KYBERTURVAAJA-HANKE

LOPPURAPORTTI, TULOKSET, YHTEENVEDOT JA TUOTOKSET

SISÄLLYSLUETTELO

TIIVISTELMÄ

Hanke:	Kyberturvaaja, S21325
Ajankohta:	1.4.2018 – 31.7.2020
Rahoittaja:	Pohjois-Pohjanmaan ELY-keskus, Euroopan Sosiaalirahasto
Toteuttajat:	Metropolia ammattikorkeakoulu, Oulun yliopisto, Tampereen ammattikorkeakoulu, Tampereen korkeakoulusäätiö sr ja Turun ammattikorkeakoulu

Tiivistelmä:
Kyberturvaaja-hanke toteutettiin viiden korkeakoulun yhteishankkeena 1.4.2018-31.7.2020. Hankkeen päätavoitteena oli vastata työelämän kyberturvallisuuden osaamistarpeisiin kehittämällä verkostona olemassa olevista tutkintokoulutusten osista työelämäkoulutuksia. Hanke oli jaettu kolmeen osatavoitteeseen, joista jokaiseen liittyi useita toimenpiteitä. Osatavoitteet olivat: 1. Yhteistyöverkoston rakentaminen, 2. Työelämäkoulutussuunnitelmien tekeminen ja 3. Kyberturvallisuuden testaus- ja pilotointiympäristöjen hyödyntäminen.

Hankkeeseen tehtiin muutoshakemus 27.11.2019, jolla korjattiin hankkeen aikataulua sekä resursointeja. Hanke toteutui muutoshakemuksen mukaisessa aikataulussa ja kaikki hankkeeseen liittyvät toimenpiteet saatiin suoritettua.

Kokonaisuutena hanke onnistui saavuttamaan sille asetetut tavoitteet kattavasti ja hanketta voi pitää onnistuneena. Eri osatavoitteiden saavuttamisissa oli eroja. Päätavoitteessaan hankkeessa saatiin aikaiseksi merkittäviä tuloksia, sillä hankkeen aikana syntyi 23 työelämäkoulutuksen suunnitelmat. Koulutusten toteuttaminen ei kuulunut hankkeeseen, mutta sillä saavutetaan pitkäaikaista vaikutusta työelämän kyberturvallisuusosaamisen kehittämisessä.

Hankkeessa syntyi myös muita tuotoksia kuten yhteistoimintamalli, malli työelämäkoulutuksen kehittämiselle sekä malli ympäristöjen yhteiskäytölle. Näiden mallien toimintaa testattiin hankkeen yhteydessä.

Tässä raportissa esitetään hankkeen tuloksia tarkemmin ja yksityiskohtaisemmin. Raportissa on myös kuvaukset jokaisesta suunnitellusta työelämäkoulutuksesta.

Kaikki hankkeen tulokset on koottu tähän raporttiin ja jaetaan avoimesti kaikkien saataville hankkeen www-sivujen kautta.

HANKKEEN TAVOITTEET, TOIMENPITEET JA TULOKSET

YLEISTÄ

Kyberturvaaja-hankkeen päätavoitteena oli vastata työelämän kyberturvallisuuden osaamistarpeisiin kehittämällä verkostona olemassa olevista tutkintokoulutusten osista työelämäkoulutuksia. Tämä päätavoite oli jaettu kolmeen konkreettiseen osatavoitteeseen, joille jokaiselle oli asetettu tavoiteltava tulos sekä määritetty erinäisiä toimenpiteitä, joilla tulokseen pyritään. Nämä osatavoitteet, toimenpiteet ja tulokset oli kuvattu hankehakemuksessa.

Hanke onnistui pääosin saavuttamaan tavoitteensa. Kaikki hankkeelle määritetyt toimenpiteet saatiin suoritettua ja hankeen tuloksina syntyi lukuisia työelämäkoulutussuunnitelmia sekä prosessien kuvauksia, jotka on jaettu hankkeen www-sivujen kautta niiden hyödyntämisestä kiinnostuneille tahoille.

Suurimmat ongelmat hankkeelle aiheutui Metropolia ammattikorkeakoulun Espoon kampuksen äkkinäisestä sulkemisesta keväällä 2019 sekä koronaviruksen aiheuttamasta mullistuksesta keväällä 2020, jolloin kaikkien oppilaitosten kampukset suljettiin. Lisäksi hankkeeseen oli jonkin verran vaikeuksia saada tekijöitä. Hankkeen alku lähti liikkeelle hiukan aikataulusta myöhässä ja hankkeelle tehtiin muutossuunnitelma marraskuussa 2019, joka hyväksyttiin rahoittajan toimesta. Hankeen toimenpiteet saatiin suoritettua muutossuunnitelman mukaisesti.

HANKKEEN MÄÄRÄLLISET TAVOITTEET

Hankesuunnitelmavaiheessa hankkeelle asetettiin määrälliset tavoitteet yritysten ja henkilöiden osallistumisesta hankkeeseen. Yritysten määrä tarkennettiin hankesuunnitelman muutoksen yhteydessä marraskuussa 2019.

OSALLISTUNEET YRITYKSET

Yrityskoko	Alkuperäinen tavoite	Tarkennettu tavoite (marraskuu 2019)	Toteuma
Mikroyritys	4	10	16
Pieni yritys	20	14	10
Keskisuuri yritys	16	10	10
Suuryritys	0	6	10
YHTEENSÄ	40	40	46

Lisäksi hankkeeseen osallistui 12 muuta organisaatiot (yhdistykset, kunnat, kuntayhtymät, valtion viranomainen).

Määrällisesti hanke tavoitti riittävästi yrityksiä mutta yritysten jakauma yrityskoon mukaisesti ei vastannut täysin alkuperäistä tavoitetta. Pieniä ja keskisuuria yrityksiä tavoitettiin merkittävästi vähemmän kuin mitä oli tarkoitus. Tämä johtui pitkälti sitä, ettei tuon koko luokan yrityksiltä tuntunut löytyvän aikaa tai muuta resurssia hankkeeseen osallistuakseen. Vastaavasti suurempia yrityksiä hanke kiinnosti enemmän kuin oli alun perin odotettu. Tämä johtunee pitkälti siitä, että suuremmissa yrityksissä on kyberturvallisuuden tarve tunnistettu ja siihen panostetaan. Pk-sektorin yritysten vähäisyyttä kompensoi kuitenkin huomattavasti ennakoitua suurempi mikroyritysten määrä sekä monen pienen yhdistyksen osallistuminen hankkeeseen.

OSALLISTUNEET HENKILÖT

Hankesuunnitelmassa asetettiin tavoitteeksi 47:n henkilön osallistuminen hankkeeseen ja näistä 7 olleen naisia. Osallistujia oli kaiken kaikkiaan 70, joista 17 oli naisia. Tältä osin voidaan todeta, että hanke saavutti hyvin tavoitteensa.

HANKKEEN LAADULLISET TAVOITTEET, TOIMENPITEET JA TULOKSET

Alla on esitetty osatavoitteet, toimenpiteet ja tavoiteltu tulos sekä kuvattu toteutunutta tulosta. Tämän dokumentin osassa Tuotokset on eriteltynä hankkeen toimenpiteiden pohjalta syntyneet tuotokset kuten selvitykset, raportit jne.

TAVOITE 1. YHTEISTYÖVERKOSTON RAKENTAMINEN

Tavoite 1. Yhteistyöverkoston rakentaminen: alueellisesti selvitetään yritykset, jotka haluavat olla mukana kehittämässä ja hyödyntämässä syntyviä työelämäkoulutuksia ja osallistua verkoston toimintaan. Lisäksi järjestetään kyberturvallisuuteen liittyviä tapahtumia koordinoidusti hankkeessa mukana olevien korkeakoulujen kesken. Tapahtumien aiheet tulevat yrityselämästä, ja niitä räätälöidään vastaamaan yritysten tarpeita.
Toimenpide 1.1 Jokainen osallistuva ammattikorkeakoulu tekee kartoituksen oman alueensa toimijoista, jotka haluavat hankkeeseen aktiivisesti osallistua, ja kokoavat toimijoista verkoston. TAMK vastaa kaikkien hankkeessa mukana olevien hanketoimijoiden välisestä yhteistoiminnasta. Toimenpide 1.2 Jokainen osallistuva ammattikorkeakoulu järjestää yhteistyössä yliopistojen kanssa omalla alueellaan alkuseminaarin, johon kutsutaan alueen pk-yrityksiä ja heidän työntekijöitään, oppilaitosten opiskelijoita, julkisia toimijoita ja muita kiinnostuneita tahoja. Alkuseminaari aktivoi kohderyhmät huomioimaan paremmin kyberturvallisuus osana toimintaansa. TAMK vastaa kaikkien hankkeessa mukana olevien hanketoimijoiden välisestä yhteistoiminnasta. Toimenpide 1.3 Kehitetään jokaiselle hanketoimijapaikkakunnalle ainakin yksi kyberturvallisuuteen liittyvä tilaisuus, jonne kutsutaan mukaan verkostossa toimivien yritysten henkilöstöä sekä oppilaitosten henkilöstöä ja opiskelijoita. Jokainen toimija suunnittelee tilaisuuden itsenäisesti ja TAMK koordinoi asian. Tilaisuuksien työmuotona voi olla seminaari, työpaja, hackathlon tai messut. Tapahtumat kehittävät alueiden yritystoimintaa. Tilaisuuksien kesto on vähintään yksi päivä ja ne suunnitellaan tavalla, jolla niitä voidaan toistaa jatkossakin, myös hankkeen jälkeen, ylläpitäen kyberturvallisuustietoisuuden kasvattamista ja verkoston yhteistoimintaa. Tilaisuuksissa annetaan yrityksille tietoa hankkeessa rakennettavista kyberturvallisuuden työelämäkoulutuksista. Toimenpide 1.4. Hankkeen lopussa jokainen osallistuva ammattikorkeakoulu järjestää yhteistyössä yliopistojen kanssa omalla alueellaan loppuseminaarin, johon kutsutaan kaikki alueen asukkaat, julkiset toimijat ja yritystahot, ja jossa esitellään hankkeen yhteydessä saatuja tuloksia ja kertyneitä tietoja sekä

verkostoidutaan alueiden eri toimijoiden kanssa. Seminaariesityksien yhteenvedot jaetaan verkoston toimijoiden kesken.

Tavoiteltu tulos 1. Hankkeessa syntyy neljän alueen asiantuntijoiden kesken aktiivinen yhteistyöverkosto, jonka avulla vastataan työelämän kyberturvallisuuden osaamistarpeisiin. Lyhyellä aikavälillä alan toimijat oppivat paremmin tuntemaan toisensa ja tämä johtaa pitkällä aikavälillä yhteistyön syventymiseen. Verkostossa saatu tietämys ja yhteistoimintamalli levitetään koko maan kattavaksi.

Toteuma:

Tässä tavoitteessa onnistuttiin kohtalaisesti. Jokaisella hankepaikkakunnalla järjestettiin hankkeen aikana useampia kyberturvallisuuteen liittyviä tilaisuuksia erilaisille kohderyhmille. Ensimmäiset tilaisuudet järjestettiin hankkeen alussa ns. aloitusseminaareilla, jotka pidettiin jokaisella hankepaikkakunnalla. Muut hankkeen aikana toteutetut tilaisuudet olivat tyypillisesti seminaareja tai työpajoja. Korona-kriisi keväällä 2020 vaikutti tapahtumien järjestämiseen ja joitakin suunnitelmia ei sen tähden kyetty toteuttamaan toivotulla tavalla. Hankkeen päätösseminaari pidettiin 20.5. kaikilla kansalaisille avoimena valtakunnallisena webinaarina. Tapahtumat omalla osallaan auttoivat verkostojen rakentamisessa. Hankkeessa syntyi hanketoimijoiden välille yhteistyötä tekevä verkosto sekä paikallisesti jokaiselle toimijalle omia verkostoja, joissa on mukana yrityksiä. Yhteistyöverkostojen rakentaminen on pitkäaikainen prosessi ja hankkeessa ei saavutettu kattavaa syvällistä yhteistyötä eri verkostojen osien välille. Pidemmällä aikavälillä yhteistyö yritysten kanssa syvenee. Hankeen aikana saatu tietämys on jaettu kaikkien hyödynnettäväksi hankkeen www-sivujen kautta. Hankkeessa kehitettiin edelleen Iotti-hankkeen yhteistoimintamallia ja sovellettiin sitä. Näin syntyi oma tämän hankkeen yhteistoimintamalli. Hankkeeseen osallistui 47 yritystä ja 12 muuta organisaatiota. Näiden yritysten jakauma yrityskoon mukaan erosi hankkeelle asetetusta tavoitteesta. Pieniä ja keskisuuria yrityksiä oli mukana ennakoitua vähemmän ja mikro- sekä suuryrityksiä ennakoitua enemmän.

Tuotokset:

- Hankkeen www-sivut: https://projects.tuni.fi/kyberturvaaja/
- Yhteistoimintamalli
- Suunnitelmat kyberturvallisuuteen liittyvistä tapahtumista

TAVOITE 2. TYÖELÄMÄKOULUTUSTEN SUUNNITELMIEN TEKEMINEN

Tavoite 2. Työelämäkoulutusten suunnitelman tekeminen: tehdään kartoitus mukana olevien korkeakoulujen tutkinto- ohjelmien kyberturvallisuuteen liittyvistä osista, alueellisista osaamisalueista ja yritysten osaamistarpeista. Kartoituksen perusteella tehdään suunnitelma verkoston tarjoamista työelämäkoulutuksista.

Toimenpide 2.1 Jokainen oppilaitos tekee selvityksen omien tutkintokoulutusten kyberturvallisuuteen liittyvistä osista sekä mahdollisuudesta muokata niitä työelämäkoulutuksiksi. Oppilaitokset selvittävät omat

kyberturvallisuuden soveltamiseen liittyvät erityisosaamisalueensa, jotka voivat vahvistaa ja tarjota verkoston käyttöön. TAMK kokoaan selvitykset yhteen kokonaiskuvan saamiseksi.

Toimenpide 2.2 Jokainen oppilaitos selvittää oman verkostonsa yrityksiltä heidän osaamis- ja kouluttautumistarpeet.

Toimenpide 2.3 Kokonaiskuvan pohjalta laaditaan suunnitelmat mitä ja miten tutkintokoulutusten osia muokataan työelämäkoulutuksiksi ja kuinka niitä tarjotaan hyödynnettäväksi oppilaitosten muodostaman verkoston kautta siellä, mistä osaamista tarvitsevia yrityksiä löytyy.

Toimenpide 2.4 Tehdään selvitys, mitä tuloksia IoTTi-hankkeessa on saatu aikaiseksi ja kuinka niitä voidaan tässä hankkeessa hyödyntää. Jaetaan tuloksia ja tietoa hyvistä käytänteistä IoTTi-hankkeen toimijoiden kanssa puolin ja toisin.

Toimenpide 2.5 Tehdään selvitys, mitä synergiaetuja kyberturvallisuuden erikoistumiskoulutusten toimijoiden asiantuntijuuksissa sekä teknisissä ympäristöissä voidaan yhteistyöllä saavuttaa.

Toimenpide 2.6 Selvitetään verkostomaisesti toteutettavan työelämäkoulutuksen mahdolliset vaikutukset opintohallintoon ja tietojärjestelmiin.

Tavoiteltu tulos 2. Hankkeessa syntyy useita työelämäkoulutuksia. Työelämäkoulutukset kehitetään yhteistyössä hanketta toteuttavien koulutusorganisaatioiden kesken, mutta ne pilotoidaan hanketuen ulkopuolella. Koulutusten avulla mahdollisuudet kyberturvallisuusosaamiseen kehittyvät, ja uudenlaiset yrityksille sopivat koulutukset helpottavat osaamisvajetta. Kyberturvallisuuden osaaminen parantuu laajasti koko Suomessa.

Toteuma:

Tässä tavoitteessa onnistuttiin hyvin. Hankkeen alussa tehtiin kartoituksia yrityksiltä heidän kyberturvallisuusosaamistarpeestaan. Selvitysten perusteella työelämäkoulutusten tarpeet jaettiin kuuteen toimenkuviin perustuvaan ryhmään. Hankkeessa selvitettiin oppilaitosten tutkintokoulutuksien ja niiden osin soveltuvuutta työelämäkoulutuksiksi. Näiden selvitysten pohjalta suunniteltiin lukuisia työelämäkoulutussuunnitelmia, jotka on kuvattu tarkemmin koulutuskuvausten dokumentissa. Nämä tulokset jäävät kaikkien hankkeen oppilaitosten hyödynnettäväksi ja näin mahdollistetaan erilaisten kyberturvallisuuteen liittyvien työelämäkoulutusten tarjoaminen kattavasti koko maassa. Työelämäkoulutusten suunnittelemisesta tehtiin oma vuokaavionsa, jossa kuvataan kaikkia työelämäkoulutuksen suunnittelussa huomioon otettavia vaiheita.

Opintohallinnollisiin liittyviin prosesseihin on valtakunnallisesti tekeillä merkittäviä muutoksia, jotka tulevat vaikuttamaan tulevaisuuden yhteistoimintamahdollisuuksiin. Tässä hankkeessa päädyttiin kuvaamaan niitä opintojärjestelmien ja oppilaitosten hallinnon asettamia vaatimuksia, joita jokaisella oppilaitoksella on järjestettäessä työelämäkoulutuksia.

Tuotokset

- Tutkintokoulutusten kyberturvallisuuteen liittyvät osat
- Yritysten osaamis- ja kouluttautumistarpeet
- Työelämäkoulutuksen suunnittelu -prosessikuvaus
- Hankkeen aikana suunnitellut työelämäkoulutukset

- Selvitys IoTTi-hankkeen tulosten hyödynnettävyydestä
- Selvitys Kyberturvallisuuden erikoistumiskoulutusten synergiaeduista
- Selvitykset työelämäkoulutusten vaikutuksesta opintohallintoon ja tietojärjestelmiin

TAVOITE 3. KYBERTURVALLISUUDEN TESTAUS- JA PILOTOINTIYMPÄRISTÖJEN HYÖDYNTÄMINEN

Tavoite 3. Kyberturvallisuuden testaus- ja pilotointiympäristöjen hyödyntäminen: kartoitetaan hankkeeseen osallistuviin korkeakoulujen jo olemassa olevat kyberturvallisuuden koulutukseen ja tutkimukseen liittyvät tekniset ympäristöt sekä prosessit ja luodaan yhteinen toimintamalli niiden hyödyntämiselle työelämäkoulutuksissa verkoston toimijoiden kesken.

Toimenpide 3.1 Jokainen oppilaitos tekee oman selvityksensä kyberturvallisuuteen liittyvistä jo olemassa olevista teknisistä koulutus- ja tutkimusympäristöistä. Oppilaitokset tekevät ehdotukset siitä, miten heidän ympäristöjään hyödynnetään työelämäkoulutuksissa koko verkoston laajuudella. TAMK kokoaa selvitykset yhteen kokonaiskuvan saamiseksi.

Toimenpide 3.2 Kokonaiskuvan perusteella esitetään malli teknisten ympäristöjen hyödyntämiselle ja yhteiskäytön mahdolliselle laajentamiselle.

Tavoiteltu tulos 3. Oppilaitosten tekniset ympäristöt saadaan tehokkaaseen käyttöön jo hankkeen aikana. Tämä tukee alueellisten yritysten toimintaa, mahdollistaa pidemmällä aikavälillä uusien liiketoimintamahdollisuuksien syntymistä sekä parantaa yhteistoimintaa ja työelämäkoulutuksen laatua.

Toteuma:

Tässä tavoitteessa onnistuttiin välttävästi. Oppilaitosten tekniset ympäristöt kuvattiin ja niiden erilaisen yhteiskäytön mahdollisuuksia selvitettiin. Yhteiskäytölle tai käytön laajemmalle avaamiselle tuli kuitenkin esiin paljon rajoitteita ja reunaehtoja. Osa niistä on sellaisia, että niiden ylittäminen vaatisi merkittäviä rahallisia panostuksia (mm. lisensoinnit). Osaa ympäristöistä päästiin kuitenkin yhteiskäyttämään ja käyttöä testaamaan hankkeen aikana. Näiden pohjalta tehtiin malli ympäristöjen tulevaisuuden hyödyntämistä varten.

Tuotokset:

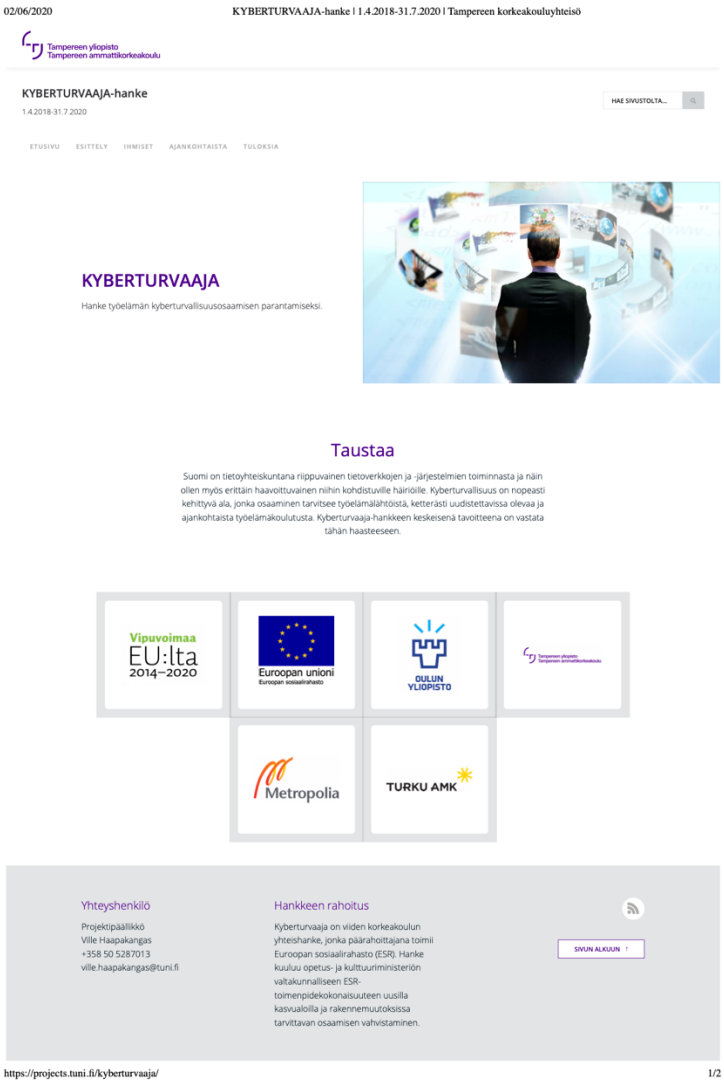
- Kooste oppilaitosten kyberturvallisuuteen liittyvistä oppimis- ja tutkimusympäristöistä
- Malli teknisten ympäristöjen hyödyntämiselle

HANKKEEN TUOTOKSET

Hankkeen merkittävin tuotos, joka oli myös hankkeelle asetettu päätavoite, oli suunnitellut työelämäkoulutukset. Niiden lisäksi hankkeessa syntyi lukuisia muita tuotoksia, jotka on pääasiassa kuvattu selvityksin tai yhteenvedoin.

WWW-SIVUT

Hankkeelle perustettiin hankkeen alussa omat www-sivut, joiden kautta on jaettu tietoa hankkeen tapahtumista ja tuotoksista. Sivuilla on julkaistu myös tämä dokumentti sekä muut hankkeen yleisesti hyödynnettävissä olevat tuotokset. Näin hankkeen tulokset pystyttiin jakamaan vapaasti hyödynnettäväksi kaikille halukkaille. Www-sivujen osoite on: https://projects.tuni.fi/kyberturvaaja/

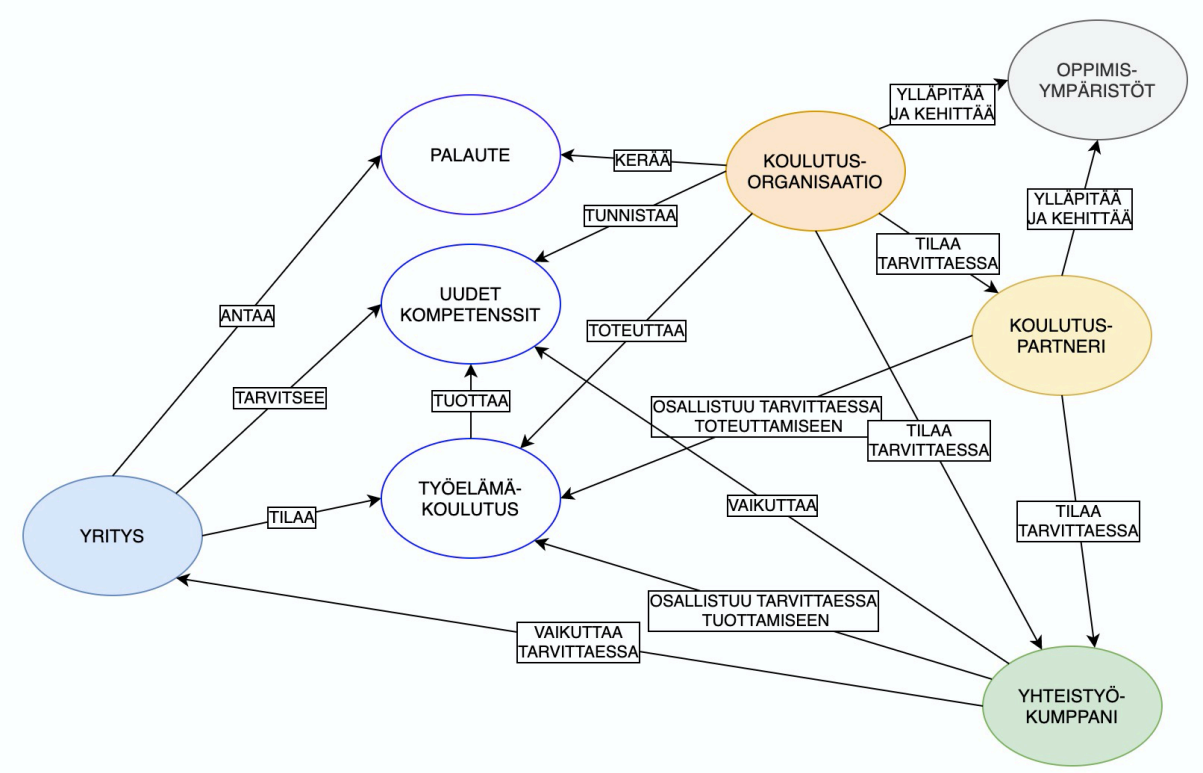


YHTEISTOIMINTAMALLI

”Hankkeessa tehdään yhteistyötä käynnissä olevan IoTTi-hankkeen kanssa, jossa kehitetään vastaavan kaltaista verkostomaista yhteistyömallia yrityslähtöisen työelämäkoulutuksen kehittämiseksi. Tässä hankkeessa mallia kehitetään edelleen ja otetaan siihen mukaan sekä yliopistojen että ammattikorkeakoulujen toimijoita.”

Hankkeessa kehitettiin seuraava malli yhteistoiminnalle IoTTi-hankkeen yhteistoimintamallia hyödyntäen:

1. Tunnistetaan tarve työelämäkoulutuksen kehittämiselle yhdessä yritysten kanssa.
2. Selvitetään oppilaitosten valmiudet koulutuksen toteuttamiselle.
3. Kootaan toteutusryhmä ja jaetaan vastuut.
4. Hyödynnetään hankkeen yhteistoimintamallia.
5. Koulutuksen suunnittelu ja toteuttaminen.
6. Palautteen kerääminen ja hyödyntäminen koulutuksen ja prosessin kehittämiseksi.
7. Viestintä osallistujien kesken ja sidosryhmille.



KYBERTURVALLISUUTEEN LIITTYVÄT TAPAHTUMAT

”Toimenpide 1.3 Kehitetään jokaiselle hanketoimijapaikkakunnalle ainakin yksi kyberturvallisuuteen liittyvä tilaisuus, jonne kutsutaan mukaan verkostossa toimivien yritysten henkilöstöä sekä oppilaitosten henkilöstöä ja opiskelijoita. Jokainen toimija suunnittelee tilaisuuden itsenäisesti ja TAMK koordinoi asian. Tilaisuuksien työmuotona voi olla seminaari, työpaja, hackathlon tai messut. Tapahtumat kehittävät alueiden yritystoimintaa. Tilaisuuksien kesto on vähintään yksi päivä ja ne suunnitellaan tavalla, jolla niitä voidaan toistaa jatkossakin, myös hankkeen jälkeen, ylläpitäen kyberturvallisuustietoisuuden kasvattamista ja verkoston yhteistoimintaa. Tilaisuuksissa annetaan yrityksille tietoa hankkeessa rakennettavista kyberturvallisuuden työelämäkoulutuksista.”

YHTEENVETO

Jokainen osatoteuttaja suunnitteli tilaisuudet omalle alueelleen itsenäisesti. Osa tilaisuuksista järjestettiin jo hankkeen aikana ja niitä voidaan järjestää vastaavalla tavalla myöhemminkin. Osa tilaisuuksista peruuntui lähinnä Covid19-tilanteen tähden keväällä 2020. Osa tilaisuuksista suunniteltiin mutta niitä ei toteutettu hankkeen aikana.

Tampereen alueen toimijat (TAMK ja TTY) suunnittelivat seuraavan laisia kyberturvallisuuteen liittyviä tilaisuuksia:

- Työpajapäivä, jossa on mukana alan asiantuntijoita
- ”Kyberturvallisuuspäivät”, useamman päivän laajempi yritysvetoinen tilaisuus
- Hakkerointipäivä, tilaisuus erityisesti ”hakkeriryhmille”
- Yleinen teema/koulutuspäivä kyberturvallisuuteen liittyvän ajankohtaisen asian pohjalta
- Kyberturvallisuusaiheen mukana olo jonkun muun teeman pohjalta järjestetyssä tilaisuudessa
- Kyberturvallisuuden webinaari

Näistä hankkeen aikana toteutettiin erilaisia työpajapäiviä. Tämän lisäksi hankkeen loppuseminaarina toteutettiin muiden osatoteuttajien kanssa yhteistyönä laajempi webinaari.

Kokemusten mukaan Tampereen alueella on kiinnostusta osallistua kyberturvallisuuteen liittyviin tilaisuuksiin. Toimivimpia malleja ovat säännölliset lyhytkestoiset asiantuntijapuheenvuorot sekä kyberturvallisuus teemana jonkun toisen alan laajemmissa seminaaripäivissä tai tilaisuuksissa. Myös työpajoista ja webinaarista saadut kokemukset olivat hyviä ja niitä kannattaa toteuttaa jatkossakin.

Oulun yliopisto suunnitteli erikseen yhteistapahtuman kyberturvallisuuteen keskittyvän yhteisön OuluSecin kanssa. Asiantuntijapuheenvuorojen ja käytännön työpajojen yhdistelmä todettiin toimivaksi ja sitä käytettiin hankkeen aikana CriM-kyberturvallisuusseminaarin yhteydessä 2019. Vastaava tapahtuma on tarkoitus järjestää säännöllisesti uudestaan.

TurkuAMK järjesti hankkeen aikana kyberturvallisuuteen liittyviä tapahtumia kuten seminaarin ja työpajoja. Tietoturvapäivä järjestettiin Turussa 10.3.2020. Tätä tapahtumaa aiotaan jatkaa, kun COVID19 pandemia hellittää. Jatkossa tilaisuutta kehitetään laajemmaksi messutapahtumaksi.

