Opinnäytetyö (AMK)

Tietojenkäsittely

2017

Kim Ristimella

MURTAUTUMISTESTAAJAN KOMPETENSSIANALYYSI

TURKU AMK
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely

2017 | 46

Kim Ristimella

MURTAUTUMISTESTAAJAN KOMPETENSSIANALYYSI

Opinnäytetyö tehdään toimeksiantona Turun ammattikorkeakoululle. Sen tarkoituksena analysoida vastaako Turun ammattikorkeakoulun opetussuunnitelma yritysten tarpeeseen murtautumistestauksen osalta. Turun ammattikorkeakoulun tietoturvaopetus analysoidaan tietoturvaopetussuunnitelman ja itselleni toteutuneen opetuksen tasosta saatujen kokemuksien analysoinnilla. Rekrytointivaatimukset on kerätty nimettömänä pysyvän suuren tietoturvayrityksen henkilöstörekrytointiosaston haastattelun avulla. Haastatteluissa käytettiin menetelmänä teemahaastattelua ja haastatteluaineisto analysoitiin sisällönanalyysin menetelmällä.

Yhteenveto tietoturvayrityksen haastattelusta tuo esille tärkeimpinä rekrytointivaatimuksina tietoturvan osa-alueiden, verkkoliikenteen ja protokollien perusperiaatteiden tuntemus. Linux ja Windows komentoriviperusteet on osattava. Sovelluskehityksessä sovelluksien toimintaperiaatteet ja toimintalogiikka on ymmärrettävä. Agile-projektinhallinnan ymmärrys ja osaaminen ovat tärkeitä.

Johtopäätös analysoidusta tiedosta on, ettei Turun ammattikorkeakoululla ole suuria ongelmia opetuksen toteutumisessa, mutta alan perustietotaitotason opetusta on korostettava. Turun ammattikorkeakoulun opetus keskittyy oikeaan kehitysalueeseen, mutta jättää perustietojen opetuksen liian vähälle.

Kehitysparannuksena ehdotetaan Linux- ja Windows-käyttöjärjestelmien komentorivikomentojen, käyttöjärjestelmien toiminnallisuuden ja sovelluksien toimintaperiaatteiden perusteellista opettamista ja pieniä muutoksia opetussuunnitelmiin.

ASIASANAT:

Tietoturva, rekrytointi, kyberturvallisuus, palomuurit, salaus, tietomurto, verkkohyökkäykset, konsultointi, sovellusohjelmointi

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Bachelor of information systems

2017 | 46

Kim Ristimella

PENETRATION TESTERS' COMPETENCE ANALYSIS

This thesis was commissioned by Turku University of Applied Sciences (TUAS). This purpose of this thesis was to analyze the information security curriculum of TUAS and its suitability to the present recruitment requirements in the field of information security penetration testing. The information security education offered by TUAS is defined by its information security curriculum and the level of education is defined by the students' own experience in information security.

To achieve the purpose of this thesis, recruitment requirements were gathered from interview with two members of the Human Resources Department of a large information security company. The type of interviewing was a semi-structured interview and the method of analyzing the collected data was content analysis.

The findings of the interview indicate that the most important requirements in recruiting is the knowledge of basic principles of information security, network traffic, and protocols.

In conclusion, TUAS does not have severe problems with their educational effectiveness but basic knowledge of information education must be emphasized. The TUAS information security education focuses on the right aspects of specific information technologies, such as firewalls but the amount of general information technology education remains disproportionately small.

Therefore, it is recommended that TUAS focus on teaching Linux and Windows operation systems, their command line commands and software's operating principles more thoroughly. This thesis also proposes some changes to the curriculum and implementation of peer teaching.

KEYWORDS:

Information security, human resources, cyber security, firewalls, encryption, penetration testing, network attacks, consulting, software development

SISÄLTÖ

KUVAT

1 JOHDANTO

Tämän opinnäytetyön aiheena on selvittää vastaako Turun ammattikorkeakoulun opetussuunnitelma yritysten tarpeeseen murtautumistestauksen osalta. Aiheessa kiinnostavinta on selvittää ammattini rekrytointivaatimuksia. Valitsin aiheen alun perin oman kiinnostukseni perusteella alaa kohtaan, mutta opinnäytetyöni muuttui myöhemmin toimeksiannoksi, koska siitä oli myös hyötyä Turun ammattikorkeakoululle. Työ rajoittuu aiheen laajuuden vuoksi yleisimpiin tietoturvakonsultin ja tietoturva-ammattilaisen työtehtäviin.

Työni tavoite on saada kattavasti kehitysehdotuksia Turun ammattikorkeakoululle, jotta tietoturvaopetus toisi opiskelijoille mahdollisimman hyvät valmiudet työelämään ja tuleviin haasteisiin. Opinnäytetyössäni haastattelen ammattikorkeakoulun tietoturvaopetuksen henkilöstöä, analysoin opetussuunnitelmaa ja haastattelen ison tietoturvayrityksen henkilöstörekrytoinnin ammattilaisia. Analysoin saamiani tietoja käyttäen tukena tutkielmani teoriaosuutta tietoturva-alasta.

Olen työskennellyt opiskelija-assistenttina Turun ammattikorkeakoulussa tietoturvaprojekteissa jo yli vuoden, jolloin olen saanut hyvän käsityksen tietoturva-ammattilaisen arjesta. Käytän työssä saatua tietoutta opinnäytetyössäni hyödyksi tekemällä haastattelukysymyksiä, jotka tiedän olevan oppimani perusteella tärkeitä. Alan tietotaidon avulla pystyn analysoimaan tarkasti haastatteluissa tulevia aiheita. Työ myös hyödyttää minua tulevaisuudessa työnhaussa, koska tiedän rekrytointivaatimukset ja voin sen vuoksi keskittyä tärkeimpien asioiden opetteluun. Työni sisältää teoriaa tietoturvasta ja rekrytoinnista. Se selvittää tietoturva-alan rekrytointivaatimuksia haastattelulla ja sisältää analyysiä saaduista tiedoista.

Haastatteluissa metodina käytän teemahaastattelua. Teemahaastattelu on vaativa tiedonkeruumuoto. Sitä edeltää asiaongelman ja tutkimusongelman pohdiskelu kuten kaikkea muutakin tutkimusta. Teemahaastattelutilanteessa esiin nostettavat teemat ovat tarkoin pohditut ja määritellyt. Teemahaastattelu on keskustelua, jolla on etukäteen päätetty tarkoitus. Se ei ole tavallista arkikeskustelua. On erittäin tärkeää, että haastattelun rakenne pysyy hallinnassa. Etuna teemahaastattelussa muihin haastattelumuotoihin nähden on, että sen kerättävä aineisto rakentuu aidosti haastateltavan henkilön kokemuksista käsin. Ongelmana teemahaastattelussa on, että haastateltava henkilö ja hänen kertomuksensa alkaa johdatella haastattelua liikaa. Silloin teemahaastatteluaineistosta tu-

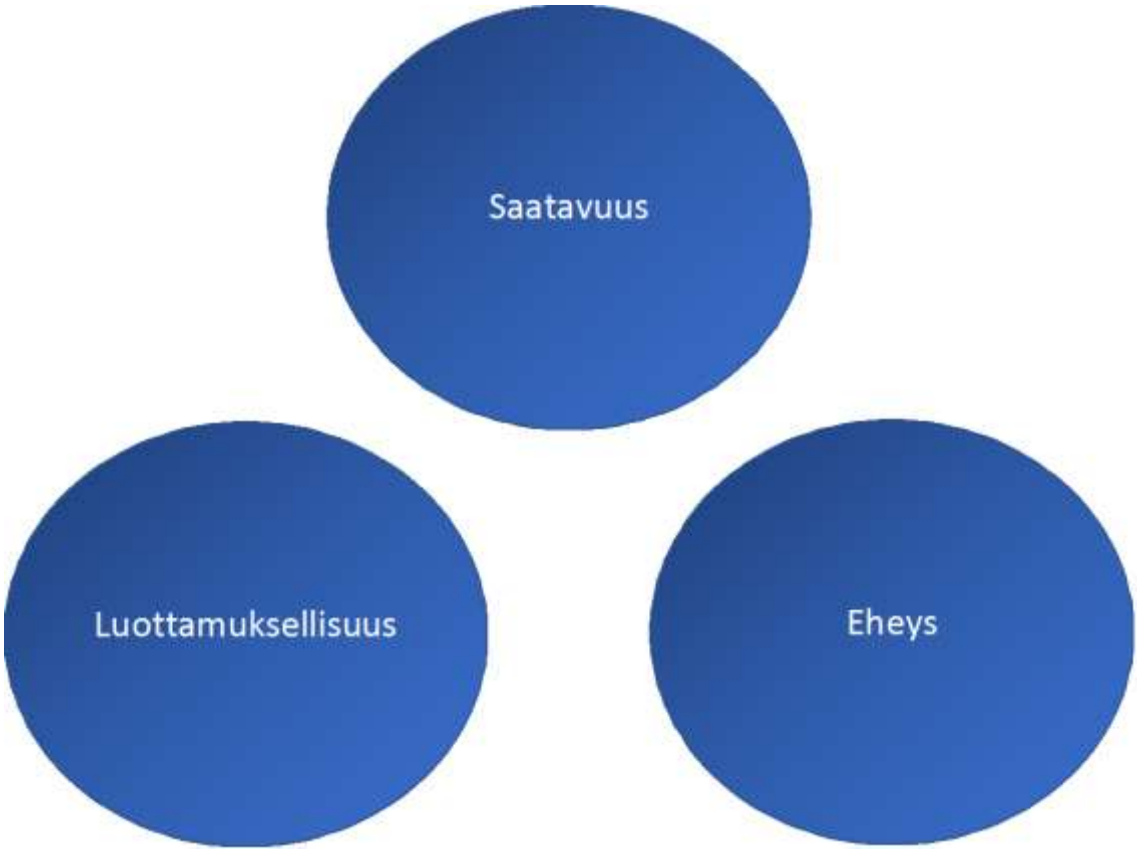
lee helposti sekava kokoelma ihmisten puhetta. Tutkijan on näin vaikea jälkeenpäin jäsennellä tekstimassaa ja muodostaa siitä analyysiä. (Tilastokeskus - Virtual Statistics – Tiedonkeruu 2017)

2 TIETOTURVA

Seuraavaksi opinnäytetyössäni kerron teoriaa tietoturvasta ja rekrytoinnista. Teoriasisältö kattaa tarvittavan informaation haastattelujen ymmärtämiseen, analysoitiin ja vertailuun. Kiinnitän huomiota myös teoriaosuuden sisällön ja haastatteluista saatujen tietojen mahdollisiin yhteyksiin, ja käytän sitä apuna analysoinnin tekemisessä.

2.1 Tietoturva

Tietoturvallisuus on tärkeä osa organisaation toiminnan laatua. Tietoturvajärjestelyn tarkoituksena on tietoaineistojen, tietojärjestelmien ja palveluiden asianmukaisen suojauksen varmistus siten, että niiden luottamuksellisuus, eheys ja saatavuus pysyvät koskemattomana ja niihin liittyvät riskit otetaan huomioon. Tätä kutsutaan CIA-triadiksi (Kuva 1).



Kuva 1. CIA-triadi.

Tiedot eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan, haittaohjelmien, laitteisto- tai ohjelmistovikojen tai muiden vahinkojen, häiriötilanteiden tai tapahtumien vuoksi. Järjestelmien, tietojen ja palveluiden on oltava luotettavia, ajan tasalla ja oikeita. Tietojen, järjestelmien ja palveluiden on pysyttävä toiminnassa ja oltava saatavilla mahdollisimman hyvin. Palveluiden on kyettävä tunnistamaan käyttäjät luotettavasti sekä tuottamaan tapahtumalokia, josta tapahtumat voidaan jälkikäteen tarvittaessa selvittää. (Pietikäinen 2013, 17.)

Tietoturvalla pyritään suojaamaan yritykselle tai yksityiselle tärkeät tiedot ulkopuolisilta. Tavoitteena tietoturvassa on säilyttää yksilön tai organisaation tiedot mahdollisimman suojassa ulkopuolisilta, mutta samalla pitää ne saatavilla niille oikeutetuille henkilöille. Näin tieto saadaan pysymään luottamuksellisena. Tiedolla ja dokumenteilla on turvaluokitus, jolla määritellään oikeus tietojen käyttöön, säilytykseen ja tuhoamiseen. Tietojen **eheydellä** tarkoitetaan muuttumattomuutta sitä käsiteltäessä. Eheyden varmistaminen tapahtuu **kiistämättömyydellä**, eli tiedon siirron tai käsittelyyn osallistuneiden käyttäjien tunnistautumisen valvonnalla. **Pääsynvalvonnalla** varmistetaan, ettei tietoihin pääse käsiksi ulkopuoliset ja niihin oikeutettujen pääsyä on mahdollista valvoa ja rajoittaa. **Saatavuudella** tarkoitetaan tiedon mahdollista käyttöä niille, jolla siihen on oikeus. Tämä on tarkoitus pystyä toteuttamaan mahdollisimman helposti ja viiveettömästi. **Tarkastettavuus** tarkoittaa sitä, että tietojenkäsittelyn tuloksena saatu tieto on kyettävä tarkistamaan ja sen oikeellisuus osoittamaan. (Tietoturva 2017.)

Tietoturvallatoimenpiteillä **turvataan kaikkien etuja**. Tietoturvallisuus on yhteiskunnan infrastruktuurin perusedellytys. Yhteiskunnan toiminnot ovat suurelta osin riippuvaisia tietoliikenteestä. Suurimmat tietoturvallisuuden ongelmat liittyvät yleisesti huolimattomuuteen ja osaamattomuuteen. (Pietikäinen 2013, 18.)

Suomen lainsäädännössä on paljon **tietoturvavelvoitteita**, jotka varmistavat, että tietoturvallisuus hoidettaisiin asianmukaisesti. Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annettuihin lakeihin, ja lisäksi useisiin muihin lakeihin. Keskeisiä tietoturvavelvoitteita ovat esimerkiksi laki viranomaisten toiminnan julkisuudesta 18§, henkilötietolaki 32§ ja valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 8§. (Pietikäinen 2013, 19 – 20.)

2.2 Tietoturvan suojausmenetelmät

Tietoturvan suojausmenetelmät voidaan jakaa kolmeen ryhmään: tekniseen, fyysiseen ja hallinnolliseen.

