

Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2013

Samu Kotilahti

E-TENTIN TIETOTURVA- JA TIETOSUOJAKARTOITUS



TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Marraskuu 2013 | 28 sivua

Ohjaaja: Esko Vainikka

Samu Kotilahti

E-TENTIN TIETOTURVA- JA TIETOSUOJAKARTOITUS

Tässä opinnäytetyössä tarkastellaan tietoturva- ja tietosuojakartoituksen laatimista Turun ammattikorkeakoulun sisäiselle E-tentti-järjestelmälle. Opinnäytetyön tavoitteena oli kartoittaa järjestelmän tietoturva opiskelijan näkökulmasta. Työssä käsitellään tietoturvan ja tietosuojan yleisiä periaatteita ja tarkastellaan niiden tarpeellisuutta E-tentti-järjestelmän näkökulmasta.

Opinnäytetyön ensimmäisessä osassa käsitellään E-tenttiä yleisellä tasolla ja Turun ammattikorkeakoulun näkökulmasta. E-tentti ja tenttiakvaario ovat Turun ammattikorkeakoulun järjestelmiä, jotka tarjoavat hyviä mahdollisuuksia tenttien joustavuudelle.

Toisessa osassa tarkastellaan tietoturvan peruseriaatteita sekä opinnäytetyön kannalta tärkeimpiä tietosuojan osa-alueita. Tietoturva perustuu kolmelle peruspilarille; tiedon saatavuudelle, eheydelle ja luottamuksellisuudelle.

Opinnäytetyön kolmas osa perustuu E-tentin tietoturva- ja tietosuojakartoituksen laatimisen tarkastelemiseen sekä tuloksien esittelyyn. Lopuksi käydään läpi kartoituksen pohjaksi laaditun kyselyn tulokset sekä työn johtopäätökset.

ASIASANAT:

tietoturva, tietosuoja, tietoturvakartoitus, e-tentti

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications

November 2013 | 28 pages

Instructor: Esko Vainikka

Samu Kotilahti

INFORMATION SECURITY SURVEY FOR E-EXAM

This thesis studies conducting an information security survey for an internal E-exam system of Turku University of Applied Sciences. The purpose of this thesis was to survey the information security of the project from a student's point of view. The thesis processes the general principles of information security and surveys their necessity regarding the E-exam system.

The first part of the thesis introduces the E-exam on a general level and from Turku University of Applied Sciences' perspective. E-exam and Exam aquarium, which were test-used in 2011 and 2012, offer good possibilities for more flexible exams.

The second part evaluates the general principles of information security and the most important sections of data protection concerning E-exam. Information security is based on three base principles: data confidentiality, data integrity and data availability.

The third part of the thesis reviews the conducting of information security survey for the E-exam system. Also, the results of the survey are demonstrated, as well as the conclusions about the conducted survey.

KEYWORDS:

information security, data security, information security survey, e-exam

SISÄLTÖ

1 JOHDANTO	6
2 E-TENTTI YLEISESTI	8
2.1 E-tentin toimintaperiaate	8
2.2 Tenttiakvaarion toiminta	8
2.3 E-tentin levinneisyys	9
2.4 E-tentti Turun amk:ssa	10
3 TIETOTURVALLISUUDEN PERUSTEET	12
3.1 Tietoturvallisuus ja CIA-malli	12
3.2 CIA-teoria e-tentin kannalta	14
4 TIETOSUOJAN MERKITYS PROJEKTISSA	15
4.1 Henkilötietolaki	15
4.2 Henkilötietojen käsittely	16
4.3 Videovalvonta oppilaitosten ATK-luokissa	17
5 E-TENTIN TIETOTURVA- JA TIETOSUOJAKARTOITUKSEN LAATIMINEN	18
5.1 Tietoturvakartoitus käsitteenä	18
5.2 Tietoturvakartoituksessa tyypillisesti arvioitavia kohteita	18
5.3 E-tentin tietoturva- ja tietosuojakyselyssä käytetyt kysymykset	19
5.4 Tietoturva- ja tietosuojakyselyn tulokset	20
6 E-TENTIN TIETOTURVALLISUUDEN PARANNUSEHDOTUKSET	25
6.1 Tietoturvan kehitysehdotukset	25
6.2 Tietosuojan kehitysehdotukset	25
7 JOHTOPÄÄTÖKSET	27
LÄHTEET	28

LIITTEET

Liite 1. E-tentin tietoturva- ja tietosuojakyselyssä käytetyt kysymykset.

Liite 2. E-tentin tietoturva- ja tietosuojankyselyn tulokset kaavioina esitettynä.

KUVIOT

Kuvio 1. Onko tietoturvaluudesta vastaavaa henkilöä nimetty?	21
Kuvio 2. Voiko tenttijä käyttää tenttitilassa omia tallennusvälineitään?	22
Kuvio 3. Voidaanko tenttiin liittää mitä tahansa tiedostotyyppisiä?	22
Kuvio 4. Otetaanko tenttitiedostoista varmuuskopioita?	23
Kuvio 5. Äänitetäänkö tenttitilaisuus?	24
Kuvio 6. Lasketaanko yhteyden katketessa kesken jäänyt tentin tenttikerraksi?	24

1 JOHDANTO

Turun ammattikorkeakoulu on vahvasti mukana etsimässä uusia suuntia opiskelun tueksi. Yksi potentiaalisimmista, joskaan ei vielä näkyvimmistä, kehityskohteista on sähköinen tenttimisjärjestelmä E-tentti. E-tentti on tehokas väline sekä opiskelijalle että opettajalle, sillä se antaa mahdollisuuden suorittaa tentin ajasta ja paikasta riippumatta.

On selvää, että E-tentin kaltaisessa järjestelmässä käsitellään ja säilytetään valtavaa määrää henkilötietoja, kuten opiskelijanumeroita. Virallisesti järjestelmään ei kerätä henkilötunnuksia, mutta jotkin opiskelijat syöttävät järjestelmään opiskelijanumeronsa sijaan oman henkilötunnuksensa. Järjestelmän tietoturvaluottuutta voidaan siis pitää erittäin tärkeänä ja kriittisenä elementtinä. Tietoturvan ja tietosuojan merkitys kasvaa jatkuvasti ja se kuuluu jo jokaisen ihmisen arkipäivään.

E-tenttiä alettiin testata vuoden 2011 aikana ja järjestelmän pilottikäyttö aloitettiin vuonna 2012. Tietoturva- ja tietosuoja-asioihin ei kuitenkaan oltu kiinnitetty juurikaan huomiota. Tästä syystä projektin tietosuojan ja tietoturvan senhetkinen tila oli tarkastettava.

Monet tietoturvaan ja tietosuojaan liittyvät käytännöt olivat olemassa mm. Turun AMK:n tietoturvapolitiikan kautta, mutta tämänkaltaisen kartoitus tulisi suorittaa jokaiselle IT-projektille tai hankkeelle riippumatta siitä, onko kyseessä Turun AMK:n kehitysprojekti tai opiskelijaprojekti. Tietoturva ja tietosuoja ovat asioita, joita ei pidä laiminlyödä.

Tietosuoja- ja tietoturvakartoituksen tulokset olivat vaihtelevia, mutta antoivat yleiskuvan siitä, millä tasolla vastaajien tietämys liikkuu. Vastaajien joukossa oli niin Turun AMK:n henkilökuntaa kuin pilottiin osallistuneita opiskelijoitakin.

Vastausten vaihtelevuudesta huolimatta E-tenttiä varten saatiin useita hyviä kehitysideoita tietoturvaluottuuden ylläpitämiseksi ja parantamiseksi. Tietosuojan osalta kehitettävää oli vähemmän, mutta siitä huolimatta siihen tulee kiinnittää

huomiota tulevaisuudessa entistä tarkemmin myös E-tentin kaltaisissa pienemmissä projekteissa.

Opinnäytetyön viitemateriaalina on käytetty E-tentin pääkäyttäjän, Matti Kuikan, laatimaa PowerPoint-esitystä Mikä on tenttiakvaario (e-Tentti, e-Exam) ? sekä Turun ammattikorkeakoulun Opiskelijan opasta. Molemmat teokset löytyvät Turun ammattikorkeakoulun sisäisestä intranetistä, Messistä, mutta niitä ei ole julkisesti saatavilla.

E-tentistä ei ollut opinnäytetyön kirjoitushetkellä saatavissa virallista esittelymateriaalia, minkä vuoksi teoriaosuudessa on viitattu epävirallisiin lähteisiin. Turun ammattikorkeakoulun Opiskelijan opas on jokaiselle uudelle opiskelijalle jaettava opas, jossa on selitetty opiskelijalle tärkeitä AMK:n toimintoja.

2 E-TENTTI YLEISESTI

2.1 E-tentin toimintaperiaate

Tenttiakvaario on tietokantapohjainen sovellus, joka on suunniteltu erityisesti yliopistojen yleisten tenttipäivien täydentäjäksi. Sen avulla opiskelija voi tenttiä kurssit verkossa itselleen parhaiten sopivana ajankohtana. Järjestelmä arpoo tentin kysymykset opettajien järjestelmään syöttämien kysymysten joukosta. Kuulusteluun vastaaminen tapahtuu valvotussa tilassa, joka voi olla esim. lasiseinäinen työpiste aulaassa tai kirjastossa, videovalvottu työtila tai valvottu atk-luokka. (Kuikka 2013.)

