Tietoturvan ja kyberturvallisuuden koulutus suomalaisten toisen asteen oppilaitosten työntekijöille

Turun yliopisto
Tietotekniikan laitos
Diplomityö
Tietoliikenne- ja kyberturvallisuusteknologia
Syyskuu 2025
Jere Kotiniemi

Tarkastajat:
Petri Sainio
Panu Puhtila

TURUN YLIOPISTO
Tietotekniikan laitos

Jere Kotiniemi: Tietoturvan ja kyberturvallisuuden koulutus suomalaisten toisen asteen oppilaitosten työntekijöille

Diplomityö, 65 s.
Tietoliikenne- ja kyberturvallisuusteknologia
Syyskuu 2025

Diplomityö käsittelee toisen asteen oppilaitoksen henkilökunnalle suunnattua kyberturvallisuuden koulutusta muuttuneessa toimintaympäristössä. Digitalisaation myötä oppilaitosten toiminta on siirtynyt yhä vahvemmin sähköisiin järjestelmiin, mikä on osaltaan lisännyt kyberuhkien määrää. Lisäksi oppilaitoksissa käsiteltävä tietoa on paljon ja se määritellään usein arkaluonteiseksi. Tutkimuksessa tarkastellaan oppilaitosten asemaa kyberturvallisuuden kentällä, lainsäädännön vaikutuksia sekä teknologian kehityksen tuomiin uhkiin varautumista. Työssä tarkastella myös uusien teknologioiden, kuten tekoälyn ja esineiden internetin synnyttämiä haasteita.
Työssä korostetaan henkilöstön roolia kyberturvallisuuden yhtenä onnistumisen tärkeimpänä osatekijänä. Tekniset ratkaisut kuten käyttöoikeuksien hallinta ja ohjelmistojen päivittäminen ovat välttämättömiä, mutta eivät yksin riitä takaamaan turvallista toimintaympäristöä. Henkilökunnan tietoisuus ja osaaminen ovat keskeisiä, sillä inhimilliset virheet ovat merkittävä riskitekijä. Koulutuksen tavoitteena on lisätä muun muassa ymmärrystä uhkien tunnistamisesta ja keinoista niiden ehkäisemiseksi.
Tutkielma esittelee koulutusmateriaalin suunnittelun periaatteet, joissa huomioidaan oppimisen psykologia, organisaation muutokset sekä konkreettiset työkalut. Materiaalin jakautumista kohderyhmittäin pohditaan, sen hyötyjen kautta. Tavoitteena on ymmärtää, miten toteutetaan käyttäjäystävällinen, selkeä ja kattava koulutus, joka tukee koko organisaation toimintaa.
Keskeisinä päätelminä voidaan todeta, että kyberturvallisuudesta on tullut kansalaistaito, joka koskettaa kaikkia oppilaitoksen toimijoita opiskelijoista ulkoisiin palvelun tarjoajiin. Koulutuksen avulla voidaan ennaltaehkäistä riskejä, vahvistaa organisaation resilienssiä ja varmistaa tietojen turvallisen käsittelyn.

Asiasanat: Kyberturvallisuus, Tietoturva, Koulutus, Turvallisuus

UNIVERSITY OF TURKU
Department of Computing

Jere Kotiniemi: Tietoturvan ja kyberturvallisuuden koulutus suomalaisten toisen asteen oppilaitosten työntekijöille

Diplomityö, 65 p.
Tietoliikenne- ja kyberturvallisuusteknologia
September 2025

This thesis examines cybersecurity training for staff at secondary education institutions in a changing operating environment. With digitalization, educational institutions have increasingly moved to electronic systems, which has increased cyber threats. In addition, educational institutions handle large amounts of data, which is often classified as sensitive. The study examines the role of educational institutions in the field of cybersecurity, the impact of legislation, and preparedness for threats posed by technological developments. The study also examines the challenges posed by new technologies, such as artificial intelligence and the Internet of Things.
The study emphasizes the role of personnel as one of the most important factors in the success of cybersecurity. Technical solutions, such as access rights management and software updates, are essential, but they alone are not enough to guarantee a secure operating environment. Staff awareness and skills are key, as human error is a significant risk factor. The aim of the training is to increase understanding of how to identify and prevent threats.
The study presents the principles of learning material design, taking into account the psychology of learning, organizational changes, and concrete tools. The distribution of materials to target groups is examined in terms of its benefits. The aim is to understand how to implement user-friendly, clear, and comprehensive training that supports the activities of the entire organization.
The key conclusions are that cybersecurity has become a civic skill that concerns all members of an educational institution, from students to external service providers. Training can be used to prevent risks, strengthen the organization's resilience, and ensure the secure handling of data.

Keywords: Cybersecurity, Information security, Education, Safety

Sisällys

Kuvat

1 Johdanto

Digitalisoituvassa maailmassa kyberturvallisuus on nykyisin yhteiskunnan toimivuuden yksi tärkeimmistä takaajista, sillä sähköisiin järjestelmiin kohdistuu jatkuvasti muuttuvia uhkia. Hyökkäyksiä ja häiriöitä vastaan tarvitaan tehokasta varautumista, ennaltaehkäisevää toimintaa ja järjestelmien aukottomuutta. Tietoturvauhat koskettavat niin yhteiskunnan kriittisiä palveluita, kuin myös yksittäisiä kansalaisia ja organisaatioita. [1] Kyberturvallisuus on joukko erilaisia toimintoja, joilla pyritään suojaamaan yhteiskunnan sähköisiä järjestelmiä, laitteita ja dataa. Sen keskiössä on muun muassa varautuminen, ennaltaehkäisy ja järjestelmien aukottomuus. Näillä toimilla pyritään varjelemaan yhteiskunnalle kriittisiä palveluja verkkoympäristössä tapahtuvilta erilaisilta hyökkäyksiltä ja häiriöiltä. Yhä nopeammin digitalisoituvassa maailmassa sähköisten järjestelmien ja tiedon määrä verkossa kasvaa jatkuvasti, samalla niihin kohdistuvien uhkien määrä lisääntyy. [2] Varautuminen hyökkäyksiä ja uhkia vastaan korostuu jatkuvasti, eikä niiden merkitystä voida vähätellä.

Tiedon kerääminen ja käsittely tapahtuu nykyisin lähes täysin sähköisissä järjestelmissä. Varsinkin organisaatioissa tämä muutos näkyy erilaisten järjestelmien määrän lisääntymisellä. Teknisten ratkaisujen lisäksi henkilökunnan rooli korostuu osana tieto- ja kyberturvallisuutta. Pääsy- ja käyttöoikeuksien hallinnalla rajoitetaan käyttäjien oikeuksia käytettävissä järjestelmissä. Mikäli esimerkiksi työtehtävien hoitaminen ei edellytä tiettyihin tietoihin tai järjestelmiin pääsemistä, on perusteltua estää käyttäjän pääsy niihin. [3] Näin saadaan minimoitua erilaisten inhi-

millisten virheiden kautta syntyneet vahingot, sekä mahdollisen tietomurron kautta tapahtuvat vahingossa saadaan rajattua mahdollisimman pieneksi. Toisinaan havahdutaan tilanteisiin, joissa esimerkiksi työntekijän roolin vaihtuessa hänen oikeutensa käytettävissä järjestelmissä kertaantuu, koska vanhemman roolin oikeuksia ei ole muistettu poistaa tai muokata. Joskus myös vanhoilla työntekijöillä, jotka eivät ole enään yrityksessä töissä on edelleen pääsy järjestelmiin sekä tietoihin.

Verkkoon ja sähköisiin järjestelmiin, joista yhteiskunta on jo osittain riippuvainen, kohdistuu toistuvia uhkia, joita kyberturvallisuuden alan yritykset ja valtiolliset tahot pyrkivät havaitsemaan ja muodostamaan tilannekuvaa alati muuttuvasta kyberturvallisuustilanteesta. [4] Suomessa toimii esimerkiksi liikenne- ja viestintäviraston alaisuuteen perustettu kyberturvallisuuskeskus, jonka päätehtävänä on luoda tilannekuvaa Suomessa vallitsevasta kyberturvallisuustilanteesta. Kyberturvallisuuskeskus tarjoaa myös tietoturvakoulutusta ja neuvontaa. Tilannekuvan lisäksi riskianalyysejä ja ennaltaehkäisevää toimintaa tehdään yhdessä eri toimijoiden kanssa, joita ovat nimenomaan alan yritykset ja niiden henkilöstö. Toiminnalla pyritään ennalta varautumaan kyberrikollisten luomia uhkia vastaan tunnistamalla haavoittuvuuksia ja riskejä. [5] Kyberturvallisuuden kansantajuistaminen ja koulutus ovat erittäin tärkeitä toimia uhkien ennaltaehkäisemiseksi. [6]

Tietoturvaympäristöön liittyvät vaikutukset koskettavat yhteiskunnan kriittiseksi luokiteltujen järjestelmien lisäksi myös yksittäisiä ihmisiä. Yhteisöjen ja organisaatioiden on hyvä laatia kattava, koordinoitu ja ajantasainen toimintaohjeistus, jotta kyberhäiriötilanteen sattuessa uhkiin pystytään reagoimaan viiveettä ja mahdollisimman tehokkaasti. [7] Yksittäisen ihmisen tärkeimpiä suojautumiskeinoja kyberrikollisuutta vastaan ovat muun muassa tarpeeksi pitkät ja monimutkaiset salasanat sekä miten niitä hallitaan. Laitteiden ja ohjelmistojen päivitysten pitäminen ajan tasalla on oleellista. Verkossa tapahtuva tietojenkalastelu tapahtuu tilanteissa, joissa käyttäjää saatetaan esimerkiksi johdatella syöttämään luottokorttitietoja tai

verkkopankkitunnuksia huijaussivustolle.

Venäjän hyökkäyssota Ukrainaa vastaan on lisännyt kyberuhkia globaalisti, myös Suomessa. Konfliktin myötä kybersodankäynti on vakiinnuttanut asemaansa osana tehokasta sodanajan toimintaa, jolla pyritään sabotoimaan vastapuolen kriittistä infraa luoden samalla painetta ja madaltaen moraalista taistelutahtoa. [8] Kybersodankäynnin merkitystä osana nykysodankäyntiä ei voi väheksyä. Uutismediat ovat osaltaan lisänneet ihmisten tietoisuutta kybersodankäynnistä. Tiedotusvälineissä on uutisoitu muun muassa konfliktin ulkopuolisia maita kohtaan suunnatuista verkossa tapahtuvista iskuista, jotka ovat toisinaan kohdistuneet elintärkeisiin toimintoihin. Tämän kaltaista toimintaa on koettu myös Suomessa.

Tietoisuus kyberturvallisuudesta on kasvanut, mutta turvallisuudesta huolehtiminen verkossa on vielä varsinkin käyttäjätasolla puutteellista.[9] Nykyisin voidaan kuitenkin puhua kyberturvallisuudesta kansalaistaitoon rinnastettavana asiana. Tahoja, jotka toteuttavat omia motiivejaan hakkeroinnin avulla, on useita. Tällaisia ovat esimerkiksi järjestäytyneet rikolliset, valtion taholta koordinoidut organisaatiot ja itsenäisesti toimivat hakkerit. [10] Tilanteesta tekee hankalan se, että kyberhyökkääjää tai -hyökkääjiä on vaikea tunnistaa ja siten saattaa edusvastuuseen. Tietyt maat myös pyrkivät suojelemaan kansalaisiaan, vaikka nämä olisivatkin syylistyneet rikoksiin.

Yksityishenkilö joutuu nykyisin paljon suuremmalla todennäköisyydellä verkkorikollisuuden uhriksi kuin tulee ryöstetyksi kadulla. [11] Kyberrikollisuuden päämääränä on usein rahan vieminen, identiteettien varastaminen, datan hävittäminen tai sen kerääminen. Myös järjestelmien häirintä ja mielipidevaikuttaminen ovat tällaisia mahdollisia motiiveja. Tekoälyä sovelletaan enenevissä määrin kyberturvallisuuden apuna, mutta toisaalta sitä käytetään myös kyberturvallisuutta vastaan esimerkiksi tehostamalla salasanojen murtamista. Tulevaisuudessa tekoälyyn ja koneoppimiseen liittyvien riskien tunnistamisen merkitys korostuu. Tietoturvaan ja kyberturvalli-

suuteen liittyviä riskejä on kyettävä hallitsemaan niiden tunnistamisen lisäksi, jotta tekoälyn kaltaisten älykkäiden ohjelmien käyttö tapahtuu mahdollisimman turvallisesti. [12]

1.1 Muuttuva oppilaitosympäristö ja kasvanut kyberturvallisuuden tarve

Digitalisaation kehitys tuo mukanaan mahdollisuuksia ja haasteita. Yritykset hyödyntävät etenevissä määrin murroksen luomia liiketoimintamahdollisuuksia, mikä vaikuttaa olennaisesti henkilöstöltä vaadittavaan osaamiseen. Koulutuksen kentällä muutos näyttäytyy ammatillisen koulutuksen uudistumisena ja vaikuttaa vahvasti opetuksen sisältöön. Näin pystytään vastaamaan yrityksien tarpeisiin ajantasaisen osaamisen suhteen.

Ammatilliseen koulutukseen haetaan joko yhteishaun tai jatkuvan haun kautta. Opiskelijan on mahdollista suorittaa ammatillinen perustutkinto, ammattitutkinto tai erikoisammattitutkinto. Ammatillisesta koulutuksesta valmistunut opiskelija saa myös kelpoisuuden jatkaa opintoja korkeakouluihin. Yhteiskunnallisesti puhuttaessa on kyse erittäin merkittävästä instituutiosta, joka vastaa työelämän tarpeisiin. Koulujen ja oppilaitosten digitalisoituminen on tuonut mukanaan uusia haasteita erityisesti kyberturvallisuuden ja tietoturvan osalta. [6] Muutoksen vaikutus on laaja niin oppilaitoksen toiminnan kuin yksilön tietoturvan kannalta, mikä tekee koulutuksentarjoajan ja henkilökunnan tietoturvaosaamisen tärkeyden entistäkin näkyvämmäksi.

Työssä perehdytään koulutuksen järjestäjän päivittäisessä käytössä oleviin digitaalisiin järjestelmiin. IT-ympäristöön tutustumalla saa hyvän käsityksen henkilöstölle kehitettävän kyberturvallisuuden koulutuksen painopisteistä. Pyrkimyksenä on saada aikaan hyvä ymmärrys koulutuksen tarpeesta ja miten se toteutetaan

kattavasti, niin että se vastaa esiin nousseita haasteita ja tukee henkilöstön kykyä toimia turvallisesti työssään. Koulutusmateriaalin tavoitteena on olla mahdollisimman käyttäjäystävällinen ja selkeä. Sen tulisi kattaa henkilöstön tarpeet ja edistää samalla koko organisaation kyberturvallisuuden tasoa. Koulutuksen järjestäjä, jolle työ tehdään. On asettanut kyberturvallisuusosaamisen vahvistamisen yhdeksi strategisista tavoitteistaan ja sen kehitystä sekä nykytilaa seurataan järjestelmällisesti.

Työssä tarkastellaan myös Keudan ja Esedun kyberhyökkäyksien kaltaisten tapausten vaikutusta organisaatioon ja sen toimintaan. Työ on keskittynyt siihen, kuinka kyberturvallisuus voidaan tehdä mahdollisimman hyvin kaikille ymmärrettäväksi, varsinkin kun puhutaan henkilökunnasta, joka työskentelee päivittäin suuren määrän arkaluontoiseksi määriteltävää materiaalia kanssa. Työ on tärkeä myös uuden kyberturvallisuusdirektiivin NIS2 kannalta, sillä direktiivi asettaa vaatimuksia kyberturvallisuuskoulutukselle, tosin oppilaitokset eivät ole suoraan NIS2 piirissä. [13] Silti se antaa hyvän perustan sille, miksi on hyvin tärkeää panostaa henkilöstön osaamisen kehittämiseen osana riskienhallintaa.

2 Tausta

Kouluihin kohdistetaan nykyisin eri tavoin toteutettuja kyberhyökkäyksiä ja tietojenkalasteluyrityksiä. Yhtenä suurimmista syistä lienee, että oppilaitosten järjestelmissä säilytetään runsaasti opiskelijoiden, huoltajien ja henkilökunnan henkilökohtaista dataa, kuten henkilötunnuksia, yhteystietoja, terveystietoja sekä opintosuorituksia. [14] Arkaluontoisen tiedon määrän lisäksi oppilaitoksessa käytettäviä järjestelmiä on paljon, mikä lisää kyberrikollisten kiinnostusta kohdistaa iskuja juuri koulumaailmaan. Varsinkin järjestelmien paljous lisää hyökkäyspinta-alaa, tarjoten näin kyberrikolliselle paremmat mahdollisuudet onnistua kyberhyökkäyksessä[15] Mikä edistää omalta osaltaan koulun kiinnostusta kohteena ja luo oppilaitokselle vaatimuksia turvallisuuden suhteen.

2.1 Oppilaitokset kyberturvallisuuden kentällä

Toisinaan voidaan ajatella oppilaitoksissa olevan muita toimijoita rajallisemmat resurssit IT-ympäristön turvallisuuden kehittämiseksi ja ylläpitämiseksi. Resurssien puute altistaa järjestelmiä ulkopuolisille uhille ja tekee niistä haavoittuvaisia kohteita. [16] Suojausjärjestelmien puute ja päivittämättömät ohjelmistot voivat vaarantaa käyttäjän esimerkiksi automatisoiduille hyökkäyksille kuten bottien suorittamille kirjautumisyrityksille. Heikot tunnistautumiskäytännöt sekä henkilöstön puutteet tietoteknisissä taidoissa lisäävät riskiä altistua erilaisille uhille kuten tietojenkalastelulle.

Koulut usein luottavatkin ulkoisiin järjestelmätoimittajiin, joiden vastuulla on palveluiden tekninen turvallisuus. Kuitenkin esimerkiksi käyttäjätunnusten ja salasanojen hallinta sekä käyttöoikeuksien jakaminen ovat lähtökohtaisesti oppilaitoksen itsensä vastuulla. On myös syytä muistaa, että kouluun kohdistuneet kyberhyökkäykset eivät aina ole ulkopuolisen ammattilaisen tai organisoidun rikollisjärjestön tarkoituksella toteuttamia iskuja. Opiskelija tai henkilökunnan jäsen voi huolimattomuudellaan mahdollistaa uhan koulun järjestelmiin, siirtämällä esimerkiksi haittaohjelman koulun hallinnoimaan koneeseen ulkoisen USB-muistin välityksellä.

Motiivina oppilaitokseen kohdistetun kyberiskun toteuttamiselle voi toimia kauna opettajaa, kollegaa tai koulua kohtaan. Varsinkin nuoren opiskelijan näkökulmasta motiiveja voivat olla myös puhdas uteliaisuus ja halu kokeilla omia teknisiä taitoja, ilman täyttä ymmärrystä teon seurauksista. [17] Toisella asteella opiskelevan nuoren ikäkehitykseen kuuluu vahvasti identiteetin etsiminen, johon saattaa liittyä kapinointia ja epävarmuutta. Tällöin ympäristötekijät korostuvat vahvasti moraalin käsityksen kehityksessä. Nuorten rikollisen käyttäytymisen taustoja ja syntyperää on tutkittu paljon. Riskitekijöiksi on nimetty esimerkiksi perheympäristö, ystäväpiiri sekä asuinalue. [18] Yksilökohtaisilla ominaisuuksilla kuten kognitiivisissa ja ei-kognitiivisilla piirteillä sekä mahdollisilla psykoottisilla häiriöillä on myös vaikutusta.

Sähköisiin järjestelmiin ja tietoverkkoihin kohdistuvaa kyberrikollisuutta ehkäisevänä toimintana tulisi antaa opetusta, kertomalla laittomasta toiminnasta ja sen seurauksista. Taitojen käyttämistä vastuullisesti ja hyviin tarkoitusperiin tulisi kannustaa. Tietoverkot ovat kiinteä osa yksilöiden ja yhteiskunnan arkea ja niiden rooli korostuu yhä kiihtyvässä digitalisaatiokehityksessä. [19] Tietoverkot ja niissä toiminen ovat osa nykypäivän lasten ja nuorten ajattelu- ja kokemusmaailmaa. Tietoisuuden lisääminen tietoverkoissa toimimisen rajoista ja siihen liittyvistä riskeistä ovat merkittävässä roolissa kyberrikollisuuden ennaltaehkäisyssä.

Opetuksen järjestäjän on tärkeää varmistaa, että myös ulkopuoliset palveluntarjoajat noudattavat tietoturvakäytäntöjä ja toimivat lainsäädännön rajoissa. Tämä koskee erityisesti digitaalisia oppimisympäristöjä ja hallintojärjestelmiä. Palvelusopimusten yhteydessä on tärkeää varmistaa, että tietoturva- ja tietosuojavaatimukset on kirjattu selkeästi. Kuitenkaan pelkkä tekninen suojaus ei yksin riitä. Jos käyttäjillä ei ole tarpeeksi hyvää osaamista tai tietoisuutta turvallisesta ja vastuullisesta toimimisesta, voi siitä koitua mittavia vahinkoja. Siksi kyberturvallisuuskasvatus ja koulutus on noussut keskeiseksi osaksi oppilaitosten turvallisuutta. [6] Tavoitteena on opettaa sekä oppilaille ja henkilökunnalle perustiedot tietoturvasta sekä kyberturvallisuudesta. Tärkeitä perusteita on vahvojen salasanojen merkityksen ymmärtäminen, tietojenkalastelun tunnistamisesta ja yksityisyyden suojaamisesta digitaalisessa ympäristössä. [11] Yhteisen toimintamallin puuttuminen altistaa yksilön turvallisuuden lisäksi pahimmillaan koko muun yhteisön uhille.