Teknisellä tietoturvalla pyritään käytettyjen laitteistojen ja ohjelmistojen tietoturvapuutteiden minimoimiseen. Järjestelmiin pääsyä ja niissä olevien tietojen säilymistä luottamuksellisina valvotaan käyttäjähallinnan avulla. Lähiverkoissa on syytä varmistaa, ettei ulkopuoliset pääse suoraan käsiksi sen sisältöön. Tällaisia varmistuksia ovat palomuurit sekä käsiteltävän tiedon salaus. (Suojausmenetelmät 2017.)

Muita teknisiä suojausmenetelmiä ovat esimerkiksi haittaohjelmien torjunta, päätelaitteiden suojaus, tiedonsiirron suojaus, varmuuskopiointi ja muut varmistukset ja käyttöturvallisuus. (Elinkeinoelämän keskusliitto 2017.)

Fyysisellä tietoturvalla tarkoitetaan suljetussa tilassa olevia järjestelmiä tai informaatiota. Lukituilla tiloilla pyritään varmistamaan, ettei järjestelmiin tai tietoihin pääse ulkopuoliset käsiksi. (Suojausmenetelmät 2017.)

Hallinnollisella tietoturvalla tarkoitetaan työntekijöiden ja organisaation jäsenten riittävää tietoturvaosaamista. Jäsenten täytyy ymmärtää käyttäjätietojen käsittelyyn kuuluvat säännöt, ja salasanojen monimutkaisuuteen liittyvät ohjeistukset. Käyttäjätietoja ei saa kirjoittaa lapuille tai säilyttää asiattomien henkilöiden ulottuvilla. Henkilökohtaisia käyttäjätunnuksia, salasanoja, toimikorttia tai PIN-koodeja ei saa antaa toisen henkilön käyttöön. Tiedusteluihin, jotka koskevat käyttöoikeuksiin tai käyttäjä-tietoihin pitää aina suhtautua epäilevästi. Salasana on vaihdettava riittävän usein ja heti, jos sen epäillään päätyneen vääriin käsiin. Työpaikan käyttäjätietoja ei saa käyttää ulkopuolisissa palveluissa. Tietohallintohenkilöstö ei koskaan tarvitse käyttäjätietojasi työtehtäviensä hoitamiseksi. (Suojausmenetelmät 2017.)

Tietoturvallisuus ja **tietoturvallisuuden tuloksellinen johtaminen** edellyttävät sitoutumista sen kehittämiseen. Johdon on pystyttävä takaamaan tietoturvatoimintaan tarvittavat resurssit. Tietoturvallisuus on kehitettävä osaksi jokapäiväistä yritystoimintaa ja sen kulttuuria. Koko henkilöstö on omalla osaamisellaan mahdollista saada kehittämään tieto-turvallisuutta. Näillä asioilla saadaan luotua organisaatioille toiminnan tarpeet täyttävä tietoturvallinen toiminta- ja palveluympäristö. Organisaation korkea tietoturvakult-

tuuri tuo edellytykset kustannustehokkaalle riskienhallinnalle ja toimivalle tietoturvallisuuden hallinnalle. Säännöllinen tietoturvakoulutus ylläpitää henkilöstön tietoturvaosaamista ja -tietoisuutta, varsinkin tiedon turvallisessa käsittelyssä. Oman organisaation tietoturvallisuutta tulee myös testata. Hyvin johdettu organisaatio määrittelee selkeät tietoturva- ja turvallisuustehtävät, tehtävissä toimivien vastuut ja raportointikäytännöt. (Valtionhallinnon tietoturvallisuuden johtoryhmä 2009.)

2.3 Murtautumistestaus

Murtautumistestauksella on pitkät perinteet tietoturva-alalla. Perinteisellä murtautumistestauksella ei ollut formaalia toteutustapaa, mutta nykyisin on. Esimerkiksi PTES-standardi (Penetration Testing Execution Standard) (PTES 2014) ja muut standardit ovat kehittäneet murtautumistestausta. PTES standardi kuvaa murtautumistestauksen prosessia ja antavat ohjeita sen suorittamiseen. (Turun ammattikorkeakoulu 2014, 17 — 18.)

Murtautumistestaus on prosessi, jossa yritetään päästä käsiksi informaatioon, johon ei pitäisi muutoin olla pääsyä. Jos murtautumisen kohteena on esimerkiksi tietokone, on onnistuneen murtautumisen merkkinä CIA-triadin rikkoutuminen. Esimerkiksi informaation lukeminen, sen sisältöön käsiksi pääseminen tai sen tuhoaminen saattavat olla onnistuneen murtautumisen jälkiä. Murtautumistestaajan ja hyökkääjän suurin ero, on murtautumistestauksen luvallisuus. Murtautumistestaajalla on aina luvat murtautumistestaukseen liittyviltä ja hän on velvollinen tuottamaan tehdystä työstä raportin. Murtautumistestauksen ideana on parantaa testattavan ympäristön tietoturvallisuutta. (SANS 2006, 3.)

Monessa murtautumistestaustapauksessa testaajalle annetaan pääsy tavalliseen käyttäjään. Näissä tapauksissa usein tarkoituksena on löytää haavoittuvuuksia, joiden avulla päästään käsiksi tietoihin, joihin ei normaalisti olisi käyttöoikeutta. (SANS 2006, 3.)

Jotkin murtautumistestaukset tehdään löytääkseen yhden haavoittuvuuden tai sen syyn. Monessa tapauksessa kuitenkin murtautumistestauksen päämäärä on löytää mahdollisimman paljon haavoittuvuuksia ja dokumentoida ne mahdollisimman hyvin. Hyvän dokumentoinnin avulla haavoittuvuuksien varmistus ja korjaus olisi helpompaa. (SANS 2006, 3.)

Murtautumistestaus on tärkeää, sillä se mahdollistaa pelkän puolustuksen lisäksi hyökkäysperspektiivin. Tämän avulla voidaan löytää nopeasti haavoittuvuuksia ja ymmärtää

miten hyökkääjä näkee järjestelmän. Suurin osa järjestelmään tulevista hyökkäyksistä ovat automatisoituja ja vanhoja. Hyvin harvalla on täysin uusia hyökkäystapoja, joihin suojauksia ei olla vielä kehitetty. Monessa tilanteessa yrityksen IT-osasto tietää haavoittuvuuksista, mutta ei saa tarvittavia resursseja niiden korjaukseen tai ei pysty tarpeeksi tehokkaasti raportoimaan niistä yritysjohdolle. Tässä tilanteessa ulkopuolisen ammattilaisen näkökulma ja tehokkaasti raportoitu haavoittuvuuksien selvitys voi antaa IT-osastolle tarvittavat resurssit. IT-osasto myös saa hyvää harjoitusta hyökkäyksien tunnistamiseen. Murtautumistestauksella voidaan testata jo olemassa olevan tietoturvallisuuden toimivuus. (SANS 2006, 5 — 6.)

Murtautumistestaus PTES-standardin mukaan alkaa aina alkukeskustelulla. Tarkoituksena on selvittää, miten laajasti murtautumistestaus tehdään. Luvat ja laillisuus tarkistetaan tässä vaiheessa ja tarvittavat dokumentit tehdään. Lähes koko prosessi suunnitellaan tässä vaiheessa, ennen kuin järjestelmää lähdetään testaamaan. (PTES 2014.)

Alkukeskustelun ja laillisuuden varmistuksen jälkeen tarkoituksena on kerätä mahdollisimman paljon informaatiota murtautumistestauksen kohteesta. Usein yritykset haluavat säästää resursseja, joten tässä tilanteessa murtautumistestaajalle annetaan valmiiksi esimerkiksi järjestelmien verkko-osoitteet, käyttöjärjestelmät ja mahdolliset järjestelmässä olevat ohjelmistot. (PTES 2014.)

Tämän jälkeen luodaan riski- ja uhkamatriisi. Etsitään mihin mahdollisiin ohjelmistoihin tai järjestelmän osiin voi olla mahdollista päästä, ja mitä siihen tarvitaan. Tämän jälkeen etsitään haavoittuvuuksia ja tutkitaan mahdollisia ongelmia järjestelmissä. Järjestelmän haavoittuvuuksien löytämisen jälkeen tarkoituksena on käyttää hyväksi löydettyjä haavoittuvuuksia ja mahdollisesti päästä järjestelmään sisälle. Järjestelmään päästyä murtautumistestaaja usein joutuu käyttämään lisää haavoittuvuuksia tai asentaa erilaisia käynnistyskomentoja, jotta järjestelmään joko päästään uudestaan helposti sisälle tai saamaan enemmän käyttöoikeuksia järjestelmään. (PTES 2014.)

Raportointi tapahtuu jatkuvasti murtautumistestauksessa, se alkaa alkukeskusteluista ja päättyy vasta murtautumistestauksen päätyttyä. Raportoinnin tärkeys murtautumistestauksessa on todella suuri, sillä sen perusteella usein mahdollisesti löydetyt haavoittuvuudet korjataan ja niiden käyttö estetään. Raportista voi myös löytyä ongelmia tai haavoittuvuuksia, joita murtautumistestaaja ei huomannut. (PTES 2014.)

3 REKRYTOINTI

Rekrytointi on yrityksessä tapahtuvaa henkilöstöhankintaa. Henkilöstöhankinta on toimenpide, jolla hankitaan organisaatioon henkilöitä, joiden ominaisuuksia organisaatio tarvitsee (Forsberg 2007, 29). Yksittäinen rekrytointi voidaan nähdä rekrytointiprojektina. Siinä on nähtävissä projektimaisesti suunnittelu-, aloitus-, toteutus-, päätöksenteko- ja seurantavaiheet. Siihen kuuluvat tarpeen arviointi, hakumenettely ja -kanavan valinta, vertailu, työntekijän valinta, päätöksenteko ja laillisuusvalvonta. (Ahvonen & Ollonqvist 2008, 20.) Rekrytoinnin onnistuminen vaatii ennakointia, pitkäjänteisyyttä ja laaja-alaisuutta (Forsberg 2007, 11).

Jokainen prosessivaihe on toteutettava hyvin. Todellisen henkilöstöhankintatarpeen arviointi on tärkeä vaihe, jo ennen työntekijän hakuvaiheen aloitusta. Prosessi ei pääty työntekijävalintaan, vaan uusi henkilö on perehdytettävä työhön ja koko henkilöstöä kehitetään. Henkilöstörekrytointi ei pelkästään tuo työpanosta, vaan uuden henkilön kautta voidaan saada inhimillistä pääomaa ja uusi yhteistyöverkosto. Uuden työntekijän kautta voidaan myös saada potentiaalisia työntekijöitä lisää, jotka eivät muutoin olisi rekrytoitavissa. (Ahvonen & Ollonqvist 2008, 21 – 22.)

Rekrytointiin liittyy myös riskejä ja erityisesti taitamattomasti, huolimattomasti tai kiireessä läpiviety rekrytointiprosessi tuo mukanaan virhemahdollisuuksia. Rekrytoinnissa tapahtuvat yritykset, erehdykset ja henkilöstön perehdyttäminen voivat tulla yritykselle kalliiksi. (Ahvonen & Ollonqvist 2008, 22.)

Rekrytointi on yksi suurimmista investoinneista yritykselle. Työntekijälle rekrytointi on kokonaisvaltainen asia, joka vaikuttaa hakijan koko elämään, myös työn ulkopuolelle. Virheellinen rekrytointi voi tulla yritykselle kalliiksi. Sen on oletettu maksavan yritykselle kymmenistä tuhansista jopa satoihin tuhansiin euroihin.

3.1 Henkilöprofiili

Rekrytointiprosessi alkaa usein henkilöprofiilin määrittelemisestä. Henkilöprofiilin muuttumiseen vaikuttavia tekijöitä on kuitenkin useita, esimerkiksi markkina- ja kilpailutilanne, työnhakijoiden käyttäytyminen, asiakasodotukset, yrityksen tunnettavuus ja työnanta-

jaimago, työntekijän kasvu- ja kehitysmahdollisuudet yrityksessä ja työntekijän perehdytykseen käytettävissä oleva aika ja resurssit. Hyvin tehdyn henkilöprofiilin ja työpaikkailmoituksen laadinnan jälkeen on helppo tehdä hakemusten karsintaa. Henkilöprofiilin tärkeitä alueita ovat: mitä osaamista henkilöllä tulee olla, voiko vaadittava osaaminen tulla esimerkiksi harrastuksen kautta, miltä alalta kokemusta tulee olla, voiko työkokemuksen paikata muuta kautta tai muualta hankitulla osaamisella. Henkilöprofiiliin voi myös sisällyttää paljon kriteereitä, mutta työtehtävälle oleellisimmat asiat ovat tärkeimmät. Henkilöprofiilissa kriteerit kannattaa jättää mieluummin liian vähäiseksi kuin liian suureksi, sillä monet kriteerit eivät välttämättä vaikuta työssä menestymiseen. (Empore Oy 2014.)

Epäonnistunut rekrytointi johtuu usein liiallisten kompromissien tekemisestä. Mahdollisen kompromissin tekeminen rekrytointitilanteessa vaikuttaa väistämättä työntekijän perehdytykseen, työhön annettavaan tukeen, työmotivaatioon tai oppimishaluun. Epäonnistuneen rekrytoinnin taustalla on usein huonosti tehty henkilöprofilointi. Mahdollisia keinoja parantaa rekrytointia on asettaa tehtävälle lisää vastuuta, jolloin saadaan erilaiset hakijat kiinnostumaan tehtävästä. Lähtökohtaisesti kuitenkin yrityksen kannattaa lähteä käydä läpi keinoja, jolla rekrytointiin saadaan lisää tehoa. Tämänlaisia voi olla uusien kanavien käyttö rekrytoinnissa. Kannattaa myös käydä läpi onko henkilö- tai tehtävämäärittelyssä asioita, joista voidaan joustaa esimerkiksi pidemmän perehdytyksen kautta. (Empore Oy 2014.)

Rekrytointihaastattelun tarkoitus on informaation keruu ja sen tavoitteena on päätöksenteko. Edellytyksenä päätöksenteolle on kokonaisvaltainen käsitys työnhakijan soveltuvuudesta tehtävään. Soveltuvuuden muodostamista tukee rekrytointiprosessin muut arviointivaiheet, kuten suositusten tarkistus, mahdollinen työtehtäväsimulaatio, sekä mahdollinen ulkopuolisen ammattilaisen tekemä henkilöarviointi. Virheellisen tai vajavaisen tiedon pohjalta työsuhteen syntyminen on molempien osapuolien kannalta huono asia. Hyvän työsuhteen edellytys on, että molemmat osapuolet tunnistavat vastuualueensa. Työnantajan vastuulla on sitoutua tarvittavan tuen antamiseen ja työntekijän vastuulla on kantaa vastuu omasta työtehtävästään. (Empore Oy 2014.)