Metropolia amk loi toimintamallin kyberturvallisuusaiheisen seminaarin järjestämisestä:

Kyberturvaaja
Hankekoodi: S21325

Kyberturvallisuusaiheisen seminaarin järjestäminen

Tässä dokumentissa käydään läpi toimenpiteet, jotka tulee huomioida järjestettäessä kyberturvallisuusseminaaria. Toimenpiteet on jaettu kolmeen osaan: ennen seminaaria, seminaaripäivänä ja seminaarin jälkeen. Suurin osa toimenpiteistä tulee tehdä ennen seminaaria, joten se on otettava huomioon seminaariajankohdassa ja varattava suunnittelulle riittävästi aikaa.

Seminaarin sisältö: Kyberturvallisuus ja sen ajankohtaiset asiat erityisesti pk-yritysten näkökulmasta. Seminaarin puhujina toimivat kyberturvallisuuden asiantuntijat.

Seminaarin tavoite: kyberturvallisuustietoisuuden kasvattaminen ja tiedon jakaminen pk-yrityksille.

Kohderyhmä: pk-yritysverkosto

Kesto: puoli päivää tai kokonainen päivä

ENNEN SEMINAARIA:

Kustannusarvio ja rahoitus. Laadi arvio seminaarin kuluista ja selvitä rahoitus. Kulut muodostuvat tilanvuokrasta, tarjoilusta, järjestäjien työaikaresursseista ja mahdollisista puhujien palkkioista.

Seminaarin ajankohta ja tilavaraus. Päätä seminaarin ajankohta ja varaa tai vuokraa seminaarille auditoriotila. Jätä seminaarin suunnittelulle riittävästi aikaa. Tarkista tilaa varatessa sen maksimihenkilökapasiteetti.

Ohjelman laatiminen ja puhujien rekrytointi. Päätä seminaarin teema ja laadi alustava aikataulurunko (aloitus- ja lopetusaika, tauot ja esitysten määrällinen tarve). Rekrytoi puhujat. Sovi puhujien kanssa esityksen aihe ja kesto. Laadi lopullinen ohjelma ja aikataulu, kun puhujat on rekrytoitu. Puhujien rekrytointi saattaa viedä aikaa, joten ole ajoissa liikkeellä ja aktiivinen.

Markkinointisuunnitelma. Laadi seminaarin markkinointisuunnitelma hyvissä ajoin jo ennen lopullisen ohjelman valmistumista. Markkinointisuunnitelma sisältää ainakin kohderyhmän, viestintäkanavat (esim. organisaation tapahtumat-tiedotteet ja uutiskirjeet sidosryhmille, sähköpostilistat, sosiaalinen media), aikataulun ja toteuttajan.

Ilmoittautuminen seminaariin. Laadi sähköinen ilmoittautumislomake. Kerää lomakkeella ainakin seuraavat tiedot: nimi, yritys ja sähköposti. Kysy myös lupa tulevien seminaarien ja tapahtumien markkinointiin. Laadi tietosuojaseloste henkilötietojen keräämisestä ja linkitä se lomakkeelle. Päätä ilmoittautumisaika. Seminaarin ilmoittautumista ei kannata sulkea liian aikaisin, mieluiten esimerkiksi kaksi päivää ennen seminaaria.

Seminaarin tietojen julkaisu. Luo tapahtumasivu organisaation internetsivustolle ja laita seminaarin kaikki tiedot sinne (mm. aika, paikka, kohderyhmä, ohjelma, ilmoittautumisohje ja linkki ilmoittautumislomakkeelle). Seminaarin internetsivun linkkiä on helppo hyödyntää markkinoinnissa.

Markkinointi. Seminaariohjelman valmistumisen jälkeen markkinoi seminaaria markkinointisuunnitelman mukaisesti. Hyödynnä ja linkitä uutiskirjeisiin ja sosiaaliseen mediaan seminaarin internetsivua. Laadi seminaarikutsu (sisältäen ohjelman), jonka voit lähettää sähköpostitse pk-yritysverkostolle. Sähköpostin liitteeksi voi laittaa seminaarikutsun myös pdf-muodossa. Muista myös informoida tapahtumasta organisaatiosi sisällä ja pyydä kollegoita jakamaan kutsua omille verkostoilleen.

Ilmoittautumisten seuraaminen. Seuraa ilmoittautumisia aktiivisesti. Jos ilmoittautumisia tulee vähän, mieti mahdollisia uusia markkinointitoimenpiteitä. Jos ilmoittautumisia tulee paljon, ota huomioon tilan maksimihenkilökapasiteetti ja tarvittaessa siirrä seminaari isompaan tilaan tai sulje ilmoittautuminen. Ilmoittautumisen sulkemisessa muista päivittää tieto seminaarin täyttymisestä myös internetsivulle.

Kyberturvaaja
Hankekoodi: S21325

Seminaarin tarjoilut. Arvioi seminaarin osallistujamäärä ja sovi tarjoiluista hyvissä ajoin ravintolan kanssa. Vahvista tarjoilujen lopullinen henkilömäärä ravintolalle heidän aikataulunsa mukaan. Riippuen seminaarille asetetusta ilmoittautumisajasta, lisäilmoittautumisia voi vielä tulla tarjoilujen henkilömäärän vahvistuksen jälkeen, joten varaa tarjoiluja mieluummin vähän yli kuin alle.

Tiedottaminen saapumisesta, pysäköinnistä ja muista käytännön järjestelyistä. Päätä miten osallistujia tiedotetaan seminaariin saapumisesta ja muista mahdollisista käytännön järjestelyistä. Laita tiedot mieluiten ennakkoon seminaarin internetsivulle tai vaihtoehtoisesti lähetä tiedot ilmoittautuneille sähköpostitse ilmoittautumisajan päättymisen jälkeen. Jos osallistujia odotetaan tulevan kauempaa, niin saapumistiedot tulee olla osallistujien tiedossa hyvissä ajoin ennen seminaaria.

Yhteydenpito puhujiin. Huolehdi yhteydenpidosta puhujiin ja myös heidän opastuksestaan. Pyydä puhujia lähettämään seminaariesitykset ennakkoon ja kysy ennakkoon lupa saako esitysmateriaalin jakaa osallistujille seminaarin jälkeen. Lähetä heille saapumis- ja muut mahdolliset ohjeet.

Osallistujalistan laatiminen ja nimikyltit. Laadi seminaarin osallistujalista (ilmoittautuneet, puhujat ja järjestäjät) ja laadi kaikille nimikyltit. Varaa tyhjiä nimikylttejä yllätysosallistujille.

Ohjelman ja muun tiedon (esim. langattoman verkon) jako seminaaripäivänä. Päätä jaetaanko ohjelma osallistujille seminaaripäivänä sähköisesti vai paperisena. Selvitä onko seminaaritilassa langaton verkko tarjolla osallistujille ja jos on, miten tieto siitä jaetaan osallistujille seminaaripäivänä.

Seminaaritilan AV-laitteet ja AV-tuki. Tarkista viimeistään seminaaria edeltävänä päivänä, että tilan AV-laitteet toimivat. Lataa tarvittaessa puhujien esitykset ennakkoon esitystietokoneelle. Ota selvää, mistä saat AV-tukea tarvittaessa seminaarin aikana.

Opasteet ja osallistujien vastaanottopiste. Opasteita tarvitaan yleensä rakennuksen ulko-ovelle ja johdattamaan seminaariin osallistujat ulko-ovelta seminaaritilaan. Mieti kulkureitti ja laadi tarvittavat opasteet. Laita opasteet paikalleen seminaaria edeltävänä päivänä. Mieti missä osallistujien rekisteröinti tapahtuu ja järjestele tarvittavat pöydät rekisteröintiä varten seminaaria edeltävänä päivänä.

SEMINAARIPÄIVÄNÄ:

Osallistujien rekisteröinti. Aakkosta nimikyltit ajoissa valmiiksi ja printtaa osallistujalista. Toivota osallistujat tervetulleeksi, merkitse listaan saapuneeksi ja jaa mahdollisesti ohjelma ja muu oheismateriaali.

Puhujien vastaanotto. Ole puhujia vastassa ja opasta mahdollisesti heille varatuille istumapaikoille.

Seminaarin vetäminen. Toivota osallistujat tervetulleeksi, esittele puhujat vuorollaan, vedä lopussa yhteenveto-/keskusteluosuus, kiitä osallistujia. Huolehdi päivän aikana, että ohjelma pysyy aikataulussa.

Tarjoilut. Tarkista ennen taukoja, että tarjoilut ovat valmiina. Pidä ravintola ajan tasalla, jos aikataluun tulee muutoksia.

SEMINAARIN JÄLKEEN:

Kerää palautetta osallistujilta. Laadi palautelomake ja laita linkki kiitosviestiin.

Kiitosviesti ja seminaariesitysten jako. Lähetä osallistujille kiitosviesti osallistumisesta, joka sisältää puhujien esitykset (joiden jakoon on saatu lupa) ja palautelomakelinkin.

Palkkioiden maksatus. Huolehdi puhujien mahdollisten palkkioiden maksusta sovitusti.

Palautteen käsittely. Käsittele saatu palaute ja kehitä seuraavan seminaarin sisältöä ja toteutusta palautteen perusteella.

TUTKINTOKOULUTUKSIEN KYBERTURVALLISUUTEEN LIITTYVÄT OSAT

Toimenpide 2.1 Jokainen oppilaitos tekee selvityksen omien tutkintokoulutusten kyberturvallisuuteen liittyvistä osista sekä mahdollisuudesta muokata niitä työelämäkoulutuksiksi. Oppilaitokset selvittävät omat kyberturvallisuuden soveltamiseen liittyvät erityisosaamisalueensa, jotka voivat vahvistaa ja tarjota verkoston käyttöön. TAMK kokoaan selvitykset yhteen kokonaiskuvan saamiseksi.

YHTEENVETO

Kukin oppilaitos teki koulutuksiaan koskevan selvityksen itsenäisesti. Niiden pohjalta on laadittu tämä yhteenveto.

Kyberturvallisuuteen liittyvät opintojaksot ovat pääsääntöisesti ICT-alan (tietotekniikka, tietojenkäsittely) opintoja jokaisessa oppilaitoksessa. Tämän lisäksi kyberturvallisuutta on mukana automaatiotekniikan, sote-alan, johtamisen, talotekniikan ja sähkötekniikan opinnoissa.

Varsinkin ICT-alan opinnoissa samoja aihealueita saatetaan käsitellä eri oppilaitoksissa erilaisilla opintojaksoilla/kokonaisuuksissa. Seuraavaan taulukkoon on koostettu olemassa olevat opintojaksot tiettyjen teemojen mukaisesti:

Teema	Opinto	Oppilaitos
Yleinen tietoturvaosaaminen, yksilötaso, perusteet, tietämys	Information Security	TurkuAMK
	Sosiaalinen media	TurkuAMK
	AV-aineiston tietoturva	TurkuAMK
	Tietoturva-arki	TTY
	Tietoturvan perusteet	TAMK
	Kyberturvallisuuden perusteet	TAMK
	Tietoturva	OY
	Computer Security	OY
Edistyneempi laaja kyberturvallisuusymmärrys, tietotekniikka, -verkot, teknisempi ”perustaso”	Kyberturvallisuus 1	TTY
	Tietoturvalliset järjestelmät	TAMK
	Johdatus kyberturvallisuuteen	TAMK
	Käyttöjärjestelmät	OY
	Tietoverkon perusteet	TurkuAMK
	Tietoliikenneverkot 1	OY
Tietosuoja, yksityisyydensuoja yms.	Data protection and Privacy	TurkuAMK
	Tietosuoja ja kyberturvallisuuteen liittyvä juridiikka	TAMK
Kyberturvallisuuteen liittyvä riskienhallinta, johtaminen	Information Security Risk Management	TurkuAMK
	Security Operations	TurkuAMK
	Information Security Management	TTY
Tietoverkkojen, palvelinten ja tiedonsiirron tekninen turvaaminen, havainnointi	Puolustava kyberturvallisuus	TurkuAMK
	Tietoverkkojen kyberturvallisuus	TurkuAMK
	Network Security	TurkuAMK
	Turvalliset tietoverkot	TAMK
	Kyberturvallisuustoiminnot	TAMK
	Verkkopalveluiden ja palvelinten kyberturvallisuus	TAMK
	Tietoverkkojen kyberturvallisuus	TAMK
	Network Security	TTY
Salaaminen, krypto, yms.	Email, vpn, TOR ja selaimet	TurkuAMK
	Cryptography Engineering	TTY
	Hyökkäävä kyberturvallisuus	TurkuAMK

Tunkeutumistestaaminen, haavoittuvuudet, ”hakkerointi”, web-palveluiden turvallisuus, yms.	Web Application Security	TurkuAMK
	Information Security Testing and Assessment	TurkuAMK
	Kyberturvallisuus 2	TTY
	Tunkeutumistestaus ja haavoittuvuuksien etsintä	TAMK
Sähkö-, automaatio- ja rakennustekniikkaan liittyvä kyberturvallisuusnäkökulma	Automaation turvallisuus	TTY
	Taloautomaatio, kiinteistöjen ohjausratkaisut, älykkäät sähköenergiajärjestelmät	TAMK
	Automaation tietotekniikka	Metropolia
	Kiinteistöjen tietotekniset järjestelmät	Metropolia
	Rakennusten automaatiojärjestelmät	Metropolia
Sosiaali- ja terveysalaan liittyvä kyberturvallisuusnäkökulma	Terveysalan turvallisuus	Metropolia
	Digitalisaatio ja toiminnan ohjaus sosiaali- ja terveysalalla	Metropolia
Turvallinen ohjelmistotuotanto	Turvallinen ohjelmointi	TTY
	Johdatus tietoturvalliseen ohjelmointiin	TAMK
	Ohjelmistotekniikka	OY
	Tietojärjestelmäsuunnittelun perusteet	OY
	Vaatimusmäärittely	OY
	Mobile Computing	OY
Laiteläheisyys, IoT ja pilviratkaisuiden kyberturvallisuus	Big Data Processing and Applications	OY
	Internet of Things	OY
	Cloud computing	OY
Muita	Identiteetin ja pääsynhallinta	TTY
	Kyberturvallisuus ja liiketoiminta	TurkuAMK
	Cryptology	TurkuAMK
	Distributed Systems	OY
	Real Time Distributed Software Development	OY
	Towards Data Mining	OY

YRITYSTEN OSAAMIS- JA KOULUTTAUTUMISTARPEET

Toimenpide 2.2 Jokainen oppilaitos selvittää oman verkostonsa yrityksiltä heidän osaamis- ja kouluttautumistarpeet. Tätä tarveselvitystä on jo aloitettu hankevalmistelun aikana.

SELVITYSTEN TEKEMINEN

Jokaisella paikkakunnalla yritysten osaamis- ja kouluttautumistarpeiden selvittäminen tehtiin itsenäisesti. Tampereen toimijat (TAMK ja TTY) tekivät yhden selvityksen ja muut omansa. Näiden yksityiskohtaisten selvitysten perusteella laadittiin tämä yhteenveto.

Jokainen toimija valitsi itse oman tapansa selvityksen tekemiseen. Tämä osoittautui jälkikäteen huonoksi ratkaisuksi, sillä selvitysten tuloksia ei voitu ”viedä yhteen” vaan niiden tulosten käsitteleminen yhtenäisenä tietona jäi suuntaa-antavaksi tulosten tulkinnaksi (ei voitu käyttää tilastollisia menetelmiä):

1. Turun ammattikorkeakoulu keräsi tiedot kaksivaiheisella kyselyllä, jossa ensin yrityksiltä tiedusteltiin alustavia ajatuksia varsinaisen kyselytutkimuksen pohjaksi. Kyselyyn vastasi 13 yritystä.
2. Metropolia ammattikorkeakoulussa selvitys tehtiin kyselytutkimuksella, johon tuli 32 vastausta.
3. Tampereella (TAMK+TTY) selvitys tehtiin kahdella tavalla. Työpajassa kerättiin yritysten näkemyksiä tarpeista ja kyselytutkimuksella haettiin määrällisiä vastauksia. Työpajaan osallistui 14 henkilöä ja kyselytutkimukseen saatiin vastaukset 26:lta yritykseltä.
4. Oulussa selvitys tehtiin haastattelemalla yritysten edustajia. Haastatteluihin halukkaiksi ilmoittautui 14 yritystä.

Tämän lisäksi osaamistarpeita selvitettiin tutustumalla aikaisempien tutkimusten/hankkeiden tuloksiin, käymällä läpi osaamistarpeeseen liittyviä selvityksiä, keräämällä kokemuksia alan tapahtumista sekä tekemällä asiantuntijahaastatteluja.

SELVITYSTEN TULOKSIA

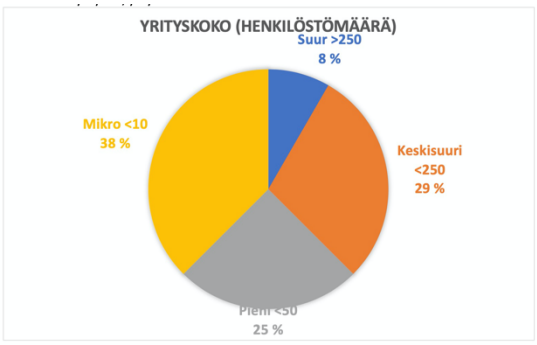
Kaikilla paikkakunnilla keskeinen selvitettävä asia oli, mitä sisältöjä tarjolle tulevissa työelämäkoulutuksissa tulisi olla. Tämän lisäksi Tampereella ja Metropoliassa selvitettiin, minkä tyyppisiä koulutusten tulisi olla.

Osaamistarpeista nousi selkeimmin esiin perustason kyberturvallisuusosaaminen – tietoturvan perusteet. Yrityksissä nähtiin laajaltikin tarve koko henkilöstön osaamistason nostamiseen. Tämän lisäksi esiintyi tarvetta johdon osaamisen kehittämiseen sekä tiettyjen toimialaosaamisten tarpeisiin sekä uusien teknologioiden (pilvi, mobiili, iot) mukanaan tuomaan osaamistarpeeseen. Sisällöllisesti osaamistarpeet kuitenkin hajaantuivat melko laajalle ja niistä oli haastavaa muodostaa kokonaisuuksia lukuun ottamatta perustason osaamistarvetta, joka esiintyi laajasti.

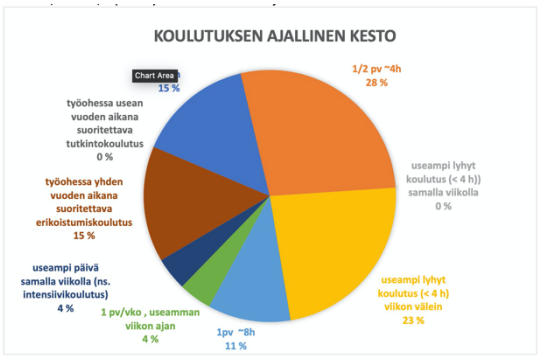
Yritykset toivoivat ennen kaikkea läsnäoloon ja kasvokkain kohtaamiseen perustuvia koulutuksia. Tämä nousi selvästi esiin. Itsenäisesti suoritettavia verkkokursseja ei pidetty kovin mielekkäinä eikä tehokkaina koulutusmuotoina. Tämän lisäksi nousi esiin käytännön läheinen koulutus, jossa päästään tekemään sekä myös harjoitustyyppinen koulutus. Yksittäisten koulutuskertojen pitäisi olla lyhyitä (muutamasta tunnista yhteen työpäivään) ja mahdollisimman lähellä (matkustusajan minimointi).

MUUTAMIA KAAVIOITA TAMPEREEN ALUEEN KARTOITUKSESTA

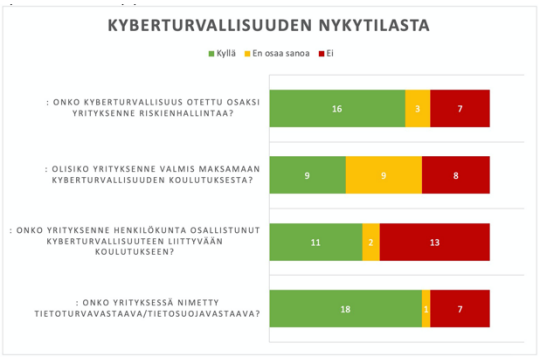
Osallistuneet yritykset, yrityskoko:



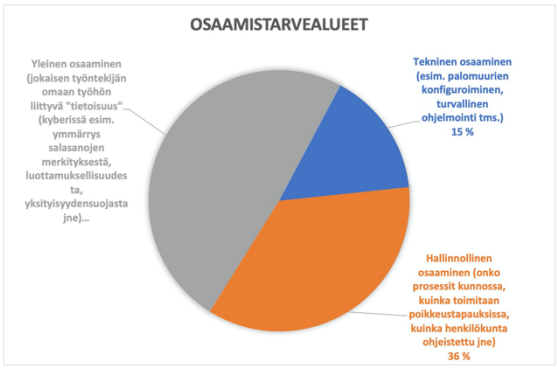
Toivotun/halutun/sopivan työelämäkoulutuksen ajallinen kesto:



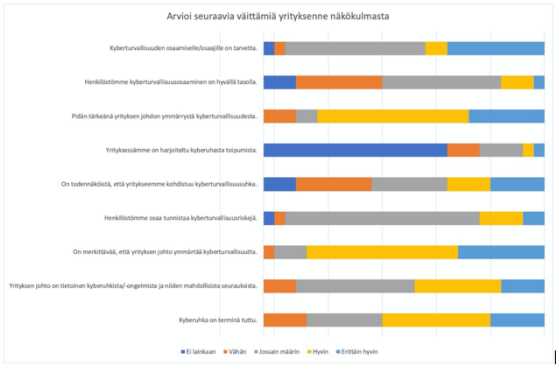
Kyberturvallisuuden nykytilanne:



Osaamis-/kouluttautumistarve:



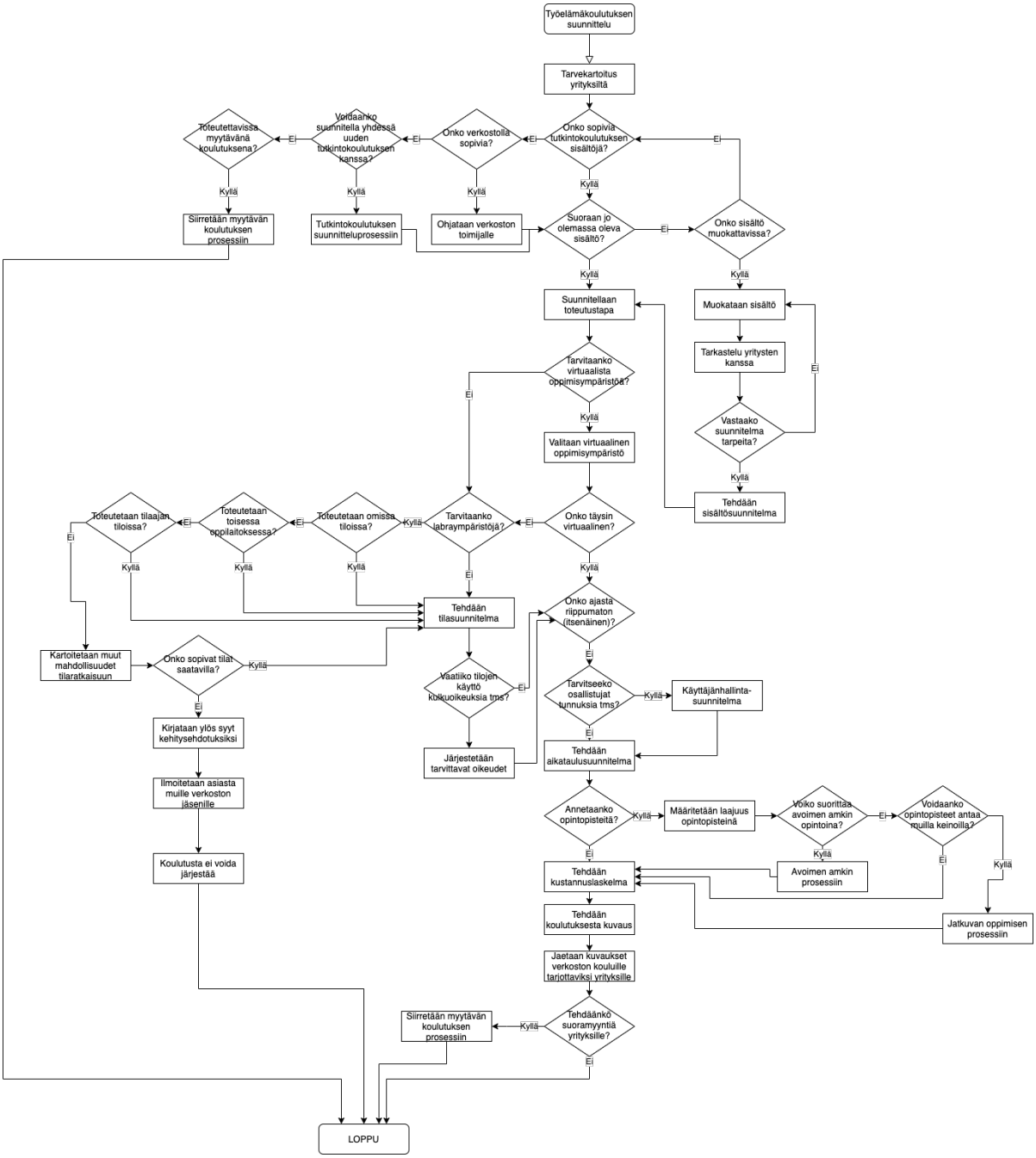
Vastauksia väittämiin. Huom. Yritykset eivät juurikaan ole harjoitelleet kyberuhkatilanteita!



TYÖELÄMÄKOULUTUKSEN SUUNNITTELU -PROSESSIKUVAUS

Toimenpide 2.3 Kokonaiskuvan pohjalta laaditaan suunnitelmat mitä ja miten tutkintokoulutusten osia muokataan työelämäkoulutuksiksi ja kuinka niitä tarjotaan hyödynnettäväksi oppilaitosten muodostaman verkoston kautta siellä, mistä osaamista tarvitsevia yrityksiä löytyy.

Työelämäkoulutusten suunnitteluprosessista laadittiin seuraava vuokaavio. Siinä on pyritty huomioimaan kaikki ne keskeiset tekijät, joita yhteistyöverkoston kanssa tarvitsee huomioida koulutusta suunniteltaessa. Kaaviota käytettiin hyväksi koulutuksien suunnittelussa.



ESIMERKKI PROSESSIKUVAUKSEN KÄYTÖSTÄ

Työelämäkoulutuksia suunniteltaessa hankkeessa laadittiin kaavio työelämäkoulutuksen suunnittelun prosessista. Alla kuvataan esimerkkinä yhden työelämäkoulutuksen (Tietosuojavaikutusten arviointi, TTY) suunnittelua prosessikaaviota soveltaen.

1 Tietosuojavaikutusten arviointi -työelämäkoulutus

Tietosuojavaikutusten arviointi -työelämäkoulutus on tarkoitettu organisaatioiden tietosuojasta vastaaville henkilöille, joilla on jo perustiedot EU:n tietosuoja-asetuksesta. Koulutuksen tavoitteena on antaa yrityksille perustiedot asetuksen edellyttämästä tietosuojavaikutusten arvioinnista ja siitä, milloin sen tekeminen on tarpeen organisaatiossa. Koulutuksessa käydään läpi tietosuojavaltuutetun ohjeita aiheesta, sekä tutustutaan eurooppalaiseen CNIL PIA -viitekehykseen, jonka perusteella arviointia voi tehdä. Koulutuksessa painottuu vaikutusten arvioinnin riskienhallinallinen luonne ja jatkuva prosessi.

2 Prosessikaavion käyttö Tietosuojavaikutusten arviointi -työelämäkoulutuksen suunnittelussa

Suunnitteluprosessi alkaa yritysten kanssa tehtävästä tarvekartoituksesta. Tampereella 23.11.2018 järjestetyn Yritysten kyberturvakoulutustarpeet -työpajan perusteella yrityksissä havaittiin tarvetta henkilötietojen suojaamiseen liittyvään koulutukseen. Lisäksi koulutuksilta toivottiin perustasoa sekä jatkotasoja tarpeen mukaan. Tämä koulutus voidaan ajatella jatkavana koulutuksena Metropolia AMK:n järjestämälle Tiedot suojassa ja saatavilla -työelämäkoulutukselle, jossa käsitellään GDPR:n perusteita.

Seuraavaksi työelämäkoulutuksen suunnitteluprosessissa selvitetään, onko olemassa sopivia tutkintokoulutuksen sisältöjä. Tietosuojavaikutusten arviointi -työelämäkoulutuksessa valmista sisältöä ei ole, mutta usealta tutkintokoulutuksen kurssilta ja opinnäytetöiden ohjaamisesta on löydettävissä tähän koulutukseen sopivaa aineistoa ja materiaalia. Näiden pohjalta prosessikaaviossa päädytään Muokataan sisältö -kohtaan. Tässä kohtaa koulukseen valitaan sopiva aineisto ja tehdään siihen tarvittavat täydennykset.

Seuraavaksi muokattua sisältöä olisi hyvä käydä läpi yritysten kanssa, jotta varmistetaan sisällön tarkoituksenmukaisuus yritysten näkökulmasta. Tarkastelu voitaisiin toteuttaa vastaavalla tavalla työpajana kuin TAISTO-harjoitus räätälöidään yritysten tarpeisiin. Tällä kertaa kuitenkin Tarkastelu yritysten kanssa -kohta jouduttiin jättämään koronakriisin ja kesälomakauden vuoksi pois. Tähän voidaan tarvittaessa palata myöhemmin myös koulutuksesta saadun palautteen kautta.

Koulutuksen sisältösuunnitelman tekemisen jälkeen siirrytään toteutustavan suunnitteluun. Tässä kohtaa huomioidaan esim. virtuaalisten oppimisympäristöjen ja laboratorioympäristöjen tarpeet. Tietosuojavaikutusten arviointi -työelämäkoulutuksella tällaisia tarpeita ei ole, joten siirrytään tilasuunnitelman tekemiseen. Tämä koulutus tarvitsee ainoastaan opetustilan, joka voi tarvittaessa sijaita myös yrityksen omassa tilassa.

Seuraavaksi kurssille laaditaan aikataulusuunnitelma ja pohditaan opintopisteisiin ja -hallintoon liittyvät asiat. Lopuksi laaditaan kustannuslaskelma ja suunnitellaan koulutuksen esitteet ja muuta markkinointia. Koulutuksen toteutuessa esimerkiksi Tampereen yliopistossa Jatkuvan oppimisen palvelut huolehtivat markkinoinnin ja kurssimaksujen käytännön järjestelyt.

--

HANKKEEN AIKANA SUUNNITELLUT TYÖELÄMÄKOULUTUKSET

Toimenpide 2.3 Kokonaiskuvan pohjalta laaditaan suunnitelmat mitä ja miten tutkintokoulutusten osia muokataan työelämäkoulutuksiksi ja kuinka niitä tarjotaan hyödynnettäväksi oppilaitosten muodostaman verkoston kautta siellä, mistä osaamista tarvitsevia yrityksiä löytyy.