Opetussuunnitelmat sisältävät jo nyt osia kyberturvallisuudesta, mutta käytännön tasolla toteutus vaihtelee suuresti eri kouluissa, yhteisen toimintamallin puuttuessa ja viitekehyksen ollessa hyvin joustava. Joissain oppilaitoksissa aihetta käsitellään osana tieto- ja viestintätekniikan opetusta tai *Toiminta digitaalisessa ympäristössä* -kurssia.[20] Koulutusta voidaan järjestää, myös erilaisina teema- ja koulutuspäivinä. Opettajien rooli on keskeinen tiedon jakamisessa ja opettamisessa. Kuitenkin moni opettaja voi kokea tarvitsevansa itsekin lisäkoulutusta aiheesta. Tietoisuus vallitsevista uhista sekä ymmärrys siitä, miten niihin tulisi reagoida ovat osa modernia digitaalista lukutaitoa, joka jokaisen tulisi hallita.

Kyberturvallisuuden kenttä muuttuu nopeasti ja tulevaisuuden uhat monimutkaistuvat entisestään. Tekoälyn yleistyminen tuo mukanaan sekä mahdollisuuksia että uusia riskejä. Hyökkääjät voivat käyttää tekoälyä automatisoidakseen hyökkäyksiä, luodakseen aidon näköisiä huijausviestejä tai jopa jäljitelläkseen henkilökunnan kirjoitustyyliä saadakseen viestit näyttämään luotettavilta. Kyberuhkien kirjo on

nykyisin laaja. Hyökkäyksien toteutustavat vaihtelevat yksinkertaisista sähköpostin kautta lähetettävistä liitetiedostoista ja hyperlinkeistä, aina monimutkaisiin teknistä osaamista vaativiin tapoihin, joilla pyritään tunkeutumaan oppilaitoksen järjestelmiin. [2] On myös tärkeää tiedostaa, että todellisuudessa kyberhyökkäysten määrä on todennäköisesti huomattavasti suurempi kuin mitä julkisuuteen päätyy. Monia tapauksia ei raportoida lainkaan, tai ne jäävät vain sisäisesti käsiteltäviksi.

Suomen kaltaisessa oikeusvaltiossa kaikki toiminta perustuu lakiin. Oppilaitoksen toimintaa ohjaa joukko erilaisia lakeja ja näiden noudattamista suomessa valvoo useampi eri taho. Kullakin taholla on nimettynä oma vastuualueensa. [21] Oppilaitoksen kokonaisuudesta vastaa viime kädessä aina koulun johto sekä rehtori. Opettajat valvovat säädösten noudattamista omassa työssään, mahdollistaen oikeudenmukaisen, turvallisen ja yhdenvertaisen opetuksen kaikille tasapuolisesti. Opiskelijaa itseäänkin koskettavat tietyt vastuut ja velvollisuudet. Kouluympäristössä oppilaitoksen ulkopuoliset tahot, kuten aluehallintovirasto valvovat opetuksen laadukasta ja oikeudenmukaista toteutumista. Opetushallituksen pääasiallinen tarkoitus on toimia koulutuksen raamien laatijana, mutta se toimii myös valvovana viranomaisena. Toisen asteen oppilaitoksen toiminnan kannalta tärkeimpiä toimintaa ohjaavia lakeja on muun muassa laki ammatillisesta koulutuksesta ja työturvallisuuslaki. Toimintaympäristön muuttuessa sähköisemmäksi on mukaan tullut joukko muitakin lakeja, joiden mukaan koulun on ohjattava päivittäistä toimintaansa.

2.1.1 Laki ammatillisesta koulutuksesta

Laki ammatillisesta koulutuksesta ohjaa vahvasti ammatillisten oppilaitosten toimintaa Suomessa. [22] Laissa ei mainita erikseen kyberturvallisuutta tai tietoturvaa, mutta se vaikuttaa useissa laissa määritellyissä kohdissa suoraan tai välillisesti. Erityisesti oppimisympäristön turvallisuuden, koulutuksen sisällön ja opiskelijan oikeuksien kautta. Yksi keskeinen lain kohta on koulutuksen järjestäjän velvollisuus

huolehtia ja taata opiskelijoille turvallinen opiskeluympäristö. [23] Tämä ei koske pelkästään oppilaitoksen ja opetustilojen fyysistä turvallisuutta, vaan myös digitaalisia ympäristöjä. Tietoturvalliset oppimisalustat, vastuullinen henkilötietojen käsittely ja suojatut yhteydet ovat kaikki osa tätä kokonaisuutta. Opiskelijan henkilötietojen suojaaminen liittyy myös EU:n tietosuoja-asetuksen noudattamiseen, johon laki velvoittaa välillisesti.

Yksi ammattikoulun vaikuttavuuden mittareita on muuttuviin työelämän tarpeisiin vastaaminen koulutukseen ja sen sisältöön tehtävillä muutoksilla. [22] Monilla aloilla tietotekniikan- ja digitaalisien ohjelmien käyttö on lisääntynyt. Perinteisen ICT-alan lisäksi liiketoiminnan ja sosiaali- ja terveysalan työssä tietotekniset taidot ovat nykyisin olennainen osa ammattitaitoa. Tämän vuoksi tutkinnon perusteisiin tulisi sisällyttää kyberturvallisuuteen liittyvää sisältöä, kuten tietoturvakäytäntöjen noudattamista, turvallista laitteiden käyttöä ja verkkoympäristöjen hallintaa. Lain mukainen oppiminen työpaikoilla edellyttää, että opiskelijat perehdytetään myös työpaikan tietoturvakäytäntöihin, mikäli se on olennaisessa osassa työtehtävien hoitamisessa. Tämä korostaa koulun ja työelämän välistä yhteistyötä digiturvallisuuden varmistamisessa.

2.1.2 NIS2- Euroopan unionin kyberturvallisuusdirektiivi

NIS2 kyberturvallisuusdirektiivin täytäntöönpano suomessa tapahtui huhtikuussa 2025 kansallisella kyberturvallisuuslailla. Direktiivi korvaa aikaisemmin käytössä olleen NIS-direktiivin, jonka myötä direktiivissä mainitut soveltamisalat laajenevat entisestää. [13] Varsinkin kriittisiksi luokiteltavien toimialojen yrityksien vaatimukset tietoturvan ja kyberturvallisuuden osalta kovenevat. Laki tuo myös mukanaan velvoitteita riskienhallinnasta ja raportoinnista. Direktiivin tarkoituksena on varmistaa Euroopan unionin alueella kyberturvallisuudelle yhtenäiset vaatimukset.

Direktiivissä mainittuja toimialoja ovat erilaiset yhteiskunnan kriittistä infraa yl-

läpitävät tahot, jotka toimivat esimerkiksi energian, pankkitoiminnan ja terveydenhoidon parissa. Säädeltävät organisaatiot on jaettu toimialan tyypin mukaan, mutta myös toimialan koko saattaa vaikuttaa joissain tapauksissa sovelletaanko direktiiviä organisaation kohdalla. Esimerkiksi julkishallinnossa keskeiset toimijat kuuluvat *keskeiseksi tai tärkeäksi* luokiteltuihin soveltamisaloihin organisaation koosta riippumatta. Useissa toimialoissa alle 50 hengen organisaatiot jotka luetaan *pieniksi ja mikrotoimijoiksi* eivät kuulu soveltamisalaan. Useita poikkeuksia koosta riippumattomille toimijoille on myös lueteltu. Jokaiselle sektorille on listattu valvova viranomainen valvomaan direktiivissä mainittujen säädösten noudattamista. Lähtökohtaisesti NIS2-direktiivi ei kosketa kouluja suoraan, koska niitä ei lasketa direktiivin mukaisiin kriittisiin toimialoihin. Tilannetta muuttaa mahdolliset vaihtelut koulun asemasta ja sen palveluntarjoajista. Mahdollisesti koulu voi olla osa laajempaa kunnallista tai alueellista organisaatiota, joka mahdollisesti kuuluu NIS2-direktiivin piiriin. Koulussa käytössä olevat ICT-palvelut ja niitä tarjoavat yritykset saattavat kuulua direktiivissä mainittuihin soveltamisaloihin. Vaikka tällöin toimija itse vastaa asetuksessa mainituista vaatimuksista, voivat vaikutukset ulottua kouluun asti.

Toimijoiden on itse ilmoittauduttava valvovan viranomaisen toimijaluetteloon. Luettelon tiedot pitää ajantasaisina, toimijat velvoitetaan ilmoittamaan muutoksista viranomaiselle viipymättä ja ilmoituksen tekemiseen on myös asetettu takaraja. [24] Luettelossa pidetään kirjaa toimijasta ja sen yhteystiedoista. Lisäksi jokaisen toimijan keskeisyys määritellään ja missä Euroopan unionin valtioissa se tarjoaa NIS2-direktiiviin kuuluvia palveluja. Lisäksi varsinkin digitaalista infrastruktuuria ylläpitäviä palveluja tarjoaville yrityksille on mainittu vielä edellä kerrottujen tietojen lisäksi useita muita ilmoitettavia tietoja. Direktiivi velvoittaa toimijoita huolehtimaan kyberturvallisuuden riskienhallinnasta. Samalla palveluihin kohdistuvasta poikkeamista on toimijalla velvollisuus ilmoittaa valvovalle viranomaiselle kolmivaiheisesti. [25]

Vaikkakin NIS2-direktiivi kohdistuu kouluun lähinnä välillisesti, eikä aseta velvoitteita. On oppilaitoksen IT-ympäristön toiminnasta ja turvallisuudesta vastaavien henkilöiden hyödyllistä käyttää direktiivissä esitettyjä toimenpiteitä osana oppilaitoksen omaa riskienhallintaa. NIS2-direktiivi korostaa varsinkin organisaation ylimmän johdon vastuuta kyberturvallisuudesta. Oppilaitoksessa tämä tarkoittaa sitä, että koulun johdon kuten rehtorin tai IT-toiminnasta vastaavien viranhaltijoiden, tulee ymmärtää kyberturvallisuuteen liittyvät riskit ja huolehtia siitä, että tarvittavat toimenpiteet toteutetaan organisaation sisällä. Tilanne voi muuttua tulevaisuudessa, jos sääntely laajenee tai koulun rooli yhteiskunnan digitaalisessa infrastruktuurissa kasvaa. Tämän vuoksi on perusteltua, että koulut seuraavat aktiivisesti tilanteen kehitystä ja varautuvat mahdollisiin tuleviin vaatimuksiin jo ennakoivasti. [26] On oleellisen tärkeää, että koulun johto tunnistaa kyberturvallisuuden strategiseksi osa-alueeksi, joka vaikuttaa sekä opetuksen jatkuvuuteen että oppilaiden ja henkilöstön tietosuojaan. Kouluympäristössä tämä voi tarkoittaa esimerkiksi sitä, että koulun johto varmistaa opetushenkilöstölle ajantasaiseen tietoturvakoulutuksen sekä huolehtii siitä, että koulun digitaaliset järjestelmät ovat riittävällä tasolla suojattuja. Myös säännölliset auditoinnit ja varautumisharjoitukset voisivat tukea koulun omaa valmiutta mahdollisiin kyberuhkiin.

2.1.3 Kyberturvallisuuslaki

Kyberturvallisuuslaki on valmisteltu edellä mainitun NIS2-direktiivin pohjalta. Sen avulla NIS2-direktiivin mukaiset vähimmäisvaatimukset pannaan täytäntöön kansallisesti. Uuden lain pääasiallisena tavoitteena on parantaa ja yhtenäistää yhteiskunnan kriittisten toimijoiden kyberturvallisuutta, varautumista ja häiriötilanteiden hallintaa. Laissa mainitaan useita kriittisiä sektoreita kuten energia, vesihuolto, terveydenhuolto ja digipalvelut, joilla on merkittävä rooli Suomalaisen yhteiskunnan toimivuudessa. Velvoitteet kohdistuvat erityisesti keskisuuriin ja suuriin organisaa-

tioihin, mutta myös pienempiin toimijoihin, jos ne tarjoavat kriittisiä palveluita. Laki määrittää lähinnä Suomeen sijoittuneita toimijoita, mutta tietyissä tilanteissa lakia sovelletaan näiden rajojen ulkopuolelle, mikäli palvelu on saatavilla Suomessa. [27] Laki edellyttää lain määrittelemiltä toimijoilta ilmoittautumista valvovan viranomaisen toimijaluetteloon. Valvontaviranomaisen pääasiallinen tehtävä on seurata sääntelyn noudattamista sekä tarjota toimijoille ohjeistusta ja tukea. Viranomaisella on oikeus tarkastella toimijoita jopa paikan päällä tehtävillä tarkastuksilla. Mahdollisten puutteiden ja laiminlyöntien seurauksena viranomaisella on oikeus määrätä tarvittaessa sanktioita, kuten huomautuksia ja varoituksia. Vakavista laiminlyönneistä voidaan määrätä merkittäviä hallinnollisia seuraamuksia, kuten sakkoja tai toimintakieltoja.

Laissa määritetään toiminnallisia velvoitteita, esimerkiksi toimijoiden on ilmoitettava kyberturvallisuuspoikkeamista viranomaiselle ensimmäisen kerran 24 tunnin sisällä tapahtuneen poikkeaman havaitsemisesta, seuraava ilmoitus on tehtävä 72 tunnin kuluessa. Loppuraportti on lähetettävä kuukauden sisällä. Loppuraporttiin on sisällytettävä kuvaus poikkeamasta ja sen vakavuudesta. [24] Samoin yksityiskohtainen kuvaus poikkeaman vaikutuksista ja tehdyistä sekä tekeillä olevista toimista. Valvovalle viranomaiselle ilmoittamisen lisäksi on tiedotettava toimijoita, joiden palveluihin häiriö mahdollisesti vaikuttaa. Poikkeamailmoitus velvoittaa myös vastaanottajaa. Valvovan viranomaisen on aina vastattava viipymättä saamaansa ilmoitukseen. Eräs lakiin määritelty kohta velvoittaa toimijoita laatimaan kattava riskienhallinnan toimintamalli, jossa tunnistetaan ja hallitaan kyberturvallisuusriskit. Malliin sisältyy henkilöstön koulutuksen lisäksi, pääsynhallinta, tietoturvapoikkeamien käsittely ja varautuminen mahdollisiin häiriöihin. Toiminnan toteutumisesta ja hyväksynnästä vastaa ylin johto. Traficomin Kyberturvallisuuskeskus toimii keskeisenä koordinoijana ja tukee toimijoita häiriötilanteiden hallinnassa.

2.2 Henkilötietojen käsittely

Yhteiskunnassa sähköisen tiedon määrä lisääntyy jatkuvasti, mikä on havaittavissa myös opetustyössä. Koulujen nykyinen toiminta on riippuvainen erilaisista tiedonhallinta järjestelmistä, sillä oppilaitoksien arjessa käsitellään suuria määriä arkaluonteista dataa, kuten henkilötietoja.

EU:n yleinen tietosuoja-asetus GDPR sekä sen pohjalta luotu kansallinen Tietosuojalainsäädäntö, velvoittaa kouluja suojaamaan henkilötietoja asianmukaisesti. [28] Tietojen suojaaminen toteutetaan hallinnollisilla ja teknisillä toimilla, joiden avulla varmistetaan aineiston eheys sekä yksityisyyden suojaaminen käsittelyn ja säilytyksen ajan. Tietojen häviäminen tai joutuminen vääriin käsiin vaatii välittömiä toimenpiteitä ja aiheuttaa lähes poikkeuksetta oppilaitokselle taloudellista vahinkoa sekä mainehaittaa, joka heikentää opiskelijoiden ja huoltajien luottamusta koulun toimintaan. Häiriön, inhimillisen virheen tai hyökkäyksen johdosta tapahtunut tietoturvaloukkaus on ilmoitettava viipymättä valvontaviranomaisille ja asianomaisille, joiden tietoa loukkaus mahdollisesti koskee. Tietoruvaloukkauksia pyritään estämään kouluttamalla henkilökuntaa oikeisiin tietoturvakäytäntöihin, Hallitsemalla käyttöoikeuksia sekä toteuttamalla säännöllisiä tarkastuksia ja arviointeja. [29]

2.2.1 GDPR Yleinen tietosuoja-asetus

EU:n yleinen tietosuoja-asetus GDPR eli General Data Protection Regulation tuli voimaan 2018. Asetuksen pääasiallisena tavoitteena on suojella yksilöiden henkilötietoja sekä yhdenmukaistaa tietosuojakäytännöt koko Euroopan unionin alueella.[30] Asetus koskee kaikkia organisaatioita, jotka käsittelevät henkilötietoja, mukaan lukien oppilaitokset.

Koulussa käsitellään opiskelijoiden ja heidän huoltajiensa henkilötietoja. Käsiteltäviä henkilötietoja on järjestelmissä henkilöstä riippuen hyvin laaja kirjo. Nimien, syntymäaikojen ja muiden henkilön tunnistamiseen soveltuvien tietojen lisäk-

si, järjestelmissä on kirjattuna arvioinnit sekä oppimisen tuen tarpeen selvityksiä ja terveystietoja. Asetuksen myötä koulujen on huolehdittava siitä, että nämä tiedot käsitellään huolellisesti, lainmukaisesti ja turvallisesti. Asetus korostaa rekisteröityjen oikeuksia, sillä tietojen käsittely pohjautuu aina suostumukseen. Henkilöllä on myös oikeus tietää, mitä tietoja hänestä kerätään tai mihin niitä käytetään ja kuinka kauan niitä säilytetään. Lisäksi rekisteröity voi pyytää tietojensa oikaisemista tai poistamista. Asetus määrittelee myös tietoja, joita ei voi käsitellä. Näitä ovat muun muassa poliittinen ja sukupuolinen suuntautuminen.

Oppilaitos velvoitetaan ilmoittamaan tietosuojaviranomaiselle mahdollisista tietoturvaloukkauksista, olipa se tapahtunut vahingossa tai tahallisesti. Tietoturvaloukkaus voi tapahtua myös häiriön tai poikkeaman seurauksena, esimerkiksi oppilasrekisteri voi joutuu kyberrikollisen haltuun kouluun kohdistetun kyberhyökkäyksen yhteydessä. Tietoturvaloukkauksista on tehtävä ilmoitus tietosuojaviranomaiselle 72 tunnin kuluessa loukkauksen havaitsemisesta. Myös rekisterissä olevan henkilön tekemään yhteydenottoon on rekisterinylläpitäjän vastattava viipymättä.

Koulut käyttävät useita ulkopuolisia digitaalisia palveluja, kuten oppimisympäristöjä ja sovelluksia. GDPR edellyttää, että kouluilla on selkeät sopimukset palveluntarjoajien kanssa henkilötietojen käsittelystä. Lisäksi monilla kouluilla on nimetty tietosuojavastaava, joka seuraa asetuksen noudattamista ja neuvoo henkilökuntaa tietosuojaan liittyvissä kysymyksissä. GDPR määrittelee reunaehtoja henkilötietojen käsittelyyn. Tietoja käsiteltäessä on panostettava tarkkuuteen ja vastuullisuuteen. [31] Sen tarkoitus on suojella sekä oppilaita että henkilökuntaa. Samalla asetus tarjoaa mahdollisuuden kehittää koko kouluyhteisön tietoturvakulttuuria ja opettaa myös oppilaille tietosuojaasioiden merkitystä digitaalisessa maailmassa.

2.2.2 Tietosuojalaki

Suomessa toimiva tietosuojavaltuutettu on kansallinen valvontaviranomainen. Sen perustoimivaltaan kuuluu tietosuojalainsäädännön noudattamisen seuranta ja tietosuojatietoisuuden edistäminen. Lisäksi tietosuojavaltuutettu antaa lausuntoja ja osallistuu tietosuojaneuvoston kautta päätöksentekoon. Viranomaisena tietosuojavaltuutetulla on oikeus määrätä hallinnollisia seuraamusmaksuja ja uhkasakkoja tietosuoja-asetuksen noudattamatta jättämisestä. Eräs keskeisiä tietosuojavaltuutetun tehtäviä on valvoa 2019 vuoden alussa voimaan astuneen Suomen tietosuojalain toteutumista. Tietosuojalaki täydentää aikaisemmin ilmestynyttä EU:n yhteistä tietosuoja-asetusta. Tietosuojalaki ei siis muuta GDPR:n perusperiaatteita, mutta tuo mukanaan erityisiä sääntöjä, joita sovelletaan Suomessa. Laki käsittelee myös valvontaviranomaisen toimintaa ja toimivaltuuksia.

Tietosuojalaki määrittelee muun muassa nuorelle lapselle tarjottavien palvelujen sovellettavaa ikärajaa, joka on 13 vuotta. Lisäksi laki täsmentää tietosuojalain soveltamista Suomessa, sekä määrittelee erityisiä vaatimuksia ja poikkeuksia, jotka tulee huomioida eri sektoreilla henkilötietoja käsiteltäessä. [28] Koulutuksen järjestäjien näkökulmasta tietosuojalain soveltaminen on keskeinen osa oppilaitoksien vastuullisuutta. Henkilötietoja käsiteltäessä, sille on oltava selkeä oikeusperuste, kuten suostumus tai lakisääteinen velvoite. Henkilötietojen käsittelyä tulee tehdä vain tarpeen täyttävässä laajuudessa ja niiden hallinta tulee toteuttaa asianmukaisesti. Rekisteröityjen tietojen omistajalla on halutessaan oikeus saada tietää mitä tietoja hänestä säilytetään ja miten niitä säilytetään. Tietoja voi pyytää myös poistettavaksi varsinkin, jos tietojen säilytykselle ei ole enää edellytyksiä.