Tenttiakvaario on tentin suorittamiseen tarkoitettu toimintapiste, jossa on tietokone, tenttiakvaario-ohjelma, verkkoyhteys sekä valvontakamera. E-tenttiohjelma tarkkailee tentin kulkua ja tenttiaikaa. Kun tietty aika on kulunut umpeen, ohjelma ilmoittaa tenttiajan loppumisesta. Valvonta voi tapahtua videokameralla, joka lähettää reaaliaikaista kuvaa valvojan tietokoneelle sekä tallentaa kuvatun materiaalin myöhempää tarkastelua varten. (Kuikka 2013.)

E-tentti on joustava tapa toteuttaa erilaisia tenttejä. Lopulliset käyttötavat riippuvat kuitenkin kulloisenkin oppilaitoksen silloisista käytännöistä. E-tenttiä on mahdollista käyttää normaalien tenttien lisäksi moniin eri käyttötarkoituksiin:

- uusintatentteihin
- kirjatentteihin
- harjoitustentteihin
- valvottuihin ryhmätentteihin.

2.2 Tenttiakvaarion toiminta

E-tentin toiminta perustuu opettajan ohjelmaan valmiiksi laatimiin kysymyksiin, joita suositellaan tallennettavan jokaista aihealuetta kohden noin viisinkertainen

määrä. Tenttitilanteessa ohjelma joko arpoo kysymykset opettajan tallentamien kysymysten joukosta tai käyttää ennalta määriteltyjä kysymyksiä, joihin opiskelijan on vastattava. Opiskelija puolestaan ilmoittautuu tenttiin ohjelman avulla ja lukee kurssivaatimuksena olevan aineiston.

E-tentti-sovelluksella voi automatisoida tenttijärjestelyt ja tiedonkulun, kuten tentti-ilmoittautumiset, tenttivastaukset ja arvostelutiedot. Aina tentti tai omien taitojen testaaminen ei edellytä valvontaa. Tällöin vastaaminen voi tapahtua vaikka opiskelijan kotoa. (Kuikka 2013.)

E-tentissä opiskelija ilmoittautuu tenttiin internetissä, vastaa kysymyksiin varaamaan ajankohtana ja saa arvostelun ja palautteen sähköpostitse. E-tentti-järjestelmä tunnistaa opiskelijan käyttäjätunnuksen ja salasanan perusteella sekä esittää kysymykset, valvoo tenttiajan kulumista, ilmoittaa opiskelijan ilmoittautumisesta ja palautetuista vastauksista opettajalle. (Turun ammattikorkeakoulu 2013.)

E-tentin avulla tenttiajankohdan voi sovittaa omaan opiskelurytmiin. Vastaaminen tietokoneella antaa mahdollisuuden paremmin jäsennelyihin vastauksiin ja rauhallinen työtila vähentää tentistä aiheutuvaa stressiä. Opiskelija saa nopeamman ja henkilökohtaisemman palautteen tentistä ja oppimisestaan. Myös turha matkustaminen vähenee erityisesti silloin, kun E-tenttiä voidaan käyttää kotoa käsin.

2.3 E-tentin levinneisyys

E-tentti -järjestelmä on käytössä jo hyvin laajalti, etenkin yliopistoissa. Lähes kaikki yliopistot ovat ainakin pilotoineet e-tenttiä ja käyttöön sen on ottanut paria poikkeusta lukuunottamatta jokainen Suomen yliopisto. (Kuikka 2013.)

AMK-sektorilla e-tentti on jossain määrin uudempi ilmiö, eivätkä läheskään kaikki ammattikorkeakoulut ole vielä edes pilotoineet e-tenttiä.

2.4 E-tentti Turun amk:ssa

Etäopetus ja -opiskelu lisääntyy jatkuvasti niin yliopistoissa kuin ammattikorkeakouluissakin. Opiskelijat vaativat yhä joustavampia ratkaisuja suorittaa opintojaan. Yliopistosektorilla e-tenttiä on pilotoitu jo useita vuosia sitten ja tällä hetkellä useat yliopistot käyttävät e-tenttiä vaihtoehtoisena tenttimismuotona.

E-tentin käyttöönotolle nähdään yleisesti ottaen useita hyviä puolia. Opettajan tulee miettiä ja tuottaa tenttikysymykset vain kerran, vaikka E-tenttiä varten pitääkin tuottaa kerralla useita kysymyksiä. Vastaukset ja tenttiarvioinnit arkistoidaan käytettävään sovellukseen, joten niiden tarkastelu on helppoa mistä tahansa. Koska vastaukset kirjoitetaan tietokoneella, saa opettaja tarkastettavakseen siististi kirjoitetut vastaukset, jolloin arviointi on opettajalle helpompaa ja nopeampaa. (Kuikka 2013.)

Haasteina e-tentin yleistymiselle voidaan nähdä mm. seuraavat seikat:

- käyttöönoton hitaus
- tenttiakvaarion ruuhkautuminen ja resurssien riittämättömyys
- piirtämistä tai matemaattisia ongelmia sisältävät tentit.

Pilotointivaihe

Turun AMK:ssa E-tenttiä alettiin testata vuoden 2011 aikana ja varsinainen pilotointi aloitettiin vuoden 2012 alussa. E-tenttiohjelmistoa valittaessa päädyttiin Sordinon toimittamaan Soft Tutor -ohjelmistoon. Ohjelmistoa ei käytetä Turun AMK:n palvelimelta, vaan ainakin pilotointivaiheessa ohjelmiston käyttämiseen tarvitaan etäyhteys Turun AMK:n ja Joensuun AMK:n välillä. (Kuikka 2013.)

Turun AMK:ssa E-tentti sisältää ainakin pilotointivaiheessa kaksi eri käyttötapaa; niin sanotun tenttiakvaarion sekä etäntin. Tenttiakvaariolla tarkoitetaan tilaa, joka on suunniteltu E-tentin tekemistä varten.

Tenttiakvaariotilassa on yleensä mahdollisuus useaan yhtäaikaiseen tenttiin ja tenttimistilannetta valvotaan kameran avulla. Joissain tapauksissa kameravalvonnan yhteydessä tallennetaan myös ääni, mutta esimerkiksi Turun AMK:n tenttiakvaariossa ei äänen taltiointia ole tällä hetkellä käytössä. (Kuikka 2013.)

Tenttiakvaariota käytettäessä tentillä on aina myös valvoja, joka huolehtii tentin sujuvuudesta. Pilottivaiheessa valvojina toimivat Turun AMK:n Lemminkäisenkadun toimipisteen kirjaston työntekijät, mutta valvoja voi olla lähes kuka tahansa kyseiseen tehtävään koulutettu ja Turun ammattikorkeakoulun henkilökuntaan kuuluva henkilö. (Kuikka 2013.)

Joissain tapauksissa tentti on sen luonteinen, ettei se edellytä valvontaa tai opiskelijan fyysistä paikallaoloa oppilaitoksen tiloissa. Tällaisissa tapauksissa voidaan käyttää etätentti-ominaisuutta, jolloin tenttiin tai kuulusteluun vastaaminen voi tapahtua vaikka opiskelijan kotoa.

3 TIETOTURVALLISUUDEN PERUSTEET

Kansankielellä puhuttaessa tietoturvilla tarkoitetaan yleensä lähinnä tietokoneen virustentorjuntaa ja palomuuria. Molemmat liittyvät tietoturvaan ja ovat yhä tärkeämpi osa nykypäivän tietoturvaa. Tietoturva on kuitenkin varsin laaja käsite ja se kattaakin käytännössä kaiken, mikä liittyy tietojen käsittelyyn, saatavuuteen, oikeellisuuteen ja luottamuksellisuuteen.

Toimiva tietoturva on riskejä ennakoivaa, tietojen suojaamista lakien edellyttämällä tavolla ja sen ylläpito on järjestelmällistä ja suunniteltua.

3.1 Tietoturvallisuus ja CIA-malli

CIA-malli on kehitetty, jotta ihmisen olisi helpompi ymmärtää tietoturvan tärkeimpiä näkökulmia. Jokainen asia tietoturvaa kehitettäessä liittyy CIA-kolmijalan johonkin osa-alueeseen.

Tietoturva käsittää yleensä kolme pääaluetta, jotka ovat luottamuksellisuus (confidentiality), eheys (integrity) ja saatavuus (availability). Nämä kolme pääkokonaisuutta muodostavat yhdessä CIA-kolmijalan, joka käytännössä tarkoittaa sitä, että CIA-teorian pohjalle rakennetun järjestelmän tietoturva kaatuu yhden jalan murtuessa. (Andress 2011, 4.)

Edellämainittujen kolmen pääalueen lisäksi CIA-teoriamallia on mahdollista laajentaa kolmella pienemmällä osa-alueella. Näistä todentaminen (authentication) liittyy läheisesti luottamuksellisuuteen, pääsynvalvonta (access control) eheyteen ja kiistämättömyys (non-repudiation) saatavuuteen. (Andress 2011, 7.) Monimutkaisempaa teoriamallia käyttämällä on mahdollista liittää oman organisaation tietoturvan osa-alueet yhtenäisen mallin alle.

Näiden pääalueiden lisäksi tietoturvallisuus voidaan jakaa käytännön osaluueisiin esimerkiksi seuraavalla tavalla:

- hallinnollinen tietoturvallisuus
- henkilöstöturvallisuus
- fyysinen turvallisuus (toimitilaturvallisuus)
- tietoliikenteen turvallisuus
- laitteistoturvallisuus
- ohjelmistoturvallisuus
- käyttöturvallisuus
- tietoaineistoturvallisuus (Viestintävirasto 2012).