Hankkeen aikana syntyi suunnitelmat useille työelämäkoulutuksille. Ne jaoteltiin toimenkuvittain ja niistä koostettiin erillinen dokumentti:

Kyberturvallisuuden

työelämäkoulutuksia

yritysten tarpeisiin

Euroopan unioni
Euroopan sosiaalirahasto

Vipuvoimaa EU:lta 2014–2020

Tampereen yliopisto
Tampereen ammattikorkeakoulu

Metropolia

TURKU AMK

OULUN YLIOPISTO

Työelämäkurssit räätälöidään sopiviksi työntekijöiden toimenkuvan mukaan:

TYÖNTEKIJÖILLE ja TOIMIHENKILÖILLE

KURSSI	KESTOAIKA
Johdatus kyberturvallisuuteen -verkkokurssi	3-4 työpäivää omaan tahtiin
Salasanojen hallintaohjelman käyttöönotto	4 tuntia
Tiedot suojassa ja saatavilla	4 työpäivää
Tietoturvallisuuden kehittäminen	1 työpäivä
Turvallinen liikkuva työ	4 työpäivää
Turvallinen verkkotyöskentely	4 työpäivää

YRITYSJOHDOLLE ja YRITTÄJILLE

KURSSI	KESTOAIKA
Johdatus kyberturvallisuuteen -verkkokurssi	3-4 työpäivää
Langaton häirintä, tahallinen vai tahaton?	4h – 2 työpäivää
Tietovuotouhkaharjoitus	1-2 työpäivää

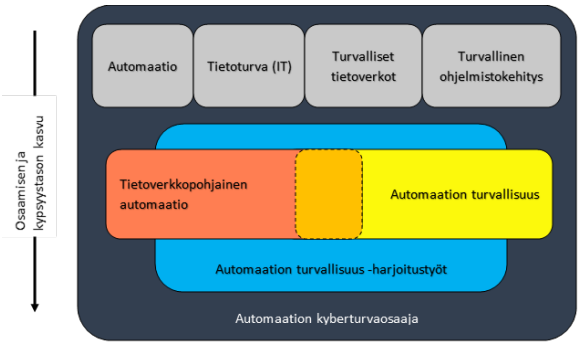
ICT-ASIANTUNTIJOILLE

KURSSI	KESTOAIKA
Blue Team -harjoitus	1-4 työpäivää
Digitaalisen forensiikan työpaja	1 työpäivä
Fuzz-testauksen työpaja	1 työpäivä
Haittaohjelmien staattinen ja dynaaminen analysointi	1 työpäivä
Kvantitatiivinen tietoriskien hallinta	1-2 työpäivää
Laitteistohaavoittuvuudet ja sivukanavahyökkäykset	1 työpäivä
Shellcoding-työpaja	1 työpäivä
Tunkeutumisenhavainnointijärjestelmä	1 työpäivä
Verkkoliikenteen analysointi -työpaja	1-3 työpäivää
Verkkosovellusten tietoturva -työpaja	1 työpäivä

MUILLE ASIANTUNTIJOILLE, YHDISTYKSILLE, YHTEISÖILLE, jne.

KURSSI	KESTOAIKA
Automaation tietoturva -kurssi	1 lukuvuosi
Automaation tietoturva -työpaja	2-3 työpäivää
Internetin käyttö rikostutkinnassa (viranomaisille)	4-5 työpäivää
Tietosuojavaikutusten arviointi -työpaja	1 työpäivä
Tietoturvapäivä	1 työpäivä

AUTOMAATION TIETOTURVA -KURSSI

Koulutuksen nimi	Automaation tietoturva
Kohderyhmä (+ennakko-osaaminen)	Automaation pariin kouluttautuvat sekä automaatioyritysten alihankkijat, tekniset ja kaupalliset henkilöt sekä sidosryhmät
Kestoaika	1 lukuvuosi
Toteutustapa	Luennot ja harjoitustyöt
Oppimisympäristö	DSACyberLab ja Moodle
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	Avoimen yliopiston kurssimaksu x2
Oppimistavoitteet	Yleistiedot ja perussanaston automaation tietoturvasta antavat kurssit. Opiskelija osaa toteuttaa yrityksen riskianalyysin tietoturvan ja toiminnallisen turvallisuuden osalta, ja ymmärtää, miten eri osa-alueet sitoutuvat toisiinsa. Hän myös osaa analysoida ja parantaa tehtyjä riskianalyysejä oppimansa pohjalta. Hän myös oppii ymmärtämään tietoturvan merkityksen automaation luotettavuudessa, ja IT-puolen tekniikoiden käytön asettamat haasteet automaation sovellusalueella.
Sisältö	 Koska automaatiotekniikan perusopetuksen toteutustapa ja ajallinen kesto eivät sovellu aina yritysmaailman tarpeisiin, on perusopetuksen sisällöstä tiivistetympi työpajaversio, jota voidaan myös muokata yrityksen tarpeiden mukaisesti. Tämä toteutustapoihin liittyvä havainto on myös yksi Kyberturvaaja-hankkeen tuloksista. Koulutuksen ytimenä toimii Automaation turvallisuus - ja Tietoverkkopohjainen automaatio -kurssit, jotka yhdessä muodostavat yhtenäisen kokonaisuuden automaation tietoturvasta. Kurssien yhteydessä pidettävät harjoitukset täydentävät tätä tietämystä.

	Kurssilla käsitellään mm. • Automaation turvallisuus kokonaisuutena, johon sisältyy riskianalyysi, tietoturva sekä toiminnallinen turvallisuus. • Automaatioon liittyvän yritystoiminnan turvallisuuteen liittyvät haasteet • Teollisuusautomaatioverkkojen tietoturva • Tietoturvaperusteet niin yksilön kuin yrityksen näkökulmasta • Erilaiset automaatiossa käytetyt verkkotekniikat ja -protokollat
Koulutuksen rakenne (aikataulu, jaksotus, yms)	2h viikossa + itsenäinen työ
Muita huomiota/vaatimuksia	Jotta kursseista saa kaiken hyödyn irti, tulisi kurssille tulevalla henkilöllä olla perustietämys automaatiosta ja tietoturvasta, sekä turvallisista tietoverkoista ja ohjelmistokehityksestä. Tämän tietämyksen voi hankkia automaatiotekniikan perusopinnoista sekä yhteistyöverkoston tarjoamista tietotekniikan ja tietoturvallisuuden kursseista.

AUTOMAATION TIETOTURVA -TYÖPAJA

Koulutuksen nimi	Automaation tietoturva -workshop
Kohderyhmä (+ennakko-osaaminen)	Automaation pariin kouluttautuvat sekä automaatioyritysten alihankkijat, tekniset ja kaupalliset henkilöt sekä sidosryhmät
Kestoaika	1,5 päivää /räätälöitävissä tarpeen mukaan
Toteutustapa	Luennot + hands-on työpaja
Oppimisympäristö	DSACyberLab ja erillinen julkaisujärjestelmä
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	Toteutustapa edellyttää toteutuskohtaista hinnoittelua, esimerkiksi opettajien matkakustannusten vuoksi
Oppimistavoitteet	Yleistiedot ja perussanaston automaation tietoturvasta antava kurssi. Opiskelija osaa toteuttaa yrityksen riskianalyysin tietoturvan ja toiminnallisen turvallisuuden osalta, ja ymmärtää, miten eri osa-alueet sitoutuvat toisiinsa. Hän myös osaa analysoida ja parantaa tehtyjä riskianalyysejä oppimansa pohjalta. Hän myös oppii ymmärtämään tietoturvan merkityksen automaation luotettavuudessa, ja IT-puolen tekniikoiden käytön asettamat haasteet automaation sovellusalueella.
Sisältö	Koulutuksen ytimenä toimii Automaation turvallisuus - ja Tietoverkkopohjainen automaatio -kurssit, jotka yhdessä muodostavat yhtenäisen kokonaisuuden automaation tietoturvasta. Kurssin hands-on -osuus täydentää tätä tietämystä. Kurssilla mm. • Käsitellään automaation turvallisuus kokonaisuutena, johon sisältyy riskianalyysi, tietoturva sekä toiminnallinen turvallisuus. • Käydään läpi yritystoiminnan turvallisuuteen liittyvät haasteet • Opetellaan keräämään verkosta ja järjestelmistä tietoa ja ymmärtämään mikä on kerätyn tiedon merkitys osana hyökkäyksiä • Annetaan ymmärrys, miten tietoturvatyökaluja voidaan käyttää luotettavan automaation aikaan- saamiseksi
Koulutuksen rakenne (aikataulu, jaksotus, yms.)	Tapauskohtainen, yleensä 2 peräkkäistä päivää + 2h etänä suoritettava ennakkotapaaminen
Muita huomiota/vaatimuksia	Jotta kursseista saa kaiken hyödyn irti, tulisi kurssille tulevalla henkilöllä olla perustietämys automaatiosta ja tietoturvasta, sekä turvallisista tietoverkoista ja ohjelmistokehityksestä. Tämän tietämyksen voi hankkia automaatiotekniikan perusopinnoista sekä yhteistyöverkoston tarjoamista tietotekniikan kursseista. Tämän toteutuksen sisällössä pyritään vähentämään esitietovaatimusten tarvetta.

BLUE TEAM -HARJOITUS

Koulutuksen nimi	Blue Team Exercise
Kohderyhmä (+ennakko-osaaminen)	IT-ylläpitotiimi (palvelin-, verkko- ja sovellusylläpidon perusteet)
Kestoaika	8h (valinnaisesti 16-32h ennakkotehtävä)
Toteutustapa	Laboratorioharjoitus / etätyöskentely
Toteutuskieli	suomi, englanti
Hinta (tai kustannusten määräytyminen)	määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutus parantaa organisaation ylläpitotiimin kykyä reagoida yhteistyössä tietoturvapoikkeamiin. Ennakkotehtävä valmentaa tiimiä IT-ympäristön tietoturvaongelmien havaitsemiseen ja korjaamiseen. Koulutuksessa keskitytään kunkin tiimiläisen erityisosaamisen tehokkaaseen hyödyntämiseen.
Sisältö	Tietoturvapoikkeamien havaitseminen SIEM-järjestelmällä Poikkeamiin reagointi Palautuminen Viestintä poikkeustilanteessa Valinnaisesti ennakkotehtävänä IT-ympäristön haavoittuvuusanalyysi ja puutteiden korjaaminen Valinnaisesti ennakkotehtävänä SIEM-järjestelmän asennus, konfigurointi ja käyttöönotto
Suunnitelma (tunti tms. sopivalla tasolla kuvattuna)	Harjoitus • ympäristöön tutustuminen(1h) • briefing (30 min) • harjoitus virtuaaliympäristössä (5h) • debriefing (1h) Ennakkotehtävät • etäyhteyksien muodostaminen (30 min) • haavoittuvuusanalyysin perusteet (1,5h) • haavoittuvuusanalyysi ja puutteiden korjaaminen (14h) • SIEM perusteet (1h) • SIEM asennus ja konfigurointi (2 * 2h) • SIEM käyttöönotto (11h)
Muita huomiota/vaatimuksia	Koulutusympäristöä on mahdollista räätälöidä yrityksen tarpeiden mukaan Koulutus on mahdollista järjestää verkkokoulutuksena
Toteuttava taho	Turun ammattikorkeakoulu

DIGITAALISEN FORENSIIKAN TYÖPAJA

Koulutuksen nimi	Digitaalisen forensiikan työpaja
Kohderyhmä (+ennakko-osaaminen)	Yrityksen tekninen henkilöstö. Vaatimuksina perusymmärrys tietokoneiden ja käyttöjärjestelmien toi minnasta sekä prosessien ja muistin hallinnasta.
Kestoaika	Yksi työpäivä
Toteutustapa	Työpaja
Oppimisympäristö	Opetustila, GitHub
Toteutuskieli	Suomi/englanti
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutuksen jälkeen osallistuja • tuntee digitaalisen forensiikan keskeisen terminologian • tietää kuinka käyttöjärjestelmä hallinnoi prosesseja ja muistia • osaa käsitellä muistivedoksia forensiikkatyökaluja käyttäen • osaa tutkia tiedostojen heksadumppeja
Sisältö	Työpaja: teoriatausta, tietokonearkkitehtuuri, tiedostojärjestelmät, muistivedokset
Koulutuksen rakenne (aikataulu, jaksotus, yms)	9-16
Muita huomiota/vaatimuksia	Harjoitus suoritetaan käyttäen annettua virtuaalikonetta (Kali Linux)
Toteuttava taho	Oulun yliopisto

FUZZ-TESTAUKSEN TYÖPAJA

Koulutuksen nimi	Haavoittuvuuksien löytäminen fuzz-testauksella
Kohderyhmä (+ennakko-osaaminen)	Yrityksen tekninen henkilöstö, vaatimuksina perustaidot ohjelmoinnista ja Unix/Linux-järjestelmien käytöstä
Kestoaika	Yksi työpäivä
Toteutustapa	Työpaja
Oppimisympäristö	Opetustila, GitHub
Toteutuskieli	Suomi/englanti
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutuksen jälkeen osallistuja • tuntee fuzz-testauksen keskeisen terminologian • ohjelmistojen muistinsuojelun periaatteet • ymmärtää sekä perusteet että syventäviä teemoja ohjelmistovirheiden ja haavoittuvuuksien löytämisestä fuzz-testauksella • hallitsee fuzz-testaustyökalujen käytön
Sisältö	Työpaja: terminologia, haavoittuvuuksien löytäminen, testaustyökalut, avoimen lähdekoodin ja omien ohjelmistojen fuzz-testaus
Koulutuksen rakenne (aikataulu, jaksotus, yms)	9-16
Muita huomiota/vaatimuksia	Työpaja suoritetaan käyttäen annettua virtuaalikonetta (Kali Linux). Mahdollista suorittaa myös itsenäisesti verkon välityksellä ilman koulutt ajaa.
Toteuttava taho	Oulun yliopisto

HAITTAOHJELMIEN STAATTINEN JA DYNAAMINEN ANALYSOINTI

Koulutuksen nimi	Haittaohjelmien staattinen ja dynaaminen analysointi
Kohderyhmä (+ennakko-osaaminen)	Yrityksen tekninen henkilöstö. Vaatimuksena perusymmärrys tietokoneiden ja käyttöjärjestelmien toiminnasta sekä prosessien ja muistin hallinnasta
Kestoaika	Yksi työpäivä
Toteutustapa	Työpaja
Oppimisympäristö	Koulutustila (mahdollista myös verkossa)
Toteutuskieli	suomi/englanti
Hinta (tai kustannusten määräytyminen)	määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutuksen jälkeen osallistuja tuntee perusteet ● ohjelmistojen takaisinmallinnuksesta (reverse engineering) ● haittaohjelmien dynaamisesta ja staattisesta analysoinnista
Sisältö	Työpaja: staattinen ja dynaaminen haittaohjelma-analyysi, ohjelmien takaisinmallinnus (reverse engineering)
Koulutuksen rakenne (aikataulu, jaksotus, yms)	9-16
Muita huomiota/vaatimuksia	Työpajassa käytetään annettua virtuaalikonetta (Ubuntu)
Toteuttava taho	Oulun yliopisto

INTERNETIN KÄYTTÖ RIKOSTUTKINNASSA (VIRANOMAISILLE)

Koulutuksen nimi	Internetin käyttö rikostutkinnassa
Kohderyhmä (+ennakko-osaaminen)	Viranomaiset
Kestoaika	32h
Toteutustapa	Lähiopetus
Toteutuskieli	suomi, englanti
Hinta (tai kustannusten määräytymin en)	määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutuksen tavoitteena on parantaa avoimista lähteistä saatavaa tiedonhankintaa, joka koskee rikoksista epäiltyjä henkilöitä. Tarkoituksena on selvittää ennaltaehkäisevästi miten rikolliset pystyvät välittämään tietoa toisilleen eri järjestelmien kautta ja miten näitä järjestelmiä on mahdollisuus päästä tutkimaan.
Sisältö	• IP-liikenteen ja yleisimpien protokollien perusteet • sähköpostiliikenne • sähköpostiviestien otsaketiedot • menetelmiä verkkoliikenteen piilottamiseen • selaimen käyttö tiedonkeruussa • selaimeen ja käyttöjärjestelmään tallentuvat tiedot • tiedon louhinta sosiaalisesta mediasta • salattu viestintä sosiaalisessa mediassa ja muissa palveluissa • kuvatiedostojen tarkastelu • videoiden ja kuvien tallentaminen
Suunnitelma (tunti tms. sopivalla tasolla kuvattuna)	• IP-verkot 6h • Sähköpostin välitys ja viestien tulkinta 2h • verkkoliikenteen piilottaminen 6h • tiedon kerääminen selaimella ja selaimesta 2h • tiedon louhinta ja viestintä sosiaalisessa mediassa 8h • kuvatiedostojen ja videoiden käsittely 8h
Muita huomiota/vaatimuksia	Koulutus on mahdollista räätälöidä organisaation tarpeiden mukaan.
Toteuttava taho	Turun ammattikorkeakoulu

JOHDATUS KYBERTURVALLISUUTEEN -VERKKOKURSSI

Koulutuksen nimi	TIEY4 Kyberturvallisuus
Kohderyhmä (+ennakko-osaaminen)	yrityksen koko henkilöstö
Kestoaika	noin 27 työtuntia, kurssin voi käydä haluamaansa tahtiin, esim. viikon aikana 3-4 tuntia kerrallaan
Toteutustapa	verkkokurssi
Hinta (tai kustannusten määräytyminen)	avoin amk
Tavoite	Yleistiedot ja perussanaston kyberturvallisuudesta antava kurssi. Kurssin pohjalta voi jatkaa opiskelua vaativammille kursseille. Sopii myös yrityksissä henkilöille, joiden vastuulla kyberturvallisuus ei suoraan ole. Kurssi pyrkii antamaan tiedot, jotka kaikkien olisi hyvä tietää kyberturvallisuudesta.
Sisältö	Johdatus kyberturvallisuuteen, kyber-sanasto Kurssi käsittelee kyberturvallisuutta kolmesta näkökulmasta: yhteiskunta, yritystoiminta, yksilö Sisältönä tekstiä, lisätietolinkkejä, pelejä ja tehtäviä
Suunnitelma (tunti tms. sopivalla tasolla kuvattuna)	Kurssin voi suorittaa esim. tähän tahtiin (mutta oma mukautus on mahdollista): 1 päivä: Yleiset asiat + johdanto 2-3 päivä: Yhteiskunnan näkökulma 4-5 päivä: Yritystoiminnan näkökulma 6-7 päivä: Yksilön näkökulma 8 päivä: tentti
Muita huomiota/vaatimuksia	
Järjestävä taho	Tampereen korkeakouluyhteisö

KVANTITATIIVINEN TIETORISKIEN HALLINTA

Koulutuksen nimi	Kvantitatiivinen tietoriskien hallinta
Kohderyhmä (+ennakko-osaaminen)	Tietohallinto
Kestoaika	8h + etätehtävät
Toteutustapa	työpaja
Toteutuskieli	suomi, englanti
Hinta (tai kustannusten määräytyminen)	määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutettava osaa organisaation tietoriskien tunnistamisen, mittaamisen ja hallinnan.
Sisältö	• ISO 27005 • Tietoriskien tunnistaminen • Tietoriskien mittaaminen • Factor Analysis in Information Risk (FAIR) -menetelmä • Tietoriskien käsittely
Suunnitelma (tunti tms. sopivalla tasolla kuvattuna)	• Ennakkomateriaaliin tutustuminen (etätehtävä) • Mittaaminen ja FAIR-menetelmä (4h) • Tietoriskiprojekti (etätehtävä) • Projektin purku ja tietoriskien käsittely (4h)
Muita huomiota/vaatimuksia	
Toteuttava taho	Turun ammattikorkeakoulu

LAITTEISTOHAAVOITTUVUUDET JA SIVUKANAVAHYÖKKÄYKSET

Koulutuksen nimi	Laitteistohaavoittuvuudet ja sivukanavahyökkäykset
Kohderyhmä (+ennakko-osaaminen)	Yrityksen tekninen henkilöstö. Vaatimuksena perustaidot Assemblysta.
Kestoaika	Yksi työpäivä
Toteutustapa	Työpaja
Oppimisympäristö	Koulutustila
Toteutuskieli	suomi/englanti
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutuksen jälkeen osallistuja ● tuntee eri sivukanavahyökkäystyyppejä ● tuntee sivukanavahaavoittuvuuksien havaitsemisen perusperiaatteet
Sisältö	Työpaja: sivukanavahyökkäykset ja -haavoittuvuudet
Koulutuksen rakenne (aikataulu, jaksotus, yms)	9-16
Muita huomiota/vaatimuksia	Työpajassa käytetään annettua virtuaalikonetta (Ubuntu Linux) ja testauslaitetta (ChipWhisperer).
Toteuttava taho	Oulun yliopisto

LANGATON HÄIRINTÄ, TAHALLINEN VAI TAHATON?

Koulutuksen nimi	Langaton häirintä, tahaton vai tahallinen
Kohderyhmä (+ennakko-osaaminen)	Yrityksen johdolle/päättäville tahoille, tietosuojasta vastaaville henkilöille, toimihenkilöt ja työntekijät
Kestoaika	Puoli päivää – kaksi työpäivä (räätälöitävissä tapauskohtaisesti)
Toteutustapa	Työpaja + käytännön mittauksia ja demoja tietoliikennelaboratoriossa (sovitaan tapauskohtaisesti)
Oppimisympäristö	Opetustila ja tietoliikennelaboratorio (+häiriösuojattu tila)
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutuksen suoritettuaan osallistuja: • Ymmärtää lisensoitujen ja lisensoimattomien taajuusalueiden merkityksen. • Ymmärtää langattoman tietoliikenne-järjestelmän perustoiminnan (Lähetin/vastaanotin/radiokanava) • Ymmärtää langattoman tietoliikennejärjestelmän toimintaperiaatteen (tukiasema, päätelaite, keskus). • Ymmärtää sähkömagneettista yhteensopivuutta (EMC) koskevia määräyksiä • Kykenee ymmärtämään häiriötilanteen vaikutuksen • Kykenee toimimaan häiriö/häirintä tilanteessa • Tuntee tilanteessa tarvittavan viranomaiskäytännön
Sisältö	*TEORIAOSUUS* Radiotaajuudet ja radiokanava Lähetin, vastaanotin Tukiasema/radiomasto, päätelaite, keskus EMC, Sähkömagneettinen yhteensopivuus *LABORATORIOTYÖSKENTELY* Radiomittauksia (vastaanotin/lähetin) Häiriömittauksia
Koulutuksen rakenne (aikataulu, jaksotus, yms)	9-16
Muita huomiota/vaatimuksia	
Toteuttava taho	Tampereen ammattikorkeakoulu

SALASANOJEN HALLINTAOHJELMAN KÄYTTÖÖNOTTO

Koulutuksen nimi	Salasanamanagerin käyttöönotto
Kohderyhmä (+ennakko-osaaminen)	Koko henkilöstö
Kestoaika	4 tuntia
Toteutustapa	Ohjattu opetustapahtuma
Oppimisympäristö	Osallistuja tarvitsee oman tietokoneen, kannettavan tai tabletin, jonne voi asentaa ohjelmia
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutukseen osallistuja tietää salasanoihin liittyvät uhkat, tunnistaa hyvät salasanojen hallintatavat ja käytänteet, on ottanut käyttöön salasanojenhallintaohjelmiston ja kykenee sitä käyttämään.
Sisältö	Salasanojen merkitys kyberturvallisuudessa Hyvät salasanojen käytänteet Salasanamanageri-ohjelmisto, sen käyttöönotto ja käyttö
Koulutuksen rakenne (aikataulu, jaksotus, yms)	4 tuntia ohjattu työskentelyä ja demonstraatioita
Muita huomiota/vaatimuksia	Osallistujilla pitää olla omat laitteet
Toteuttava taho	Tampereen ammattikorkeakoulu

SHELLCODING-TYÖPAJA

Koulutuksen nimi	Shellcoding-työpaja
Kohderyhmä (+ennakko-osaaminen)	Yrityksen tekninen henkilöstö. Vaatimuksena perustaidot ohjelmoinnista, ohjemistojen muistinhallinnasta ja *nix-järjestelmien käytöstä.
Kestoaika	Yksi työpäivä
Toteutustapa	Työpaja
Oppimisympäristö	Koulutustila (toteutus mahdollista myös verkossa)
Toteutuskieli	suomi/englanti
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutuksen jälkeen osallistuja ● osaa tunnistaa ylivuotovirhetilanteita ● tuntee perusteet ohjelmistohaavoittuvuuksien käyttämisestä oman koodin suorittamiseen
Sisältö	Työpaja: ylivuotovirheiden analysointi ja hyödyntäminen, ret2libc ja ROP
Koulutuksen rakenne (aikataulu, jaksotus, yms)	9-16
Muita huomiota/vaatimuksia	Työpajassa käytetään annettua virtuaalikonetta (Kali Linux)
Toteuttava taho	Oulun yliopisto

TIEDOT SUOJASSA JA SAATAVILLA

Koulutuksen nimi	Tiedot suojassa ja saatavilla
Kohderyhmä (+ennakko-osaaminen)	Toimihenkilöt ja työntekijät
Kestoaika	Noin 32 työtuntia, kurssin voi käydä haluamaansa tahtiin, esim. viikon aikana 3-4 tuntia kerrallaan ja työpajaan osallistuminen
Toteutustapa	Räätälöidyt työpajat ja verkkomateriaali
Hinta (tai kustannusten määräytyminen)	Määrätytyy tapauskohtaisesti
Tavoite	Koulutuksen suoritettuaan osallistuja tuntee tietosuojalainsäädännön perusteet, tietää tietojen suojaamismenetelmien perusteet ja osaa suojata työssään tarvitsemansa tiedot
Sisältö	GDPR:n perusteet Tietojen tallentaminen ja suojaaminen Vaatimustenmukaisuus ja lainsäädäntöä
Suunnitelma (tunti tms. sopivalla tasolla kuvattuna)	Kurssin voi suorittaa esim. tähän tahtiin (mutta oma mukautus on mahdollista): 1 päivä: GDPR:n perusteet 2 päivä: Tietojen tallentaminen ja suojaaminen 3 päivä: Vaatimustenmukaisuus ja lainsäädäntö 4 päivä: Työpaja Metropoliassa
Muita huomiota/vaatimuksia	
Järjestävä taho	Metropolia

TIETOSUOJAVAIKUTUSTEN ARVIOINTI -TYÖPAJA

Koulutuksen nimi	Tietosuojavaikutusten arviointi
Kohderyhmä (+ennakko-osaaminen)	Yrityksen tietosuojasta vastaavat henkilöt
Kestoaika	Yksi työpäivä
Toteutustapa	Työpaja
Oppimisympäristö	Opetustila ja Internet-yhteys
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti, perusteena pääsääntöisesti todelliset kustannukset, mahdollinen koulutukseen kohdistuva tuki vähentää kustannuksia
Oppimistavoitteet	Koulutuksen suoritettuaan osallistuja: • Tietää, mikä tietosuojavaikutusten arviointi on ja milloin se on tarpeen tehdä • Tuntee tietosuojavaltuutetun ohjeistuksen vaikutusten arviointiin • Tuntee muutamia eurooppalaisia viitekehyksiä, joiden pohjalta vaikutusten arviointia voi täydentää ja räätälöidä yrityksen tilanteeseen • Ymmärtää vaikutusten arvioinnin hyödyt, vaikutusten arvioinnin osana yrityksen riskienhallintaa, ja miten siitä tehdään jatkuva prosessi
Sisältö	• Tietosuojavaikutusten arviointi, mikä se on ja missä tilanteessa tarvitaan • Tietosuojavaikutusten arviointi osana riskienhallintaa • Tietosuojavaltuutetun ohjeet vaikutusten arviointiin • Eurooppalaiset viitekehykset, tarkemmin ranskalainen CNIL PIA –viitekehys (tarkoituksenmukaisuus, lainmukaisuus, minimointi, täsmällisyys, säilytysajat, kontrollien arviointi, rekisteröidyn oikeuksien arviointi, riskit) • Esimerkki CNIL PIA -viitekehyksen soveltamisesta • Mitä vaikutusten arviointi voisi tarkoittaa omassa yrityksessä, keskustelu- ja pohdintaosuus
Koulutuksen rakenne (aikataulu, jaksotus, yms)	9-16
Muita huomiota/vaatimuksia	Osallistujilla tulisi olla perustiedot GDPR:stä
Järjestävä taho	Tampereen yliopisto

TIETOTURVALLISUUDEN KEHITTÄMINEN

Koulutuksen nimi	Tietoturvallisuuden kehittäminen
Kohderyhmä (+ennakko-osaaminen)	toimihenkilöt
Kestoaika	8h
Toteutustapa	työpaja
Toteutuskieli	suomi, englanti
Hinta (tai kustannusten määräytyminen)	määräytyy tapauskohtaisesti
Oppimistavoitteet	Kurssin suoritettuaan oppija tuntee tietoturvan peruskäsitteet ja on tietoinen tietoturvaan ja tietosuojaan liittyvästä lainsäädännöstä Suomessa ja EU:ssa. Oppija ymmärtää organisaation tietoturvapolitiikan merkityksen tietoturvan johtamisessa.
Sisältö	Peruskäsitteistö Suomen ja EU:n lainsäädäntö (miten vaikuttaa organisaation toimintaan käytännössä) Tietoturvapolitiikka ja sen koulutus Tietoturvan johtaminen
Suunnitelma (tunti tms. sopivalla tasolla kuvattuna)	Työpajat aiheittain á 2h • Käsitteet ja niiden liittäminen organisaatioon • EU lainsäädäntö • Suomen lainsäädäntö • Tietoturvapolitiikka, koulutuksen suunnittelu ja tietoturvan johtamistavat
Muita huomiota/vaatimuksia	
Toteuttava taho	Turun ammattikorkeakoulu

TIETOTURVAPÄIVÄ

Koulutuksen nimi	Tietoturvapäivä
Kohderyhmä (+ennakko-osaaminen)	Pienten yritysten ja yhdistysten henkilöstö
Kestoaika	1 päivä
Toteutustapa	Ryhmätyöskentelyä ja oppimiskeskusteluja asiantuntijavetoisesti
Oppimisympäristö	-
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	järjestelykustannukset
Oppimistavoitteet	Parantaa osallistujen tietämystä ajankohtaisista kyberturallisuuteen liittyvistä aiheista ja uhkista.
Sisältö	Sisältö räätälöidään tarkemmin tapauskohtaisesti seuraavien aihealueiden pohjalta • tietosuoja/-murtoharjoitus • kyberturvallisuuden ajankohtaiset asiat • jonkin teknisemmän ratkaisun (esim. salasanamanageri, etäyhteydet, ...) käyttöönotto
Koulutuksen rakenne (aikataulu, jaksotus, yms)	Yhden päivän kestävä asiantuntijan vetämä tilaisuus
Muita huomiota/vaatimuksia	
Toteuttava taho	Tampereen ammattikorkeakoulu

TIETOVUOTOUHKAHARJOITUS

Koulutuksen nimi	Tietovuotouhka -harjoitus
Kohderyhmä (+ennakko-osaaminen)	Koko henkilöstö, sopivasti valikoitu yrityskohtainen ryhmä
Kestoaika	1 päivä
Toteutustapa	Fasilitoitu harjoitus
Oppimisympäristö	Voidaan järjestää ilman erillistä ympäristöä, osallistujat tarvitsevat tietokoneita ja internet-yhteydet
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	järjestelykustannukset
Oppimistavoitteet	Osallistuja saa kokemusta kyberturvallisuuteen liittyvästä harjoitustoiminnasta. Harjoitus keskittyy osallistujayrityksen omien prosessien läpikäyntiin kuvitteelliseen tietovuototapaukseen liittyen.
Sisältö	Fasilitoidusti etenevä kuvitteellinen tietovuototapahtuma
Koulutuksen rakenne (aikataulu, jaksotus, yms)	1 työpäivä
Muita huomiota/vaatimuksia	Koulutuksessa hyödynnetään Väestörekisterikeskuksen julkishallinnon organisaatioille toteuttamisen TAISTO-harjoitusten materiaaleja räätälöiden ne kohdeyrityksiin sopiviksi.
Toteuttava taho	Tampereen korkeakouluyhteisö, Metropolia

