

Toimenpide 3.1 Teknisten ympäristöjen selvitys – yhteenveto

Taustat

Tavoite 3. Kyberturvallisuuden testaus- ja pilotointiympäristöjen hyödyntäminen: kartoitetaan hankkeeseen osallistuvien 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.

Yhteenveto

Jokainen oppilaitos teki selvityksiä ja raportin omista teknisistä tutkimus- ja koulutusympäristöistään, joita käytetään, tai voidaan tulevaisuudessa käyttää, kyberturvallisuuteen liittyvissä asioissa. Tämän yhteenveton liitteinä (ei-julkisia, hanketoimijoiden käyttöön) ovat nuo oppilaitosten selvitykset.

Yhteiskäyttömahdollisuudet työelämäkoulutuksissa

Toimenpiteessä selvitettiin erilaisia mahdollisuuksia, miten teknisiä ympäristöjä voisi käyttää koko verkoston laajuudella työelämäkoulutuksissa. Ympäristöjen käytön laajentaminen ei ole yksiselitteinen asia vaan siihen liittyy paljon erilaisia reunaehtoja. Ympäristöt on luotu tiettyjen käyttötapojen ja tarkoitusten mukaisiksi ja niiden räätälöiminen muutostarpeisiin vaatii aina ympäristö hallinnoivan oppilaitoksen mukana oloa ja usein merkittävää työpanosta. Tämän lisäksi ohjelmistojen lisenssit voivat jopa estää järjestelmien käyttämisen muuhun kuin tutkintokoulutukseen.

Koko hankeryhmällä oli oikeastaan vain kaksi heti laajemmin hyödynnettävää teknistä ympäristöä: Turun ammattikorkeakoulun virtuaalisesti toteutettu ”kybertestausympäristö” on hyödynnettävissä laajemminkin hanketoimijoiden kesken yhteistyössä ja maksullisena palveluna. Tampereen yliopiston automaatiotekniikan CSST-harjoitusympäristö on toteutettavissa missä tahansa TAU:n asiantuntijoiden toimesta vaatien toteutuspaikalta vain tilan ja sähköt. Tämä on saatavilla hanketoimijoiden keskuudessa työelämäkoulutukseksi maksullisena palveluna.

Erillisenä toimenpiteenä on kehitetty mallia yhteistoiminnalle.

Tekniset ympäristöt

Oppilaitoksilla on merkittäviä teknisiä ympäristöjä laajasti erilaisilta sovellusalueilta. Suuria ”pääallekkäisyyksiä” ei ole. ICT- sekä automaatioala ovat ympäristöissä keskeisissä rooleissa. Ympäristöjen käyttötarkoitukset ja tavat ovat huomattavan erilaisia eikä niiden käytölle voi olla yhteistä mallia vaan se on tehtävä jokaisessa oppilaitoksessa itsenäisesti.

Teknisten ympäristöjen hyödynnettävyys laajemmin oppilaitoksen oman toiminnan ulkopuolella on erittäin haastava asia, johon liittyy paljon rajoitteita. Hankkeen aikana

teknisissä ympäristöissä on myös tapahtunut muutoksia ja niitä kehitetään jatkuvasti – tilanne ei ole mitenkään stabiili ja se tuo oman haasteensa erilaisille yhteistyömuodoille sekä ympäristöjen avaamiseen laajemmin esim. yrityselämän hyödynnettäväksi.