Tiedon luottamuksellisuus

Luottamuksellisuus on keino piilottaa tietoa käyttäjiltä, joilla ei ole sen tarkasteluun lupaa. Luottamuksellisuus on CIA-triadin ilmeisin näkökulma, mutta sitä vastaan myös hyökätään kaikkein useimmin. Esimerkiksi erilaisilla salausmenetelmillä voidaan yrittää varmistaa tiedon luottamuksellisuus, kun tietoa siirretään tietokoneelta toiselle tietoverkon välityksellä. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

Tiedon eheys

Tiedon eheydellä tarkoitetaan tietoaineiston paikkansapitävyyttä. Tiedon ei myöskään tule olla virheellistä. Jotkin tietomurrot liittyvät juuri tiedon eheyteen ja sen muuttamiseen alkuperäisestä, ennen kuin tieto lähetetään palvelimelta käyttäjälle. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

Tiedon eheyden varmistamiskeinona voidaan käyttää esimerkiksi tietojen säännöllistä varmuuskopiointia. Tiedon eheyden menettämisen riskiä voidaan yrittää pienentää esimerkiksi virustorjuntaohjelmistoilla tai tietoturvakoulutuksilla. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

Tiedon saatavuus

Tiedon luottamuksellisuuden ja eheyden ohella myös tiedon saatavuus on tärkeää. Tietoaineiston pitää olla jatkuvasti saatavilla henkilöille, joilla on oikeus tiedon tarkasteluun. Joidenkin tietomurtojen erityispiirre on pääsyn kieltäminen henkilöiltä, joilla kuuluisi olla oikeus tiedon tarkasteluun. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

3.2 CIA-teoria e-tentin kannalta

Lähes kaikki e-tentissä kerättävä tieto on luottamuksellista. Ohjelmiston käytön kannalta on tärkeää, että vähintään käyttäjänimet ja käyttöoikeudet on suojattu siten, että niitä voi hallinnoida vain ylläpitäjä. Tavallisten käyttäjien ei tule olla mahdollista lisätä tai poistaa käyttöoikeuksia tai muuta tietoa. Lisäksi ohjelmiston tulee olla saatavilla siten, että ylläpitäjän on koska tahansa mahdollista lisätä käyttäjiä tai muokata käyttöoikeuksia.

Yksi tärkeimmistä saatavuuteen liittyvistä seikoista on ohjelmiston saatavuus käyttäjille. Koska E-tentti on toteutettu pilvipalveluna, pitää palvelua käyttävien opiskelijoiden pystyä kirjautumaan palveluun milloin tahansa joko tenttimään tai varaamaan tenttimisaikaa. E-tenttiä käyttävien opettajien taas tulisi pystyä arvioimaan tenttejä sekä laatimaan kysymyksiä milloin tahansa. Mikäli palvelu ei ole hetkellisesti saatavilla, tulisi siitä tiedottaa selkeästi sekä senhetkisille että potentiaalisille käyttäjille.

4 TIETOSUOJAN MERKITYS PROJEKTISSA

4.1 Henkilötietolaki

Henkilötietolain tarkoitus on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista. (Henkilötietolaki 523/1999.)

Henkilötietojen käsittelyyn vaikuttaa henkilötietolain lisäksi myös laki yksityisyydensuojasta työelämässä (759/2004). Lukuisissa muissakin laeissa on useita henkilötietojen käsittelyyn vaikuttavia säädöksiä. Henkilötietolain yleisvelvoitteita sovelletaan aina, vaikka erityislakien säännöksiä sovelletaankin ensisijaisena. (Tietosuojavaltuutettu 2001.)

Henkilötietolain soveltaminen

Henkilötietolakia sovelletaan sekä automaattiseen tietojenkäsittelyyn että automaattisesti tapahtuvaan henkilötietojen käsittelyyn. Henkilötietolaki koskee viranomaisten, yritysten, järjestöjen sekä muiden yhteisöjen ja yksityisten henkilöiden toimintaa. (Tietosuojavaltuutettu 2001.)

Henkilötietolain ulkopuolelle jää joitakin erityistapauksia tietyin rajoituksin. Niitä ei kuitenkaan käsitellä tässä, sillä niillä ei ole E-tentin tietosuojan kannalta merkitystä.

Henkilötietolakia sovelletaan pääasiassa henkilötietojen käsittelyyn silloin, kun rekisterinpitäjän toimipaikka on Suomen alueella tai muulla tavalla Suomen oikeudenkäytön piirissä (Henkilötietolaki 523/1999). Lakia sovelletaan myös joissain muissa tapauksissa, mutta niillä ei ole E-tentin tietosuojan kannalta juurikaan merkitystä.

4.2 Henkilötietojen käsittely

Henkilötietojen keräämisen ja käsittelyn tarkoitus tulee määritellä etukäteen. Henkilötietojen käsittelyn määrittelystä tulee käydä ilmi, mitä varten tietoja kerätään ja käsitellään. Hyvän tietojenkäsittelytavan mukaisesti ennen määrittelyä tulisi arvioida, onko henkilöiden tunnistamistietoja kerättävä tehtävän hoitamista varten vai riittävätkö ilman tunnisteita olevat tiedot. (Tietosuojavaltuutettu 2001.)

Ennen keräämistä tulisi myös selvittää, mitä tarkoitusta varten ja millä tavoin henkilötietoja on kulloisenkin tehtävän hoidossa tarpeellista kerätä ja käyttää. Samoin tulisi selvittää, mitä henkilötietoja on säilytettävä ja mitä tietoja mahdollisesti olisi luovutettava. (Tietosuojavaltuutettu 2001.)

Henkilötietojen käsittelyn lainmukaisuus on varmistettava rekisterinpitäjän toimesta. Jokaisen henkilötietojen käsittelyvaiheen tulee olla sekä henkilötietolain että mahdollisten erityissäännösten mukaisia. Rekisterinpitäjän on lisäksi huolehdittava, että rekisteröityjen oikeudet on toteutettu lainmukaisesti. (Tietosuojavaltuutettu 2001.)

Kaikki henkilötiedot on suojattava ulkopuolisilta henkilötietolain edellyttämällä tavalla jokaisessa käsittelyvaiheessa. Lisäksi tiedon laadusta ja virheettömyydestä on huolehdittava. Jokaisessa tehtävässä tulisi käyttää vain siihen tarkoitettuja henkilötietoja. (Tietosuojavaltuutettu 2001.)

Henkilötietorekisterin ylläpitäjän on laadittava rekisteriseloste, joka on luettavissa milloin tahansa. Rekisteriselosteeseen on hyvä merkitä myös informointivelvoitteen edellyttämät tiedot, mikäli informointivelvoite koskee rekisteriä. (Tietosuojavaltuutettu 2001.)

Henkilötietojen käsittelyn vastuut ja niihin liittyvät tehtävät pitää olla määriteltyinä. Tarvittaessa voidaan nimetä tietosuojavastaava tai tietosuojasta vastaava ryhmä. Henkilöstöllä tulee olla riittävät ohjeet ja tiedot henkilötietojen käytöstä ja käsittelystä. (Tietosuojavaltuutettu 2001.)

4.3 Videovalvonta oppilaitosten ATK-luokissa

Koska videovalvonta on osa myös Turun AMK:n E-tentin valvontaa, tulee sitä käsitellä omana kokonaisuutenaan. Opinnäytetyön kirjoittamishetkellä käytössä oli tallentava videovalvonta ilman äänen tallennusta (Kuikka 2013). Tallentavaa kameravalvontaa suoritettaessa sovelletaan Henkilötietolain periaatteita niiltä osin kuin siinä säädetään henkilötietojen käsittelystä.

Tietosuojavaltuutetun kannanotossa koskien oppilaitosten ATK-luokkien videovalvontaa otetaan kantaa siihen, että tallentavaa kameravalvontaa tulee käyttää vain silloin, kun sen käyttö on asiallisesti perusteltua. (Tietosuojavaltuutetun toimisto 2001.) Kameralla kerättävien henkilötietojen käsittely tulee suunnitella etukäteen ja tietojen tallennusaika on määritettävä. Tallentavaa kameravalvontaa varten tulee järjestelmästä laatia rekisteriseloste.

E-tentti Turun AMK:ssa täyttää kaikki lain ja hyvän tietojenkäsittelytavan kriteerit niin, että tallentavaa kameravalvontaa voidaan suorittaa. Rekisteriseloste on laadittu huolellisesti ja se on kaikkien saatavilla oppilaitoksen intranetissä. Ääntä ei kuitenkaan tallenneta toistaiseksi, sillä tietosuoja sen kannalta ei ole vielä kunnossa.

5 E-TENTIN TIETOTURVA- JA TIETOSUOJAKARTOITUKSEN LAATIMINEN

5.1 Tietoturvakartoitus käsitteenä

Tiivistettynä tietoturvakartoituksella tarkoitetaan kyselyä tai haastattelua, jonka avulla voidaan päätellä esimerkiksi yrityksen tietoturvallisuuden taso sekä kehittää yrityksen tietoturvakäytäntöjä paremmiksi.