3.2 Murtautumistestaajan rekrytointi

Murtautumistestaajan rekrytointi ei usein käytä julkisia rekrytointialustoja. Yritykset etsivät usein tietoturvallisuuteen keskittyviä konsultteja. Konsultin työt usein sisältävät myös

murtautumistekniikkaa, kuten yrityksen KMPG Cyber Security Consultant avoimesta työpaikasta selviää. (KPMG 2017.)

Cyber Security Consultant tehtävään haetaan hallinnollisia ja teknisiä tietoturvakonsultteja. Konsulttien työtehtäviin kuuluu asiakkaiden tietoturvan ja tietosuojan sekä riskienhallinnan kehityshankkeisiin osallistuminen sekä hankkeiden läpivienti joko teknisenä asiantuntijana ja/tai projektipäällikkönä. Lisäksi tehtäviin kuuluu muun muassa tietoturva-auditoinnit, ISO 27001 sertifioinnit, erilaiset varmennustoimeksiannot sekä tietoturvallisuuden arviointilaitoksena suoritettavat tietoturvan ja tietosuojan auditoinnit. (KPMG 2017.)

Tehtävässä menestyminen edellyttää tuntemusta ja kokemusta esimerkiksi tietoturvallisuuden kansallisista ja kansainvälisistä standardeista sekä viitekehyksistä, riskienhallinnasta, tietosuojasta, liiketoimintaan liittyvistä prosesseista, hankinnoista ja ulkoistusten tietoturvasta sekä pilvipalveluista. Koulutukseksi edellytetään soveltuvaa korkeakoulu- tai yliopistotutkintoa ja teknologiaosaamista. Työkokemusta edellytetään vähintään 2 vuotta. Paineensietokyky, oma-aloitteisuus, joustava työskentelytapa ja tiimihenkisyys ovat myös vaatimuksina. Kansainvälisten projektien vuoksi myös erinomainen suullinen ja kirjallinen suomen ja englannin kielen taito sekä hyvät kommunikointitaidot ovat välttämättömiä konsultin työssä. (KPMG 2017.)

4 TIETOTURVA-ALAN NYKYINEN TILANNE

Turun ja sen lähialueiden tietoturvaan liittyvien avoimien työpaikkojen määrä TE-palvelun mukaan on 30 kappaletta. Näistä yli puolet sijaitsee Helsingissä. Työpaikkailmoitusten vaatimukset sisälsivät paljon samoja pääpiirteitä, kuin tietoturvayrityshaastattelusta keräämäni informaatio. Esimerkiksi yleisen tietoturvaprosessin ymmärtäminen, hallintajärjestelmien osaaminen ja sosiaalisten taitojen omaaminen. Lähes jokaisessa työpaikkailmoituksessa ilmeni vaatimuksissa liiketoimintaosaamisen tärkeys. Teknillinen osaaminen ei ollut päävaatimuksena monessakaan ilmoituksessa. Yleinen käsitys tietoturva-alan, johon työntekijää haettiin, oli usein tärkein vaatimus. Tämä vaatimus esitettiin joko työkokemuksen tai erilaisten yleisten käsityksien osaamisen vaatimuksena. (TE-palvelut 2017.)

4.1 Haastattelu

Haastattelussa on käytetty menetelmänä teemahaastattelua. Haastattelu on tapahtunut Helsingissä 24.4.2017. Haastateltavina on toiminut sovellusohjelmointiosasto ja riski ja strategia -osasto suuresta tietoturvayrityksestä. Haastattelijana oli Kim Ristimella. Yrityksen vastaukset ovat lainausmerkeissä, oma pohdintani niiden alla.

4.1.1 Tärkeimmät hakijoiden tekniset tietoturvaosaamiset

”Verkkoliikenteen perusperiaatteet ja protokollat ovat tärkeitä. Linux osaaminen ja komentoriviperusteet vähintään osattava Linuxissa, Windowsissa tämä olisi plussaa. Sovelluskehityksessä erittäin hyvä olisi, jos henkilö on ollut mukana edes jossain sovelluskehityksen projektissa, jotta tietäisi miten se todellisuudessa toimii. Miten asiat tapahtuvat sovelluksissa ja mitkä komponentit tekevät mitäkin - ymmärtää sovelluksen logiikan.”

”Yksittäiset, jopa monimutkaiset asiat ovat opetettavissa työn ohessa, jolloin rekrytoinnissa ei keskitytä yksittäisten protokollien, esimerkiksi MySQL-injektioiden osaamiseen. Tärkeintä on teoreettinen pohjaymmärrys, joka tukee oppimista, eikä oppiminen hankaloidu. Selkeä ymmärrys yhteydellisen ja yhteydettömän protokollan ero, eli käytännössä lähinnä TCP ja UDP. Ymmärtää niiden realiteetit, mitkä käyttävät portteja ja yleiset perusasiat.”

”Julkisen ja yksityisen verkko-osoitteen erot. Ymmärtää keskeiset asiat verkkolaitteissa, komponenttien merkitys, lokit, hyökkäyspinta-ala ja haavoittuvuuksien ulottuvuus. Yleinen ymmärrys tietoturva-asioista.”

”Harvoin vastavalmistunut pystyy pääsemään suoraan työelämään, ellei ole erittäin paljon harrastuneisuutta.”

”Ymmärrys ja osaaminen Agile-projektienhallinnasta ja mitä se todellisuudessa sisältää.”

Sisällöltään haastattelukysymyksen vastaus vastasi odotuksiani. Verkkoliikenteen siirtyminen tietojenkäsittelystä insinöörien koulutukseen voi olla rekrytoinnin kannalta vaikeuttava tekijä. Tietojenkäsittelijäkin tarvitsee tietoliikenteen perusymmärrystä valtavasti työssään. Tietojenkäsittelyn koulutuksen muutokset soveltuvat kuitenkin hyvin sovelluskehitykseen.

4.1.2 Yleisimmät puutteet hakijoiden teknisessä osaamisessa

”Perustiedot, miten sovellukset toimivat, mediaseksikkäät kielet liian suosittuja, jolloin tärkeät isojen yritysten käyttämät kielet, kuten .NET, C, Java, SQL jäävät puuttumaan, eikä kiinnostusta niiden opetteluun ole. Linux-osaamisessa puutteita komentorivin käytössä esimerkiksi navigointi, haut, putkittaminen ja tulosten editointi. Osattujen asioiden yhdistäminen suurena puutteena. Windowsilla myös, mutta ei niin tärkeää, koska komentorivin osaaminen tuo vain lisäsisältöä osaamiseen. Tulee vaikeaksi ohjeistaa työntekijää, jos ei voida suoraan pyytää esimerkiksi hakemaan tiettyä tiedostoa tietyillä argumenteilla, jos joutuu jokaisen kohdan opettamaan erikseen.” ”Yhtäläisyys; asioita opetetaan liian pitkälle, jolloin peruskäsitys jää hataraksi.”

Java ja SQL ovat ainakin vielä osana tietojenkäsittelyn koulutusta, ja toivottavasti on tulevaisuudessakin. Kysymys oli tärkeä juuri selvittääkseen, minkälaisiin teknisiin osaamisiin kannattaa tietojenkäsittelyn koulutuksessa panostaa. Yhtäläisyys voi kärsiä aiemmasta haastattelusta selvinneen ailahtelevaisuutensa vuoksi. On erittäin tärkeää, ettei Turun ammattikorkeakoulu vähennä perusosaamista laajentaakseen muiden alueiden erityisosaamista.

4.1.3 Tärkeimmät hakijan ominaisuudet

”Ymmärrys tietoturvasta kokonaisuutena, esimerkiksi Frameworkit. Osaa laittaa tietoturvan palasiksi, eikä keskity pelkästään tekniseen puoleen. Henkilöstöasiat, prosessiasiat ja paljon muutakin sisältyy tietoturva-alaan.”

”Esiintymisvalmius ja -halukkuus, pystyy antamaan oman mielipiteensä ja esittämään palaverissa oman näkemyksensä, pystyy visualisoimaan asioita ja käydä niitä läpi suullisesti. Ratkaisukeskeisyys, vahva halu oppia, kehittää itseään ja omaa osaamistaan on usein tärkeämpiä kuin jo osaaminen.”

”Aito kiinnostus alaa kohtaan esimerkiksi harrastuneisuudesta. Kokonaisvaltainen syventyminen alaan, uteliaisuus, kärsivällisyys, ongelmaratkaisukyky, oma-aloitteisuus, itsensä kehittäminen ja sen haluaminen.”

”Sinnikkyys ja pitkäjänteisyys, jotta ei hukata muiden projektityöntekijöiden työaikaa kyselemällä jatkuvasti asioita joihin vastaukset löytyvät jo olemassa olevista lähteistä."

”Konsultoinnissa osaa laittaa asiat tärkeysjärjestykseen uhka- ja riskimatriisi. Tietää yleiset haasteet ja riskit yrityksille, jotta yritys olisi mahdollisimman kustannustehokkaasti vähemmän haavoittuvainen. Ymmärtää hyökkääjän ajatusmaailman. Peruskäsitteet olisi hyvä olla yläkäsitetasolla tiedossa.”

Kokonaisvaltaisen tietoturvan ymmärrys on osa tietojenkäsittelyn tietoturvakoulutusta. Esiintymisvalmius ja -halukkuus tulevat kehittymään lähes jokaisen toteutussuunnitelman sisällön kanssa. Lähes jokaisessa kurssissa on jossain kohtaa kurssia oman työn suullista esittämistä. Projektitöiden ohella on myös pakollisia palavereja, joihin osallistuvat henkilöt selvittävät oman projektiosansa työn etenemistä, keskustelevat ilmenevistä ongelmista ja niiden mahdollisista ratkaisumalleista. Tietojenkäsittelyn koulutuksen sisältöön kuuluu myös pakollinen tiedonhakukurssi. Sen tarkoituksena on opettaa oppilaille, miten tietoa haetaan tehokkaasti internetistä, ja miten sen sisältöä tulee kritisoida varmistaakseen lähteen laadun. Tietoturvaopetukseen kuuluu myös pakollisena osana tietoturvan uhka- ja riskimatriisin käytön ymmärtäminen. Hyökkääjän ajatusmaailmaan opetetaan murtautumistestauksen ohessa. Murtautumistestaus tietojenkäsittelyn koulutuksessa sisältää hyökkäyksen toteutuksen, löytyneiden haavoittuvuuksien ja ratkaisumallien ammattimaista dokumentaatiota.

4.1.4 Yleisimmät ongelmat hakijoiden ominaisuuksissa

”Oma-aloitteisuuden puute, jäädään odottamaan, että joku sanoo mitä pitää tehdä, vaikka voisi tehdä omia ratkaisuja ja kokeilla asioita valmiiksi. Itsensä kehittämisen puute, kärsivällisyyden puute, nopea turhautuminen ja siitä seuraava avuttomuus. Perusasioita ei lähdetä selvittämään, vaikka ne olisivat nopeita selvittää itse, esimerkiksi palvelimen lokitiedostojen sijainnit. Ei osata rakentaa putkituksia komennoille, jotka helpottaisivat ja nopeuttaisivat työskentelyä. Ongelmia jo opittujen asioiden soveltamiseen keskenään ja niiden hyödyntäminen uusissa projekteissa.”

”Eivät ymmärrä minkälaisilla prosesseilla, teknologialla ja toimintatavoilla pyritään riskejä estämään tai havaitsemaan. Tietoturvatiedon ja tapahtumienhallinta, jotka ovat yritysmaailmassa perusjuttuja, mutta niitä ei kouluissa käsitellä edes käsitetasolla. Ei tiedetä tietoturvan operatiivisista keskuksista tai shokkipalveluista.”

Tällä hetkellä suurin osa koulutuksesta vaatii myös oppilaalta oma-aloitteista oppimista aiheesta. Kotitöinä on usein seuraavan aiheesta tiedonhakua ja sen ymmärtämistä. Opittujen asioiden ja niiden soveltaminen keskenään uusien ratkaisujen kehittämisessä on usein oppilaan opittava itse. Tietoturvatiedon ja tapahtumienhallintaa ei tietoturvakoulutus sisällä paljoa, mutta teoriatasolla niiden toimintaa opetellaan.

4.1.5 Mitä työ todellisuudessa sisältää?

”Tietoturvainformaation analysointia, johtopäätöksen tekemistä, tietoturvaprosessien kehittämistä, tietoturvapoikkeavuuksiin reagointia, asiakkaan avustamista, sovellusten ja järjestelmien asennusta ja ylläpitoa, pienkehitystä esimerkiksi säännöstöt ja raporttien suunnittelu ja toteutus ja tietenkin asiakastyöskentelyä.”

”Tietoturvakyvykkyyksien selvitystyöt; onko jotain missä ei ole ollenkaan kyvykkyyksiä. Riski ja uhkalähtöisyysselvitystä. Budjetointia eli mihin raha kannattaa sijoittaa, jotta kyvykkyyskokonaisuus nousisi mahdollisimman korkealle. Mitä kontrolleja pitää olla sovelluksissa, jotta ne ovat turvallisia ja kustannustehokkaita.”

Mielestäni Turun ammattikorkeakoulusta tietojenkäsittelyn koulutuksesta tietoliikenne ja tietoturva puolelta vastavalmistunut on kykenevä suoriutumaan näistä työtehtävistä

opastuksella ja lisäkouluttamisella. Mielestäni näitä työtehtäviä kohtaan koulutus kehittää ja tukee tulevaa oppimista huomattavasti.

4.1.6 Oletteko valmiita kouluttamaan vastavalmistunutta Junior-tason tehtävissä, jos kyllä, millaisessa tilanteessa tietotaitotason on vähintään oltava?

”Vähintään jokin seuraavista hyvällä tasolla, tai useampi kohtalaisella: komentoriviosaaminen, lokien tulkinta, käyttöjärjestelmien perusymmärrys, verkko-osaaminen ja kyberhyökkäyksien ymmärrys.”

”Olemme valmiita opettamaan ja kouluttamaan, suurin osa opetuksesta tapahtuu työtilanteissa, kokeneemmassa tiimissä. Asiakastilanteita ei voida oppia koulussa, joten ne joudutaan oppimaan pikkuhiljaa kokemuksien kautta.”

