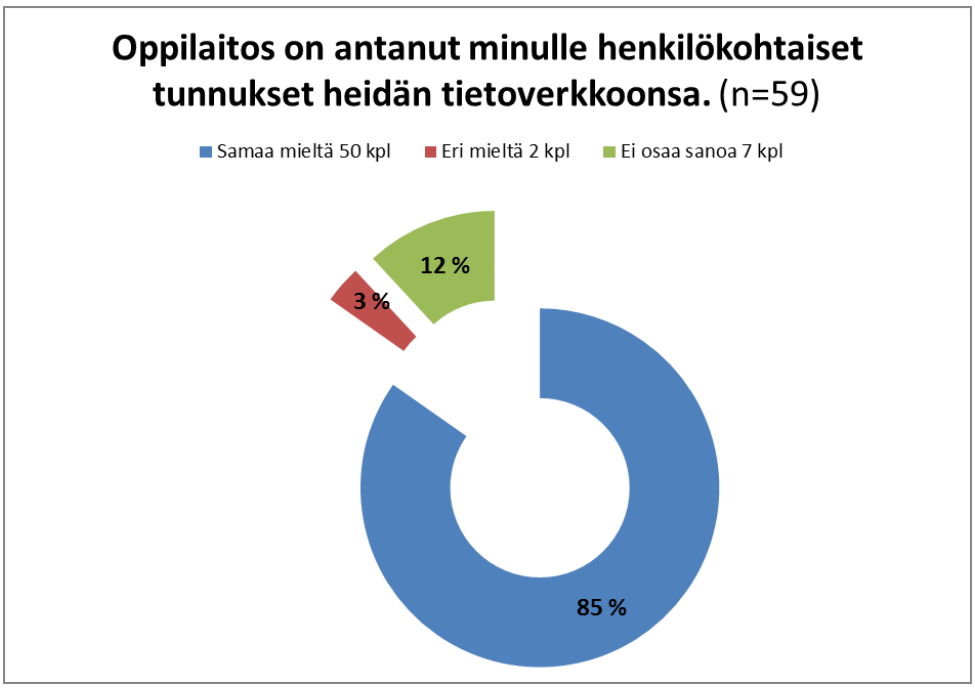
Kymenlaakson ammattikorkeakoulu on laatinut oppilaiden ja opettajien käyttöön omat tietoturvaohjeet. Kysymys numero 15 pyrki selvittämään oppilaiden tietoisuuden näistä ohjeista sekä sen, ovatko he tutustuneet tähän ohjeeseen. 31 % vastanneista ilmoitti lukeneensa ohjeistuksen. 5 % ei osanneet sanoa kysymykseen vastausta. 64 % ilmoitti, että ei ole tutustunut ohjeeseen.

Tietoturvan toteutumisen sekä sen varmistamisen vastuuta kysyttäessä vastaajista vain 19 % oli sitä mieltä, että se kuuluu yksinomaan oppilaitoksen vastuulle. Vastuu kuuluu tästä kaikille tietoverkon tai tietokoneen käyttäjille itselle. Tietoverkkojemme käyttäjät luovat tietoturvan organisaatioiden verkkoympäristöissä sekä kotonaan heidän omalla tietoturvakäyttäytymisellään. 59 % kyselyyn vastanneista oli asiasta samaa mieltä.



Kuva 18. Tietoturvan vastuu

Oppilaitoksen antamat henkilökohtaiset käyttäjätunnukset heidän tietoverkkoonsa ymmärrettiin hyvin. 85 % vastanneista tiedosti asian. 3 % oli väittämän kanssa eri mieltä ja 7 % vastanneista ei osannut sanoa mielipidettään.



Kuva 19. Henkilökohtainen käyttäjätunnus

6.4 Tietoturvaopetukseen liittyvät opiskelijoiden toiveet

Vapaamuotoiseen kenttään, jossa tiedusteltiin tietoturvaan liittyviä asioita, joita toivoisi käsiteltävän lisää opintojen aikana, tuli kaikkiaan kahdeksan vastausta. Näissä vastauksissa oli toiveita. Lopuissa kolmessa ei vastannut henkilö tarvinnut mitään lisätietoa tietoturvasta tai todettiin, että koulun alussa saadaan tärkeimmistä tietoturvaasioista tietoisku ja koulun atk-tuelta voi kysyä lisätietoja tarvittaessa.

Kahdeksan toivetta:

• "Lisätietoa erilaisista virustorjuntamahdollisuuksista, sekä siitä mitä ne käytännössä tarkoittavat ja toimivat, eikä vain paperiversiona."

• "Semmosesta normaalin ihmisen arjen käytön tietoturvasta_ suomenkielellä ei millään tietotekniikan kielellä. Ei oo mitää havaintoa, että mitä ohjelmia omalla läppärillä tulisi olla tai miten niitä päivitettään. Sen jälkee ku läppärin on hakenu kaupasta ja"

• "yleistä termistöä tietokoneesta"

• "Lisää pitäisi painottaa tietoturvan tärkeyttä."

• "ihan peruskäsitteet voisi avata, juuri esim palomuuri, virustorjunta yms"

• "Varmuuskopiointiin liittyviä"

• "Sellaiset välttämättömän tärkeät tieoturva ohjeet, jotka on helppo muistaa ja ymmärtää ja jotka tällänen tavallinen koneen käyttäjä osaa ottaa käyttöön."

• "Ei niinkään tietokoneen tietoturvaa koskevia asioita, koska oletan niiden tulevan koulun puolesta, mutta omien tiedostojen säästämiseksi voisi kertoa joitain vinkkejä. Tosin, eipä siihenkää oo muuta vaihtoehtoo ku varmuuskopiot."

6.5 Yhteenveto tutkimustuloksista

Tutkimukseen osallistuneiden terveysalan opiskelijoiden tietotekniikan käyttömäärä oli korkeaa luokkaa. Vastanneista 97 % opiskelijoista voidaan pitää tietotekniikan tehokäyttäjinä. Samoin oma hallinta tietoturvan merkityksestä koti ja työyhteisöissä oli myös 76 %:n mielestä hallinnassa. Sama 76 % vastanneista kertoi ymmärtävänsä suojausmenetelmien merkityksen tietotekniikassa. Tunne tietoturvan hallinnasta on korkeaa luokkaa opiskelijoilla.

Terveysalan oppilaille tehdyn kyselyn perusteella todellista tietoturvakäytäntöä mittaavat kysymykset antoivat poikkeavaa näyttöä oppilaiden osaamisesta verrattuna heidän tuntemuksiinsa osaamisestaan. Kysyttäessä virustorjunnan riittävyyttä tiedostojen suojana tietokoneissa jakoi tämä puoliksi vastaukset: 44 % piti tätä riittävänä tai melko riittävän menetelmänä suojaamaan tiedostojaan, toiset 44 % opiskelijoista oli eri mieltä ja 12 % ei osannut sanoa mielipidettään. Todellisuudessa tämä ei ole riittävä suoja koneelle, mikäli kone on yhteydessä verkkoon tai siihen liitetään jokin ulkoinen tallennusmedia.

Terveysalan oppilaille tehdyn kyselyn perusteella palomuurin suojaamisen merkitys oli 78 %:sti hallinnassa. Sen varmasti omisti koneillaan 85 % terveysalan opiskelijoista. Tätä voidaan pitää rehellisenä tuloksena, mutta ei riittävän suojauksen kannalta.

Terveysalan oppilailta käyttöjärjestelmän merkitystä sekä sen päivitystä kyseltäessä tulokset olivat yhdenmukaisia. 61 % opiskelijoista tiedosti oikein käyttöjärjestelmän merkityksen tietokoneilla. 83 % vastaajista päivitti käyttöjärjestelmäänsä jollain tasolla. Vastaajat käyttivät sekä automaattipäivitysmenetelmää että manuaalista päivitystä, aina kun muistavat. Tuloksista selvästi luettavissa, mikäli opiskelijalla ei ollut tietoa asiasta, ei myöskään käytännön toteutusta ollut aiheesta.