Valtava luottamuksellisen ja salaisen tietomäärän kasvu on luonut yrityksille ja muille organisaatioille paineen kehittää tietoturvaansa. Joillakin tietoturvallisuus on otettu asianmukaisesti todesta heti automaattiseen tietojenkäsittelyyn siirryttäessä, mutta suuri määrä yrityksiä ja yhteisöjä kamppailee tietoturvariskien parissa.

Maailmassa on suuri määrä yrityksiä, jotka tekevät tietoturvakartoituksia. Yleinen, vakiintunut käytäntö on, että jokaisella tietoturvakartoituksia tekevällä yrityksellä on oma kyselynsä, jota käytetään kartoituksen apuvälineenä (Nietula 2011).

Tietoturvakartoitus on organisaation johdolle hyvä työkalu, jonka avulla se saa hyvän kuvan organisaation tietoturvallisuuden tasosta ja siitä, mitä vaatimuksia suojattavat kohteet asettavat tietoturvallisuuden ylläpidolle.

5.2 Tietoturvakartoituksessa tyypillisesti arvioitavia kohteita

Tietoturvakartoituksessa arvioitavat kohteet vaihtelevat arvioitavan organisaation toimialan ja toimenkuvan mukaan. Yleisiä arvioitavia kohteita ovat muun muassa tietoturvaohjeistus, tietoturvallisuuden johtaminen, työasemien ja tietoliikenneverkon tietoturvallisuus sekä palveluiden ulkoistamiseen liittyvät sopimukset. Muita arvioitavia kohteita voivat olla esimerkiksi etäyhteydet,

mobiilipalvelut sekä –laitteet ja henkilökunnan tietoturvallisuuden tietämyksen taso. (Tietosuojavaltuutettu 2001.)

Tietoturvakartoitus voi sisältää esimerkiksi seuraavanlaisia kysymyksiä, jotka tässä esitetään kuitenkin havainnollisuuden vuoksi yksinkertaistettuina:

- Mitä tietoja pitäisi suojata?
- Miltä mitäkin tietoja pitää suojella?
- Kenen tietoja suojellaan ja keneltä?
- Kenen on päästävä tietoihin käsiksi?
- Miten tietoja suojataan?
- Mikä on tietoturvan heikoin lenkki?
- Miten tietoturvaresursseja käytetään?

Kartoitusta varten organisaatiolta kerätään pohjatietoja erilaisin haastatteluin tai kyselylomakkein. Tärkeää on huomioida myös varsinaiseen tietoturvallisuuteen liittymättömät seikat, kuten organisaation toimiala. Pohjatietojen perusteella organisaatiolle voidaan suorittaa riskianalyysi tai laatia tietoturvapoliittikka ja – ohjeistus sekä tietoturvallisuuden kehittämissuunnitelma.

5.3 E-tentin tietoturva- ja tietosuojakyselyssä käytetyt kysymykset

Tietoturvakartoituksessa käytettiin pohjana Santa Fe –yhteisön kehittämää SIG-tietoturvakyselyn versiota 6.0, joka on yleisesti hyväksytty tietoturvakartoitusten laatimisen pohjaksi. SIG-kysely on erittäin laaja, joten tähän tietoturva- ja tietosuojakyselyyn otettiin mukaan vain projektin kannalta oleellimmat aihealueet.

Opinnäytetyön kirjoittamisen aikana julkaistiin SIG-kyselystä uusi versio 7.0, joka on maksullinen. Samalla myös ilmainen 6.0 versio poistettiin yleisestä jakelusta, joten sitä ei enää ole mahdollista hankkia. Kyselyn eri versiot ovat kuitenkin sisällöltään hyvin samankaltaisia.

Kyselyyn kuului yhteensä 34 kysymystä. Jokaisen kysymyksen yhteydessä oli mahdollisuus valita tyhjä kohta tai vaihtoehto ”En tiedä”. Kysymyksiä ei ollut jaoteltu ryhmiin, vaan kaikki kysymykset esitettiin peräkkäin vapaassa järjestyksessä. Jokaisen kysymyksen yhteydessä oli myös mahdollisuus antaa lisätietoja tai tarkennuksia vastaukseen.

Kyselyssä kysytyt asiat voidaan jaotella kuuteen osa-alueeseen:

- tietoturva teknisestä näkökulmasta
- tietoturva opiskelijan näkökulmasta
- tietoturva muiden käyttäjien näkökulmasta
- tietosuoja käyttäjän näkökulmasta
- tietosuoja hallinnollisesta näkökulmasta
- yleinen tietämys E-tentin ja Turun AMK:n tietoturvakäytännöistä.

Kaikki kysymykset ovat vastausvaihtoehtoinen opinnäytetyön liitteenä.

5.4 Tietoturva- ja tietosuojakyselyn tulokset

Tietoturva- ja tietosuojakysely toteutettiin vuoden 2012 syksyllä. Kyselyyn vastasi sekä E-tenttiä pilottikäyttäneitä opiskelijoita että sen teknisestä toteutuksesta Turun ammattikorkeakoulussa vastanneita henkilökunnan edustajia. Kyselyyn vastasi yhteensä kymmenen E-tenttiä enemmän tai vähemmän käyttänyttä henkilöä.

Kyselyn ensimmäinen versio toteutettiin Excel-muotoisena, ja siitä tehtiin mahdollisimman helppokäyttöinen. Kysely lähetettiin sähköpostitse kahdeksalle henkilökunnan edustajalle, joista kuitenkin vain yksi vastasi.

Tämän vuoksi kysely päätettiin toteuttaa uudelleen lomakemuotoisena kyselynä. Tähän käytettiin Google Docs -palvelua, jonka avulla tulokset sai vietyä helposti taulukkomuotoon myöhempää tarkastelua ja arkistointia varten. Linkki uudistettuun kyselyyn lähetettiin sähköpostitse usealle E-tenttiä

käyttäneelle opiskelijalle ja henkilökunnan edustajalle. Tavoitteena oli saada vähintään 20 vastausta, mutta tavoitteesta kuitenkin jäätin reilusti.

Kyselyn ensimmäisen version kohderyhmään kuului vain henkilökunnan edustajia, mutta erittäin huonon vastausprosentin vuoksi toisessa versiossa kohderyhmää laajennettiin koskemaan myös E-tenttiä pilotoineita opiskelijoita. Vastausprosentti jäi kuitenkin laajemmasta kohderyhmästä huolimatta varsin pieneksi.

Suurimpaan osaan kysymyksiä eniten vastauksia sai ”En tiedä” -vaihtoehto. Järjestelmän parissa työskenteleville tämä on selkeä herätys tiedottamisen tärkeydestä. Monien kysymysten vastauksista käy ilmi vastaajien tietämättömyys. Joissain tapauksissa se on hyväksyttävää, mutta selkeästi monessa asiassa olisi vielä parannettavaa.

Tässä luvussa tarkastellaan tuloksien havainnollistamiseksi muutamien kysymysten vastausjakaumat. Kaikkien kysymysten vastaukset ovat tarkasteltavissa opinnäytetyön liitteessä.



Kuvio 1. Onko tietoturvallisuudesta vastaavaa henkilöä nimetty?

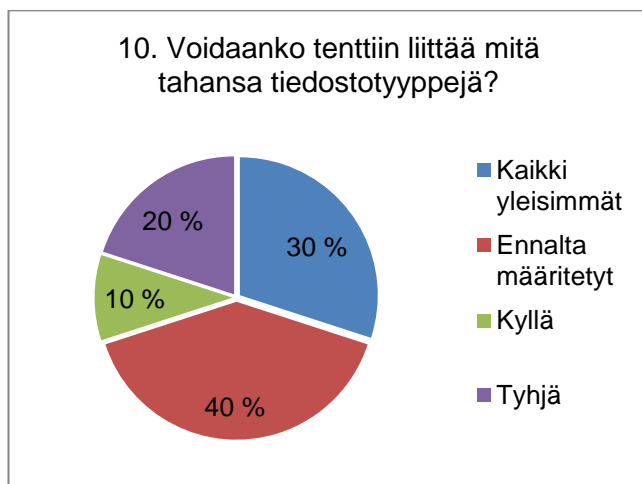
E-tentin kohdalla tietoturvallisuudesta vastaavat käytännössä samat henkilöt, jotka vastaavat yleisesti Turun AMK:n tietoturvallisuudesta. Lisäksi E-tentin

Turun AMK:n pääkäyttäjällä on vastuu ohjelmiston tietoturvallisuuden ajantaisuudesta.



Kuvio 2. Voiko tenttijä käyttää tenttitilassa omia tallennusvälineitään?

E-tenttiä varten suunnitellussa tenttiakvaario-tilassa ei ole toistaiseksi sallittua käyttää omia tallennusvälineitä. E-tentin peruseräilyksen mukaisesti omia tallennusvälineitä ei myöskään tulisi olla tarvetta käyttää.

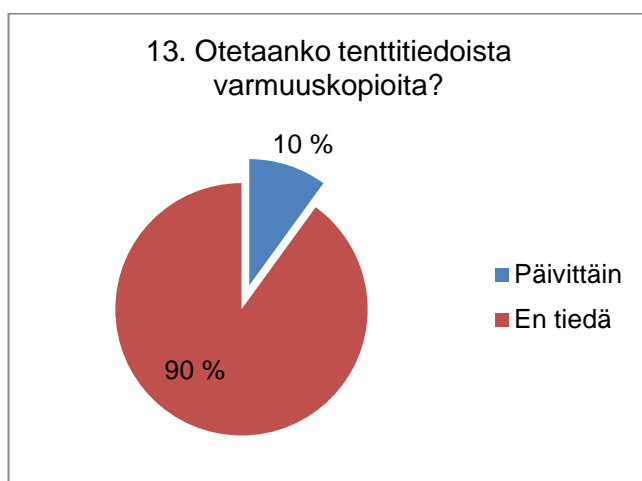


Kuvio 3. Voidaanko tenttiin liittää mitä tahansa tiedostotyyppisiä?