TUNKEUTUMISENHAVAINNOINTIJÄRJESTELMÄ

Koulutuksen nimi	Tunkeutumisenhavainnointijärjestelmä
Kohderyhmä (+ennakko-osaaminen)	Yritysten ict-henkilöstö
Kestoaika	1 päivä
Toteutustapa	Laboratoriatyöskentelyä
Oppimisympäristö	TAMKin kyberlabra (tai vastaava ympristö)
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutukseen osallistuvat tietävät kuinka verkkoon tunkeutuminen (haitallinen liikenne) voidaan havainnointijärjestelmällä tunnistaa, osaavat ottaa käyttöön havainnointijärjestelmät ja kykenevät tulkitsemaan sen tekemiä havaintoja
Sisältö	Koulutus perustuu SecurityOnion-järjestelmään: • mitä on tunkeutumisen havainnointi? • kuinka ids-järjestelmä toimii • SO:n käyttöönotto • SO:n eri ohjelmat ja niiden käyttö • SO:n säätäminen tarpeisiin soveltuvalla tavalla
Koulutuksen rakenne (aikataulu, jaksotus, yms)	Koulutus on lähiopetuksessa tapahtuvaa laboratoriotyöskentelyä.
Muita huomiota/vaatimuksia	
Toteuttava taho	Tampereen ammattikorkeakoulu

TURVALLINEN LIIKKUVA TYÖ

Koulutuksen nimi	Turvallinen liikuva työ
Kohderyhmä (+ennakko-osaaminen)	Toimihenkilöt ja työntekijät
Kestoaika	Noin 32 työtuntia, kurssin voi käydä haluamaansa tahtiin, esim. viikon aikana 3-4 tuntia kerrallaan ja työpajaan osallistuminen
Toteutustapa	Räätälöity työpaja ja verkkomateriaali
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti
Tavoite	Koulutuksen suoritettuaan osallistuja tietää liikkuvan työn periaatteet, tietojen suojaamisen perusteet ja osaa työskennellä turvallisesti etätyöympäristössä
Sisältö	Etätyöskentely Liikkuvan työn tietoturva Mobiililaitteiden suojaaminen
Suunnitelma (tunti tms. sopivalla tasolla kuvattuna)	Kurssin voi suorittaa esim. tähän tahtiin (mutta oma mukautus on mahdollista): 1 päivä: Etätyöskentelyn perusteet 2 päivä: Liikkuvan työn tietoturva 3 päivä: Mobiililaitteiden suojaaminen 4 päivä: Työpaja Metropoliassa
Muita huomiota/vaatimuksia	
Järjestävä taho	Metropolia

TURVALLINEN VERKKOTYÖSKENTELY

Koulutuksen nimi	Turvallinen verkkotyöskentely
Kohderyhmä (+ennakko-osaaminen)	Toimihenkilöt ja työntekijät
Kestoaika	Noin 32 työtuntia, kurssin voi käydä haluamaansa tahtiin, esim. viikon aikana 3-4 tuntia kerrallaan ja työpajaan osallistuminen
Toteutustapa	Räätälöity työpaja ja verkkomateriaali
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti
Tavoite	Koulutuksen suoritettuaan osallistuja osaa turvallisen verkkotyöskentelyn periaatteet, tietää tavallisimmat verkkotyöskentelyn riskit ja niiltä suojautumisen
Sisältö	Työskentely verkossa Verkkoturvallisuuden perusteet Turvalliset työskentelytavat
Suunnitelma (tunti tms. sopivalla tasolla kuvattuna)	Kurssin voi suorittaa esim. tähän tahtiin (mutta oma mukautus on mahdollista): 1 päivä: Tietoverkkotekniikan perusteet 2 päivä: Verkkoturvallisuuden perusteet 3 päivä: Turvalliset työskentelytavat 4 päivä: Työpaja Metropoliassa
Muita huomiota/vaatimuksia	
Järjestävä taho	Metropolia

VERKKOLIIKENTEEN ANALYSOINTI -TYÖPAJA

Koulutuksen nimi	Verkkoliikenteen analysointi
Kohderyhmä (+ennakko-osaaminen)	Yritysten ict-henkilöstö ja verkosta vastuussa olevat tahot
Kestoaika	1-3 päivää, räätälöitävissä sisältöjen mukaan
Toteutustapa	Laboratoriatyöskentelyä
Oppimisympäristö	TAMKin kyberlabra
Toteutuskieli	Suomi
Hinta (tai kustannusten määräytyminen)	määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutus antaa organisaation verkosta vastaavalle henkilöstölle osaamista verkkoliikenteen kaappaamisen ja analysoinnin keinoihin ja mahdollisten kyberuhkien havainnointiin verkkoliikennettä seuraamalla.
Sisältö	Sisältö räätälöidään laajuuden mukaan seuraavista osa-alueista: • Verkkoliikenteen kaappaaminen • Pakettien syväanalysointi (DPI) • Flow-liikenne ja sen tuomat analysoinnin mahdollisuudet • Tunkeutumisenhavainnoinjärjestelmän käyttö
Koulutuksen rakenne (aikataulu, jaksotus, yms)	Koulutus on lähiopetuksessa tapahtuvaa laboratoriotyöskentelyä ja sisältää myös itsenäisesti tehtäviä case-tyyppisiä analysointitehtäviä.
Muita huomiota/vaatimuksia	
Toteuttava taho	Tampereen ammattikorkeakoulu

VERKKOSOVELLUSTEN TIETOTURVA -TYÖPAJA

Koulutuksen nimi	Verkkosovellusten tietoturva (työpaja)
Kohderyhmä (+ennakko-osaaminen)	Yrityksen tekninen henkilöstö
Kestoaika	9-16
Toteutustapa	Työpaja
Oppimisympäristö	Opetustila, verkko
Toteutuskieli	suomi/englanti
Hinta (tai kustannusten määräytyminen)	Määräytyy tapauskohtaisesti
Oppimistavoitteet	Koulutuksen jälkeen osallistuja ● tuntee yleisimmät verkkohyökkäystyypit ● osaa käyttää verkkosovellusten testaustyökaluja omien ohjelmistojen testauksessa
Sisältö	Työpaja: yleisimmät web-haavoittuvuudet, testaustyökalut, verkkosovellusten testaus
Koulutuksen rakenne (aikataulu, jakso tus, yms)	9-16
Muita huomiota/vaatimuksia	Työpajassa käytetään annettua virtuaalikonetta (Kali Linux). Mahdollista suorittaa myös itsenäisesti verkon välityksellä ilman kouluttajaa.
Toteuttava taho	Oulun yliopisto

SELVITYS IOTTI-HANKKEEN TULOSTEN HYÖDYNNETTÄVYYDESTÄ

KYBERTURVAAJAHANKE JA IoTTi -selvitys

IoTTi-hankkeen raportti löytyy seuraavasta linkistä: https://iotti-hanke.fi/wordpress/wp-content/uploads/2019/05/yhteistoimintamalli.pdf

Selvityksessä on aluksi kerrottu IoTTi-hankkeen yhteydessä kehitetyn yhteistoimintamallin mukainen prosessi. Prosessin tuloksia on seuraavaksi verrattu kyberturvaajahankkeeseen. Huomiot, miten eri hankkeissa toimenpiteet ja käytänteet poikkeavat toisistaan, on erikseen mainittu. Muussa tapauksessa IoTTi-hankkeessa suunniteltua verkostomaista yhteistoimintamallia voidaan käyttää sellaisenaan.

IoTTi –YHTEISTOIMINTAMALLI

YLEISKUVAUS JA RAKENNE

IoTTi hankkeen yhteistoimintamallin (YTM) mukaan järjestävä ammattikorkeakoulu (AMK) vastaanottaa tarjouspyynnön koulutusta tarvitsevalta taholta. Tarjottavan koulutuksen sisällöstä ja toteutuksesta on vastuussa järjestävä ammattikorkeakoulu. Tarjouksen tekemiseen tarvitaan tietoja toisten ammattikorkeakoulujen opintojaksoista (IoTTI mallissa IOT-opintojaksoista) koulutusohjelmatasolla. Mallissa käytetään toisista ammattikorkeakouluista termiä Toteuttava AMK. Tarjouksen tekemiseksi tietoja täydennetään opettaja- ja kurssikohtaisilla resurssitiedoilla.(Lähde: https://iotti-hanke.fi/yhteistoimintamalli/)

https://iotti-hanke.fi/wordpress/wp-content/uploads/2019/03/verkostomallin_rakennekuva.png

Soveltuvuus Kyberturvaajahankkeeseen:

Malli on sovellettavissa myös kyberturvaaja hankkeessa toteutettuihin koulutuksiin seuraavilla lisähuomioilla:

5. Koulutuksen järjestävänä tahona voi toimia myös yliopisto.
6. Koulutuksen tarjoajat muodostavat yli AMK-rajoista muodostava toimijaverkosto, sillä mukana on myös Tampereen ja Oulun yliopistot.
7. TAMK on omalta osaltaan mukana Tampereen yliopistoyhteistyössä, joten ohjeistus yliopiston sisällä muovautuu ajan mittaan samankaltaiseksi.

KOULUTUSTARPEET

IoTTI hankkeessa IoT-järjestelmien koulutustarpeet voidaan jaotella kehittämiseen, liiketoimintamahdollisuuksiin ja järjestelmien käyttäjien koulutuksiin. Osa koulutuksesta sisältyy jo nyt ammattikorkeakoulujen koulutusohjelmiin, mutta IoT-verkoston toimijat voivat täydentää tarjontaansa toisten ammattikorkeakoulujen tarjoamilla sisällöillä.

Soveltuvuus Kyberturvaajahankkeeseen:

Kyberturvaajahankkeen koulutustarpeet sisältyvät samoin jo olemassa oleviin koulutusohjelmiin ja opintojaksoihin. Koulutusta tarjoava verkosto koostuu IoTTI-verkostoa laajemmasta yhteisöstä. Näin koulutustarjonta ja yhteistyö voidaan katsoa laajemmaksi. Muutoin koulutus ja sen tarjonta ovat rinnastettavissa toisiinsa molemmissa hankkeissa.

KOULUTUKSEN SUUNNITTELU

Yhteisen koulutuksen suunnittelua ja toteuttaminen IoTTi-verkostossa vaatii muiden ammattikorkeakoulujen koulutustarjonnan tuntemista. Ensivaiheessa tarjontaan tutustuminen tehdään tutkimalla toisen ammattikorkeakoulujen opetussuunnitelmia opintojaksotasolla. Tietoja voidaan sen jälkeen täydentää henkilökohtaisilla kontakteilla, joiden avulla syntyy tarkempi käsitys opintojakson sisällöstä.

Verkostomaisen koulutusmallin avuksi voidaan luoda tietovarasto, johon tiedot tallennetaan. Opintojaksojen tiedot kerätään niiltä opettavilta oppilaitokselta yhteyshenkilöiden avulla osaamisrekisteriin. Heidän vastuullaan on myös tietojen päivittäminen.

8. toteuttava ammattikorkeakoulu
9. osaamiskuvaus
10. opintojakson nimi
11. opetuksen kesto
12. opetuksen laajuus opintoviikkoina tai tunteina
13. opetustavat ja työmenetelmät
14. tarvittavat resurssit / teknologiat, erityisesti tarvittavat lisenssit
15. mihin tutkintokoulutuksen kurssiin osaaminen sisältyy
16. hinta-arvio (kustannukset)
17. opetuksen yhteystiedot

Järjestävä ammattikorkeakoulu voi käyttää esimerkiksi osaamisrekisterin tietoja tarjouksen tekemiseen asiakkaalle.

Soveltuvuus Kyberturvaajahankkeeseen :

Kyberturvaajahankkeessa tarjottava koulutus on suunniteltu jo hankkeen yhteydessä valmiiksi, toteutuskelpoisiksi kokonaisuuksiksi. Näin koulutustarjonnan ei tarvitse lähteä eri oppilaitosten koulutustarjonnan tuntemisesta, samassa mittakaavassa kuin IoTTi-hankkeessa. Tosin kaikkia tulevaisuudessa tarjottavia mahdollisia koulutuksia ei voida etukäteen suunnitella, vaan ne tulevat tapauskohtaisesti, yleensä yrityskentästä. Näin kyberturvaajahankkeen yhteistyöverkoston aktiivinen yhteistyö mahdollistaa reagoinnin nopeisiin koulutustarjontakyselyihin.

Kyberturvaajahankeen osalta voidaan hyödyntää IoTTi-mallin osaamisrekisteriä. Nopea tilanteiden muuttuminen, mm, henkilöiden vaihtuvuus, tuo haasteen osaamisrekisterin ylläpitoon. Siksi kyberturvaajahanke peräänkuuluttaa toimivan verkoston olemassaoloa. Näin tieto muiden oppilaitosten koulutustarjonnasta saadaan nopeasti muiden tietoisuuteen.

Kyberturvaajahankkeessa toteuttavana tahona voi toimia myös yliopisto. Osaamiskuvaukset, opintojakson nimet ja kesto sekä laajuus noudattavat vakiintunutta tapaa molemmissa hankkeissa.

Kyberturvaajahankkeen suunnittelemat koulutukset ovat pääasiassa lyhytkestoisia, jolloin puhutaan muutaman tunnin kestoisista koulutuksista. Kyberturvaajahankkeen suunniteltu koulutustarjonta on tehty yrityselämästä saatujen selvitysten pohjalta.

Kyberturvahankkeessa suunnitellut koulutukset vaativat, ainakin jatkossa, verkkoympäristön, missä erilaisia uhkatilanteita voidaan harjoitella turvallisesti.

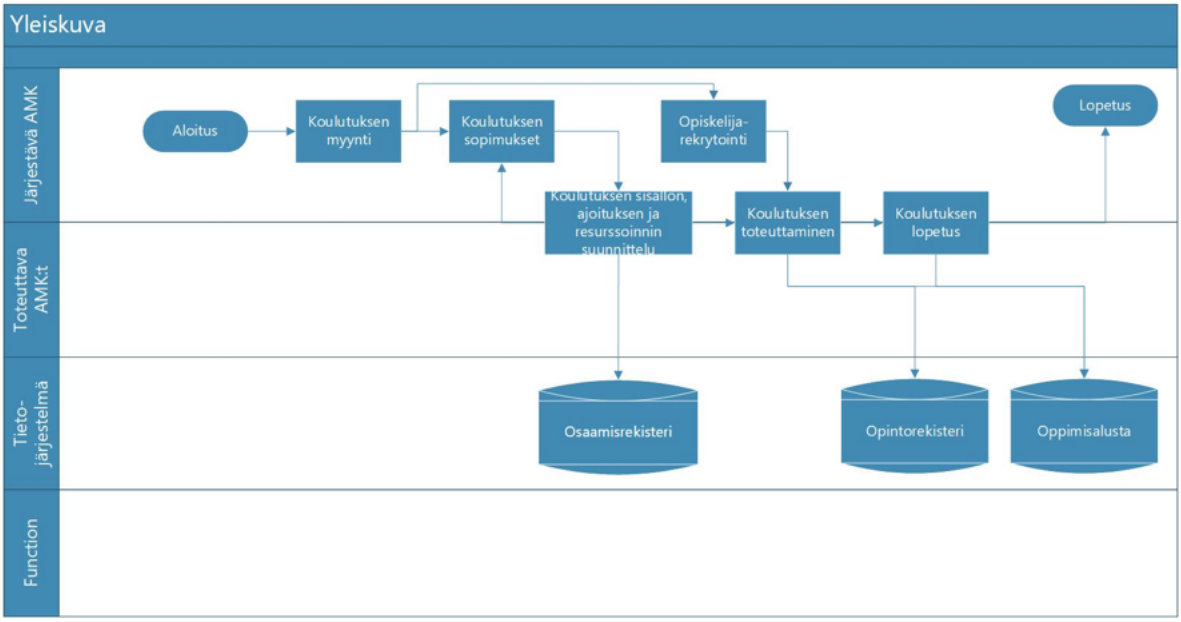
Kyberturvaahankkeessa kehitettyjen koulutusten kesto on yleensä lyhyt. Tällöin kustannustehokaan koulutuksen järjestäminen tiedostetaan haasteeksi. Opettajien liikkuminen eri paikkakunnille, erilaiset vuosisuunnittelumenetelmät ja sitä kautta resursointi, pitäisi pystyä suunnittelemaan joustavaksi.

KOULUTUKSEN JÄRJESTÄMINEN

IoTTi hankkeen mukaisessa mallissa koulutusta järjestävä ammattikorkeakoulu markkinoi toteuttamaansa IOT-koulutusta. Koulutuksesta tehdään sopimus ja aloitetaan opiskelijahankinta jos se on koulutuksen järjestäjän vastuulla. Koulutuksen sisältö suunnitellaan sopimuksen mukaiseksi hyödyntäen muiden ammattikorkeakoulujen resursseja. Siinä huomioidaan kouluttaja-, tila-, ohjelmisto- ja opiskelijaresurssien saatavuus. Niistä laaditaan aikataulu toteutusta varten. Toteutuksen päättyä arvioidaan mahdollisesti opiskelijoiden osaamista ja kirjataan tiedot suorituksista. Koulutuksen lopputulosta arvioidaan yhdessä tilaajan kanssa.

Koulutuksen järjestämisen prosessi on seuraava: (Lähde: Lähde: https://iotti-hanke.fi/yhteistoimintamalli/

18. Myynti
19. Sopimus
20. Opiskelijarekrytointi
21. Opetuksen suunnittelu
22. Toteutus
23. Päätöstoimenpiteet



Soveltuvuus Kyberturvaajahankkeeseen:

IoTTi yhteistoimintamallin soveltamisohje soveltuu kyberturvaajahankkeen yhteistoimintaan:

1. Tarjousvaihe, osa 1
    - Asiakkaalla on tarve IoT-aiheiseen koulutukseen TAI IoT-koulutus suunnitellaan AMKssa tarjolle TAI aloite koulutukseen tulee koulutusviranomaiselta (esim. OKM)
    - Mikäli tarve tulee ulkoiselta asiakkaalta asiakas toimittaa verkoston järjestävään AMKiin tarjouspyynnön.
2. Verkoston tarjoamat palvelut
    - Tarjousta varten koulutusverkoston osaamisrekisterin (spesifioitu IoTTi-hankkeessa) avulla selvitetään mitä osaamisia koulutukseen voitaisiin tarjota järjestävän AMKin

ulkopuolelta (jostain toteuttavasta AMK:sta). Vaiheessa hyödynnetään myös eri AMKien opintojaksotarjontaa.
    - Koulutuksen laajuuden on oltava riittävän iso jotta verkoston käyttämisestä koituu lisäarvoa. Neljän tunnin koulutusta ei kannata tilata vieras-AMKsta.
    - Järjestävä AMK ja verkostosta poimitut AMKit laativat yhdessä asiakkaalle tarjouksen. Tässä kohden on huomioitava kaikkien osallistuvien AMKin hinnoitteluperiaatteet, tarvittavien opettajien saatavuus, laboratoriojärjestelyt, opetusteknologiat jne.
3. Tarjousvaihe, osa 2
    - Vaiheen 2. selvitysten perusteella laaditaan asiakkaalle varsinainen tarjous sisältäen mm. seuraavat asiat: koulutuksen sisältö, ajankohdat, opettajat ja käytössä oleva koulutusverkosto, opetus- ja laboratorioteknologiat, osallistujat, muut järjestelyt (arvioinnit, palaute, todistukset jne.), koulutuksen hinta. Tarjouksen sisältö on spesifioitu IoTTi-hankkeessa.
    - Tässä vaiheessa tehdään alustavat sopimukset järjestäjäAMKin ja toteuttajaAMKien välillä yhteisen koulutuksen järjestämisestä. Sopimuksen sisältö on IoTTi-hankkeen sopimusmallin mukainen.
4. Sopimus
    - Mikäli asiakas hyväksyy edellisessa vaiheessa tehdyn tarjouksen ja tilaa koulutuksen käynnistyy koulutusprosessi. Järjestävä AMK tilaa osakoulutukset toteuttaja-AMKeilta ja pitää mahdollisesti osan koulutuksesta itse.
    - Järjestävän AMKin ja toteuttavien AMKien välillä tehdään koulutussopimukset, joilla kaikki osapuolet sitoutetaan koulutuksen järjestämiseen. Sopimuksesta selviää yhteiset asiat: koulutuksen sisältö ja erityisesti toteuttavan AMKin vastuut siinä, eri AMKien roolit tässä, koulutuksen hinta ja jakautuminen eri AMKeille, eri AMKien vastuut ja toimenpiteet jos niitä ei hoideta jne.
5. Koulutuksen toteuttaminen
    - Asiakkaalle toteutetaan aiottu koulutus tarjouksen, tilauksen ja verkoston toimijoiden välisten sopimusten asettamissa raameissa.
    - Koulutuksen osat sisällytetään ao. opettajien työaikasuunnitelmiin.
    - Koulutuksen ollessa iso se ja sen osat hallinnoidaan järjestävän AMKin opetuksen hallinnointijärjestelmällä (esim. peppi); pienet koulutukset hallinnoidaan toimisto-ohjelmistoilla.
    - Isojen koulutuksen osalta noudatamme opetuksen hallinnointijärjestelmän työnkulkuja: koulutus perustetaan järjestelmään osineen päivineen, oppilaat ilmoittautuvat koulutukseen ja sen osiin, oppilaat hyväksytään koulutukseen, opetus pidetään annettujen raamien ja sopimusten mukaan ja oppilaiden osaaminen arvioidaan ko. järjestelmään. Pienten asiakaslähtöisten koulutusten osalta prosessi on paljon keveämpi; yritys ilmoittaa henkilöstönsä koulutukseen, koulutus pidetään ja osallistujat saavat siitä todistuksen.
6. Lopputoimenpiteet
    - Isojen koulutusten osalta opintosuoritukset arvioidaan; pienten osalta osallistujat saavat osallistumistodistuksen.
    - Koulutuksesta kerätään palaute, jota käytetään kun kehitetään uutta vastaavaa koulutusta.
    - Osallistujille kirjoitetaan todistukset.
    - Koulutuksen tiedot arkistoidaan kahden vuoden ajaksi.

SELVITYS KYBERTURVALLISUUDEN ERIKOISTUMISKOULUTUSTEN SYNERGIAEDUISTA

Toimenpide 2.5 Tehdään selvitys, mitä synergiaetuja kyberturvallisuuden erikoistumiskoulutusten toimijoiden asiantuntijuuksissa sekä teknisissä ympäristöissä voidaan yhteistyöllä saavuttaa.

TIIVISTELMÄ TULOKSISTA

Selvitysten perusteella tultiin seuraaviin tuloksiin:

- Koulutusten järjestämistavoissa on merkittäviä eroja
- Erot luovat hyvin suuria reunaehtoja merkittävän yhteistoiminnan aikaansaamiselle
- Synergiaetuja voidaan saada pienillä toimilla jonkin verran reunaehtojen puitteissa mutta ei varsinaisesti koulutusten toteuttamisissa vaan muissa koulutuksiin liittyvissä asioissa, mm. teknisten ympäristöjen yhteiskäyttö on yksi tällainen asia
- Koulutus on määritelty 2015 ja se kaipaisi uudistamista
- Olisi hyvä, jos erikoistumiskoulutuksen koordinointivastuu olisi taholla, joka aikoo koulutusta tulevaisuudessa järjestää ja omaa siten intressit sen kehittämiselle

Alla vielä yksityiskohtaisempi analyysi Kyberturvallisuuden erikoistumiskoulutuksista TAMKissa, Metropoliassa ja TurkuAMKissa.

KYBERTURVALLISUUDEN ERIKOISTUMISKOULUTUKSET

Yleistä

Kyberturvallisuuden erikoistumiskoulutus ICT-alan on valtakunnallisesti erikseen sovittu ylemmän ammattikorkeakoulututkinnon tasoinen 30 opintopisteen laajuinen koulutus. Koulutuksen koordinoiva taho on XAMK. Tälle hetkellä koulutusta järjestää kolme ammattikorkeakoulua: TAMK, Metropolia ja TurkuAMK. Koulutuksen julkinen kuvaus:

https://wiki.eduuni.fi/display/csckshj/Julkinen+luettelo+-+ammattikorkeakoulut

Lyhyet kuvaukset koulutuksista

TAMK:

- Koulutus on alkanut vuonna 2020 3. kerran, tulevaisuuden toteuttamisista ei päätöksiä vielä (mahdollisesti joka toinen vuosi)
- Sisäänotto 20 opiskelijaa (täysi ryhmä 2020)
- Opiskelijamaksu 1800€ (alv 0%)
- Tehty oma opintosuunnitelma, jossa valtakunnallisen sopimuksen osaamistavoitealueita käsitellään eri opintojaksoilla “ristiin” (https://opinto-opas-ops.tamk.fi/index.php/fi/123163/fi/133542/20KYBE/year/2019)
- Toteutetaan kalenterivuoden mukaisesti tammikuusta joulukuulle. Monimuoto-opiskelua, jossa lähipäiviä on joka toisen viikon torstai-illat sekä perjantait

METROPOLIA:

- Koulutus on toteutettu vuodesta 2016 lähtien
- Sisäänotto vuosittain 24 opiskelijaa
- Opiskelijamaksu 450€ (alv 0%)

- Opintosuunnitelma seuraa valtakunnallisen sopimuksen opintosuunnitelmaa
- Toteutetaan lukuvuosittain monimuoto-opintoina, iltaopetusta 1-2 kertaa viikossa koko lukuvuoden ajan

TURKUAMK:

- 3. Koulutuksen piti alkaa 9.3.2020, mutta hakijapulan vuoksi aloitusta siirrettiin. Koulutus on järjestetty n. 1,5 vuoden välein.
- Sisäänotto 20 opiskelijaa
- Opiskelijamaksu 2100€ (alv 0%)
- Opintosuunnitelma noudattaa sopimuksen osaamistavoitealueita, joitakin osaamistavoitteita on siirretty opintojaksojen välillä. https://opinto-opas.TurkuAMK.fi/index.php/fi/21645/fi/22991/EKYBERS18/year/2018
- Toteutetaan monimuoto-opiskeluna, lähiopetus kerran kuussa maanantaina ja tiistaina 9-16. Yhteensä 18 lähipäivää.

YHTEISTYÖMAHDOLLISUUKSIA

Mahdollisina yhteistyönä saavutettavissa olevina synergiaetuina toimijat tunnistivat mm. seuraavat kohdat:

- Laadun paraneminen
- Uudistuminen – useita näkökulmia
- Teknisten ympäristöjen kehittäminen, ongelmatilanteista selviäminen

Koulutuksen laatutasoa voidaan parantaa jakamalla asiantuntijuuksia, suunnitelmia ja materiaaleja. Näin myös laatutasoa on mahdollista pitää yhdenmukaisena.

Kyberturvallisuuden erikoistumiskoulutuksen sopimus on tehty vuonna 2015 ja kokonaisuus suunniteltu ennen sitä. Koska ala on nopeasti muuttavaa ja osaamistarpeet muuttuvat jatkuvasti, on koulutusta uudistettava lähivuosina. Tässä uudistyössä koulujen välisellä yhteistyöllä voidaan saavuttaa huomattavia etuja.

Koulutukseen liittyy tarve käytä monenlaisia teknisiä ympäristöjä. Oppilaitoksilla on omia ympäristöjä ja ne hankkivat opetukseen soveltuvia ympäristöjä kaupallisilta toimijoilta. Sekä omien ympäristöjen ylläpidossa että ulkopuolelta hankituissa palveluissa saavutetaan synergiaetuja jo sillä, että jaetaan toimijodien välillä avoimesti tietoa hyviksi havaituista käytänteistä. Myös yhteiskäyttöä voidaan vielä kehittää mm. Hyödyntämällä toisten oppilaitosten ympäristöjä (reunaehdot huomioiden).

HAASTEITA YHTEISTYÖLLE

Toimijoiden kesken tunnistetiin lukuisi haasteita yhteistyölle. Osa haasteista on jo hankkeen aikana saatu ratkaistua ja osa on sellaisia, joiden tiedostamisella on arvoa ja se auttaa yhteistyömahdollisuuksien lisäämiseen. Tällaisia haasteita ovat mm.

- Erisuuruiset osallistumismaksut
- Ajoitus (milloin koulutus alkaa ja päättyy)
- Aikataulu ja lähipäivät (toteutusmuotoerot -> illassa/päivässä, mikä viikonpäivä)
- Erot opintosuunnitelmien soveltamisessa
- Hallinnoidaan eri tavoin eri oppilaitoksissa
- Ympäristöjen yhteiskäytön vaatimukset – resurssit, lisenssit, ylläpito, kustannukset
- Valtakunnallisen sopimuksen koordinointi ja opintosuunnitelman uudistus

Yksi suurimmista haasteista on koulutuksen uudistamisen tarve sekä valtakunnallinen koordinointi. Tällä hetkellä koordinointivastuu on XAMKilla, joka ei itse järjestä koulutusta. Hankkeen toimijoilla on yhteinen näkemys siitä, että koordinointivastuu olisi hyvä olla taholla, joka koulutusta järjestää ja näin kokee omaksi intressiksi sitä myös kehittää ja uudistaa. Koordinointivastuun siirtämisestä on käynnissä selvitystyö yhteistyössä XAMKin kanssa.

YHTEISTYÖMAHDOLLISUUKSIA ASIANTUNTIJUUKSISSA

Asiantuntijuuksien suhteen yhteistyötä voidaan tehdä monella tavalla mutta niihin liittyy myös hyvin suuria haasteita.

- Asiantuntijaluennot
    - Vierailijat (mahdolliset luennot jaetttuna verkon kautta)
    - Koulujen asiantuntijat ostopalveluna?
- Yhteistyötä oppimateriaalien tuotannossa ja jaossa
- Opintosuunnitelman uudistaminen
- Ideoidenvaihto

Selkein yhteistyömahdollisuus löytyy ideoidenvaihdon tehostamisesta. Tämän lisäksi hyvin merkittävänä pidettäisiin mahdollisuutta uudistaa koulutusta yhteistyönä.

YHTEISTYÖMAHDOLLISUUKSIA TEKNISISSÄ YMPÄRISTÖISSÄ

Kouluilla on monenlaisia ympäristöjä, joihin liittyy hyvin erilaisia toimintatapoja. Toimintatapojen erot vaikuttavat yhteistyömahdollisuuksiin sekä myös mm. lisenssiehdot. Hanketoimijoilla on kuitenkin näkemys, ettei samanlaisia ympäristöjä kannata täysin rakentaa vaan yhteistyöllä voidaan saavuttaa kaikille paremmat toimintaedellytykset. Ympäristöihin liittyvä työ on kuitenkin merkittävää jokaiselle, sillä työn kautta luodaan pohja toiminnalle ja saadaan sellaista kokemusta, jota ei saa käyttämällä vastaavia täysin ulkoisina (tai toiselta toimijalta saaduilla) palveluina. Yhteistyö tällä saralla toimii parhaiten ympäristöjen kehittämisestä, käytöstä, hankinnasta ja ylläpidosta saadun tiedon jakamisessa.

- Liittyy toimenpiteeseen teknisten ympäristöjen käytöstä
- TurkuAMKin kyberympäristön mahdollinen hyödyntäminen muiden toimesta
    - Tamk-TurkuAMK tekee kokeilun keväällä 2020
- Ympäristöjen hankinta ja kehitys – tietojenvaihto

SELVITYKSET TYÖELÄMÄKOULUTUSTEN VAIKUTUKSESTA OPINTOHALLINTOON JA TIETOJÄRJESTELMIIN

Jokainen oppilaitos teki oman selvityksen tietojärjestelmistä ja opintohallinnollisista asioista, jotka työelämäkoulutusten järjestämisessä tulisi huomioida.

