Tietoturvallisuuskoulutuksen vaikuttavuuden arviointi

Turvallisuusjohdon koulutusohjelma

Lopputyöraportti

Laura Kujala

Puolustusvoimat

Tampere 02.12.2023

Aalto University Executive Education and Professional Development

Tiivistelmä

Työn tavoitteena oli tarkastella, mitä tarkoitetaan tietoturvallisuuskoulutuksella ja miten sen vaikuttavuutta voidaan arvioida. Tarkoituksena oli kuvata lähdeaineiston perusteella vaiheet, joiden kautta organisaatio pystyy toteuttamaan tietoturvallisuuskoulutuksen vaikuttavuuden arviointia huomioiden arvioinnin kohteena oleva koulutus. Käytettäväksi teoreettiseksi viitekehykseksi valikoitui Kirkpatrickin nelitasoinen koulutuksen vaikuttavuuden arviointimalli.

Lähdeaineiston perusteella voidaan todeta, että tietoturvallisuuskoulutuksen vaikuttavuuden arvioinnin on oltava kiinteä osa itse koulutusta. Arviointiin liittyvät kokonaisuudet (esimerkiksi tavoitteet, arvioinnin tasot ja arviointimenetelmät, toteutusajankohdat) on huomioitava osana koulutuksen suunnittelua, ennen itse koulutusta. Toimimalla näin tietoturvallisuuskoulutuksen vaikuttavuuden arviointi on kokonaisvaltaista ja hyödyttää parhaiten organisaatiota ja sen toimintaa.

Sisältö

1 Johdanto

Yritysten ja organisaatioiden toimintaympäristöt ovat muuttuneet hyvin paljon viimeisten vuosikymmenten aikana. On keskitytty ydintoimintoihin, ulkoistettu ja digitalisoitu toimintoja sekä –toimintaprosesseja, otettu käyttöön uusia teknologioita ja tietojärjestelmiä, siirretty toimintoja internettiin, siirrytty lähityöskentelystä etä- ja hybridityöhön. Nämä ovat suuria muutoksia, joissa organisaatioiden työntekijöiden on pitänyt mukautua ja osata toimia oikein tietoturvallisesti, suojaten toiminnan kannalta kriittisiä tietoja. Tieto- ja kyberturvallisuuden merkitys on korostunut toimintaympäristöjen ollessa entistä verkottuneempia ja monimutkaisempia. Usein tieto- ja kyberturvallisuus mielletään teknisiksi asioiksi, kuten palomuureiksi ja haittaohjelmatorjunnaksi, ja unohdetaan keskeisin elementti, henkilöstö. SANS Instituten selvityksen (2023) mukaan keskeisimmän uhkavektorin kyber- ja tietoturvallisuusriskien toteutumiselle muodostaa henkilöstö. Henkilöstön tietoturvallisuusosaamisen ja koulutuksen lisääminen on tunnistettu Digi- ja väestötietoviraston Digiturvakyselyssä (2023) yhdeksi Johtaminen-osa-alueen kehittämiskohteeksi. Koulutukset itsessään eivät kuitenkaan ole itseisarvo. Tietoturvallisuuskoulutuksilla on oltava sekä selkeät tavoitteet että vaikutus henkilöstön toimintaan. Tietoturvallisuuskoulutusten vaikuttavuuden arvioinnit koetaan organisaatioissa kuitenkin vaikeaksi eikä niitä välttämättä edes yritetä toteuttaa.

1.1 Lopputyön tavoite ja rajaukset

Lopputyössä pyritään vastaamaan seuraaviin kysymyksiin:

1. Mitä tietoturvallisuuskoulutuksella tarkoitetaan?
2. Miten tietoturvallisuuskoulutuksen vaikuttavuutta voidaan arvioida?

Työssä ei käsitellä tietoturvallisuuskoulutusten sisältöä eikä tietoturvallisuusohjelman tai -kampanjan suunnittelua ja toteutusta. Lopputyössä keskitytään

tietoturvallisuuskoulutusten vaikuttavuuden arviointiin. Teoreettisena viitekehyksenä tietoturvallisuuskoulutuksen vaikuttavuuden arvioinnissa on Donald Kirkpatrickin kehittämä nelitasoinen koulutusten vaikuttavuuden arviointimalli.

1.2 Työn rakenne

Teoriaosassa tarkastellaan ensin osaamista, oppimista sekä koulutuksia oppimisen keinona. Tämän jälkeen tarkastellaan tietoturvallisuuuskoulutusta käsitteenä: mistä se muodostuu ja mihin se liittyy. Kolmanneksi tarkastellaan ja käydään läpi Kirkpatrickin koulutuksen vaikuttavuuden arviointimalli, jota sovelletaan lopputyön empiirisessä osiossa.

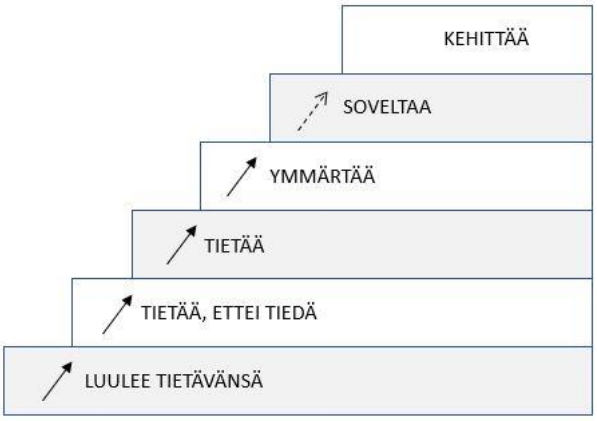
Empiirisessä osiossa kuvataan vaiheet, joiden kautta organisaatio pystyy toteuttamaan tietoturvallisuuskoulutuksen vaikuttavuuden arviointia teoriaosassa kuvatun Kirkpatrickin mallin mukaisesti. Osana empiiristä osiota haastatellaan kahden suomalaisen yrityksen tietoturvallisuushenkilöitä. Haastattelujen tarkoituksena on saada kuva siitä, miten käytännössä ao. yritykset toteuttavat tietoturvallisuuskoulutuksia ja miten niiden vaikuttavuutta arvioidaan. Tietoturvallisuuskoulutusten vaikuttavuuden arviointi kuvataan kahden kuvitteellisen tietoturvallisuuskoulutuksen avulla.

2 Osaaminen ja oppiminen

2.1 Oppimisen perusteet

Organisaation toiminnan keskiössä ovat yksilöt ja heidän osaamisensa. Organisaation toiminnan laatu ja tehokkuus perustuvat siihen, miten hyvin organisaation työntekijät osaavat työnsä, miten hyvin osaamista hyödynnetään sekä miten hyvin ja nopeasti työntekijät oppivat uusia tarvittavia tietoja ja taitoja. Organisaation on siis tunnistettava olemassa oleva osaaminen ja osattava hyödyntää sitä. Samalla organisaation on tunnistettava mahdolliset uudet osaamistarpeet osana osaamisen kehittämistä (Viitala 2013). Tarkasteltaessa koulutusta osaamisen kehittämisen menetelmänä, on huomioitava yksilön oppiminen. Sydänmaanlakan (2012, s. 33-37) mukaan oppiminen voidaan määritellä prosessiksi, jossa yksilö hankkii uusia tietoja, taitoja ja asenteita, jotka johtavat muutoksiin hänen toiminnassaan. Oppimisprosessissa motivaatio eli halu oppia on kaiken oppimisen lähtökohta. Ilman motivaatiota oppiminen ei ole mahdollista.

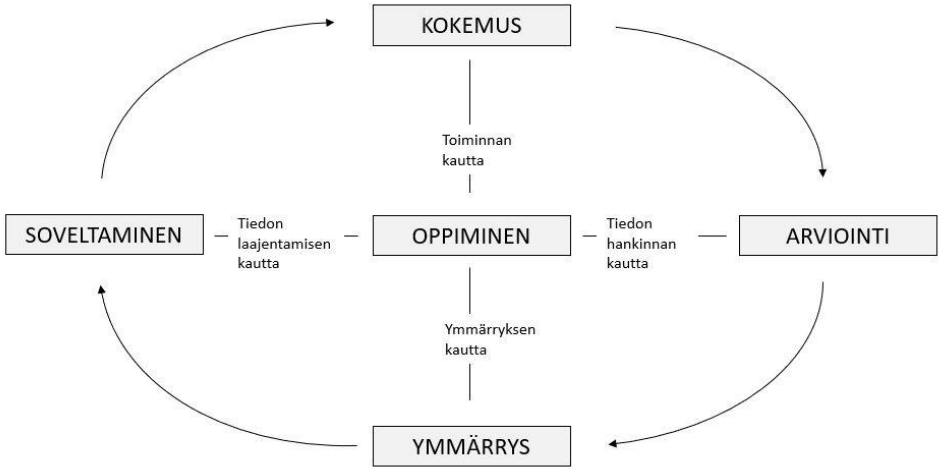
Oppimista tapahtuu usealla eri tasolla. Sydänmaanlakka (2012, s. 34-35) on kuvannut oppimisen portaat, jotka on esitetty kuvassa 1.



Kuva 1 Oppimisen portaat (Sydänmaanlakka 2012)

Tietämisen tasolla tarkoitetaan kuvassa 1 uuden tiedon hankintaa. Alimmat kaksi tasoa, luulee tietävänsä ja tietää, ettei tiedä, voidaan havaita jo ennen tietämisen tasoa. Edellytys uuden oppimiselle on siis oman tietämättömyyden tunnistaminen. Ymmärtämisellä tarkoitetaan, että opittava asia on ymmärretty eli sisäistetty. Tähän tasoon sisältyvät yksilön asenteet ja tunteet. Soveltaminen on astetta korkeampi taso. Sillä tarkoitetaan, että yksilö pystyy soveltamaan uutta opittua asiaa käytännössä onnistuneesti. Edellisten tasojen tietäminen ja ymmärtäminen on tuolloin hallinnassa. Todellinen oppiminen pitää sisällään kaikki kuvatut tasot. Ylimpänä ja viimeisenä tasona on kehittämisen taso. Tällä tasolla jo hyvin hallussa olevia toimintamalleja pyritään uudistamaan ja kehittämään (Sydänmaanlakka 2012, s. 34-35).

Sydänmaanlakka (2012, s. 37-39) on esitellyt Kolbin perusmallin oppimisprosessissa. Kolbin malli on esitetty kuvassa 2.