E-tentti tukee periaatteessa kaikkia mahdollisia tiedostotyyppisiä, sillä sen sisäänrakennettu tiedostojärjestelmä ei itsessään avaa vastausten

liitetiedostoja, vaan ne tulee avata arvioijan käyttämän tietokoneen ohjelmistoja käyttämällä. Tämä voi väärin toteutettuna aiheuttaa tietoturvariskin etenkin etätenttiä käytettäessä, jolloin opiskelija pystyy liittämään tenttiin tiedostoja omalta tietokoneeltaan. Tenttiin tallennetut tiedostot kuitenkin tarkastetaan haittaohjelmien varalta palvelun toimittajan palvelimella, jolloin tietoturvariski pienenee oleellisesti.

Tenttiakvaarion suhteen ongelma ei ole yhtä suuri, sillä tietokoneita hallitaan keskitetysti ja niiden ohjelmisto virtualisoidaan Turun AMK:n omilta palvelimilta. Näin tenttiakvaariossa jokaisesta tietokoneesta voidaan olettaa löytyvän samat ohjelmistot. Tiedostojen varsinainen tallennus ei tenttiakvaarion tietokoneilla tule olla mahdollista.

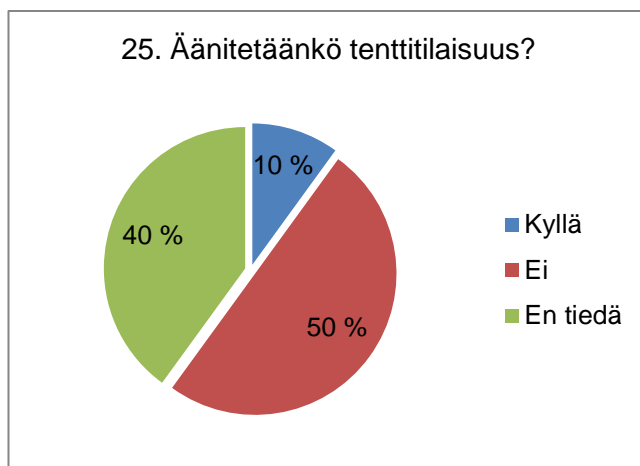


Kuvio 4. Otetaanko tenttiedostoista varmuuskopioita?

E-tenttiohjelmiston toimittaja varmuuskopioi E-tentin tiedostot päivittäin. Turun AMK ei ainakaan toistaiseksi luo varmuuskopioita ohjelmistosta tai siinä käytettävästä datasta, mikä luo selkeän tietoturvariskin. Nykyisin E-tentin ohjelmistotoimittaja säilyttää varmuuskopioita vain yhdessä paikassa, minkä vuoksi myös Turun AMK:n kannattaisi luoda tiedoista varmuuskopioita.

Tiedossa olevat ongelmakohtat

Avoimia kysymyksiä opinnäytetyön kirjoittamisen aikaan olivat vielä äänen taltiointi kameravalvonnan yhteydessä (Kuvio 5) sekä lasketaanko esimerkiksi sähkökatkoksen vuoksi keskeytynyt tentti tenttimiskerraksi (Kuvio 6). Kyselyn vastauksista käy hyvin ilmi ainakin näiden aiheiden kohdalla projektin yksityiskohtien epäselvyys. Ennen kuin pilotointivaiheesta siirrytään varsinaiseen käyttöönottoon, on näihin asioihin saatava yhtenäinen linja ja niiden on selkeästi tultava ilmi vähintäänkin projektin dokumentaatiossa.



Kuvio 5. Äänitetäänkö tenttitilaisuus?



Kuvio 6. Lasketaanko yhteyden katketessa kesken jäänyt tentin tenttikerraksi?

6 E-TENTIN TIETOTURVALLISUUDEN PARANNUSEHDOTUKSET

6.1 Tietoturvan kehitysehdotukset

Hämmästyttävien seikka tietoturvakartoituksen tuloksien valossa oli vastaajien tietämättömyys. Suurin osa vastaajista ei tiennyt oikeastaan mitään E-tentin tietoturvasta. Tietoa on saatavilla Turun AMK:n intranetistä, mutta tieto on tällä hetkellä todella hajanaista. Mikäli tietoturvan tasoa aiotaan nostaa, tulisi tieto saada helposti ymmärrettävänä jokaisen mahdollisen käyttäjän saataville.

E-tenttiä käyttävä ja ylläpitävä henkilöstö on koulutettava vastuulliseen tietoturvaan välittömästi, mikäli se etenee pilotointivaiheesta varsinaiseen tuotantokäyttöön. Suurelta osin tietoturvaa toki ohjaa AMK:n sisäinen tietoturvapoliittikka ja tietoturvakäytänteet.

E-tentissä on mahdollista käyttää monia eri tiedostomuotoja. Näin tulee ollakin, mutta sallittavat tiedostomuodot ja niiden tietoturvallisuus tulisi tarkastaa tasaisin väliajoin.

Tenttiin on mahdollista kirjautua ympäri vuorokauden. Tätä kannattaisi tarkastella kriittisesti, sillä ympärivuorokautiseen täysimittaiseen saatavuuteen ei pitäisi olla ainakaan toistaiseksi tarvetta, sillä tentit yleensä halutaan suorittaa päivä- tai ilta-aikaan. Kuitenkin esimerkiksi opiskelijan näkökulmasta tenttejä olisi hyvä pystyä varaamaan mihin kellonaikaan tahansa.

6.2 Tietosuojan kehitysehdotukset

Ensimmäinen asia, jonka huomasin tarkastellessani E-tenttiohjelmistoa, oli varaustietojen näkyminen jokaiselle käyttäjälle. Varaustiedon näkeminen sinänsä ei ole huono asia, mutta tässä tapauksessa jokainen käyttäjä näkee, kuka on varannut minkäkin tenttiajan. Tämä on selvä tietosuojariski, johon Turun AMK:n on otettava kantaa vaikuttaessaan ohjelmiston ajantasaisuuteen.

Ehdottomasti hyvä asia on, että Turun AMK:lla on ohjelmistolle oma pääkäyttäjä. Koska itse ohjelmisto ei sijaitse Turun AMK:n tiedostopalvelimella, vaan se on tuotettu pilvipalveluna, tulee tietosuojaan kiinnittää erityistä huomiota. Tämä onnistuu vain, jos pääkäyttäjäksi on nimetty tietty henkilö, joka vastaa yhteydenpidosta palvelimen ylläpitäjään.

Tenttitilassa on käytössä tallentava kameravalvonta, mutta ääntä ei kuitenkaan tallenneta. Tämä on selvä puute, joka tulisi ratkaista mahdollisimman nopeasti. Ongelmaksi muodostui ainakin pilotointivaiheessa se, että myös muiden kuin tenttijöiden oli mahdollista työskennellä kameravalvotussa tilassa.

E-tentin tenttiakvaariota valvoo tällä hetkellä Lemminkäisenkadun toimipisteen kirjaston henkilökunta. Käytettävien tietosuojakäytäntöjen puitteissa olisi syytä miettiä, kenelle vastuu valvonnasta ja tietosuojan ylläpitäminen halutaan antaa. Koulutuksella ja tietoisuuden lisäämisellä tähän voidaan toki vaikuttaa, mikäli nykyinen malli halutaan säilyttää myös tulevaisuudessa.

7 JOHTOPÄÄTÖKSET

E-tentti oli tietoturva- ja tietosuojakartoitusta tehdessä vasta pilotointivaiheessa, joten tietämys sen toiminnasta tai olemassaolosta ei ollut kovinkaan laajalle levinnyttä. Pilotointiryhmät olivat tehneet jo muutaman tentin käyttäen E-tenttiä, mutta nämä olivat olleet vain yksittäistapauksia, joilla lähinnä oli testattu palvelun teknistä toimivuutta.

Osittain tästä syystä kyselyyn vastanneita oli varsin pieni määrä verrattuna asian tärkeyteen. Vastaukset antoivat siis varsin vaihtelevan, mutta realistisen kuvan koko oppilaitoksen tietämyksestä E-tentin suhteen. Tietämys tietoturvasta ja tietosuojasta, jopa vain yleisellä tasolla, oli palvelun käyttäjillä melko heikkoa. E-tentin parissa päivittäin työskenteleville henkilökunnan edustajille tietoturva- ja tietosuoja-asiat olivat kuitenkin tuttuja.

Tietoturva- ja tietosuojakartoituksesta oli hyötyä E-tentti -järjestelmän suunnittelussa. Ohjelmistopalvelujen tarjoamisessa tulee ottaa huomioon monia asioita ja useimmiten tietoturva- ja tietosuoja-asiat jäävät liian vähäiselle huomiolle. Kartoituksen laatimisen tarkoituksena oli herättää projektin kanssa työskenteleviä ottamaan huomioon myös tietoturva- ja tietosuoja-asiat.