Ulkoisten tallenteiden tarkastaminen viruksien varalta oli 8 %:lla opiskelijoista automaattinen käytäntö, 25 % tarkisti ulkoiset tallennusmediat jokseenkin aina. 52 % opiskelijoista ei tarkistanut tallennusmedioitaan ja 14 % ei osannut muodostaa mielipidettä. Nämä prosenttiluvut osoittavat hyvää pyrkimystä tietoturvallisuuden takaamiseksi, mutta eivät riitä ylläpitämään riittävää turvaa ulkopuolelta tulevien virusten ja haittaohjelmien torjumiseksi. Suuremmissa tutkimuksissa käy selville, että automaat-

tinen median käyttöönoton laukaisu on suuri uhka viruksien ja haittaohjelmien leviämiselle.

Varmuuskopiointi eli ennakointi ongelmatilanteen ratkaisemiseksi oli vain 47 %:lla terveysalan opiskelijoista käytössä. TeliaSonera Finland sekä Ground Communicationsin tutkimuksessa vastaava prosentti oli vain 23 %. Tutkimuksen tulokset olivat hyvät tähän verrattuna, mutta kuitenkin osoitus siitä, että opiskelijoilta puuttuu tietoa tai että he ovat vain välinpitämättömiä. Ennalta varautuminen ongelmatilanteisiin on kuitenkin halvin ja tehokkain keino turvata tietonsa. Tämän asian opettamiseen oppilaille tulisi kiinnittää enemmän huomiota.

TeliaSonera Finland sekä Ground Communicationsin tutkimuksesta on tutkija pyytänyt luvan tulosten vertailemiseen, mutta aineisto ei ole julkinen. Siksi en niitä tässä tutkimuksessa julkaise erikseen. Keskeiset tulokset tutkimuksesta Soneran on julkaissut Internet sivuillaan osoitteessa: http://uutishuone.sonera.fi/2012/01/26/varmuuskopiointi-ja-salasanojen-vaihtaminen-ei-kiinnosta-suomalaisia/.

Terveysalan opiskelijoiden mielipiteet tietoturvan vastuusta vakiintuivat kahteen yhtä suureen osaan. Kyselyn väittämässä vastuu vieritettiin pelkästään tietoverkkojen ylläpidolle. 19 % oppilaista oli samaa mieltä ja 22 % ei osannut muodostaa mielipidettä. Tämä kertoo vahvasti siitä, että itse tietoturvasta ja sen muodostumisesta ei tiedetä tarpeeksi. Teorian mukaan vain 20 % tietoturvasta on tekniikkaa ja loput tietoturvasta muodostuu käyttäjästä ja hänen toiminnastaan.

Terveysalan opiskelijat olivat salasanojen käytön suhteen odotusten mukaisia. Niiden vaihtoa harrastettiin verrattain vähän. Vain 20 % ilmoitti vaihtavansa niitä säännöllisin väliajoin. Vastanneista 69 % ilmoitti käyttävänsä erilaisia salasanoja eri verkkopalveluiden kesken. Vastanneista 95 % ei luovuta mikrotukihenkilölle tai kaverille pyynnöstäkään henkilökohtaisia salasanojaan. Näyttäisi siltä, että käyttäjätunnuksen ja salasanojen henkilökohtainen käyttö on mennyt opetuksena erittäin hyvin oppilaiden tietoisuuteen. Edes mikrotukihenkilönä itseään esittelevä henkilö ei tulisi heiltä näitä tunnuksia ja salasanoja saamaan.

Työaseman käytön päätyttyä sieltä kirjautuu ulos 98 % opiskelijoista. Mikäli työasemalta poistutaan hetkeksi ja sen käyttö lopetetaan väliaikaisesti, ulos kirjautuu vain

enää 58 % käyttäjistä. Tässä tilanteessa voi tietenkin lukita käyttäjätunnuksensa eikä kirjautua kokonaan ulos käyttöjärjestelmästä. Lopputulos on sama kuin jos halutaan suojata oma henkilökohtainen käyttäjätunnus toisen henkilön käytöltä. Koneen väliaikaisen käytön loputtua, tulisi opiskelijan kiinnittää vielä tarkemmin huomiota koneen lukitsemisessa. Kun tämä käytäntö jää opiskelijan mieleen, tulee tämä hänelle toimintatavaksi. Näin pysyy tieto niiden tahojen hallinnassa kenelle se kuuluu, myös myöhemmin työelämässäkin

Viimeisessä kysymyksessä, tiedusteltiin terveysalan opiskelijoiden omia toiveita tietoturvakoulutuksen osalta. Vapaissa kommenteissa tuli esille terveydenhuollon opiskelijoiden halu saada selkokielisiä tietoturvaohjeita. Perinteiset virustorjunta ja varmuuskopiointi herättivät mielenkiintoa opiskelijoiden keskuudessa. Kirjoista saa tietotekniikan tietoa, mutta opiskelijat kaipaavat konkreettisia esimerkkejä käytännöstä ja henkilökohtaisia neuvoja.

7 POHDINTA

7.1 Tutkimustulosten tarkastelu

Aiemmissa vastaavissa tutkimuksissa samat ilmiöt ovat tulleet esille. Toni Korhosen 2009 tekemän pro gradu -tutkielman mukaan vastanneista 68 % piti tietojaan ja taitojaan hyvänä tai erittäin hyvänä, n=197. Kuitenkin vastanneista 45 % oli saanut koulutusta tietoturvasta työssäoloaikanaan. Vastanneilla esiintyi epätietoisuutta niin tietoturvan perusteissa kuin tietoturvalainsäädännössä. Tulokset antoivat selkeän näytön siitä, että tietoturvakoulutusta saaneet osasivat paremmin kuin koulutusta vaille jääneet. (Korhonen T, 2009.)

Verrattaessa Toni Korhosen pro gradu -tutkielmaa ja nyt tätä tekemääni tutkimusta Toni Korhosen tutkimukseen osallistuneet osasivat hiukan huonommin tietoturvan perusteita kuin Kymenlaakson ammattikorkeakoulun. terveysalan opiskelijat.

Anu Laukkasen 2008 pro gradu -tutkielman mukaan, vastanneet n=219 ymmärsivät tietoturvallisuuden merkityksen omassa työssään 100 %:sti. Enemmistö 86 % oli sitä mieltä, että aiheesta tulisi keskustella enemmän työyksikössä. Riittävästi tietotekniikkakoulutusta oli saanut 73 % vastaajista. 89 % halusi lisää koulutusta tietotekniikan käyttötaitoihin. Yleisesti haluttiin lisää tietoturvakoulutusta. Käytännön tietoturvasuo-

ritteista kysyttäessä 47 % vastanneista tarkasti aina erilliset tallennusvälineet virusten varalta. Käyttäjätunnusten ja salasanojen merkitys oli ymmärretty. Anu Laukkasen Pro gradu -tutkielmassa käyttäjätunnusten ja salasanojen merkitys tutkittaville oli samaa luokkaa kuin nyt tässä terveydenhuollon opiskelijoita koskevassa tutkimuksessa. Vain 3 % vastanneista luovuttaisi tunnukset muiden käyttöön. Koneelta uloskirjautuminen sen käytön loputtua oli myös samaa luokkaa kuin terveydenhoidon oppilailla eli 96 %. Perustason tietoturvatietämys oli myös melko hyvää luokkaa. Erot tulivat esille, kun lainsäädännön asettamia vaatimuksia kyseltiin. Työyksiköiden tietoturvaohjeisiin sekä tietoturvastrategiaan oli vain osa vastanneista tutustunut. Niiden olinpaikasta ja sisällöstä kaivattiin lisää keskustelua ja tietoutta työyksiköissä. Sama ilmeni myös terveysalan oppilaille teetetyssä kyselyssä tietoturvaohjeiden osalta. (Laukkanen A, 2008)

TeliaSonera Finland ja Ground Communications antoivat Taloustutkimus Oy:lle toimeksiannon mitata kyselytutkimuksena suomalaisten huolestumista omasta digitaalisen omaisuuden turvallisuudesta. Tutkimuksessa mitattiin siihen käytettäviä palveluita sekä eri keinoja. Tutkimuksen kohderyhmänä olivat 18 – 79-vuotiaat suomalaiset. Hyväksytysti kyselyyn vastasi N=1519, joilla oli taloudessa tietokone. Tämä tutkimus valmistui 2.1.2012. Tutkimuksessa 92 % tietokoneen käyttäjistä käytti virustorjuntaa. Loput käyttäjistä elivät väärässä uskossa Linux- tai Mac -käyttöjärjestelmänsä haavoittumattomuuden kanssa. Uskottiin, että alustoille ei ole kirjoitettu viruksia. (Korpela 2005, 63 - 66; Microsoft Security Intelligence Report 2012.)