On tärkeää, että tulevat työnantajat ovat valmiita lisäkouluttamaan ja kehittämään vastavalmistuneen osaamista. Näin saadaan nopeasti kehitettyä uudesta työntekijästä tuottava henkilötarpeen täyttävä onnistunut rekrytoinnin kohde.

4.1.7 Sertifikaatit joita arvostatte

”Kaikki tietoturvaan liittyvät sertifikaatit ovat eduksi. CISSP (Certified Information System Security Professional), CEH (Certified Ethical Hacker), GIAC (Global Information Assurance Certification), CISM (Certified Information Security Manager), tietoturvaohjelmistojen sertifikaatit esimerkiksi käyttäjäpääsyhallinta, lokit, skannaukset ja niin edelleen, vaikka ei olisikaan samaa järjestelmään käytössä. Tietoturvaohjelmistojen sertifikaatit todistavat hakijan ymmärtävän ohjelmiston, joka kautta uuden ohjelmiston oppiminen helpottuu huomattavasti. Koskaan ei ole kuitenkaan sertifikaatin puutteen vuoksi hylätty hakijaa. Hakijan omassa kehityssuunnitelmassa sertifikaattien harkitseminen on jo plussaa, sillä se kertoo, että hakija on seurannut hakuympäristöä ja alan keskeisiä juttuja.”

Sertifikaatit joita haastattelussa mainittiin ovat kaikki globaalisti korkeasti arvostettuja sertifikaatteja. Näiden sertifikaattien hankkiminen on usein kallista ja niiden suorittamiseen tarvittavat valmennukset kestävät kauan. Tämä hankaloittaa huomattavasti opiskelijoiden kykyä hankkia kyseisiä sertifikaatteja. Kuitenkin pelkästään näiden sertifikaattien maininta omassa työhakemuksessa on yritysten mielestä positiivista, sillä se kertoo

hakijan kiinnostuksesta kehittää itseään. Yritykset kyllä ymmärtävät, että monen tuhannen euron sertifikaatti vastavalmistuneen tuloilla voi olla täysi mahdottomuus. Tutkielmani tietoturvateorian CIA-triadi on esimerkiksi yksi osa CISSP-sertifikaatin osista, joten voidaan olettaa, että tietoturvan perusosaamisen opettelu voidaan suorittaa myös harrastuneisuuden ja tietoturvan teorian lukemisen yhdistelmällä. Sertifikaatit ovat todiste siitä, että hakija ymmärtää tietoturvan perusasiat.

4.1.8 Mihin haluaisitte ammattikorkeakouluopetuksen kiinnittävän huomiota opetuksessaan

”Linux ja Windows komentoriviosaaminen ja verkko-osaaminen. Mieluummin teoreettisesti protokollat ja niiden hierarkiat. Ei tarvitse osata palomuurien konfiguraatiota, vaan ymmärtää mitä ne ovat ja mitä ne tekevät. Ei tarvitse välttämättä osata työkaluja, jos ymmärtää perusteet ja on kiinnostusta oppia työkalujen käyttö niiden perusteella. Ehdottomasti oikeita tilanteita, aidot ongelmat, haasteet ja sitä kautta tuodaan ymmärrystä miksi jotain puolustuskyvykkyyttä pitää parantaa. Mitä, miten ja miksi jotain tapahtui organisaatiolle ja mitä he tekivät sen korjaamiseksi. Teoriaopetuksessa reaalimaailman asioita ja tapahtumia mukaan, jotta opiskelijat ymmärtäisivät miksi tietoturva on tärkeää - nostaa motivaatiota. Tietoturvatrendit ja hyökkäykset mukaan opetukseen.”

Jokainen ilmenevä asia on otettu huomioon myös Turun ammattikorkeakoululle tarkoitetuissa kehitysehdotuksissa. Jotkin asiat, esimerkiksi reaalimaailman asiat ja tapahtumat, voivat olla erittäin hankalia toteuttaa. Tämä on huomioitu kehitysehdotuksessa.

4.1.9 Pidättekö teoria- vai käytännönosaamista tärkeämpänä tekijänä etsiessänne työntekijöitä, miksi?

”Käytännönosaaminen on erottautumistekijä, mutta konseptitasolla teoriaosaaminen ja kyky keskustella on tärkeämpää, ilmaista halukkuutta oppia ja ymmärtää uusia asioita. Jos yrityksellä on tarve tietynlaiselle työtehtävälle, on kuitenkin käytännönosaaminen suuri plussa. Henkiset ominaisuudet jotka tukevat kehitystä ovat tärkeimmät - kaikki muu on järjestettävissä. Kummasta on enemmän hyötyä, riippuu siitä, minkälaista työtä henkilö tekee. Teoria on ehdottomasti tärkeämpää konsulttipuolella, käytännönosaaminen kehityspuolella. Paras on kompromissi kaikesta.”

Vastauksesta huomaa selkeästi saman perusajatuksen. Perustietous pitää olla kunnossa, ennen kuin voi lähteä laajentamaan osaamistaan. Pelkkä käytännönosaaminen ei riitä, vaan pitää olla sen perustana hyvä teoriaosaaminen ja kyky keskustella löydöksistään. Peruspohja ja henkiset ominaisuudet, jotka tukevat sen oppimista työn ohessa ovat tärkeimpiä tekijöitä uusissa työntekijöissä. Se kumpi on tärkeämpää teoria- vai käytännönosaaminen riippuu rekrytointitarpeesta.

4.1.10 Vapaa sana

”Yleisesti vaikuttaa, että Turun ammattikorkeakoulussa on otettu asiat vakavasti ja osaamista opettaa löytyy. Ymmärretään mitkä ovat tärkeitä asioita, joita halutaan opettaa. Ei opeteta vaan opettamisen vuoksi, vaan halutaan oikeasti opettaa työhön ammattilaisia, jotka tuovat lisäarvoa yritykselle. Toivomme opinahjoilta, että he innostaisivat nuoria ymmärtämän tietoturvallisuuden laajuuden ja ne monet suuntaukset joita voi tehdä. Monet ominaisuudet joista on käyttöä ja että tietoturva on tärkeää. Saamaan oppilaat ottamaan itselleen asian kiinnostuksen ja tärkeyden arvon, sillä tietoturva on tulevaisuuden kannalta tärkeää kaikille.”

Olen haastateltavan kanssa samaa mieltä. On erittäin tärkeää, että oppilas ymmärtää tietoturvan monialaisuuden ja keskittyy sen perustiedon hankintaan, josta on kiinnostunut eniten. Tietoturvan teoriaosaamisesta selviää tarkemmin, mitä haastateltava tarkoittaa sillä, että tietoturva on tulevaisuuden kannalta tärkeää kaikille. Lähes jokainen yritys nykyaikana käyttää erilaisia teknologioita hyväksi toiminnassaan, jotka edellyttävät jatkuvaa tietoturvan ja CIA-triadin ylläpitoa.

4.2 Haastattelun analysointi

Haastattelusta ilmenee selkeästi toistuvia asioita, kuten perusosaamisen puute. Yrityksillä on valmiudet opettaa monimutkaisiakin työtehtäviä, mutta hyvä peruspohjatietous on tärkein ominaisuus hyvän kehittymisen kannalta. Tärkeintä hakijalle on keskittyä tietoturvaperusteiden ja hyvän pohjatiedon hallitsemiseen, eikä keskittyä mihinkään tiettyyn protokollaan tai ohjelmointikieleen. Harrastuneisuus on suuri etu tietoturva-alalle haluavalle henkilölle. Haastattelusta käy ilmi, että sosiaaliset taidot, kyky keskustella ja henkiset valmiudet alalle ovat tärkeimmät osa-alueet tietoturva-alalle hakevassa henkilössä. Oikeiden tietoturvatilanteiden kokemus on tärkeää jo opiskeluvaiheessa. Tietoturva-alan

yrityksien riskien ja niiden hallinta järkevillä resursseilla on asioita, jotka tietoturva-alalle haluavan on opeteltava.

Tietoturva-alan työtehtävien monimuotoisuus myös tuo erilaisia tarpeita työntekijöiden ominaisuuksista. Esimerkiksi konsultointityössä on tärkeämpää osata teoriatasolla tietoturva-asioita ja omistaa hyvät sosiaaliset taidot. Kehityspuolella sen sijaan käytännönosaaminen on tärkeämpää, eikä samanlaisia sosiaalisia taitoja tarvita. Tietoturva-alalla työskentely ei siis vaadi yhtenäistä osaamista, vaan jokaiselle osaamisalueelle on omat tarpeensa.

Haastattelusta käy ilmi, että hyökkäyksien estämisessä on tärkeää tietää sen hetken tietoturvatrendit, eli eniten käytetyt hyökkäys- ja puolustusmetodit. Näiden metodien osaaminen on tärkeää peruskäsitteinä, ja esimerkiksi sertifikaattien suorittaminen kertoo yritykselle näiden asioiden osaamisen.

Tietoturva-alalla työskentelevillä on selkeä käsitys osaamistarpeistaan. Rekrytointitilanteissa ei vaadita heti osaamista, vaan työntekijälle opetetaan suurin osa työtehtävistä työnaikana.

Haastattelusta selviää selkeä ongelma hakijoiden tietoturvaymmärtämisestä. Henkilöillä saattaa olla paljonkin osaamista taustallaan, mutta niiden toiminnan ymmärryksessä saattaa olla puutteita, jolloin tositilanteessa soveltaminen voi olla erittäin hankalaa.

Kouluissa ei kerrota tarpeeksi erilaisten tietoturvapalveluiden olemassaolosta ja tarkoituksista. Haastattelusta selviää, ettei hakijat ole tietoisia esimerkiksi shokkipalveluista ja operatiivisista keskuksista. Yrityksissä paljon käytettyjen palveluiden, kuten tietoturvatiedon ja tapahtumienhallinnan käytön ymmärtämisessä on myös puutteita. Tietoturvaan kuuluu myös kyseisien palveluiden lisäksi muitakin hakijoille usein tuntemattomia alueita. Henkilö- ja prosessiasiat ovat myös tärkeitä osia yrityksen tietoturvassa. Usein tietoturva-aukkoja löytyy juuri työntekijöiden päivittäisistä työntekotavoista ja hallintaprosesseista.

5 TRADENOMILIITTO TRAL

Tradenomiliitto TRAL on tehnyt tutkimuksen vuonna 2013 IT-tradenomin osaamisvaatimuksista. Toteutuneen tutkimuksen kyselyssä vastaajat arvioivat kuinka paljon he tarvitsivat osaamista työssään ja kuinka paljon koulutus kehitti heidän osaamistaan. Tutkitut osaamisalueet olivat yleinen osaaminen, kehittämisosaaminen, eettinen osaaminen, kansainvälisyysosaaminen, liiketoimintaosaaminen, ICT-perusosaaminen ja ICT-kehittämisosaaminen. (Tuovinen 2013, 1.)

Pääsääntöisesti tietojenkäsittelyn koulutus koettiin vastaavan työelämän tarpeisiin. Kehitettävää koulutuksessa koettiin olevan pilviratkaisuiden merkityksen ja toimintaperiaatteiden ymmärryksen, toiminnanohjausjärjestelmien käyttämisen sekä kestävän kehityksen periaatteiden osalta. Myös esimies- ja johtamistyön osalta ero koulutuksesta saaman osaamisen ja työelämän tarpeiden välillä oli merkittävä. (Tuovinen 2013, 1.)

Vastaajilta kysyttiin näkemystä siitä, miten osaamisvaatimukset tulevat muuttumaan ja miten sen pitäisi näkyä koulutuksessa. Vastauksista esiin nousi neljä teemaa: pilvipalvelut, mobiiliteknologia, kestävä kehitys ja kansainvälisyys liiketoiminnassa. Yleinen osaaminen ja liiketoimintaprosessien ymmärrys koettiin hyvin tärkeiksi. (Tuovinen 2013, 2.)

6 TURUN AMMATTIKORKEAKOULUN TIETOJENKÄSITTELYN OPETUSSUUNNITELMA

Lähden selvittämään kohtaako SoleOPS:in sisältö tutkimuksessa selvinneisiin rekrytointivaatimuksiin ja valmistaako opetus opiskelijoita yritysten rekrytointivaatimuksien mukaisesti.

SoleOPS on opetuksen suunnitteluun tehty selainpohjainen väline. Sen avulla voidaan tehdä saapumisryhmien opetussuunnitelmat, lukusuunnitelmat, opintojaksokuvaukset ja toteutussuunnitelmat. Sen avulla voidaan myös hallita vuositeemoja ja osaamistavoitteita opiskelijoiden tavoitteelliseen opiskelun johdattamiseksi. Se sisältää myös henkilökohtaiset opintosuunnitelmat (SoleHOPS). Syötetyistä tiedoista voidaan tuottaa raportteja hallinnon tarpeisiin. Tiedot voidaan myös helposti siirtää toisiin järjestelmiin. (SoleOPS, Turun ammattikorkeakoulu 2017. Etusivu.)

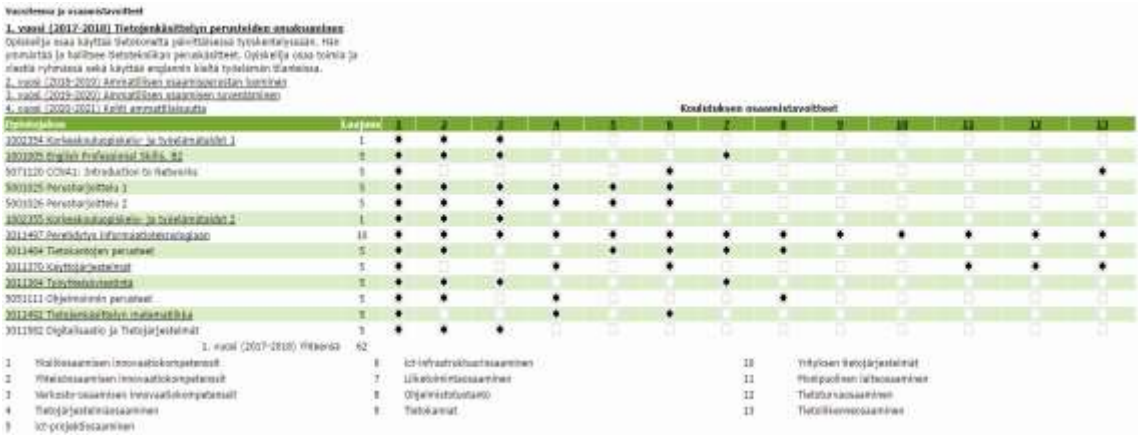
Opiskelijoille järjestelmä tarjoaa tavan päästä käsiksi opetustarjontaan ja omaa opiskelua koskevaan tietoon. Opettajille ja henkilökunnalle järjestelmä tarjoaa uusimmat tiedot opetussuunnitelmista, lukuvuoden opetustarjonnasta sekä opintojaksojen toteutussuunnitelmista. (SoleOPS, Turun ammattikorkeakoulu 2017. Etusivu.)