Suurin uhka ohjelmistoratkaisujen tietoturvalle ovat yleensä loppukäyttäjät. Vaikka Turun AMK:lla on olemassaolevat tietoturva- ja tietosuojapolitiikat sekä ohjeistukset sekä henkilökunnalle että opiskelijoille, on E-tentin käyttöönottovaiheessa muistutettava sen käyttäjiä vastuistaan.

Monet haittaohjelmat pääsevät tietokoneille vain käyttäjien tekemien virheiden vuoksi. Kun haittaohjelma pääsee käyttäjän tietokoneelle, voi se suorittaa tietokoneessa haitallista ohjelmakoodia ja levittää itseään eteenpäin muihin tietokoneisiin. Siksi tietoturvallisen ajattelun levittäminen on tärkeää sekä E-tentin että koko Turun AMK:n järjestelmien toimivuuden kannalta.

LÄHTEET

Andress, J. 2011. The Basics of Information Security – Understanding the Fundamentals of Infosec in Theory and Practice. Waltham: Elsevier Inc.

Henkilötietolaki 22.4.1999/523.

ISO/IEC 17799 2000.

ISO/IEC 27001 2005.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Nietula, V. 2011. Yrityksen tietoturvakartoitus. Viitattu 23.4.2012 https://publications.theseus.fi/bitstream/handle/10024/33969/Nietula_Veli.pdf?sequence=1.

Nilsson, A. 2008. Tietoturvakartoitus yrityksen Internet-palveluja tuottavassa yksikössä. Viitattu 24.4.2012 http://www.netlab.tkk.fi/opetus/s38310/07-08/Nilsson_090108.pdf.

Sorsa, N. 2011. Tietojärjestelmää uhkaavia tekijöitä ja tietoturvakartoitus. Viitattu 22.4.2012 https://publications.theseus.fi/bitstream/handle/10024/31913/Sorsa_Nina.pdf?sequence=1.

Spagnoletti, P.; Resca, A. 2007. The Duality of Information Security Management: Fighting Against Predictable and Unpredictable Threats. Viitattu 4.11.2012 http://eprints.luiss.it/955/1/JISSec_LUISSearch.pdf.

Stoneburger, G.; Hayden, C.; Feringa, A. 2004. Computer Security. Viitattu 4.11.2012 <http://csrc.nist.gov/publications/nistpubs/800-27A/SP800-27-RevA.pdf>.

Tietosuojavaltuutettu 2001. Ota oppaaksi henkilötietolaki! Viitattu 13.11.2012 <http://www.tietosuoja.fi/uploads/wvzmhnffsvyrhb5.pdf>.

Tietosuojavaltuutetun toimisto 2001. Oppilaitosten ATK-luokkien videovalvonta – Tietosuojavaltuutetun kannanotto. Viitattu 13.11.2012 <http://www.tietosuoja.fi/13740.htm>.

Viestintävirasto 2012. Tietoturvalliseen yhteiskuntaan. Viitattu 25.4.2012 <http://www.ficora.fi/index/palvelut/palvelutaiheittain/tietoturva.html>.

E-tentin tietoturva- ja tietosuojakyselyssä käytetyt kysymykset ja vastausvaihtoehdot	
Kysymyksen numero	Kysymys
1	Onko tietoturvallisuudesta vastaavaa henkilöä nimetty?
	On
	Ei ole
	En tiedä
2	Vahditaanko tenttimistä jonkun henkilön toimesta?
	Kyllä
	Ei
	En tiedä
3	Tapahtuuko tunnistautuminen samoilla tunnuksilla kuin Turun AMK:n windows-verkkoon?
	Kyllä
	Kyllä, pienin poikkeuksin
	Ei
	En tiedä
4	Onko Turun AMK:lla ajantasainen tietoturvapolitiikka ja toteutetaanko sitä e-tentin suhteen?
	Kyllä
	Kyllä on, mutta ei sovelleta e-tenttiin
	Ei ole
	En tiedä
5	Onko etätentin yhteys salattu?
	Kyllä, Turun AMK:lla on oma salaus
	Kyllä, käytetään palveluntarjoajan salausta
	Ei ole
	En tiedä
6	Voiko tenttijä käyttää tenttitilassa omia tallennusvälineitään?
	Kyllä, mitä tahansa
	Kyllä, muistitikkoa
	Kyllä, opiskelijan on mahdollisuus hakea tiedostoja verkkoasemaltaan
	Ei
	En tiedä
7	Lasketaanko yhteyden katketessa kesken jäänyt tentti tenttikerraksi?
	Kyllä
	Ei

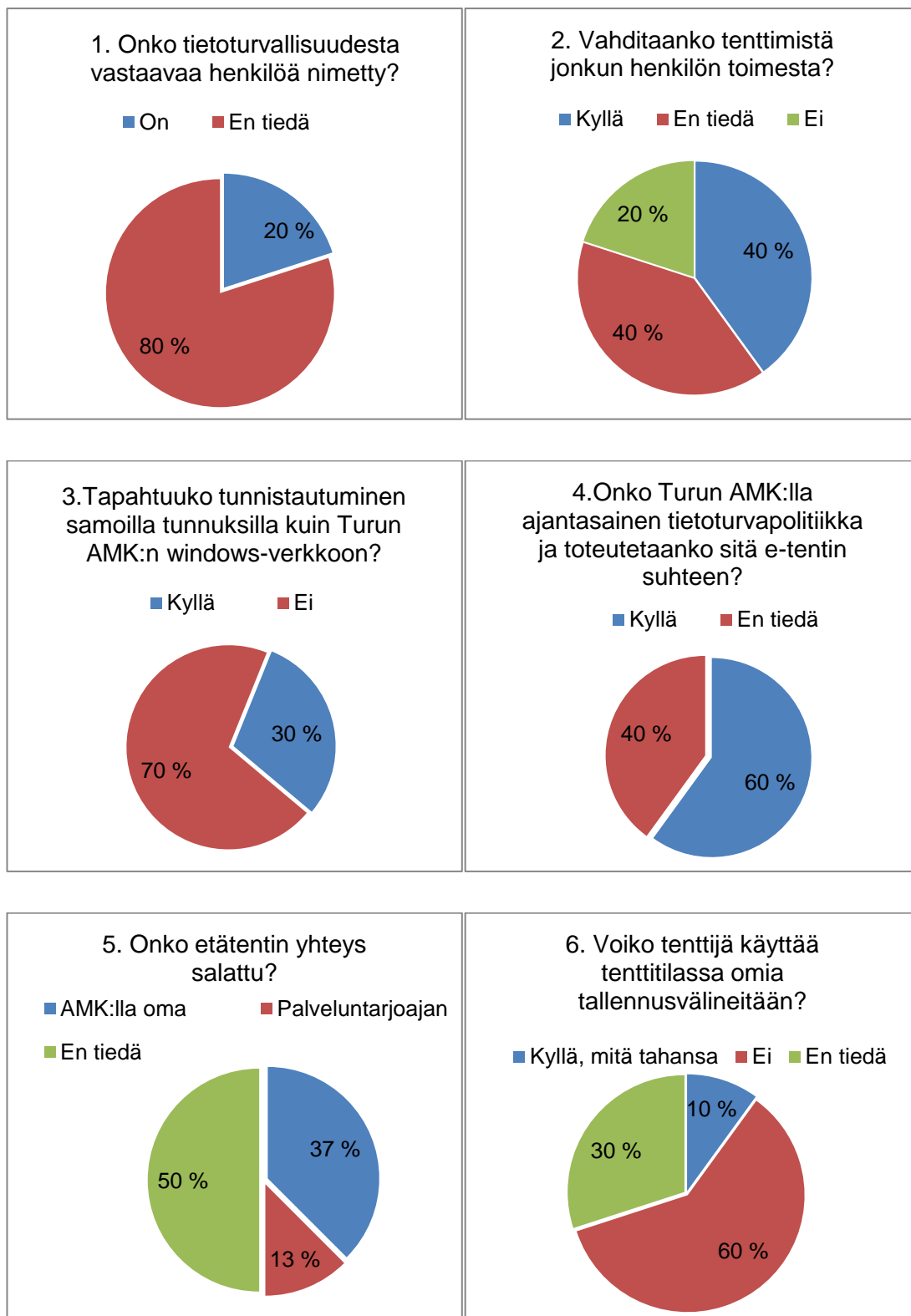
	En tiedä
8	Onko tenttitilasta mahdollista poistua vaaratilanteissa helposti?
	Kyllä
	Ei
	En tiedä
9	Käytetäänkö Turun AMK:n pelastussuunnitelmaa?
	Kyllä
	Kyllä, muokattuna
	Ei
10	Voidaanko tenttiin liittää mitä tahansa tiedostotyyppisiä?
	Kyllä
	Kaikki yleisimmät tiedostomuodot
	Vain muutama olennaisin
11	Voidaanko tenttiin liittää mitä tahansa tiedostotyyppisiä?
	Kyllä
	Ei
	Kyllä, mutta harvinaisemmat määritetään tapauskohtaisesti
12	Onko opiskelijoille kerrottu, mitä tiedostotyyppisiä on mahdollista tuoda e-tenttiin?
	Kyllä
	Ei
	Kyllä, mutta harvinaisemmat määritetään tapauskohtaisesti
13	Onko opettajien tiedot e-tenttiin luovutettu?
	Kyllä
	Jossain määrin
	Vain kriittisimpien asioiden osalta
14	Perehdytetäänkö e-tenttiä käyttävä henkilökunta tietoturvallisuuteen?
	Kyllä
	Ei
	En tiedä
15	Otetaanko tenttitiedoista varmuuskopioita?
	Kyllä, päivittäin
	Kyllä, viikoittain
	Kyllä, kuukausittain
16	Säilytetäänkö tenttitietojen varmuuskopioita useassa paikassa?
	Kyllä
	Ei
	En tiedä
17	Pystyykö Turun AMK vaikuttamaan e-tenttiohjelman ajantasaisuuteen?
	Kyllä, ja tekee sitä aktiivisesti
	Jossain määrin
	Kyllä, mutta ei tee sitä aktiivisesti