Kuva 2 Oppimisprosessi Kolbin mukaan (Sydänmaanlakka 2012)

Kolbin mallissa oppiminen lähtee liikkeelle kokemuksista ja siitä, että yksilöllä on halu ja motivaatio oppia niistä. Yksilö muokkaa aikaisempaa tietoa ja kokemuksia synnyttäen uutta tietoa. Viitalan (2013) mukaan motivaatio on yksilön sisäinen voima, joka suuntaa ja virittää toiminnan. Motivaatio saa yksilön toimimaan tietyllä tavalla. Motivaatiota voidaan tarkastella sekä sisäisen että ulkoisen motivaation näkökulmasta. Ulkoisella motivaatiolla tarkoitetaan tilaa, jossa syy toimintaan perustuu ulkoisten palkkioiden tavoitteluun. Ulkoisia palkkioita voivat olla esimerkiksi parempi rahallinen palkka, bonus tai arvostus. Henkilön saadessa tyydytyksen itse työstä ja siinä onnistumi-

sesta (aikaansaannoksistaan) on kyse sisäisestä motivaatiosta. Se liittyy Viitalan mukaan itsensä toteuttamisen ja kehittämisen tarpeisiin (Viitala 2021, s. 42). Uuden oppimista ja kehittymistä tapahtuu, kun yksilölle syntyy kokemus, että edistyminen on tärkeää ja mielekästä (Viitala 2013).

Tämän jälkeen yksilöllä pitää olla aikaa sekä hankkia kokemukseen liittyvää tietoa että pohdiskella ja arvioida sitä. Tässä erilaisia näkemyksiä ja tosiasioita prosessoidaan ja muunnetaan tiedoksi. Tämän jälkeen tiedot pyritään ymmärtämään ja sisäistämään. Seuraavassa soveltamisen vaiheessa sisäistettyä tietoa sovelletaan käytäntöön ja kokeillaan erilaisissa yhteyksissä. Täydellinen oppimisprosessi pitää sisällään kaikki nämä vaiheet. Oppimistapahtuma tulisi suunnitella siten, että kaikki vaiheet käytäisiin läpi (Sydänmaanlakka 2012, s. 38-39).

2.2 Oppiminen työelämässä

Viitala (2013) on esittänyt Dohmenin luokituksen työelämässä tapahtuva oppimiseen:

1. Oppiminen, joka tapahtuu koulutusorganisaatioiden piirissä. Opiskelu on määrämuotoista ja johtaa tavallisesti tutkinnon tai opintokokonaisuuden suorittamiseen. Opiskelu voi olla ulkopuolisen järjestämää tai organisaation sisäinen opinto-ohjelma todistuksineen.
2. Oppiminen, joka sisältää yrityksen itsensä järjestämiä tai ulkopuolelta hankkimia oppimistapahtumia. Nämä tilaisuudet eivät johda muodollisiin tutkintoihin.
3. Oppiminen, joka ei ole systemaattisesti suunniteltua ja organisoitua. Oppiminen tapahtuu työssä ja työympäristössä.
4. Oppiminen, joka tapahtuu tahattomasti ja suunnittelemattomasti. Eteentuleva työtehtävä tai ongelma voi pakottaa oppimaan. Tällainen oppiminen on yleensä tiedostamatonta.

Organisaation koulutuksilla tavoitellaan usein yksilön käyttäytymisen muutosta. Henkilöstölle koulutetaan uusia tietoja ja taitoja, joiden halutaan siirtyvän yksilöiden toimintaan. Uusien tietojen kouluttaminen on nopeampaan kuin uusien taitojen. Vielä vaikeampaa on yksilön asenteiden muuttaminen. Yksilön käyttäytyminen muuttuu vasta kun tarvittavat tiedot, taidot ja asenteet ovat muuttuneet. Käyttäytyminen ei siis muutu vain tiedon vaikutuksesta, vaan myös tunteet ovat tärkeitä (Sydänmaanlakka 2012, s. 71). Tietoturvallisuusalan tutkimuksissa on tunnistettu tietämisen ja tekemisen välinen kuilu (eng. Knowing-doing-gap). Vilander (2021, s. 3) on tutkinut tuota kuilua eli miksi työntekijät tarkoituksellisesti jättävät noudattamatta ohjeita ja mikä on

asenteen rooli toiminnassa. Tutkimuksen mukaan asenne tietoturvallisuutta kohtaan olisi merkittävämpi tekijä käyttäytymisen kannalta kuin tieto.

2.3 Oppimisen esteet

Kirjallisuudessa on tunnistettu useita oppimisen esteitä. Sydänmaanlakka (2012, s. 45-46) on tunnistanut seuraavia oppimisen esteitä:

- ei ole halua oppia, motivaatio on matala
- ei ole selkeitä oppimistavoitteita
- tieto ei ole saatavilla
- tietoa on liikaa
- tiedot ovat ristiriitaisia, epäjohdonmukaisia ja sekavia
- ymmärtämistä ei pidetä tarpeellisena, ajatellaan, että pinnallinen tieto riittää
- nykyisen ja uuden tiedon välillä on liian suuri muutos
- asiat unohdetaan, jos dokumentaatio on puutteellista.

Organisaation on tunnistettava mahdollisia oppimisen esteitä etukäteen ja pyrittävä pienentämään niitä esimerkiksi osana koulutusten suunnittelua.

2.4 Yksilön osaaminen

Organisaation työntekijöiden osaaminen muodostaa pohjan organisaation toiminnan päämäärien ja perustehtävän toteutumiselle. Lisäksi yksittäisen työntekijän osaaminen muodostaa perustan hänen onnistumiselleen ja kehittymiselleen omassa työtehtävässään ja työyhteisössään. Osatessaan hoitaa työtehtävänsä, henkilö saa muilta työntekijöiltä arvostusta, tuntee pätevyyden ja merkityksellisyyden tunnetta (Viitala 2013).

Työelämäkvalifikaatioilla tarkoitetaan työntekijän työssä ja työorganisaatiossa tarvitsemia valmiuksia eli osaamista. Osa näistä on yksiön persoonallisia ominaisuuksia tai henkilökohtaisia kykyjä, osa taas koulutuksessa, työssä tai muualla kehittyneitä valmiuksia eli osaamista. Ammattitaito koostuu useista kvalifikaatioista, joita on ryhmitelty yleisiin, ammattikohtaisiin ja tehtäväkohtaisiin kvalifikaatioihin. Yleiset kvalifikaatiot liittyvät valmiuksiin, joita tarvitaan työelämässä yleensä eivätkä ne ole tehtäväriippuvaisia. Ammattikohtaiset kvalifikaatiot liittyvät tiettyyn ammattialaan ja muodostavat substanssiosaamisen. Tehtäväkohtaiset kvalifikaatiot liittyvät tiettyyn tehtävänkuvaan. Osaa kvalifikaatiosta voidaan nimittää osaamiseksi, osa taas

on ennemminkin henkilökohtaisia kykyjä, joita ei koulutuksen tai työkokemuksen kautta ole suoraan hankittavissa (Viitala 2013).

Asenteet ja motivaatio liitetään oppimisen lisäksi usein myös osaamiseen. Asenne katsotaan melko pysyväksi, hitaasti muuttuvaksi perusvireeksi, kun taas motivaation katsotaan olevan melko lyhytaikainen ja yleensä myös tilannekohtainen. Molemmat niistä ovat tärkeitä sen kannalta, miten yksilö hyödyntää ja käyttää omaamiaan tietoja ja taitoja työtehtävissään. Myönteinen asenne ja motivaatio mahdollistavat parhaiten sen, että yksilön osaaminen hyödyttää organisaatiota. Osaaminen hyödyntyy organisaatiossa parhaiten myönteisen asenteen ja motivaation varassa ja samanaikaisesti se myös vaikuttaa niihin (Viitala 2013).

2.5 Koulutus osaamisen kehittämisen keinona

Yksilön osaamisen kehittämisessä koulutus on yksi monista käytettävissä olevista keinoista. Koulutuksella tarkoitetaan Viitalan (2013) mukaan kaikkea oppimiseen tähtäävää toimintaa, jossa joku järjestää muille työntekijöille mahdollisuuden oppimiseen. Koulutus tapahtuu erillään työnteosta, erikseen järjestetyssä tilassa tiettynä ajankohtana. Oppimista tapahtuu kuitenkin myös muualla organisaatioiden tilaisuuksissa ja tapahtumissa kuten esimerkiksi henkilöstöinfoissa, tiedotustilaisuuksissa, tiimi- ja ryhmäpalavereissa (Viitala 2021. s. 136).

Koulutuksissa voidaan käyttää useita eri koulutusmenetelmiä, ja koulutukset voivat olla hyvin eri mittaisia. Koulutuksen kesto voi vaihdella lyhyestä 30 minuutin luennosta vuosia kestävään tutkintoon johtavaan koulutukseen. Koulutusten kestolla on merkitys koulutuksen tavoitteisiin. Lyhytkestoiset, yksittäiset koulutukset soveltuvat parhaiten jonkin selkeän ja konkreettisen työssä tarvittavan tiedon päivittämiseen tai uuden konkreettisen asian käsittelyyn. Lyhytkestoiset koulutukset soveltuvat myös uuden konkreettisen taidon opetteluun. (Viitala 2013) Ammattitaidon kehittämisessä pitkäkestoisilla koulutuksilla tuetaan paremmin laajemman ja syvällisemmän osaamisen hankkimista sekä tuetaan käsitteellisten tietojen ja taitojen hankkimista (Viitala 2021, s. 135).

Kouluttajina voidaan käyttää joko organisaation omia asiantuntijoita tai organisaation ulkopuolisia henkilöitä. Omien kouluttajien käyttö mahdollistaa

koulutuksissa käsiteltävän asian käsittelyn syvällisemmin osana organisaation toimintoja. Ulkopuolisten kouluttajien avulla organisaatio voi tuoda uusia näkökulmia ja ajatuksia. Samalla mahdollistetaan kokemusten vaihto muiden organisaatioiden edustajien kanssa (Viitala 2013).