METROPOLIA AMMATTIKORKEAKOULU

Selvitys Metropoliassa käytössä olevista opintohallinto- ja tietojärjestelmistä

Metropolian täydennyskoulutus- ja yrityspalveluiden sekä jatkuvan oppimisen (muut oppimisratkaisut) palveluiden toteuttamiin koulutuksiin ja tapahtumiin käytetään asiakkuuksien hallintaan ja koulutuksien hallinnoimiseen pääasiassa kolmeatietojärjestelmää:

1. CRM-asiakkuudenhallintajärjestelmää,
2. Lyyti-tapahtumanhallintajärjestelmää ja
3. Metropolian Peppi/OMA-tietojärjestelmää.

1 Asiakkuuksien hallinta (CRM)

Asiakkuuksien hallintatapahtuu CRM asiakkuudenhallintajärjestelmässä. CRM-järjestelmässä on tiedot asiakasroolista, lähetetyistä tarjouksista, tehdyistä sopimuksista ja toimeksiannoista sekä asiakastapaamisista ja yhteistyöstä.

2 Ilmoittautuminen koulutuksiin (Lyyti)

Koulutuksiin tai tapahtumiin ilmoittaudutaan ensisijaisesti tapahtumahallintajärjestelmässä Lyyti tai tarvittaessa vielä elomake-ohjelmistossa (elomakkeesta tiedot siirretäänosallistujatietojen hallinnoimiseksi Exceliin). Lyyti-palvelu on verkkopohjainen tapahtumanhallintajärjestelmä. Lyytiä käytetäänkoulutuksiin ilmoittautumisessa ja osallistujatietojen hallinnassa (osallistujatietojen keräys,käsittely ja jalostus hyötykäyttöön) ja koulutusten seurannassa (palautekyselyt, raportit,tietojen analysointi).

3 Koulutus on opintopisteytetty (Peppi/OMA-tietojärjestelmä)

Jos osallistuja saa koulutuksen suorittamisesta opintopisteitä, niin osallistujien ja koulutuksen tiedot tallennetaan Lyytistä Peppi-tietojärjestelmään, jota Metropoliassakutsutaan OMAksi. Tiedot muodostavat osan Metropolian opiskelijarekisteriä ja lain mukaantiedot säilytetään pysyvästi (laki valtakunnallisista opinto- ja tutkintorekistereistä 884/2017). Jos koulutuksesta ei saa opintopisteitä, tietoja ei siirretä Peppi/OMA-tietojärjestelmään.

Peppi-tietojärjestelmä on käytössä useassa korkeakoulussa ja siihen on tulossa tulevaisuudessa ristiinopiskelu-toiminnallisuus. Metropolian tiedonhallinta- ja järjestelmäpalveluilta 20.5. saadun tiedon mukaan kehittämisprojektin puitteissakokonaisuus olisi valmis arviolta vuoden 2020 lopussa. Sen jälkeen varsinainenkäyttöönotto riippuu 1) testauksesta, 2) mitä ristiinopiskeluprosessiin liittyviä päätöksiä jalinjauksia on tehty ja 3) minkälaisia ristiinopiskelusopimuksia tehdään korkeakoulujen välillä.Tulevaisuudessa saattaa olla mahdollista hyödyntää Pepin ristiinopiskelutoiminnallisuuttamyös verkostomaisesti toteuttavissa työelämäkoulutuksissa.

4 Henkilötietojen keräys ja säilytys

Henkilötiedot saadaan pääsääntöisesti rekisteröidyltä itseltään koulutuksiinilmoittautumisen yhteydessä. Joissakin tapauksissa koulutusta ostava työnantajayrityssaattaa välittää listan työntekijöistään Metropolialle ja pyytää ilmoittamaan heidät osallistujiksi johonkin yrityksen/organisaation työntekijöilleen kustantamaan koulutukseen.

Henkilötietoja säilytetään järjestelmissä seuraavasti:

24. Opintopisteytetyt opintosuoritukset säilytetään opintorekisterissä (Peppi/OMA)pysyvästi. Opintopisteellisiä opintosuorituksia säätelee laki valtakunnallisista opinto-ja tutkintorekistereistä (884/2017).
25. Muut henkilötiedot säilytetään rekisterissä asiakkuussuhteen ajan ja kaksi vuotta senpäättymisen jälkeen.

5 Verkostomaisesti toteutettavien työelämäkoulutusten hallinnointi

Verkostomaisesti toteutettavien työelämäkoulutuksien toteuttamisessa kannattaa hyödyntää yllä olevia tietojärjestelmiä ja täydennyskoulutus- ja yrityspalveluissa sekä jatkuvan oppimisen palveluissa laadittuja prosesseja soveltuvin osin. Verkostomaisesti toteutettavien työelämäkoulutusten hallinnoinnissa ja prosesseissa tulee ottaa huomioon verkostomainen toteutustapa, esim. yhteisen tietosuojaselosteen luomisessa ja mahdollisuuksien mukaan hyödyntää tietojärjestelmiä, jotka ovat käytössä useassa korkeakoulussa, kuten Lyytiä.

Metropolian tietosuojaselosteet löytyvät Metropolian internetsivuilta:https://www.metropolia.fi/fi/metropoliasta/tietosuoja-ja-gdpr/tietosuojaselosteet

Tietosuojaselosteet perustuvat EU:n tietosuoja-asetuksen (2016/679, General DataProtection Regulation, ”GDPR”) rekisteröityjen informointivelvoitteeseen (GDPR:n artiklat12-14), GDPR:n artiklan 30 mukaiseen rekisterinpitäjän velvoitteeseen ylläpitää selostettavastuullaan olevista käsittelytoimista sekä GDPR:ää täydentävän kansallisen tietosuojalain(1050/2018) velvoitteisiin. Täydennyskoulutus- ja yrityspalveluiden sekä jatkuvan oppimisen palveluidenhenkilörekisterin tietosuojaselostetta voi hyödyntää soveltuvin osin laadittaessa tietosuojaselostetta verkostomaisesti toteuttavista työelämäkoulutuksista. Henkilörekisterivoi myös olla yhteisrekisteri muiden organisaatioiden kanssa, jolloin laaditaan yhteistyössä yhteinen tietosuojaseloste.

OULUN YLIOPISTO

Oulun yliopistolla on käytössä kaksi koulutusten erityyppisiin toteutuksiin soveltuvaa tietojärjestelmää: WebropolEvents-tapahtumanhallintajärjestelmä ja Oodi-opintotietojärjestelmä. Näiden järjestelmien käyttötarve työelämäkoulutuksen toteutuksessa riippuu asiakkaan tarpeesta ja siitä, onko koulutusta opintopisteytetty.

Koulutuksesta ei saa opintopisteitä

Mikäli koulutusta ei ole opintopisteytetty tai osallistujilla ei ole tarvetta saada koulutuksesta opintopisteitä, toteutus vaatii ainoastaan ilmoittautumisjärjestelmän käytön (ja mikäli koulutus järjestetään Oulun yliopiston tiloissa, myös tietohallinnolta väliaikaisten kevyttunnusten hankkimisen STUDENT-toimialueen työasemiin ja palvelimiin). Oulun yliopistolla on tapahtumiinilmoittautumista varten käytössä WebropolEvents-tapahtumanhallintajärjestelmä, joka mahdollistaa ilmoittautumislomakkeiden luomisen koulutuksia varten, osallistujatietojen hallinnan ja palautteen keräämisen koulutusten jälkeen. Osallistujilta kerätään

ilmoittautuessa ainoastaan tarpeelliset yhteystiedot, eikä kerättyjä tietoja ole tarvetta säilyttää koulutuksen jälkeen.

Koulutuksesta saa opintopisteitä

Mikäli asiakas haluaa soveltuvista työelämäkoulutuksista, opintojaksoista tai-kokonaisuuksista opintopisteitä ja heillä ei ole voimassa olevaa opinto-oikeutta Oulun yliopistossa, heidän tulee hakea erillisopinto-oikeutta. Ohjeet ja hakulomake löytyvät Oulun yliopiston verkkosivuilta: https://www.oulu.fi/tst/content/erillisvalinnat. Tällöin osallistujien tiedot tallennetaan Oodiin, joka on opetus-ja opiskelutoimintojen tukemiseen tarkoitettu tietojärjestelmä, joka sisältää tiedot opiskelijoista, opinto-oikeuksista, ilmoittautumisista ja opintosuorituksista. Koulutuksiin ilmoittautumiseen käytetään pääasiassa WebropolEvents-tapahtumanhallintajärjestelmää, mutta koulutuksen tyypistä riippuen ilmoittautuminen täytyy suorittaa lisäksi Weboodin, Oodin verkkokäyttöliittymän kautta. Osallistujat saavat erillisopinto-oikeuden mukana henkilökohtaisen käyttäjätilin yliopistontietojärjestelmien STUDENT-toimialueelle, joten väliaikaistentunnusten hankkimiselle ei ole tarvetta. Tiedot osallistujista ja heidän suorittamistaan opintopisteytetyistä koulutuksista ja opintojaksoista tallennetaan opintorekisteriin.

TAMPEREEN AMMATTIKORKEAKOULU

Toimenpide on toteutettu Tampereen ammattikorkeakoulussa tekemällä sisäisiä selvityksiä pohjautuen erilaisiin työelämäkoulutusten opintohallinto- ja tietojärjestelmiin kohdistamiin vaatimuksiin. Toimenpiteessä on myös hyödynnetty aikaisempaa Iotti-hankkeen selvitystyötä sekä tehty yhteistyötä Tampereen yliopiston kanssa.

Tulokset

Selvityksessä tunnistettiin muutama keskeisesti huomioitava asia:

1. opinsuorituksiin, opintopisteisiin, opiskelijarekisteriin liittyvät asiat
2. oppimisympäristöihin ja materiaalien yms. jakoon liittyvät asiat
3. labra-/tietokoneympäristöihin, tiloihin ja kulunvalvontaan liittyvät asiat

1 Opintosuorituksiin liittyvät asiat ja opiskelijoiden rekisteröinnit

Työelämäkoulutuksiin opiskelijoina osallistuvia henkilöitä ei tarvitse rekisteröidä TAMKin järjestelmiin eikä he tarvitse niihin TAMKin tunnuksia mikäli työelämäkoulutukset eivät tuota opintopisteitä. Mikäli koulutuksista annetaan opintopisteitä tulee ne tehdä koulutuksesta vastaavan tahon toimesta ja myöskään tällöin TAMKin järjestelmiin ei liity tarpeita.

Tarve TAMKin opintohallinnollisiin järjestelmiin syntyy silloin, kun TAMK myöntää koulutuksesta opintopisteitä. Tällöin osallistujien tulee rekisteröityä TAMK avoimen ammattikorkeakoulun opiskelijoiksi ja tuon prosessin kautta he saavat tarpeelliset tunnukset opintohallintojärjestelmiin ja oikeuden mm. opintosuoritusotteiden tulostamiselle.

Hankkeen ajankohtana on kehitteillä koko valtakunnallisesti uusia opintosuoritusrekistereitä/-järjestelmiä, joiden vaikutusta ei osattu tässä yhteydessä vielä arvioida. Tämän lisäksi Tampereen korkeakouluyhteisöllä (TAMK+TTY) on kehitteillä omia yhteisiä järjestelmiään. Näistä on lisätietoa TTYn selvityksessä.

2 Oppimisympäristöt ja materiaalien yms. jako

TAMKissa on käytössä useita erilaisia oppimisympäristöjä yms. tapana järjestää verkkoresursseja koulutuksille oleville. Käytetyimmät tavat ovat Tabula sekä Teams, jotka ovat molemmat TUNI-yhteisön hallinnoimia palveluita. Tabulasta ollaan luopumassa ja siirtymässä käyttämään Tampereen yliopiston Moodle-palvelua. Tämän käytöstä ei ole tällä hetkellä tarkempaa tietoa. Teams-palvelua voidaan käyttää TUNI-tietohallinnon tunnuksilla mutta sen käyttö on mahdollista myös ns. vierailijatunnuksilla. Näin ollen työelämäkoulutuksissa ei ole tarpeen erikseen luoda tähän järjestelmän kursseille osallistuville tunnuksia.

Labrat, tietokoneet ja tilat

TAMKin kyberturvallisuuteen liittyvät labraympäristöt on toteutettu erillisverkossa, jossa on oma käyttäjähallintonsa. Työelämäkoulutuksiin osallistujille voidaan luoda omat väliaikaistunnukset aina jokaisen kurssin tarpeen mukaan. Sama koskettaa labraan liittyviä tietokoneluokkia, jotka tältä osin ovat käytettävissä verkostolle ilman ulkopuolista käyttäjähallintaa/rekisteröitymisiä.

Tiloihin on sähköinen kulunvalvonta eikä niihin päästä ilman kulkulupaa. Lupia ei myönnetä vierailijoille, joten toteutettaessa työlämäkoulutusta TAMKilla tulee mukana olla TAMKin oma vastuuhenkilö, joka huolehtii tiloissa kulkemisista.

TAMPEREEN YLIOPISTO

Yhteenveto

Tampereen yliopistossa työelämäkoulutettavat tarvitsevat opinto-oikeuden, jotta heille voidaan kirjata suorituksia, jotta heidän on mahdollista saada kulkukortti ja jotta he voivat käyttää yliopiston tietojärjestelmiä.

Tarvittavat opinto-oikeudet on mahdollista rekisteröidä erillisopiskeluoikeuksina. Toistaiseksi tiedot toimitetaan opintotoimistoon joko paperisella ilmoittautumislomakkeella tai e-lomakkeella. Jatkossa uuteen opintotietojärjestelmä Sisuun on tulossa myös ilmoittautuminen erillisopintoihin. Tällöin työelämäkoulutusten suoritukset voidaan kirjata suoraan opintotietojärjestelmään.

Tampereen yliopistossa useamman yliopiston yhteistyöhankkeena kehitettävä opintotietojärjestelmä Sisu korvaa monia vanhoja opintotietojärjestelmiä elokuussa 2020. Sisun ajatuksena on helpottaa yhteistyötä korkeakoulujen välillä ja myös sisäisesti, kun opintoihin liittyvät tiedot ovat yhdessä järjestelmässä. Mikäli Sisu on jossakin vaiheessa käytössä myös Kyberturvaaja-hankkeen ammattikorkeakouluissa, järjestelmä voisi helpottaa opistokokonaisuuksien rakentamista työelämäkoulutettaville siten, että opintoja voisi helposti yhdistää kokonaisuuteen useamman korkeakoulun opintotarjonnasta.

Tampereen yliopistossa siirryttiin maaliskuun puolivälissä 2020 etäopetukseen koronapandemian vuoksi. Tämän siirtymän aikana etäopetusjärjestelmät ovat tulleet laajamittaiseen käyttöön tutkinto-opetuksessa. Näitä kokemuksia voidaan hyödyntää myös työelämäkoulutuksessa. Etäopetusta hyödyntämällä työelämäkoulutuksiin voidaan helpommin osallistua paikkakuntarajojen yli. Tässä dokumentissa käsitellään etäopetusta tukevista ohjelmistoista lyhyesti Tampereen yliopistossa käytössä olevaa Panoptoa, Microsoft Teamsia ja Zoomia.

1 Opintohallinto

Tampereen yliopistossa työelämäkoulutettavat tarvitsevat opinto-oikeuden, jotta heille voidaan kirjata suorituksia ja jotta heidän on mahdollista saada esim. kulkukortti. Lisäksi yliopiston tietojärjestelmien käyttöön tarvittavien tunnusten myöntäminen edellyttää opinto-oikeuden. Työelämäkoulutettavat rekisteröidään järjestelmään erillisopiskeluoikeuksin.

Opintotoimistossa on mahdollista rekisteröidä tarvittavia erillisopiskeluoikeuksia, kun koulutuksen järjestämisestä on tehty virallinen päätös. Toistaiseksi yliopistolla ei ole tarjolla helppoa ilmoittautumistapaa erillisopintoihin. Opintotoimistoon täytyy kuitenkin toimittaa opiskelijoiden rekisteröimiseen tarvittavat tiedot. Näitä on toistaiseksi kerätty joko paperisella ilmoittautumislomakkeella tai e-lomakkeella. Jatkossa uuteen opintotietojärjestelmä Sisuun on tulossa myös ilmoittautuminen erillisopintoihin.

2 Uusi opintotietojärjestelmä Sisu

Tampereen yliopistossa siirrytään käyttämään uutta opintotietojärjestelmää, Sisua. Sisu on Funidatan opintotietojärjestelmä, jota kehitetään yhteistyössä yliopistojen kanssa, nämä ovat: Aalto-yliopisto, Hanken, Helsingin yliopisto, Jyväskylän yliopisto, LUT-yliopisto ja Tampereen yliopisto. Tampereen yliopistossa Sisu korvaa monia vanhoja opintotietojärjestelmiä elokuussa 2020. Sisussa ovat koko yliopiston opetussuunnitelmat, opetustarjonta, opintosuunnitelmat, HOPS-ohjaus, opetukseen ilmoittautuminen, arviointi, opiskeluoikeudet, opiskelijarekisteri, todistukset ja sähköinen asiointi.

Sisun ajatuksena on helpottaa yhteistyötä korkeakoulujen välillä ja myös sisäisesti, kun opintoihin liittyvät tiedot ovat yhdessä järjestelmässä. Sisuun on saatavilla työkaluja myös avoimen yliopiston suoritusten hallinnointiin. Ei ole tiedossa, ovatko nämä ominaisuudet samat kuin aikaisemmin mainittu Tampereen yliopiston Sisuun tulossa oleva erillisopintoihin ilmoittautuminen. Funidatan mukaan avoimen yliopiston toiminnallisuuksien koodaaminen Sisuun on alkanut keväällä 2020 ja on tätä raporttia viimeisteltäessä vielä kesken.

Funidatan kuvauksen mukaan avoimen opiskelija ostaa Sisussa tuotepaketin, joka antaa suoritusoikeuden opetukseen. Tuotepaketille annetaan suoritusaika ja samalla voidaan rajata myös kuinka monta kertaa opiskelija voi ilmoittautua opetukseen tai mitkä opetukset hän voi suorittaa. Opiskelija voi ennen maksamista laittaa ostoskoriin useamman opintojakson eli tuotepaketin. Näin opiskelija voi kerralla ostaa esim. jonkin opintokokonaisuuden kaikkien opintojaksojen opetuksen.

Vastaavan mallin mukaan Sisussa mahdollisesti voitaisiin käsitellä myös työelämäkoulutettaville tarjotut kurssit. Mikäli Sisu on jossakin vaiheessa käytössä myös Kyberturvaaja-hankkeen ammattikorkeakouluissa, järjestelmä voisi helpottaa opistokokonaisuuksien rakentamista työelämäkoulutettaville siten, että opintoja voisi helposti yhdistää kokonaisuuteen useamman korkeakoulun opintotarjonnasta.

3 Etäopetusta tukevat ohjelmistot

Tampereen yliopistossa siirryttiin maaliskuun puolivälissä 2020 etäopetukseen koronapandemian vuoksi. Tämän siirtymän aikana etäopetusjärjestelmät ovat tulleet laajamittaiseen käyttöön tutkinto-opetuksessa. Näitä kokemuksia voidaan hyödyntää myös työelämäkoulutuksessa. Etäopetusta hyödyntämällä työelämäkoulutuksiin voidaan helpommin osallistua paikkakuntarajojen yli.

Panopto

Panopto on videotallennusohjelmisto, jolla voi tallentaa oppimistapahtumia ja samanaikaisesti myös suoratoistaa. Tallenteet voidaan integroida kurssin Moodle-sivujen kanssa siten, että oppimistapahtumista tallennetut videot ovat siellä vapaasti kurssin opiskelijoiden katsottavissa. Suoratoiston aikana opiskelijoiden kanssa voi keskustella tekstipohjaisen chatin kautta, mutta kaksisuuntaista kuva- ja ääniyhteyttä yleisöön ei ole.

Microsoft Teams

Microsoft Teams palvelussa yksittäiset henkilöt tai suuremmat ryhmät voivat osallistua videotapaamisiin. Niissä voidaan jakaa ääntä, videokuvaa ja tietokoneen näyttö. Videotapaamisissa kaikki voivat tarvittaessa käyttää mikrofonia tai jakaa videota tai näyttökuvaa. Osallistujia tapaamisessa voi olla enintään 250, mutta Teamsin kautta on myös mahdollista toteuttaa isojen osallistujamäärien (max. 10000 henkilöä) Teams-suoratoistoja. Niissä osallistujat voivat seurata Teams-suoratoistoa, mutta osallistujat eivät voi jakaa ääntä eivätkä videota. Tekstipohjaisia kysymyksiä voi kuitenkin lähettää, jos järjestäjä on ne sallinut.

Tampereen yliopistossa Teamsilla on mahdollista luoda kurssin opiskelijoille, kokous, ryhmä tai tarvittaessa useampia ryhmiä. Tällöin ryhmät saavat käyttönsä oman Teams-tilan, jossa voi keskustella eri kanavilla, pitää videotapaamisia, jakaa ja editoida yhteisiä tiedostoja, tai jakaa esim. yhteisiä videoita tai linkkejä. Teamsin tiimitilalla on helppo järjestää kurssin osallistujille yhteinen kanava, jonka kautta ryhmätyöskentely on mahdollista esim. yli paikkakuntarajojen. Kokoustilaa voi käyttää opetuksessa ryhmätyöskentelyyn, harjoitusten pitämiseen tai etäluentoihin.

Teams-tapaamisen voi myös tallentaa. Tapaaminen tallentuu Microsoft Stream -palveluun, josta sen voi siirtää omalle koneelleen ja edelleen esimerkiksi Panopton kautta kurssin Moodle-sivulle opiskelijoiden käyttöön.

Zoom

Zoom-videotapaamispalvelussa on mahdollista jakaa ääntä, videokuvaa, näyttökuvaa ja materiaaleja. Palvelu toimii Windows, Mac, Linux, iOS ja Android -laitteilla. Zoomilla voidaan järjestää pienryhmätyöskentelyä, verkkokokouksia, etäluentoja ja webinaareja. Tapahtumissa käytössä on erilaisia ominaisuuksia, kuten chat, luonnostelutaulu, äänestykset, kyselyt, ryhmätyöhuoneet ja videotallennus. Zoom-tapahtumassa voi olla 300 henkilöä yhtä aikaa, mutta tätä määrää voidaan it-helpdeskin kautta nostaa 500 henkilöön webinaarilisenssin avulla. Tällöin käyttöön tulee myös erikoistoimintoja, kuten ennakkorekisteröitymislomake ja Q&A-toiminto.

Zoom-tapahtuman voi tallentaa videolle paikallisesti, eli käyttäjät voivat tallentaa kokousvideon ja -äänen tietokoneelleen. Jos käytetään ryhmätyötiloja, tallennus keskeytyy ja jokaisessa ryhmässä tallennus pitää tehdä erikseen. Zoomilla tallennetut videot voi julkaista esim. Panopto-videopalvelun kautta, jolloin ne ovat saatavissa opiskelijoiden käyttöön esimerkiksi kurssin Moodle-sivuille.

TURUN AMMATTIKORKEAKOULU

Turun ammattikorkeakoulun selvitys verkostomaisesti toteutettavan työelämäkoulutuksen vaikutuksista opintohallintoon ja tietojärjestelmiin

1.Turun AMK:n työelämäkoulutusten hallinnointi, tietojärjestelmät ja oppimisympäristöt

Mukana olevat yksiköt

Työelämäpalvelut

Turun AMK:n tarjoaa työelämäpalvelujen kautta ratkaisuja yritysten ja organisaatioiden kehittämistarpeisiin. Jokaisella sektorilla, Turun AMK:n osaamisalueella, on työelämäpalveluhenkilöstöä ja lisäksi yhteiset palvelut -sektorilla toimii Työelämäpalvelut-koordinaatioyksikkö. Työelämäpalvelut- koordinaatioyksikkö on Turun

AMK:n kumppanuus- ja liiketoimintaa sekä alumniyhteistyötä koordinoiva palvelutoiminto, ja sen vastuualueina on mm. Turun AMK:n liiketoimintaprosessin kehittäminen, yhteisten käytäntöjen luominen asiakasyhteistyöhön sekä kumppanuuksien johtamiseen ja hallintaan, ASKO-asiakkuushallintajärjestelmän kehittäminen ja pääkäyttäjyys, rekrytointipalvelujen kehittäminen sekä yritysten ja yhteisöjen toimeksiantojen välittäminen sekä työelämäpalvelujen viestintä ja markkinointi.

Turun AMK:n sektoreilla, eli osaamisalueilla, on lisäksi omat täydennyskoulutusvastaavansa, joiden tehtävänä on arvioida ja hallinnoida koulutukseen osallistujia, sekä vastata sektorikohtaisten koulutusten markkinnoinnista.

Opintohallinto

Opintohallinto toimii osana Turun AMK:n opiskelijapalvelukokonaisuutta. Opintohallinnon tehtäviin kuuluu Peppi-opintotietojärjestelmän ylläpito, tietojen oikeellisuuden ja laadun valvonta sekä opiskelijoiden ja henkilökunnan neuvonta opiskeluoikeuteen, läsnä-/ ja poissaoloilmoittautumiseen, opintosuoritusmerkintöihin ja valmistumiseen liittyvissä asioissa. Opintohallinnon vastuulla ovat myös valtakunnallisten VIRTA- ja KOSKI-tietovarantojen ylläpito, ml. suoritus- ja valmistumistietojen tuottaminen viranomaisten ja opiskelijoiden saataville. korkeakoulujen rahoitusmallin tarvitsemien tietojen tuottaminen, Viranomaisten (esim. KELA, Tilastokeskus, Valvira) tarvitsemien tietojen tuottaminen sekä Oma Opintopolku – palvelun hallinnointi. Lisäksi Opintohallinto vastaa valtakunnallisesta kehitysyhteistyö (VIRTA, Peppi, korkeakoulujen ristiinopiskelu).

Täydennyskoulutusten osalta opintohallinnon keskeisenä tehtävänä on jouhevan yhteistyön varmistaminen opintohallinnon ja täydennyskoulutuksesta vastaavien tahojen kanssa erityisesti Peppi – opintotietojärjestelmän osalta.

Käytössä olevat tietojärjestestelmät

ASKO

Turun AMK: lla on käyttössää ASKO- asiakkuudenhallintojärjestelmä. Microsoft D365- ympäristössä toimiva ASKO mahdollistaa aiempaa paremman tiedonkeruun yritysten ja muiden organisaatioiden kanssa tehtävästä yhteistyöstä eri sektoreilla. ASKOn alla hallitaan kolmea eri toimintoa: myyntiprosessi (tarjous, tilaus, laskutus), markkinointi (postituslistojen hallinnointi, uutiskirjeet Apsiksen kautta) ja toimeksiannot (yritys-opiskelijayhteistyönä tehtävät toimeksiannot). Lisäksi myyntiä, markkinointia ja toimeksiantoja tekevät henkilöt ovat saaneet ASKOsta itselleen tehokkaan työkalun: ”tilauskirjan”, jossa omia tehtäviä on helppo seurata ja hallita. ASKOn avulla saamme myös reaaliaikaista dataa Turun AMK:n liiketoiminnan osalta.

Lyyti

Lyyti-palvelu on Turun kaupungin omistama tapahtumien hallintapalvelu, jolla hallitaan tapahtumien ilmoittautumista, viestintää, raportointia sekä myös mahdollista maksuliikennettä. Lyytin kautta on mahdollista toteuttaa myös kyselyjä ja sen lomakepohjia on mahdollista hyödyntää moniin tarpeisiin. Turun AMK: lla on useampia käyttölisenssejä järjestelmään.

Webropol – kysely- ja raportointi ohjemisto

Webropol on Turun AMK:n käytössä oleva kysely- ja raportointisovellus, jota käytetään laajasti myös asian- ja tapahtumanhallintaan. Webropoliin kirjaudutaan HAKA-tunnuksilla. Opiskelijoilla ja henkilökunnan jäsenillä on oma ympäristö Webropolissa. Opiskelijan tunnuksilla tehtyä kyselyä ei voi jakaa henkilökunnalle eikä

toisinpäin. Avoimen AMK:n ja täydennyskoulutuksen opiskelijat eivät pääse kirjautumaan Webropol järjestelmään.

Peppi

Peppi on Turun AMK:n käytössä oleva koulutusorganisaatioiden tarpeisiin suunniteltu ohjelma, jossa mm. hallinnoidaan, toteutetaan ja suunnitellaan oppimissuunnitelmia, niiden aikataulutusta ja resursointia. Pepissä on oma työpöytänsä/palvelunsa eri roolissa toimiville tahoille. Opiskelija pääsee katsomaan työpöydältään suoritusotteet, kalenterit, Hops:n, seuraamaan opintojen edistymistä, sopimuksia, Ahotia sekä todistuksiaan kun taas opettajalla on käytössään resurssisuunnittelufunktio, Ahot, raportointi, OPS:t, toteutukset ja oppimateriaalit. Suunnittelijan työpöytään kuuluvat resurssien suunnittelu, Ahot, raportointi, OPS-hallinta, vuosisuunnittelu, ja opiskeljapalveluilla keskiössä ovat hakijoiden tuominen järjestelmään, opiskelijoiden hallnta, todistukset ja raportit.

TEPPO (Thinking Portfolio)

Thinking Portfolio on projekti-, sovellus- ja palvelusalkunhallinnan järjestelmä, jota Turun AMK: ssa käytetään erityisesti TKI- hankkeiden hallintaan, aina projektien ideoinnnista projektisalkun hallintaan, resursointiin ja työajan seurantaan.

Zoom

Turun AMK:n opiskelijoiden ja henkilökunnan käytettävissä on Zoom-videoneuvotteluohjelmisto, jota käytetään erityisesti etäkokousten ja virtuaalisten tilaisuuksien järjestämiseen.

Teams

Turun AMK:ssa on käytössä Microsoft Teams, joka on yrityksille ja yhteisöille suunnattu ryhmätyön ja yhteistyö- alusta, joka kokoaa tärkeimmät keskustelut, pilvipalvelut ja tiedostot yhteen jaettuun työtilaan. Teams- alustaa käytetään kasvavissa määrin myös opetustarkoituksessa.

Käytössä olevat oppimisympäristöt

Optima ja Itslearning

Optima on Turun Ammattikorkeakoulun aikaisemmin käytössä ollut oppimisympäristö, mutta Alkukeväästä 2020 Turun AMK:n uudeksi oppimisympäristöksi valikoitui Sanoma Oyj:n omistama Itslearning. Uudesta järjestelmästä ei AMK:ssa vielä ole paljon kokemusta, mutta Optima- verkkoympäristöä on käytetty sekä opetuksessa ja projekteissa. Optimassa on tyypillisesti jaettu kurssimateriaalit minkä lisäksi se on toiminut kurssitehtävien palautuslaatikkona, keskusteluympäristönä sekä oppimispäiväkirja-alustana. Opiskelijalla on myös ollut mahdollisuus seurata Optimassa omia opintosuorituksiaan.

Yrityksille suunnatuissa koulutuksissa oppimisympäristöt (Optima, jatkossa Itslearning) eivät ole perinteisesti olleet käytössä, sillä niiden haltuun ottaminen yrityksissä on ollut haastavaa. Yrityskoulutukset onkin toteutettu tavanomaisesti lähiopetuksena tai vaihtoehtoisesti verkkoalustoilla, kuten Teams- tai Zoom-sovellusten kautta.