Oppilaitoksen omiin käyttäjän tietoturvaohjeisiin oli tutustunut oletetusti vain 31 % opiskelijoista. Syynä voi olla tiedonpuute ohjeiden olemassaolosta. Tutkijalle nämä tulivat myös vahingossa vastaan oppilaitoksen www-sivuilta. Ohjeet olivat ajan tasalla. Ne olivat hyvin selkeät ja niissä oli tiivistetty tärkeimmät asiat. Tulokset ovat hyvin samansuuntaisia kuin Anu Laukkasen pro gradu -tutkielmassa sekä Toni Korhosen pro gradu -tutkielmassa (Laukkanen, 2008; Korhonen, 2009).

Tuloksia tarkastellessa kokonaisuutena voidaan koko tutkimuksessa todeta, että ne osa-alueet mistä ei terveysalan oppilailla ollut tarpeeksi tietoa eivät myöskään siltä osin toteutuneet käytännössä. Sanomattakin on selvää, että mikäli ihminen ei tiedä jostakin asiasta tarpeeksi, ei hän pysty myöskään toteuttamaan tätä työyhteisöjen odotusten mukaisesti. Tämä tosiseikka pätee myös perustason tietoturvan osalta. Riittävä

koulutus on ainoa näkemäni ratkaisu tämän asian parantamiseksi. Koulutuksen tulee jatkua myös työelämässä säännöllisin väliajoin, koska ohjelmistot, laitteet sekä tietoturva lainsäädäntö päivittyvät kovaa vauhtia. Näistä nopeinten päivittyvät terveydenhoidossa käytetyt tietojärjestelmät. Sairaanhoitajan on kyettävä työssään hoitamaan potilasta sekä häntä koskevia tietoja samalla huolellisuudella.

Käytännössä tänä päivänä tietojen kirjaaminen sekä niiden asianmukainen arkistointi ovat sairaanhoitajan oman oikeusturvan kannalta tärkeitä asioita. Sanotaan, että jälkeenpäin tarkasteltuna sitä, mitä ei ole kirjattu, ei myöskään ole tehty. Potilasta koskeva tieto on yhtä tärkeä kuin potilas itse hoitotyössä. Tätä tietoa tulee suojella, siksi perusteet tietoturvalle ovat erittäin tärkeitä sairaanhoitajalle.

7.2 Luotettavuus ja eettisyys

Kaikissa tutkimuksissa arvioidaan myös tutkimuksen luotettavuutta. Sitä voidaan arvioida useiden eri mittaus- ja tutkimustapojen avulla. Tämän tutkimuksen luotettavuutta arvioidaan reliabiliteetin ja validiteetin näkökulmista. (Hirsjärvi ym. 2010, 231.) Validiteetti tarkoittaa pätevyyttä ja reliabiliteetti luotettavuutta (Vilkka, 2005, 150).

Tästä tutkimuksesta ei voi tehdä mitään tilastollista yleistytystä. Tämä on tekijän ensimmäinen tutkimus, joka vähentää tutkimuksen luotettavuutta teknisessä mielessä. Kato vastauksissa on sangen suuri. Tämä oli oletettavissa, sillä niin tapahtuu kaikissa verkkokyselyissä. Puutteistaan huolimatta tutkimuksesta käy ilmi pienen joukon tietoturvakäsityksiä sekä heidän tietoturvan käytännöntason suorituksiaan. Tämä tutkimus on tuottanut samansuuntaisia tuloksia, joita on saatu tähän verrattavista aikaisemmista tutkimuksista.

Reliaabeliudella tarkoitetaan mittaustulosten toistettavuutta. Esimerkiksi kahden arvioijan päätyessä samaan tulokseen voidaan tulosta pitää reliaabelina. Samoin, jos samalla henkilöllä mitataan eri tutkimuskerroilla sama tulos, on se silloin reliaabeli. (Hirsjärvi ym. 2010, 231.)

Validiteetti tarkoittaa mittarin tai tutkimusmenetelmän kykyä mitata juuri sitä, mitä on tarkoitus mitata. Esimerkiksi kyselylomakkeen kysymyksiin saadaan vastaukset, mutta vastaajat ovat saattaneet käsittää kysymykset aivan toisin kuin tutkija on ajatellut.

Jos tutkija käsittelee saatuja tuloksia edelleen alkuperäisen oman ajatusmallinsa mukaisesti, ei tuloksia voida pitää luotettavina. (Hirsjärvi ym. 2010, 231–232.) Tässä tutkimuksessa kysymykset perustuvat tietoturvateoriaan, tulosten tarkastelu perustuu ja saatuja tutkimustuloksia on verrattu muihin vastaavan kaltaisiin tutkimuksiin.

Hyvät eettiset periaatteet edellyttävät sen että tutkimustuloksia ei kirjata yksilöittäin. Yksittäistä henkilöä ei saa tunnistaa. Tutkimustulosten sanallisessa esittämisessä tulee huomioida, ettei ilmaisutyyli ole loukkaavaa. Sen ei tule leimata tutkimusryhmää mitenkään. Lähteiden merkitsemisessä tulee olla huolellinen. Kun tutkija analysoi ja tulkitsee toisen tutkijan työtä, hän ei hänen saa muuttaa tai vähätellä toisen tutkimustuloksia. (Vilkka 2005, 164 - 166.)

Kyselyt on lähetetty tutkittaville sähköpostin välityksellä saatekirjeen kera. Kysymykset tai annetut vastaukset eivät pysty yksilöimään vastaajia eivätkä loukkaa tutkittavaa joukkoa. Tutkimuksessa on kautta linjan neutraali sävy tutkittavaa joukkoa sekä toisia tutkimuksia kohtaan.

7.3 Tulosten hyödynnettävyys

Tutkimustuloksia vodaan käyttää hyväksi laadittaessa uutta opetussuunnitelmaa ammattikorkeakoulun terveysalan opiskelijoille. Tunne tietoturvaosaamisesta oli selvästi korkeampi kuin käytännön suoritteiden hallinta. Toiveita, joita tässä tutkimuksessa tuli opiskelijoilta tietoturvaopetuksen suhteen, tulisi kuunnella.

Tämä aihe on vasta tulemassa julkiseen keskusteluun. Palvelunestohyökkäykset kohdistuvat nyt meidän maaperällemme myös Suomessa. Hyökätään esimerkiksi julkisten uutissivustojen kimppuun ja kaadetaan tahallisesti niiden toiminta. Tähän käytetään luvattomasti huonosti suojattuja tietokoneita ympäri maan. Hyökkäyksien alkuperää on vaikea jäljittää (Kymen Sanomat 2012a) Haittaohjelmilla vakoillaan kotiemme yksityisyyttä. Tekniikkana on käytetty ihmisten hyväuskoisuutta sekä sellaista ikäryhmää, jolla ei vielä ole elämänkokemuksen suomaa harkintakykyä. (Kymen Sanomat 2012b)

Suomessa sisäministeriö on maaliskuussa 2011 antanut puolustusministeriölle tehtäväksi laatia koko yhteiskuntaa palveleva kansallisen kyberturvallisuusstrategia. Tällaiseen ei varmasti olisi ilman havaittavaa uhkaa syytä ryhtyä tällaisena aikana, jolloin

talous on heikoimmillaan ja jolloin säästötarve on ilmeinen. (Sisäministeriö, Turvallisuus, Tietoverkkorikollisuus.) Sosiaalinen media hallitsee valtaosan suomalaisen elämää. Siellä esiintyy aivan uudenlaista rikollisuutta, johon emme ole aiemmin tottuneet, emmekä osaa siihen varautua. Keskusrikospoliisi on herännyt hyvin tilanteeseen. Se on luonut myös käytännön ohjeistuksia niin nuorille kuin vanhemmille, jotta he osaavat varoa tietotekniikkarikollisuutta. (Poliisi, Nettirikosten Pohdintaa.)