Oppilaitoksiin nimetyt tietosuojavastaavat toimivat koulujen lainsäädännön noudattamisesta vastaavina henkilöinä, sekä ilmoittavat tietosuojavaltuutetulle mahdollisista tietojen katoamisesta tai joutumisesta vääriin käsiin. [32] Opetushallitus on laatinut tietosuojaoppaan, joka tukee koulutuksen järjestäjiä lain soveltamisessa ja

käytännön toteutuksessa. Ammatilliset oppilaitokset kuten kaikki oppilaitokset ovat velvollisia huolehtimaan siitä, että opiskelijoiden, henkilöstön ja yhteistyökumppaneiden henkilötiedot käsitellään lainmukaisesti, turvallisesti ja läpinäkyvästi. [33] Tietosuojalain vaikutus ei rajoitu pelkästään teknisiin ratkaisuihin, kuten käyttäjähallintaan tai oppilaitoksen tapaan säilyttää ja hallita henkilötietoja. Myös itse koulutuksessa tietosuojaan liittyvä osaaminen onkin noussut keskeiseksi osaksi aloja, joissa tietojenkäsittely ja digitaalinen työskentely ovat jatkuvaa.

2.2.3 Julkisuuslaki

Suomalaisen hallintokulttuurin yksi keskeinen osa on julkisuusperiaate, jonka mukaan viranomaisten toiminta tulee olla mahdollisimman läpinäkyvää, mikä mahdollistaa ja helpottaa julkisen vallan käytön valvomista. Julkisuuslaki pyrkii avoimuuden lisäksi mahdollistamaan parempaa hallintoa ja yksilöiden oikeuksien toteutumista. Julkisuuslaissa määritellään muun muassa perusteet salassapidolle. Tilanteissa, joissa asiakirjan julkisuus mahdollisesti vaarantaa turvallisuuden, yleisen järjestyksen tai yksityisyyden suojan on erityisen tärkeää asettaa se salassa pidettäväksi. [34] Eteen saattaa tulla tilanteita, joissa asiakirjat sisältävät mahdollisia tietoja järjestelmien haavoittuvuuksista, turvajärjestelyistä tai tehdyistä toimenpiteistä. Tämän kaltaisten tietojen julkistaminen voi pahimmillaan helpottaa kyberrikollisten tai vihamielisten toimijoiden tavoitteiden saavuttamista. Tiedon Salaaminen tämän kaltaisissa tilanteissa voidaan nähdä keinona estää hyökkäyksiä ja suojata yhteiskunnan kriittisiä toimintoja.

Kyberturvallisuuden näkökulmasta viranomaisella on tärkeä tehtävä arvioida saatuja tietopyyntöjä siten, ettei turvallisuus vaarannu. Asiakirjojen luokittelun arviointi vaatii toimivalta viranomaiselta hyvää teknistä ja juridista osaamista. Väärä päätös voi johtaa pahimmillaan tarpeettomaan salailuun tai tietovuotoon, joista kummatkin ovat ei-toivottavia tapahtumia. Toisinaan asiakirja voi myös sisältää

osia, jotka ovat julkisia ja samalla osia, jotka täyttävät salassapidon kriteerit.

Julkisuuslakia sovelletaan yhdessä muiden vallitsevien lakien kanssa. Läheisesti vaikuttavia lakeja ja säädöksiä on muun muassa yleinen tietosuojaasetus ja tietosuojalaki. Tietosuoja esimerkiksi rajoittaa henkilötietojen julkisuutta, vaikka asiakirja olisi muuten julkinen. Oppilaitoksen toiminnassa julkisuuslaki toimii yhtenä oikeudellisena kehyksenä, joka ohjaa vahvasti koulun toimintaa. Samalla kun laki edistää avoimuutta ja luottamusta, se mahdollistaa kriittisten tietojen suojaamisen. [35] Kyberturvallisuuden ja tietoturvan kannalta salassapito on tärkeä työkalu, jonka käyttö vaatii tarkkaa harkintaa.

2.2.4 Tiedonhallintalaki

Julkisen hallinnon tietoaineiston hallintaa ohjaa tiedonhallintalaki, joka on säädetty ohjaamaan digitalisaation myötä kasvaneen tiedon määrän turvallista, yhdenmukaista ja laadukasta hallintaa. Tiedonhallintalailla pyritään määrittelemään miten viranomaisten tulee hallita tietoa, jotta se tapahtuisi mahdollisimman johdonmukaisesti, suunnitelmallisesti ja turvallisesti. Lain määrittelemä tiedonhallintamalli kuvaa käsiteltävän tiedon elinkaarta, jossa tietoturvan ja tietosuojan toteutumista korostetaan. [36] Lain määrittelemiä tietoturvavelvoitteita toteutetaan muun muassa kiinnittämällä huomiota käytössä olevien tietojärjestelmien suojauksen suunnitteluun ja toteutukseen, jotta ne olisivat tietoturvaperiaatteiden mukaisia. Dokumentoinnin ja läpinäkyvyyden tehostuminen auttaa rakentamaan toimivan kyberturvallisuusympäristön. Tietovarantojen dokumentointi auttaa tunnistamaan, mitä pitää suojata ja missä kriittinen tieto sijaitsee. Tiedon jakamisessa on erityisen tärkeää, että siinä käytettävät tekniset rajapinnat ovat hallittuja ja turvallisia. Kyberturvallisuuden näkökulmasta tämä vähentää tietovuodon ja väärinkäytöksien riskiä. Erityisen tärkeää tämä on tilanteissa, joissa arkaluontoista ja salattavaa tietoa siirretään järjestelmien välillä. [37] Ammattikoulu jakaa ja välittää tietoja useiden eri viranomaisten

ja yhteistyötahojen kanssa. Näihin kuuluvat muun muassa Kela, Opetushallitus sekä eri kunnat. Tietojen jakamisen tarkoituksena on varmistaa opiskelijoiden etuuksien, koulutuksen järjestämisen ja hallinnollisten velvoitteiden asianmukainen hoitaminen.

2.2.5 Muita aihetta sivuavia sekä välillisesti vaikuttavia lakeja, asetuksia ja ohjeistuksia

Edellä mainittujen lisäksi on suuri joukko muita lakeja, asetuksia ja ohjeistuksia, joiden raameissa oppilaitoksen ja sen kanssa tekemisissä olevien tahojen tulee toimia. Näin varmistetaan vastuullinen toiminta, joka suojaa kaikkien osapuolien oikeuksia. Yleisen tietosuojaasetuksen ja tietosuojalain lisäksi henkilötietojen käsittelyyn ja tietosuojan sääntelyyn vaikuttaa oppilas- ja opiskelijahuoltolaki, jonka on kohdennettu opiskelijahuollon arkaluonteisten tietojen suojaamiseen. Opiskelijahuollossa toimii esimerkiksi kuraattoreja ja muita terveydenhuollon ammattilaisia. [38] Muita tiedon hallintaa määritteleviä lakeja on muuan muassa laki digitaalisten palvelujen tarjoamisesta. Rikoslaissa luku 38 käsittelee tieto- ja viestintärikoksia, luvussa käsitellään tiedonhallintaan ja tietoliikenteeseen liittyvien rikkomusten määritelmiä sekä niistä seuraavia sanktioita. [39] Viestintäverkkoihin vaikuttavista laeista voidaan mainita sähköisen viestinnän palveluun vaikuttava laki ja tietoyhteiskuntakaari. [40] On tärkeää huomata, että ammattikoulun tietoturva ja kyberturvallisuus eivät perustu vain yksittäiseen lakiin, vaan niitä ohjaa laaja lainsäädännöllinen kokonaisuus.

2.3 Teknologian muutos tuo mukanaan uusia uhkia

IoT ja tekoälyn kaltaiset uudet teknologiat mullistavat tällä hetkellä yhteiskuntaa ja sen toimintaa, mutta toisaalta samaan aikaan ne altistuvat ja altistavat meidät uusille riskeille. Digitalisaation varjopuolena kyberuhkat ovat nousseet merkittäväk-

si globaaliksi huolenaiheeksi. Erilaiset kyberhyökkäykset voivat aiheuttaa laajoja taloudellisia vahinkoja ja häiriöitä yhteiskunnassa. Maailman talousfoorumin riskiraportti nostaa kyberturvallisuuden vaarantumisen yhdeksi viidestä suurimmasta maailmanlaajuisesta riskistä, mikä korostaa sen kriittistä merkitystä. [15] Organisaatioiden ja hallitusten onkin panostettava ennakoiviin toimenpiteisiin ja vahvistettava kyberturvallisuuttaan.

2.3.1 Tekoäly

Tekoälyn uskotaan mullistavan tietoturva-alaa, mikä on jo osittain havaittavissa. Varsinkin järjestelmät jotka tukeutuvat täi hyödyntävät tekoälyä ovat lisääntyneet. näiden työkalujen on tarkoitus havaita ja torjua erilaisia uhkia ilman ihmisen apua. Ihmisen jääminen pois toimintaketjun välistä nopeuttaa reagointia ja vähentää ihmisestä johtuvia virheitä. Mullistavaa tekoälyssä on sen kyky oppia ja kehittyä hyvinkin itsenäisesti, pysyen näin paremmin muuttuvien kyberuhkien tasalla. [41] Vaikka tekoälyyn perustuvat järjestelmät vapauttavat ihmisen vastuusta, ei ole kuitenkaan syytä luottaa näihin järjestelmiin sokeasti.

Tekoälyä käytetään samalla myös tehostamaan kyberhyökkäyksiä. Yhtenä esimerkkinä voidaan pitää tekoälyllä luotavia deepfake -väärennöksiä ja imitaatioita. Ne ovat videoita, kuvia ja ääntä, joita luodaan algoritmille annettujen syötteiden perusteella. Videoita tai äänitteitä voidaan manipuloida siten, että esimerkiksi rehtorin tai opettajan lausunnot voidaan tekaista täysin tyhjästä. Tämän kaltaiset videot leviävät verkon eri viestintäalustoilla nopeasti. Hyvin toteutettuja deepfake -videoita on vaikea erottaa oikeasta. [42] Näin voidaan pyrkiä erehdyttämään työntekijää esimerkiksi hyväksymään tekaistu maksu.

2.3.2 Esineiden internet

Internet of Things (IoT) tai esineiden internet tarkoittaa laitteita, joista käytetään arkikielessä nimitystä IoT-laitteet joita ovat muun muassa älytaulut, verkkotulostimet, valvontakamerat ja koulun WLAN-verkkoon yhdistetyt sensorit, lisäävät hyökkäyspinta-alaa. [43] IoT käsitteenä sisältää lähes kaikki esineet, joissa on antureita, ne saadaan liitettyä verkkoon ja niiden välillä liikkuu dataa. Näiden laitteiden tietoturva on usein heikompi kuin perinteisten päätelaitteiden kuten tietokoneiden. Siksi ne voivat toimia helppona porttina hyökkäyksille, jos niiden suojaus on laiminlyöty.

IoT-laitteiden haasteet johtuvat suurimmaksi osaksi laitteen valmistuksesta. Alalla kasvavan kilpailun johdosta laitteiden valmistus joudutaan siirtämään maihin ja valmistajille, jotka eivät ole kiinnostuneita laitteiden tietoturvasta ja käyttäjän tietojen suojaamisesta. Edullisesti tuotettuihin laitteisiin ei lähtökohtaisesti ole saatavilla ohjelmistopäivityksiä, jotka korjaisivat tai parantaisivat laitteiden suojausta. Laitteiden yhteinen standardointi estäisi heikkolaatuisten tuotteiden joutumisen markkinoille. [44] Ongelma näyttäytyy varsinkin yksittäisten kuluttajien keskuudessa, jotka tekevät ostopäätöksen halvan hinnan perusteella. Tulevaisuudessa oppilaitosten täytyykin varautua yhä monipuolisempiin uhkiin sekä teknisesti että toiminnallisesti. Ennaltaehkäisy, jatkuva koulutus ja selkeät toimintamallit kyberturvallisuuden hallintaan muodostavat perustan turvalliselle digitaaliselle oppimisympäristölle.

2.4 Suomalaiset toisen aseteen oppilaitokset ja niissä käytössä olevat järjestelmät hyökkäyksien kohteena

Suomessa on kohdattu jo useita eri oppilaitoksiin ja niiden käytössä oleviin tietoteknisiin järjestelmiin kohdennettuja kyberiskuja. Näiden järjestelmien häiriintyminen voi aiheuttaa merkittäviä ongelmia opetuksen jatkuvuudelle, tiedon saatavuudelle sekä henkilötiedot saattavat vaarantua. Verkosta löytyy jo jonkin verran erilaisia raportteja ja lopputöitä, jotka käsittelevät kyberiskuja sekä niistä toipumista. On tärkeä muistaa, että kaikkia hyökkäyksiä tai niiden yrityksiä ei tuoda yleiseen tietoisuuteen ja joskus niitä saatetaan jopa peitellä. Tiedotus ja läpinäkyvyys olisivat olennaisessa osassa iskuista toipumiselle.

Kyberhyökkäyksien motiivi ja toteutustapa riippuu usein kohteen luonteesta sekä iskun toteuttaneesta tahosta. Erilaisia motiiveja iskun taustalla saattaa olla muun muassa taloudellisen hyödyn tavoittelu, kiristys tai pelkkä häiriön aiheuttaminen. [17] Viime vuosina kiristyshaittaohjelmat ovat yleistyneet useilla sektoreilla ja niiden seurauksena on jouduttu sulkemaan järjestelmiään pitkiksikin ajoiksi.

2.4.1 Keski-Uudenmaan Koulutuskuntayhtymä

Vuonna 2022 marraskuun lopulla kohdistui Keski-Uudenmaan koulutuskuntayhtymä Keudaan Suomen oloissa poikkeuksellisen voimakas kyberhyökkäys. [1] Isku toteutettiin LockBit- kiristyshaittaohjelmaa käyttäen ja se aiheutti laajasti haittaa koulutuksen järjestäjän toimintaan. Hyökkäyksen torjumiseksi organisaation verkko- ja palveluyhteydet katkaistiin ja koko IT-ympäristö pysähtyi lähes kuukauden ajaksi. Keudan maaliskuussa 2023 julkaisemassa loppuraportista todetaan, että hyökkäyk-

[1] https://www.keuda.fi/2023/03/10/keudan-loppuraportti-kyberhyokkayksesta-on-valmistunut/

sestä toipuminen jatkuu edelleen loppuraportin julkaisuaikana. Loppuraportin mukaan hyökkäys ei johtunut varsinaisesti henkilökunnan, eikä opiskelijoiden toimista.

Keuda on Suomen viidenneksi suurin ammatillisen koulutuksen järjestäjä. Keski-Uudellamaalla sijaitsevalla koulutuskuntayhtymällä on 10 toimipistettä ja yli 800 työntekijää. Vuosittain koulussa opiskelee hieman yli 12 000 opiskelijaa. Hyökkäyksen kohteena on ollut kooltaan ja koulun käsittelemien opiskelijoiden ja henkilökunnan henkilötietojen arkaluonteisuuden vuoksi hyvin merkittävä kohde. Keudan IT-ympäristöön kohdistunut hyökkäys on kasvattanut huolta suomalaisten koulujen kyberturvallisuudesta. Koulujen digitalisoituminen luo väistämättä opetuksen järjestäjille uusia haasteita, joihin on pakko reagoida. Kouluissa tapahtunut digitaalinen kehitys on lisännyt huolta varsinkin kyberturvallisuuden osaamisen tasosta. Henkilöstön riittävä osaaminen tulisi varmistaa, jotta digitaaliset resurssit saadaan mahdollisimman hyvin ja turvallisesti hyödynnettyä. Nykyisin kyberturvataidot korostuvat työ- ja opiskeluelämässä. [45]

2.4.2 Etelä-Savon Ammattioppilaitos

Etelä-Savon ammattioppilaitos Esedu kohtasi marraskuussa 2023 haasteita siihen kohdistetun kyberhyökkäyksen vuoksi.[2] Kuten Keudan tapauksessa, kyberhyökkäyksen taustalla ei tässäkään tapauksessa ollut opiskelijoista tai henkilökunnasta johtuvia syitä. Vaikka Etelä-Savon ammattioppilaitos on kooltaan noin neljänneksen keudasta, opiskelee siellä kuitenkin vuosittain useita tuhansia opiskelijoita. Hyökkäyksen torjumiseksi ammattiopiston verkko- ja palvelinyhteydet suljettiin, jotta vahinkojen määrä saatiin rajattua mahdollisimman pieneksi. Laitteiden käyttöä rajoitettiin aluksi hyvin voimakkaasti, eikä verkon kautta toteutettua opetusta voitu järjestää. Oppilaitos toipui hyökkäyksestä suhteellisen nopeasti ja opetus saatiin palautettua lähes normaaliksi muutamassa viikossa. Maksujärjestelmien palauttami-

[2]https://esedu.fi/ajankohtaista/eseduun-kohdistunut-kyberhyokkays/

nen kesti hieman pidempään, mikä johdosta koulun ruokalan maksutoiminnoissa oli käytössä poikkeusjärjestelyt. Hyökkäyksen ja sen jälkeisien häiriöiden aikana henkilötietoja ei ole vuotanut ulkopuolisille. Syytä, miksi oppilaitos joutui hyökkäyksen kohteeksi ei ole tiedossa.

2.4.3 Helsingin kaupunki

Keväällä 2024 Helsingin kaupunki ilmoitti siihen kohdistuneesta tietomurrosta. [46] Tapahtuman tultua ilmi epäiltiin, että tekijä sai haltuunsa vain oppilaiden ja henkilöstön käyttäjätunnuksia ja sähköpostiosoitteita tietojenkalastelun seurauksena. Tapauksen selvittelyn yhteydessä ilmeni, että tietomurron kohdejoukko on paljon oletettua laajempi. Tapaus lukeutuu nykyisin Suomen mittakaavassa suurimpiin julkiseen sektoriin kohdistuneista tietomurroista. Tapaus sai alkunsa, kun kasvatuksen ja koulutuksen toimialan käyttämään taustajärjestelmään murtauduttiin, käyttämällä etäkäyttöpalvelimessa ollutta haavoittuvuutta. Ikävintä tapauksessa oli, että haavoittuvuuden korjaava päivitys oli jo saatavilla, mutta se oli jostain syystä jätetty päivittämättä. Tietomurron seurauksena hyökkääjä sai haltuunsa arkaluonteisia tietoja kaikista vuosina 2005–2018 syntyneistä helsinkiläisistä oppivelvollisista ja heidän huoltajistaan, kuten henkilötunnuksia, osoitteita, kansalaisuuksia, äidinkieliä ja uskonnollisia tietoja. Lisäksi vuoto koski myös kaupungin työntekijöitä, sijaisia ja työnhakijoita. Arvioiden mukaan tietomurto koski vähintään 150 000 henkilöä, mutta todellinen määrä voi olla jopa 300 000.

2.4.4 Wilma

Useissa suomalaisissa kouluissa on käytössä ohjelmistoyritys Visman julkiselle sektorille tuottama Wilma oppilashallintojärjestelmä, jonka yhtenä tärkeänä ominaisuutena on toimia yhteydenpidon välineenä koulun ja huoltajien välillä. Lukujen valossa kyseessä on erittäin laajalti käytössä oleva ohjelma, joka on käytössä yli 500

oppilaitoksessa ja organisaatiossa. Sen käyttäjämäärä on 2 miljoonan tienoilla. Hyvin laajalti suomen kouluissa käytössä oleva Wilma-järjestelmä pitää siis sisällään suuren määrän arkaluonteisia tietoja. [47]

Wilmaan on kohdistunut runsaasti hyökkäysyrityksiä pitkin vuoden 2024 syksyä. Organisaatio on ottanut vakavasti esiin tuodut epäilyt tietoturvariskistä, jonka taustalla on pääasiassa heikot salasanat. Järjestelmässä on ollut katkoja myös palvelunestohyökkäyksistä johtuen. Viime aikoina Wilma on lähestynyt asiakkaitaan kohonneen uhan vuoksi, ja onkin muistuttanut heidän osuudestaan vastata hallinnoimiensa käyttäjätunnuksien turvallisuudesta. Wilman sivuilla myös varoitetaan, että jos käyttää toisen henkilön käyttäjätunnuksia tai salasanoja ilman lupaa, se on rikos. Virkavalta tutkii tarvittaessa väärinkäytöksiä tunnuksien käytöstä jäävien jälkien perusteella.