Simulaatiotilat ja laboratoriotilat

Turun AMK: lla on käytössään myös eri koulutusaloille soveltuvia simulaatio- ja laboratoriotiloja, joita käytetään tarpeen mukaan myös yrityskoulutuksissa. Näiden tilojen hyödyntäminen yrityskoulutuksissa on

perinteisesti toiminut hyvin (haasteeksi silloin tällöin on noussut tilojen myöhäiset varaukset ja päällekkäiset varaukset).

Verkostomaisesti toteutettavien koulutusten osalta huomioon otettavat asiat sekä vaikutukset opintohallintoon ja tietojärjestelmiin

Sopimus- ja lakiasiat

Immateriaalioikeudet

Turun AMK: lla on kokemusta muiden korkeakoulujen kanssa verkostomaisesti toteutettavista myydyistä koulutuksista (esim. HAUS:llle). Haasteeksi joissakin toteutuneissa koulutuksissa on nousseet laki- ja sopimus- ja lakiasiat: on hyvä varmistaa ennen koulutuksen toteutusta, millaisia käyttö- ja jako- oikeuksia koulutuksessa käytettävällä materiaalilla on. Immateriaalioikeuksista on hyvä sopia etukäteen mikäli on oletettavissa, että koulutuksen aikana tehtävissä toimeksiannoissa tai projektiluontoisissa toimeksiannoissa syntyy tuotoksia, jotka voivat olla merkityksellisiä innovaatio- ja patenttinäkökulmasta.

Salassapito- ja tietoturva-asiat

Yrityskoulutusten osalta haasteita voi syntyä koulutuskokoonpanosta, jossa on mukana useampi korkeakoulu ja useampi yritys, sillä salassapitovelvollisuudet voivat rajata käytävien keskustelujen avoimuutta. Näin ollen ennen koulutuksen toteutusta onkin hyvä sopia toteuttajien ja osallistujien kesken hyvissä ajoin, millaiset keskustelukäytänteet koulutuksen aikana tulee olla ja mitkä oikeudet ja velvollisuudet kouluttajia ja osallistujia koskee. On mahdollista sopia esim. niin, että yhteiskäytössä olevilla alustoilla ei jaeta materiaaleja tai että keskusteluja/koulutuksia ei tallenneta, jolloin salassa pidettävän tiedon leviämisen riski pystytään minimoimaan.

Julkiselle sektorille suunnatut koulutukset ovat joskus haastavia tietoturvanäkökulmasta, sillä monilta julkissektorin toimijoilta on pääsy mm. Teamsiin tai Zoomiin kokonaan kielletty. Näin ollen koulutuksen suunnitteluvaiheessa on hyvä pohtia etukäteen, millä alustoilla koulutukset toteutetaan, erityisesti mikäli iso osa koulutuksesta toteutetaan verkossa etäopetuksena.

GDPR-asetuksen huomioiminen

Tietosuoja-asiat nousevat usein haasteeksi myös perinteisissä, ei- verkostomaisesti toteutettavissa yrityskoulutuksissa. Verkostotototeutuksissa olisikin hyvä, että korkeakoulut varmistaisivat ja yhtenäistäisivät käytäntönsä tietosuoja-asioiden osalta ja osana laajempaa keskustelua koulutuksen toteutukseen liittyvistä laki- ja sopimusasioista. Korkeakoulujen tulisikin, mahdollisuuksien mukaan, laatia yhtenäiset tietosuoja-ohjeistukset ja – prosessit sekä viestiä käytänteistä yrityksiin keskitetysti. Tutkintopuolella on jo voimassa olemassa puitesopimus (v.2019) opetusyhteistyöstä suomalaisissa korkeakouluissa. Sopimuksessa on kuvattu mm. se, että ”yksi sopijapuolena oleva korkeakoulu voi toimia yhteistyössä annettavan opetuksen osalta tietojen käsittelijänä ja hallinnoijana muiden sopijakorkeakoulujen lukuun.”1 Tällainen valtuutus tulee osaltaan sisällyttää erilliseen opetusyhteistyötä koskevaan verkostosopimukseen. 2

Käytännön suunnittelu ja toteutus

Lähiopetus/verkko-opetus

Turun AMK: lla on kokemusta verkostomaisesti toteutettavista koulutuksista erityisesti erikoistumiskoulutusten osalta. Kokemukset erikoistumiskoulutusten verkostototeutusten osalta ovat

verrattain myönteisiä, eikä suurempia haasteita ole noussut esiin. Korona-aika on parantanut entisestään opettajien ymmärrystä siitä, mitä osioita koulutuksista kannattaa toteuttaa etänä ja mitä ei.

Koska kaikilla korkeakouluilla ei ole käytössään samoja oppimisympäristöjä, opetusmateriaalit on yleensä toimitettu kootusti koulutuksesta vastaavalle taholle, joka manuaalisesti siirtää ne omaan, käytössään olevaan oppimisympäristöön. Koska yrityskoulutuksissa ei perinteisesti ole ollut käytössä korkeakoulujen omia oppimisympäristöjä, onkin syytä sopia materiaalien jaosta ja käytössä olevasta oppimisalustasta yhdessä muiden toimijoiden kanssa siten, että kokonaisuus parhaiten vastaa asiakkaan tarpeita ja toteutus onnistuu mahdollisimman ketterästi. Olisikin hyvä käydä vertailevaa keskustelua korkeakoulujen välillä siitä, mikä taho kussakin tilanteessa parhaiten soveltuu vetovastuuseen toteutuksesta, sisältöjen mutta myös teknisen toteutuksen osalta.

Tiedonkulku, viestintä ja markkinointi

Turun AMK: ssa Työelämäpalvelut- yksikkö mainostaa koulutuskortteja verkkosivuillaan, minkä lisäksi yrityksille laaditaan flyer- tyyppisiä kohdennettuja uutiskirjeitä. Yritykset voivat kontaktoida Työelämäpalveluita Ota yhteyttä – lomakkeen kautta, ja siten suoraan kuvata koulutustarvettaan.

Verkostomaisen kyberturvallisuus- koulutuksen toteutuksen osalta olisikin hyvä, että kunkin mukana olevan korkeakoulun Työelämäpalvelu-yksikköä vastaava taho on tarkasti briiffattu olemassa olevasta koulutustarjonnasta, jotta ensikontaktoinnissa mukana olevat tahot osaavat ohjata tiedustelut eteenpäin oikeille tahoille sekä vastata yritystiedusteluun olemassa olevan koulutustarjonnan mukaisesti.

Turun AMK: ssa koulutusten markkinointi hoidetaan osaamisalueilla eli sektoreilla. Sektorit vastaavat myös opiskelijavalinnoista. Valintaperusteet on syytä avata ja kuvata selkeästi läpinäkyvyyden ja soveltuvien osallistujatahojen varmistamiseksi. Verkostomaisesti toteuttavien koulutusten osalta on hyvä sopia valintakriteereiden lisäksi selkeät vastuut ilmoittautumisten ja valintaprosessin toteutuksen osalta, jotta roolitukset ja tehtävänkuvat ovat selkeät kaikille mukana oleville tahoille.

Koulutuspalvelujen markkinoinnissa Turun AMK toimii pitkälti sosiaalisen median markkinoinnin, uutiskirjeiden ja erilaisten verkostotapahtumiensa varassa. Onnistuneessa ja tavoitteellisessa markkinnoinnissa on tärkeää, että myytävä koulutuspalvelutuote on selkeä ja että markkinoijat osaavat tavoittaa oikeat koulutuksen kohderyhmät.

Hinnoittelu ja resursointi

Organisaatioiden sisäinen hallinto- ja asiantuntijatyö tulisi huomioida myytävien koulutusten hinnoittelussa opetushenkilöstön työn lisäksi. Tulisi tarkastella, työllistääkö, ja missä määrin, myytävä koulutus esim. opintohallintoa, kirjasto- ja tietopalveluita tai TKI- palveluilta.

Koulutuksen jälkeen: opintosuoritukset ja jatkokehittäminen

Opintosuoritukset: hyväksi lukeminen, opintopisteet ja todistukset

Kaikista koulutuksista ei automaattisesti anneta todistusta, vaan tarvetta todistukselle arvioidaan tapauskohtaisesti. Mikäli AMK- tasoisia koulutuksia toteutetaan täydennyskoulutuksesssa, opintosuoritukset tulisi tallentaa Peppi- järjestelmään.

Koulutukseen osallistuvat tahot saattavat haluta koulutuksestaan todistuksen tai sertifikaatin todentaakseen käyneensä koulutuksen tai pystyäkseen osoittamaan osallistumisensa tietyn kestoiseen koulutukseen. Jos

kyseessä on säädeltyyn osaamiseen liittyvä koulutus, kouluttajien tulee olla valmiudessa laatia koulutuksesta virallinen todistus, josta saavutettu osaamisen taso käy ilmi.

Korkeakoulujen välillä ristiinopiskelun toteutus tulee jatkossa helpottumaan entisestään, sillä v. 2021 otetaan käyttöön ristiinopiskelun palveluväylä, joka virtaviivaistaa prosessia automatisoitumisen avulla.

Jatkokehittämiseen liittyvät toimenpide-ehdotukset

Korkeakouluverkoston tulisi kehittää ja integroida IOTTI-malliin yhteinen jatkokehittämisen malli jonka puitteissa voisi yhteistoiminnassa arvioida koulutusten sisältöjä ja jatkokehittämistarpeita. Arvioinnissa tulisi huomioida koulutettavilta saadut palautteet mutta myös verkoston sisällä arvioida kokemusten pohjalta yhteistoimintaan liittyvät kehittämistarpeet.

Lähteet:

- Turun Ammattikorkeakoulun intranet Messi
- syventävät asiantuntijahaastattelut (Työelämäpalvelut 3.6.2020, Opintohallinto 5.6.2020 sekä täydennyskoulutuspäälliköt 10.6.2020)
- Puitesopimus opetusyhteistyöstä suomalaisissa korkeakouluissa, 21.10.2019

KOOSTE OPPILAITOSTEN KYBERTURVALLISUUTEEN LIITTYVISTÄ OPPIMIS- JA TUTKIMUSYMPÄRISTÖISTÄ

Toimenpide 3.1 Jokainen oppilaitos tekee oman selvityksensä kyberturvallisuuteen liittyvistä jo olemassa olevista teknisistä koulutus- ja tutkimusympäristöistä. Oppilaitokset tekevät ehdotukset siitä, miten heidän ympäristöjään hyödynnetään työelämäkoulutuksissa koko verkoston laajuudella. TAMK kokoaa selvitykset yhteen kokonaiskuvan saamiseksi.

TAMPEREEN YLIOPISTO

KYBERLABORATORIO, TAMPEREEN YLIOPISTO, TIETOTEKNIIKKA

Kyberlaboratorion ympäristö (Dependable Systems - Information Security CyberLab) on pääosin tarkoitettu verkon laitteiden ja palvelinsovellusten tietoturvallisuuden tutkimiseen. Tämä pitää sisällään työasemien käyttöjärjestelmät, palvelinsovellukset ja verkon laitteet (esim. reitittimet, kytkimet ja palomuurit).

Laboratoriolla on oma mikrointernet, joka vastaa karkealla tasolla Internetin toimintaa. Tässä mikrointernetissä voidaan tehdä verkkohyökkäys/murtautumisharjoituksia sekä niiden puolustamisharjoituksia. Tutkinto-opetuksessa ympäristöä hyödynnetään nykyisellään erilaisten hakkerointiharjoitusten toteuttamisessa. Tavoitteena harjoituksilla on simuloida esimerkiksi penetraatiotestaajan mahdollista työnkuvaa.

Ympäristö rakentuu työasemista, kytkimistä, palomuureista ja palvelimista. Työasemiin on mahdollista laittaa mikä tahansa ympäristö, johon on tarvittavat lisenssit. Työasemiin asentuu nykyisin valinnan mukaan joko BackBox tai Kali Linux. BackBox on penetraatiotestaukseen suuntautunut Linux-jakelu, joka tarjoaa verkko- ja järjestelmäanalyysityökaluja. Se sisältää joitain yleisimmin käytetyistä tietoturva- ja analysointityökaluista, jotka liittyvät esim. verkkoanalyysiin, haavoittuvuuksien arviointiin ja

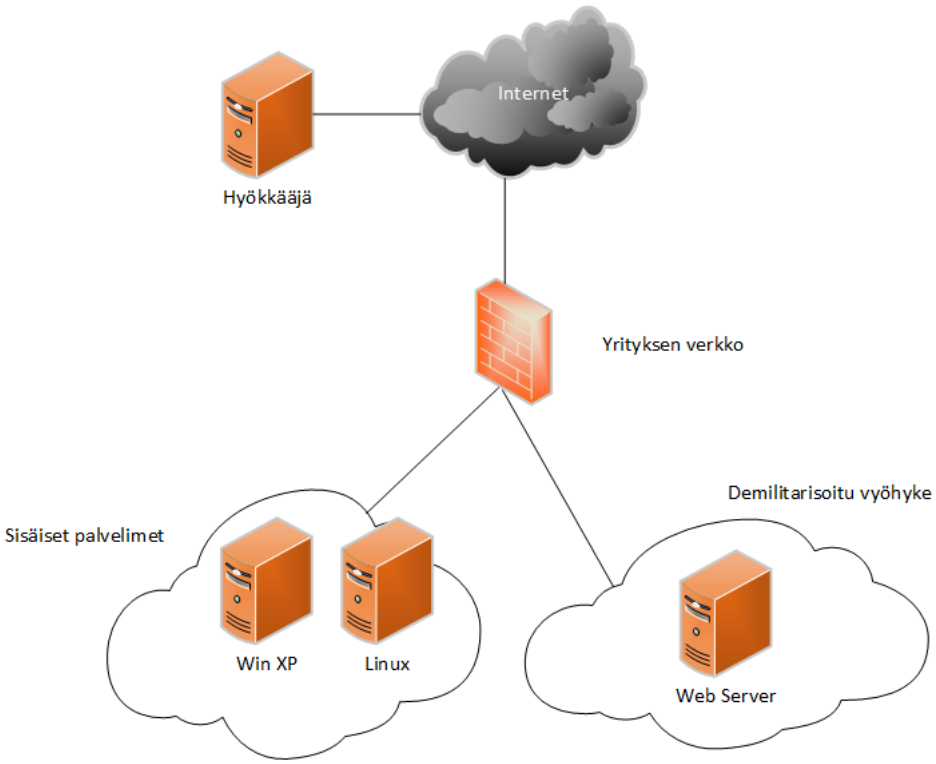
haavoittuvuuksien hyödyntämiseen. Kali Linux sisältää kattavan kokoelman murtautumiseen, verkkohäirintään ja verkon tutkimiseen tarkoitettuja työkaluja.

Laboratoriossa on 4 työasemaryhmää, joissa kussakin on 3 opiskelijapaikkaa. Opiskelijaryhmäkohtaisesti käytössä on seuraavat laitteet:

- 1x Cisco 3750 switch
- 2x SRX220 router /Firewalls
- 1x Cisco ASA551-x
- 2x Intel ATOM servers
- 2x Cisco 3750-X Switch in stacked mode
- 1x HP SDN capable switch

Palvelimia ajetaan ESXi-virtuaalisointiympäristössä. Jokaisella opiskelijalla on siis käytössään VMwaren ESXi-virtuaalisointiympäristö.

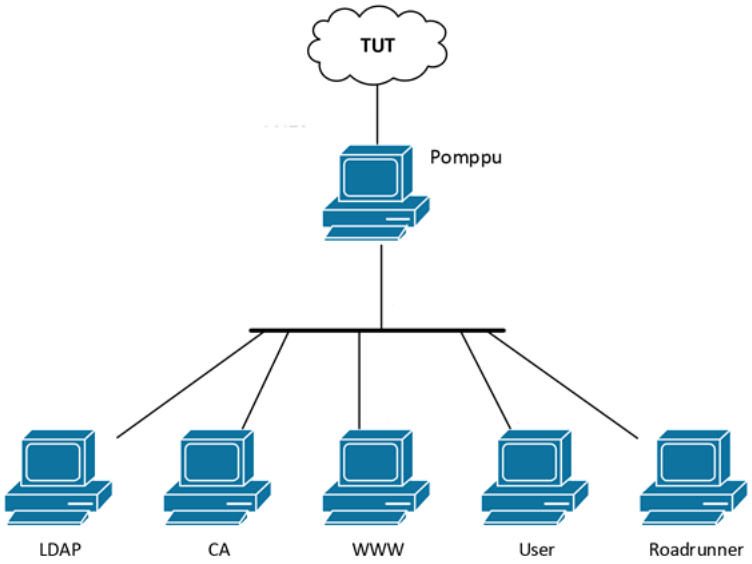
Laboratorion verkkoympäristössä voidaan käyttää ja testata erilaisia hakkerointi- tai murtautumistyökaluja suljetussa ympäristössä. Virtuaalisointiympäristön ja verkkolaitteiden avulla voidaan esimerkiksi mallintaa yrityksen sisäverkkoa ja liitäntää Internetiin. Tässä tapauksessa kyseessä on itse rakennettu mikrointernet. Mikrointernetistä voidaankin tehdä hyökkäyksiä yrityksen palveluihin ja aiheuttaa esim. hajautettu palvelunestohyökkäys (DDoS). Tutkinto-opetuksessa käytössä on esimerkiksi haavoittuva pienimuotoinen yrityksen verkkoa matkiva ympäristö (kuva 1), josta tehdään opiskelijoille omat virtuaalikloonit. Jokainen opiskelija voi tämän jälkeen etsiä haavoittuvuuksia ja harjoitella murtautumista omassa ympäristössään.



Kuva 1: Penetraatiotestausharjoituksen verkkoympäristö

Kuvan 1 harjoituksessa opiskelijat ottavat penetraatiotestaajan roolin. Kuvitteellinen yritys on palkannut heidät testaamaan yrityksen verkkoa. Yritys itse on vakuuttunut verkkoratkaisunsa turvallisuudesta ja palomuurinsa suojaavan sisäverkkoa aukottomasti. Opiskelijoiden tehtävänä on osoittaa, että näin ei ole. Aluksi opiskelijat keräävät tietoa yrityksen verkosta ja etsivät sopivia haavoittuvuuksia. Tämän jälkeen opiskelijat murtautuvat verkkoon. Tarkoituksena on löydettyjä haavoittuvuuksia hyödyntämällä ja sopivia työkaluja käyttämällä edetä web-palvelimelta yrityksen sisäverkkoon ja lopulta ottaa suoraan haltuun sisäverkon haavoittuva XP-kone. Harjoituksessa opiskelijoilla on usea mahdollinen etenemisreitti ja sen vuoksi mahdollisuus kokeilla ja soveltaa useaa erilaista murtautumistapaa ja työkalua. Harjoituksen edetessä tutuksi tulevat esimerkiksi tiedon hankinta erilaisilla skannaustyökaluilla, salasanojen murtaminen, Metasploit ja jotkin sen valmiit payloadit, eteneminen sisäverkossa ja reitittimelle murtautuminen.

Verkkoympäristössä voidaan toteuttaa ja käyttää myös erilaisia virtuaalipalvelinympäristöjä opetustarkoituksiin. Tutkinto-opetuksessa esimerkiksi identiteetin- ja pääsynhallintaa käsittelevällä kurssilla opiskelijat saavat käyttöönsä oman virtuaalipalvelinympäristön (kuva 2), jonne he kurssin harjoituksissa asentavat ja konfiguroivat LDAP-palvelimen, toteuttavat autentikointimenetelmiä Apache Internet -palvelimeen tutustuen samalla julkisen avaimen autentikointiin ja varmenteisiin, sekä tutustuvat ja toteuttavat Apache-palvelimen federointia Shibboleth ja OpenID Connect -ohjelmistoilla.



Kuva 2: Virtuaalipalvelinympäristö Identiteetin- ja pääsynhallinta -kurssilla

Verkkoympäristössä voidaan toteuttaa myös OWASP Juice Shop –harjoituksia. (Tämä ympäristö on rakenteilla tällä hetkellä, eikä vielä käytössä.) Juice Shop on OWASPin tuottama valmis verkkokauppasivusto, joka sisältää useita erilaisia haavoittuvuuksia (>60 kpl) useissa eri haavoittuvuuskategorioissa ja useilla eri vaikeustasoilla. Opiskelijoille voidaan antaa haavoittuvuuksia varten tehtävänanto ja kun opiskelija osoittaa

löytäneensä haavoittuvuuden, hän saa pisteitä suorituksesta. Juice shop sisältää haavoittuvuuksia liittyen esimerkiksi injektioon, rikkinäiseen autentikointiin, arkaluontoisen tiedon paljastumiseen, syötteentarkastukseen, virheelliseen turva-asetusten konfigurointiin, XSS:n (cross-site scripting), haavoittuviin komponentteihin ja rikkinäiseen pääsynvalvontaan.

KYBERLABORATORION HYÖDYNTÄMINEN VERKOSTOSSA

Kyberlaboratoriolla ei ollut valmista mallia siitä, miten ympäristöä voitaisiin hyödyntää koko verkoston laajuudessa työelämäkoulutuksiin. Ympäristöä on toistaiseksi käytetty yliopiston opetus- ja tutkimustarkoituksiin, jolloin esimerkiksi käyttöoikeudet ovat selvät. Hyödyntäminen verkoston laajuisessa työelämäkoulutuksessa edellytti lisäselvityksiä ainakin seuraavista asioista:

- ohjelmistojen lisenssit (esim. VMware)
- kulkuluvat
- opetusresurssit, erityisesti henkilökunnan saatavuus työelämäkoulutukseen
- yliopiston hallinnon edellytykset työelämäkoulutuksen järjestämiseen

Lisäselvitykset ja ehdotukset löytyvät seuraavista dokumenteista:

- Teknisten toimintaympäristöjen yhteiskäytön reunaehdot (Tampereen yliopisto)
- Kyberturvallisuuskurssien tarjoaminen tutkintokoulutuksen ulkopuolelle (Tampereen yliopisto)

DEPENDABLE SYSTEMS - AUTOMATION CYBERLAB, TAMPEREEN YLIOPISTO, AUTOMAATIOTEKNIIKKA

Automaatiotekniikan kyberlaboratorio on koulutus-, opetus- ja tutkimusympäristö. Ympäristö on rakennettu erityisesti kriittisen infrastruktuurin automaatiota varten. Se sisältää automaatiolaitteita, automaatiojärjestelmiä sekä automaatioon liittyviä tukijärjestelmiä mukaan lukien automaation tietoturvavalvonnan. Ympäristön rakentamisessa on kiinnitetty erityistä huomiota automaation normaalista toimisto-IT:stä poikkeaviin ominaisuuksiin. Tällaisia ovat mm. pitkä elinkaari sekä luotettavuus- ja reaaliaikavaatimukset. Ympäristö toteuttaa IEC-62443-standardin mukaista tietoturvallista automaatioverkkoa mahdollistaen monitoimijaympäristössä tehtävät kehittämistehtävät.

Ympäristö koostuu lukuisista automaatiojärjestelmistä ja -laitteista, jotka on verkotettu omalla automaatiorunkoverkolla yhdeksi isoksi kokonaisuudeksi. Runkoverkko on rakennettu vastaamaan teollisuudessa käytettäviä automaatiorunkoverkkoja sekä laitteiden että konfiguraation osalta.

Ympäristön keskeinen osa on 36 paikkainen mikroluokka, joka on verkotettu osaksi automaation runkoverkkoa. Luokasta voidaan käyttää kaikkia laboratorion järjestelmiä. Luokkaa käytetään osana automaatio-opetusta ja siellä järjestetään myös erilaisia tapahtumia yhteistyössä yritysten kanssa, kuten eri toimialueille kohdennetut Hackfest-tapahtumat ja räätälöidyt yrityskoulutukset sekä ryhminä toteutettavat puolustus/hyökkäysharjoitukset (red team/blue team).

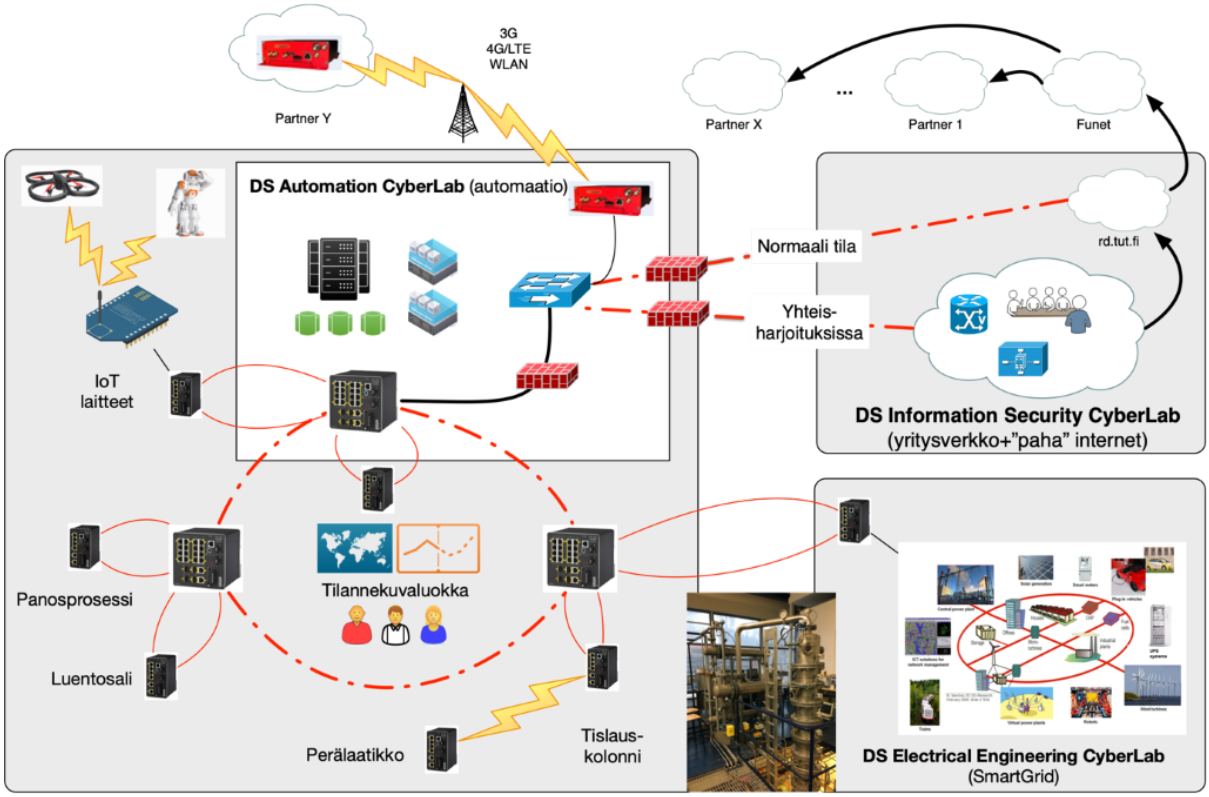
Ympäristöön ytimenä on virtualisointi klusteri, jossa on ajossa automaatiojärjestelmien sekä laboratorion tutkimusta ja opetusta tukevia muita palveluita. Virtualisoinnin

toteutuksessa on huomioitu automaation tietoverkkojen erityistarpeet. Yksittäisiä virtualisoituja palvelimia on päivittäisessä käytössä 50-150. Virtualisointiympäristön merkitys opetuksen ja tutkimuksen mahdollistajana on erittäin suuri ja sen tehokas hyödyntäminen mahdollistaa ympäristön joustavan ja luotettavan hyödyntämisen osana muuttuvia opetus- ja koulutustarpeita. Virtualisoinnin järkevä käyttö myös nopeuttaa merkittävästi ylläpidon työtehtäviä ja pienentää muutosten toteuttamiseen kuluvia resursseja. Virtualisointi on edellytys tietoturvaan liittyvässä tutkimuksessa vaaditulle mielekkäälle jatkuvuus- ja häiriöhallinnalle sekä opetustilanteiden vaatima nopea palautuminen.

LABORATORION IT-JÄRJESTELMÄ

IT-järjestelmän (Kuva 3) runko on teollisuustasoinen valokuiturengasverkko, joka on rakennettu moderneja teollisuusympäristöön soveltuvia komponentteja käyttäen. Se tukee nopeaa vikasietoisuutta kaapeliongelmien varalta sekä useita teollisuudessa standardoituja tietoliikenneprotokollia. Runkoverkko yhdistää sähkötalon kolme eri siipeä yhdeksi kokonaisuudeksi.

Verkon tietojenkäsittelyinfrastruktuurin ytimenä toimii kaksi VMware vSphere -klusteria, jotka koostuvat tällä hetkellä seitsemästä palvelimesta, joissa on 68 CPU:ta, 1 teratavu keskusmuistia, 58 teratavua massamuistia, 10Gbs levypalveluverkosta, vikasietoisesta kahdennetusta verkkoinfrastruktuurista sekä varavoimalla varmistetusta virransyötöstä. Klusteri tarjoaa ympäristön tukijärjestelmille ja ratkaisuille, sekä koulutus- ja tutkimustarpeisiin.



Kuva 3: Tampereen yliopiston laboratorioiden IT-järjestelmän periaatekuva

LABORATORION AUTOMAATIOJÄRJESTELMÄT

Kyberlaboratorioon kuuluu useita eri automaatiojärjestelmiä ja -laitteita. Näistä laajimmat kokonaisuudet ovat

- Tislauskolonni ja sitä ohjaava Valmet DNA automaatiojärjestelmä
- Panosautomaatioprosessia simuloiva säiliöprosessi toteutettuna Beckhoff PLC-ympäristöllä
- Taajuusmuuttajajärjestelmä toteutettuna Siemen S7-tekniikalla
- Paperikoneen perälaatikko, jonka ohjaus on toteutettu osaksi tislauskolonnin Valmet DNA-automaatiojärjestelmää
- Langaton taloautomaatiojärjestelmä, joka koostuu useista eri pientoteutuksista
- CSST-harjoitusympäristö, joka mahdollistaa laboratorion laajentamisen automaatioverkkotasolla eri etäpisteisiin

VALMET DNA AUTOMAATIOJÄRJESTELMÄ

Laitoksen teollisenmittakaavan alkoholitislausprosessia, kolonnia, (Kuva 4) ohjaa Valmet DNA -automaatiojärjestelmä. Prosessi on poikkeuksellinen opetus- ja tutkimusympäristö mittakaavansa takia ja vastaavaa ympäristöä ei ainakaan Tampereen yliopistojen laboratorioista löydy. Sitä hyödynnetään opetuksessa ja tutkimuksessa jatkuvasti. Ympäristö oli Valmet Automaation toinen palvelinten osalta virtualisointiin perustuva automaatiojärjestelmä maailmassa.

Kuva 4: Teollisen mittakaavan kaksikerroksinen alkoholintislausprosessi (Kolonni)

PANOSAUTOMAATIOPROSESSIA SIMULOIVA SÄILIÖPROSESSI (BECKHOFF PLC)

Panosprosessit ovat yleisiä teollisuuden eri osa-alueilla. Ne ovat prosesseja, joissa tuotetaan äärellinen määrä tuotteita (panoksia) tietyn reseptin mukaisesti määritellyistä raaka-aineista, hyödyntäen kemiallisia, fysikaalisia tai biologisia tapahtumia. Laboratoriossa on pienoismalli eräästä panosprosessista, sellunkeittolaitteistosta, jota ohjataan Beckhoffin ohjelmoitavalla logiikalla. Koska pienoismalleja on vain yksi, siitä on tehty simulaattorisovellus NodeJS:ää hyödyntäen. Opiskelijat voivat ohjelmoida itse laitteiston ohjaamisen tarkoitetun sovelluksen, jonka toimintaa testataan simulaattorilla. Simulaattori ja sovellus kommunikoivat keskenään OPC UA –protokollalla. Sovellusta voi myös kokeilla pienoismallin kanssa.