Tutkimuksen teoriaosa on läpileikkaus tietoturvan perusteista, jonka päälle on mahdollista kasvattaa ja lisätä tietoa. Teoriaosa antaa ajanmukaista tietoa tietoturvan perusteista. Terveydenhuollon työntekijän on osattava ja tiedettävä laajasti asioita monesta elämänosa-alueesta. Tietoturva osa-alue lainsäädäntöineen muodostuu lähes kaikki työntekijän omasta tietämyksestä sekä käytännön ratkaisuista. Työyhteisöiden tietoverkoissa on laadittu omat säännöt, nämä tulisi kaikkien käyttäjien tietää. Käyttäjän oma tietoturvakäyttäytyminen alkaa jo kotikoneelta. Urheilussa on sanonta ”niin pelaat kuin harjoittelet”. Tämä kuvaa hyvin myös tietoturvakäyttäytymistä. Teknisin ratkaisuin tietoverkkojen ylläpito pystyy tekemään vain pienen osan turvatakseen tietoverkkoja niiden väärinkäytöksiltä tai ylläpitämään tietoturvaa sen sisällä. Jatkuva työntekijän kouluttaminen on ratkaisu pitää yllä heidän tietouttaan tietoturvasta. Jatkotutkimuksena voisi tutkia tässä tutkimuksessa mukana olleiden terveydenhuollon opiskelijoiden saamaa tietoturvakoulutusta työelämään sijoittumisensa jälkeen.

Itselleni tieteellinen tutkimus antoi varmistusta ja vahvistusta tietoturvateoriasta. Tämä laajensi omaa tietouttani tietoturvatietämyksestäni.

Internet, joka aluksi oli pienen eliitin hupi, on noussut koko kansakuntamme pelikentäksi. Ei voi olla liian epäileväinen liikkuessaan maailmanlaajuisessa verkossa. Psykiatrisen vankisairaalan ylilääkäri Hannu Lauerma valotti keinoja miten siellä huijataan STT:lle antamassaan haastattelussa, jonka mm. Aamulehti uutisoi. Hän luonnehtii ihmisiä luottavaisiksi. Hänen mukaansa luottamuksellisuuden välttämättömyys yhteiskunnassa tuo aina mahdollisuuden törmätä tätä hyväksikäyttävään henkilöön. Ihmisten tunteisiin voidaan vedota. Ihminen on pohjimmiltaan toiveajattelija, joka haluaa uskoa esimerkiksi ystävän lähettäneen 15 € nettipelisivustolle käytettäväksi. Lauermanin mukaansa uusissa huijausmenetelmissä voi nähdä yhtymäkohtia vanhoihin menetelmiin. Ihminen hahmottaa huonosti todennäköisyyksiä, suuria ja pieniä lukuja. Huijareiden omaatuntoa tämä ei paina, he ajattelevat että tyhmän ihmisen ei tule omistaa

rahaa. Näiden seikkojen johdosta hän pitääkin Internetiä täydellisenä alustana huijaamiselle. Siellä nimettömänä esiintyminen vailla kasvoja on mahdollista. Lopuksi Lauerman kuitenkin painottaa, että yletön epäluulo sosiaalisessa kanssakäymisessä kasvokkain ei ole hyvästä (Lauerman 2012.)

LÄHTEET

Anttila, P.1996. Tutkimisen taito ja tiedon hankinta. Helsinki: Akatiimi Oy.

CERTI-FI. Viestintävirastossa toimiva tietoturvaviranomaisen internetsivut. Saatavissa: http://www.cert.fi/index.html. [viitattu: 6.1.2012].

FBI. Quik facts. FBI:n internetsivut. Saatavissa: http://www.fbi.gov/about-us/quick-facts. [Viitattu 1.2.2012].

Hakala, M., Vainio, M. & Vuorinen, O. 2006. Tietoturvallisuuden Käsikirja. Docendo Finland Oy. Jyväskylä.

Henkilötietolaki, 7. luku 32. §, Finlex. 22.4.1999/523. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990523. [Viitattu 28.1.2013].

Hirsjärvi, S., Remes, P., Sajavaara, P. 2003. Tutki ja kirjoita. Dark Oy. Vantaa.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2009. Tutki ja kirjoita. 15. uudistettu painos. Helsinki: Tammi.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2010. Tutki ja kirjoita. 15. - 16.. uudistettu painos. Helsinki: Tammi.

Järvinen, P. 2010. Yksityisyys. Turvaa digitaalinen kotirauhasi. WSOYpro Oy. Jyväskylä.

Järvinen, P. 2005 Salausmenetelmät. Dark Oy. Vantaa.

Järvinen, P. 2002 Tietoturva & yksityisyys. Docendo Finland Oy. Jyväskylä.

KOPPA, Jyväskylän yliopisto. Saatavissa: https://koppa.jyu.fi/avoimet/mit/virtuaalisetoppimisympaeristoet/oppimisympaeristoejen-tietoturva/tietoturvariskit. [Viitattu 4.12.2012].

Korhonen T, 2009. Terveydenhuollon henkilöstön tietoturvaosaaminen. Pro gradu -tutkielma. Kuopion yliopisto.

Korpela K, 2005. Turvallisesti netissä. Docendo Finland Oy. Jyväskylä.

Kymenlaakson ammattikorkeakoulu, Käyttäjän Tietoturvaohje. Saatavissa: http://www.kyamk.fi/Intra%20opiskelija/Opinnot%20ja%20oppaat/Turvallisuus/Tietoturvaohjeita. [Viitattu 12.12.2012].

Kymen Sanomat 2012a, Nettihyökkäysten Alkuperää Vaikea Selvittää, uutiset, 26.12.2012. Saatavissa: http://www.kymensanomat.fi/Online/2012/12/26/Nettihy%C3%B6kk%C3%A4ysten+alkuper%C3%A4%C3%A4+vaikea+selvitt%C3%A4%C3%A4/2012314922859/4. [Viitattu: 26.12.2012].

Kymen Sanomat 2012b, Netissä Nuoria Naisia Vakoillut Hakkeri Syytteisiin, uutiset, 13.12.2012. Saatavissa: http://www.kymensanomat.fi/Online/2012/12/13/Netiss%C3%A4+nuoria+naisia+vakoillut+hakkeri+syytteisiin/2012314837436/4. [Viitattu: 26.12.2012].

Laki viranomaisten toiminnan julkisuudesta 5. luku 18. §, Finlex. 21.5.1999/621. Saatavissa: http://www.finlex.fi/fi/laki/ajantasa/1999/19990621. [Viitattu 28.1.2013].

Lauerman H, 2012, Psykiatri: Tästä syystä sinunkin huijaamisesi on helppoa - Viisi yleisintä tapaa 28.1.13, Aamulehti, uutiset. Saatavissa: http://www.aamulehti.fi/Kotimaa/1194785506366/artikkeli/tasta+syysta+sinunkin+huijaamisesi+on+helppoa+-+viisi+yleisinta+tapaa.html. [Viitattu: 28.1.2013].

Laukkanen A, 2008. Hoitohenkilöstön Tietoturvatietoisuus ja Tietoturvaosaaminen. Pro gradu -tutkielma. Kuopion yliopisto.