6.1 Osaamistavoite

Osaamistavoitteena on valtakunnalliset tarpeet kyseiselle alalle. Nämä tarpeet usein saadaan erilaisista kompetenssianalyyseistä, tai esimerkiksi haastattelemalla lähiympäristön yrityksiä ja kuuntelemalla heidän tarpeitaan. Seuraavaksi esittelen tietojenkäsittelyn koulutuksen seuraavan saapumisryhmän osaamistavoitteet lukuvuosittain kuvina ja kerron niistä opintojaksoista, joiden sisällössä on tietoturvaosaamista.

Osaamistavoitteet jakautuvat yhteisiin opintoihin, ICT-palvelut ja liiketoiminnan ratkaisu -suuntautumiseen ja tietoverkot ja tietoturva -suuntautumiseen. Erottelen koulutussuunnat toisistaan osaamistavoitteiden esittelyssä.

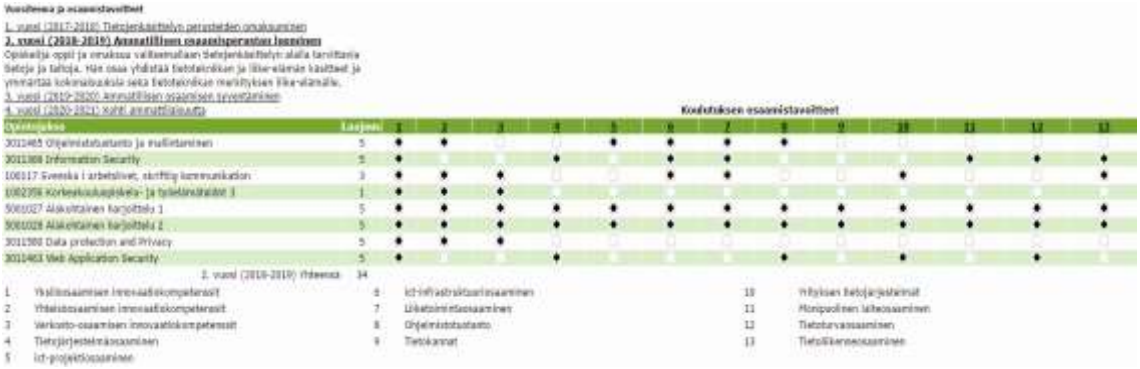
6.1.1 Lukuvuosi 2017 - 2018 (Kuva 2).



Kuva 2. SoleOPS vuositeema ja osaamistavoitteet. Tietojenkäsittelyn koulutus 2017-2018.

- **Perehdytys informaatioteknologiaan**, kymmenen opintopistettä, yhteinen opinto: Opintojakson tavoite on kouluttaa opiskelija toimimaan projektiryhmän jäsenenä, kuvata, miten ICT-projekteja hallitaan, käyttää sujuvasti ja oikeaoppisesti viestinnän välineitä, dokumentoida ja raportoida projektin tuloksia. Lisäksi oppilas oppii kertomaan tietoturvan merkityksen organisaation toiminnalle ja nimetä yrityksen tärkeimmät lähiverkon laitteet ja niiden tehtävät. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Perehdytys informaatioteknologiaan.)
- **Käyttöjärjestelmät**, viisi opintopistettä, yhteinen opinto: Opintojakson suorittanut oppilas osaa selittää tietokoneen toimintaperiaatteet, käyttöjärjestelmän toimintaperiaatteet, erilaisten käyttöjärjestelmien käyttö laitteissa ja virtualisoinnin toimintaperiaatteet. Oppilas asentaa käyttöjärjestelmän ja päivittää sen, käyttää järjestelmää komentotulkilla ja graafisella käyttöliittymällä, konfiguroi järjestelmän ja sen toimintaa, huolehtii tietoturvasta ja käyttäjäpääsyhallinnasta, luo, hallitsee ja käyttää virtuaalikoneita sekä arvioi mobiilikäyttöjärjestelmien ominaisuuksia, tilaa ja kehitystä. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Käyttöjärjestelmät.)

6.1.2 Lukuvuosi 2018-2019 (Kuva 3).

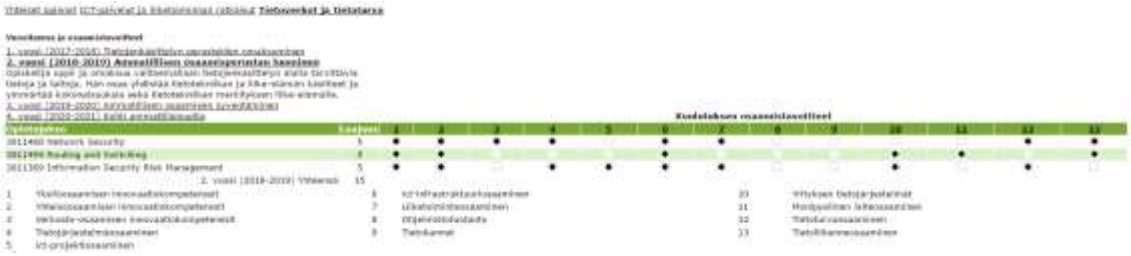


Kuva 3. SoleOPS vuositeema ja osaamistavoitteet. Tietojenkäsittelyn koulutus 2018-2019.

- **Information Security**, viisi opintopistettä, yhteinen opinto: Suoritettuaan oppilas pystyy nimeämään ja selittämään tietoturvallisuuden peruskäsitteet, luokittelemaan informaatiota ja tietojärjestelmiä, tunnistamaan turvallisuusriskejä, antamaan esimerkki tietoturvallisuuden kontrolleista ja niiden toteutuksesta, tunnistamaan ja listaamaan tietoturvavaatimuksia erilaisille organisaatioille, ottaen huomioon lain ja säädösten vaatimukset. Oppilas pystyy myös selittämään tietoturvan riskihallinnan perusteet. Luomaan, arvioimaan ja kehittämään yritysjatkuvuutta ja palautumissuunnitelmaa. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Information Security.)
- Turun ammattikorkeakoulussa harjoittelut sisältävät kaksi viiden opintopisteen pituista **alakohtaista harjoittelua**. Alakohtaiset harjoittelut sisältävät oman koulutuksen mukaiseen tekniikan alan ammattiin tutustumista. Tämän lisäksi on kaksi viiden opintopisteen pituista ammattiharjoittelua. Ammattiharjoittelut sisältävät omaa osaamispolkua vastaavaan ammattiin ja työtehtäviin tutustumista. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, alakohtainen harjoittelu 1 ja 2.)
- **Web application security**, viisi opintopistettä, yhteinen opinto: Opettaa oppilaalle tiedon ja ymmärryksen suosituimpiin web-sovelluksen tietoturvariskeihin, tietoturvaheikkouksiin ja hyökkäyksiin. Oppilas pystyy evaluoimaan teknisiin laitteisiin ja yritykseen kohdistuvien erilaisten hyökkäysten vaikutuksen. Tietää tur-

vallisen web-sovelluksen periaatteet. Pystyy osallistumaan turvallisen web-sovelluksen kehittämisprojekteihin. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Web application security.)

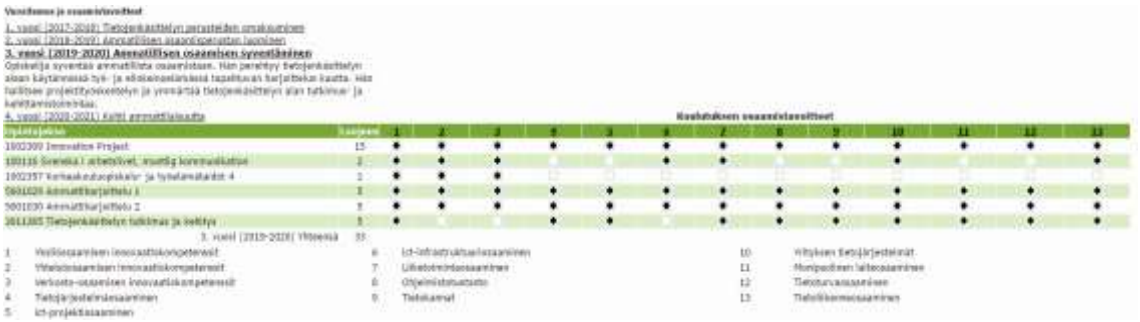
Tietoverkot ja tietoturva -suuntautumisen kurssit (Kuva 4):



Kuva 4. SoleOPS vuositeema ja osaamistavoitteet. Tietojenkäsittelyn koulutus 2018-2019. Tietoverkot ja tietoturva -suuntaus.

- **Network Security**, viisi opintopistettä, **tietoverkot ja tietoturva**: Tavoitteena on käyttää kryptografisia työkaluja tunnistautumisen, salauksen ja tiedon eheyden säilyttämiseen tietoliikenteessä. Palomuurien hyödyntäminen operatiivisessa turvallisuudessa tietoverkoissa. Toteuttaa turvallinen ympäristö virtuaalisen erillisverkon ylitse. Tunnistaa ja ehkäistä verkkotunkeutumisia havainnointi- ja estojärjestelmillä. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Network security.)
- **Information Security Risk Management**, viisi opintopistettä, tietoverkot ja tietoturva: Oppilas pystyy selittämään perusperiaatteet tietoturvan riskihallinnasta. Kykenee listaamaan riskihallinnan eri prosessivaiheet. Luokittelemaan tietoturvallisuuden riskit erilaisten lähestymistapojen kautta. Antamaan esimerkkejä erilaisista tietoturvan riskienhallinnan metodeista. Järjestämään ja toteuttamaan tietoturva riskikartoituksen Pk-yritykselle. Analysoimaan riskienhallinta-arviosta saatuja tuloksia ja antamaan perusteltuja parannusehdotuksia. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Information security risk management.)

6.1.3 Lukuvuosi 2019-2020 (Kuva 5).



Kuva 5. SoleOPS vuositeema ja osaamistavoitteet. Tietojenkäsittelyn koulutus 2019-2020.

- **Innovation project**, 15 opintopistettä, yhteinen opinto: Oppilas osallistuu systemaattiseen tutkimukseen ja kehitystyöhön projektijäsenenä. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Innovation project.)
- **Tietojenkäsittelyn tutkimus ja kehitys**, viisi opintopistettä, yhteinen opinto: Opintojakso keskittyy tietojenkäsittelyn alalle soveltuviin tutkimusmenetelmiin, tietolähteiden käyttöön ja tiedonhakutekniikkaan sekä tutkimusviestintään. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Tietojenkäsittelyn tutkimus ja kehitys.)
- **Ammattiharjoittelut** sisältävät omaa osaamispolkua vastaavaan ammattiin ja työtehtäviin tutustumista. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, ammattiharjoittelu 1 ja 2.)

ICT-palvelut ja liiketoiminnan ratkaisut -suuntautumisen kurssit (Kuva 6):

Kuva 6. SoleOPS vuositeema ja osaamistavoitteet. Tietojenkäsittelyn koulutus 2019-2020. ICT-palvelut ja liiketoiminnan ratkaisut -suuntautuminen.

- **Sovellusohjelmointi**, viisi opintopistettä, ICT-palvelut ja liiketoiminnan ratkaisut: Jakson käytyä oppilas osaa ohjelmoida ryhmän jäsenenä toimivan sovelluksen,

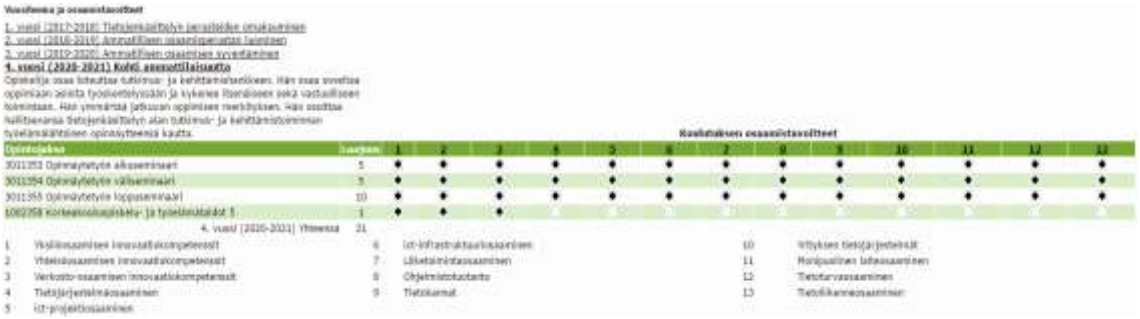
hyödyntää olemassa olevaa koodia, kirjastoja ja lukea kaavioita. Oppilas ymmärtää ja soveltaa joitakin suunnittelumalleja, käyttää sovelluskehitintä koodaustyökaluna ja käyttää versionhallintajärjestelmää. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Sovellusohjelmointi.)

Tietoverkot ja tietoturva -suuntautumisen kurssit (Kuva 7):

Kuva 7. SoleOPS vuositeema ja osaamistavoitteet. Tietojenkäsittelyn koulutus 2019-2020. Tietoverkot ja tietoturva -suuntautuminen.

- **Information Security Testing and Assessment**, viisi opintopistettä, tietoverkot ja tietoturva: Opintojaksolla oppilas oppii selittämään peruskäsitteenä tietoturvatestauksesta, oppii listaamaan tietoturvatestauksen prosessin vaiheet ja antamaan esimerkkejä tietoturvatestauksen metodeista. Järjestämään ja toteuttamaan tietoturvatestauksen PK-yrityksen kokoiseen ympäristöön, analysoimaan ja raportoimaan tuloksia sekä antamaan perusteltuja kehitysehdotuksia tietoturvariskien vähentämiseksi. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Information security testing and assessment.)