Koulutuksia voidaan toteuttaa eri opetusmenetelmin: behavioristisen tai konstruktionismisen lähestymistavan mukaisesti. Lähestymistapojen ero on siinä, miten oppijaan suhtaudutaan. Behavioristisen lähestymistavan koulutuksissa oppija nähdään passiivisena tiedon vastaanottajana, jolle tieto siirretään sellaisenaan. Konstruktionistisessa lähestymistavassa oppija nähdään aktiivisena tiedon tuottajana ja oppija pidetään keskiössä. Koulutus lähtee siis oppijan omista lähtökohdista ja tarpeista. Lisäksi koulutus aktivoi oppijaa (Viitala 2021, s. 135).

3 Henkilöstön koulutus – osa organisaation tietoturvallisuutta

Jokainen organisaatio määrittelee organisaatiokohtaisesti mitä tietoturvallisuudella tarkoitetaan, mitkä ovat sen tavoitteet ja miten tavoitteisiin päästää. Yhteistä eri määritelmille on, että tietoturvallisuus rakentuu tiedon kolmen ominaisuuden: luottamuksellisuuden, eheyden ja käytettävyyden (saatavuuden) turvaamisesta.

Keskiössä tietoturvallisuudessa on siis organisaation suojattavien kohteiden turvaaminen eri suojaustoimenpiteiden avulla. Toimenpiteet voidaan jakaa karkeasti hallinnollisiin ja teknisiin. Usein käytetään termiä kyberturvallisuus kuvaamaan toimenpiteitä, joilla voidaan ennakoivasti hallita ja tarvittaessa sietää erilaisia kyberuhkia ja niiden vaikutuksia. Kyberturvallisuudella tarkoitetaan digitaalisen ja verkottuneen organisaation turvallisuutta ja sen vaikutusta niiden toimintoihin (Sanastokeskus, TEPA-termipankki).

Henkilöstöä pidetään organisaatioiden tärkeimpänä voimavarana ja henkilöstön merkitys tietoturvallisuuden toteutumisessa on hyvin merkittävä. Edellä mainittujen syiden vuoksi voisi kuvitella, että henkilöstön tietoturvallisuuskoulutukseen panostamisen tärkeys olisi itsestään selvää mutta näin ei välttämättä ole. Euroopan tietoturvallisuusviranomaisen ENISA:n (The European Union Agency for Cybersecurity) mukaan syyt organisaation tietoturvallisuuskoulutus- ja tietoisuusohjelmalle voivat olla joko organisaation sisäisiä tai ulkoisia. Ulkoisia syitä ovat esimerkiksi uusi velvoittava lainsäädäntö, kansallinen ohjeistus tai noudatettavan tietoturvallisuusstandardin velvoite. Sisäisiä syitä voivat olla yritysfuusio, uuden tuotteen tai palvelun lanseeraus, tapahtunut tietoturvallisuuspoikkeama tai läheltä piti tapaus (ENISA 2010, s. 15-16).

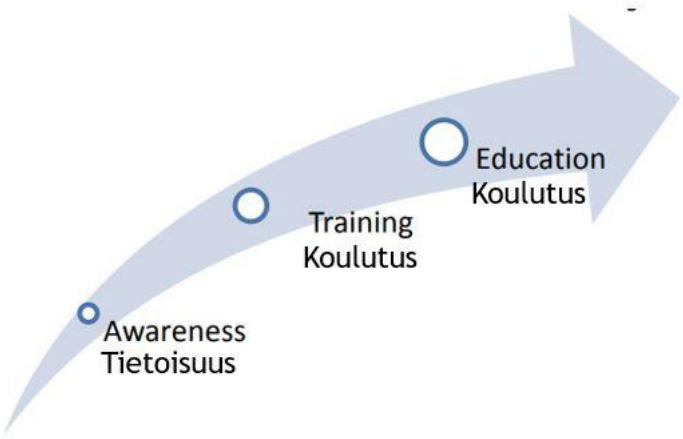
Tietoturvallisuuden hallintaan on käytettävissä useita eri viitekehyksiä ja hallintamalleja kuten esimerkiksi ISO/IEC 27001 standardien mukainen tietoturvallisuuden hallintajärjestelmä. Henkilöstön tietoturvallisuustietoisuus on yksi hallintajärjestelmässä esitetyistä vaatimuksista. Tietoisuudella viitataan henkilöstön tarvitsemaan ymmärrykseen siitä, mitä heiltä odotetaan tietoturvallisuuden osalta sekä siihen liittyvään motivaatioon. Henkilöiden pitää esimerkiksi tuntea, ymmärtää, hyväksyä sekä tukea tietoturvapolitiikassa esitettyjä tavoitteita. Lisäksi henkilöiden tulee noudattaa annettuja sääntöjä suorittaakseen päivittäiset tehtävänsä oikein huomioiden tietoturvallisuusohjeistus. Käytännössä vaatimus tarkoittaa organisaation toteuttamaa tietoturvallisuustietoisuus- ja -koulutusohjelmaa, jossa edellä mainittuja asioita käsitellään kohderyhmäkohtaisesti. Tietoisuusohjelma koostuu useista yksittäisistä toimenpiteistä, jotka nivoutuvat yhdeksi kokonaisuudeksi. Tietoturvallisuuden hallintajärjestelmää pitää luomisen jälkeen suunnitelmallisesti ylläpitää ja kehittää. Tämä edellyttää nykytoiminnan seuraamista ja analysointia. On siis tiedettävä, miten nykyinen tietoisuus- ja koulutusohjelma toimii ja mikä on sen vaikuttavuus, jotta toimintaa voidaan kehittää (ISO 27003:2017, ISO 27001:2022).

3.1 Tietoturvallisuustietoisuus vs. tietoturvallisuuskoulutus

Tieto- ja kyberturvallisuutta käsittelevistä materiaaleista löytyy useita artikkeleita ja tutkimuksia tietoturva- tai kyberturvallisuustietoisuus- sekä koulutusohjelman rakentamiseksi ja toteuttamiseksi, esimerkiksi ENISA:n julkaisut The new user’s guide: How to raise information security awareness sekä Your guide to designing a cyber-awareness programme. Termejä tietoturvallisuustietoisuus ja tietoturvallisuuskoulutus käytetään vaihtelevasti. Organisaatioissa voidaan käyttää termiä tietoturvakoulutus siten, että se kattaa myös tietoturvallisuustietoisuuden. Nykäsen (2011, s. 20) mukaan tietoturvallisuuskoulutuksen tavoitteena on parantaa yksilön tietoturvallisuustietoisuutta, asenteita, totuttuja tapoja ja motivaatiota sekä ohjata siten organisaation henkilöstön tietoturvallisuuskäyttäytymistä haluttuun suuntaan. Jos koulutus ei ole hyvin suunniteltua, jatkuvaa, tehokasta ja systemaattista, eivät organisaatiossa työskentelevät ihmiset saa tarpeeksi tietoturvallisuustoimintaa tukevaa informaatiota. Hyvä tietoturvallisuustietoisuus vaikuttaa ihmisen motivaatioon ja asenteisiin kohti oikeanlaista tietoturvallisuuskäyttäytymistä. On huomioitava, että suomenkielen sanalla koulutus voidaan tarkoittaa sekä englannin kielistä termiä training että education. Tässä lopputyössä sanalla training

tarkoitetaan organisaation itse tuottamaan tai ostamaa tietoturvallisuuskoulutusta. Sanalla education tarkoitetaan toisen tai kolmannen asteen tutkintoon johtavaa opiskelua.

Tietoturvallisuustietoisuus (awareness) , tietoturvallisuuskoulutus (training) ja tutkintoon johtava tietoturvallisuuskoulutus (education) ovat omia kokonaisuuksiaan, kuten on esitetty kuvassa 3 (kuvaan lisätty suomennokset) (ENISA 2010, s.15). Vaikka ne on esitetty peräkkäisinä ja erillisinä osioina, käytännössä ne menevät usein osittain päällekkäin (Guimaraes 2021, s. 31).

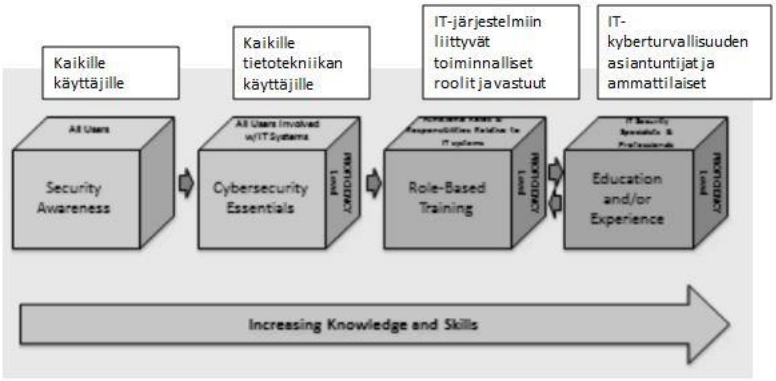


Kuva 3 Tietoturvallisuustietoisuus ja -koulutus (ENISA 2010)

3.2 Tietoturvallisuustietoisuus

Tietoturvallisuustietoisuudella (awareness) Dhakalin (2010) mukaan Bulgurcu et al. tarkoittavat työntekijän yleistä tietämystä ja ymmärrystä tietoturvallisuuteen liittyvistä ongelmista ja niiden seurauksista. NIST:n (National Institute of Standards and Technology) mukaan tietoturvallisuustietoisuuden tarkoituksena on kiinnittää henkilöstön huomio tietoturvallisuuteen ja siitä annettuihin ohjeisiin. Näin toimimalla luodaan valmius tietoturvallisuuteen liittyvien uhkien ja haavoittuvuuksien tunnistamiseen ja tietoisuuteen oikeista toimenpiteistä eri tilanteissa. Tietoturvallisuustietoisuuden avulla selitetään perusteet organisaation tietojen ja tietojärjestelmien käsittelylle ja kerrotaan organisaation hyväksytty tietojen ja tietojärjestelmien käyttö (Toth & Klein 2014, s. 28-29). Veselin (2011, s. 5) mukaan tietoturvallisuustietoisuudella henkilöstöä opetetaan sekä suojaamaan organisaation tietoja että estämään tietoturvallisuuspoikkeamien syntyminen.

NIST:n mukaan tietoturvallisuustietoisuus on ”Mitä”-komponentti organisaation tietoturvallisuuskoulutusstrategiassa. Tietoturvallisuustietoisuudella luodaan organisaation tietoturvallisuudelle pohja, jonka päälle tietoturvallisuuskoulutukset voidaan suunnitella ja toteuttaa. Tarvittaessa koulutuksia järjestetään eri kohderyhmille. Tietoturvallisuustietoisuus ja -koulutukset muodostavat tietoturvallisuusoppimisessa jatkumon kuvan 4 mukaisesti (Wilson et al 1998, s. 18, Toth & Klein 2014, s. 25-26).