Luoto, R 2009. Lääketieteellinen Aikakausikirja, Duomecim, nro 15/2009. Saatavissa: http://www.duodecimlehti.fi/web/guest/etusivu?p_p_id=dlehtihaku_view_article_WAR_dlehtihaku&p_p_action=1&p_p_state=maximized&p_p_mode=view&_dlehtihaku_view_article_WAR_dlehtihaku__spage=%2Fportlet_action%2Fdlehtihakuartikkeli%2Fviewarticle%2Faction&_dlehtihaku_view_article_WAR_dlehtihaku_tunnus=duo98221&_dlehtihaku_view_article_WAR_dlehtihaku_p_frompage=uusinnumero. [Viitattu 25.12.2012].

Poliisi, Huijauksen Monet Muodot. Saatavissa: http://www.poliisi.fi/poliisi/krp/home.nsf/pages/5aba1cd4b1d3b896c22570fb0057ca71. [Viitattu: 26.12.2012].

Poliisi, Nettirikosten Pohdintaa. Saatavissa: http://www.poliisi.fi/poliisi/helsinki/home.nsf/files/Nettirikosten%20pohdintaa/$file/Nettirikosten%20pohdintaa.pdf. [viitattu: 26.12.2012].

Microsoft, Microsoft Security Intelligence Report (SIR). Saatavissa: http://www.microsoft.com/security/sir/default.aspx. [viitattu 7.12.2012].

Microsoft, Safety & Security Center, Internet safety essentials for home and school. Saatavissa: http://www.microsoft.com/security/resources/home.aspx. [viitattu: 7.12.2012].

Microsoft, Safety & Security Center, How to boost your malware defense and protect your PC. Saatavissa: http://www.microsoft.com/security/pc-security/protect-pc.aspx#Build. [viitattu: 7.12.2012].

Microsoft, Safety & Security Center, Spyware protection with Microsoft Security Essentials. Saatavissa: http://www.microsoft.com/security/pc-security/mse.aspx. [Viitattu: 7.12.2012].

Microsoft, Safety & Security Center, Family Safety. Saatavissa: http://www.microsoft.com/security/family-safety/default.aspx#Social-media. [Viitattu: 7.12.2012].

Microsoft, Windows 7 consumer security software providers. Saatavissa: http://www.microsoft.com/windows/antivirus-partners/windows-7.aspx. [Viitattu: 7.12.2012].

Microsoft, Safety & Security Center, What is a firewall? Saatavissa: http://www.microsoft.com/security/pc-security/firewalls-whatis.aspx. [Viitattu: 12.12.2012].

Microsoft Tuotetuki, Automaattisen Käynnistyksen Poistaminen Käytöstä Windowsissa. Saatavissa: http://support.microsoft.com/kb/967715. [Viitattu 26.12.2012].

Salminen, H. 1998. Internetin historiaa. CSC:een internetsivut. Saatavissa: http://www.nic.funet.fi/index/FUNET/history/internet/fi/etusivu.html. [Viitattu 8.1.2013].

Sisäministeriö, Turvallisuus, Tietoverkkorikollisuus. Saatavissa: http://www.intermin.fi/fi/turvallisuus/rikostorjunta/tietoverkkorikollisuus. [Viitattu: 26.12.2012].

Thomas, T. 2005 Verkkojen tietoturva. Edita Publishing Oy, Helsinki.

Valtiovarainministeriö 2013a. Ministeriö. Valtiovarainministeriön kotisivut. Saatavissa: http://www.vm.fi/vm/fi/02_ministerio/index.jsp. [viitattu 8.1.2013].

Valtiovarainministeriö 2013b. Tietoturvallisuus. Valtiovarainministeriön kotisivut. Saatavissa: http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp. [viitattu 8.1.2013].

Valtiovarainministeriö 2013c. Voimassa olevat tietoturvaohjeet ja – määräykset, Teknisen ICT-ympäristön tietoturvataso-ohje, VAHTI 3/2012. Valtiovarainministeriön kotisivut. Saatavissa: http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp. [Viitattu 8.1.2013].

Valtiovarainministeriö 2013d. Voimassa olevat tietoturvaohjeet ja – määräykset, Henkilöstön tietoturvaohje, VAHTI 10/2006. Valtiovarainministeriön kotisivut. Saatavissa: http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/02_tietoturvaohjeet_ja_maaraykset/index.jsp. [Viitattu 8.1.2013].

Vilkka, H. 2005. Tutki ja kehitä. Helsinki: Tammi.

Vilkka, H. 2007. Tutki ja mittaa. Määrällisen tutkimuksen perusteet. Helsinki: Tammi.

Windows Microsoft.com, Support, Performance, Back up your files. Saatavissa: http://windows.microsoft.com/en-US/windows7/Back-up-your-files. [Viitattu 13.12.2012].

WSOY iso tietosanakirja, 9, Sp-T 1997. Tiedonhaku. yleiset tietoteokset.

Kymenlaakson ammattikorkeakoulu
University of Applied Sciences

SOPIMUS OPINNÄYTETYÖSTÄ

Lomake 026
id 26750

OPISKELIJA

Opiskelijanumero	Viralliset etunimet
0901186	Antti Olavi
Sukunimi	
Tiittanen	
Lähiosoite	Postinumero ja -toimipaikka
Lukkarinkatu 11 A 1	48700 Kotka
Sähköposti	Puhelin
antti.tiittanen@student.kyamk.fi	04[illegible]
Toimipiste ja koulutusohjelma	
Jylpyn toimipiste, Hoitotyön ko.	
Suuntautumisvaihtoehto ja ryhmätunnus	
Sairaanhoitaja AMK	

TOIMEKSIANTAJA

Toimeksiantaja ja yritys/yhteisö	Yrityksen/yhteisön yhteyshenkilö
Kymenlaakson ammattikorkeakoulu	Päivi Mäenpää
Lähiosoite	Postinumero ja -toimipaikka
Takojantie 1	48220 Kotka
Sähköposti	Puhelin
paivi.maenpaa@kyamk.fi	[illegible]

OPINNÄYTETYÖN HANKKEISTUS

- ☐ Toimeksiantaja maksaa opinnäytetyöstä opiskelijalle tai ammattikorkeakoululle korvauksen, josta on kirjallisesti sovittu ennen opinnäytetyön aloittamista.
- ☒ Opinnäytetyöllä on toimeksiantajan puolelta nimetty ohjaaja ennen opinnäytetyön aloittamista.
- ☐ Toimeksiantajan tarkoituksena on alusta lähtien hyödyntää opinnäytetyön tuloksia toiminnassaan.

OPINNÄYTETYÖN OHJAUS

Ohjaava(t) opettaja(t)
Anttonen Satu
Sähköposti
satu.anttonen@kyamk.fi
Yrityksen/yhteisön ohjaaja(t)
Sähköposti

Kymenlaakson ammattikorkeakoulu
University of Applied Sciences

SOPIMUS OPINNÄYTETYÖSTÄ

Lomake 026
id 26750

OPINNÄYTETYÖ

Opinnäytetyön aihe (max. 200 merkkiä) Terveysalan opiskelijoiden käsitykset tietoturvasta ensimmäisen opiskeluvuoden jälkeen
Kehittämis- tai tutkimustavoite ja toimeksianto (max. 300 merkkiä) Tutkimuksen tarkoitus on selvittää tietoturvan merkityksen ymmärtäminen ja sen valmiuksia sekä toteutumista opiskelijan omassa toiminnassaan.
Keskeiset menetelmät (max. 300 merkkiä) Kvantitatiivinen eli määrällinen kyselytutkimus.

Opinnäytetyön aloitus	Opinnäytetyön luovutus toimeksiantajalle
1/2012	12/2012

Opinnäytetyö täyttää Tilastokeskuksen T & K määritelmän *) ☒ Kyllä ☐ Ei

*) T & K määritelmän saa opintotoimistosta tai Internetistä,
http://www.tilastokeskus.fi/til/tkke/kas.html

OPINNÄYTETYÖN SOPIMUSEHDOT

Opinnäytetyön ohjaus ja vastuu
Vastuu opinnäytetyön tekemisestä ja tuloksista on opiskelijalla. Kymenlaakson ammattikorkeakoulun vastuu rajoittuu opinnäytetyön tavanomaiseen ohjaukseen.
Toimeksiantaja sitoutuu antamaan opiskelijan käyttöön kaikki opinnäytetyön tekemisessä tarvittavat tiedot ja aineistot sekä ohjaamaan opinnäytetyötä toimeksiantajaorganisaation näkökulmasta.

