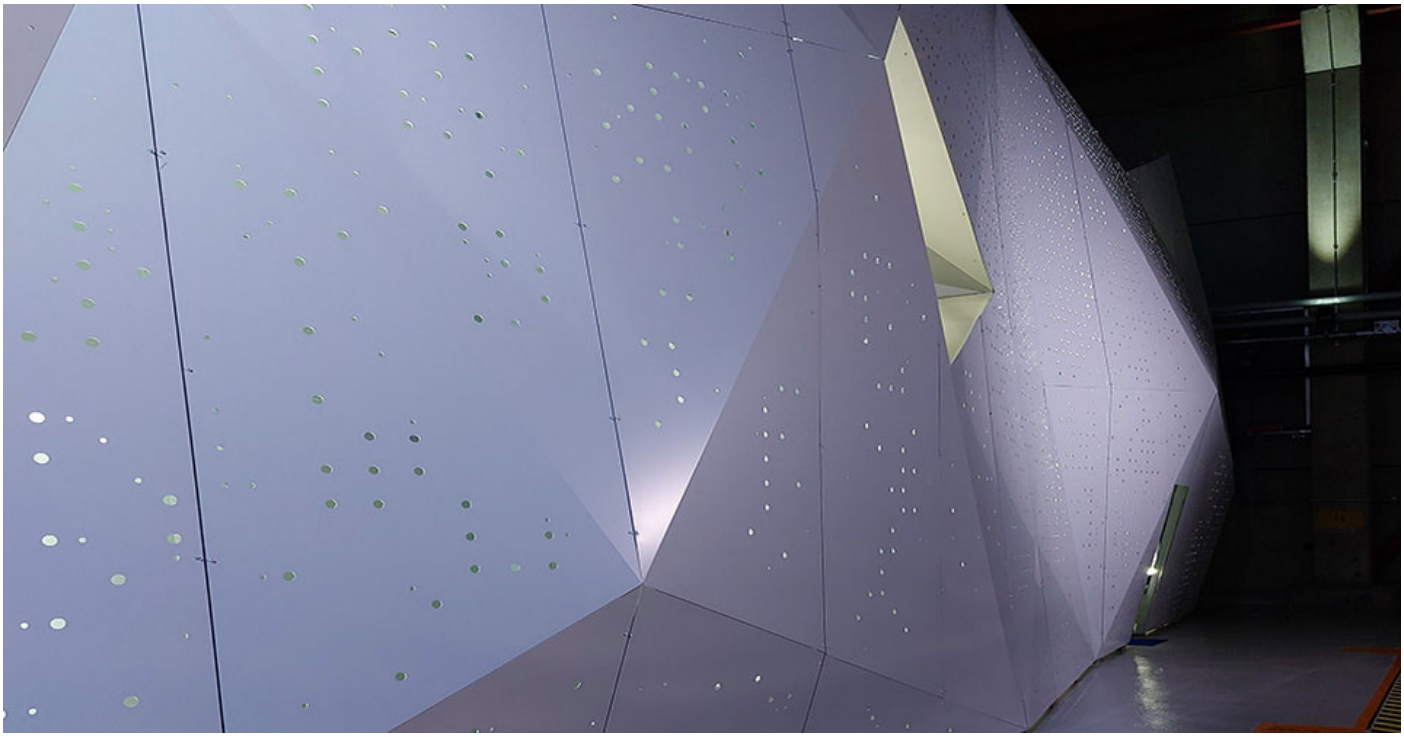
Digiaika edellyttää korkeakouluilta yhtenäistä tietoturvaosaamisen kehittämistä - UAS Journal



LUMI-supertietokoneen suojarakenteita. Kuva: Jaakko Riihimaa.

Jaakko Riihimaa & Kimmo Pettinen

02.10.2023

Digitalisaation edetessä toiminnan jatkuvuuden varmistaminen on korkeakouluissa yhä tärkeämpi teema. Digitaaliset toimintaympäristöt, myös oppimisympäristöt, ovat kyberrikollisille houkutteleva kohde. Kyberhyökkäykset ovat merkittävä toiminnan keskeytysriski. Keskeytys tietojärjestelmien toiminnassa voi johtaa opetuksen keskeytymiseen. Käyttäjätunnusten kalastelu avaa rikollisille tunkeutumismahdollisuuksia mm. kiristysohjelmien levitykseen ja palvelunestohyökkäyksiin. Seuraukset voivat olla vakavia niin maineelle kuin taloudellisesti. Varautuminen ja ennakointi on elintärkeää.

Henkilöstön ja opiskelijoiden tietoturvaosaamisesta huolehtiminen on keskeisimpiä keinoja torjua uhkia. Useat korkeakoulut ovat mm. kohdistaneet käyttäjilleen hallittuja sähköpostikampanjoita, jotka muistuttavat rikollisten lähettämiä viestejä. Tavoitteena on ollut lisätä käyttäjien tietoisuutta sekä valmentaa raportoimaan epäilyttävistä havainnoista.

Kysely tietoturvakoulutuksista

Korkeakoulujen tietohallintojohtajien verkostot (ammattikorkeakoulujen AAPA ja yliopistojen

FUCIO) toteuttivat alkuvuonna 2023 kartoituksen korkeakoulujen tietoturvakoulutuksista ja niihin liitetyistä testeistä. Ammattikorkeakouluista kyselyyn vastasi 80 % ja vain kaksi niistä ilmoitti, etteivät ne olleet suunnitelleet tai toteuttaneet mitään perehdytysaktiviteetteja.