Kuva 4 Kyberturvallisuuden oppimisjatkumo (Toth & Klein 2014)

Oppiminen alkaa tietoisuudella (awareness), jota seuraa koulutus (training) ja toisena ääripäänä on muodollinen, pitkäkestoinen koulutus ja/tai osaaminen (education/experience). Standardin 800-16 ”A Role-Base Model for Federal Information Technology/Cybersecurity Training” uusimmassa päivitysversiossa NIST on tuonut jatkumoon mukaan kyberturvallisuuden, cybersecurity essentials, kuvan 4 mukaisesti (Toth & Klein 2014, s. 26). Riippuen organisaatiosta kyberturvallisuus voi sisältyä tietoturvallisuuteen tai se voi olla oma kokonaisuutensa.

Tietoturvallisuustietoisuustoimenpiteillä vastataan myös kysymykseen, millaista käyttäytymistä ja hyviä tietoturvallisuuskäytänteitä haluamme vahvistaa (Wilson & Hash 2003, s. 23). On kuitenkin hyvä huomioida, että Veselin (2021, s. 2) mukaan tietoisuustoimenpiteillä ei ainoastaan haluta lisätä henkilöstön tietämystä tietoturvallisuudesta, vaan halutaan, että henkilöstö osaa toteuttaa tietoturvallisuutta jokapäiväisissä tehtävissään. Tietoisuustoimenpiteillä voidaan tähdätä myös siis henkilöiden käyttäytymisen muuttamiseen.

Hyvällä tietoturvallisuustietoisuudella varmistetaan, että henkilöstö ymmärtää,

- mitä organisaatiossa tietoturvallisuudella tarkoitetaan ja mitkä voivat sitä uhata
- miksi tietoturvallisuus on tärkeää
- mikä on henkilön rooli tietoturvallisuudessa
- miten henkilö voi edesauttaa tietoturvallisuuden toteutumista omassa työtehtävässään/roolissaan
- mitä tapahtuu, jos annettuja ohjeita ja toimintatapoja ei noudateta (Veseli 2011, s. 5).

Tietoisuutta edistävät toimenpiteet ovat yleensä tiettyyn aihealueeseen liittyviä lyhytkestoisia, tietoiskunomaisia, selkeitä sekä informatiivisia ja niiden kohderyhmänä on koko henkilöstö (Toth & Klein 2014, s. 29). Tyypillisiä tietoturvallisuustietoisuuden toteutustoimenpiteitä ovat esimerkiksi sarjakuvat, sähköpostitiedotteet- ja uutiskirjeet, julisteet, tietoiskut, työasemien näytönsäästäjät, esitteet, kirjoitukset henkilöstölehdessä ja tiedotteet intranetissä (ENISA 2010, s. 62-63). Tietoturvatietoisuustoimenpiteiden toteuttamisen jälkeen organisaatio voi alkaa suunnittelemaan ja toteuttamaan syvällisempiä tietoturvallisuuskoulutuksia (Wilson & Hash 2003, s.9).

3.3 Tietoturvallisuuskoulutus (training)

Tietoturvallisuuskoulutuksella tarkoitetaan toimenpiteitä, joiden tavoitteena on luoda koko henkilöstölle heidän työssään tarvitsemaa tietoturvallisuustietämystä ja -osaamista sekä tehtäväkohtaisia tietoturvallisuustaitoja (Anabkwa et. al, 2014) Tietoturvallisuuskoulutuksilla organisaatio vastaa kysymykseen, mitä tietoturvallisuustaitoja ja -osaamista työntekijöiden halutaan oppivan ja käyttävän omissa työtehtävissään. Osittain nämä taidot vaihtelevat henkilöiden työtehtävien mukaisesti. On kuitenkin yhteisiä taitoja ja toimintatapoja, joita edellytetään kaikilta. Lisäksi on tehtäväkohtaisia vaatimuksia kuten kuvassa 4 on esitetty. Kaikilta edellytettäviä taitoja voidaan kouluttaa yhteisillä, koko henkilöstölle suunnatuilla tietoturvallisuuskoulutuksilla. Nämä koulutukset toteutetaan yleensä aihelähtöisesti (Toth & Klein 2014, s. 9, 18, 35).

Merkittävin ero tietoturvallisuustietoisuuden ja -koulutuksen välillä on, että koulutuksen tavoitteena on mahdollistaa tietyn toiminteen, toiminnon tai työtehtävän suorittaminen tietoturvallisesti. Tietoturvallisuustietoisuuden tavoitteena on kiinnittää yksilön huomio tietoturvallisuusasioihin yleisemmällä tasolla (Toth & Klein 2014, s. 9, 20). Dhakal (2018) on esittänyt, että Higtin mukaan tietoturvallisuuskoulutuksia käsiteltäessä on hyvä huomioida, että tietoturvallisuuskoulutuksilla ei opeteta henkilöstöä tekemään työtään vaan

opetetaan henkilöstöä tekemään työnsä tietoturvallisesti. Guimaraesin (2021, s. 31) mukaan henkilöstön tulisi saada lisäksi tietoturvallisuuskoulutusta, jotta tietoturvallisuustietoisuustoimenpiteet olisivat vaikuttavia. Tietoisuustoimenpiteet eivät siis yksinään ole riittäviä suojaamaan organisaation sitä uhkaavilta tietoturvallisuusuhilta.

Tietoturvallisuuskoulutukset ovat yleensä muodollisempia ja niiden rakenteissa on huomioitu koulutuksen päämäärä: jonkin tietyn taidon/osaamisen oppiminen. Tietoisuudella varmistetaan, että henkilö esimerkiksi havaitsee tietoturvallisuusongelman ja reagoi siihen ohjeistetusti. Koulutuksella mahdollistetaan, että henkilö reagoi ongelmaan sekä tarvittaessa kehittää ja toteuttaa ongelmaan vastatoimenpiteitä (Toth & Klein 2014, s. 31).

Tietoturvallisuuskoulutuksia käsiteltäessä voidaan erottaa omaksi kokonaisuudekseen roolipohjaiset koulutukset, kuten kuvassa 4 on esitetty. Niillä tarkoitetaan koulutuksia, jotka on suunnattu henkilöille, joilla on merkittäviä vastuita organisaation tietojärjestelmiin tai tieto- tai kyberturvallisuuteen liittyen. Tehtävä- tai roolipohjaiset koulutukset ovat keskenään eri laajuisia ja sisältöisiä Esimerkiksi tietoverkkojen ylläpidossa toimivat henkilöt tarvitsevat enemmän tekniseen tietoturvallisuuteen liittyvää koulutusta kuin tavalliset loppukäyttäjät, kun taas ohjelmistokehitystä tekevät henkilöt tarvitsevat koulutusta tietoturvalliseen ohjelmistokehitykseen. Tärkeää on, että organisaatio on tunnistanut roolit ja tehtävät sekä määritellyt tarvittavat koulutukset kunkin roolin ja tehtävän vastuiden sekä työtehtävien perusteella (Toth & Klein 2014, s. 9, 27, 30-31). Haastatelluissa yrityksissä tehtäväkohtaisten tietoturvallisuuskoulutusten tarve on tunnistettu ja niitä toteutetaankin käytännössä. Jatkossa niiden merkitys ja määrä tulee lisääntymään.

Koulutuksia voidaan toteuttaa usein eri tavoin. Ne voivat olla itseopiskelua, luokkaopetusta, keskustelupohjaisia, verkko-opetusta, epävirallisia tai virallisia koulutuksia. Tärkeää on, että koulutuksen suunnitteluvaiheessa huomioidaan koulutuksen kohderyhmä, sisältö ja toteutustapa. Nämä vaikuttavat koulutusmetodiin ja toteutustapaan (Toth & Klein 2014, s. 44, Da Veiga, s. 100). Haastelluissa yrityksissä on havaittu, että koko henkilöstölle suunnatut tietoturvallisuuden verkko-koulutuskurssit eivät itsessään ole kovinkaan vaikuttavia, vaan niillä lisätään enemmänkin henkilöstön tietoisuutta sekä ohjeiden olemassa olosta, sijainnista että oikeista toimintatavoista. Koulutusten

vaikuttavuutta luodaan ja parannetaan muilla koulutuksia tukevilla ja liittyvillä toimenpiteillä kuten esimerkiksi tuottamalla henkilöstölle mahdollisuuksia harjoitella koulutettua toimintatapaa säännöllisesti. Simuloitujen kalastelusähköpostiviestien tunnistaminen oikeiden sähköpostiviestien joukosta on esimerkki tällaisesta. Molemmissa haastatelluissa yrityksissä oli käytössä edellä kuvatun mukainen pelillistetty tietoturvahyökkäyksiä simuloiva järjestelmä. Haastateltujen mukaan vaikuttavuus henkilöstön toimintaan on ollut suuri ja että ko. koulutus on ollut hyvin suosittu ja pidetty henkilöstön keskuudessa. Ko. järjestelmä mahdollistaa myös yrityksille henkilöstön osaamisen kehittymisen seurannan. Lisäksi loppukäyttäjä itse pystyy seuraamaan omaa kehittymistään sekä sijoittumistaan muiden osallistuvien henkilöiden suhteen.

3.4 Tietoturvallisuuskoulutus (education)

NIST:n mukaan education-tason koulutuksen voidaan katsoa olevan tutkintoon johtavaa yliopisto- ja korkeakouluopiskelua, jonka tarkoituksena on saada tietoturvallisuudesta laajempaa ja syvällisempään osaamista sekä ymmärrystä yhdistäen sitä osaksi yleistä tietämystä ja osaamista. Useimmiten tietoturvallisuusalan ammattilaiset ja asiantuntijat sekä henkilöt, joiden työtehtävissä vaaditaan tietoturvallisuuden syvempää osaamista ja kehittämistä, osallistuvat tämän tason koulutuksiin. Education-tasolla ei opiskella tiettyjä taitoja tai osaamista kuten tehdään training-tasolla. On kuitenkin mahdollista, että tutkintoon johtavissa opinto-ohjelmissa voi suorittaa yksittäisiä kursseja, jolloin selkeä määrittely training ja education tasojen välillä voi olla vaikeaa (Wilson & Hash 2003, s. 5-6, 9, Toth & Klein 2014, s. 28).