Tampereen yliopisto

- Dependable Systems
 - o kolmen toisiinsa kytkeytyvän laboratorioympäristön kokonaisuus
 - Information Security CyberLab
 - Automation CyberLab
 - Electrical Engineering CyberLab
 - o mahdollistaa sovellusalueittain koulutus, tutkimus- ja opetustoiminnan
 - o labroihin sisältyy verkkojen lisäksi fyysisiä tiloja (mm. opetustilat) sekä erilaisia laitteistoja, virtuaalisia ratkaisuja ja ohjelmistoja
- Käyttömahdollisuuksia
 - o teknisiä ympäristöjä pystytään osittain hyödyntämään myös etänä sekä viemään muihin tiloihin kuten yrityksiin (esim. automaation CSST-ympäristö)
 - o ympäristöjä on käytetty aikaisemmin täydennyskoulutuksissa mutta niiden yhteiskäyttämiseen liittyy rajoitteita sekä räätälöintejä, joissa on oltava mukana niistä vastaavat UTAn henkilöt
 - o yksi merkittävä tekijä mm. yrityskäytölle on käyttölisenssien asettamat rajoitteet

Oulun yliopisto

- Kyberturvallisuuden tekniset ympäristöt ICT-alaan keskittyviä, tausta turvallisen järjestelmä- ja ohjelmistokehityksen koulutuksessa
 - o Teknisiä ympäristöjä, jotka liittyvät kyberturvallisuuden asioihin:
 - Tietokonelaboratoriot
 - Laskentaklusterit
 - 5G-testiverkko
 - o Muita mahdollisesti hyödynnettäviä ympäristöjä
- Käyttömahdollisuudet
 - o yhteistoiminta eri tahojen välillä mahdollista mutta vaatii käyttäjälupahallintaa sekä tilanteen mukaista räätälöintiä ja hallinnollisia toimia
 - o vaatii OY:n henkilöstön mukanaoloa

Tampereen ammattikorkeakoulu

- Erillisiä laboratorioympäristöjä, jotka on rakennettu opetuksen lähtökohdista
- Osaa hyödynnetään kyberturvallisuuteen liittyvissä koulutuksissa ja osassa ei ole vielä tätä tulokulmaa tehty
- Teknisiä ympäristöjä, joita hyödynnetään kyberturvallisuuteen liittyvässä koulutuksessa
 - o Tietoverkkolabra
 - o KyberLabra
 - o Tietoliikennetekniikan labra
 - o Titenet, tietotekniikan labraympäristö

Kyberturvaaja-hanke
Hankekoodi: S21325

- Muista mahdollisesti soveltuvia teknisiä ympäristöjä on tekniikan alan erilaiset labrat kuten IoTn, ajoneuvotekniikan, automaatiotekniikan, konetekniikan, rakennustekniikan ja sähkövoimatekniikan laboratoriot
- Muita huomionarvoisia ympäristöjä
- Käyttömahdollisuudet
 - o Laajempi käyttö vaatii paljon ympäristöjen räätälöintiä ja kehittämistä, ovat nyt tamkin koulutustoimintaan luotuja ja vaativat fyysisen läsnäolon
 - o Yhteiskäyttömahdollisuuksia on mutta myös merkittäviä reunaehtoja kuten räätälöinti, tarve tamkin henkilöstön osallistumiseen, lisensoinnit ja pääsy-/käyttöoikeudet

Turun ammattikorkeakoulu

- Virtualisoitu ympäristö kyberturvallisuuden opettamisen tarpeisiin
 - o Kyberturvallisuustestausympäristö
 - o Kyberpuolustamisen harjoitteluympäristö
 - o Automaattinen uhkaemulaattori (kehitteillä)
- Käyttömahdollisuudet
 - o ympäristöt ovat muiden toimijoiden hyödynnettävissä reunaehtoien mukaisesti (lisensointi, ylläpito- yms. maksut)
 - o pääsy etänä mahdollinen
 - o yhteiskäyttöprosessia testattu hankkeen yhteydessä TAMKin kanssa

Metropolia ammattikorkeakoulu

- vanha kampus jouduttiin äkillisesti sulkemaan 4.3.2019
- kampuksen sulkeminen aiheutti myös teknisten ympäristöjen ”alas ajamisen”
- vuonna 2020 uusi kampusalue on rakenteilla mutta erillisiä suuremmin hyödynnettäviä teknisiä ympäristöjä ei ole