Wilman kehityksessä panostetaan tietoturvan laatuun. Käyttämällä kehittyneimpiä saatavilla olevia suojausmekanismeja, joiden avulla hankaloitetaan tuntuvasti rikollisten toimintaa. Visma toteuttaa aktiivisesti ennalta ehkäisevää toimintaa auditoimalla tietoturvaa, tekemällä valvontaa ja omatoimista haavoittuvuustestausta. Näin tunnistetaan mahdollisia puutteita, joita päästään korjaamaan havaitsemisen jälkeen.[3] Wilman tietoturvan kannalta hyvin vaikuttava meriitti on kansainvälinen ISO 27001 standardi, joka luo tiukat vaatimukset tietoturvan hallintatoimille. Wilman tietoturvaa pyritään parantamaan myös ulkopuolisten tahojen avulla. Visma Bug Bounty-ohjelman avulla jossa eettisiä hakkereita palkitaan mahdollisien haavoittuvuuksien havaitsemisesta ja raportoinnista. [48] Wilma korostaa varsinkin monivaiheisen tunnistautumisen merkitystä hyvän tietoturvan luomisessa. Siksi selvityksen alla onkin, miten käyttäjät saataisiin kaikkein tehokkaimmin siirrettyä käyttämään monivaiheista tunnistautumista sisään kirjautumisessa. Haasteita monivaiheisen tunnistautumiseen siirtymiseen on luonut esimerkiksi se, ettei kaikilla käyt-

[3]https://www.wilma.fi/ajankohtaista/wilma-ottaa-tietoturvariskit-vakavasti-ja-auttaa-asiakkaita-suojautumaan-tietomurroilta

täjillä ole käytössään puhelinta, johon monivaiheiseen tunnistautumiseen soveltuvaa ohjelmaa voisi asentaa.

ISO 27000/ISO 27001

ISO 27001 on osa ISO 27000 standardisarjaa, joka on tietoturvallisuuden johtamisjärjestelmä. Lyhyesti ISO/IEC 27001 on kansainvälinen standardi, joka auttaa organisaatioita suojaamaan tietonsa luottamuksellisuuden, eheyden ja käytettävyyden osalta. Standardi ohjaa tietoturvallisuuden hallintajärjestelmän ISMS suunnittelua, käyttöönottoa, valvontaa ja jatkuvaa parantamista. [49] ISMS perustuu riskienhallintaan, jossa tunnistetaan ja käsitellään tietoturvariskejä organisaation tarpeiden mukaan. Johto on keskeisessä roolissa, sen on osoitettava sitoutumisensa, määriteltävä tietoturvapolitiikka ja varmistettava henkilöstön tietoturvatietoisuus. [50] Sisäiset ja ulkoiset auditoinnit arvioivat järjestelmän toimivuutta. Poikkeamat käsitellään korjaavilla toimenpiteillä ja järjestelmää kehitetään jatkuvasti. ISO 27001 ei koske vain teknologiaa, vaan koko organisaation toimintaa. Se tukee luotettavaa ja tehokasta tietoturvaa liiketoiminnan vaatimusten mukaisesti.

3 Oppilaitoksien kyberturvallisuudesta tehtyjä aikaisempia tutkimuksia ja kirjallisuutta

Viime vuosina kyberturvallisuudesta on julkaistu runsaasti kirjallisuutta, artikkeleita ja tutkimuksia. Varsinkin tieteellisten tutkimusten määrä on lisääntynyt, mikä johtunee kyberturvallisuuden noususta hyvin keskeiseksi aiheeksi. Suuri osa tieteellisestä tekstistä käsittelee aihetta yleisellä tasolla tai keskittyy yritys- ja organisaatiolähtöisiin tarpeisiin. Kouluympäristöön erityisesti suunnattua tutkimusmateriaalia on edelleen verrattain vähän saatavilla. Aiheesta on kuitenkin tehty joitakin opinnäytetöitä, jotka tukevat tämän työn taustaa ja muodostavat tärkeän viitekehyksen tarkastelulle.

Jyväskylän yliopiston opiskelija Annika Nykänen on julkaissut pro gradu -tutkielman, joka käsittelee kyberturvallisuutta ja tietoturvaa suomalaisessa peruskouluympäristössä. [14] Tutkielmassa tarkastellaan nopeasti kehittyvän teknologian aiheuttamia haasteita opetuksessa, kun koulujen odotetaan pysyvän digitalisaation tahdissa. Opetussuunnitelmat korostavat yhä enemmän digitaalisten taitojen opetusta, mikä vaatii niin oppilailta kuin opettajilta uudenlaista osaamista ja ymmärrystä

tietoturvasta. Pro gradu -tutkielma osoittaa, että sekä opettajien että oppilaiden digitaaliset taidot ovat usein heikkoja tai korkeintaan perustasoisia. Monet opettajat eivät ole saaneet koulutusta tieto- ja viestintäteknologiasta opiskeluaikoinaan, ja täydennyskoulutus keskittyy usein laitteiden käyttöön pedagogisen osaamisen sijaan. Oppilaiden digitaaliset taidot puolestaan painottuvat viihdekäyttöön kuten pelaamiseen tai sosiaalisen median käyttöön, mikä korostaa tarvetta systemaattiselle kyberturvallisuusopetukselle. Työ nostaa esiin eräitä riskejä, kuten plagioinnin, verkkokiusaamisen ja yksityisyyden loukkaukset. Tutkielmassa arvioidaan myös opettajien ja oppilaiden valmiuksia toimia turvallisesti digitaalisessa ympäristössä. Tulosten perusteella esitetään kehitysehdotuksia, joiden avulla koulujen kyberturvallisuutta voitaisiin parantaa. Digitaalisiin avaintaitoihin kuuluu tiedonhallintaa, laitteiden ja ohjelmistojen sekä verkon turvallista käyttöä. Peruskoulun tehtävänä on vahvistaa näitä taitoja, taaten opiskelijoille valmiudet menestyä tulevaisuudessa. Opetushallitus on määritellyt tietoturvallisuuden keskeiseksi osa-alueeksi, mikä tarkoittaa koulujen kontekstissa esimerkiksi oppilaiden henkilötietojen suojaamista, laitteiden ja ohjelmistojen turvallista käyttöä sekä selkeää tietoturvapolitiikkaa. GDPR-asetuksen mukaisesti oppilaiden tiedot kuten arvosanat, poissaolot ja valokuvat on suojattava huolellisesti, mikä edellyttää kouluilta selkeitä käytäntöjä ja ohjeistuksia.

Annika Nykäsen tutkimus osoittaa, että kyberturvallisuuden opetus peruskouluissa vaihtelee suuresti. [14] Osa opettajista sisällyttää aihetta opetukseensa aktiivisesti, kun taas osa ei lainkaan. Alakoulun opettajat huomioivat kyberturvallisuuden opetuksessaan useammin kuin yläkoulun opettajat. Lisäksi opettajat kokevat, että opetussuunnitelman ohjeet ovat liian yleisluontoisia ja täydennyskoulutus riittämätöntä. Tämä johtaa siihen, että käytännöt vaihtelevat huomattavasti eri koulujen ja kaupunkien välillä. Tutkimuksen lopussa esitetään kaksi kehityspolkua kyberturvallisuuden opetuksen vahvistamiseksi. Ensimmäinen polku korostaa kyberturvalli-

suuden sisällyttämistä kaikkiin oppiaineisiin osana laaja-alaista osaamista. Toinen vaihtoehto on eriyttää kyberturvallisuuden kokonaan omaksi oppiaineekseen, jolloin sille annettaisiin selkeämpi asema koulun opetuksessa. Lisäksi ehdotetaan yleisten tietoturvaohjeiden laatimista opettajille, jotta käytännöt olisivat yhtenäisempiä ja tukisivat oppilaiden turvallista toimintaa digitaalisessa ympäristössä.

Toinen aihetta läheisesti käsittelevä työ on Miiro Pyysingin ja Sari Kaipaisen opinnäytetyö, jossa tarkastellaan kyberturvallisuuden opetuksen nykytilaa ja tulevaisuuden kehitystarpeita. [6] Työssä haastateltiin opettajia ja kyberturvallisuuden asiantuntijoita. Hämeen ammattikorkeakoulussa vuonna 2022 valmistunut insinöörіopinnäytetyö tarkastelee, miten kyberturvallisuutta opetetaan suomalaisessa peruskoulussa ja millaisia tulevaisuuden suuntaviivoja alan asiantuntijat näkevät opetukselle. Työn tilaajana toimi Opetushallitus, mikä kertoo aiheen ajankohtaisuudesta ja yhteiskunnallisesta painoarvosta. Tutkimus rakentui kahdesta kyselytutkimuksesta joista toinen suunnattiin peruskoulun opettajille ja toinen kyberturvallisuusalan ammattilaisille. Erityisesti asiantuntijat korostivat sitä, kuinka opetettavat sisällöt ovat vielä hajanaisia ja varsinaista ohjeistusta on niukasti. Kyberturvallisuuden opetus on tällä hetkellä pitkälti opettajan oman kiinnostuksen ja osaamisen varassa. Opettajat kokevat tarvitsevansa lisäkoulutusta ja konkreettisia ohjeita, jotta kyberturvallisuutta voitaisiin opettaa systemaattisemmin. Sekä opettajat että asiantuntijat pitävät kyberturvallisuustaitoja välttämättöminä kansalaistaitoina. Työssä esitetään ratkaisuksi opetushenkilökunnan koulutuksen lisäämistä sekä opetussuunnitelmien täsmentämistä kyberturvallisuuden osalta.

Oulun ammattikorkeakoulussa toteutettu ylemmän ammattikorkeakoulun opinnäytetyö paneutuu päiväkodin henkilöstön tietosuoja- ja tietoturvakoulutuksen kehittämiseen. Opinnäytetyön tekijöinä Heli Mönttinen ja Heidi Piekkari. [51] Työssä perehdytään digitalisaation luomiin osaamistarpeisiin ja päiväkodin henkilöstön tietosuoja- ja tietoturvakoulutuksen kehittämiseen. Työn lähtökohtana oli Touhula

Leikki Oy:n tunnistama tarve vahvistaa henkilöstön osaamista tietoturva-asioissa. Työssä korostetaan, että teknologian nopea kehitys ja henkilötietojen kasvava arvo lisäävät riskejä, jotka kohdistuvat sekä organisaatioihin että yksilöihin. Kyberhäiriöt, tietojenkalastelu ja huijaukset ovat yleistyneet, ja niiden seuraukset voivat olla taloudellisia ja maineeseen liittyviä. Päiväkotien kontekstissa erityisen kriittistä on lasten henkilötietojen suojaaminen, sillä lapset eivät itse kykene arvioimaan tietojensa jakamisen riskejä. Työn konkreettisena tuotoksena syntyi kuusiosainen koulutusmateriaali ja uusi koulutusmalli. Materiaali koostuu koulutusvideoista, jotka on suunnattu päiväkodin arkeen sekä kirjallisesta tietosuoja- ja tietoturvaohjeistuksesta.

Vaikka materiaalin tarkkaa sisältöä ei raportoitu julkisesti sen arkaluontoisuuden vuoksi, sen tarkoituksena on lisätä henkilöstön tietoturvatietoisuutta ja kykyä toimia oikein erilaisissa digitaalisissa tilanteissa. Koulutusmalli on itsessään joustava ja sitä voitaisiin soveltaa myös muiden ammattiryhmien koulutuksiin. Työ osoittaa, että tietosuoja- ja tietoturvakoulutuksen kehittäminen on välttämätöntä varhaiskasvatuksen nykyisessä toimintaympäristössä. Henkilöstön osaaminen liittyy laajasti organisaation vastuullisuuteen ja lasten oikeuksien turvaamiseen. Lisäksi työ tuo esiin, että henkilöstön toiminta voi olla suurin uhka organisaation kyberturvallisuudelle, mikä tekee koulutuksesta entistä tärkeämpää. Koulutusmallin kehittäminen vahvistaa organisaation kykyä vastata digitalisaation haasteisiin ja luo pohjan jatkuvalle osaamisen kehittämiselle. Työ kuvastaa hyvin oman työni tarpeellisuutta ja ajankohtaisuutta.

Edellä tarkasteltujen lopputöiden yhteenvetona voidaan todeta, että tutkimusta koulumaailman kyberturvallisuudesta on olemassa, mutta se on hajanaista ja usein paikallisesti toteutettua. Lisäksi monet julkaisut keskittyvät yksittäisiin osa-alueisiin, kuten opettajien osaamiseen tai opetussuunnitelmien kehittämiseen, mutta kokonaisvaltaista tarkastelua on vähemmän. Tämä osoittaa tarpeen lisätutkimuksel-

le, jossa koulujen kyberturvallisuus nähdään sekä teknisenä että kasvatuksellisena ilmiönä, joka vaikuttaa välillisesti myös kaikkiin koulun sidosryhmiin. Vaikka tietoturvaohjelmistot ja laitehallintaan ovat tärkeitä, on tukimusta ja osaamista edistettävä niin, että huomioi myös pedagogiset ulottuvuudet. Kokonaisvaltainen lähestymistapa edellyttää selkeitä linjauksia siitä, miten turvallinen digitaalinen kulttuuri rakennetaan ja ylläpidetään. Kyberturvallisuus olisi syytä nähdä osana koulun laajempaa kasvatustehtävää. Se ei ole vain suojaamista uhkia vastaan, vaan myös oppimisen mahdollistamista turvallisessa ympäristössä.

Kyberturvallisuuden tutkimuksessa olisi hyödyllistä tarkastella myös koulujen arjen käytäntöjä ja niiden vaikutusta oppilaiden digitaaliseen turvallisuuteen. Esimerkiksi se, miten opettajat ohjaavat oppilaita käyttämään verkkoa vastuullisesti, vaikuttaa suoraan siihen, millainen turvallisuuskulttuuri koulussa muodostuu. Samalla tulisi kiinnittää huomiota oppilaiden osallisuuteen ja heidän kokemuksensa sekä näkemyksensä voivat tarjota arvokasta tietoa siitä, millaisia riskejä ja haasteita koulun digitaalisessa ympäristössä kohdataan. Lisäksi laajempi vertailu voisi tuoda esiin, miten eri koulut lähestyvät kyberturvallisuutta ja mitä hyviä käytäntöjä voitaisiin soveltaa laajemmin. Tämä auttaisi hahmottamaan, onko kyseessä paikallinen ilmiö vai laajemmalle ulottuva haaste. Samalla se loisi pohjaa yhteisille standardeille ja suosituksille, jotka tukisivat koulujen kykyä vastata digitaalisen maailman riskeihin.

Työn ollessa hyvin poikkitieteellinen on syytä tarkastella kyberturvallisuuden opetuksen lisäksi aineistoa pedagogiikasta, kyberturvallisuudesta, tietoturvallisuudesta ja osin käyttäytymismallien sekä psykologian tuntemuksesta on apua. Perustuuhan kyberturvallisuus itsessäänkin osittain psykologiaan ja ihmisen käyttäytymisen tuntemiseen.

Työssä tukeudutaan myös kyberturvallisuudesta yleisesti kertovaan kirjallisuuteen, sekä teknisesti hyvin yksityiskohtaiseen materiaalin, missä käsitellään vain yhtä

osa-aluetta. Aineistossa tutustuttiin esimerkiksi oppivelvollisuusikäisten opiskelijoiden kokemuksia tuntoaistin vaikutuksesta käsitöitä tehdessä. [52] Työ paneutuu käsitöiden tulevaisuuteen pohtimalla tuntoaistin merkitystä. Työ antaa hyvän kuvan kinesteettisestä oppimistyylistä. Muita pedagogiikkaan ja oppimistyyleihin keskittyviä aineistoja oli Jyväskylän Yliopiston lopputyö Oppilaan visuaalisen hahmottamisen vaikeudet opettajien kertomana ja Oppimistapojen huomioiminen musiikinopetuksessa. [53] Oppimista käsitteleviä lopputöitä ja kirjallisuutta on työn tekemiseen käytetty noin kymmenkunta kappaletta. Aineistoa on laajalti myös käyttäytymismalleista, jotka painottuvat lähinnä nuoriin ihmisiin.

4 Kyberturvallisuus oppilaitoksessa

Koulun tieto- ja kyberturvallisuudesta vastaa joukko eri tahoja ja henkilöitä, joiden määrä riippuu oppilaitoksen koosta ja rakenteesta. Päävastuu oppilaitoksen kyberturvallisuudesta on kuitenkin johdolla ja ICT-osastolla. ICT-henkilöstön lisäksi erilaiset tietotekniikkaan sekä turvallisuuteen perehtyneet asiantuntijat huolehtivat teknisistä ratkaisuista joko itse tai yhdessä ulkoisten palveluntarjoajien kanssa. Perinteisiä teknisiä suojautumismenetelmiä ovat erilaiset palomuuri- ja virustorjuntaratkaisut. Käyttäjien pääsyä rajoitetaan ja henkilökunnan käyttämä verkko on eristetty koulun muusta verkosta. Lisäksi suojausta tehostetaan esimerkiksi tunkeutumisen tunnistavilla järjestelmillä ja turvallisen etäyhteyden mahdollistavalla virtual private network (VPN) verkkoyhteyden salauksella.

Käyttäjähallinalla saadaan rajattua pääsy vain niihin tietoihin ja järjestelmiin, mitä henkilöstö työssään tarvitsee. [54] Varsinkin oppilaitos ympäristössä tämä on oleellista. Kirjautumisesta turvallisempaa tekee monivaiheisen tunnistautumisen käyttöönotto, mikä lisää merkittävästi tilien ja tietojen suojausta. On hyvä muistaa, että suurin osa kyberhyökkäyksistä saa alkunsa käyttäjän tekemästä inhimillisestä virheestä. [51] Varsinaisen ICT-henkilöstön lisäksi on nimetty erillisiä vastuuhenkilöitä, joiden tehtävänkuvaan kuuluu normaalin työn lisäksi erinäisiä vastuutehtäviä. Koulun johto vastaa strategia tasolla, että kyberturvallisuus on osa toimintakulttuuria ja sille on varattu riittävät resurssit.

Henkilökunnan ja opettajien rooli kyberturvallisuudessa on toimia annettujen

ohjeiden mukaan ja ohjeistaa osaltaan opiskelijoita toimimaan turvallisesti opetusympäristössä. Varsinkin opettajilla on suuri rooli opiskelijoiden opastamisessa turvalliseen digikäyttäytymiseen. On hyvä ymmärtää kuinka suuressa roolissa opiskelijat ovat turvallisen toimintaympäristön ylläpitämisessä. Vaikka tekniset ratkaisut ja henkilökunnan ohjeistus sekä toiminta olisivat kunnossa, opiskelijan toiminta vaikuttaa yhtä lailla suoraan oppilaitoksen tietoturvaan. [45] Tärkeää on varmistaa myös opiskelijoiden ajantasainen osaaminen ja varmistaa, että oppilaat noudattavat annettuja ohjeita.

4.1 Tekniset ratkaisut

Erilaiset ratkaisut ja palvelut ovat tärkeä osa koulun kyberturvallisuutta ja ne on osittain toteutettu tiiviissä yhteistyössä ulkoisten palveluntarjoajien kanssa. Kyberturvallisuuden kenttä muuttuu jatkuvasti ja uusia uhkia ilmestyy yksi toisensa jälkeen. Ulkoistetuilla palveluntarjoajilla on kyberturvallisuuteen liittyvää asiantuntemusta ja osaamista jota IT-henkilöstöltä ei välttämättä löydy. Ulkoistamisella saadaan aikaan usein myös säästöjä, sillä oman henkilöstön palkkaaminen ja kouluttaminen on lähtökohtaisesti kallista. Palveluntarjoajilla on valmiiksi räätälöityjä ratkaisuja, joita voidaan helposti muokata asiakkaan vaatimusten ja tarpeen mukaan. Ulkoistamalla kyberturvallisuusratkaisuja saadaan vapautettua IT-henkilöstön resursseja muuhun käyttöön. [5] Samoin eri palvelujen päivittäminen ja ylläpito on palveluntarjoajan vastuulla, jolloin organisaation oman henkilöstön ei tarvitse huolehtia siitä. Usein reagointi poikkeustilanteisiin on myös ulkoisilla palvelujentarjoajilla nopeampaa.

Palomuuriratkaisut toimivat suojana koulun sisäverkon ja ulkomaailman välillä, pyrkien estämään luvattoman pääsyn koulun verkkoon. Koulun verkon reunalle toteutetut palomuurit ovat useimmiten laitepohjaisia, kun taas ohjelmistopohjaisia palomuureja käytetään loppukäyttäjien laitteilla. Palomuurin lisäksi yksi oleellisim-

pia suojauksia ovat virustorjunta- ja haittaohjelmasuojaohjelmistot. [27] Ne tunnistavat, estävät ja poistavat havaittuja haittaohjelmia, jotka aiheuttavat ei-toivottua toimintaa laitteella ja verkossa. Ohjelmien ajantasaisuus on hyvin ratkaisevassa roolissa niiden toimivuuden kanssa, siksi ohjelmien päivitykset tulee asettaa automaattiseksi. Ohjelmistojen toiminnallisuuksissa on eroja ja ne monesti räätälöidään organisaation tarpeisiin sopiviksi.

Oppilaitoksen verkkoa on pyritty suojaamaan jakamalla sitä osiin. Esimerkiksi vieraille tarkoitettu verkko ja opiskelijoiden käyttämä verkko pidetään erossa hallinnon verkosta, näin mahdolliset opiskelijaverkosta alkaneet tai sinne levinneet hyökkäykset eivät pääse etenemään niin helposti kriittisiin järjestelmiin. Varmuuskopiointi auttaa tietojen palauttamisessa nopeasti. Jos hyökkäyksen sattuessa tietoja yritettäisiin tuhota, olisivat ne varmuuskopioituna pilvipalvelussa tai fyysisellä laitteella. Jo pelkästään laitteen tavanomainen rikkoutuminen voi johtaa tietojen menetykseen ilman varmuuskopiointia.