Oikeudet tuloksiin ja muuhun opinnäytetyöhön liittyvään aineistoon, laitteisiin ja sovelluksiin.
Tekijänoikeus ja omistusoikeus opinnäytetyön tuloksiin kuuluvat opinnäytetyön tekijälle.
Toimeksiantaja saa käyttöoikeuden opinnäytetyön tuloksiin ja niiden kaupalliseen hyödyntämiseen ainoastaan sopimalla niistä erikseen opinnäytetyön tekijän kanssa.
Opinnäytetyön tekijä on velvollinen raportoimaan opinnäytetyön tulokset toimeksiantajalle.

Tulosten julkaiseminen ja luottamuksellisuus
Opinnäytetyö on kokonaisuudessaan julkinen. Mikäli opinnäytetyö sisältää liikesalaisuuksia tai muita julkisuuslaissa salassa pidettäväksi määrättyjä tietoja, on opinnäytetyön raportti laadittava niin, että tietojen luottamuksellisuus säilyy. Tarvittaessa salassa pidettävät tiedot on jätettävä työn tausta-aineistoon. Opinnäytetyö voidaan julkaista myös Internetissä.

Opinnäytetyön osapuolet (opiskelija, toimeksiantaja ja opinnäytetyön ohjaaja) sitoutuvat pitämään salassa kaikki opinnäytetyön tekemisessä ja sitä edeltävissä tai sen jälkeisissä neuvotteluissa esiin tulevat luottamukselliset tiedot ja asiakirjat sekä pidättäytymään käyttämästä hyväkseen toisen osapuolen ilmaisemia luottamuksellisia tietoja ilman erillistä lupaa.

Opinnäytetyön kustannukset ja niiden korvaaminen
Opinnäytetyöstä mahdollisesti aiheutuvien kustannusten (ml. aineistojen hankinta, raaka-aineet, matkat, työkorvaus jne.) korvaamiseta sopivat toimeksiantaja ja opiskelija keskenään. Pääsääntöisesti Kymenlaakson ammattikorkeakoulu ei vastaa yksittäisen opinnäytetyön kustannusten korvaamisesta.

Olemme yhteisesti sopineet opinnäytetyön toteutuksesta ja ohjauksesta yllä sovitulla tavalla.

ALLEKIRJOITUKSET

PAIKKA, PÄIVÄYS JA TOIMEKSIANTAJAN EDUSTAJAN ALLEKIRJOITUS
Kotka 30 / 10 20 12 Pasi Mäenpää

PAIKKA, PÄIVÄYS JA OPISKELIJAN ALLEKIRJOITUS
Kotka 17 / 10 20 12

PAIKKA, PÄIVÄYS JA OHJAAVAN OPETTAJAN ALLEKIRJOITUS
Kotka 19 / 10 20 12 Satu Anttonen

Tämä sopimus on kirjoitettu kolmena kappaleena, yksi toimeksiantajayritykselle, toinen opiskelijalle ja kolmas opintotoimistoon rekisteröintiä varten.

Tutkimusongelmat & muuttujat

Tutkimusongelmat	Muuttujat	Teoreettinen tarkastelu	Kysymyslomakkeen kysymykset
1. Millaiset valmiudet tutkittavalla joukolla on toteuttaa perustason tietoturvaa?	Tietoturvan hallinta	8, 9, 10, 20 - 22	5. Hallitsen sekä ymmärrän mielestäni tietoturvan merkityksen niin kotona kuin työyhteisössä
	Suojausmenetelmien merkitys	12, 13, 14, 15, 18, 20 - 22	6. Tietotekniikassa käytettyjen suojausohjelmien merkitys minulle on selvä asia
	Palomuurin käyttö	15, 16, 20 - 22	9. Minulla on kotikoneessani palomuuri käytössä
	Käyttöjärjestelmä	14	10. Käyttöjärjestelmä puolestaan toimii tietokoneessa
			11. Päivitän käyttöjärjestelmäni
	Virustarkistus	14, 15, 20 - 22	12. Tarkistan aina ulkoiset tallennusvälineet joita kiinnitän tietokoneeseen virusten varalta (esim. CD-levykkeet, USB-muistitikut tai ulkoiset kovalevyt)
	Varmuuskopiointi	13, 17, 20 - 22	14. Olen varautunut kotona tietokoneen rikkoutumiseen ja varmuuskopioinut tärkeimmät tiedostoni erilliselle tallennus välineelle, josta virhetilanteen sattuessa voin palauttaa tilanteen ennalleen niin kuin se oli ennen onnettomuutta
	Salasanojen käyttö	17, 18	18. Vaihdan salasanani koulun tietoverkkoon sekä siellä olevien palveluiden sisällä säännöllisin aikavälein
	Salasanojen käyttö	17, 18, 20 - 22	19. Käytän erilaisia salasanoja käyttämissäni eri verkkoympäristöissä sekä työasemissa. Esim. kotikoneelle, Internet, sähköpostiin, verkkokauppoihin tai harrastusta koskeviin palveluihin, jotka vaativat sisään kirjautumisen

	Henkilökohtainen käyttäjätunnus	20 - 22	20. Luovutan henkilökohtaiset käyttäjätunnukset muiden tietoon tai käyttöön mikäli kaverini tai mikrotukihenkilö näitä pyytää
	Ulos kirjautuminen	18, 20 - 22	21. Kirjaudun ulos aina työasemalta kun lopetan sen käytön 22. Kirjaudun ulos aina työasemalta kun poistun sen välittömästä läheisyydestä enkä käytä sitä hetkeen
2. Millainen käsitys tutkittavalla joukolla on tietoturvan toteutuksesta ja sen vastuunkannosta?	Virustorjunta	14, 15 20 - 22	7. Virustorjunta on riittävä suoja tiedostojeni suojaamiseksi tietokoneessani.
	Palomuuri	15, 16 20 - 22	8. Palomuuri suojaa sen takana olevia tiedostoja sekä laitteita luvattomalta käytöltä.
	Tietojen suojaaminen	16,	13. Minulla ei ole kotona mitään niin tärkeää tietoa tietokoneella, jotta sitä pitäisi suojella millään tavalla
	Tietoturva vastuu	22, 23	15. Olen tutustunut koulun tekemään ”Käyttäjän Tietoturvaohje” teokseen, joka pohjautuu lainsäädäntöömme ja normiohjeistukseen tietoturvan osalta. (Viimeisin päivitys: 23.2.2010/Timo Pirtilä
		20 - 22	16. Tietoturvan toteutuminen sekä sen varmistaminen kuuluvat oppilaitoksessa tietoverkkojen ylläpidolle yksinomaan. 17. Oppilaitos on antanut minulle henkilökohtaiset tunnukset heidän tietoverkkoonsa.
3. Millaisia toiveita tutkittavalla joukolla on opiskelun aikana saamaansa tietoturvaopetukseen?	Tietoturvan opetus	40	23. Millaisia tietoturvaan liittyviä asioita toivoisit käsiteltävän lisää opintojesi aikana?