	Ei lainkaan
16	Säilytetäänkö tenttitiedot sekä sähköisesti että paperisena?
	Kyllä, molemmin tavoin
	Vain sähköisenä
	Vain paperisena
	Ei lainkaan
	En tiedä
17	Pääsevätkö kaikki opettajat käsiksi kaikkiin tenttietoihin?
	Kaikki pääsevät käsiksi kaikkiin tentteihin
	Vain omiin tentteihinsä
	Vain tietyt opettajat
	En tiedä
18	Onko ohjelmalla pääkäyttäjää?
	Kyllä, myös Turun AMK:n puolella
	Kyllä, mutta vain palveluntarjoajalla
	Ei ole
	En tiedä
19	Ovatko tenttien varaustiedot kaikkien nähtävillä?
	Kyllä
	Vain opettajille
	Vain omien tenttien varaustiedot
20	Onko asiakirjojen hävityksestä ohjeistusta?
	Kyllä
	Ei
	En tiedä
21	Miten tietoaineisto salataan?
	Sekä laitteistopohjaisesti että ohjelmistopohjaisesti
	Vain laitteistopohjaisesti
	Vain ohjelmistopohjaisesti
	Ei lainkaan
	En tiedä
22	Perehdytetäänkö henkilökunta henkilötietojen käsittelyyn?
	Perehdytetään
	Ei perehdytetä
	Vain tietyt henkilöt
	En tiedä
23	Onko henkilötiedot suojattu?
	Kokonaan
	Osittain
	Ei lainkaan
	En tiedä
24	Voiko kuka tahansa olla tenttien valvoja?
	Kyllä

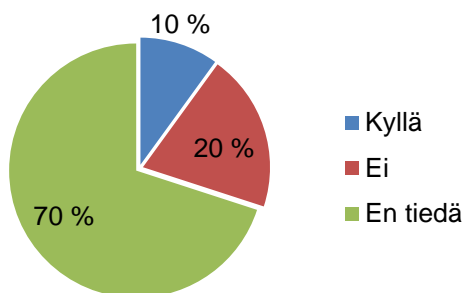
	Vain tietyt henkilöt valvovat tenttejä
	En tiedä
25	Äänitetäänkö tenttitilaisuus?
	Kyllä
	Ei
	En tiedä
26	Onko tenttitilassa käytössä kameravalvonta?
	Kyllä
	Ei
	En tiedä
27	Onko tenttitilassa mahdollisuus moneen yhtäaikaiseen tenttiin?
	Kyllä
	Ei
	En tiedä
28	Mikäli tentti tehdään etätenttinä, jättääkö tenttisivu jonkin tiedoston käytetylle tietokoneelle?
	Kyllä
	Ei
	En tiedä
29	Onko etätenttiä mahdollista tehdä mobiililaitteella?
	Ei ole
	Sekä tabletilla että älypuhelimella
	Vain tabletilla
	Vain älypuhelimella
	En tiedä
30	Testataanko varmuuskopioiden toimivuutta säännöllisesti?
	Päivittäin
	Viikoittain
	Kuukausittain
	Vuosittain
	Ei lainkaan
	En tiedä
31	Onko käytössä toipumissuunnitelmaa?
	Kyllä
	Ei
	Laatiminen on työn alla
	En tiedä
32	Annetaanko e-tentistä riittävästi tietoa sen käyttäjille?
	Kyllä
	Vain opettajille
	Vain opiskelijoille
	Ei
	En tiedä

33	Onko tietoa e-tentistä saatavilla helposti?
	Kyllä
	Ei
	En tiedä
34	Milloin e-tenttiin on mahdollista kirjautua?
	Ympäri vuorokauden
	Vain päivisin
	En tiedä

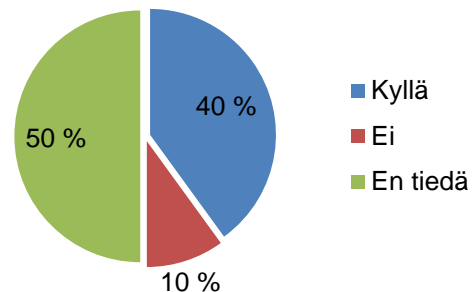
E-tentin tietoturva- ja tietosuojakyselyn tulokset kaavioina esitettynä



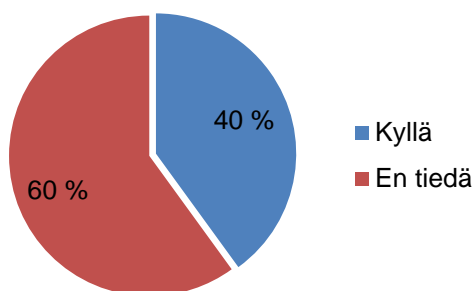
7. Lasketaanko yhteyden katketessa kesken jäänyt tentti tenttikerraksi?



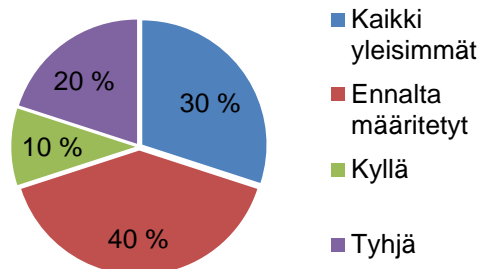
8. Onko tenttitilasta mahdollista poistua vaaratilanteissa helposti?



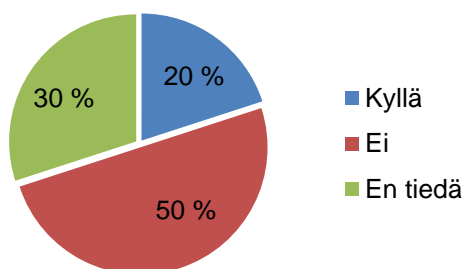
9. Käytetäänkö Turun AMK:n pelastussuunnitelmaa?



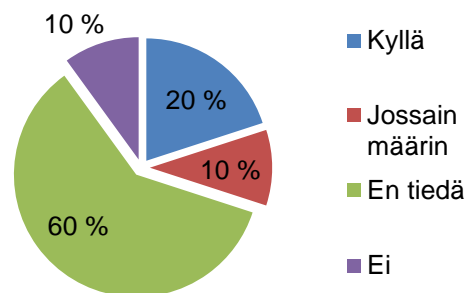
10. Voidaanko tenttiin liittää mitä tahansa tiedostotyyppiä?



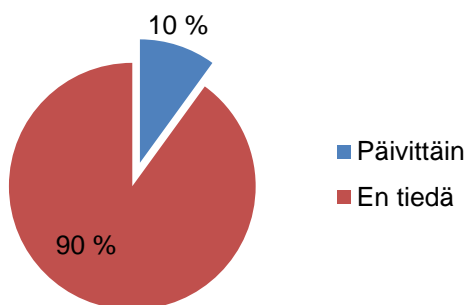
11. Onko opiskelijoille kerrottu, mitä tiedostotyyppiä on mahdollista tuoda e-tenttiin?



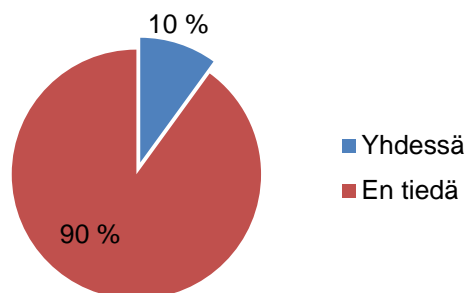
12. Perehdytetäänkö e-tenttiä käyttävä henkilökunta tietoturvasuuteen?



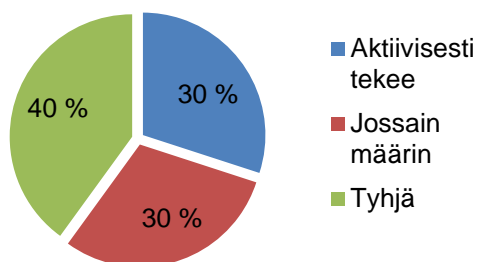
13. Otetaanko tenttitiedoista varmuuskopioita?



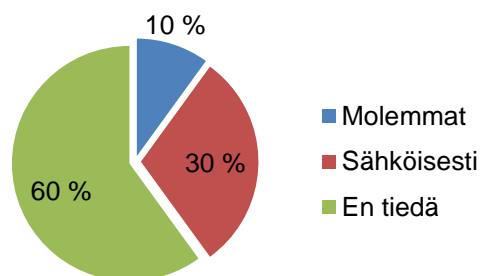
14. Säilytetäänkö tenttitietojen varmuuskopioita useassa paikassa?