Tekniset ympäristöt koonti

Tekninen ympäristö, kuvaus	Työelämäkoulutus/yhteistoiminta-mahdollisuudet	Oppilaitos
Kybertestaus, virtualisoitu ympäristö kyberturvallisuustestauksen opiskeluun	Hyödynnettävissä verkostolle ”ostopalveluna”	TurkuAMK
Kyberpuolustus, virtualisoitu ympäristö kyberpuolustuksen opiskelemiseen	Hyödynnettävissä verkostolle ”ostopalveluna”	TurkuAMK
Kyberuhkaemulaattori	kehitysvaiheessa	TurkuAMK
Kyberlabra, järjestelmien kyberturvallisuustestauksen opiskeluun	Vaatii fyysisen läsnäolon sekä asiantuntijan räätälöintiä tilannekohtaisesti	TAMK
Tietoverkkolabra, tietoverkkojen puolustaminen kyberuhkilta	Vaatii fyysisen läsnäolon, lisenssiehtoja käytölle	TAMK

Tietoliikennetekniikan labra, langattomien verkkojen ja signaalien testaus, tutkinta ja opetus, WLAN, 2-4G, häiriösuojattu tila, häirintämahdollisuus	Vaatii fyysisen läsnäolo TAMKilla sekä asiantuntijan mukanaolon ja räätälöintiä	TAMK
Titenet	Virtuaalikoneiden käyttömahdollisuuksia erilaisiin tarkoituksiin.	TAMK
Muita tekniikan alan labroja (auto, automaatio, kone, rakennus, sähkövoima)	Ei hyödynnetä tällä hetkellä kyberturvallisuuden koulutustoiminnassa	TAMK
Heat Lab, terveysteknologian testausympäristö	Laitteistoa voidaan tarvittaessa hyödyntää kyberturvallisuuteen liittyvässä työelämäkoulutuksessa	TAU (TAMK)
Information Security CyberLab, verkkolaitteiden ja palvelinsovellusten tietoturvatutkimus ja koulutus, mikrinternet mm. laajempien uhkien tutkimiseen	Merkittäviä reunaehtoja käytän laajentamiselle, vaatii yliopiston asiantuntijoiden mukanaoloa ja räätälöintiä	TAU
Automation CyberLab, kriittisen infrastruktuurin automaation kyberuhkien tutkimiseen ja kouluttamiseen, runkoverkko+automaatiolaitteita	Ympäristöä on käyty aikaisemmin yrityskoulutuksissa ja sitä voidaan jatkaa. Vaatii toimijoiksi TAU:n asiantuntijat.	TAU
CSST-harjoitusympäristö, tekninen ympäristö teollisuuden tietoturva-auditointi- ja puolustusharjoitteluun, voidaan siirtää koulutuspaikalle	Tekniikan lisäksi ”ympäristöön” liittyy sen asiantuntijat. Koulutus on saatavana verkostolle ”ostopalveluna”.	TAU
Electrical Engineering Cyberlab, sähkötekniikan soveltavaan kyberturvallisuustutkimukseen ja opiskeluun, mm. sähköasemien automaation ja jakeluautomaatioratkaisujen tietoturva testaaminen	ei tiedossa	TAU
Tietokonelaboratoriot, tietokoneluokkia, missä on mahdollisuus mm. virtualisointien kautta tehdä ohjelmistojen kyberturvallisuustestausta	Hyödynnettävissä reunaehtojen mukaisesti sekä OY:n asiantuntijoiden mukanaololla	OY
Laskentaklusterit	OY:n ICT-palvelujen ”ostopalvelu”	OY
5G-testiverkko	Hallinnointi CWC-yksiköllä	OY

Kyberturvaaja-hanke

Hankekoodi: S21325

Muita: FabLab, Itseohjautuva auto, häiriösuojattu huone	Erikseen sovittaessa voi olla käytettävissä ”ostopalveluna” OYn asiantuntijoiden mukanaololla.	OY
---	--	----