TUTKIMUSTAULUKKO, aikaisempia tutkimuksia

Tutkijat	**Tutkimuksen tarkoitus**	**Osallistujat (N)**	**Menetelmät**	**Keskeiset tulokset**
Noora Von Fieandt, Pro gradu – tutkielma. HENKILÖSTÖN TIETOTEKNINEN OSAAMINEN JA KOULUTUSTARVE TERVEYDENHOIDOSSA. Sosiaali- ja terveydenhuollon tietohallinto. Kuopion yliopisto 2005.	Tavoitteena selvittää minkälainen tietotekninen osaaminen ja koulutustarve potilaan hoitoon osallistuvalla henkilöstöllä eräissä Helsingin ja Uudenmaan sairaanhoitopiirin sairaalassa.	795N joista vastanneita 622N. Kyselyn vastausprosentti oli 78.	Kysely, analysoitiin tilastollisin menetelmin tarkastelemalla muuttujien frekvenssejä, ristiintaulukoimalla ja vertaamalla korrelaatiota.	1)Kyselyn tulokset osoittivat että tietokoneen hallinta oli nuoremmilla parempaa, ohjelmistojen/sovellusten osalta. 2)Tietotekninen osaaminen parempaa mikäli kotikäyttö runsaampaa. 3)Ammattiryhmä vertailussa parhaiten tunsivat osaavansa tekstinkäsittelijät sekä osastosihteerit ja heikoiten perus- ja lastenhoitajat. 4) 30 % vastanneista tunsi tarvitsevansa lisäkoulutusta tietotekniikan eri osa-

				alueilla.
Tutkijat	**Tutkimuksen tarkoitus**	**Osallistujat (N)**	**Menetelmät**	**Keskeiset tulokset**
Minna Hyvärinen, Pro gradu – tutkielma. VERKKOPALVELUN KEHITTÄMINEN KUNTOUTUKSEN TYÖVÄLINEEKSI– KÄYTTÄJIEN JA KEHITTÄMISEEN OSALLISTUNEIDEN KOKEMUKSIA KUNNET-HANKEESTA JA SEN TOTEUTUKSESTA. Sosiaali- ja terveydenhuollon tietohallinto. Kuopion yliopisto	Tarkoituksena on hahmottaa teoreettisesti suunnitteluun suuntautuneen sosiologian ja teknologian tarjoaman näkemysten kytkeytymisestä tietojärjestelmäsuunnitteluun ja tietotekniikan käytön omaksumiseen sosiaali- ja terveydenhuollon ympäristössä.	Aineiston keruu: aluksi hyväksi käytettiin pilottikäytön lopulla tehtyä verkkopalvelun arviointi- ja tarvekartoitus suunnattua verkkokyselyä 2005 (N=179), myös hankkeen aikana tehtyjä dokumentteja käytettiin tiedonkeruussa. Merkittävin aineisto kerättiin 2006 henkilöhaastatteluin (N=7), hankkeen ylläpidosta, toimituskunnan jäseniä sekä verkkopalvelutoimittajia hankkeessa	Kvalitatiivisen ja kvantitatiivisen yhdistelmä.	1) Sosiaalinen konteksti ja käyttäjän uskomukset tuotteen koetusta helppokäyttöisyydestä ja hyödyllisyydestä vaikuttavat merkittävästi tietotekniikan käyttöönoton hyväksymiseen ja omaksumiseen osaksi jokapäiväistä käytännön työtä. 2) Tietotekniikan vastaaminen käyttäjän tarpeisiin vaikuttaa siihen, missä määrin käyttäjät omaksuvat tuotteen tai palvelun

2008.		olevilta henkilöiltä yhteistyökunnista.		käyttöönsä ja hyödyntävät sitä tiedonhaussa, tietohallinnan ja verkostoitumisen välineenä. 3) Edellä mainitut näkökulmat vaikuttavat merkittävästi organisaatioon tuodusta tuotteen saamasta näkökulmasta, käyttäjäystävällisyydestä sekä sen kehittämisestä. Onnistuneesta palvelusta.
Tutkijat	**Tutkimuksen tarkoitus**	**Osallistujat (N)**	**Menetelmät**	**Keskeiset tulokset**
Toni Korhonen, Pro gradu – tutkielma. TERVEYDEN-HUOLLON HENKILÖSTÖN TIETOTURVA-OSAAMINEN. Sosiaali- ja ter-	Tietoturvallisuus on yksi tärkeimmistä osa-alueista terveydenhuollosta, hoitotyön ollessa tärkein. Tavoitteena oli selvittää terveydenhuollon hoitohenkilöstön	Tutkimuksen vastausprosentti oli 33. (N=197) Kysely toteutettiin strukturoidulla Internet-kyselylomakkeella.	Kysely muodostui tietoturvalliseen toimintaan ja koulutukseen liittyvistä kysymyksistä sekä väittämistä. Tutkimus analysoitiin SPSS -tilasto-analyysiohjel-	1) vastanneista 45 % oli saanut tietoturvakoulutusta. 2) 68 % piti omia tietoteknisiä taitojaan hyvinä tai erittäin hyvinä. 3) Vähän yli puolet oli tyyty-

veydenhuollon tietohallinto. Kuopion yliopisto 2009.	tietoturvaosaamista Eteläkarjalan sairaanhoitopiirissä sekä sairaanhoitopiirin tarjoamaa tukea sen koulutuksen ja viestinnän kautta.		malla.	väisiä saamaansa tietoturvallisuus ohjeistukseen ja tietoihin työyhteisössä. 4) Hieman yli puolet tiesivät kenen puoleen kääntyä tietoturvallisuuteen liittyvissä kysymyksissä sekä lähes puolelle ei oltu tietoturvapolitiikkaa esitelty. 5) Tuloksien perusteella tietoturvakoulutusta tulisi tarjota lisää koko henkilöstölle. 6) Hoitohenkilöstön tulisi kiinnittää huomiota omaan toimintaansa, sillä edelleen potilastietoja tutkitaan uteliaisuudesta ja ollaan valmiita luovuttamaan käyttäjä-

				tunnukset sekä salasanat atk-henkilöstön näitä pyytäessä.
Tutkijat	**Tutkimuksen tarkoitus**	**Osallistujat (N)**	**Menetelmät**	**Keskeiset tulokset**
Anu Laukkanen, Pro gradu – tutkielma. HOITOHENKILÖSTÖN TIETOTURVATIETOISUUS JA TIETOTURVAOSAAMINEN Sosiaali- ja terveydenhuollon tietohallinto. Kuopion yliopisto 2008.	Tutkimuksen tarkoitus oli selvittää terveydenhuollon organisaation hoitohenkilöstön tietoturvatietoisuutta ja –osaamista. Ohjelmistojen sekä siihen rakentuvan tekniikan kehityttyä sairaaloissa, tietoturvallisuuden hallinnalla on entistä suurempi merkitys.	Tutkimus toteutettiin s-postin välityksellä lähetetyllä strukturoidulla nelisivuisella kyselylomakkeella. Kohteena oli Kuopion yliopistollisen sairaalan operatiivisella tulosalueella työskentelevä hoitohenkilöstö. Tutkimuksen vastausprosentti oli 31 % (N=252)	Kysely muodostui kolmesta osa-alueesta: tietoturva osaaminen, -tietoisuus ja lainsäädäntö.	1) Hoitohenkilöstön tietoturvatietoisuus ja –osaaminen on suhteellisen hyvä. 2) Yleiset tietotekniset taidot ja valmiudet hyvät, mutta koulutusta erilaisten työohjelmien hallintaan tarvittaisiin. 3) Henkilökohtaisten käyttäjätunnuksien sekä salasanojen osalta käyttäytyminen sekä tietoisuus oli tiedossa. 4) Lainsäädännön tietämys ja sen

				asettamat vaatimukset eivät välttämättä olleet hallinnassa. Sen sijaan ohjeet sekä säännöt potilaiden henkilötietojen käsittelylle tunnettiin tai tunnistettiin. 5) Oman organisaation tietoturva politiikkaan ja ohjeistuksiin oli osa tutustunut. 6) Koulutusta kaivattiin aiheeseen lisää. 7) Tutkimuksen pohjalta koulutus tulisi tarpeeseen. Ohjeistuksen tulisi pysyä ajan tasalla sekä ohjaamisen tulisi olla käytäntö niin uusille kuin vanhoille työntekijöille. Avainhenkilöiden tulisi

				kommunikoida sekä kehittää tie-toturva käytän-töjä.

Hei Sinä!

Opiskelen Kymenlaakson ammattikorkeakoulussa sairaanhoitajaksi. Teen opinnäytetyönäni tutkien TERVEYSALAN OPISKELIJOIDEN KÄSITYKSET TIETOTURVASTA ENSIMMÄISENOPISKELUVUODEN JÄLKEEN. Tutkittava joukko on aloittanut opiskelunsa vuonna 2011KyAMK:ssa. Opinnäytetyöni valmistuu tammikuun2013 aikana.