4 Koulutuksen vaikuttavuus ja sen arviointi

4.1 Koulutuksen vaikuttavuus

Koulutuksen vaikuttavuuden määrittely koetaan usein organisaatioissa vaikeaksi ja haasteelliseksi. Raivolan (2000, s. 195) mukaan koulutuksen vaikuttavuudella tarkoitetaan koulutukselle asetettujen tavoitteiden ja tehtävien täyttymistä. Tietoturvallisuuskoulutusten osalta tavoitteiden ja tehtävien asetanta vaihtelee. Usein yleisenä tavoitteena on vain henkilöstön käyttäytymisen muutos mutta organisaatio ei mieti lainkaan tarkempia tavoitteita tai tarvittavia mittareita. Hyvin usein koulutuksia järjestetään, koska niitä pitää järjestää eikä niiden vaikuttavuutta pyritä edes mittaamaan. Organisaatio saattaa seurata koulutusten suorittaneiden henkilöiden lukumäärää mutta ei mitään muuta. Näin toimimalla saadaan täytettyä ns. compliance-vaatimus (vaatimus, että henkilöstöä on koulutettava) mutta sillä ei vielä pystytä mitenkään arvioimaan vaikuttavuutta henkilöstön toimintaan.

4.2 Koulutuksen arviointi

Arvioinnilla tarkoitetaan tarkastelun kohteen analysointia ja sen tuottaman hyödyn tai arvon selvittämistä ja määrittämistä. Saatu hyöty voi olla sekä yksilölle itselleen tai organisaatiolle. Koulutuksen arvioinnin kohteena voivat olla esimerkiksi osallistujien tyytyväisyys tai koulutuksen vaikuttavuus (Frisk 2006, s. 3). Organisaatiot arvioivat koulutuksiaan, koska koulutuksia halutaan kehittää, maksimoida opitun asian siirtymistä käytäntöön ja edelleen organisaation toimintaan. Halutaan osoittaa organisaation saama hyöty koulutuksesta (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 5).

Arviointi on otettava mukaan jo koulutuksen suunnitteluvaiheessa koulutusten tulosten ja vaikutusten tarkasteluun. Suunnitteluvaiheessa tulisi jo miettiä, mihin arvioinnin tuloksia käytetään ja miten arviointia eri vaiheissa suorite-

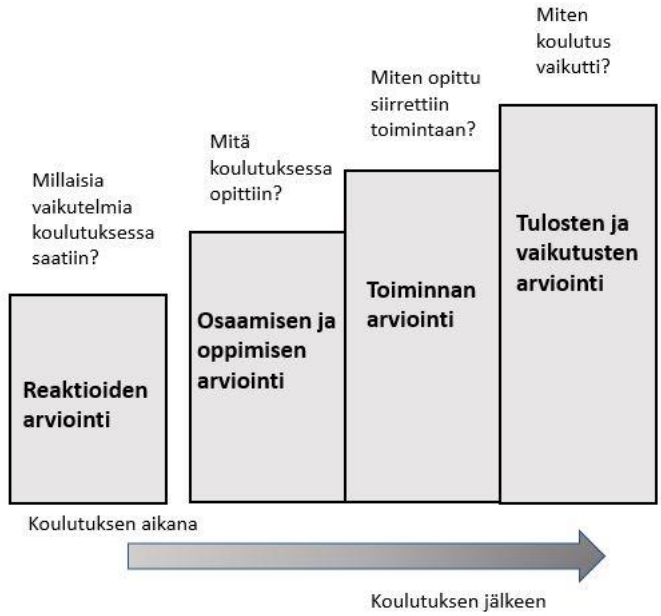
taan. Näin arviointi hyödyttää parhaiten koulutusten kehittämistä ja päätöksentekoa. Koulutuksen loppuvaiheessa tehtävät arvioinnit eivät yksinään riitä, vaan arviointipisteitä pitää olla koko koulutuksen ajan (Frisk 2006, s. 7). Lisäksi arviointia pitää tapahtua useammalla tasolla: yksilötasolla tiedon ja asenteiden muutokset sekä muutosten vaikutukset käyttäytymiseen työssä ja koko organisaatioon, eli organisaatiotason muutokset (Viitala 2013). Koulutuksen eri osa-alueiden arviointia varten on oltava tiedossa niiden tavoitteet ja lähtötilanteet, joita vasten muutoksia arvioidaan (Wilson & Hash 2003, s. 50). Lisäksi on hyvin tärkeää, että arvioinnista saaduilla havainnoilla ja palautteilla on kytkös koulutuksen kehittämiseen esimerkiksi koulutusmateriaaleihin ja koulutusmenetelmiin (Wilson & Hash 2003, s. 51-52).

Donald Kirkpatrick kehitti 1950-luvulla koulutuksen vaikutusten arviointiin mallin, joka perustuu arviointitasoihin. Mallia on käytetty hyvin laajasti vuosikymmenten ajan. Vuonna 2016 julkaistiin päivitetty arviointimalli, The New World Kirkpatrick Model. Uusi arviointimalli huomioi työympäristössä ja oppimisessa tapahtuneet muutokset kuten esimerkiksi tietokoneiden käytön lisääntymisen ja työssä oppimisen. Lisäksi arviointitasojen järjestystä itse arvioinnissa muutettiin (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 9-11).

Kirkapatrickin malli pohjautuu neljään arviointitasoon:

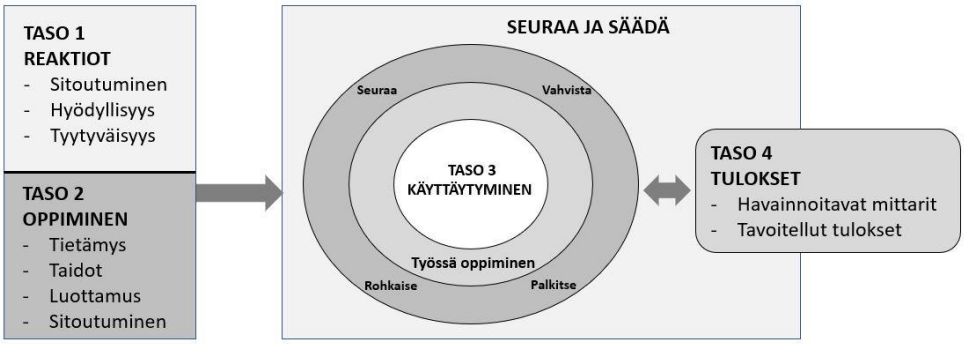
- Taso 1 – Reaktiot
- Taso 2 – Oppiminen
- Taso 3 – Käyttäytyminen
- Taso 4 – Tulokset

Arviointitasot ja niiden tavoitteet on kuvattu kuvassa 5 (Frisk 2005).



Kuva 5 Vaikuttavuuden arvioinnin tasot ja niiden tavoitteet

Uudessa Kirkpatrickin mallissa (kuva 6) arvioinnin tasot ovat edelleen samoja mutta niiden esitystapaa on muutettu. Uudella mallilla pyritään muuttamaan käsitystä, että tasoja 3 ja 4 olisi liian kallista tai vaikeaa toteuttaa. Lisäksi pyritään pienentämään tasojen 1 ja 2 liian suureksi tulkittua merkitystä arvioinnissa (Kirkpatrick J. & Kayser Kirkpatrick 2016, s 11).



Kuva 6 Uusi Kirkpatrickin arviointimalli (Kirkpatrick J. & Kayser Kirkpatrick 2016)

4.2.1 Taso 1 – Reaktiot

Reaktioiden arviointia on verrattu asiakastyytyväisyyden mittaamiseen eli miten tyytyväisiä koulutukseen osallistujat ovat koulutukseen (Kirkpatrick D. & Kirkpatrick J. 2006, s. 21). Tyytyväisyys tai tyytymättömyys koulutukseen muodostuu sekä siitä, miten hyödyllisenä koulutusta pidettiin ja siitä, miten

tyytyväisiä koulutuksen osatekijöihin ja koulutuksen toteutukseen kokonaisuudessaan ollaan (Kirkpatrick J. & Kayser Kirkpatrick 2016, 40-41). Friskin (2005, s 16) mukaan reaktioiden arvioinnilla kerään tietoa käytännössä seuraavista asioista:

- osallistujien tyytyväisyys koulutuksen toteutukseen
- osallistujien tyytyväisyys koulutuksen käytännön järjestelyihin ja ulkoisiin puitteisiin
- osallistujien ja muiden osapuolten (esim. esimiehet) näkemykset koulutuksen hyödyllisyydestä ja tarpeellisuudesta.

Kirkpatrick (Kirkpatrick D. & Kirkpatrick J. 2006, s. 28) on esittänyt reaktioiden arvioinnin periaatteet:.

- Määrittele mitä halutaan selvittää.
- Suunnittele missä muodossa reaktiot kerätään ja mitataan.
- Rohkaise osallistujia kirjalliseen palautteeseen ja sekä antamaan kehitysehdotuksia.
- Pyri saamaan kaikilta osallistujilta palaute heti koulutuksen jälkeen.
- Pyri saamaan osallistujien todelliset palautteet.
- Määrittele saadun palautteen perusteella minimitaso koulutukselle.
- Arvioi reaktioita suhteessa standardeihin ja toteuta tarvittavat kehittämistoimenpiteet.
- Kommunikoi saaduista reaktioista asianmukaisesti.

Koulutuksen kesto vaikuttaa reaktioiden keräämiseen ja arviointiin. Pitkäkestoisissa koulutuksissa reaktioiden arviointia on hyvä tehdä koulutuksen aikana. Tällöin saatua tietoa voidaan hyödyntää jo käynnissä olevan koulutuksen kehittämiseksi. Lyhytkestoisten koulutusten arviointi kerätään yleensä koulutuksen lopussa (Frisk 2005, s. 18). Tärkeää on, että välitön palaute saataisiin kaikilta osallistujilta (Kirkpatrick D. & Kirkpatrick J., s. 35). Reaktioiden arvioinnissa käytettäviä menetelmiä voivat Friskin (2005, s. 18) mukaan olla kyselylomakkeet, koulutustilanteen havainnointi ja keskustelut.