Henkilökunnalle tulee eteen tilanteita, jolloin joutuu työtehtävien vuoksi poistumaan oppilaitoksen alueelta, mutta koulun järjestelmien käyttäminen on työtehtävien hoitamiseksi välttämätöntä. Tällöin tulee käyttää virtuaalista erillisverkkoa muodostaakseen turvallisen etäyhteyden koulun sisäverkkoon. VPN on hyödyllinen työkalu henkilökunnan arjessa, mutta sen käyttöä pitää hallita ja valvoa, jotta sitä ei käytetä väärin. Mikäli VPN-yhteys on konfiguroitu väärin, se voi pahimmillaan avata väylän koulun verkkoon ilman rajoituksia. Näissä tilanteissa henkilökunnan kotilaite voi toimia väylänä haittaohjelmille, jotka pääsevät koulun sisäverkkoon avoimen VPN-yhteyden kautta. Ilmaisia VPN-palveluja ei tule käyttää, sillä ne vuotavat ja keräävät tietoa käyttäjän tietämättä, pahimmillaan ilmainen VPN voi olla itsessään haittaohjelma. [55] Verkossa liikkuvan tiedon suojaamista toteutetaan salaamalla tiedonsiirtoa, aikaisemmin mainittu VPN-yhteys on yksi monista menetelmistä, joilla estetään tietojen sieppaamista verkossa. Yhtenä tärkeänä ratkaisuna

voidaan pitää verkonvalvontajärjestelmiä, jotka auttavat koulun IT-henkilöstöä ja ulkopuolisia palveluntarjoajia havaitsemaan sekä torjumaan kyberuhkia nopeasti. Käyttäjähallinnan kautta tehtyjen rajauksien lisäksi salasanoihin ja monivaiheiseen tunnistautumiseen kiinnitetään huomiota.

4.2 Henkilökunnan rooli

Kyberturvallisuus ei rajoitu pelkästään teknisiin ratkaisuihin, siihen kuuluu myös ihmisten toimintaa. Oppilaitoksessa henkilökunnalla on tärkeä rooli kyberturvallisuuden ylläpitämisessä. Vaikkakin verkkoa ja järjestelmiä suojataan erillaisin menetelmin, inhimilliset virheet voivat johtaa tietovuotoihin ja kyberhyökkäyksiin. Sen vuoksi henkilökunnan vastuullinen toiminta on ratkaisevaa. Käsiteltävän luottamuksellisen tiedon kanssa on noudatettava tietoturvakäytäntöjä ja työskenneltävä vastuullisesti. Laitteiden ja ohjelmien turvallinen käyttö kuuluu henkilökunnan vastuulle. [6] Salasanojen ja käyttäjätunnusten hallinnassa on oltava tarkkana, salasanojen tulisi olla yksilöllisiä ja mahdollisimman monimutkaisia, tunnuksien ei myöskään pidä joutua ulkopuolisten käsiin.

Kyberturvallisuus harvemmin rajoittuu pelkästään teknisiin ratkaisuihin, siihen kuuluu oleellisesti myös ihmisten toimintaa. Oppilaitoksessa henkilökunnalla on tärkeä rooli kyberturvallisuuden ylläpitämisessä. Vaikkakin verkkoa ja järjestelmiä suojataan erilaisin menetelmin, inhimilliset virheet voivat johtaa tietovuotoihin ja kyberhyökkäyksiin. [6] Käsiteltävän luottamuksellisen tiedon kanssa on noudatettava tietoturvakäytäntöjä ja työskenneltävä vastuullisesti. Laitteiden ja ohjelmien turvallinen käyttö kuuluu henkilökunnan vastuulle. Salasanojen ja käyttäjätunnusten hallinnassa on oltava tarkkana.

Henkilökunnalla tulisi olla osaamista tunnistaa ja toimia mahdollisten verkkouhkien varalta. Esimerkiksi henkilökuntaa piinataan jatkuvasti epäilyttäviä linkkejä sisältävien tietojenkalasteluviestien avulla. Henkilöstön tulisi osallistua kyberturvalli-

suutta ja tietoturvaa sisältäviin koulutuksiin, jotta heillä olisi ajantasainen ymmärrys vallitsevista riskeistä. Voidaan sanoa, että kyberturvallisuus on jatkuva prosessi, jonka onnistumisessa koulun henkilökunta on tärkeimpänä osatekijänä. Teknisten ratkaisujen ja henkilöstön toiminnan onnistuminen on suurelta osin kiinni johdon määrittelemistä raameista, joiden puitteissa koko koulu ja sen kyberturvallisuus toimii. Johdon tehtävänä on vastata siitä, että oppilaitoksessa on selkeä suunnitelma ja strategia, kuinka kyberturvallisuutta hoidetaan. Tavoitteet, vastuut, riskienhallinta ja ohjeistus tulee olla ajan tasalla. [45] Johdon rooli tällöin on näyttää esimerkkiä ja varmistaa, että kaikki työntekijät sitoutuvat siihen. Tieto- ja kyberturvallisuus vaatii toimiakseen resursseja, kuten rahaa, aikaa ja osaamista. Johdon tuleekin varmistaa, että koululla on riittävät resurssit kyberturvallisuuden hoitamiseksi. Kriisitilanteissa johdon rooli on ohjeistaa ja johtaa viestintää henkilökunnan, huoltajien ja viranomaisten suuntaan. Päättävässä asemassa olevien henkilöiden tulee olla tilanteen tasalla ja ohjata toimintaa. Lopuksi voidaan todeta, että oppilaitoksen johto toimii kyberturvallisuuden selkärankana.

4.3 Opiskelijoiden rooli

Opiskelijan vaikutus kyberturvallisuuteen lähtee liikkeelle yksinkertaisista arjen valinnoista. Esimerkiksi salasanat, kalasteluviestien tunnistaminen sekä verkkosivujen turvallinen käyttäminen ovat peruskäytäntöjä, joilla opiskelija voi vaikuttaa merkittävästi koko koulun turvallisuuteen. Heikon salasanan vuotaminen tai haittaohjelman lataaminen koulun verkossa voi johtaa pahimmillaan koko järjestelmän vaarantumiseen. Sähköpostiin tulevat viestit, jotka yrittävät saada opiskelijaa klikkaamaan haitallista linkkiä voivat avata hyökkääjälle pääsyn koulun järjestelmiin. Opiskelijat käyttävät usein omia laitteitaan koulutehtävien tekemiseen, joko koulun verkossa tai sen ulkopuolella. Näissä tilanteissa on tärkeää ymmärtää, että epähuomiossa asennettu haittaohjelma tai suojaamaton laite voi toimia väylänä kyberhyökkäykselle.

Myös laitteiden jättäminen ilman valvontaa ja jakaminen toisten kanssa voivat vaarantaa koulun tietoturvan.

Koulujen tarjoamien laitteiden ja järjestelmien käyttäminen vastuullisesti edellyttää myös, että opiskelija ei pyri kiertämään järjestelmien suojaustoimia, kuten estettyjä sivustoja tai ohjelmistorajoituksia. Vaikka nämä rajoitukset voivat tuntua turhauttavilta, ne on yleensä asetettu suojaamaan oppilaitosta ja sen käyttäjiä. [20] Opiskelijoiden asenteella on keskeinen merkitys kyberturvallisuuskulttuurin muodostumisessa kouluyhteisössä. Jos turvallisuutta pidetään vain rajoittavana tekijänä, opiskelijat voivat suhtautua siihen välinpitämättömästi tai jopa uhmakkaasti. Sen sijaan, jos opiskelijat ymmärtävät, että heidän toimintansa vaikuttaa myös muiden turvallisuuteen, syntyy vastuullinen ja yhteistyöhön perustuva ilmapiiri.

4.4 Kyberturvallisuuden opetus kouluympäristössä

Kyberturvallisuuden opetus kouluympäristössä on hyvä nähdä osana laajempaa digitaalista osaamisen kehittämistä. Digitalisaation myötä kouluissa käytettävien digitaalisien laitteiden ja verkkoalustojen määrä on lisääntynyt. Vastuullisuuden opetuksen tärkeys korostuu digitaalisessa ympäristössä. Kyberturvallisuuden opetuksella tarkoitetaan tässä yhteydessä oppilaiden ja koulun henkilöstön ohjaamista ja opetusta, jotta heillä olisi tarvittava tieto ja taito verkkoympäristöön liittyvien riskien ymmärtämisessä ja hallinnassa. Heillä tulisi olla myös ymmärrys tietoturvallisesta ja eettisestä toimimisesta digitaalisissa tilanteissa. [20] Vuonna 2014 julkaistussa perusopetuksen opetussuunnitelman perusteissa velvoitetaan kouluja tukemaan oppilaiden laaja-alaista osaamista, johon sisältyy digitaalisten taitojen lisäksi myös tietoturva- ja tietosuojaosaaminen. Opiskelijoita kannustetaan käyttämään tieto- ja viestintäteknologiaa oppimisen tukena, jotta heidän osaamisensa esimerkiksi erilaisten laitteiden ja ohjelmistojen käytöstä syvenee. Tietoturvaan liittyvä opetus tapahtuu osana muita aineita. [56] Käytännössä tämä tarkoittaa, että esimerkiksi äidinkie-

len tunneilla voidaan käsitellä verkkokirjoittamisen pelisääntöjä ja lähdekritiikkiä, kun taas tietotekniikan tunneilla keskitytään esimerkiksi salasanojen turvalliseen käyttöön ja ohjelmistojen päivityksiin.

Tutkimusten ja opinnäytetöiden mukaan kyberturvallisuuden opetus on kouluissa vielä hajanaista. [6] Opetuksen laajuus ja sisältö riippuvat usein yksittäisten opettajien osaamisesta ja kiinnostuksesta aihetta kohtaan. Selkeitä yhtenäisiä ohjeistuksia on vähän. Harva koulutus itsessään tarjoaa opettajalle tarpeeksi laajaa ymmärrystä aiheen opettamiseen. Myös koulun resurssit, kuten tekninen tuki, ajantasainen laiteympäristö ja yhteiset toimintamallit, vaikuttavat merkittävästi opetuksen toteutukseen. Oppilaiden, joskin myös henkilökunnankin kohdalla osaamisen taso vaihtelee suuresti. Vaikka nuoret käyttävät pääsääntöisesti digitaalisia palveluita sujuvasti, heillä ei välttämättä ole riittävää ymmärrystä tietoturvariskeistä tai omien tietojen suojaamisen merkityksestä. Siksi kyberturvallisuuden opetus ei voi rajoittua vain teknisiin taitoihin, vaan sen tulee sisältää myös kriittistä ajattelua, eettisyyttä ja vastuullisuutta korostavia näkökulmia. Kyberturvallisuuden opetus tulisi olla enemmässä määrin osa koulujen kasvatustehtävää. Sen tukisi tukea oppilaiden valmiuksia toimia turvallisesti ja vastuullisesti digitaalisessa yhteiskunnassa ja ehkäistä osaltaan myös digitaalisia uhkia, kuten identiteettivarkauksia, Tämän kaltainen osaaminen korostuu työelämään siirryttäessä. Kokonaisvaltaisesti toteutettuna kyberturvallisuuden opetus ei ole vain yksittäisten opettajien vastuulla, vaan se tulisi sisällyttää osaksi koko kouluyhteisön arvoja, käytänteitä ja pedagogista kulttuuria.

Koulujen henkilökunnan koulutus on pääsääntöisesti oppilaitoksen vastuulla. Tietoturvan ja kyberturvallisuuden osaamisen varmistaminen on kuitenkin keskeinen osa organisaation turvallisuutta. Tietoturvaloukkauksista suurin osa johtuu käyttäjän inhimillisestä virheestä, joten henkilökunnan kouluttaminen auttaa ehkäisemään riskejä ja parantaa koko organisaation turvallisuuskulttuuria. Ammatillisessa koulutuksessa kyberturvallisuus nousee vahvasti esiin tieto- ja viestintätekniikan

alalla. Opiskelijoille opetetaan konkreettisia taitoja, kuten tietoverkkojen suojaamista, haittaohjelmien torjuntaa ja turvallista ohjelmistokehitystä. Useissa tutkinnoissa on tarjolla valinnaisia opintokokonaisuuksia, joissa käsitellään osana kokonaisuutta tietoturvallisuutta ja kyberturvallisuutta.

Esimerkiksi tieto- ja viestintätekniikan perustutkinnossa on mahdollista opiskella tutkinnon osa nimeltä Kyberturvallisuuden ylläpitäminen, joka kehittää opiskelijan valmiuksia toimia tietoturvaa vaativissa tehtävissä. Lisäksi ammatillisessa koulutuksessa panostetaan työelämälähtöiseen osaamiseen, jolloin opiskelijat pääsevät harjoittelemaan kyberturvallisuutta käytännön ympäristöissä, esimerkiksi osana työssäoppimisjaksoja tai projektitöitä. Tämä vahvistaa valmiuksia vastata nopeasti muuttuviin digiturvallisuusvaatimuksiin työelämässä. Kyberturvallisuuden koulutus ei ole vain tekninen kysymys. Se on osa laajempaa yhteiskunnallista sivistystä, jossa yhdistyvät kriittinen ajattelu, vastuu, tietosuoja ja turvallinen digitaalinen vuorovaikutus. Opetuksen avulla rakennetaan digitaalista resilienssiä, joka auttaa sekä yksilöitä että yhteisöjä toimimaan turvallisesti nopeasti muuttuvassa teknologisessa ympäristössä.

Opetuksen tavoitteena on kehittää opiskelijoiden kykyä toimia vastuullisesti ja turvallisesti digitaalisessa ympäristössä, niin koulussa, työelämässä kuin vapaa-ajalla. Kyberturvallisuusopetus tukee myös opiskelijan työelämävalmiuksia, sillä lähes jokaisella alalla käsitellään nykyisin henkilötietoja, käytetään digitaalisia järjestelmiä ja ollaan osa verkottunutta toimintaympäristöä. Esimerkiksi lähihoitajaopiskelijalle voi olla ratkaisevan tärkeää ymmärtää potilastietojen tietoturva, tai logistiikka-alan opiskelijalle sähköisen kuljetustiedon suojaaminen. Lopulta kyberturvallisuuden koulutus ei pääty kouluun. Se on elinikäinen oppimisprosessi, jossa myös opettajien, vanhempien ja työelämän toimijoiden rooli on keskeinen. Yhteistyöllä voidaan varmistaa, että jokaisella on valmiudet suojautua digitaalisessa maailmassa, niin nyt kuin tulevaisuudessakin. Voidaan todeta, että toisen asteen koulutus toimii keskei-

senä porttina kyberturvallisuustietoisuuden ja osaamisen rakentamisessa. Ammatillisessa koulutuksessa konkreettisten osaamisen lisäksi kehitetään kriittistä ajattelua ja digiturvallista toimintakulttuuria. Tämä on elintärkeää, jotta nuoret voivat toimia turvallisesti ja vastuullisesti sekä opinnoissa, työelämässä että vapaa-ajalla. [6]

5 Koulutusmateriaalin suunnittelun periaatteet

Koulutusmateriaali on keskeinen osa laadukasta ja vaikuttavaa opetusta. Koulutuksen tueksi toteutetun materiaalin pitää tukea oppimista tehokkaasti. Materiaalin tulee ottaa huomioon henkilökunnan ja mahdollisesti myös opiskelijoiden erilaiset tarpeet, sen vuoksi sisällön on oltava selkeä, monipuolinen ja kohderyhmälle sopiva. Sen tulee täyttää sille asetetut vaatimukset oppimisen tavoitteista. Laadukkaan opetusmateriaalin tekeminen vaatii hyvää suunnittelua. On kuitenkin hyvä muistaa, että materiaalin pysyminen ajantasaisena ja toimivana kokonaisuutena vaatii sen jatkuvaa kehitystä. Varsinkin kyberturvallisuuden kenttä muuttuu jatkuvasti, joka luo paineita materiaalin päivittämiselle. Itse opetusmateriaalin suunnittelussa lähtökohtana tulee olla oppimistavoitteet. On pohdittava mitä opetuksella halutaan saavuttaa ja mitä opetettavan toivotaan oppivan. Kun tavoitteet ovat selvät, niiden pohjalta on helpompi alkaa toteuttamaan varsinaista koulutuksen sisältöä.

Koulutusmateriaalia tehdessä on kiinnitettävä huomiota siihen, että materiaali vastaa mahdollisimman hyvin opetettavien ikätasoa, lähtötasoa ja taustaa. Siksi kohderyhmän tunteminen on välttämätöntä, jotta materiaali saadaan kohdennettua mahdollisimman tarkkaan, näin opetusmateriaali saadaan tuntumaan opetettavista merkitykselliseltä ja ymmärrettävältä. Tiedon omaksuminen helpottuu, kun materiaali on hyvin jäsenneltyä ja selkeää. Opetusmateriaalin on hyvä sisältää havainnol-

listavia kuvia ja kaavioita, jolloin näköaistiin ja näkemiseen perustuva visuaalinen oppiminen paranee. Onkin hyvin kannattavaa tehostaa opetusta esittämällä tietoa monessa muodossa. Äänen rinnalle voidaan tuoda visuaalista esitystä, joka edistää syvempää ymmärrystä. Joissain tilanteissa koulutuksen on hyvä sisältää myös osallistavia harjoituksia. Erilaisten harjoitusten kautta opetettava kykenee siirtämään uuden tiedon käytäntöön ja edistää syvempää ymmärrystä oppimastaan.

Kyberturvallisuus ja tietoturvallisuus ovat aloja, joissa tieto muuttuu nopeasti. Siksi materiaalin säännöllinen päivittäminen on välttämätöntä. Koulutusta ylläpitävän henkilön tai tahon tulee olla sitoutunut koulutuksen pitämiseen ajantasaisena. Koulutusta ja materiaalia suunnitellessa on tärkeä miettiä sen saavutettavuutta ja säilyvyyttä. Ennen toteutusta on pohdittava miten koulutus tullaan tallentamaan ja mitä alustoja sen tekoon kannattaa hyödyntää. Tallennuksen ajatuksena on varmistaa, että materiaali on jatkossakin helposti saatavilla ja jaettavissa. Materiaalin päivittämisen tulisi olla jatkossa mahdollista. Koulutuksen vaikuttavuutta pitäisi voida myös mitata. On olennaista seurata onko oppimista tapahtunut, sekä mahdollista palautteen keruuta olisi asianmukaista pohtia. [57]

5.1 Oppimisen psykologia

Ihmisellä aivojen rakenne alkaa kehittyä jo raskausaikana, toiminnallinen kehitys alkaa muodostua kuitenkin lapselle vasta syntymän jälkeen. [58] Raskauden ensimmäisien kuukausien aikana alkiolle kehittyy aivot, jotka muokkautuvat asteittain, kohdussa ollessaan sikiö alkaa tuntea sekä reagoida valoon ja ääniin. Ensimmäisien vuosien aikana lapsen aivojen kehitys on vilkkaimmillaan. Tällöin puhutaan ajanjaksosta, jolloin kehitys on erittäin nopeaa. Synnynnäiset taikka lapsen kehityksen myötä ilmenevät aivojen kehityshäiriöt esiintyvät eri asteisina tiedonkäsittelyn häiriöinä. Lievät kapea-alaiset häiriöt ilmenevät monesti erilaisina oppimisvaikeuksina. [59]

Oppiminen on välttämätön taito, joka säilyy läpi koko ihmisen elämän. Oppiminen on toiminnan muutosta, joka perustuu kokemukseen. Ihmisen oppiminen on eräänlainen tiedonkäsittelyprosessi, kun hän vastaanottaa, valikoi, tulkitsee ja tallentaa saatavilla olevaa tietoa. Oppiminen edellyttää muistin toimintaa. Aistimuisti, työmuisti ja pitkäkestoinen muisti ovat muistin muotoja, joiden välinen yhteistyö on olennaista oppimisen kannalta. [60] Oppimis- prosessiin vaikuttaa joukko yksilöllisiä tekijöitä, kuten henkilön vireystila ja motivaatio. Unella on merkittävä vaikutus oppimiseen. Univajeisena henkilön tarkkaivaisuus ja kyky käsitellä tietoa vaikeutuu, kokonaisuudessaan suoriutuminen heikkenee. Unen puutteen tiedetään myös lisäävän alttiutta sairastua masennukseen ja muihin psyykkisiin häiriöihin. [61] Oppimis- ja ääniympäristöllä sekä tunneilmapiirillä on oma vaikutuksensa oppimistilanteen laatuun, opetustilanteessa vallitseva melu ja rauhattomuus lisäävät tilanteen kuormittavuutta. [62] Ihmismielen kasvun ja kehityksen taustalla on joukko psykologisia osa-alueita, joiden mukaan määräytyy kuinka ihminen omaksuu, säilyttää ja käyttää tietoa. Varsinkin opetustyössä ja yksilön omassa kehityksessä on olennaista ymmärtää mihin oppiminen perustuu.