Kerään tietoja aiheesta kyselylomakkeella. Kyselylomake täytetään nimettömänä ja ne käsitellään luottamuksellisesti. Kyselyn valmistuttua, vastausaineisto analysoidaan opinnäytetyöhön ja se hävitetään tämän jälkeen asianmukaisesti. Pyydän teitä ystävällisesti vastaamaan kysymyksiin 1 – 22. Kysymyksiin voi vastata vain yhdellä ennalta annetuista vaihtoehdoista. kysymys nro. 23 on avoinkysymys, johon voitte vapaasti vastata oman mielipiteenne aiheesta. Kyselyyn vastaaminen ottaa aikaa sinulta vain Max 6 min, mutta annat sitäkin arvokkaampaa apua ja tietoa tutkimukselleni.

Kysely on voimassa 7.12.2012 asti. Toivon että suhtaudutte myönteisesti opinnäytetyöhöni vastaamalla kyselylomakkeeseen oheisesta linkistä:

http://zef.kyamk.fi/player/?q=474-2cf76647

Mikäli linkki ei toimi, niin kopioi linkki Internet-selaimen osoiteriville manuaalisesti.

Kiitos yhteistyöstä.

Vastauksista kiittäen,

Antti Tiittanen, HO09SC

antti.tiittanen@student.kyamk.fi

Tietoturvakysely

Tietoturva

1.0 Vastaaminen

Ohessa on vastauslomake. Jokainen kappale sisältää joukon kysymyksiä tai väittämiä. Näiden kysymys- tai väittämäjoukkojen vieressä on kysymystyypin mukainen vastausalue, esim. jana tai nelikenttä.

Janalle ja nelikenttään vastaus merkitään kirjoittamalla kysymyksen numero siihen kohtaan taulua, mikä vastaa mielipidettäsi kyseiseen kysymykseen/väittämään. Vastausvinkki: Etsi ensin sopiva kohta vaakasuunnassa ja vasta tämän jälkeen pystysuunnassa. Monivalintakysymyksessä kysymyksen numero kirjoitetaan valintojen perään. Vapaan tekstipalautteen voit antaa paperin alalaitaan tai kääntöpuolelle. Muista merkitä kysymyksen numero myös vapaapalautetta antaessasi

2.0 Vastauslomakkeet

3.1 Taustatiedot

Seuraavilla kysymyksillä tutkitaan tutkittavan joukon taustatiedot sekä tietotekniikan käyttömäärää. Valitse oikea vaihtoehto joka on itsellesi sopivin ja kuvaavin (vain yksi per kysymys)

1. Sukupuoli (Vaihtoehtokysymys) **Vaihtoehdot:** - 1. Nainen - 2. Mies **2. Ikä (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Alle 20 vuotta - 2. 20-29 vuotta - 3. 30-39 vuotta - 4. 40-49 vuotta - 5. 50-59 vuotta tai vanhempi **3. Aikaisempi koulutus tasoni on (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Lukio - 2. Ammatillinen koulutus - 3. Lukio ja Ammatillinen koulutus - 4. Ammattikorkea koulu tai muu ylempi tutkinto **4. Käytän tietotekniikkaa yleisesti ottaen ajallisesti (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Jatkuvasti jokin multimedialaite käytössä - 2. Useita kertoja päivässä - 3. Harvoin, vain muutaman kerran viikossa - 4. Todella harvoin, muutaman kerran kuukaudessa - 5. En koskaan	**Vastausalueet:**

3.2 Yleinen tietämys tietoturvasta ja henkilökohtainen

käyttäytyminen tietotekniikan kanssa

Seuraavat väittämät mittaavat yleisesti omia tietoteknisiä valmiuksia sekä tietoteknistä käyttäytymistäsi eri ympäristöissä. Valitse yksi vastausvaihtoehto, joka kuvaa parhaiten tilannettasi.

5. Hallitsen sekä ymmärrän mielestäni tietoturvan merkityksen niin kotona kuin työyhteisöissä. (Vaihtoehtokysymys) **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **6. Tietotekniikassa käytettyjen suojausohjelmien merkitys on minulle selvä asia. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **7. Virustorjunta on riittävä suoja tiedostojeni suojaamiseksi tietokoneessani. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **8. Palomuuri suojaa sen takana olevia tiedostoja sekä laitteita luvattomalta käytöltä. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **9. Minulla on kotikoneessani palomuuri käytössä. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Kyllä - 2. Ei - 3. En osaa sanoa - 4. Minulla ei ole omaa kotikonetta **10. Käyttöjärjestelmä puolestaan toimii tietokoneessa … (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Internet selaimena - 2. Sähköpostiohjelmana - 3. Taulukkolaskentaohjelmana - 4. Tekstinkäsittelyohjelmana	**Vastausalueet:**

- 5. Tulkkina koneen ja käyttäjän välillä - 6. En osaa sanoa **11. Päivitän käyttöjärjestelmäni (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Manuaalisesti aina kerran kuukaudessa - 2. Manuaalisesti aina kun muistan sen tehdä - 3. Käytän automaattista päivitystoiminnetta koneessani - 4. En päivitä lainkaan käyttöjärjestelmääni - 5. En osaa sanoa **12. Tarkistan aina ulkoiset tallennusvälineet joita kiinnitän tietokoneeseen virusten varalta. (esim. CD-levykkeet, USB- muistitikut tai ulkoiset kovalevyt) (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **13. Minulla ei ole kotona mitään niin tärkeää tietoa tietokoneella, jotta sitä pitäisi suojella millään tavalla. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **14. Olen varautunut kotona tietokoneen rikkoutumiseen ja varmuuskopioinut tärkeimmät tiedostoni erilliselle tallennus välineelle, josta virhetilanteen sattuessa voin palauttaa tilanteen ennalleen niin kuin se oli ennen onnettomuutta. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Kyllä - 2. En - 3. En osaa sanoa **15. Olen tutustunut koulun tekemään ”Käyttäjän Tietoturvaohje” teokseen, joka pohjautuu lainsäädäntöömme ja normiohjeistukseen tietoturvan osalta. (Viimeisin päivitys: 23.2.2010/Timo Pirtilä) (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Kyllä - 2. En - 3. En osaa sanoa **16. Tietoturvan toteutuminen sekä sen varmistaminen kuuluvat oppilaitoksessa tietoverkkojen ylläpidolle yksinomaan. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä	

- 5. Täysin eri mieltä - 6. En osaa sanoa **17. Oppilaitos on antanut minulle henkilökohtaiset tunnukset heidän tietoverkkoonsa. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **18. Vaihdan salasanani koulun tietoverkkoon sekä siellä olevien eri palveluiden sisällä säännöllisin aikavälein. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **19. Käytän erilaisia salasanoja käyttämissäni eri verkkoympäristöissä sekä työasemissa. Esim. kotikoneelle, Internet sähköpostiin, verkkokauppoihin tai harrastusta koskeviin palveluihin, jotka vaativat sisään kirjautumisen. (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Täysin samaa mieltä - 2. Jokseenkin samaa mieltä - 3. En samaa enkä erimieltä - 4. Jokseekin eri mieltä - 5. Täysin eri mieltä - 6. En osaa sanoa **20. Luovutan henkilökohtaiset käyttäjätunnukset muiden tietoon tai käyttöön mikäli kaverini tai mikrotukihenkilö näitä pyytää.** **Vaihtoehdot:** - 1. Kyllä - 2. En - 3. En osaa sanoa **21. Kirjaudun ulos aina työasemalta kun lopetan sen käytön (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Kyllä - 2. En - 3. En osaa sanoa **22. Kirjaudun ulos aina työasemalta kun poistun sen välittömästä läheisyydestä enkä käytä sitä hetkeen (Vaihtoehtokysymys)** **Vaihtoehdot:** - 1. Kyllä - 2. En - 3. En osaa sanoa **23. Millaisia tietoturvaan liittyviä asioita toivoisit käsiteltävän lisää opintojesi aikana?** Kirjoita vapaasti tekstikenttään vastauksesi.	