6.1.4 Lukuvuosi 2020-2021 (Kuva 7).



Kuva 8. SoleOPS toteutussuunnitelma. Tietojenkäsittelyn koulutus 2020-2021

- **Opinnäytetyön alkuseminaari**, viisi opintopistettä, yhteiset opinnot: Opiskelija osaa kurssin suoritettuaan suunnitella opinnäytetyöskentelynsä, määritellä tutkimusongelmansa, valita tutkimukseensa soveltuvan lähestymistavan ja menetelmät, laatia tutkimussuunnitelmansa ja esitellä sen. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, opinnäytetyön alkuseminaari, 2019-2020.)
- **Opinnäytetyön väliseminaari**, viisi opintopistettä, yhteiset opinnot: Opiskelija osaa kurssin suoritettuaan valita tutkimukseensa soveltuvat kirjalliset ja muut lähteet, rajata tarvittaessa tutkimustaan, muodostaa tutkimuksensa tietoperustan ja esitellä sen. Oppilas pystyy myös esittelemään ja perustelemaan työssään tekemiä valintoja. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, opinnäytetyön väliseminaari, 2016-2017.)
- **Opinnäytetyön loppuseminaari**, 10 opintopistettä, yhteiset opinnot: Opiskelija osaa toteuttaa tutkimuksensa empiirisen osion, kirjoittaa tutkimusraportin, ottaa huomioon työhönsä saamat kommentit ja esitellä koko tutkimus. Lisäksi opiskelija kykenee kirjoittamaan kypsyysnäytteen hyväksytysti. (Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, opinnäytetyön loppuseminaari, 2016-2017.)

Turun ammattikorkeakoulun tietoturvakoulutus on laaja-alaista ja kokonaiskoulutuksesta (210 opintopisteestä) tietoturvaa sisältävää koulutusta on 105 opintopistettä. Onnistuneen tietoturvaopetuksen jälkeen oppilas ymmärtää tietoturvan merkityksen organisaation toiminnalle ja tuntee tietoturvan osa-alueet. Oppilas myös tuntee tietoturvan osa-alueet ja tietoturvaan liittyvät keskeisimmät lait ja viranomaismääräykset. Osaa arvioida tietoturvariskejä ja etsiä organisaatioille niihin sopivia ratkaisuja. Osaa toteuttaa tietojärjestelmien ja tietoverkkojen suojaamisen käyttäen erilaisia teknillisiä ratkaisuja.

6.2 Haastattelu

Haastattelussa on käytetty menetelmänä teemahaastattelua. Haastattelu on tehty Turun ammattikorkeakoulussa 1.5.2017. Haastattelijana oli Kim Ristimella. Haastattelukysymyksiin vastaukset ovat lainausmerkeissä, jonka jälkeen on oma pohdintani vastauksesta.

6.2.1 Onko Turun ammattikorkeakoulun toteutussuunnitelmien onnistuneisuus varmistettu, jos on niin miten?

"Siihen pyritään. Tehtävillä ja usein myös tentillä varmistetaan oppilaiden osaamisen kehitys ja taso. Toisin sanoen perinteiset menetelmät ovat käytössä. Meillä ei ole opetukseen liittyvää laadunvalvontaa, koska pedagogiset opintojen ovat jokaiselle opettajalle pakollisia. Oppilaiden palautejärjestelmä on ainoa laadunvalvontajärjestelmä, joka kohdistuu opettajiin ja kurssien sisältöön. Ongelmana olemme huomanneet palautteen pitkän viiveen. Opiskelijapalautteen perusteella tehdään korjauksia jopa kesken kurssin, jos siihen nähdään syytä."

Tehtävien ja tenttien varmistuksella ylläpidetään tarvittavia osaamistavoitteita, mutta se ei välttämättä ole tarpeeksi tarkka tapa valvoa toteutussuunnitelmien onnistuneisuutta. Oppilaiden motivaatio täyttää palautekyselyitä on usein liian heikko, jotta pienet ongelmat paranisivat. Palautteisiin pystytään reagoimaan liian myöhään. Oppilaat usein antavat palautetta vasta sitten, kun ongelmat ovat kehittyneet suuriksi ja vaikeiksi korjata.

6.2.2 Onko toteutussuunnitelmien tavoitteita verrattu oppilaiden todelliseen oppimiseen?

"Tehtävien tekeminen ja joissain kursseissa myös tentit ovat tapa, jolla varmistetaan oppilaan osaaminen. Ilman osaamista ei pääse kurssista läpi. Näyttökokeet voisivat olla hyvä idea, varsinkin käytännöllisissä kursseissa esimerkiksi murtautumistestauksessa. Me emme tee tilastointia oppilaiden keskiarvoista."

Tehtävillä ja kurssien läpäisyllä pystytään määrittelemään minimiosaaminen. Arvostelun avulla pystytään määrittämään oppilaiden osaamiserot. Näyttökokeiden tarkoituksena on opitun asian soveltaminen todelliseen tilanteeseen, ja parhaissa tapauksissa myös monen opitun asian yhdistäminen käytettäväksi kokonaisuudeksi. Tällä tavoin oppilas pääsee hyödyntämään opittuja taitoja mahdollisimman todellisessa ympäristössä. Samalla oppilas oppii hyödyntämään oppimiaan asioita kokonaisuuksina.

6.2.3 Onko opetussuunnitelmien sisältöä verrattu vallitseviin rekrytointivaatimuksiin, jos on, niin minkälaisia ongelmia on huomattu?

"Meillä on ICT neuvottelukunta, jossa on mukana myös yrittäjiä. Kuuntelemme heidän tarpeitaan ja teemme ratkaisuja niiden pohjalta. Vähäinen edustus kuitenkin on ollut tietoturva-alalla, mutta nykyään tilanne on parempi ja parantumassa. Murtautumistestauksen mukauttaminen opetukseen on ollut viime sisältömuutos, vaikka tarve ei tullutkaan suoraan yrityksiltä - vaan yleisistä vaatimuksista ja osaamistrendeistä. Tietoturvatestaus on kuitenkin tärkeä osa yleistä tietoturvaa."

Neuvottelukunnan kuunteleminen on Turun ammattikorkeakoululle erittäin tärkeää. Turun ammattikorkeakoulun on jatkuvasti valvottava tietoturva-alan kehitystä, jotta mahdolliset muutokset opetussuunnitelmiin voidaan tehdä tarpeeksi nopeasti.

6.2.4 Mihin Turun ammattikorkeakoulu aikoo jatkossa panostaa opetussuunnitelmissaan?

"Tietoverkkojen painopiste siirtyvät insinööreille. Tietoverkot ja kyberturvallisuus on uusi koulutuslinja. Tietojenkäsittelyn tradenomeille vastaava on liiketoiminnan tietojärjestelmiä ja tietoturvaa."

Tietoverkkojen siirtäminen insinööreille voi luoda heikon perustan tietojenkäsittelyn tietoturvaosaamiselle. Tietoturva-alan haastattelussa käy ilmi, että tietoverkkojen ja yhteyksien ymmärrys on tärkeä elementti vastavalmistuneen osaamiselle rekrytoinnin kannalta. Tietojärjestelmien lisääminen tietojenkäsittelyn tradenomeille sen sijaan tuo kokonaisuudessaan uuden mahdollisuuden erilaisiin työtehtäviin, esimerkiksi suoraan sovellusohjelmointiin ja erilaisiin tietojärjestelmien rakentamiseen.

6.2.5 Onko mielestäsi toteutussuunnitelmissa panostettu tarpeeksi sosiaalisten taitojen osaamiseen yrityskulttuurissa, esimerkiksi konsultin työssä?

"Tietojenkäsittelyn puolella kyllä, paljon ryhmätöitä ja esityksiä. Sitä voisi olla aina kuitenkin enemmän. Tiimityöskentely on keskeisiä osaamistavoitteita. Suoraan konsultin työhön ei olla keskitytty, mutta monet opittavat asiat liittyvät vahvasti aiheeseen, joten

perustieto tulee opittua. Esityksien lisäksi kirjallinen ja suullinen viestintä on osa toteutussuunnitelmia lähes poikkeuksetta.”

Tiimityöskentelyä, sosiaalista osaamista ja kirjallista viestintää on tietojenkäsittelyn puolella erittäin paljon. Lähes jokaisessa toteutussuunnitelmassa on jonkinlainen raportti tai esitelmä tehdystä työstä, jonka kautta saadaan hyvää kokemusta oman asian esittämisestä ja tutkimusten tekemisestä.

6.2.6 Näetkö tarvetta opettaa myös alaan liittyviin vähemmän teknillistä osaamista vaativiin työtehtäviin, esimerkiksi henkilöstörekrytointiin?

"Kyllä, mutta kolmen ja puolen vuoden tutkintoon ei yksinkertaisesti pysty lisäämään kaikkea mitä haluaisi. Murtautumistestausta on aivan liian vähän. Liiketalouden puoli on keskittynyt paljon enemmän esimerkiksi henkilöstörekrytointiin.”

Henkilöstörekrytoinnin osaamiseen kuuluu myös rekrytointiin liittyvän alan tietous. Henkilöstörekrytoinnin opettaminen tietojenkäsittelyn alalla voi olla hankalaa, mutta sille pystyisi luomaan pohjan käsittelemällä esimerkiksi viiden opintopisteen laajuudesta onnistuneen rekrytoinnin pääasioita.

6.2.7 Näetkö tarpeellisemmaksi opettaa ammattikorkeakouluissa alan perustietoutta vai tarkentaa osaaminen tiettyyn syvällisempää osaamiseen?

"Perustietoutta ehdottomasti. Ohjelmointi, tietokannat ja käyttöjärjestelmät, koska ympäristö muuttuu niin vauhdikkaasti. Muuten menee tosi helposti ohi alan vaatimuksista, jos lähdetään keskittymään johonkin tiettyyn syvällisempään osaamiseen. Tärkeämpää on oppilaiden motivointi oppia itse syvällisempiä asioita vapaa-ajallaan. Esimerkiksi ohjelmointikieliä on helppo omaksua lisää, kun ymmärtää muutaman kielen logiikan.”

Perustietouden osaaminen on tärkeä elementti kehittymisen kannalta. Ilman kehittymistä tukevaa perustietoutta, on hankala sisäistää uusia asioita. Nopeasti muuttuvan ympäristön vuoksi on turha lähteä opettamaan syvempiä opintoja pakollisten kurssien avulla, vaan ne voidaan siirtää vapaavalintaisiin, jolloin oppilas saa itse päättää mihin tietoturvaalan alueeseen haluaa panostaa enemmän.

6.2.8 Jos voisit muuttaa jotain opetussuunnitelmassa, mikä se olisi?

"Vähentäisin vapaavalintaisten määrää ja antaisin opiskelijoille mahdollisuuden käyttää ne mieluummin oman koulutusohjelmansa sisällön syventämiseen sen sijaan, että laajennettaisiin osaamista. Rahoitusta on vedetty alas, joka vaikuttaa huomattavasti mahdollisuuksiin. Perusasiat ja perustietouden tärkeys tulevat aina välillä takaisin opetussuunnitelmiin, ja häviävät vähän ajan päästä muiden asioiden tieltä. Perusosaaminen on siis opetuksen kannalta aaltoilevaa riippuen sen hetken suunnitelmista."

Aikaisemmassa kysymyksessä kerroin mielipiteestäni vapaavalintaisten suhteen. Tämä mielipide täsmää myös opettajan antamaan mielipiteeseen. Perusasioiden ymmärrys, kuten CIA-triadin ymmärtäminen ja soveltaminen tietoturvassa ovat asioita, joiden opetuksesta ei voida luopua.

6.2.9 Joudutaanko mielestäsi kiirehtimään liikaa kurssien tekemisessä, jotta toteutussuunnitelma saadaan pidettyä ajan tasalla nopeasti kehittyvässä tietoturva-alassa?

"Tietty pohja, perusasiat ja riskienhallinta pysyy paikoillaan. Syy kiireelle on kuitenkin aina sama, työtunteja saa käyttää aina vaan vähemmän per kurssi, jolloin valmisteluun käytetty aika jää alhaiseksi. Koko ajan haluttaisiin kehittää opetusta, mutta aika ei vain riitä. Kyseessä on tasapainoilua kiireen kurssivaatimuksien kanssa, mutta kontaktitunneista ei haluttaisi luopua yhtään enempää kuin on pakko."

On hyvä, että opettajat eivät halua luopua kontaktitunneista, sillä ne ovat erittäin tärkeitä oppilaan kehittymisen kannalta. Tiettyjen perusasioiden säilyminen ja riskihallinta on erittäin tärkeitä asioita pitää hyvällä mallilla, jotta toteutussuunnitelmat pysyvät laadukkaina.

6.2.10 Pitäisikö mielestäsi opetukseen sisällyttää enemmän läheisten yritysten kanssa tehtävää yhteistyötä, jotta oppilaat olisivat mahdollisimman paljon perillä yritysten osaamistarpeista?

"Ehdottomasti. Tietoturvatestauksessa on se haaste, että yritys on epäluuloinen päästämään oppilasta testaamaan ympäristöjä. Siihen pitäisi löytää joitain keinoja, esimerkiksi

joku toisi tuotantojärjestelmän replikan, eli vastaavan kopion, jota oppilas saisi sitten yrittää itse ohjeistetusti selvittää. Näin saataisiin oppilaille kokemusta oikeista ympäristöistä, ja ehkä jopa yrityksille uusia ratkaisuja."

Opettajan ratkaisumalli olisi hyvä kehitys oppimiselle, mutta mielestäni vielä kustannustehokkaampi tapa olisi palkata kehittyneempiä oppilaita rakentamaan erilaisia järjestelmiä ja aloittaa opettaminen niistä. Syy tähän on yritysverkkojen monimutkaisuus ja oppilaiden vähäinen murtautumistestauksen tietous. Liian korkean aloituskynnyksen johdosta oppilaan motivaatio voi laskea liian alas, jolloin ympäristöistä ei ole mitään hyötyä. Tarkoituksena on opettaa kolmen ja puolen vuoden tutkinnon aikana murtautumistestausta perusasioista mahdollisimman pitkälle. Yksinkertaisten perusasioiden opettaminen on tärkeämpää, sillä samalla oppilas tulee ymmärtämään komentoriviperusteita ja käyttöjärjestelmien toimintaa. Protokollat ja yhteystavat tulevat myös tutuiksi.

6.3 Haastattelun analysointi

Haastattelusta käy ilmi pieniä haasteita opetuksen tason ylläpitämisessä rekrytointivaatimuksien vaatimalla tasolla. Suurimpana ongelmana rahoitukset ja työtuntien määrä verrattuna tarvittavaan opetukseen. Työtuntien vähäinen määrä aiheuttaa kiireitä opetussuunnitelmien laatimiseen, eikä opetukselle jää tarpeeksi aikaa.