Reaktioiden arvioinnin tulosten perusteella organisaatio pystyy kehittämään koulutusta tarkoituksenmukaisemmiksi. Näin osallistujien saama hyöty koulutuksesta on parempaa. Lisäksi saadaan lisätietoa tulevien koulutusten suunnitteluun ja kehittämiseen (Frisk 2005, s. 11).

Koulutuksen tavoitteena tulee olla positiivisten reaktioiden tuottaminen osallistujille, koska tällöin osallistujat ovat on todennäköisesti motivoituneempia oppimaan. Itse oppimista positiiviset reaktiot eivät kuitenkaan takaa, mutta ne toimivat hyvänä edellytyksenä oppimiselle (Kirkpatrick D. & Kirkpatrick

J. 2006, s.22). Positiiviset reaktiot eivät myöskään takaa opittujen asioiden siirtymistä käytäntöön tai koulutuksen vaikuttavuutta yksilöön tai organisaatioon. Reaktioiden arvioinnissa on huomioitava, että negatiiviset reaktiot eivät välttämättä kerro koulutuksen tuloksen huonoudesta (Frisk 2005, s. 14).

Ennen koulutusta voidaan selvittää osallistujien odotukset ja tarpeet koulutukselle. Saadun tiedon perusteella koulutusta pystytään muokkaamaan paremmin odotuksia ja tarpeita vastaavaksi. Tämä taas parantaa koulutuksen hyödyllisyyden tunnetta (Frisk 2005, s. 16).

4.2.2 Taso 2 - Oppiminen

Kirkpatrickin mukaan (Kirkpatrick J. & Kayser Kirkpatrick 2016, s 42) taso 2, oppiminen, muodostuu viidestä oppimiseen liittyvästä elementistä: tietämys, taidot, asenne, luottamus ja sitoutuminen. Elementtien toteutumista koulutuksessa on arvioitava, koska jokainen elementti vaikuttaa siihen, miten hyvin koulutukseen osallistujat oppivat. Osaamisen arvioinnilla organisaatio saa vastaukset seuraaviin kysymyksiin:

- Mitä tietoja on opittu?
- Mitä taitoja on opittu tai parannettu?
- Mitä asenteita on muutettu?

Oppimisen arvioinnilla on merkitystä koko koulutuksen vaikuttavuuden arvioinnissa. Jos nimittäin yhtäkään edellä mainituista koulutustavoitteista ei ole saavutettu, ei ole oletettavaa, että henkilön käyttäytyminenkään (taso 3) olisi muuttunut (Kirkpatrick D. & Kirkpatrick J. 2006, s. 42, 45).

Friskin (2005, s. 22) mukaan oppimisen arvioinnilla on toteava ja suunnittelua (diagnostinen) ja oppimista (formatiivinen) ohjaava sekä kokoava ja ennustava (summatiivinen) tehtävä.

Diagnostisessa arvioinnissa tehdään tilannekartoitus koulutukseen osallistujien osaamisen lähtötasosta, odotuksista ja kokemuksista. Arviointia tehdään, jotta kouluttaja pystyisi suuntaamaan koulutusta paremmin osallistujien mukaisesti. Lisäksi oppija itse saa tietoa omien oppimistavoitteidensa määrittelyä varten. Arviointimenetelminä voidaan käyttää esimerkiksi itsearviointia, kyselyä tai ennakkotehtäviä (Frisk 2005, s. 22-26) Kirkpatrickin uuden mallin mukaan koulutukseen tulisi sisällyttää erilaisia aktiviteetteja, jotka testaavat

osallistujien osaamista sen sijaan, että osaamista testattaisiin ennen ja jälkeen koulutuksen (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 44).

Formaalin arvioinnin tehtävänä on seurata osallistujien oppimisen edistymistä koulutuksen aikana ja sen eri vaiheissa. Seuraaminen toteutetaan etukäteen suunniteltujen tarkastuspisteiden ja määriteltyjen seurantatapojen avulla. Menetelminä oppimisen edistymisen seurannassa ovat Friskin (2005, s.22-26) mukaan mm. havainnointi, tehtävät, keskustelut ja haastattelut. Lisäksi voidaan käyttää osaamista mittaavia tenttejä ja testejä, simulointia sekä roolipelejä ((Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 43).

Summatiivinen arviointi toteutetaan koulutuksen lopussa ja sen avulla kootaan oppimistulokset. Tarkoituksena on arvioida miten oppimistulokset saavutettiin, opittiinko jotain muuta ja miten jatketaan tästä eteenpäin. Menetelminä voidaan käyttää mm. yksilö- ja ryhmähaastatteluja, osaamista mittaavia testejä ja tenttejä (suullinen/kirjallinen), esitelmiä, osaamisen näyttöjä, kyselyitä, keskusteluja ja päättötyötä (Frisk 2005, s. 22-26, Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 43).

Tasoon 2 sisältyvien elementtien arviointia voidaan toteuttaa samanaikaisesti jopa samoilla arviointimenetelmillä. Organisaation on hyvä suunnitella arvioinnit ja niiden toteuttaminen etukäteen, jolloin ne voidaan toteuttaa halutulla tasolla ja mahdollisimman tehokkaasti (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 44).

Kirkpatrickin suuntaviivat oppimisen arvioinnille (Kirkpatrick D. & Kirkpatrick J. 2006, s. 43)

- Mikäli mahdollista, käytä verrokkiryhmää, joka ei ole saanut vastaavaa koulutusta.
- Arvioi osaamista, taitoja ja tietoja sekä asennetta ennen ja jälkeen koulutuksen.
- Käytä ”kynä- ja paperi-muotoista" testiä osaamisen ja asenteiden arviointiin.
- Käytä taitojen arvioinnissa taitoa mittaavaa testiä esim. näyttökoetta.
- Pyri saamaan palautteet kaikilta osallistujilta.
- Hyödynnä arvioinnin tuloksia jatkokehityksessä.

4.2.3 Taso 3 – Käyttäytyminen

Käyttäytymisen arvioinnin tarkoituksena on selvittää, miten koulutus on muuttanut toimintaa organisaatiossa koulutuksen jälkeen eli arvioinnin avulla käyttäytymisen muutos tehdään näkyväksi (Kirkpatrick J. & Kayser Kirkpatrick 2016, 50-56). Frisk (2005) käyttää tasosta kuvaavasti nimeä ”Toiminnan muuttuminen”. Käyttäytymisen muutos ei välttämättä näy heti koulutuksen jälkeen. Organisaation onkin mietittävä missä vaiheessa ja miten käyttäytymisen muutosta arvioidaan (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 52- 53).

Käyttäytymisen muutoksen arviointi ei ole suoraviivaista ja helppoa, koska on huomioitava, että halutun muutoksen toteutumiseen vaikuttaa moni tekijä. Muutokseen vaikuttavia tekijöitä ovat Friskin (2005, s. 29) mukaan

- koulutukseen ja opetukseen liittyvät tekijät,
- yksilölliset tekijät
- esimiehen toiminta
- ohjaus ja tuki
- organisaatiota koskevat tekijät
- välineet, laitteet ja materiaali.

Kirkpatrick nostaa esiin koulutuksen jälkeisen tuen käyttäytymisen muutokseen. Siinä keskeinen käsite on kriittinen käyttäytyminen (critical behaviour) sekä sitä tukevat ja valvovat toiminnot ja prosessit (drivers). Kriittisellä käyttäytymisellä tarkoitetaan käyttäytymistä, joka on oleellinen tason 4 tulosten saavuttamisessa. Käyttäytymisen tulee olla selkeä ja määritelty, havainnoitavissa ja mitattavissa oleva. Kriittisen käyttäytymisen toteutuminen mahdollistetaan ja sitä tuetaan ja valvontaan tietyillä toiminnoilla ja prosesseilla. Nämä vahvistavat, valvovat, rohkaisevat ja palkitsevat kriittisen käyttäytymisen toteuttaminen työtehtävissä (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 50-56).

Frisk (2005, s. 28) nostaa esiin muutamia kysymyksiä, joiden avulla kouluttaja voi parantaa koulutuksen vaikuttavuutta:

- Millaista tukea ja ohjausta koulutettavat tarvitsevat koulutuksen jälkeen työpaikallaan, jotta käyttäytyminen muuttuisi?
- Mikä estää ja haittaa osallistujia käyttämästä koulutuksessa opittua osaamista?

Organisaation on siis tunnistettava kriittinen käyttäytyminen, määriteltävä sitä tukevat ja valvovat toiminteet ja prosessit sekä suunniteltava, miten niitä arvioidaan. Vasta sitten käyttäytymisen arviointia voidaan toteuttaa. Lisäksi parantaakseen koulutuksen vaikuttavuutta organisaation on tunnistettava haluttua muutosta haittaavat tekijät ja pyrittävä pienentämään tai poistamaan niitä (Kirkpatrick J. & Kayser Kirkpatrick 2016, 50-56).

Koulutuksen aikana kouluttaja voi arvioida käyttäytymisen muutosta esimerkiksi opetusmenetelmien valinnalla sekä soveltavilla etätehtävillä. Opittujen asioiden soveltamista ja siirtymistä käytäntöön edistää, että oppimistilanteet ja -tehtävät ovat mahdollisimman samanlaisia kuin itse työtehtävissä. Lisäksi siirtymistä käytäntöön tuetaan sillä, että työympäristössä on mahdollista soveltaa ja harjoitella opittua asiaa (Kirkpatrick J. & Kayser Kirkpatrick 2016, 30-31).

Kirkpatrickin suuntaviivat käyttäytymisen arvioinnille (Kirkpatrick D. & Kirkpatrick J. 2006, s. 53)

- Mikäli mahdollista, käytä verrokkiryhmää, joka ei ole saanut vastaavaa koulutusta.
- Anna aikaa käyttäytymisen muutoksen toteutumiselle.
- Mikäli mahdollista, arvioi käyttäytymistä ennen ja jälkeen koulutuksen.
- Tee kysely/haastattele ainakin yhtä seuraavista: koulutettavat, koulutettavien esimiehet, alaiset, muut, jotka havannoivat koulutettavien käyttäytymistä.
- Pyri saamaan palautteet kaikilta osallistujilta.
- Toista arviointi sopivan ajan kuluttua.
- Tee käyttäytymisen arvioinnin kustannus-hyötyanalyysi.