SIEMEN S7 -YMPÄRISTÖ JA SÄHKÖMOOTTORIN OHJAUS

Tässä järjestelmässä on Siemensin ohjelmoitava logiikka (PLC), jota ohjelmoidaan Simatic STEP 7 -ympäristössä. Järjestelmässä on myös sähkömoottori, jonka ohjaus logiikalla voidaan tehdä, jotta opiskelijat oppivat tämän tyyppisen ohjaustavan käyttöä.

PAPERIKONEEN PERÄLAATIKKO -JÄRJESTELMÄ

Osana Valmet DNA -järjestelmää on erillinen koelaitteisto, jossa simuloidaan paperikoneen perälaatikon dynamiikkaa. Tätä järjestelmää käytetään säädön riippuvuuksien ja dynamiikan opetuksessa.

LANGATON TALOAUTOMAATIO

Erilaiset langattomat ohjausjärjestelmät sekä etäyhteydet eivät enää ole vain teollisuuden juttu, vaan ohjaustekniikkaa käytetään myös taloyhtiöissä sekä yksityisihmisten kodeissa ja kiinteistöissä. Tämän takia laboratoriossa on langatonta tekniikkaa hyödyntävä taloautomaation ohjausjärjestelmän demoympäristö.

CSST-HARJOITUSYMPÄRISTÖ (CONTROL SYSTEM SECURITY TRAINING)

CSST-harjoitusympäristö on DSA CyberLabista kutakin teollisuuden auditointi- tai puolustustyöpajaa varten koostettu kokonaisuus. Ympäristössä olevia järjestelmiä voidaan mukauttaa tarpeen mukaan sekä laajentaa osallistujien omilla laitteilla. Kulloinkin tarpeeseen valittua kokonaisuutta hyödynnetään opetuksessa esimerkiksi automaation tietotekniikkaa käsittelevillä kursseilla ja osana yrityksille suunnattuja hands-on -harjoituksia. CSST-harjoitusympäristö on siirrettävissä ja sen suunnitteluperiaatteena on DSA CyberLabin automaatioverkon vieminen yrityksen tiloihin yrityskoulutusta varten.

MUUT IOT- JA AUTOMAATIOLAITTEET

Muita laboratorioon kuuluvia automaatiolaitteita ovat:

- MSDOS-ohjelmoitava internet-kykyinen Omron-ohjelmoitava logiikka
- Beckhoff ohjelmoitava logiikka + ohjelmointiympäristö (1 kpl Atom CPU, 1 kpl ARM CPU, 1 kpl i7 CPU)

- Cisco IE2000 ja IE4000 -sarjojen teollisuuskytkimillä tehty teollisuusautomaatiojärjestelmän runkoverkko. Kytkee kolme siipeä yhdeksi vikasietoiseksi automaatioverkoksi.
- Cisco IR829 ja IR1101 -reitittimillä toteutettu automaatioverkon etälaajennusratkaisu
- Cisco ASA 5512-X -etäyhteyspiste
- AJECO monikanavainen tietoliikennereititin - turvallisen ja luotettavan etäkäytön järjestelmä kriittisen infrastruktuurin järjestelmien tarpeisiin
- National Instruments PLC + Cube kääntöheilurijärjestelmä
- Valmet DNA -salkku, joka sisältää kaksi Valmet SR1-prosessiasemaa ja automaatiojärjestelmän. Salkulla voidaan mallintaa useita erityyppisiä automaatioprosesseja.
- Vacon inverter -salkut (2kpl), jotka toimivat yhdessä Redlion HMI -paneelin kanssa mallintaen eri taajuusmuuntajien käyttötapauksia
- pienoismallihöyrykone, jonka automaatiota tehdään opiskelijaprojekteina (Projektin aloitus 2020)
- Vaisala ROSA -tiesääasema, joka on kytketty omaan pilviratkaisuun MQTT-tiedonvälitystavalla.
- sekä lukuisia muita pienoisautomaatiolaitteita ja toimistointegraatioon tarvittavia tietoliikenneratkaisuja.

EHDOTUS LABORATORION HYÖDYNTÄMISESTÄ VERKOSTOSSA

Työelämäkoulutus yhdessä yritysten kanssa

Automaatiorunkoverkkoon verkotettu tilanneluokka sekä virtuaalikoneisiin pohjautuva toimintamalli on yhteistyön perusta. Mallina voidaan käyttää luokassa aiemmin järjestettyjä yrityskoulutuksia sekä Hackfest-tapahtumia. Työssä käyville opiskelijoille mikroluokka on tarjonnut mahdollisuuden harjoitella turvallisesti automaatioverkkojen tutkimiseen tarvittavia taitoja, kuten verkkotopologian muodostusta, haavoittuvuuksien etsintää ja verkkoliikenteen nauhoitusta ja analysointia. Mikroluokan ja muidenkin fyysisten laboratoriotilojen käyttöä rajoittaa ympäristön toiminnan edellyttämä automaation erikoisosaaminen sekä ympäristön käyttöön liittyvä työturvallisuuskoulutus.

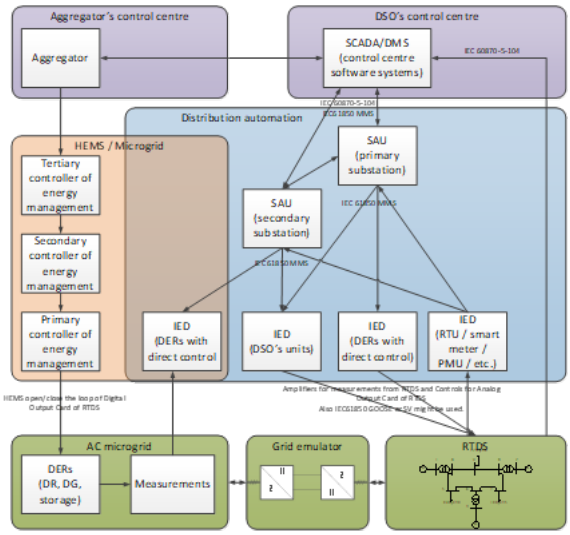
Työelämäkoulutus korkeakoulujen yhteistyöverkoston kanssa

Automaatiotekniikan laboratoriolla on aikaisemmin ollut yhteistyötä Oulun yliopiston kanssa, missä Oulun yliopistolle tarjottiin Tampereen puolelta verkkoinfrastruktuuri, virtuaalikoneet ja muu laitteisto, jota Oulun yliopiston väki sitten hyödynsi projektissaan etäyhteyttä käyttäen. Tämän kaltaista yhteistyömallia voidaan käyttää myös muiden verkoston oppilaitosten kanssa.

Laboratorion perusratkaisu on kehitetty Tampereen korkeakoulukonsernissa tarvittavan haastavien laboratorioympäristöjen opetuskäyttöä varten. Tämän toimintamallin laajentaminen Tampereen ammattikorkeakoulun automaatio-opetuksen käyttöön evaluoidaan tämän hankkeen osana. Malli mahdollistaa erikoisosaamista vaativan ympäristön teknisen tarjoamisen myös verkoston muille korkeakouluille.

DEPENDABLE SYSTEMS - ELECTRICAL ENGINEERING CYBERLAB, TAMPEREEN YLIOPISTO, SÄHKÖTEKNIIKKA

Sähkötekniikan kyberlaboratorio (DSE CyberLab, RTDS laboratory) koostuu smart grid -sähköverkkolaboratorioista, joissa kehitetään ja testataan sähkönjakeluun liittyvää automaatiota ja toiminnallisuutta. Laboratorio edustaa kriittisen infrastruktuurin sovellusaluetta kyberturvallisuuden tutkimusalassa. Järjestelmässä esitellään myös laaja joukko automaation reaaliaikaisuuteen liittyviä vaatimuksia sekä automaatiosuunnittelumalleja.



Laboratorion perusta on RTDS (Real-Time Digital Simulator), joka simuloi sähkönsiirtojärjestelmää reaaliajassa ja tarjoaa analogiset sekä digitaaliset sisään- ja ulostulot automaatiojärjestelmän laitteisto- ja ohjelmistokomponenteille. Laitteisto- ja ohjelmistokomponenteista tulee osa simulaatiota ja siksi simulaatioita kutsutaankin nimityksillä hardware-in-the-loop sekä software-in-the-loop. Toinen fyysisten järjestelmien tila on mikroverkkolaboratorio, joka edustaa loppukäyttäjää, jolla on mahdollisuus omavaraiseen energian tuotantoon, varastointiin ja joustavuuteen (kysyntään vastaaminen) sähköä kuluttavien laitteiden lisäksi. Nämä kaksi fyysistä järjestelmää voidaan yhdistää käyttäen tehovahvistinta. Laboratoriojärjestelmiä voidaan käyttää muun muassa sähköasemien automaation ja jakeluautomaatioratkaisujen tietoturva testaamiseen.

TAMPEREEN AMMATTIKORKEAKOULU

Kuinka selvitys on tehty?

TAMKissa on kerätty tietoa koulutusten ja ympäristöjen vastuuhenkilöiltä sekä asiantuntijoilta, jotka ympäristöjen kanssa toimivat. Tietojen keräämisen pohjalta on muodostettu tämä selvitys.

Yhteenveto TAMKin tilanteesta

TAMKissa kaikki ympäristöt ovat pääsääntöisesti koulutusympäristöjä eikä tutkimukselle ole omia dedikointuja ympäristöjään. Kyberturvallisuuden koulutusta järjestetään pääasiallisesti tietotekniikan ja tietojenkäsittelyn koulutuksissa ja merkittävimmät ympäristöt ovat näiden koulutusten ympäristöjä. Kyberturvallisuuteen liittyy suoraan Kyberlabra, tietotekninen muusta verkosta eriytetty ympäristö. Myös verkkolabraa käytetään kyberturvallisuuden opetukseen lähinnä verkon puolustamiseen liittyvissä asioissa. WPK-verkossa tehdään liikenteen ja uhkatilanteiden havainnointia ”aidossa ympäristössä”. Tämän lisäksi kyberturvallisuuteen liittyvissä koulutuksissa käytetään ja olisi mahdollista käyttää jonkin verran muuta infraa.

TAMKilla on olemassa prosessit siitä, kuinka tiloja ja ympäristöjä voidaan hyödyntää muiden toimesta (tila- ja asiantuntijakustannukset). Näiden prosessien puitteissa kyberturvallisuuteen liittyviä ympäristöjä voi hyödyntää myös hankkeen muut toimijat. TAMKin ympäristöjä voi hyödyntää verkoston laajuudella paikallisesti tilanteissa, joissa tarvitaan tilaa tai ratkaisuja, joita TAMKin ympäristöt tukevat. Ympäristöissä voidaan tehdä erilaisia harjoitteita ja testaustoimintaa mutta melko usein se vaatii tilanteen mukaista räätälöintiä. Rajoitteita asettaa erityisesti ohjelmistojen lisenssointi.

Vuoden 2019 alusta TAMKin omistajaksi tuli Tampereen yliopistosäätiö ja näin tilojen omistus siirtyi yliopistolle. Tämä määrittää omalla tavallaan tulevaisuudessa ympäristöjen käyttöä ja kehittämistä. Yhteistyössä yliopiston kanssa tullaan tätä suunnittelemaan kyberturvallisuudenkin osa-alueen puitteissa.

TAMKIN YMPÄRISTÖT

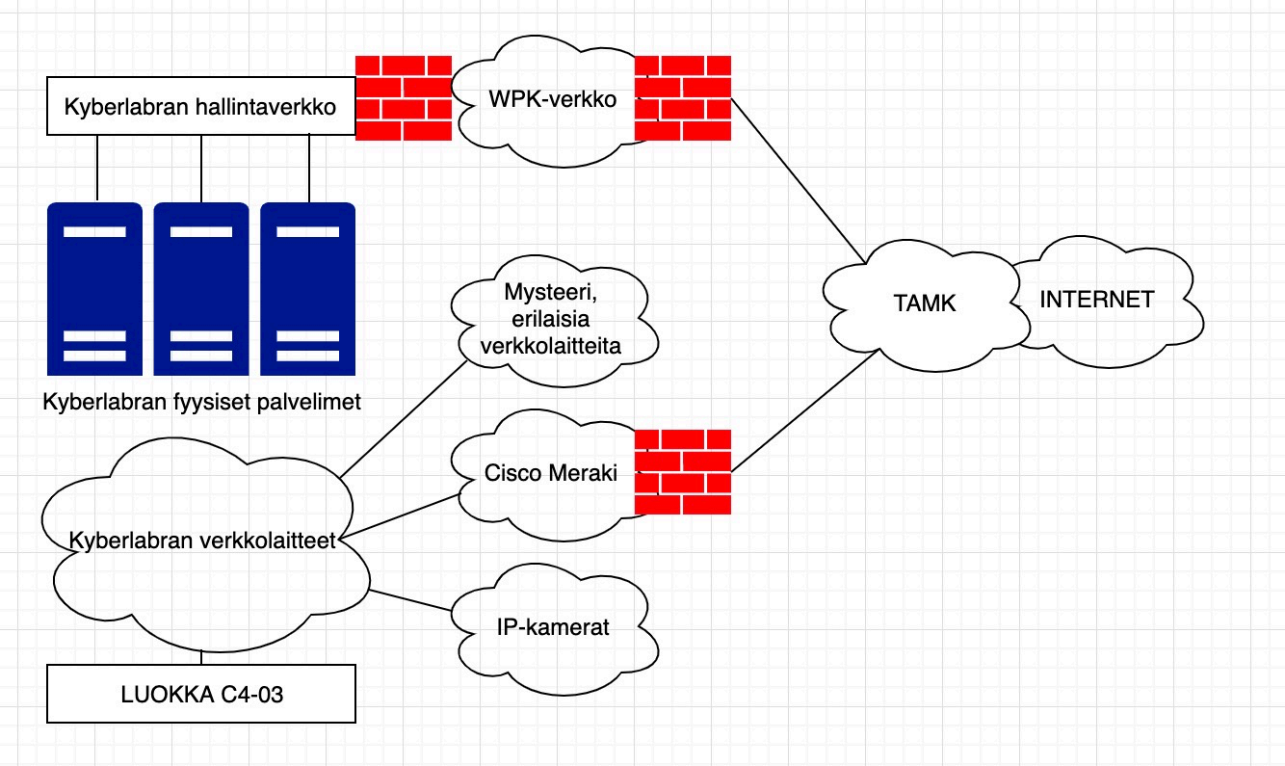
KYBERLABRA

Kyberlabra on WPK-verkosta (tarkemmin myöhemmin) ja myös muusta TAMKin tietokoneverkosta sekä Internetistä palomuureilla erotettu kyberturvallisuuden teknisiin asioihin, erityisesti testaamisen opettamiseen, liittyvä ympäristö. Kyberlabran perusta on virtualisoidut palvelimet, joiden avulla toteutetaan erilaisia ympäristöjä opetustarpeiden mukaisesti. Kyberlabraan saa yhteyden luokan työasemilta, joille on asennettu erilaisia virtuaalikoneita opiskelukäyttöön. Työasemien ja palvelimien lisäksi kyberlabrassa on erilaisia verkkolaitteita (ip-kameroita, NAS-tallennuslaitteita, jne). Kyberlabran verkko on toteutettu omilla erillisillä verkkolaitteilla. Kyberlabrassa on myös erillinen Cisco Meraki -järjestelmällä toteutettu verkko, joka mahdollistaa mm. langattomat yhteydet sekä etäyhteydet Internetin kautta sekä Meraki-tekniikkaan, mm. valvontakameroihin liittyvät harjoitteet.

Pääsääntöisesti kyberlabrassa toteutetaan tunkeutumistestaukseen ja haavoittuvuusanalyysiin liittyviä harjoituksia.

Kyberlabran laitteet:

- Luokan C4-03 jokaisella työasemalla (24 työasemalla) virtuaalikoneita
- Kolme palvelinta, joilla 30 ”pysyvää” virtuaalipalvelinta sekä lukuisia hetkellisiä/tarpeen mukaan käyttöön otettavia virtuaalikoneita
- Lukuisia IP-kameroita sekä NAS yms. verkkolaitteita
- 2 L3-kytkintä ja 6 L2-kytkintä
- Cisco Meraki -ympäristössä 2 palomuurireititintä, kytkin ja 2 ip-kameraa
- Paloalto-palomuuri, jolla toteutettu 15 virtuaalipalomuuria



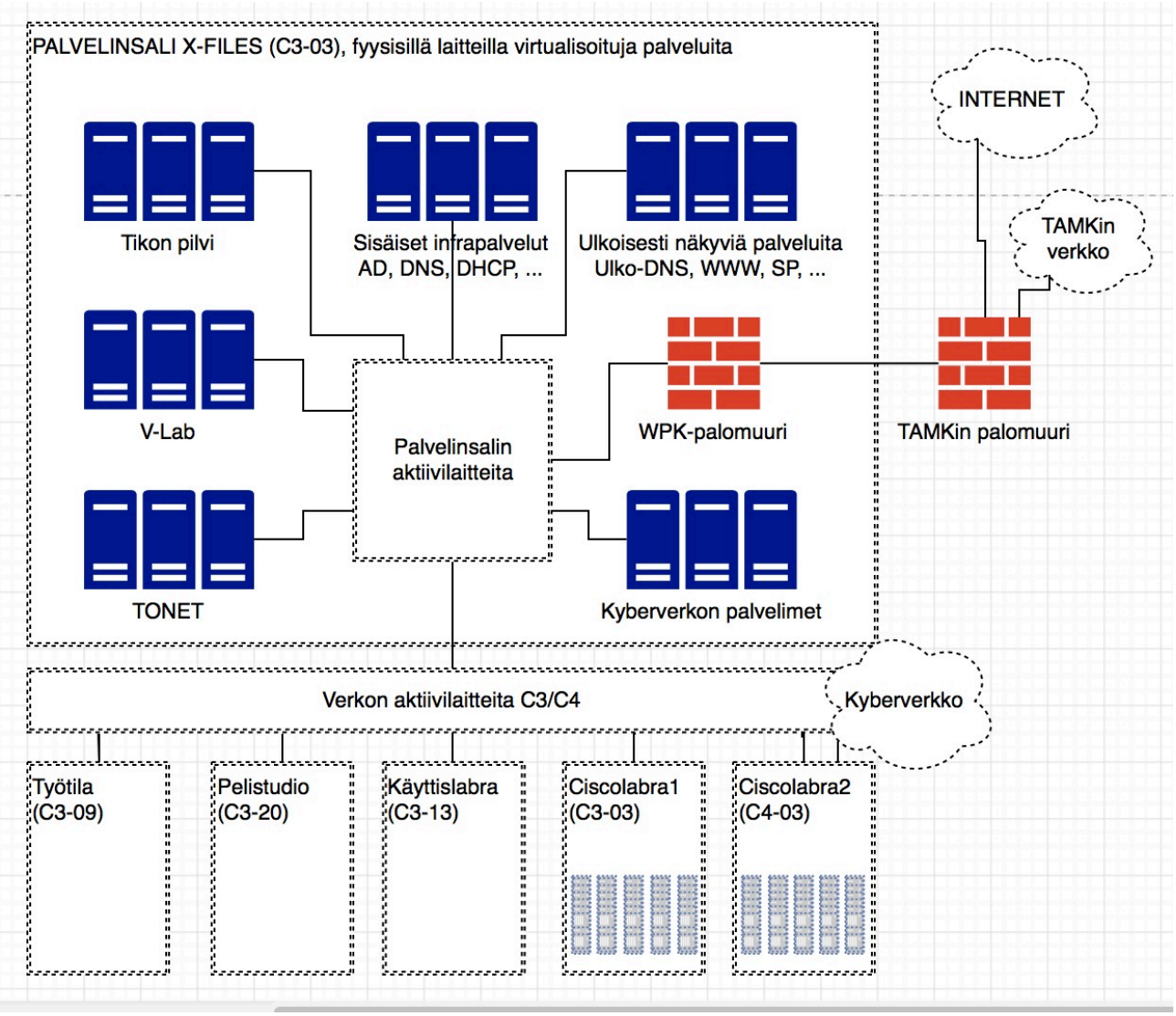
Kuva 1. Kyberlabran topologia

Kyberlabran toimintoja ei ole automatisoitu vaan asetukset määritetään tarpeen mukaan. Verkon ylläpidosta vastaa opettajat, jotka opintojaksoja pitävät ja heillä on ollut apunaan WPK-verkon harjoittelijat.

Kyberverkkoa voidaan käyttää työelämäkoulutuksiin mutta ympäristö tulee räätälöidä erikseen jokaista käyttökertaa varten. Hankeen verkoston puitteissa kyberlabra on käytettävissä mm. testaustoiminnan kouluttamiseen TAMKin yleisten tila- ja asiantuntijapalveluiden prosessien mukaisesti.

WPK-VERKKO JA TIETOVERKKOLABRAT

WPK-verkko on tietojenkäsittelyn koulutuksen TAMKin verkosta erotettu verkkoympäristö. Se on ollut toiminnassa TAMKissa jo 20 vuotta. WPK-verkossa jäljitellään erilaisia suurehkon yrityksen verkkoympäristön toimintoja ”oikeassa ympäristössä”. WPK-verkkoon kuuluu n. 100 työasemaa sekä 30 pääosin virtualisoitua palvelinta. Tämän lisäksi WPK-verkossa on palvelimia, joita voidaan käyttää tarpeen mukaan erilaisten koulutusten apuna.



Kuva 2. Suuntaa-antava kuva WPK-verkosta

Kyberturvallisuuteen liittyen WPK-verkko toimii lähinnä erilaisten projektitöiden reaalimaailman kaltaisena ympäristönä. WPK-verkkoon on toteutettu mm. liikenteen seurantaan ja kyberuhkien havainnointia. Tämän lisäksi WPK-verkon palvelimille on luotu virtuaalikoneita kyberturvallisuuden koulutusten tarpeisiin (esim. opiskelijoille omia virtuaalikoneita ylläpidettäväksi/kovennettaviksi).

WPK-verkko mahdollistaa Kyberlabran toiminnan ja sen ylläpito avustaa kyberlabran ylläpidossa ja toimintojen käyttöönotoissa sekä kehittämisessä. WPK-verkon ylläpidosta vastaa tietojenkäsittelyn opettajat ja ylläpitotyötä tekee siihen palkatut harjoittelijat.

Kahden luokkatilan C3-03 ja C4-03 työasemat on liitetty WPK-verkkoon ja näiltä työasemilta on yhteydet myös luokkatilojen omiin labraverkkoihin. Luokkatiloissa on laitekaapit. Laitekaapeissa on erilaisia aktiivilaitteita, joilla voidaan luoda monenlaisia tietoverkkoympäristöjä. Kyberturvallisuuteen liittyen labroissa tehdään verkon suojatilanteita sekä testataan niitä erilaisia hyökkäysvektoreita vastaan. Erityisen hyvin tähän toimintaan soveltuu luokkatila C4-03. Tämän lisäksi luokan C4-03 työasemilta on yhteys Kyberlabraan.

Luokkatilassa C4-03 on 24 opiskelijakäyttöön tarkoitettua työasemaa sekä 1 opettajakäyttöön tarkoitettu työasema. Jokaiselta työasemalta on pääsy tilan labralaitteille sekä Kyberlabraan. Luokassa on labralaiteta seuraavasti (noin):

- 12 palomuuria
- 30 reititintä
- 24 reitittävää kytkintä
- 24 kytkintä

TIETOLIIKENNETEKNIIKAN LABRA

TAMK tietoliikennelaboratoriossa on langattomien signaalien/verkkojen tutkimiseen signaaligeneraattoreita, spektrianalysaattoreita sekä piirianalysaattoreita useita eri malleja. Taajuusalue yltää suurimmassa osassa laitteissa 6GHz:iin (spektrianalysaattoreita löytyy jopa 28GHz:iin). Modulaatiomenetelmistä löytyy kaikki tämän päivän verkkotekniikat, kuten WLAN, 2G, 3G, 4G/LTE. Tietoliikennelaboratoriossa on myös häiriösuojattu huone, jossa pystytään tekemään mm. mittauksia oikeassa verkossa/päätelaitteella ilman kaupallisten verkkojen häiriintymistä. Häiriösuojattua tilaa voidaan myös käyttää tarkoituksellisen, tahallisen häirinnän demonstroimiseen (mm. vastaanottimien tukkeutumiseen voimakkaan häiriösignaalin vaikutuksesta), ilman huolta kaupallisten verkkojen/taajuusalueiden toimintahäiriöistä.

LISENSSOINTI

TAMKin tietoverkko- ja kyberlabroissa käytetään laitteilla ja palvelimille ohjelmistoja, joissa on “oppilaitoslisenssi”. Nämä lisenssiehdot saattavat tietyissä tapauksissa estää ympäristöjen hyödyntämisen kaupalliseen tarkoitukseen. Samoin verkkolabrassa on laitteita, jotka on hankittu ehdoilla, jotka rajoittavat niiden käyttöä kaupallisessa tarkoituksessa. Tulisi aina tapauskohtaisesti selvittää, milloin lisenssi/hankintaehdot ovat esteenä toiminnalle.

MUITA KYBERTURVALLISUUTEEN MAHDOLLISESTI LIITTYVIÄ YMPÄRISTÖJÄ TAMKISSA

TAMKissa on ympäristöjä, joita voi hyödyntää monin tavoin. Laboratorioissa on käytettävissä hyvin paljon erilaisia laitteita. Näissä ei ole erillistä kyberturvallisuuden fokusta tällä hetkellä olemassa. Mm:

- Titenet: tietotekniikan palvelimet, joille asennetaan virtuaalikoneita eri tarpeiden, ohjelmistotuotantoa, versionhallintaa
- Sulautettujen järjestelmien opetusympäristöjä, mm. IoT-tekniikoita
- Ajoneuvotekniikan laboratorio
- Automaatiotekniikan laboratorio
- Konetekniikan laboratorio
- Rakennuslaboratorio
- Sähkövoimatekniikan laboratorio
- Heat Lab: terveys- ja hyvinvointiteknologian laitteita
- Taitokeskus: sairaanhoitopiirin koulutuskeskus, simuloitu sairaalaympäristö

OULUN YLIOPISTO

Teknisistä tutkimusympäristöistä:

RADAMSA: HTTPS://WWW.EE.OULU.FI/RESEARCH/OUSPG/RADAMSA

Radamsa on avoimeen lähdekoodiin perustuva fuzzeri, jolla generoidaan käyttäjän syötteen pohjalta mutaatioita automaattisesti. Radamsaa käytetään luomaan suuri määrä syötettä muistuttavia uusia syötteitä, joiden pohjalta varsinainen testaus on helpompi suorittaa. Koska Radamsa perustuu avoimeen lähdekoodiin, sen ottaminen osaksi tutkimusympäristöjä on yksinkertaista.

Koulutusympäristöistä:

Oulun Yliopistolla on olemassa kyberturvallisuutta opettavia kursseja, joista tosiaan on tehty yhteenveto jo aiempaan raporttiin. Osassa kursseista kyberturvallisuutta tosin vain sivutaan, joten ne eivät sovellu ainakaan suoraan varsinaisiksi kyberturvallisuuskoulutuksiksi. Näitä varsinaisesti kyberturvallisuutta opettavia kursseja joita jo nyt voitaisiin periaatteessa tarjota ovat lähinnä:

Tietojenkäsittelytieteiden tarjoama yleinen Tietoturva-kurssi 811168P, sekä Tietoteknikan tiedekunnan käytännönläheisempi Computer security-kurssi 5521155S.

Selvitys Oulun yliopiston teknisistä koulutusympäristöistä

Oulun yliopiston tekniset koulutusympäristöt

Oulun yliopiston kyberturvallisuuskoulutuksen eri osiot keskittyvät antamaan ICT-alan opiskelijoille ammattitaitoa järjestelmä- ja ohjelmistokehityksen tietoturvallisesta toteutuksesta. Koska koulutus ja tutkimus on tähän asti painottunut ohjelmistojen turvallisuuden kehittämiseen, kyberturvallisuuskoulutuksen järjestämiseen ei ole vaadittu erillistä muusta verkosta eristettyä kyberympäristöä.

Oulun yliopistolla on kuitenkin käytössään joitakin hankkeen kuvauksen mukaisia ympäristöjä, joita muutkin verkoston jäsenet voivat tapauskohtaisesti määritettävien reunaehtojen puitteissa mahdollisesti käyttää.

TIETOKONELABORATORIOT

Kyberturvallisuuskoulutuksen järjestelyissä hyödynnetään yliopiston tiloissa sijaitsevia tietokonelaboratorioita TS135 ja TS137, joiden työasemat (TS135 21 kpl ja TS137 27 kpl) kuuluvat tiedekunnan ITEENET-verkkoon. Työasemilta löytyy valmiudet virtuaalikoneiden käyttöön, joten erilaisten ympäristöjen hyödyntäminen ohjelmistotestauksessa on mahdollista. Tietokonelaboratorioiden omassa sisäverkossa onnistuu myös verkkopohjaisten projektien, työpajojen ja harjoitustöiden toteuttaminen.

LASKENTAKLUSTERIT

Tieto- ja sähkötekniikan tiedekunnalla on käytössään 20 Linux-laskentapalvelinta, joiden lisäksi yliopiston tietohallinnolta löytyy 10 tutkimuskäyttöön tarkoitettua palvelinta. Palvelimia hallinnoi Oulun yliopiston ICT-palvelut, ja niiden käyttö vaatii henkilökohtaisen opiskelija-, henkilökunta- tai kevyttunnuksen.

5G-TESTIVERKKO

Oulun yliopiston Linnanmaan kampuksen alueella on käytössä avoin 5G-testiverkko, jota on käytetty mm. Traficomin kanssa yhteistyössä järjestetyssä 5G Cyber Security Hackathonissa. Testiverkon avulla on mahdollista

luoda erilaisia virtuaalisia verkkoympäristöjä ja sitä kautta kouluttaa tietoturvakontrollien testausta. Verkon tutkimus- ja koulutuskäyttöä hallinnoi Centre for Wireless Communications (CWC).

MUITA MAHDOLLISESTI HYÖDYLLISIÄ YMPÄRISTÖJÄ

Oulun yliopistolta löytyy yllä kuvattujen lisäksi myös

- FabLab: digitaalisen valmistuksen tiloista löytyvien mittauslaitteiden käyttö laitteistojen tietoturvatestaukseen
- Itseohjautuva auto: käyttö mobiilin ohjelmistoympäristön, ohjausjärjestelmien ja tietoliikenneratkaisuiden kyberturvallisuuden testaukseen
- Sähkö- ja tietoliikennetekniikan häiriösuojattu huone

Oulun yliopisto on myös julkaissut ohjelmistojen tietoturvatestaukseen liittyvää materiaalia, joista muutkin verkoston jäsenet voivat koulutuksia järjestäessään hyötyä:

- https://github.com/ouspg
- https://gitlab.com/CinCan
- https://www.ee.oulu.fi/research/ouspg/Radamsa

Verkoston jäsenet voivat käyttää yliopiston julkaisemaa tietoturvakoulutusmateriaalia kunkin lisenssin mukaisesti koulutuskäyttöön.

ESITYS YHTEISKÄYTÖSTÄ

Lähtökohtaisesti kaikki Oulun yliopiston tutkimus- ja koulutusympäristöt vaativat henkilökohtaisen käyttäjätunnuksen käyttöä varten. Jos yliopiston ympäristöjä hyödyntävään koulutukseen osallistuu henkilöitä, joilla ei itsellään ole yliopiston käyttäjätunnusta, heille voi tilata tietohallinnolta kevyttunnuksen. Kevyttunnus toimii samoilla oikeuksilla kuin opiskelijatunnus, eli se antaa vierailijoille käyttöoikeuden työasemille ja laskentapalvelimille.