Tiimityöskentelyyn keskittyminen on erittäin tärkeää jo varhaisessa opetusvaiheessa, sillä se on lähes jokaista tietoturva-ammattilaista koskeva osaaminen. Asiakaspalvelua on hankala opettaa kouluissa, jolloin sen osaaminen yleensä kehittyy vasta työkokemuksella. Perustaito kuitenkin asiakaspalvelusta tulee koulusta, jolloin saadaan sen opettelemiseen hyvä tukeva pohja.

Turun ammattikorkeakoulussa ei suoranaisesti valvota opettajien opetuslaatua, eikä myöskään oppilaiden kehitystä. Tehtävillä ja tenteillä varmistetaan oppilaan kyky ylittää vähimmäisvaatimus kursseja kohden. Opettajien opettamistapoja tai -laatua ei valvota, mutta oppilailla on kuitenkin mahdollisuus palautekyselyjen kautta antaa opettajille palautetta opetuksestaan.

Perusosaamisen aaltoilevuus on vaarallista, sillä yrityksien odotukset vastavalmistuneista ja heidän tietotaitotasosta on yleensä samankaltainen. Jos opetuksesta jää kokonaisuuksia välillä pois, voi tämä aiheuttaa valtavia pettymyksiä yrittäjille, jotka saattavat

tulevaisuudessa hankkia uudet työntekijänsä muista kouluista. Perusosaamisen on oltava mahdollisimman korkealla oppilaan valmistuttua, jotta oppilaan on helpompi myös syventää osaamistaan jälkikäteen. Heikolla perusosaamisella oppilaan mahdollisuudet syventää osaamistaan heikontuu huomattavasti, eikä yhden tietyn osaamiseen ole välttämättä työmarkkinoilla tarvetta, jolloin vastavalmistuneen arvo työmarkkinoilla hupenee huomattavasti.

Opetuksen pysyminen jatkuvasti kehittyvän alan vauhdissa on haastavaa, sillä oppilaan valmistuessa uudet teknologiat voivat kokonaan korvata oppilaan opetteleman teknologian. Tästä syystä myös oppilaan itseopiskelu on erittäin tärkeää, ja se myös opetuksessa on otettu huomioon. Oppilaille opetetaan tapoja löytää informaatiota ja tehdä siitä tutkimuksellista analyysiä.

Yritykset eivät luota tarpeeksi päästääkseen opiskelijoita testaamaan heidän ympäristöään, mutta harkinnassa on esimerkiksi ympäristön kopiointi nimettömänä ja opiskelijoiden ratkaisujen anto eteenpäin yritykselle korjauskehotuksina. Näin saataisiin hyötyä jokaiselle. Vaikka opetus ei suoranaisesti ole kohdistettu työtehtäviin, on sen sisällössä keskitytty mahdollisimman laajasti eri työtehtävien tukemiseen

Yrityksien järjestelmien replikointi voi olla erittäin vaikea haaste. Monet yritykset eivät tule suostumaan kyseiseen toimenpiteeseen. Yrityksille pitää turvata anonymiteetti, ja ympäristöä pitää muokata sellaiseksi, ettei sen sisällöstä voida millään tavalla päätellä yritystä. Positiivisia puolia tämän onnistumisesta olisi paljon. Oppilaat oppisivat todellisen maailman tietoturvaa, saisi testata omaa osaamistaan realistisessa ympäristössä ja rakentamaan kustannustehokkaita ja järkeviä tietoturvaratkaisuja. Tulevaisuudessa voidaan esimerkiksi rakentaa opiskelijaprojekteja sen mukaan, millaisia tietoturvaratkaisuja yritys haluaa. Esimerkiksi pienien tietoturvariskien osalta yritykset harvoin lähtevät niitä korjaamaan, koska niiden korjaus voisi olla hyötyyn nähden liian kallista. Opiskelijoiden rakentamat tietoturvaratkaisut ovat usein paljon halvempia kuin alan ammattilaisten, vaikka niiden laatu ei välttämättä olisi yhtään huonompaa. Tällä tavoin yritys saisi pienemmätkin riskit ratkaistua suhteellisen halvalla, ja oppilaat oppisivat yrityksen tarpeiden ymmärtämistä ja todellista tietoturvatyötä. Tämä myös yhdistäisi tietojenkäsittelyyn tulevan tietojärjestelmän osaamisen, sillä lähes jokaisessa yrityksessä on jonkinlainen tietokanta tai muunlainen järjestelmä toimintansa taustalla.

Oppilaat voisivat myös valvoa erilaisia lokitiedostoja yritysten puolesta, jolloin yritys saisi halvemmalla toteutettua tietoturvaseurantaa, ja oppilaat saisivat jälleen hyvää kokemusta todellisten yritysten tietoliikennetapahtumista. Oppilaan huomattua esimerkiksi verkkohyökkäyksiä, voi hän alustavasti tehdä myös toimenpiteitä sen ehkäisemiseksi. Tällä tavoin yrityksen ei tarvitse odottaa ammattilaista hoitamaan asiaa, joka on todennäköisesti jo liian myöhäistä, vaan saa oppilaasta niin sanotusti ensiapua hyökkäyksen torjuntaan. Tämä on tietenkin valtava luottamuskysymys, mutta tähän tehtävään voisi päästää ainoastaan kehittyneimmät oppilaat. On kuitenkin tärkeää, ettei mikään näistä mahdollisista toimenpiteistä, joita haastattelusta analysoin jarruttaisi oppilaan oppimista tai koulutuksen etenemistä, vaan aikaa näihin projekteihin pitää säännöstellä oppilaan sen hetken etenemisen kanssa oikeassa suhteessa. Koulutus on aina joka tapauksessa ensisijainen asia.

7 POHDINTA

Haastattelujen saatujen tietojen perusteella selvisi, ettei Turun ammattikorkeakoululla ole valtavia ongelmia tietoturvaopetuksessa. Ongelmina ilmenivät tietoturvaperusteiden vähäinen opetus, esimerkiksi Windows ja Linux käyttöjärjestelmien komentorivit. Haastatteluista selviää selkeä puutteiden yhtäläisyys tietoturvan perusosaamisessa, esimerkiksi käyttöjärjestelmien komentoriviosaaminen ja yleistietous protokollista. Perusosaaminen, halu oppia ja kiinnostus alaa kohtaan ovat ylivoimaisesti tärkeimmät ominaisuudet tietoturva-alalle hakevilla, muut puutteet voidaan korjata työn ohessa. Turun ammattikorkeakoulun tietojenkäsittelyn koulutuksen opintojaksoista puolet sisältävät tietoturvaopetusta. Opetuksen sisältö on omiaan vastaamaan vallitseviin rekrytointivaatimuksiin tietoturva-alalla. Turun ammattikorkeakoulu on tämän vuoden osaamistavoitteissaan keskittynyt selkeästi enemmän haastatteluissa löytyneisiin ongelmakohtiin, esimerkiksi Linux-käyttöjärjestelmän komentoriviosaamista on aloitettu opettamaan enemmän ja perusosaamiseen on panostettu enemmän.

Yritykset arvostavat tietoturvan perustietoutta eivätkä vaadi suurta yksityiskohtaista osaamista. Turun ammattikorkeakoulu keskittyy tietoturvan perustietouteen. Turun ammattikorkeakoulun opetus on pääosin teoriaopetusta, joka yrityshaastattelun perusteella vastaa parhaiten tietoturvakonsultoinnin tarpeisiin. Käyttöjärjestelmien perusosaamiseen on keskitytty aiempaa enemmän.

Turun ammattikorkeakoulun on tuotava opetukseensa oikeassa elämässä tapahtuvan tietoturvan tapauksia, jotta opiskelija ymmärtää tietoturvan merkityksen yritysmaailmassa. Turun ammattikorkeakoulun on jatkuvasti kehitettävä osaamistavoitteitaan vastaamaan muuttuvia rekrytointivaatimuksia. Tämä tapahtuu jatkuvalla yhteistyöllä yritysten kesken, jolloin saadaan arvokasta tietoa sen hetken tilanteesta. Ammattikorkeakoulun on tulevaisuudessakin koulutettava tulevia ammattilaisia vastaamaan mahdollisimman laajasti yrityksien henkilöstötarpeeseen.

Ammattikorkeakoulun on varmistettava opetuksensa ajankohtaisuus jatkuvan seurannan avulla. Tietoturva-alan nopean kehityksen vuoksi on oltava mahdollista muuttaa opetussuunnitelmia nopeasti, jotta voidaan varmistaa oppilaiden osaamisen ajankohtaisuus valmistumishetkellä. Tällä tavoin saadaan mahdollisimman hyvät lähtökohdat työmarkkinoille.

Turun ammattikorkeakoulun olisi hyvä olla avoimempi yrityksiä kohtaan opetussisällöstään, jolloin yritykset tietäisivät etukäteen millaista osaamista he voivat vastavalmistuneilta odottaa. Samalla voidaan saada tärkeää informaatiota siitä, mitä yritykset sillä hetkellä toivovat uusilta työntekijöiltä. Turun ammattikorkeakoulu saisi myös tärkeää tietoa teknologiaosaamisista, jotka eivät muutu nopeasti, esimerkiksi tietoturva-alan haastattelusta saatujen koodauskielien kohdalla. Usein juuri isot yritykset pitävät samoja vaatimuksia yllä pitkään, sillä uusien teknologioiden käyttöönotto voi olla todella kallista.

Tietoturvayritykset usein rekrytoivat joko vakituisia työntekijöitä, jolloin perusosaaminen on erittäin tärkeää, jotta hyvän osaamispohjan kautta voidaan opettaa tarvittavia osaamisia nopeasti. Henkilön kehittymistä tukevat asiat ovat yrityksille tärkeitä. Yritykset myös rekrytoivat määräaikaisia työntekijöitä projektien osaamistarpeiden mukaisesti, jolloin on tärkeää osata perusteellisesti myös yksi tai kaksi teknologiaa tai ohjelmistokieltä, jotta vastavalmistuneella olisi mahdollisimman hyvät lähtökohdat työmarkkinoilla.

Ilman oppilaan harrastuneisuutta, halua kehittyä ja itseopiskelua on erittäin vaikea ylläpitää tarvittavaa osaamistaustaa. Oppilaan on pystyttävä oppimillaan perustiedoilla parantaa omaa osaamistaan koulutuksen aikana ja sen jälkeen. Tämä asian tärkeyden ymmärtämisen varmistaminen on jäänyt opetuksesta pois. Oppilas ei saa luulla pelkän koulussa opitun asian olevan tarpeeksi. Koulussa opittu on pohja, jolla voi kehittää omaa ammattiosaamistaan hallitusti eteenpäin.

Vapaavalintaisten kurssien sisällön samankaltaisuus oppilaan omaan koulutusalaan on välillä erittäin heikkoa, jolloin vapaavalintaisten kurssien mahdollinen muuttaminen oman alan syventäviin opintoihin olisi erittäin hyvä asia. Tämän voisi toteuttaa esimerkiksi yliopiston kanssa yhteistyössä, jolloin oppilaat voisivat ottaa toisista kouluista paremmin kursseja omaan opintosuunnitelmaan. Näin saataisiin myös yliopiston opiskelijoille mahdollisuus ottaa omaan suunnitelmaansa ammattikorkeakoulun opintoja. Näin saadaan toteutettua realistinen ja hyvä pohja oppilaan osaamiselle ja syvennys osaamiselle, johon oppilaalla on omaa motivaatiota. Insinööreille siirtyvän tietoliikenne opetuksen sisältö olisi myös vapaavalintaisten kannalta erittäin hyvä lisä tietojenkäsittelyä opiskelevalle. Samoin insinööreille tietojärjestelmien opettelu.

Yliopiston ja ammattikorkeakoulun yhteistyössä tehtyjen projektien avulla myös ammattikorkeakoulussa opiskelevat saisivat paremman käsityksen tutkimuksista ja niiden dokumentaatiotavoista, ja yliopistossa opiskelevat saisivat tärkeää käytännönkokemusta tietoturvasta.

Yrityksien kanssa tehdyt projektit ja niistä saadut todellisen tietoturvatilanteen kokemukset ovat tärkeitä osia oppilaan kehittymisessä ammattilaiseksi. Yrityksien kanssa tehtävä yhteistyö on pidettävä mahdollisimman turvallisena yrittäjän kannalta, jotta yritys uskaltaa antaa oppilaiden käsitellä heidän tietojaan. Yritys voi esimerkiksi luovuttaa järjestelmästään kopion opettajalle, joka poistaa siitä tunnistettavat tiedot, jolloin oppilas pääsee käsiksi todelliseen yritysympäristöön, ja voi näin myös ratkaista ohjatusti yrityksen tietoturvaongelmia. Tämä olisi erittäin hyvä tapa opettaa ja siitä olisi myös hyötyä yhteistyöyrityksille.

Tällä hetkellä Turun ammattikorkeakoulussa kehitetään jatkuvasti uudenlaisia tietoturvaopetukseen tarkoitettuja ympäristöjä, jotka sisältävät Linux- ja Windows-käyttöjärjestelmiä. Nämä ovat hyviä keinoja tämän hetken ongelmien korjaamiseen, jotka myös haastatteluista käy ilmi. Komentoriviperusteet tulevat hyvin opetuiksi käytännön tietoturvatestauksen aikana, ja Windows-käyttöjärjestelmien lisäys tietoturvaopetukseen on erittäin tervetullut ratkaisu.

Komentoriviosaaminen ja erilaisten protokollien kehittäminen tulisi myös olla osana käyttöjärjestelmien perusosaamista. Oppilas voisi käyttää järjestelmiä etäyhteyksien avulla, jolloin erilaiset yhteysprotokollat tulisivat helpommin sisäistettyä ja samalla komentorivien käyttö tulisi tutuksi. Toiminnallisesti tästä ei ole haittaa, sillä yhteydelliset protokollat tarkistavat liikennettä jatkuvasti, jolloin tietoja ei häviä välistä. Näin myös oppilas ymmärtää yhteydettömän ja yhteydellisen protokollan eron nopeasti ja oppii käyttämään erilaisia etäyhteysprotokollia. Tällä myös helpotettaisiin nykyistä kiintolevyjen tilaongelmaa. Monet oppilaat jättävät luomiaan virtuaalikoneita kurssin loputtua fyysisille koneille, jolloin niiden kiintolevyt täyttyvät nopeasti. Virtuaalisoimalla koko opetusympäristö takaisi jo valmiiksi asennetut ympäristöt oppilaille, ja niitä voisi käyttää monet kurssit uudestaan ja uudestaan. Päivittäminen myös kävisi nopeammin, sillä ympäristöt olisivat kopioita toisistaan. Tämä kuitenkin edellyttäisi sitä, ettei oppilaat vaihtaisi virtuaalisten ympäristöjen kirjautumistietoja. Ympäristön ylläpitäjällä on oltava jonkinlainen mahdollisuus palauttaa koneet alkuperäisiin asetuksiin kurssin loputtua.