Frisk (2005, s. 30-35) on kuvannut Kirkapatrickin mukaan arviointien suoritustavat:

1. Toimintaa arvioidaan ennen ja jälkeen koulutuksen.
2. Valitaan kontrolliryhmä tulosten vertailua varten.
3. Arvioidaan käyttäytymistä koulutuksen jälkeen eri osapuolten käsitysten mukaan.

Käytettävä arviointimenetelmä määräytyy arvioinnin suoritustavan perusteella. Jos käytössä on tietoa toiminnasta ennen koulutusta ja koulutuksen jälkeen, arviointia voidaan tehdä saman koulutusryhmällä tai käyttää verrokki-

ryhmää. Tällöin arviointimenetelminä voivat olla esimerkiksi soveltuvat tehtävät, toiminnan havainnointi (näytöt) ja osaamiskartoitukset (Frisk 2005, s. 35).

Käyttäytymisen arviointia eri osapuolten käsitysten mukaan voidaan toteuttaa esimerkiksi selvittämällä koulutukseen osallistuneiden, heidän esimiestensä ja työkavereidensa tai asiakkaiden käsityksiä. Menetelminä voidaan käyttää kyselyitä, haastatteluja, havainnointia tai keskusteluja (Frisk 2005, s. 36).

4.2.4 Taso 4 – Tulokset

Tulosten arvioinnin tarkoituksena on arvioida koulutuksen vaikutusta organisaatioon ja sen toimintaan sekä arvioida, millaista hyötyä organisaatio on koulutuksesta saanut. Tulokset voivat näkyä vasta pitkän ajan kuluttua. Kaikkien koulutusten tavoitteena on vaikuttaa jollakin tavalla toimintaan ja sitä kautta organisaation liiketoimintaan. Organisaation on kuitenkin hyvä saada tietoa tulosten saavuttamisen tilasta. Tämän mahdollistaa kriittiseen käyttäytymiseen liittyvät havainnoitavat asiat tai mittarit (leading indicators), jotka voidaan jakaa organisaation sisäisiin ja ulkoisiin. Sisäisiä havainnoitavat asioita voivat olla esimerkiksi laatupoikkeamat ja turvallisuushavainnot. Ulkoisia ovat esimerkiksi asiakaspalautteet, tunnustukset ja uudet asiakkaat (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 60-63). Vaikutusten arvioinnissa on kuitenkin eroteltava koulutusten tulokset kuten koulutukseen osallistuneiden henkilöiden lukumäärä koulutusten vaikutuksista (esim. asiakaspalautteiden määrä koulutusten jälkeen) (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 5).

Suuntaviivat tulosten arvioinnille (Kirkpatrick D. & Kirkpatrick J. 2006, s. 65):

- Mikäli mahdollista, käytä verrokkiryhmää, joka ei ole saanut vastaavaa koulutusta.
- Anna aikaa tulosten näkyväksi tulolle.
- Mikäli mahdollista, arvioi tuloksia ennen ja jälkeen koulutuksen.
- Toista arviointi sopivan ajan kuluttua.
- Tee arvioinnin kustannus-hyötyanalyysi.
- Ole tyytyväinen koulutustuloksiin, vaikka numeraalista näyttöä ei tuloksista olisi käytettävissä.

4.2.5 Koulutuksen arvioinnin suunnittelu ja toteuttaminen

Koulutuksen arvioinnin suunnittelua ja toteuttamista ei voida Kirkpatrickin mukaan suorittaa tehokkaasti koulutuksen jälkeen. Koulutuksen arvioinnin eri tasot ja arvioinneissa käytettävät menetelmät on huomioitava jo koulutuksen suunnitteluvaiheessa ja niitä pitää toteuttaa kaikissa koulutuksen vaiheissa prosessinomaisesti ja osittain jopa samanaikaisesti. Samaa arviointityökalua ei pidä käyttää kaikissa koulutuksissa vaan käytettävää työkalua pitää muokata arvioitavan koulutuksen mukaan. Muokkauksen pohjana on tieto, jota arvioitavasta koulutuksesta halutaan saada. Koulutuksen hyöty organisaatioille saavutetaan yleensä toiminnan muutoksen kautta. Koulutuksella tavoitellaan jotakin muutosta/vaikutusta, joka hyödyttää organisaatiota (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 96, s. 122).

Koulutuksen ja sen arvioinnin suunnittelun pitäisi alkaa Tulokset-tasolta (taso 4). Tämän jälkeen edetään suunnittelussa tasojen kolme ja kaksi kautta tasolle 1. Toimimalla näin organisaatio varmistuu jo koulutuksen suunnitteluvaiheessa, että suunniteltavalla koulutuksella on kytkös organisaation päämäärään ja toimintaan. Organisaatio on tunnistanut havainnoitavat asiat ja mittarit, joista saadaan tietoa tavoitteen saavuttamisen tilasta. Organisaatio on tunnistanut kriittisen käyttäytymisen ja toimenpiteet, joilla sen toteutumista työpaikalla tuetaan ja valvotaan. Organisaatio on tietoinen siitä, mitä tietoja, taitoja ja asenteita kriittinen käyttäytyminen edellyttää ja mitä koulutustarpeita siihen organisaatiossa liittyy (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 22-26, Wilson & Hash 2003, s. 2, 11, 16, 42).

Huomioimalla koulutuksen arvioinnin toteutus jo koulutuksen suunnitteluvaiheessa voidaan käytettävissä arviointimenetelmissä toteuttaa eri tasojen aihealueet laajemmin ja suunnitelmallisemmin. Lisäksi voidaan suunnitella myös koulutuksen jälkeen pidemmän ajanjakson jälkeen toteutettava arviointi, eli ns. viivästetty arviointi. Saatavat tulokset hyödyttävät organisaatiota paremmin kuin ainoastaan tiettyyn tasoon liittyvät arvioinnit (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 28).

Koulutuksien pituudet vaihtelevat lyhyistä, yksittäisistä koulutustilaisuuksista pitkäkestoisiin koulutusohjelmiin. Koulutuksen arviointia ei pidä jättää toteutettavaksi ainoastaan koko koulutusohjelman päättymisen jälkeen vaan arviointia on hyvä suorittaa koulutuksen aikana. Tällöin voidaan toteuttaa

kenties tarvittavia toimenpiteitä koulutuksen vaikuttavuuden parantamiseksi (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 126).

Kirkpatrikin mukaan arviointimenetelmistä kyselyt ja yksilö- ja ryhmähaastattelut sopivat kaikkien tasojen (tasot 1- 4) arvioimiseen. Tällöin eri tasoja voidaan myös arvioida samanaikaisesti samalla työkalulla (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 96).

4.2.6 Arviointien tulosten analysointi ja jatkotoimet

Koulutuksen arvioinnista saatavan tiedon analysoinnissa on Kirkpatrikin mukaan ensimmäiseksi selvitettävä, täyttyvätkö koulutuksen eri tasoille asetetut odotukset. Jos asetetut vaatimukset eivät ole täyttyneet, selvitetään syyt tähän sekä tunnistetaan mahdolliset korjaavat toimet ja toteutetaan ne. Jos taas odotukset ovat täyttyneet tai jopa ylittyneet, selvitetään vastaavasti syyt tähän. Olemalla tietoisia onnistumisen syistä organisaatio pystyy ylläpitämään ja parantamaan koulutusta (Kirkpatrick J. & Kayser Kirkpatrick 2016, luku 12, s. 122).

Tulosten analysoinnissa on hyvä huomioida, että Kirkpatrikin mukaan koulutusten arviointien tulokset ovat ennalta arvattavissa: suurin osa koulutettavista toteuttaa työssään pieniä, minimaalisia muutoksia ja loppujen lopuksi jatkavat työssään kuten ennenkin. Hyvin pieni osa toteuttaa suuria muutoksia koulutusten vuoksi. Lisäksi Kirkpatrikin mukaan koulutukset eivät yksinään ole riittäviä toimenpiteitä, koska aina on olemassa tekijöitä, jotka estävät koulutuksen haluttua vaikutusta. Nämä tekijät ovat usein koulutuksesta johtumattomia kuten koulutuksen ajankohta tai mahdollisuus testata koulutettuja asioita. Koulutuksesta johtumattomat syyt vaikuttavat Kirkpatrikin mukaan eniten koulutuksen onnistumiseen tai epäonnistumiseen (Kirkpatrick J. & Kayser Kirkpatrick 2016, s. 128-132).

5 Tietoturvallisuuskoulutuksen vaikuttavuuden arviointi käytännössä

Lopputyön empiirisen osion tarkoituksena on kuvata vaiheet, joiden kautta organisaatio pystyy suunnitelmallisesti toteuttamaan tietoturvallisuuskoulutuksen vaikuttavuuden arviointia. Tietoturvallisuuskoulutuksen vaikuttavuuden arvioinnin toteutus kuvataan kahden tietoturvallisuuskoulutuksen avulla. On huomioitava, että tietoturvallisuuskoulutukset vaihtelevat hyvin paljon esimerkiksi tavoitteiden, laajuuden, sisällön, keston, kohderyhmän sekä toteutustavan osalta. Haastelluissa yrityksissä esimerkiksi on käytössä erilaisia koulutuksia: koko henkilöstölle, esimiehille, asiakkaille sekä toimittajille suunnattuja koulutuksia. Kuten teoriaosuudessa on todettu, yksi yleinen arviointimalli ei sovellu kaikkiin koulutuksiin vaan mallia on aina muokattava koulutuksen mukaan. Tämän vuoksi lopputyössä käytetään esimerkkinä kahta kuvitteellista tietoturvallisuuskoulutusta, joiden vaikutusten arviointiin luodaan soveltuvat mallit. Empiria osassa ei oteta kantaa tietoturvallisuuskoulutusten sisältöön syvällisesti vaan keskitytään vaikuttavuuden arviointiin. Koulutuksia käsitellään irrallisina koulutustilaisuuksina eikä osana suunniteltua tietoturvallisuustietoisuusohjelmaa tai -kampanjaa. Käytännössä kuitenkin näin ei välttämättä ole. Haastatelluissa yrityksissä tietoturvallisuuskoulutukset ja niitä tukevat muut toimenpiteet suunniteltiin etukäteen, ns. vuosikelloajattelun mukaisesti.