Oppimiskäsityksien tarkoituksena on kuvata miten oppiminen tapahtuu. Kukin oppimiskäsitys eroaa toisistaan oppimisen luonteen ja painotuksen suhteen. Yksi tunnetuimmista oppimiskäsityksistä on behaviorismi, jonka mukaan oppiminen tapahtuu, kun ihminen reagoi ulkoisiin ärsykkeisiin. Tällöin käyttäytymistä muokataan voimistamalla tiettyjä reaktioita.[63] Muita tutkittuun tietoon pohjautuvia oppimiskäsityksiä ovat Kognitiivinen, humanistinen, konstruktivistinen ja sosiokonstruktivistinen käsitys. [64]

Kuulemisen kautta tapahtuva oppiminen, eli auditiivinen oppiminen. On ihmiselle hyvin luontaista, varsinkin kun pohditaan kuuntelutaidon vaikutusta henkilön hyvän kasvun perustaitona. Kun pohditaan opetustilannetta, joka painottuu auditiiviseen oppimiseen, tilanteen ääniympäristöllä on valtava vaikutus opetuksen on-

nistumiseen. [65] Mahdollisesti taustalla kuuluvat äänet ja melu aiheuttavat muun muassa opetettaville keskittymisvaikeutta. On hyvä pohtia hieman äänen ergonomiaa. Ääntä luodessa puheen oikeaoppiseen tuottoon voidaan vaikuttaa useilla eri kehon ja ympäristön seikoilla. Ääntä suulla tuotettaessa on vältettävä limakalvojen kuivamista sekä liiallista liman eritystä, joihin vaikuttavat muun muassa useat nautittavat juomat ja ruuat. Ääntä tuotettaessa on hyvä kiinnittää huomiota asentoon, joka tulisi olla mahdollisimman ryhdikäs. Äänen kulkeminen hankaloituu ryhdin ollessa huono. Paras asento äänen tuottamiseen on ryhdikäs seisoma-asento. Puhuessa artikuloinnin on oltava selkeää. Sanojen tulisi erottua toisistaan, jotta kuunteleminen olisi mahdollisimman helppoa, niin sanottu "mumiseminen"hankaloittaa puheen ymmärtämistä. Puhenopeuden on oltava maltillinen, jotta kuuntelija ehtii ajatella ja sisäistää asian. Puhuessa äänensävyä on hyvä vaihdella, varsinkin monotoninen ääni hankaloittaa oppimista sillä se passivoi kuuntelijaa. Hyvä puhuja osaa käyttää tauotusta ja tärkeiden asioiden painotusta oikein. [66] Puhujan olisi syytä painottaa äänessään lempeää ja rauhoittavaa sävyä, joka luo kuulijalle turvallisen ilmapiirin tunteen. Näin vähennetään kuuntelijan kuormitusta.

Visuaalinen oppiminen perustuu näkemiseen ja kuvien hahmottamiseen. Visuaaliselle oppijalle näköaisti on keskeinen oppimisen väline, ja hän muistaa asioita parhaiten mielikuvien avulla. Tällainen oppija käyttää usein näkemiseen liittyviä ilmauksia ja elehtii käsillään puhuessaan, aivan kuin "piirtäisi"asiansa näkyväksi. Hän arvostaa selkeitä kuvia, kaavioita ja järjestelmällisyyttä niin oppimisessa kuin arjessakin. Oppimisessa visuaalinen henkilö hyötyy erityisesti piirroksista, korostuksista, kaavioista ja miellekartoista. Suurille paperiarkeille tehdyt muistiinpanot, värien ja tikkukirjainten käyttö sekä muistiinpanojen näkyvä sijoittelu auttavat muistamista. Pelkän kuuntelemisen sijaan visuaalinen oppija tarvitsee kirjallista tai kuvallista materiaalia. Myös kuullun asian piirtäminen auttaa ymmärtämisessä. [53] Visuaalinen oppimistyyli korostaa havainnointia, keskittymistä ja mielikuvien hyödyntämistä, ja

sopivilla oppimiskeinoilla visuaalinen oppija saa opin tehokkaasti omaksuttua.

Kinesteettinen oppiminen perustuu tuntoaistiin ja fyysiseen kokemiseen. Kinesteettinen oppija omaksuu tietoa parhaiten tekemällä, kokeilemalla ja liikkumalla. Hänelle on tärkeää, miltä asiat tuntuvat – ei vain fyysisesti, vaan myös henkisesti. Opiskelutilanteessa ympäristön viihtyisyys ja mukavuus vaikuttavat oppimiseen olennaisesti. Tällainen oppija käyttää konkreettista ja tunnepitoista kieltä, kuten ”minusta tuntuu” tai ”tämä vaikuttaa hyvältä”. Hän tulkitsee toisten viestintää eleiden, ilmeiden ja liikkeiden kautta, ja muistaa asioita erityisesti siihen liittyvien tuntemusten ja kokemusten perusteella. Fyysisyys on tärkeä osa oppimisprosessia – esimerkiksi lukeminen kävellessä tai sormen käyttäminen apuna rivien seuraamisessa voivat tukea muistamista ja keskittymistä. Kinesteettinen oppija hyötyy opiskelussaan havainnollistavista esityksistä, liikkeestä ja käytännön tekemisestä. Muistiinpanojen tekeminen pahvilapuille tai marginaaleihin, sekä taukojen pitäminen istumisen sijaan liikkeellä pysymällä, tukevat oppimista. Parhaimmillaan oppiminen tapahtuu kehollisesti ja elämyksellisesti – kokemalla, ei vain lukemalla tai kuuntelemalla [52]

5.1.1 Oppimisen psykologian vaikutus kyberturvallisuuden opetuksessa

Oppimisen psykologia vaikuttaa merkittävästi siihen, kuinka tehokkaasti opetettavaa aihetta opitaan, opetetaan ja sovelletaan käytännössä. Keskeisessä roolissa ovat ihmisen tavat ajatella ja käyttäytyä. Kyberturvallisuuteen liittyy runsaasti monimutkaisia ja abstrakteja käsitteitä sekä mekanismeja, joiden ymmärtäminen edellyttää kykyä jäsentää tietoa ja hahmottaa kokonaisuuksia. Uutta opetettaessa on tärkeää edetä maltillisesti, jotta oppiminen ei kärsi liiallisesta kognitiivisesta kuormituksesta. Behavioristisen oppimiskäsityksen näkökulmasta välitön palaute lisää oppimisen vaikuttavuutta, minkä vuoksi koulutuksen tulisi sisältää myös toiminnallisia harjoituksia.[64] Näiden avulla omaa osaamista voidaan kehittää tehokkaammin kuin

pelkän luento-opetuksen kautta.

Konstruktiivinen oppiminen perustuu aiempien kokemusten hyödyntämiseen ja uuden tiedon rakentamiseen niiden päälle. [67] Kyberturvallisuuskoulutuksessa erityisesti erilaiset skenaariot ja case-tapaukset tukevat syvällistä oppimista ja auttavat ymmärtämään teorian soveltamista käytäntöön. Työyhteisön näkökulmasta ryhmässä tapahtuva oppiminen olisi erityisen kehittävää, sillä se tukee uhkien tunnistamista ja yhteistä ymmärrystä. Yhteisöllinen oppiminen voi vahvistaa organisaation turvallisuuskulttuuria sekä lisätä henkilöstön motivaatiota ja sitoutumista, kun oppiminen koetaan merkitykselliseksi ja käytännönläheiseksi.

5.2 Kyberturvallisuuden olennaiset osa-alueet henkilöstön näkökulmasta

Vaikka organisaatiolla olisi käytössään maailman parhaimmat tietoturvajärjestelmät, yksittäisen työntekijän huolimattomuudesta tai osaamattomuudesta voi olla erittäin vakavat seuraukset. Ennen kaikkea ihmisten toimista organisaation kyberturvallisuuden osana on kriittinen. Tärkeimpiä seikkoja lienee henkilöstön tietoturvatietoisuus. Jokaisen tulee ymmärtää, mitä kyberturvallisuus tarkoittaa omassa työssä ja miksi se on tärkeää. Tämän kaltainen tietoisuus ei synny itsestään, vaan sen ymmärtämiseen vaaditaan usein säännöllistä koulutusta. Henkilöstön taustoista riippuen tietoteknisen osaamisen taso voi olla hyvinkin vaihteleva. Tämän vuoksi voi olla kannattavaa painottaa myös yleiseen tietotekniikan osaamiseen, mikä osaltaan parantaa turvallista työskentelyä. Henkilöstön mielipidettä koulutuksen tarpeesta on hyvä tutkia, sillä yleisesti juuri kohderyhmä tietää parhaiten minkälaista tukea työssään tarvittavien ohjelmien ja käytäntöjen kanssa kaipaa. [50] Hyväkin koulutusmateriaali on hyödytöntä, jos se on kohdennettu väärin.

On olennaista hahmottaa henkilöstön käytössä olevat ohjelmistot. Vaikka ohjel-

mien kehittäjä vastaakin pääasiassa ohjelmien turvallisuudesta, on käyttäjällä suuri vastuu ohjelman käyttöön liittyvästä turvallisuudesta. On muistettava, etteivät kaikki henkilökunnan jäsenet käytä kaikkia organisaation käytössä olevia ohjelmia. Oleellista kuitenkin olisi, että ohjelmaa käyttävä henkilökunnan jäsen ymmärtää järjestelmien turvallisen käytön. Työssä tulisi käyttää vain organisaation hankkimia ja hyväksymiä ohjelmia. Työkoneelle ei tulisi ladata tai asentaa mitään ohjelmistoa ilman työnantajan lupaa. Ohjelmia käyttäessä tulee ymmärtää tietojen oikeanlaisen käsittelyn periaatteet. Työntekijän on kyettävä tunnistamaan luottamuksellinen ja arkaluontoinen tieto. Tietoa on osattava myös käsitellä oikein, mikä on osa jokaisen työntekijän vastuuta Ja varsinkin luottamuksellista tietoa jakaessa tulee toimia harkiten.

Järjestelmien hallinnasta vastaavat henkilöt pyrkivät parantamaan kyberturvallisuutta käyttöoikeuksien hallinnan kautta. Hyvä sääntö on, että työntekijällä tulisi olla vain ne oikeudet, jotka ovat hänen työnsä hoitamiseksi välttämättömiä. Työnantajan tulisi nimetä myös vastuuhenkilöt, joille poikkeukset ja uhat raportoidaan. Tavallinen käyttäjä usein havaitsee poikkeaman ensimmäisenä, jolloin tilanteesta raportointi on hyvin kriittistä. Jokaisen käyttäjän vastuulla on hallita tunnuksiaan turvallisesti. Omia tunnuksia ei tulisi ikinä luovuttaa ulkopuolisten käsiin. Vahva salasana ja kaksivaiheinen tunnistautuminen ovat erittäin tärkeitä toimenpiteitä oman ja yhteisön turvallisuuden takaamiseksi. On hyvä ymmärtää, että huono salasana voi vaarantaa pahimmillaan koko organisaation. Työntekijän vastuulla on huolehtia, ettei työvälineitä jätetä valvomatta, siksi tietokone ja työpuhelin olisi syytä lukita aina kun poistuu niiden välittömästä läheisyydestä.

Erilaisten huijaus- ja tietojenkalasteluviestien kautta toimiva rikollinen toiminta on lisääntynyt ja henkilökunta kohtaa sellaista jatkuvasti työssään. On kriittistä tunnistaa huijausyritykset ja toimia annetun ohjeistuksen mukaisesti sitä kohdatessaan. Uusia haasteita kyberturvallisuuteen on luonut tekoälyn yleistyminen. Jonka

avulla hyökkäyksiä voidaan tehostaa ja kohdentaa paremmin. Toisaalta tekoälyä käytetään myös uhkien ja poikkeamien tunnistamiseen. Henkilöstön tulee olla tietoinen vallitsevista muutoksista, joita kyberturvallisuuden kentällä tapahtuu. Turvalliset työskentelytavat ja käytännöt, joita noudatetaan myös etätyöskentelyn aikana ovat avainasemassa, kun organisaatiossa rakennetaan turvallista toimintaympäristöä. [68]

5.3 Kyberturvallisuuden konkreettisien työkalujen koulutus

Oppilaitosten suojautumiskyky edellyttää käytännönläheistä koulutusta eri työkaluista ja menetelmistä, minkä avulla uhkia voidaan tunnistaa ja estää tehokkaasti. Koulutuksessa voidaan hyödyntää esimerkiksi NIST:in kaltaisia viitekehyksiä, jotka jaottelevat osaamisen eri tasoihin. Tällaisissa malleissa tekninen osaaminen nähdään osana laajempaa kokonaisuutta. [69] Oppilaitoksissa koulutuksen tulee vastata eri käyttäjäryhmien tarpeita. Koko henkilökunta hyötyy perustyökalujen käyttöön liittyvästä koulutusta. Näitä ovat muun muassa tietojenkalastelun tunnistaminen ja salasanatyökalujen hyödyntäminen. Osalle henkilökunnan jäsenistä on myös hyödyllistä opettaa vaativampia keinoja ja menetelmiä. Hyödyllinen harjoitus, jonka vaikutuksia voidaan analysoida, on eräänlaisien simuloitujen huijausviestien lähettäminen henkilökunnalle. Tällaiset työkalut tukevat käytännön oppimista ja auttavat tunnistamaan huijausviestejä. Turvallisen tunnistautumisen käytäntöjä ja salasanojen hallintaa on hyvä harjoitella, miten luodaan vahvoja salasanoja tai käytetään monivaiheista tunnistautumista. Koulutuksessa voidaan konkreettisesti käydä läpi, miten tällaiset ohjelmat otetaan käyttöön ja miten niitä käytetään eri järjestelmissä.

Koulutuksessa voidaan hyödyntää erilaisia analysointityökaluja, joiden avulla voidaan havainnoida tietoliikennettä ja tunnistaa poikkeavaa toimintaa. Näiden työkalujen käyttöön liittyvä koulutus vaatii jo syvempää teknistä osaamista, mutta nii-

den avulla voidaan ehkäistä merkittäviä uhkia. Järjestelmien ja ohjelmien haavoittuvuuksia tunnistavien työkalujen käyttöä voidaan tietenkin opettaa. Eikä välttämättä ole perusteltua ottaa niitä osaksi koulutusta koska oppilaitoksesta riippuen vain noin kourallinen henkilöitä hyötyisi siitä.

Käyttäjien työasemiin asennetut ohjelmistot mahdollistavat jatkuvan suojauksen. Koulutuksessa tulisi käsitellä myös, miten ohjelmat toimivat ja miten tulisi reagoida mahdollisiin uhkatilanteisiin. Suurten oppilaitosten tapauksessa voidaan käyttää SIEM ratkaisua, jonka avulla kyberturvallisuuden tilasta saadaan luotua kattava kokoaniskuva. Security Information and Event Managment (SIEM) on järjestelmä joka auttaa meitä tunnistamaan uhkia nopeasti.[1] Tämä mahdollistuu keräämällä, analysoimalla ja yhdistämällä lokitietoja eri lähteistä. Näin voidaan havaita poikkeamia, tunnistaa uhkia ja vastata niihin nopeasti.

Kyberturvallisuustyökalujen koulutus vaatii opettajalta laaja osaamista opettamastaan asiasta. Myös kohderyhmän pitää valikoitua vaadittavan tason mukaan. Parhaiten oppimista tukevat käytännön harjoitukset, joissa osallistujat pääsevät käyttämään työkaluja oikeissa tai simuloiduissa ympäristöissä. Tämän lisäksi uhkasimulaatiot ja interaktiiviset harjoitukset voivat parantaa oppimista ja sitoutumista. Koulutuksen tulisi myös olla jatkuvaa, sillä kyberturvallisuuden kenttä muuttuu nopeasti ja työkalut kehittyvät samaa vauhtia. Säännölliset opetuskoulutukset tukevat pitkäjänteistä osaamisen kehittämistä. [70]

Vaikka työkalujen koulutus on hyödyllistä, siihen liittyy myös haasteita. Resurssipula, henkilöstön aikarajoitteet ja teknologian nopea muutos voivat estää tehokkaan koulutuksen järjestämistä. Lisäksi on tärkeää, ettei koulutus jää pelkäksi työkalujen läpikäynniksi. Koulutuksen yhteydessä on syytä käydä läpi kokonaisvaltainen kyberturvallisuusajattelu, riskien ymmärtäminen, toimintamallien kehittäminen ja yhteistyö eri toimijoiden välillä. Oppilaitosten tulisi laatia koulutussuunnitelmat, joissa

[1] https://www.microsoft.com/en-us/security/business/security-101/what-is-siem?msockid=078a01239a44692704e017929b7968b1

kyberturvallisuusosaaminen jaetaan selkeästi eri kohderyhmien mukaan ja joissa on määritelty konkreettiset osaamistavoitteet, menetelmät ja seuranta. [5]

5.4 Organisaation muutosten huomioon ottaminen

Uudet opetusteknologiat, etäopetus, palveluiden ulkoistaminen ja rakenteelliset uudistukset vaikuttavat oppilaitosten toimintaympäristöihin. Näillä muutoksilla on suora vaikutus myös kyberturvallisuuteen. Jotta organisaatio voi ylläpitää turvallista toimintaa muuttuvassa tilanteessa, kyberturvallisuuden kehittämisen on oltava jatkuvaa, joustavaa ja organisaation muutoksiin kytkeytyvää. Organisaatiomuutoksilla tarkoitetaan tässä tilanteessa henkilöstömuutoksia, uusien teknologioiden käyttöönottoa, toimintamallien muutoksia tai hallintorakenteiden uudistamista. Jokainen muutos voi luoda uusia tietoturvahaavoittuvuuksia tai vaikuttaa olemassa olevien suojausten tehokkuuteen. [33]

Oppilaitoksen henkilökunnassa tapahtuu väistämättä muutoksia. Mahdolliset uudet työntekijät voivat olla alttiita esimerkiksi tietojenkalastelulle, joita jo olemassa olevan henkilökunnan kanssa on harjoiteltu tunnistamaan. Samalla organisaatiosta poistuvien henkilöiden käyttöoikeuksien hallinta voi epäonnistua, mikä kasvattaa riskiä sisäisistä uhkista. Muutokset organisaation koossa ja rakenteessa vaikuttavat kyberturvallisuuteen varattujen resurssien määrään. [71] Teknologiset uudistukset, kuten uudet oppimisympäristöt tai hallintajärjestelmät, voivat sisältää oletusasetuksia, jotka eivät ole turvallisia. Lisäksi käyttäjien koulutuksen laiminlyönti voi johtaa virhekäyttöön. Kun teknisiä toimintoja siirretään kolmansille osapuolille, riskienhallinta monimutkaistuu. Tällöin on syytä laatia tarkat sopimukset, joiden avulla myös ulkoiset toimijat saadaan sitoutumaan organisaation tietoturvakäytäntöihin ja noudattamaan niitä.

Esimerkiksi uuden pilvipalvelun käyttöönotto vaatii koulutusta tietojen jakamisen turvallisista käytännöistä, käyttöoikeuksien hallinnasta sekä vastuista palvelun-

tarjoajan ja organisaation välillä. Pelkkä tekninen käyttöönotto ei riitä. Yksi keskeinen osa muutoksiin varautumista on henkilöstön tietoisuuden ylläpito. Uudet prosessit ja järjestelmät edellyttävät usein uusien toimintatapojen omaksumista. Kyberturvallisuuskoulutusta tulisi päivittää muutostilanteissa vastaamaan muuttunutta riskiympäristöä. Kyberturvallisuustietoisuus ei saa olla irrallinen osa koulutuskokonaisuutta, vaan sen tulisi olla kytköksissä kaikkeen muutokseen liittyvään perehdytykseen ja osaamisen kehittämiseen.

Muutostilanteet aiheuttavat usein epäselvyyttä siitä, kuka vastaa mistäkin. Kyberturvallisuudessa tämä voi tarkoittaa sitä, että kukaan ei tiedä, kenen vastuulla on esimerkiksi käyttöoikeuksien hallinta, varmuuskopiointi tai poikkeamien käsittely. [71] Siksi jokaisen organisaatiomuutoksen yhteydessä henkilöiden vastuualueet tulee tarkistaa ja dokumentoida. Näiden asioiden läpikäynti voi tapahtua osana muutoksenhallintaprosessia tai tietoturvallisuuden vuosikelloa, mikäli sellainen on käytössä. Muutokset ja niiden vaikutukset eivät ole koskaan täysin hallittavissa etukäteen ja siksi jatkuva arviointi sekä palautteen kerääminen ovat olennaisia. Oppilaitokset, jotka suhtautuvat muutoksiin dynaamisena prosessina ovat usein valmiimpia myös digitaalisten uhkien edessä.

6 Koulutusmateriaalin suunnittelu ja tekninen toteutus

Aikaisemmassa luvussa läpi käytyihin seikkoihin pohjautuen koulutusmateriaali on lähtökohtaisesti kaikkein hyödyllisintä toteuttaa videoiden muodossa. Näin varmistettaan, että materiaali on helposti saatavilla ja siihen voi palata tarvittaessa. Videomateriaali mahdollistaa auditiivisen kuuntelemalla oppimisen. Koulutusmateriaalia pystyy kuuntelemalla käymään läpi esimerkiksi muiden töiden ohessa tai autoa ajaessa, mikä mahdollistaa koulutusmateriaalin läpikäynnin ilman paikkasidonnaisuutta. Lisäksi materiaali tarjoaa mahdollisuuden visuaaliseen oppimiseen, tämä on tärkeää henkilöille, jotka oppivat ja omaksuvat tietoa tehokkaammin, kun opetettava asia tarjotaan heille visuaalisessa muodossa. Videoiden muodossa oleva materiaali on helppo tallentaa ja hyödyntää myöhempää käyttöä ajatellen, mikä on tärkeää kohderyhmää ja sen tarpeita pohtiessa.

Koulutusmateriaalin saavutettavuus on tärkeä näkökulma. Riippumatta opetettavan teknisistä taidoistaan tai mahdollisista rajoitteistaan, tulisi heidän pystyä käyttämään materiaalia sujuvasti. Tämä tarkoittaa esimerkiksi tekstitysten tarjoamista videoihin, selkeää ja ymmärrettävää kieltä sekä käyttöliittymän yksinkertaisuutta.