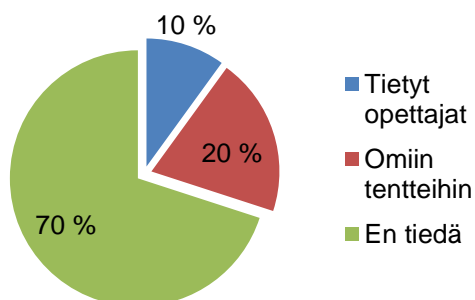
15. Pystyykö Turun AMK vaikuttamaan e-tenttiohjelman ajantasaisuuteen?



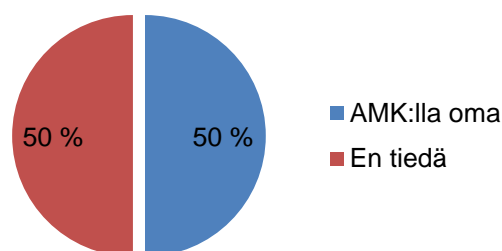
16. Säilytetäänkö tenttitiedot sekä sähköisesti että paperisena?



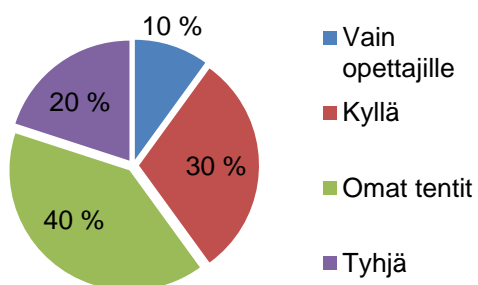
17. Pääsevätkö kaikki opettajat käsiksi kaikkiin tenttitietoihin?



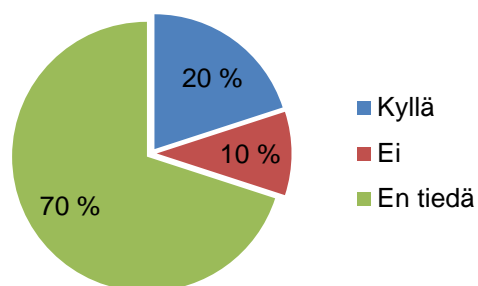
18. Onko ohjelmalla pääkäyttäjää?



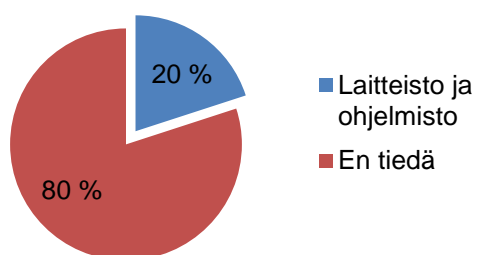
19. Ovatko tenttien varaustiedot kaikkien nähtävillä?



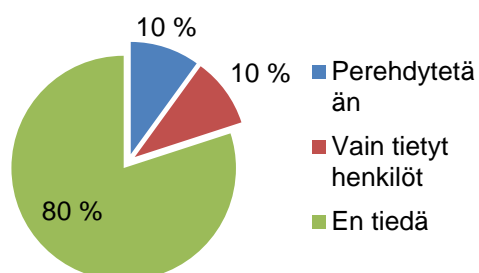
20. Onko asiakirjojen hävityksestä ohjeistusta?



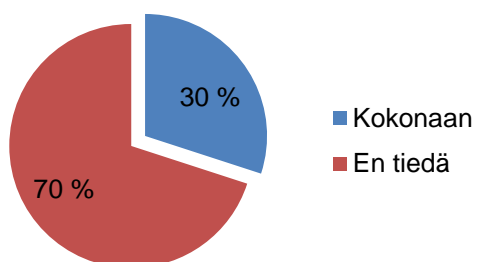
21. Miten tietoaineisto salataan?



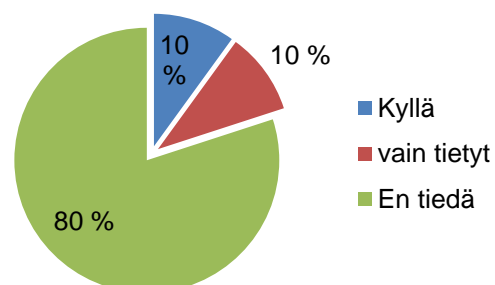
22. Perehdytetäänkö henkilökunta henkilötietojen käsittelyyn?



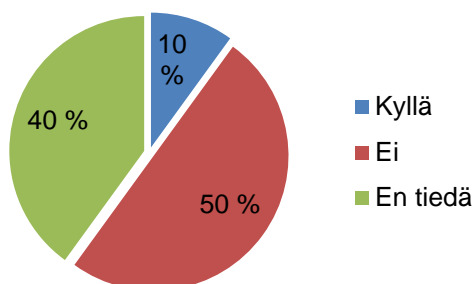
23. Onko henkilötiedot suojattu?



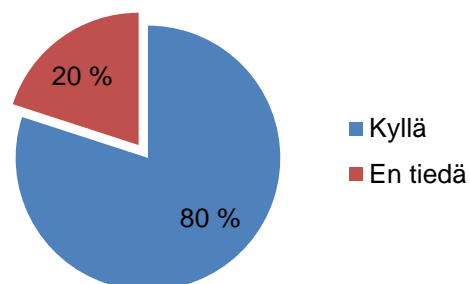
24. Voiko kuka tahansa olla tenttien valvoja?



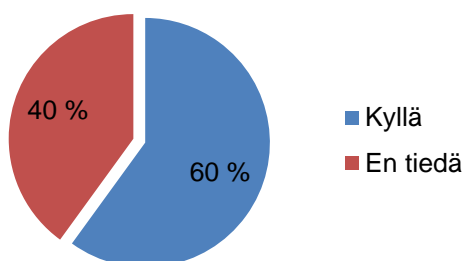
25. Äänitetäänkö tenttitilaisuus?



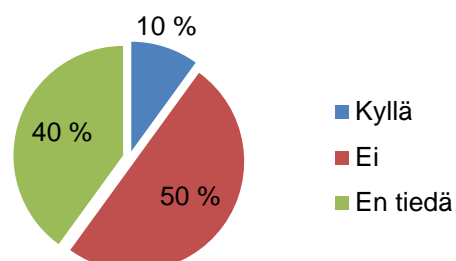
26. Onko tenttitilassa käytössä kameravalvonta?



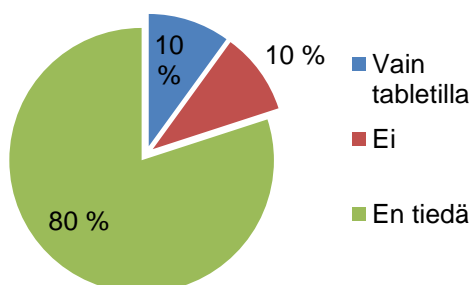
27. Onko tenttitilassa mahdollisuus moneen yhtäaikaiseen tenttiin?



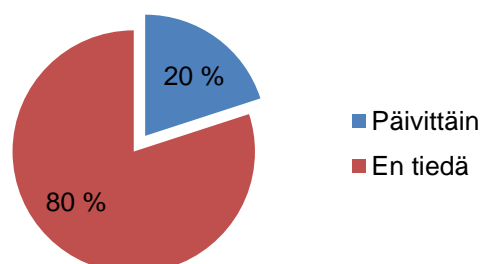
28. Mikäli tentti tehdään etätenttinä, jättääkö tenttisivu jonkin tiedoston käytetylle tietokoneelle?



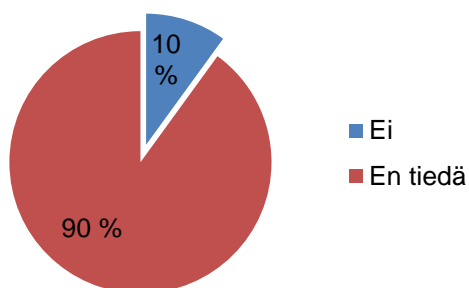
29. Onko etätenttiä mahdollista tehdä mobiililaitteella?



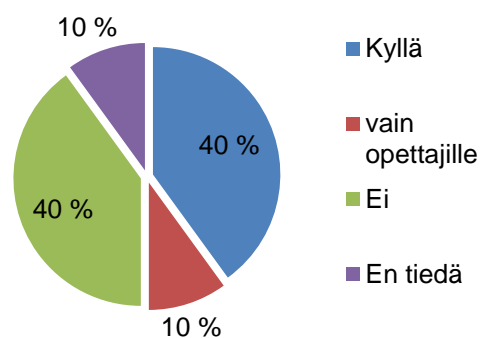
30. Testataanko varmuuskopioiden toimivuutta säännöllisesti?



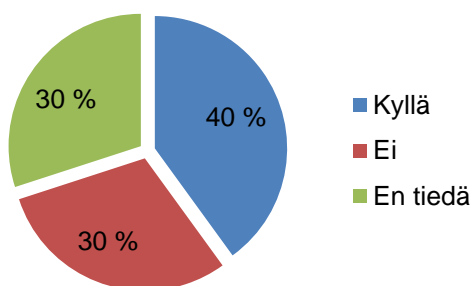
31. Onko käytössä
toipumissuunnitelmaa?



32. Annetaanko e-tentistä
riittävästi tietoa sen käyttäjille?



33. Onko tietoa e-tentistä
saatavilla helposti?



34. Milloin e-tenttiin on
mahdollista kirjautua?