Kyselyn jatkotoimenpiteenä AAPA järjesti toukokuussa 2023 AMK-päivien yhteydessä kolme ideatyöpajaa. Niiden tavoitteina oli kartoittaa osallistujien kokemuksia ja tietoturvakoulutuksen toteutustapoja sekä keskustella, miten yhteistyötä voisi tietoturvakoulutuksen osalta tehdä, ja miten sitä voitaisiin toteuttaa käytännössä.

Kartoituksen ja työpajojen tulosten perusteella vaikuttaa siltä, että kaikki 38 korkeakoulua miettivät samoja tietoturvakoulutuksen kysymyksiä. Yhteistyön puuttuessa ne joutuvat tekemään omia ratkaisujaan, jotka ovat keskenään hyvin erilaisia. Jotkut korkeakoulut ovat pitäneet tietoturvaan perehtymistä suosituksena, toisissa käyttäjätunnukset sulkeutuvat, jos osaamisen tasoa ei ole todennettu. Opiskelijoille perehdytys on joissakin korkeakouluissa osa opintopisteytettyä toteutusta ja pakollista, mutta pääsääntöisesti osaamisen todennusmenettelyjä ei ole käytössä.

Kyberturvaan koulutuslinjauksia

Saatujen tulosten perusteella korkeakoulusektorin yhteisille kyberturvaan liittyville koulutuslinjauksille ja -aineistoille on tilausta. Ammattikorkeakoulujen toiminnan jatkuvuuden turvaamisen, kustannusten ennakoinnin ja tulevien lakisääteisten vaatimusten lisäksi asia on erityisen merkittävä myös opiskelijoiden ja opiskelijaliikkuvuuden osalta.

Opiskelijoille luonteva tietoturvakoulutuksen ajankohta olisi heti opintojen alussa, mutta ei kuitenkaan orientaatioviikolla, jolloin on paljon myös muuta yleisperehdytystä. Koulutus sisällytettynä osaksi pakollista opintojaksoa, ehkä myös opintopisteytettynä, lisäisi motivaatiota. Opintojen loppuvaiheessa olisi hyvä olla toinen osio varmistamassa työelämään siirtymisen vaatimukset.

Opiskelijaliikkuvuuden lisääntyessä korkeakoulujen toisistaan poikkeavat tietoturvaosaamisen vaatimukset eivät saa johtaa tilanteisiin, joissa eroavaisuudet estäisivät vierailevalta opiskelijalta opintojen suorittamisen. Siksi erilaisten skenaarioiden tarkempi tarkastelu on tarpeen ja tämä myös laajentaisi käsitystä yhtenäisen tietoturvakoulutuksen tarpeellisuudesta.

Korkeakouluille yhteinen koulutusmateriaali

Korkeakoulujen käyttöön tulisi laatia yhteinen perustason tietoturvakoulutusmateriaali sekä siihen liittyvää osaamista mittaava kysymyspatteristo. Toimintaympäristössä tapahtuvien muutosten takia koulutusmateriaalin sisällön tulee olla jatkuvasti päivittyvä. Materiaalin ajantasaistamisen vastuut on sovittava, jakelun tulee olla helposti järjestettävissä ja muutoksista on tiedotettava. Asiaa tulisi edistää niin, että tavoitteena olisivat ammattikorkeakoulu- ja yliopistosektoreiden kesken yhtenäiset tietoturvakoulutusten sisällöt sekä mahdolliset sanktiot.

Ammattikorkeakoulujen osalta asian liikkeelle saamisessa Arenen rooli nähtiin työpajoissa keskeiseksi. Aineisto voitaisiin koostaa yhteistyössä korkeakoulujen tietoturvaverkostojen (AMK-SEC, YO-SEC) kesken. Aineisto ja sen ajan tasalla pito voitaisiin hankkia myös ostopalveluna ulkoiselta toimijalta (Tieteen tietotekniikan keskus CSC taikka muu yritys) tai käyttää valmiita kaupallisia toteutuksia.

Kaikista toimintamalleista on korkeakouluissa jo esimerkkejä. Niistä olisi pystyttävä yhdessä valitsemaan parhaat käytännöt ja saatettava yhtenäinen tietoturvakoulutus osaksi korkeakoulujen arkea.

> Korkeakoulujen tietohallinnot kansallisen henkilöstölle ja opiskelijoille suunnatun tietoturvakoulutuksen puolesta!

Kirjoittajat

Jaakko Riihimaa, FT, IT-pääsihteeri, AMK-tietohallintojohtajien AAPA-verkosto, jaakko.riihimaa(at)haaga-helia.fi.

Kimmo Pettinen, FM, tietohallintojohtaja, Laurea-ammattikorkeakoulu, kimmo.pettinen(at)laurea.fi.

Abstract

As digitalization proceeds in higher education institutes (HEI), comes continuity of operations and how to ensure it more important theme than ever before. Cyber-attacks are significant risks for interruptions for the operation. The most important factor in preventing cyber threats is to make sure both students, staff and faculty have up to date knowledge of information security.

In the beginning of year 2023 CIO networks AAPA and FUCIO executed a survey to find out how information security is trained and tested in HEI's. 80 % of UAS's answered, of which only two indicated they have not yet started any activities. As a follow-up in May 2023 AAPA organized three workshops as a part of yearly UAS days. Objective was to map and discuss how cyber security training could be done in co-operative way.

Results of these activities related to cyber security training were:
– all 38 HEI's are pondering same questions
– a common basic-level material and set of test-questions should be produced
– materials should be easy to maintain, and they should be continuously updated.

LISÄÄ AIHEEN YMPÄRILTÄ / RELATED POSTS