Tulevaisuutta ajatellen Turun ammattikorkeakoulun kannattaa yhdistää jo tällä hetkellä oleviin toteutussuunnitelmiin uusia asioita, jotka eivät vaadi suuria lisäresursseja. Esimerkiksi aikaisemmin mainittu etäyhteys käytettäviin tietokoneisiin fyysisen kontaktin sijaan toisi nopeasti uutta sisältöä kursseihin, ilman suurta muutosta suunnitelmiin. Joissain tilanteissa tämä ei tietenkään ole mahdollista, jos fyysinen kontakti kohdekoneeseen vaaditaan.

Turun ammattikorkeakoulussa sijaitsevan tietoturvalaboratorion pitäisi olla myös paikka oppilaille, jotka ovat kiinnostuneita opettelemaan tietoturvaa. Siellä tällä hetkellä työskentelevät henkilöt ovat osaamiseltaan usein paljon edelle ensimmäisen ja toisen vuoden opiskelijoita, jolloin opiskelijat voisivat toisilleen opettaa myös tietoturvaa kontrolloidussa laboratoriossa. Oppilaat saisivat hyvää käytännönkokemusta tietoturvasta, ja samalla opintopisteitä raportoiduista projekteistaan. Samalla opettava opiskelija saisi projektityöstään opintopisteitä esimerkiksi esimies- tai opetustehtävistä, kokemusta opettamisesta ja parantaisi sosiaalisia taitojaan työyhteisössä. Oppilas voi myös antaa palautetta opettavalle oppilaalle, jonka kautta oppilas kehittää opettamistaitojaan eteenpäin. Kyseiseen kehitysehdotukseen tarvittavat laitteistot ja ympäristöt ovat joko olemassa tai kehitteillä valmistuen lähitulevaisuudessa. Ratkaisumalli olisi erittäin kustannustehokas ja projektiopintopisteiden vaatimuksien täyttävä.

Haastattelusta selviää, ettei opettajilla ole tällä hetkelläkään aikaa tarpeeksi opettamiseen, joten yllä mainittu opiskelijoiden vapaaehtoinen opettaminen helpottaisi takkaa. Tietenkin raportti on tarkistettava myös vakiohenkilökunnan toimesta, mutta sitä ennen opettava oppilas tarkistaa raportin itse, ja päättää kannattaako projektia edes lähettää eteenpäin henkilökunnalle tarkistettavaksi. Opettava oppilas voi myös merkitä kohtia, jotka voivat raportissa olla esimerkiksi huonosti raportoituja tai liian lyhyitä.

Turun ammattikorkeakoulun opetusta voidaan kehittää rakentamalla tarkemmat pohjatavoitteet toteutussuunnitelmiin, tällä tavoin joka vuosi toteutussuunnitelmat sisältäisivät saman pohjatietouden, jonka avulla voidaan varmistaa toteutuksen laatu. Hyvän ja jatkuvan pohjan päälle voidaan lisätä juuri sen hetken tärkeimpiä asioita. Tietoturvan teoriaosuudesta voidaan tehdä kattava kuva siitä, mitä yritykset tarvitsevat. Esimerkiksi erilaisten riskihallintajärjestelmien, shokkipalveluiden ja muiden ulkoisten tietoturvarakenteiden osaaminen teoriatasolla olisi suotavaa. Näiden olemassaolon tietäminen on jo haastatteluista saatujen tietojen perusteella positiivinen asia rekrytointia ajatellen.

Ammattikorkeakoulun pitää tehostaa yrityksiin yhteydenottoja yhteistyöajatusten kanssa. Mitä enemmän yrityksiä on yhteistyössä Turun ammattikorkeakoulun kanssa, sitä enemmän mahdollisuuksia erilaisten opetustapojen ja ympäristöjen kehittämiseen on. Yritykset voisivat esimerkiksi kertoa tapahtuneiden tietoturvariskien hallintatavoista tai esimerkiksi omien kokemusten ja tapahtuneiden tietoturvaongelmien taustoista ja miten ne ratkaistiin heidän yrityksessään. Tämän jälkeen ammattikorkeakoulu voisi esimerkiksi jäljentää samantapaisen tilanteen ja antaa oppilaiden keksiä siihen ratkaisu. Näin

oppilaat saisivat todellisia tilanteita ja ymmärtäisivät tietoturvaratkaisujen ongelmia. Ratkaisut pitää olla kustannustehokkaita ja niiden toimivuus on testattava ennen käyttöönottoa tai tässä tapauksessa oppilaan ratkaisun hyväksyntää.

Turun ammattikorkeakoulu on opettanut minulle monia asioita, on silti selvää, että olen oppinut enemmän tehdessäni työkseni tietoturvaprojekteja. Pääsääntöisesti työni opiskelija-assistenttina on sisältänyt erilaisten laitteiden tai järjestelmien murtautumistestausta tai kehitystä. Opin paljon tietoturvasta ensimmäisen kehitysprojektini ansiosta, jossa pääsin tutustumaan murtautumistestausopetukseen tehtyyn ympäristöön. Ympäristö sisälsi kaiken kaikkiaan noin 17 erilaista järjestelmää, joiden haavoittuvuuksien ymmärtäminen vei aikaa. Haavoittuvuuksien syyn ja haavoittuvuuksien hyväksikäytön opettelun aikana opin samalla paljon erilaisista protokollista ja komentorivin käyttö alkoi sujua luonnostaan. Itseopiskelu työn ohella on mahdollistanut nopean kehittymiseni tietoturvaammattilaiseksi. Olen keskittynyt murtautumistestaukseen ja erilaisten järjestelmien ymmärtämiseen. Olen oppinut tunnistamaan riskejä ja haavoittuvuuksia niin sisäisistä järjestelmistä ja niiden toiminnasta, kuin verkkopalveluista ja verkkopalvelimista. Olen myös työssäni päässyt murtautumistestaamaan paljon erilaisia laitteita, kuten langattomassa verkossa toimivaa kahvinkeitintä ja Bluetooth-tekniikalla toimivia laitteita. Olen kehittänyt ympäristöjä, joissa käytetään erilaisia protokollia ja yhteyskeinoja. Olen myös murtautumistestauksessa päässyt käyttämään erilaisia haittasovelluksia, verkon yli tapahtuvia hyökkäyksiä ja esimerkiksi selainkaappausta.

Kuten ammattikorkeakoulussa tapahtuneesta haastattelusta selvisi, on monimutkaisten tietoturvaprotokollien tai muiden taitojen opettaminen koulutuksen ohella vaikeaa vähäisen ajan vuoksi. Tästä syystä harrastuneisuus tai omassa tapauksessani työnteko opiskelun ohella on erittäin tärkeää oppilaan kehityksen kannalta. Turun ammattikorkeakoulu luo tähän hyvän mahdollisuuden ja takaa oppimiselle tehokkaan ja järjestelmällisen pohjan.

LÄHTEET

Ahvonen, H ja Ollonqvist, M. 2008. Onnistunut rekrytointi ja sitouttaminen, CASE: Lammin osuuspankki. Opinnäytetyö, AMK, Lahden ammattikorkeakoulu, liiketalouden koulutusohjelma, taloushallinto/yrityshallinto. Viitattu 22.4.2017 https://www.theseus.fi/bitstream/handle/10024/11370/2009-03-05-02.pdf?sequence=1

Elinkeinoelämän keskusliitto 2017. Tietoturvallisuus. Viitattu 20.4.2017 https://ek.fi/mita-teemme/tyoelama/yritysturvallisuus/tietoturvallisuus/

Empore Oy 2014. Opas rekrytointiin ja rekrytoinnin suunnitteluun. Viitattu 26.5.2017. http://www.empore.fi/tyonantaja/rekrytointiopas.php

Forsberg, L. 2007. Onnistunut rekrytointi ja sitouttaminen. Opinnäytetyö, AMK, Lahden ammattikorkeakoulu, liiketalouden laitos, taloushallinto. Viitattu 20.4.2017 https://www.theseus.fi/bitstream/handle/10024/11261/2008-01-18-02.pdf?sequence=1

KPMG 2017. Lisätietoa työpaikasta. Cyber Security Consultant. Viitattu 31.5.2017 https://krbsjobs.brassring.com/tgwebhost/searchresults.aspx?PartnerId=30008&SiteId=5056&Function=LinkQuery&LinkId=291

Pietikäinen, S. 2013. Tietoturva. Valtionhallinnon tieto- ja kyberturvallisuuden ohjausryhmän (VAHTI) ohjesivusto. Viitattu 26.4.2017 https://www.vahtiohje.fi/c/document_library/get_file?uuid=4e21a518-82ff-4dfe-b725-efcb6f97126d&groupId=10229

PTES 2014. Penetration Testing Execution Standard. Viitattu 31.5.2017 http://www.pentest-standard.org/index.php/Main_Page

SANS 2006. Penetration testing: Accessing your overall security before attackers do. Viitattu 31.5.2017 https://www.sans.org/reading-room/whitepapers/analyst/penetration-testing-assessing-security-attackers-34635

Suojausmenetelmät 2017. Artikkeli internetopas-sivustolla. Viitattu 26.4.2017 http://www.internetopas.com/yleistietoa/tietoturva/suojausmenetelmat/

TE-palvelut 2017. Avoimet työpaikat. Helsinki, Espoo, Tampere, Turku. Tietoturva. Viitattu 24.5.2017 http://paikat.te-palvelut.fi/tpt/?searchPhrase=tietoturva&locations=Helsinki%2CEspoo%2CTampere%2CTurku&announced=0&leasing=0&english=false&sort=1

Tietoturva 2017. Artikkeli internetopas-sivustolla. Viitattu 22.4.2017 http://www.internetopas.com/yleistietoa/tietoturva/

Tilastokeskus - Virtual Statistics – Tiedonkeruu 2017. Haastattelutavat, Teemahaastattelu. Viitattu 24.5.2017 https://www.stat.fi/virsta/tkeruu/04/03/

Tuovinen, J. 2013. TRAL tutkii 2013. IT-tradenomin osaaminen. Tradenomiliitto TRAL. Viitattu 24.5.2017 https://www.tral.fi/site/assets/files/1197/it-tradet.pdf

Turun ammattikorkeakoulu 2014. Turun ammattikorkeakoulun raportteja 179. Viitattu 31.5.2017 http://julkaisut.turkuamk.fi/isbn9789522164445.pdf

Turun ammattikorkeakoulu SoleOPS 2017. Etusivu. Viitattu 24.5.2017 https://ops.turkuamk.fi/opsnet/disp/fi/welcome/nop

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, opinnäytetyön alkuseminaari, 2019-2020. Viitattu 31.5.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=21831964&opettap_kohde=&soleid=ade076a5de07b8963718e86b6005ef8a&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, opinnäytetyön väliseminaari, 2016-2017. Viitattu 31.5.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=18912510&opettap_kohde=&soleid=3d3123412d45733eb5cb72a2d23af791&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, opinnäytetyön loppuseminaari, 2016-2017. Viitattu 31.5.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=19779384&opettap_kohde=&soleid=7dc1eaa52e0ef7d4a3089eebdd11d787&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, alakohtainen harjoittelu 1 ja 2, harjoittelu, 2018-2019. Viitattu 26.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_VuosTeemMat/tab/nop/sea?ryhma_id=20707561&opettaposa_opinvuos=2&ryhmopinkoht_suunvaiheht=&valkiel=

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, ammattiharjoittelu 1 ja 2, harjoittelu, 2019-2020. Viitattu 27.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_VuosTeemMat/tab/nop/sea?ryhma_id=20707561&opettaposa_opinvuos=3&ryhmopinkoht_suunvaiheht=&valkiel=

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Information Security, tietoturvan perusteet, ammattiopinnot, 2018-2019. Viitattu 26.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=21407887&opettap_kohde=&soleid=47593c8ef803f25633a0f5bffaf9f2ed&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Innovation project, projektiosaaminen ja yrittäjyys, 2017-2018. Viitattu 26.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=21408484&opettap_kohde=&soleid=7c48fee910ab62b39c2c0a7bba414b88&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Information security testing and assessment, enterprise information security management, suuntautumisvaihtoehdot, 2017-2018. Viitattu 27.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=19779384&opettap_kohde=&soleid=7dc1eaa52e0ef7d4a3089eebdd11d787&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, information security risk management, enterprise information security management, suuntautumisvaihtoehdot, 2017-2018. Viitattu 27.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=19779384&opettap_kohde=&soleid=7dc1eaa52e0ef7d4a3089eebdd11d787&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Käyttöjärjestelmät, tietojenkäsittelyn perusteet, ammattiopinnot, 2017-2018. Viitattu 26.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=21408842&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, network security, enterprise information security management, suuntautumisvaihtoehdot, 2017-2018. Viitattu 27.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=19779384&opettap_kohde=&soleid=7dc1eaa52e0ef7d4a3089eebdd11d787&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Perehdytys informaatioteknologiaan, muut yhteiset perusopinnot, perusopinnot. 2017-2018. Viitattu 26.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=21408731&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Sovellusohjelmointi, liiketoimintaratkaisujen ohjelmointi, ammattiopinnot, 2015-2016. Viitattu 27.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=19779384&opettap_kohde=&soleid=7dc1eaa52e0ef7d4a3089eebdd11d787&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, tietojenkäsittelyn tutkimus ja kehitys, 2016-2017. Viitattu 26.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=21268823&opettap_kohde=&soleid=2c11b690c6d6d3eba7b68f2154a93186&stack=push

Turun ammattikorkeakoulu SoleOPS 2017. Tietojenkäsittelyn koulutus, Web application security, tietoturvan perusteet, ammattiopinnot, 2017-2018. Viitattu 26.4.2017 https://ops.turkuamk.fi/opsnet/disp/fi/ops_OpetTapTeks/tab/tab/sea?opettap_id=21610533&opettap_kohde=&soleid=f43a089a1850a5fe67c96ac7c6b2399e&stack=push

Valtionhallinnon tietoturvallisuuden johtoryhmä 2009. Vahtiohje, tietoturvallisuudella tuloksia. Viitattu 27.4.2017 https://www.vahtiohje.fi/web/guest/chapter1