Koulutusmateriaalin tarkoitus on auttaa työntekijöitä tunnistamaan ja ehkäisemään kyberturvallisuusuhkia arjessaan. Sisällön tulee olla ajankohtaista ja perustua

ajantasaiseen tietoon. Kyberuhkat muuttuvat nopeasti, joten materiaalin päivittäminen on tärkeää. Tuotetun materiaalin sisällön tulee olla monipuolista, mutta se on tehtävä mahdollisimman helposti omaksuttavaksi. Koulutusten suhteen on hyvä muistaa sisällyttää niihin tarpeeksi toistoa, joka auttaa asioiden muistamisessa. Toiston suhteen on kuitenkin tärkeä välttää liiallisuutta, jotta vältytään tautologialta.

Ryhmä	Koulutuksen keskeiset painopisteet
Johto	Kyberturvallisuuden johtaminen, kriisiviestintä, juridiikka, resurssit ja osaamisen kehittäminen
Opetushenkilökunta	Kyberturvallisuus arjen työssä, tietosuoja, digitaallisten järjestelmien turvallinen käyttö, opiskelijoiden ohjaus, uhkien tunnistaminen ja reagointi
Tukihenkilöstö	Henkilötietojen turvallinen käsittely, laitteiden sekä järjestelmien turvallinen käyttö ja turvallinen viestintä
Koko henkilöstö	Kyberturvallisuuden perusteet

Kuva 6.1: Mahdolliset koulutuksen painotukset eri ryhmille

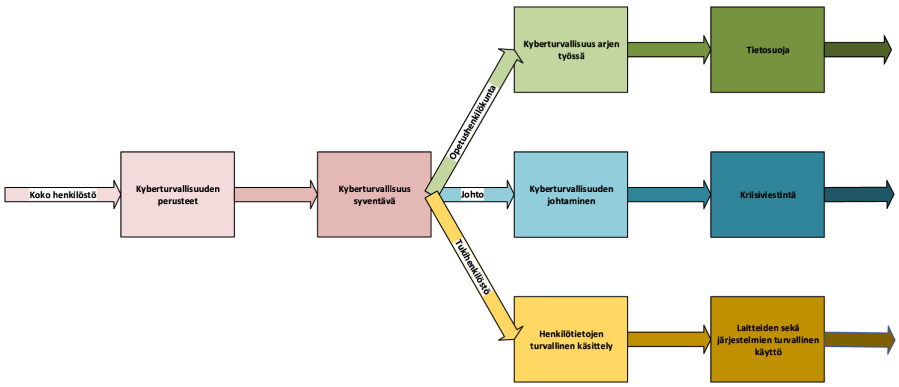
Koulutuksen rakenteen ja materiaalin tulee olla piirteiltään mahdollisimman selkeä ja hyvin jäsennelty. Kun edetään materiaalin suhteen loogisesti, on perusteltua aloittaa tavoitteista, jotka auttavat kohderyhmää hahmottamaan kokonaisuuden. Liian sekava ja hajanainen materiaali vie kohdeyleisön huomion pois ydinsisällöstä. Materiaalin ja koulutuksen on syytä olla mahdollisimman käytännönläheistä, joka helpottaa asian omaksumisen osaksi omaa työtä. Vaikkakin vuorovaikutus sekä osallistaminen tukisivat oppimista parhaiten, toisin kuin pelkkä passiivinen kuunteleminen, on sitä tässä tilanteessa lähes mahdotonta järjestää osaksi koulutusta. Jatkossa olisi syytä pohtia enemmän osallistavan koulutuksen järjestämistä taikka ottamalla osallistamisen osaksi koulutusta. Pedagogiselta näkökantilta ajateltuna pelkkä teoreettinen tieto ei välttämättä riitä, vaan oppimisen tueksi tarvitaan käytännön harjoituksia, interaktiivisia elementtejä ja mahdollisuuksia testata opittua.

Ryhmä	Aihe	Keskeinen sisältö ja tavoitteet
Johto	Kriisiviestintä	Vastuunjako, ohjeistus (toimintamallit), lakisääteiset aikarajat ja viestintäkanavat

Kuva 6.2: Tarkempi kuvaus yksittäisen aiheen sisällöstä

Koulutusmateriaalin tulee olla kohderyhmälleen sopivaa. Eri toimissa työskentelevillä henkilöillä on erilaiset tarpeet ja lähtötasot. Esimerkiksi johdolle suunnattu materiaalin pääpaino tulee olla riskienhallinnassa ja strategisessa päätöksenteossa, kun taas tekniselle henkilöstölle voidaan tarjota syvällisempää tietoa uhkien torjunnasta ja järjestelmien suojaamisesta. Myös peruskäyttäjille tulee tarjota käytännönläheistä sisältöä, joka auttaa heitä tunnistamaan huijauksia ja toimimaan turvallisesti verkossa.

Koulutuksen vaikuttavuuden arvioimiseksi on tärkeää mitata oppimistuloksia. Tämä voidaan toteuttaa kyselyiden tai palautteenkeruun avulla. Mittaaminen ei ainoastaan osoita, onko tavoitteet saavutettu, vaan siten voidaan auttaa myös tunnistamaan kehitys tarpeet. Palautteen hyödyntäminen on keskeistä koulutusmateriaalin jatkuvassa parantamisessa. Koulutus ei myöskään saa jäädä yksittäiseksi tapahtumaksi, jatkuva oppiminen on keskeistä kyberturvallisuuden kentässä, jossa uhkakuvat kehittyvät nopeasti. Säännölliset päivitykset, uudet materiaalit ja ajankohtaiset esimerkit pitävät aiheen elävänä ja ajankohtaisena. Tehokas kyberturvallisuuskoulutus ei vaadi monimutkaisia järjestelmiä, vaan ennen kaikkea selkeää, ajankohtaista ja käytännönläheistä sisältöä. Kun koulutus on helposti lähestyttävää ja liittyy suoraan työntekijän arkeen, sen omaksuminen on helpompaa ja vaikutus pitkäaikaisempi. Organisaation kannattaakin panostaa koulutuksen saavutettavuuteen, jatkuvuuteen ja käyttäjälähtöisyyteen. Tietoturvakoulutus on investointi, joka maksaa itsensä takaisin riskien pienentyessä.



Kuva 6.3: Vaihtoehtoisen koulutuksen etenemisen prosessikuvaus

6.1 Koulun johdon koulutusmateriaali

Koulutuksen tavoite on lisätä koulun johdon ymmärrystä kyberturvallisuuden merkityksestä, vastuualueista ja strategisista toimenpiteistä. Sen tulee tarjota tukea strategisessa päätöksenteossa, joka parantaa turvallista digitaalista toimintaympäristöä oppilaitoksessa. Koulun johdolle suunnatun kyberturvallisuuskoulutuksen ydin on strategisen ymmärryksen lisääminen ja käytännön vastuiden selkeyttäminen. Kyse ei ole teknisestä osaamisesta, vaan johtamisesta, riskien hallinnasta ja turvallisuuskulttuurin rakentamisesta. Koulun turvallisuus paranee, kun johto on sitoutunut kyberturvallisuuteen. Tosin myös johdon henkilöstön kuten muidenkin yksilöiden työnkuvasta riippumatta on syytä olla perusosaaminen hallussa.

Johdon on tärkeää ymmärtää, että koulut ovat yhä useammin kyberuhkien kohteena. Riskienhallinnan parantamisen perustana toimii tietoisuuden lisääminen. Olisi myös aiheellista paneutua esimerkkeihin aikaisemmin kouluihin kohdistuneista kyberhyökkäyksistä, joita suomessa on jo koettu useampia. Esimerkkien kautta teroittuu ymmärrys miksi kyberturvallisuus koskee niin vahvasti myös kouluja.

Koulutusmateriaalin johdannossa olisi tärkeää painottaa johdon roolia koskien koulun kyberturvallisuudessa ja käydä läpi perusteita. Kouluun kohdistuvia keskeisiä riskejä läpi käydessä johdolle muodostuu konkreettinen ymmärrys, mitä uhkia koulussa voi esiintyä ja mitkä toiminnat ovat erityisen haavoittuvia. Vastuun ja-

kautumista ja lainsäädäntöä läpi käydessä on hyvä paneutua siihen tosiseikkaan, että koulun johto kantaa suurta juridista vastuuta. Tämän osion tarkoituksena on selkeyttää, mitä laki velvoittaa ja miten koulun tulee toimia poikkeustilanteissa. Tiedon lisäksi tarvitaan toimivia käytäntöjä. Materiaalin tarkoituksena on antaa työkaluja käytännön toteutukseen ja jatkuvaan kehitykseen. Johdon henkilöstö voisi hyötyä myös kyberturvallisuuteen liittyvästä työpajatyylisistä harjoituksista, joiden lopputuloksena saadaan lyhyessä aikaa paljon konkreettista aikaan.

Vaikka pyrittäisiinkin välttämään katastrofiajattelua, on riskien hallinnan näkökulmasta hyvä varautua aina pahimpaan. Siksi johdon kanssa onkin hyvä käydä läpi esimerkiksi sitä ajatusta, että mitä oppilaitoksella tapahtuisi, jos kaikki tietojärjestelmät kaatuisivat nyt.

6.2 Opetushenkilökunnan koulutusmateriaali

Johdon toiminnasta vahvasti poiketen opetushenkilökunta toimii opiskelijarajapinnassa mikä lisää riskejä tietoturvan ja yksityisyyden suojan näkökulmasta. Lehtorit, opettajat sekä muut opetukseen osallistuvat henkilökunnan jäsenet käsittelevät työssään päivittäin suuria määriä arkaluonteista tietoa. Lisäksi opetushenkilökunnan jäsenet käyttävät monia digitaalisia järjestelmiä, kuten Wilmaa, Google Workspacea ja Microsoft 365 ohjelmistoja. Jokainen käyttäjä on mahdollinen hyökkäyksen kohde ja samalla väylä syvemmälle koulun järjestelmiin. Opettajien kyberturvallisuustaidot suojaavat oppilaita, kollegoja ja koko kouluyhteisöä. Opettaja toimii lähtökohtaisesti myös opiskelijoiden digikäyttäytymisen ohjaajana.

Koulutus olisi hyvä aloittaa tutustumalla kyberturvallisuuden perusteisiin ja mitä, että kyberturvallisuus koulussa tarkoittaa kaikkia niitä toimenpiteitä, joilla suojataan oppilaiden, henkilökunnan ja koulun digitaalista toimintaa ulkoisilta ja sisäisiltä uhkilta. Henkilötietoja käsiteltäessä opetushenkilökunnan toimintaa ohjaa laki. Se määrittelee hyvin selkeästi, että henkilötietojen käsittelijänä opettajan on huo-

lehdittava siitä, että tiedot säilytetään ja käsitellään turvallisesti. Henkilötietoja ei tule jakaa ulkopuolisille ja niihin pääsy on rajoitettu tyypillisesti vain niille, joilla on siihen työtehtävien perusteella oikeus. Tietoja ei myöskään tule säilyttää pidempään kuin on tarpeellista. Virheellinen käsittely voi johtaa tietovuotoon tai rikkomukseen, josta koululla on ilmoitusvelvollisuus viranomaisille ja asianomaisille.

Kyberuhkia olisi tärkeää käydä läpi jo koulutuksen alussa, varsinkin minkälaiset uhat kohdistuvat useimmiten oppilaitokseen ja sen henkilökuntaan. Tietojenkalastelun, haittaohjelmien ja kiristysohjelmien toimintaa käymällä läpi henkilökunnalle muodostuu hyvä ymmärrys tunnistaa ja välttää uhkia työssään. Oppilaitoksen omista ohjeistuksista ja käytännön toimintatavoista riippuen hyödyllistä olisi laatia kaikille yhteiset toiminta ohjeet, eri tilanteissa toimimiselle. Yhteinentoiminta malli lisää koulun yleistä turvallisuutta ja toiminnan läpinäkyvyyttä, mikä on oleellista laadun valmistamisessa. On tärkeää käydä läpi, kuinka viestitään turvallisesti eri alustoilla. Viestien sisältö ja vastaanottajat tulee harkita tarkkaan. Henkilökohtaisia tai arkaluonteisia tietoja ei tule lähettää ilman salattua yhteyttä tai suojattua järjestelmää.

Oppilaitoksen latteita ja verkkoa tulee käyttää turvallisesti. Laitteet ja järjestelmät tulee suojata salasanalla, monivaiheisella tunnistautumisella eikä laitteita tule jättää valvomatta tai avoimeksi julkisilla paikoilla. Koulun laitteisiin tai verkkoon ei saa asentaa ohjelmia tai yhdistää laitteita ilman lupaa. Julkisten verkkojen käyttöä tulee välttää työasioita hoitaessa.

Opettajilla on tärkeä rooli opiskelijoiden turvallisen digikäyttäytymisen tukemisessa. Opettajan tulee ohjata oppilaita turvalliseen ja vastuulliseen verkon ja laitteiden käyttöön. Usein nuorelle tulee yllätyksenä, että kaikkea verkkoon laitettua ei voi enää poistaa. Hyvät käytöstavat ulottuvat myös verkkoon. Opettajan tehtävänä on puuttua verkkokiusaamiseen ja ohjata keskustelua digietiikasta. Opiskelijoita on myös ohjeistettava käyttäjätunnusten salassapidon, turvallisen viestinnän

ja varovaisuuden sosiaalisessa mediassa. Opiskelijoita on ohjeistettava myös käyttäjätunnusten käsittelyssä, turvallisesta viestinnästä ja varovaisuudesta sosiaalisessa mediassa.

Opetushenkilökunnan olisi oltava myös tietoisia, miten toimitaan mahdollisissa poikkeustapauksissa. Onko oppilaitoksessa mahdollisesti laadittuna suunnitelma tietomurto tai tietoturvaloukkauksia varten? Kenen olla yhteydessä, jos jotain tavallisesta poikkeavaa tapahtuu.

6.3 Koulun muun henkilöstön koulutusmateriaali

Koulun arjen sujuvuus perustuu monien eri ammattilaisten yhteistyöhön. Opetushenkilökunnan ja johdon lisäksi kouluyhteisössä toimii joukko oppilaitoksen arjen sujuvuuden kannalta tärkeää tukihenkilökuntaa. Joita ovat muun muassa koulusihteerit, opinto-ohjaajat, erityisopettajat, kuraattorit, keittiöhenkilökunta, siivoajat ja kiinteistöhuollon henkilökunta, joiden työpanos tekee koulupäivästä turvallisen ja toimivan. Myös tukihenkilöstö käyttää päivittäin erilaisia järjestelmiä, viestii oppilaiden ja huoltajien kanssa sekä käsittelee tietoa, joka vaatii huolellisuutta ja tietosuojaa.

Muulle oppilaitoksen henkilökunnalle esitettävä materiaali ei juurikaan eroa opetushenkilökunnalle esitettävästä. Ainoastaan opiskelijoiden ja opettajien roolia kyberturvallisuuteen ja tietoturvaan ei ole tarpeen esittää siinä määrin mitä opetushenkilökunnalle. Kuitenkin opiskelijat seuraavat, miten aikuiset toimivat digitaalisissa tilanteissa. Perusteet, uhat ja käytännön toimintatavat on kuitenkin oleellista sisällyttää koulutusmateriaalin.

7 Yhteenveto ja johtopäätökset

Digitalisaation kehitystä arvioivissa vertailuissa Suomi on ollut pitkään tilastojen yhtenä kärkimaana. [72] Suomi onkin yksi maailman digitalisoituneimmista maista ja meillä yhteiskunnan toiminnot nojaavat vahvasti tietojärjestelmiin. Suomalaisen väestön digitaaliset perustaidot ovat myös EU:n parhaimmistoa.[1] On tärkeää huomioida, että näin vahvasti digitalisoituneessa maassa yhteiskunnan toimintakyky on altis kyberhyökkäyksille, tietomurroille ja järjestelmien häiriöille. Suomen geopoliittinen asema lisää entisestään kyberturvallisuuden merkitystä. Kybervaikuttaminen on halpa ja tehokas tapa horjuttaa yhteiskuntaa ilman fyysistä hyökkäystä yli aluerajojen.

Kyberturvallisuus itsessään ei ole uusia asia, mutta alana melko uusi. Suomalaisissa oppilaitoksissa ja organisaatioissa on havahduttu vasta ikään tarpeeseen vahvistaa varautumista mahdollisia poikkeustilanteita varten. Vuonna 2025 voimaan tullut NIS2-direktiivi on hyvä esimerkki, miten lainsäädännöllä ohjataan organisaatioita panostamaan kyberturvallisuutta koskevaan riskienhallintaan. Aikaisemmin kyberturvallisuuden riskien vakavuudesta ei usein ole selkeää ymmärrystä, jonka vuoksi se on nähty usein asiana, joka ei kosketa itseä tai omaa organisaatiota. Eikä siihen ole koettu olevan järkeä panostaa. Monesti turvallisuuteen on alettu panostaa vasta kun jotain on jo tapahtunut. Nykyisin näkemykset ja asenteet ovat muuttuneet, jonka vuoksi siihen on alettu priorisoida mikä puolestaan on johtanut resurssien

[1] https://dvv.fi/-/digitaitoraportointi-2023-digi-ensin-mutta-ei-yksin

puutteeseen.

Ymmärrys kyberturvallisuudesta ei ole mikään itsestäänselvyys. Ja siksi kehityksen tuomiin haasteisiin on vastattava koulutuksen kautta saatavan osaamisen avulla. Varsinkin sekä nuorien ja vanhempien ikäryhmien tiedot ja taidot ovat heikot. Minkä vuoksi vanhemman ikäryhmän ihmiset ovat usein haavoittuvaisempia ja alttiimpia joutumaan kyberrikollisten uhreiksi. Nuorempi väestö altistuu kyberuhille monesti hieman eri syistä kuin vanhempi ikäpolvi. Nuorten vähäinen kokemus ja tieto internetin turvallisesta käytöstä altistaa heidät usein erilaisille uhille. Aika ja sen mukana tulleet muutokset, esimerkiksi verkkokäyttäytymisessä tuo aivan uusia haasteita. Nuorten suosimassa sosiaalisessa mediassa he voivat joutua huijareiden, kiristäjien tai nettikiusaamisen kohteeksi. Nuori voi tuntea painetta esimerkiksi jakaa kuvia, klikata linkkejä tai osallistua haasteisiin, joita muut suosittelevat. Nuorilla ei ole välttämättä kykyä kriittiseen ajatteluun, joka altistaa nuoren uskomaan helpommin valeuutisia, mainoshuijauksia tai tekaistuja viestejä. Nuorilla voi olla myös lähtökohtaisesti heikko käsitys tekojensa seurauksista.

Nykypäivän työelämässä digitaidot ja niiden myötä myös ymmärrys kyberturvallisuudesta ovat lähes poikkeuksetta välttämättömiä. Niiden puute estää meitä menestymästä työelämässä ja luo arkeen ylimääräisiä haasteita, joiden vaikutus voi olla pitkäkantoinen ja erittäin laaja. Heikko ymmärrys kyberturvallisuudesta ja tietoturvasta tekevät meidät ja työyhteisömme alttiiksi erilaisille uhille ja väärinkäytöksille. On hyvä muistaa, että joukkue on yhtä vahva kuin sen heikoin lenkki. Voidaan ajatella kyberhyökkäyksen onnistuvan usein siksi, että ihmiset eivät tunnista vaaraa tai toimivat huolimattomasti, tällöin kyberturvallisuuden koulutuksen tärkeys konkretisoituu. Lisäämällä tietoisuutta uhista, voidaan pyrkiä välttämään henkilökuntaa astumasta niin sanotusti kyberrikollisen ansaan. Kun yksilöt ymmärtävät, mitä esimerkiksi tietoturva tarkoittaa arjen tasolla, he osaavat suojella paremmin itseään ja muita. Olipa kyseessä pieni yritys tai kansainvälinen organisaatio, kaikki

toimijat ovat digitaalisessa ympäristössä alttiita hyökkäyksille. Työntekijöiltä vaaditaan yhä enemmissä määrin yhä laajempaa osaamista ja ymmärrystä siitä, miten vaikka salasanat, sähköposti, ohjelmistot ja tiedostojen käsittely voidaan hoitaa turvallisesti. Edellä mainittujen seikkojen vuoksi meidän on varmistettava, että ihmiset saavat tarvittavan koulutuksen kyberuhkien ymmärtämiseen ja torjumiseen. Kyberturvallisuuden opettaminen kouluissa, työpaikoilla ja osana jatkuvaa oppimista on keskeinen askel kohti turvallisempaa digitaalista tulevaisuutta.

Koska kyberturvallisuus on alana melko uusi, on kasvanut kysyntä asiantuntijoista muodostunut jo osaajapulaksi. Vaikka tilanteeseen on reagoitu, osaajien saaminen vastaamaan kysyntää on pitkä ja aikaa vievä prosessi. Aikaisemmin kyberturvallisuus ja tietoturva on ollut organisaation ICT-työntekijöiden hoidettavana. Varsinkin päteviä kyberturvallisuusalan kouluttajia on todella vähän, mikä puolestaan vaikeuttaa koulutuksen järjestämistä, erityisesti oppilaitoksissa. Mikäli tarkkaillaan itse koulutusjärjestelmää, kyberturvallisuuden koulutukseen on alettu panostaa muissakin kuin tietotekniikan alan koulutuksissa. Vaikka kyberturvallisuuden opetus on lisääntynyt, meidän on hyvä pysähtyä pohtimaan nykyisien järjestelyjen riittävyyttä.