Yliopiston tietojärjestelmät eivät nykyisellään salli laajamittaista palvelujen tarjoamista koko hankeverkostolle, mutta yhteistoiminta koulutusten järjestämisessä voidaan määrittää tapauskohtaisesti. Jos verkoston jäsenet haluavat hyödyntää yliopiston tarjoamia ympäristöjä, heillä täytyy olla yliopiston henkilökuntaan kuuluva vastuuhenkilö joka toimii rajapintana verkoston ja yliopiston palveluita tarjoavien yksiköiden välillä ja tarvittaessa hoitaa tilavaraukset tilapalveluilta, tilojen valvonnan ja kevyttunnustilaukset tietohallinnolta. Tilavarausten ja tunnustilausten kulut määräytyvät tilapalveluiden ja tietohallinnon hinnastojen mukaan.

YHTEENVETO

Selvityksessä kuvattujen koulutusympäristöjen ja -materiaalien yhteiskäyttö koko hankeverkoston kesken on pääosin mahdollista sillä edellytyksellä, että reunaehdot ja yliopiston henkilökuntaan kuuluva vastuuhenkilö määritetään tapauskohtaisesti.

METROPOLIA

Metropolia ammattikorkeakoulun Espoon kampus jouduttiin äkillisesti sulkemaan helmikuussa 2019. Tämä vaikutti merkittävästi oppilaitoksen ympäristöihin ja erilaisiin tilajärjestelyihin.

Metropolia Ammattikorkeakoululla on tutkintoon johtavan koulutuksen tuottamista varten käytössä VMwaren teknologiaan perustuva virtualisointialusta, jonka käyttö on mahdollista oppilaitoksen sisäverkossa. Yleisesti oppilaitoksen tietokoneilla on käytössä oppilaitoskäyttöön lisensioituja Microsoftin työasema-, palvelin- ja sovellusohjelmistoja. Erillisiä kyberturvallisuuden oppimisympäristöjä ei ole käytössä.

Työpajoja varten on käytettävissä RaspBerry Pi -pienoistietokoneita sekä langattoman verkon itsenäisiä tukiasemia. Näiden avulla voidaan tuottaa paikallisesti koulutuskäyttöön tarkoitettuja ympäristöjä. Alustat ovat myös helposti muokattavissa erilaisten paikallisten toteutusten tarpeisiin.

Tietohallinnon kanssa käydyissä neuvotteluissa selvitettiin käytössä olevat opetusympäristöt sekä niiden käytettävyyttä työelämäkoulutusten järjestämiseen.

Selvitysten aikana havaittiin, että tietohallinnon tuottamat järjestelmät ja palvelut on suunniteltu ja toteutettu palvelemaan tutkintoon johtavaa koulutusta eikä niiden muokkaaminen yrityksille tarjottavien työelämäkoulutuksen tarpeisiin ole muutostöistä aiheutuvien kustannusten takia kannattavaa.

Sisäverkossa tarjottavien oppimisympäristöjen etäkäyttö edellyttää suojatun yhteyden (VPN) rakentamista jokaisen yhteistyökumppanin etätoimipisteeseen mikä osaltaan rajoittaa oppimisympäristöjen etäkäyttöä sekä aiheuttaa lisäkustannuksia.

Työpajakäyttöön tarkoitettuja pienoistietokoneympäristöjen asennus- ja asetustiedostoja voidaan jakaa verkoston toimijoiden kesken. Metropoliassa tällaista järjestelyä on testattu syksyllä 2019 järjestetyssä työpajassa.

TURUN AMMATTIKORKEAKOULU

KYBERTURVALLISUUDEN TEKNISET KOULUTUSYMPÄRISTÖT

Turun AMK:lla on tällä hetkellä käytössä tekniset harjoitusympäristöt kyberturvallisuustestauksen ja kyberpuolustuksen harjoitteluun. Lisäksi kehitteillä on erillinen ympäristö hyökkäysten havainnoinnin ja jäljittämisen harjoitteluun.

ETÄYHTEYDET JA PÄÄSYNHALLINTA

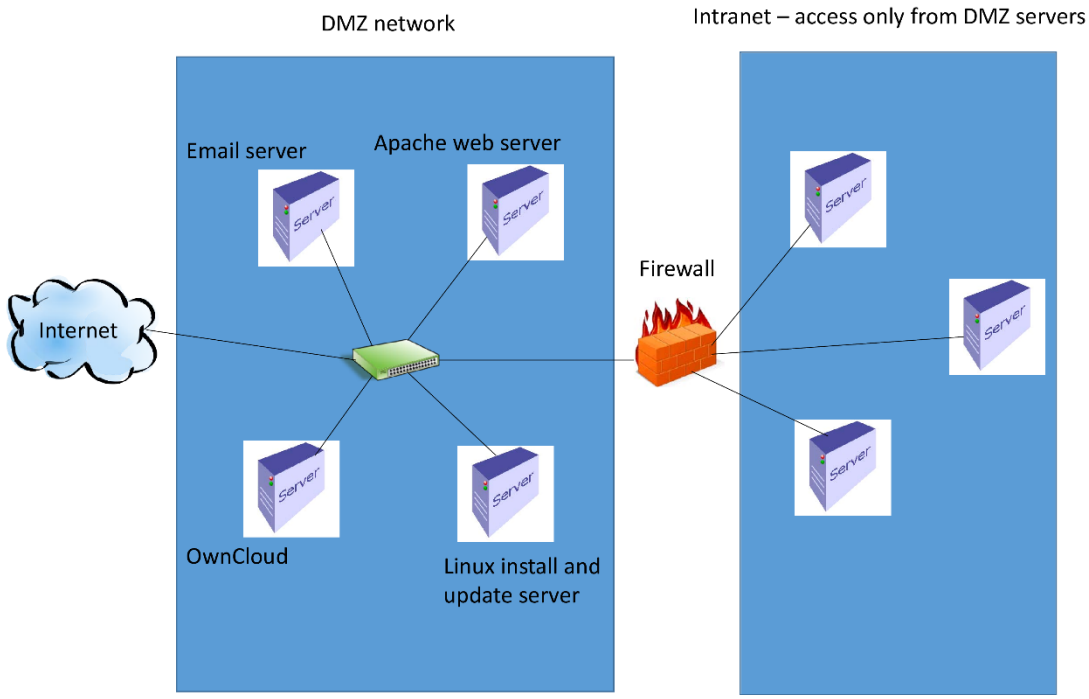
Teknisen ympäristön palomuuri toimii myös OpenVPN-reitittimenä. Etäopiskelijat lataavat itselleen AMK:n luoman Kali-linux virtuaalikoneen, johon on valmiiksi konfiguroitu etäyhteysasetukset. Virtuaalikone kysyy ensimmäisessä käynnistyksessä opiskelijanumeroa ja salasanaa, ja lataa AMK:n palvelimelta autentikointiperusteet ja yhteysavaimet. Jatkossa se muodostaa yhteyden automaattisesti ja ohjaa kaiken liikenteen harjoitusverkkoon. Näin vältetään harjoitusliikenteen vuotaminen vahingossa julkiseen verkkoon. Liikenteen ohjaus on tilapäisesti kytkettävissä pois päältä esimerkiksi ohjelmistopäivitysten noutoa varten. Opiskelija voi tarvittaessa kopioida yhteysasetukset ja -avaimet itselleen toiseen ympäristöön, koska esimerkiksi Windows-koneiden etäkäyttö on sujuvampaa Windows-työasemalla kuin Kalin avulla.

Etäyhteydet perustetaan palvelimella syöttämällä tekstitiedosto, jossa on listattu halutut opiskelijanumerot. Ohjelmisto tuottaa automaattisesti tarvittavat varmenteet ja pääsyoikeudet, ja palauttaa tulostettavaksi listan, jossa on kullekin opiskelijanumerolle generoitu salasana asetusten noutoa varten. Lista voidaan leikata opiskelijakohtaisiksi suikaleiksi jaettavaksi kontaktitunnilla, tai toimittaa sähköisesti. Jatkokehitystoimena on integroitua AMK:n IT-järjestelmiin, jolloin opiskelijanumeron perusteella voidaan noutaa sähköpostiosoite ja toimittaa salasana suoraan sähköpostitse.

Tällä hetkellä yhteysavainten voimassaoloaika on vakioitu ohjelmistossa. Myyntikoulutuksia varten aika kannattaa muuttaa konfiguroitavaksi, jotta voidaan helposti luoda eri kestoisia koulutuksia. Pääsyoikeuksien luontiohjelmisto on helppo myös integroida osaksi nettikauppaa tai muuta portaalia, jolloin pääsyoikeuksia voidaan myydä joustavasti ilman ihmistyötä.

KYBERTURVALLISUUSTESTAUS

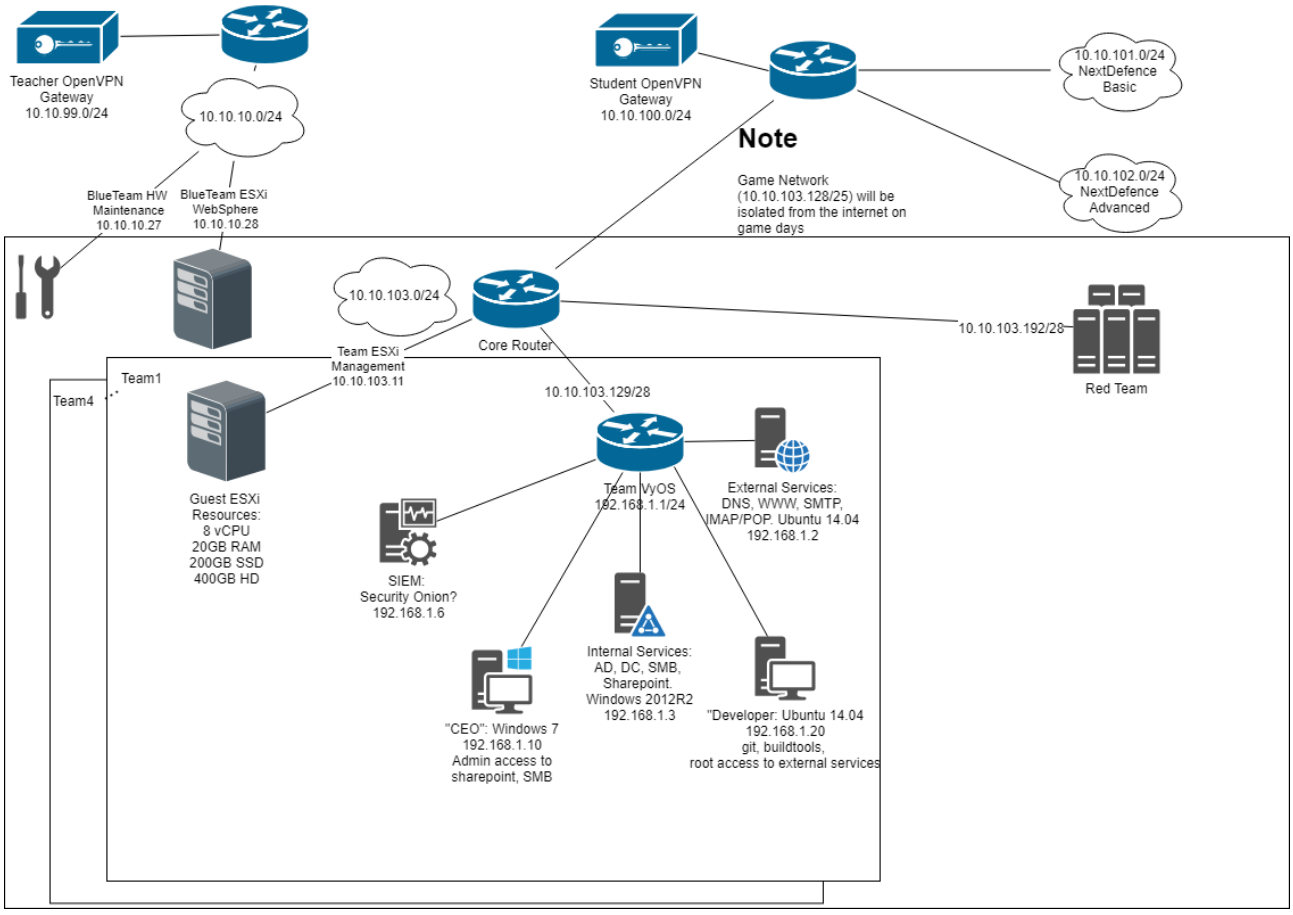
Harjoitusympäristö koostuu perus- ja jatkotasosta. Perustason ympäristössä on yhteensä kahdeksan Linux-palvelinta, joissa on joitakin haavoittuvuuksia. Neljä koneista on http-palvelimia. Pääsy suoraan ylläpitäjäksi ei ole koneissa mahdollista, vaan opiskelijan täytyy ensin löytää haavoittuvuus, jolla saa peruskäyttäjän tai daemonin oikeudet, ja sen jälkeen toinen, jolla käyttöoikeuden saa korotettua. Jatkotason ympäristö mallintaa pientä yritysverkkoa ja koostuu seitsemästä palvelimesta. Opiskelijan täytyy saada hallintaansa jokin neljästä DMZ-verkon palvelimesta, ja käyttää sitä reittinä sisäverkon kolmeen taustapalvelimeen.



Perustason ympäristössä harjoitellaan ohjatusti, kun taas jatkotaso on käytössä itsenäiseen opiskeluun. Jatkotasolla opiskelija saa yhden opintopisteen jokaisesta murretusta ja hyväksytysti raportoidusta harjoituskoneesta. Harjoitusympäristössä on lisäksi varastoituna viisi vaativampaa kohdekonetta, jotka eivät ole tällä hetkellä käytössä. Ympäristön haasteena on ylläpito, sillä osa koneista on jo vanhentuneiden Linux-jakeluiden päälle rakennettuja, ja niihin on mahdollista murtautua helposti luontihetken jälkeen löytyneillä yleisillä haavoittuvuuksilla.

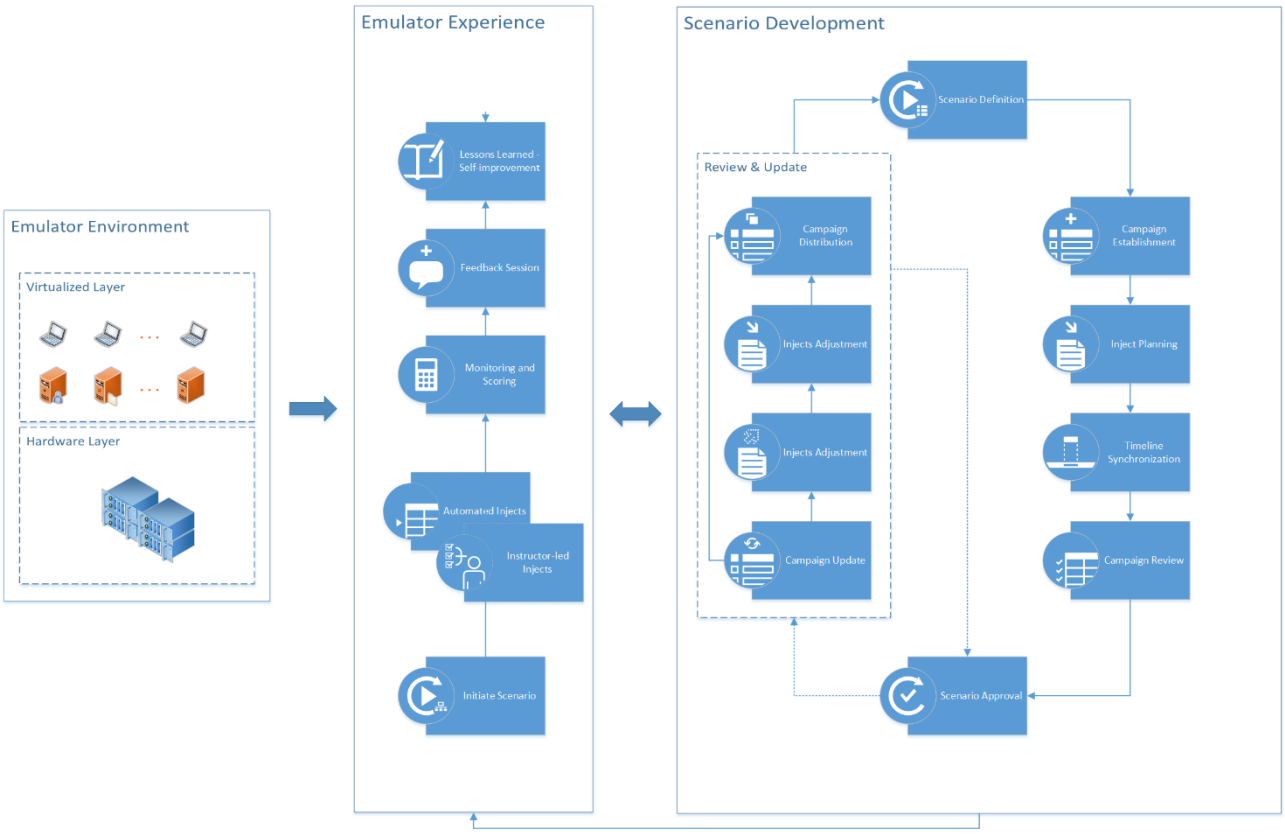
KYBERPUOLUSTUS

Kyberpuolustusympäristö on rakennettu sisäkkäisen virtualisoinnin avulla. Opiskelijat jaetaan tiimeihin, jotka toimivat MSSP:n roolissa PK-yritykselle. Tiimi saa kovennettavaksi ja monitoroitavaksi yhden virtuaaliympäristön, joka koostuu palomuurista/reitittimestä, ulkoverkon Linux-palvelimesta, sisäverkon Windows-palvelimesta, Linux-työasemasta, Windows-työasemasta sekä WiFi-tukiasemasta. Tiimillä on vapaat kädet muokata verkon asetuksia ja segmentointia, palomuuria ja koneita. Lisäksi tiimi pystyttää verkkoon SIEM:in erilliselle virtuaalikoneelle. Ympäristössä järjestetään yhden päivän mittainen harjoitus, jossa Red Teamit testaavat verkot. Ympäristö on pelillistetty siten, että samaan aikaan pelipalvelin testaa tiimien palveluiden toiminnan ja ylläpitää pistetilannetta kaikkien nähtävillä.



HYÖKKÄYSTEN HAVAINNOINTI JA JÄLJITTÄMINEN

Turun AMK:ssa on kehitteillä automaattinen uhkaemulaattori, jonka avulla voi harjoitella organisaation verkkoon jo päässeen hyökkääjän tunnistamista, jäljittämistä ja torjuntaa. Järjestelmä toimii automaattisesti, jolloin opiskelija voi käynnistää harjoituksen itsenäisesti, ja emulaattori tuottaa harjoitusympäristöön halutun tilanteen. Samalla harjoitukset voidaan pelillistää.



YKSITYISPILVI

Turun AMK on ottamassa laboratoriokäyttöön hyperkonvergenttia infrastruktuuria ja sen mahdollistamaa yksityispilveen pohjautuvaa ympäristöä. Nutanix-pohjainen ympäristö mahdollistaa tutkimus- ja harjoitusympäristöjen joustavan luonnin ja käyttöönoton. Alkuvaiheessa ympäristössä on kapasiteettia 250 yhtäaikaisen virtuaalipalvelimen ajamisen. Harjoitusympäristöt siirtyvät pilveen vaiheittain.

MALLI TEKNISTEN YMPÄRISTÖJEN HYÖDYNTÄMISELLE

Toimenpide 3.2: Kokonaiskuvan perusteella esitetään malli teknisten ympäristöjen hyödyntämiselle ja yhteiskäytön mahdolliselle laajentamiselle.

Tässä dokumentissa esitetään malli teknisten ympäristöjen hyödyntämiselle ja yhteiskäytön mahdolliselle laajentamiselle. Malli pohjaa toimenpiteen 3.1 tuloksiin ja yhteenvetoon.

Kaikilla hankkeen osapuolilla on lisäksi verkossa tapahtuvaa koulutusta ja muuta työelämälle soveltuvaa tutkintokoulutusta, jotka on rajattu tämän dokumentin ulkopuolelle. Niitä käsitellään hankkeen muissa dokumenteissa:

- Selvitys tutkintokoulutusten kyberturvallisuuteen liittyvistä osista (toimenpide 2.1.)
- Kyberturvallisuuden työelämäkoulutuksia yritysten tarpeisiin (toimenpide 2.3)
- Selvitys erikoistumiskoulutuksista (toimenpide 2.5)

YHTEENVETO

Toimenpiteen 3.1 ja TAMK:n ja TurkuAMK:n kybertestaus- ja kyberpuolustusympäristön yhteiskäyttötestin pohjalta kehitettiin malli, jonka pohjalta hankkeessa toimivien korkeakoulujen teknisten oppisympäristöjen yhteiskäyttöä voidaan työelämäkoulutuksissa toteuttaa. Malli on kuvattu luvussa 3 ja esitetty kuvassa 2.

Mallissa oletetaan, että työelämäkoulutus on päätetty toteuttaa ja sekä opetuksen järjestäjä ja oppimisympäristön tarjoaja pystyvät toteuttamaan koulutuksen sovittuna aikana. Mallissa oppimisympäristö sisältää tilat ja tietotekniset ratkaisut. Malli on jaettu hallinnolliseen ja opetuksen järjestämiseen liittyviin osiin. Mallin toimijat ovat opetuksen järjestäjä (OJ) ja oppimisympäristön tarjoaja (OT).

Hallinnollisessa osassa OJ huolehtii koulutukseen ilmoittautumisista, opintohallinnollisista järjestelyistä ja koulutuksen laskutuksesta. OT varaa tarvittavat tilat ja laskuttaa koulutuksesta sovitun osan OJ:ltä.

Opetuksen järjestäminen -osassa OJ vahvistaa tarvittavien tilojen ja laitteiden varauksen OT:lta. OT luo opettajien tunnukset oppimisympäristöön ja toimittaa käyttöohjeet ja tunnukset OJ:lle. OJ testaa yhteyksien toimivuuden ja luo työelämäkoulutettaville tarvittavat tunnukset. OJ ohjeistaa koulutukseen osallistujat ja pitää koulutuksen, jonka aikana OT valvoo oppimisympäristöä sovitulla tavalla. Koulutuksen jälkeen OT huolehtii oppimisympäristön siivoamisesta ja tunnusten poistamisesta.

Koulutuksen päätteeksi OJ kerää palautteen koulutuksesta ja toimittaa sen myös OT:lle. Molemmat reagoivat palautteeseen ja koulutusta kehitetään yhteistyössä palautteen perusteella.

1 YHTEISKÄYTTÖMALLIN RAJOITTAVAT TEKIJÄT

Toimenpiteessä 3.1 selvitettiin erilaisia mahdollisuuksia, miten teknisiä oppimisympäristöjä voisi käyttää koko verkoston laajuudella työelämäkoulutuksissa. Tässä yhteydessä havaittiin, että eri korkeakoulujen ympäristöihin liittyy useita yhteiskäyttöä rajoittavia tekijöitä. Tällaisia tekijöitä ovat esimerkiksi ympäristöjen räätälöintiin työelämäkoulutusten tarpeiden mukaisiksi tarvittavat resurssit. Lisäksi olemassa olevissa oppimisympäristöissä on suoraan yhteiskäyttöä rajoittavia tekijöitä kuten esimerkiksi kaupallisen käytön kieltävät lisenssit. Huomioitavaa on myös se, että ympäristöjä eri korkeakouluissa kehitetään jatkuvasti

ja tällöin myös edellytykset yhteiskäytölle voivat muuttua. Tärkeimmät rajoittavat tekijät korkeakouluittain on koottu taulukkoon 1.

Oppilaitos	Rajoitteet	Suora hyödynnettävyys
TurkuAMK		Kybertestaus- ja kyberpuolustusympäristöt hyödynnettävissä verkostolle ostopalveluna
TAMK	Räätälöintitarve, fyysisen läsnäolon tarve, lisenssit	
TTY	Räätälöintitarve, TTYn asiantuntijan tarve, lisenssit	Dependable Systems Automation CyberLab ja CSST-harjoitusympäristöt ovat käytettävissä työelämäkoulutuksiin TTYn asiantuntijoiden kanssa
OY	Räätälöintitarve, OYn asiantuntijan tarve	
Metropolia	Kampuksen sulkemisesta johtuen ei ympäristöjä tällä hetkellä	

Taulukko 1: Teknisiä ympäristöjä rajoittavat tekijät korkeakouluittain

2 SUORAAN HYÖDYNNETTÄVISSÄ OLEVAT YMPÄRISTÖT

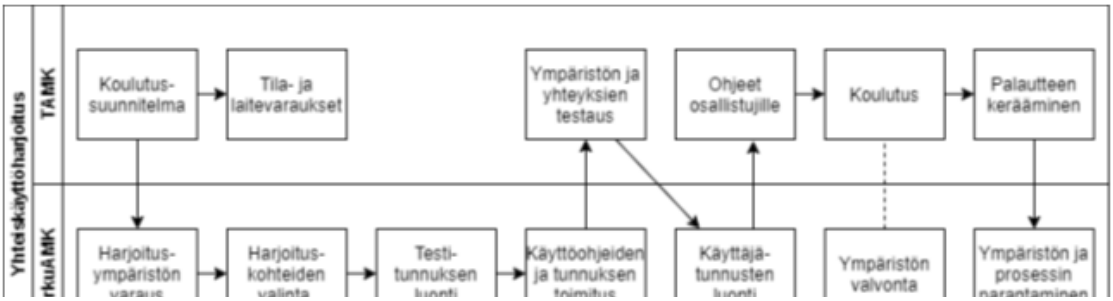
Yhteistyöverkostossa heti hyödynnettävissä olevia ympäristöjä on kaksi:

1. Turun ammattikorkeakoulun kybertestaus- ja kyberpuolustusympäristö on hyödynnettävissä hanketoimijoiden kesken yhteistyössä ja maksullisena palveluna.

2. Tampereen yliopiston automaatiotekniikan CSST-harjoitusympäristö (Control System Security Training) on toteutettavissa missä tahansa TTYn asiantuntijoiden toimesta vaatien toteutuspaikalta vain tilan ja sähköt. Tämä on saatavilla hanketoimijoiden keskuudessa työelämäkoulutukseksi maksullisena palveluna.

3 YHTEISKÄYTTÖHARJOITUS

TAMK ja TurkuAMK testasivat Turun ammattikorkeakoulun kybertestaus- ja kyberpuolustusympäristön yhteiskäyttöä keväällä 2020. Harjoituksessa TAMK huolehti osallistujille tilat ja laitteet harjoituksen ajaksi



Kuva 1: Yhteiskäyttöharjoituksen prosess 1

ja TurkuAMK huolehti harjoitusympäristöstä. Käytännössä siis Tampereelta käytettiin TurkuAMK:n järjestelmää etäyhteyden kautta. TAMK:n opettaja hoiti opetuksen ja TurkuAMK valvoi järjestelmän toimintaa harjoituksen aikana. Prosessi toimi kuvan 1 mukaan.

Harjoituksen pohjalta suunniteltiin yhteiskäyttömalli.

4 YHTEISKÄYTTÖMALLI

Mallissa oletetaan, että kyseinen koulutus on päätetty toteuttaa ja sekä opetuksen järjestäjä ja oppimisympäristön tarjoaja pystyvät toteuttamaan koulutuksen sovittuna aikana (koulutussuunnitelma). Malli ei ota kantaa esim. koulutuksen kustannusten arviointiin ja jakautumiseen, vaan nämä sisältyvät koulutussuunnitelmaan ja ne on selvitetty ja sovittu koulutussuunnitelmaa laadittaessa.

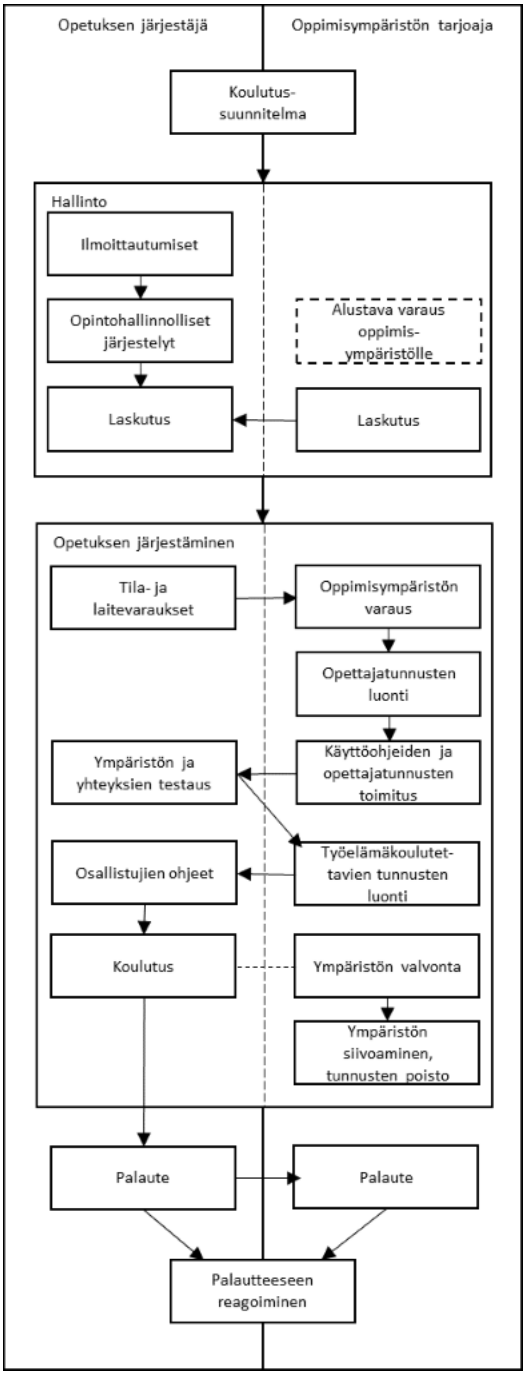
Mallissa oppimisympäristö sisältää tilat ja tietotekniset ratkaisut. Jos oppimisympäristöksi tarvitaan ainoastaan tila, voidaan käyttää tavallisen tilavuokrauksen prosesseja.

Malli on esitetty kuvassa 2. Mallin toimijat ovat opetuksen järjestäjä (OJ) ja oppimisympäristön tarjoaja (OT). Mallissa hallinnollinen osa ja opetuksen järjestämisen osa on eroteltu toisistaan.

OJ:n vastuulla hallinnollisessa osassa ovat ilmoittautumiset, opintohallinnolliset järjestelyt (esim. kulkuluvat, opintosuoritukset) ja koulutuksen laskutus. OT huolehtii oppimisympäristön alustavasta varauksesta ja laskuttaa koulutuksesta sovitun osan opetuksen järjestäjältä.

Opetusta järjestettäessä OJ vahvistaa tarvittavien tilojen ja laitteiden varauksen OT:ltä. OT luo opettajien tunnukset oppimisympäristöön ja toimittaa käyttöohjeet ja tunnukset OJ:lle. OJ testaa yhteyksien toimivuuden ja luo työelämäkoulutettaville tarvittavat tunnukset (tarvittaessa tunnusten luonti voidaan tehdä myös OT:n toimesta). OJ antaa ohjeet koulutukseen osallistujille ja pitää koulutuksen, jonka aikana OT valvoo oppimisympäristöä sovitulla tavalla. Koulutuksen jälkeen OT huolehtii oppimisympäristön siivoamisesta ja tunnusten poistamisesta.

Koulutuksen päätteeksi OJ kerää palautteen koulutuksesta ja toimittaa sen myös OT:lle. Molemmat reagoivat palautteeseen ja koulutusta kehitetään yhteistyössä palautteen perusteella.



Kuva 2: Yhteiskäyttömalli 1