Vaikka tämä opinnäytetyö ei valmista koulutusmateriaalia lukijalleen tarjoakaan, pyrkii se hahmottelemaan puitteet ja perustelut henkilöstön koulutuksen toteuttamista ajatellen. Todettakoon, että koulun henkilökunnan kouluttaminen kyberturvallisuusasioissa ei ole vain suositeltavaa, vaan välttämätöntä. Oppilaitoksen henkilökunnan kyberturvallisuuskoulutus on investointi, joka tukee turvallista oppimisympäristöä, edistää digiosaamista ja vähentää tietoturvariskejä tehokkaasti. Se on panostus koko kouluyhteisön hyvinvointiin ja tulevaisuuteen. Henkilökunnan jäsenet toimivat myös esimerkkeinä opiskelijoille. Kun henkilökunta ymmärtää kyberturvallisuuden periaatteet, he voivat välittää näitä taitoja myös oppilaille. Tämä tukee laajemmin digitaalisen sivistyksen kehittymistä ja auttaa valmistamaan nuoria

toimimaan vastuullisesti verkossa.

Kyberturvallisuuden perusperiaatteet kuten turvallisten toimintatapojen noudattaminen eivät juurikaan muutu. Tästä syystä kouluttavien tahojen olisi järkevä luoda yhteinen koulutusmateriaali, jota voisi joustavasti soveltaa ja kohdentaa. Nykytilanteessa kouluttavat tahot laativat omat materiaalinsa, joiden sisältö kuitenkin on suurilta osin lähes identtinen. Mielestäni ei ole järkevää käyttää resursseja päällekkäisien materiaalien tekemiseen. Yhteisen materiaalin etuina olisi kustannustehokas ja vaikuttava ratkaisu.

7.1 Haasteet

Työtä tehdessä suurimmaksi haasteeksi osoittautui ajankäyttö ja siitä johtunut viivästyminen, mikä oli pääasiassa osaksi seurausta kirjoittajan huonosti suunnittelemalle aikataululle. Koska työn tekemiselle ei määritetty selvää määräaikaa, oli todella helppoa jättää työn kirjoittaminen määrittelemättömän pitkäksi hetkeksi tauolle, muiden kiireiden varjolla. Pitkät tauot kirjoituksessa pahensivat tilannetta, sillä työhön piti paneutua aina uudestaan. Aikaisemmin kirjoitettu oli saattanut unohtua tauon aikana tai uudelleen tekstiä lukiessa alkoi vanhaa tekstiä kirjoittamaan monia kertoja uudestaan. Lopulta työn suhteen havahtui tilanteeseen, että työ on ollut näennäisesti tekeillä jo todella pitkän ajan ja se olisi hyvä saada pikimmiten pois. Tutkielman piti lähtökohtaisesti sisältää myös paljon laajemmin tiedonkeruuta, kuten haastattelu ja kyselyitä. Näistä jouduttiin kuitenkin karsimaan edellä mainitun huonon ajankäytön vuoksi. Loppua kohden alkanut kiire sai jättämään kaiken ylimäärisen pois tehtävälistalta.

Motivaatio on ollut kohtalaisen hyvä läpi koko työn, joskin aivan työn alussa ahdistusta toi edessä häämöttävä työn määrä ja kuormitus. Toisinaan kirjoittajan omat ominaisuudet ja suhde akateemisen tekstin kirjoittamiseen toimivat hieman motivaatiota laskevina seikkoina. Varsinkin tekstin luomisessa johdonmukaisuus tuotti

haasteita aiheen lähtiessä kulkemaan sivuteille. Myös tekstin siirtäminen kesken prosessin LaTeX-pohjaan toi haasteita, tosin tämä muutos myös helpotti lopullisen työn asettelua.

7.2 Tutkimuksesta saadun tiedon hyödyntäminen oppilaitoksessa

Diplomityön pohjalta on alettu toteuttaa oppilaitokselle kyberturvallisuutta käsittelevää videosarjaa, jotka kootaan säilytettäväksi ja katsottavaksi oppilaitoksen intraan. Videot ovat noin 2–5 minuutin pituisia tietoiskuja, joissa pyritään käsittelemään vain yhtä aihetta kerrallaan. Säännöllisin väliajoin erilaisissa kehittämispäivissä on ollut jo pidempää ja syvällisempää kyberturvallisuuteen ja tietoturvallisuuteen liittyvää luentoa. Lisäksi ulkopuoliselta palveluntarjoajalta on ostettu palveluna henkilökunnan tietoturvallisuuden osaamista testaavia harjoituksia ja toimintaa. Ymmärryksen lisääntymisen tuloksia pääsee havainnoimaan jo nyt, sillä tietoturvaosaamisen lisääntyminen on nähtävissä koulun arjessa. Kyberturvallisuuden koulutuksen alkamisen jälkeen henkilökunta on alkanut kiinnittää toimintaansa entistä enemmän huomiota.

7.3 Tutkimuksen jatkaminen

Mahdollista jatkoa ajatellen heräsi työtä tehdessä mielenkiinto tarkastella ja tutkia kyberturvallisuuden koulutuksen vaikuttavuutta. Olisi mielestäni hyödyllistä ja arvokasta tutkia kyberturvallisuuden koulutukseen käytettyjen resurssien määrää ja niillä saavutettuja tuloksia. Koulutuksen tehokkuutta olisi mielestäni tärkeää arvioida vaikuttavuuden kautta. Mittailemalla saatuja tuloksia voitaisiin kehittää parempia koulutusmenetelmiä ja tehostaa kyberturvallisuuden opetusta sekä määrit-

tää koulutuksen todellinen arvo. Koulutuksesta saatava hyöty riippuu myös pitkälti siitä, miten ja millaiseen koulutukseen ohjataan resursseja. Lähtökohtaisesti hyvin kohdennettu koulutus lisää riskienhallintaa ja luo säästö potentiaalia. Toisaalta koulutuksen kustannuksilla saavutettuja hyötyjä voi olla haasteellista puntaroida, mutta saatu data voisi olla erittäin yleishyödyllistä ja muuttaisi koulusta kohtaan jossain määrin vallitsevia negatiivisia ennakkoluuloja. Lienemme yhtä mieltä siitä, että kyberturvallisuuteen liittyvä tietoisuuden parantaminen on meidän kaikkien etu. Nykyistä tutkimusta olisi helppo jatkaa tuottamalla valmis koulutusmateriaali, joka olisi helposti kohdennettavissa.

Lähdeluettelo

[1] R. Paananen, M. Soikkeli, M. Starck, M. Aro, T. Kuusisto, T. Rusila ja T. Tuulensuu, ”Suomen kyberturvallisuusstrategia 2024–2035”, *Valtioneuvoston kanslian julkaisu 2024:11, Valtioneuvosto*, 2024.

[2] N. Takala, ”Ulkoisten kyberturvallisuuden riskien arviointi finanssialan organisaatiossa”, *Pro gradu -tutkielma, Jyväskylän yliopisto*, 2019.

[3] A. Teerisalo, ”Identiteetin-ja pääsynhallinnan hyödyntäminen organisaatioissa”, *AMK-opinnäytetyö, Turun ammattikorkeakoulu*, 2021.

[4] R. Luoma, ”Viranomaisten toimivaltuudet häiriötilanteissa”, *Selvityksiä ja ohjeita 2019:18, Oikeusministeriö*, 2019.

[5] E. Vornanen, ”Kyberturvallisuuden tarkastaminen Suomen kuntien sisäisessä tarkastuksessa”, *Pro gradu -tutkielma, Tampereen yliopisto*, 2021.

[6] S. Kaipainen ja M. Pyysing, ”Kyberturvallisuus suomalaisessa perusopetuksessa: suomalaisessa peruskoulussa tapahtuvan kyberturvallisuuden opetuksen nykytila ja opetussuunnitelmien perusteiden tulevaisuuden suuntaviivat”, *AMK-opinnäytetyö, Hämeen ammattikorkeakoulu*, 2022.

[7] K. Rousku, ”Ohje riskienhallintaan”, *VM 22/2017 Ohje riskienhallintaan, Valtiovarainministeriö*, 2017.

[8] P. Järvinen, ”Kyberuhkia ja somesotaa”, *Kirja, Docendo*, 2018.

[9] P. Järvinen ja K. Rousku, ”Työpaikan tietoturvaopas–tunnista uhat, hallitse riskit”, *kirja, Alma Talent*, 2017.

[10] T. Monto, ”Eettisen hakkeroinnin vaikutukset tietojärjestelmän tietoturvan kehityksessä”, *Kandidaatintutkielma, Jyväskylän yliopisto*, 2023.

[11] I.-N. Oinonen, ”Verkkorikollisuuden kasvu ja sen vaikutus yksityisyyden suojaan”, *AMK-opinnäytetyö, Haaga-Helia ammattikorkeakoulu*, 2024.

[12] M. Hämäläinen, ”Analysis of artificial intelligence in cybersecurity identity and access management: potential for disruptive innovation”, *Diplomityö, Lappeenrannan–Lahden teknillinen yliopisto*, 2024.

[13] T. Vartio, ”Kyberturvallisuuden sääntely Suomessa-NIS2-direktiivi”, *AMK-opinnäytetyö, Satakunnan ammattikorkeakoulu*, 2024.

[14] A. Nykänen, ”Kyberturvallisuuden/tietoturvallisuuden opetus peruskoulussa”, *Pro gradu -tutkielma, Jyväskylän yliopisto*, 2023.

[15] K. Hälvä ja K. S. Laari, ”Digitaalisen toimitusketjun kyberturvallisuuden tehostaminen uusien teknologioiden avulla”, *Kandidaatintutkielma, Turun yliopisto*, 2024.

[16] K. Kananoja, ”Kyberturvallisuuden hallinnan kehittäminen pk-yrityksessä: lähtötilanne ja vaatimustenmukaisuus”, *Ylempi AMK-opinnäytetyö, Turun ammattikorkeakoulu*, 2025.

[17] A. Limnell, ”Kyberrikollisuuden trendit nyt ja seuraavan kolmen vuoden aikana”, *AMK-opinnäytetyö, Poliisiammattikorkeakoulu*, 2021.

[18] H. Lahtonen, ”Hatkaamista, päihteitä ja jengejä-Nuoret rikoksentekijät mediassa”, *AMK-opinnäytetyö, Hämeen ammattikorkeakoulu*, 2022.

[19] M. Mikkola, ”Kyberrikosuhrikokemukset ja niitä selittävät tekijät”, *Pro gradu -tutkielma, Tampereen yliopisto*, 2019.

[20] O. Jurmu, ”Yläkouluikäisten kyberturvallisuus”, *Pro gradu -tutkielma, Jyväskylän yliopisto*, 2025.

[21] M. Soikkeli, ”Lainsäädäntö tieto-ja kyberturvallisuuden perustana: valtionhallinnon viranomaisen näkökulma”, *Pro gradu -tutkielma, Jyväskylän yliopisto*, 2021.

[22] E. Honkanen ja L. Nuutila, ”Ammatillisia opintoja yksilöllisesti. Kokemuksia ohjauksesta ja ammattilaisten yhteistyöstä”, *Julkaisu, Haaga-Helian ammattikorkeakoulu*, 2011.

[23] R. Salo, ”Miten laki ammatillisesta aikuiskoulutuksesta käytännössä toteutuu”, *AMK-opinnäytetyö, Satakunnan amamttikorkeakoulu*, 2011.

[24] P. Timlin, ”Kyberturvallisuusstandardit NIS2-direktiivin riskienhallintavelvoitteen tukena”, *Pro gradu -tutkielma, Jyväskylän yliopisto*, 2024.

[25] P. Waldén, ”NIS2-direktiivi ja valmistava teollisuus”, *AMK-opinnäytetyö, Kaakkois-Suomen ammattikorkeakoulu*, 2024.

[26] N. Kujala, ”NIS2-direktiivin mukainen toiminta pienessä yrityksessä”, *AMK-opinnäytetyö, Jyväskylän ammattikorkeakoulu*, 2025.

[27] H. Koskinen ja V. Varis, ”Kybervesimittari: itsearviointityökalu vesihuoltolaitosten kyberturvallisuuden kehittämiseen”, *AMK-opinnäytetyö, Jyväskylän ammattikorkeakoulu*, 2025.

[28] A. Lappalainen, ”Tietosuoja ja sen turvaamat oikeudet henkilötietojen käsittelyssä”, *AMK-opinnäytetyö, Savonia-ammattikorkeakoulu*, 2025.

[29] A. Koskela-Laakso, ”Tiedon suojaamisen kehittäminen hybridityössä case yritys X”, *AMK-opinnäytetyö, Laurea-ammattikorkeakoulu*, 2024.

[30] J. Linnala, ”Yleinen tietosuoja-asetus (GDPR) pk-yrityksissä”, *Ylempi AMK-opinnäytetyö, Kaakkois-Suomen ammattikorkeakoulu*, 2020.

[31] H. Helander, ”GDPR-vaikutukset yrityksen tietosuoja-ja tietoturvatyössä”, *AMK-opinnäytetyö, Tampereen Ammattikorkeakoulu*, 2017.

[32] M. Melto, ”Eu-asetuksesta kansalliseen lainsäädäntöön: tietosuojalaki”, *AMK-opinnäytetyö, Laurea-ammattikorkeakoulu*, 2019.

[33] J. Seiluri, ”Tietosuojatyön johtaminen vaativan erityisen tuen oppilaitoksessa”, *Ylempi AMK-opinnäytetyö, Jyväskylän ammattikorkeakoulu*, 2025.

[34] L. Kammonen, ”Tietosuojan hallintamallin laatiminen”, *Ylempi AMK-opinnäytetyö, Tampereen ammattikorkeakoulu*, 2024.

[35] P. Vehkamäki, M. Lahtinen ja U. Vanttaja, ”Julkisuus ja tiedonhallinta opetustoimessa”, *Julkaisut ja oppimateriaalit, Opetushallitus*, 2018.

[36] S. Andersson, ”Tiedonhallintalain vaikutus Tullin asiakirjahallintoon”, *AMK-opinnäytetyö, Turun ammattikorkeakoulu*, 2019.

[37] A. Saarenpää ja J. Riekkinen, ”Oikeusinformatiikan perusteet”, *Teos, Lapin yliopisto*, 2023.

[38] T. Elovaara, ”Oppilas-ja opiskelijahuoltolaki osana suomalaista hyvinvointipolitiikkaa”, *Pro gradu -tutkielma, Helsingin yliopisto*, 2017.

[39] A. Jounio et al., ”Tieto-ja viestintärikokset rikoslain 38 luvussa”, *Pro gradu -tutkielma, Lapin yliopisto*, 2011.

[40] R. Neuvonen ja K. Karppinen, ”Viestintäpolitiikkaa hatusta? Avoimuus ja osallistuminen tietoyhteiskuntakaaren valmistelussa”, *Katsaus, Työelämän tutkimus*, 2016.

[41] T.-J. Widgrén, ”Tekoäly ja kyberturvallisuus”, *AMK-opinnäytetyö, Hämeen ammattikorkeakoulu*, 2023.

[42] R. Åkerlund, ”Tekoälyn käyttö kyberrikollisuudessa”, *Kandidaatintutkielma, Jyväskylän yliopisto*, 2025.

[43] M. Laiso, ”Toimintamalli turvateknisten IoT-laitteiden kyberturvallisuustason arviointiin laite-ja järjestelmäasentajille”, *Ylempi AMK-opinnäytetyö, Laurea-ammattikorkeakoulu*, 2021.

[44] T. Haakana, ”IoT-protokollat ja niiden tietoturva”, *Kandidaatintutkielma, Vaasan yliopisto*, 2025.

[45] S. Kiiskinen, ”Ammatillisen oppilaitoksen henkilöstön kyberturvallisuustietoisuus oppilaitoksen arjessa”, *AMK-opinnäytetyö, Laurea-ammattikorkeakoulu*, 2023.

[46] E. Häyrinen, ”Suomessa tapahtuneet julkisen sektorin tietojärjestelmien tietomurrot lähivuosina”, *AMK-opinnäytetyö, Haaga-Helia ammattikorkeakoulu*, 2025.

[47] H.-L. Karppanen ja H. Töllinen, ”Wilma luokanopettajan työssä ja osana kodin ja koulun välistä vuorovaikutusta”, *Pro gradu -tutkielma, Jyväskylän yliopisto*, 2019.

[48] M. Jarnola, ”Bug Bountyn hyödyt tietoturvatestauksessa: tapaustutkimus-Lähitapiola”, *Pro gradu -tutkielma, Jyväskylän yliopisto*, 2018.

[49] I. Antila, ”ISO/IEC 27001: 2022-standardin tuomat muutokset organisaatiossa”, *AMK-opinnäytetyö, Tampereen ammattikorkeakoulu*, 2023.

[50] A. Moilanen, ”Tietoturvallisuuden hallintajärjestelmä: sisältö ja kehittäminen valtionhallinnon organisaatiossa”, *AMK-opinnäytetyö, Mikkelin ammattikorkeakoulu*, 2012.

[51] H. Mönttinen ja H. Piekkari, ”Päiväkodin henkilöstön tietosuoja-ja tietoturvakoulutuksen kehittäminen”, *Ylempi AMK-opinnäytetyö, Oulun ammattikorkeakoulu*, 2024.

[52] E. Paavola, E. Mäki ja Y. V. Yliverronen, ”Alakoulun 5.–6.-luokkalaisten oppilaiden kokemuksia tuntoaistin merkityksestä käsityön oppimisessa”, *Kandidaatintutkielma, Turun yliopisto*, 2024.

[53] K. Kiiski, ”Oppilaan visuaalisen hahmottamisen vaikeudet opettajien kertomana: näkökulmina koulun arki ja matematiikan oppiminen”, *Pro gradu - tutkielma, Jyväskylän yliopisto*, 2022.

[54] T. Salminen, ”Identiteetin-ja käyttövaltuushallinnan kehittäminen Sipoon kunnassa”, *Ylempi AMK-opinnäytetyö, Kaakkois-Suomen ammattikorkeakoulu*, 2022.

[55] E. Oksanen, ”VPN-erillisverkon käyttöönotto yrityksessä”, *AMK-opinnäytetyö, Turun ammattikorkeakoulu*, 2019.

[56] J. Saarinen, S. Venäläinen, P. Johnson, H. Cantell, G. Jakobsson, P. Koivisto, M. Routti, J. Väänänen, M. Huhtanen, A. Kivistö et al., ”OPS-työn askeleita: Esi-ja perusopetuksen opetussuunnitelmien perusteiden 2014 toimeenpanon arviointi”, *Julkaisu 1:2019, Kansallinen koulutuksen arviointikeskus*, 2019.

[57] J. Juntunen, ”Koulutusmateriaali: tietoturvallisuuden perusteet”, *AMK-opinnäytetyö, Lapin ammattikorkeakoulu*, 2023.

[58] S. Lehtola, J. J. Tuulari, L. Karlsson, R. Parkkola, H. Karlsson ja N. M. Scheinin, ”Miten varhainen stressi vaikuttaa aivojen kehitykseen”, *Julkaisu, Duodecim*, 2016.

[59] E. Salmi, ”Motivaatio, oppimisvaikeudet ja ammatillisten opintojen loppuun suorittaminen”, *Väitöskirja, Jyväskylän yliopisto*, 2022.

[60] T. Heiska, ”Neurostimulaatio muistin ja oppimisen tehostamisessa”, *AMK-opinnäytetyö, Metropolia ammattikorkeakoulu*, 2025.

[61] U. Valve, ”Unen merkitys sairauksien synnyssä”, *Julkaisu, Duodecim*, 2008.

[62] T. Myllynen, ”Vertailussa oppimisympäristöjen toiminnallisuus ja akustiikka”, *AMK-opinnäytetyö, Oulun ammattikorkeakoulu*, 2018.

[63] T. Kallio, ”Oppiminen on moniulotteinen prosessi”, *Pro gradu -tutkielma, Tampereen yliopisto*, 2016.

[64] H. Karjalainen, ”Oppimiskäsityksistä opettamiseen”, *Pro gradu -tutkielma, Tampereen yliopisto*, 2006.

[65] M. Huhtala, ”Oppimistapojen huomioiminen musiikinopetuksessa”, *Kandidaatintutkielma, Jyväskylän yliopisto*, 2014.

[66] J. Mokko, ”Laulajan ergonomia: laulajan joustavuuden näkökulmasta”, *AMK-opinnäytetyö, Centria-ammattikorkeakoulu*, 2025.

[67] H. Soini, ”Oppiminen sosiaalisena käytäntönä”, *Artikkeli, tievie Oulu*, 2001.

[68] M. T. Hasan, ”Cybersecurity in bank: a case on employee engagement and responsibility for a Secure Digital Environment (SDE) in the selected branch”, *Pro gradu -tutkielma, Tampereen yliopisto*, 2023.

[69] I. Nirvi ja F. K. Kimppa, ”Yleisen tietosuoja-asetuksen noudattaminen pilvipalveluissa”, *Kandidaatintutkielma, Turun yliopisto*, 2024.

[70] G. Ho, A. Mirian, E. Luo, K. Tong, E. Lee, L. Liu, C. A. Longhurst, C. Dameff, S. Savage ja G. M. Voelker, ”Understanding the efficacy of phishing training in practice”, *Artikkeli, San Diego Yliopisto*, 2025.

[71] A.-L. Ojala, K. Saharinen ja T. Sipola, ”Suomalaisten oppilaitosten valmius kohdata kyberkriisejä”, *Tutkimushankkeen loppuraportti, Jyväskylän ammattikorkeakoulu*, 2025.

[72] J. Mattila, M. Pajarinen, T. Seppälä, K. Mäkäräinen ja V. Neuvonen, ”Digibarometri 2021: Vuosikymmen verkkokauppaa ja alustataloutta”, *Tutkimus, Taloudellisen tutkimuksen laitos*, 2021.