Esimerkkikoulutukset ovat:

1. Esimerkkikoulutus 1: koko henkilöstölle suunnattu verkkopohjainen itseopiskeltava yleinen tietoturvallisuuskoulutus. Koulutus sisältää osa-alueet ovat:

- Tietoturvallisuuden perusteet
- Tietoturvallisuus toimistolla
- Tietoturvallisuus etätöissä
- Tietoturvallisuustapahtumien ja - poikkeamien tunnistaminen
- Toiminta tietoturvallisuustapahtumassa

2. Esimerkkikoulutus 2: tiedostojen salausohjelmiston käyttökoulutus yksittäisille henkilöille, jotka tarvitsevat ohjelmistoa työtehtävissään. Tällaisia henkilöitä ovat projektipäälliköt ja suunnittelijat. Koulutus toteutetaan verkkokoulutukseen soveltuvalla ohjelmistolla (esimerkiksi Teams, Zoom) kouluttajan johdolla.

5.1 Vaihe 1 – tietoturvallisuuskoulutuksen suunnittelu

Tietoturvallisuuskoulutuksen vaikuttavuuden arvioinnin luominen käynnistyy koulutuksen suunnittelun yhteydessä. Etukäteen on suunniteltava kaikissa vaiheissa (vaiheet 1- 5) toteutettavat arviointiin liittyvät toimenpiteet. Organisaatio määrittelee koulutuksen tavoitteet ja päämäärät sekä sen, miten koulutus liittyy organisaation toimintaan. Lisäksi on määriteltävä mittarit, joilla tavoitteiden saavuttamista voidaan mitata. Tietoturvallisuuskoulutuksissa on yleensä tavoitteena saada aikaan käyttäytymisen muutosta henkilöstössä. Muutoksen toteutuminen kuitenkin vaatii aikaa, samoin kuin sen mittaaminenkin. Vaiheessa 4. toteutettavia ns. myöhästettyjä arviointeja voidaan toteuttaa useampiakin. Oleellista on, että kaikkien vaiheiden toimenpiteet suunnitellaan jo koulutuksen suunnitteluvaiheessa.

Esimerkkikoulutus 1

Esimerkkikoulutuksessa 1 on tavoitteena yleisen tietoturvallisuustietoisuuden lisääminen sekä henkilöstön uhkatietoisuuden lisääminen. Tarkemmat tavoitteet ja niiden mittarit on kuvattu taulukossa 1.

Taulukko 1 Koulutuksen tavoitteet ja niiden mittarit.

Tavoitteet	**Mittarit**
Henkilöstö tunnistaa oman roolinsa tietoturvallisuuden toteutumisessa.	Henkilöstöltä saatu palaute ja kysymykset.
Henkilöstö osaa etätyöskentelyn periaatteet.	Henkilöstöltä saatu palaute ja kysymykset.
Henkilöstö tunnistaa tietoturvallisuushavainnot.	Ilmoitettujen tietoturvallisuushavaintojen lukumäärä.
Henkilöstö tietää miten toimia havaitessaan tietoturvallisuustapahtuman.	Henkilöstöltä saatu palaute ja kysymykset.
Henkilöstö tietää mistä tietoturvaohjeet löytyvät.	Henkilöstöltä saatu palaute ja kysymykset.

Esimerkkikoulutus 2

Esimerkkikoulutus 2:n konkreettinen tavoite on opettaa valitun salausohjelmiston käyttö ja varmistaa, että henkilöt käyttävät sitä kuten on tarkoitettu. Mittareina tavoitteen saavuttamisessa ovat henkilöstöltä saatu palaute sekä saadut havainnot toiminnasta kuten asiakkailta saadut palautteet.

5.2 Vaihe 2 – nykytilanteen kartoitus

Jotta koulutuksen vaikuttavuutta voidaan arvioida, organisaation on tiedettävä henkilöstön tietoturvallisuuden osaamisen tila keskeisimmiksi tunnistettujen tavoitteiden osalta tällä hetkellä. Jos nykytila ei ole tiedossa, se pitää selvittää nykytilanteen kartoituksella. Kartoituksen toteuttamiseen voidaan käyttää useita eri menetelmiä kuten haastatteluja tai kyselylomakkeita.

Esimerkkikoulutus 1

Organisaatiolla ei ole luotettavasti tiedossa henkilöstönsä tietoturvallisuuden osaamisen nykytilaa. Tämän vuoksi toteutetaan nykytilanteen kartoitus. Esimerkkikoulutus 1:n nykytilanteen kartoituskyselyssä on huomioita kaikki koulutuksen osa-alueet. Ne voidaan tehdä esimerkiksi seuraavin kysymyksin

- Tiedän mitä tarkoitetaan tietoturvallisuudella organisaatiossani.
- Tiedän miten toimia tietoturvallisesti työssäni.
- Tiedän miten toimia tietoturvallisesti etätöissä.
- Tunnistan tietoturvallisuustapahtumat.
- Tiedän miten toimia havaitessani tietoturvallisuustapahtuman.
- Tiedän mistä löydän organisaation tietoturvallisuusohjeistuksen.

Esimerkkikoulutus 1:n nykytilanteen kartoituskysely suunnataan koko henkilöstölle ja se julkaistaan kyselypalvelussa. Kartoitus toteutetaan muutama kuukausi ennen itse koulutuksen toteuttamista. Näin kartoituksen tuloksia voidaan vielä mahdollisesti hyödyntää koulutuksen sisältöjen luomisessa.

Esimerkkikoulutus 2

Organisaatiolla on tiedossa aikaisemmin saatujen havaintojen kautta, että henkilöstö kokee salausohjelmistojen käytön hankalaksi eikä välttämättä tunnista tilanteita, jolloin sitä tulisi käyttää. Havaintoja on saatu asiakaspalautteina sekä henkilöstöltä tulleista kysymyksistä. Organisaatio haluaa vielä var-

mentaa saadun käsityksensä ja toteuttaa nykytilanteen kartoituksen koulutuksen tunnistetulta kohderyhmältä. Esimerkkikoulutus 2:n osalta lähtötilanteen kartoitus toteutetaan pienimuotoisemmin kuin esimerkkikoulutus 1:n vastaava kysely. Lähtötilanteen kartoitus toteutetaan kyselypalvelussa, jonne kaikille osallistujille lähetetään linkki sähköpostilla.

Koulutuksen lähtötilanteen kartoituksen kysymykset voivat olla:

- Tunnistan organisaationi käyttöön hyväksymät salausohjelmistot.
- Tunnistan tilanteet, joissa minun tulee niitä käyttää.
- Osaan käyttää salausohjelmistoja työssäni.
- Tiedän mistä löydän niiden käyttöohjeet.

5.3 Vaihe 3– koulutuksen toteutus

Seuraavaksi organisaatiossa toteutetaan suunniteltu tietoturvallisuuskoulutus. Koulutuksen jälkeen toteutetaan koulutuksen ja sen vaikuttavuuden arviointi suunnitteluvaiheen mukaisesti.

Esimerkkikoulutus 1

Esimerkkikoulutus 1 on verkko-opetuspaketti, jonka koulutettava suorittaa itsenäisesti sopivana ajankohtana. Verkkokoulutus muodostuu eri aiheosioista. Jokaisen osion lopussa on lyhyt, aiheen osaamista mittaava kysymys- ja testiosio. Kysymyksiä on 3-5. Kysymyksiin oikein vastaaminen on edellytys seuraavaan osioon pääsemiselle. Kysymysosioiden kysymykset ja tehtävät tukevat vaiheessa 1 määriteltyjen tavoitteiden saavuttamista. Viimeisen osion jälkeen on kaikkien osa-alueiden yhteinen lopputesti. Lopputesti muodostuu 15 kysymyksestä, joista pitää saada oikein 12. Osiokohtaisten ja lopputestin kysymyksiä ja tehtäviä ei tässä lopputyössä määritellä, koska ne määräytyvät koulutusaineiston perusteella.

Lopputestin jälkeen koulutettavalta pyydetään palautetta opetuspaketista seuraavin kysymyksin:

Osaamiseen liittyvät kysymykset

- Tiedän mitä tarkoitetaan tietoturvallisuudella organisaatiossani.
- Tiedän miten toimia tietoturvallisesti työssäni.
- Tiedän miten toimia tietoturvallisesti etätöissä.
- Tunnistan tietoturvallisuustapahtumat.

- Tiedän miten toimia havaitessani tietoturvallisuustapahtuman.
- Tiedän mistä löydän organisaation tietoturvallisuusohjeistuksen.
- Aion muistuttaa työkavereitani oikeista toimintatavoista, mikäli huomaan heidän toimivan toisin.
- Miten parantaisit koulutusta?

Koulutuksen toteutukseen liittyvät kysymykset

- Koulutus paransi tietämystäni työympäristöni tietoturvariskeistä ja uhista.
- Koulutus paransi tietämystäni tietoturvallisista toimintatavoista ja käytännöistä.
- Koulutus lisäsi kykyäni toimia tietoturvallisesti työtehtävissäni.
- Koulutus lisäsi kykyäni havaita tietoturvallisuustapahtumia.
- Koulutuksen toteutus tuki oppimistani.
- Oppimateriaalia oli helppo seurata.

Esimerkkikoulutus 2

Esimerkkikoulutus 2 toteutetaan online-koulutuksena verkkokoulutukseen soveltuvalla ohjelmistolla, Teamsilla. Koulutuksen aikana osallistujilla on mahdollisuus kysyä ja keskustella kouluttajan kanssa tai kommunikoida pikaviestivälineellä. Koulutuksessa opetetaan valitun salausohjelmiston käyttö: ensin koulutetaan käyttö vaiheittain, jonka jälkeen osallistujat pääsevät harjoittelemaan ohjelmiston käyttöä itsenäisesti. Kouluttajalta on mahdollisuus kysyä tukea ja neuvoa ja koulutettava voi jakaa näyttönsä kouluttajalle. Osana koulutusta toteutetaan harjoitustehtävä, joka palautetaan koulutustilaisuuden jälkeen. Kouluttaja antaa palautteen jokaiselle henkilökohtaisesti. Harjoitustehtävässä osallistujien pitää salata tiedosto ja lähettää se kouluttajalle. Näin tuetaan opitun taidon siirtymistä käytäntöön.

Koulutustilaisuuden jälkeen osallistujille toteutetaan palautekysely osana koulutusta. Palautekyselyn sisältö voi olla:

Koulutettava aihe:

- Tunnistan organisaationi käyttöön hyväksymät salausohjelmistot.
- Tunnistan tilanteet, joissa minun tulee niitä käyttää.
- Osaan käyttää salausohjelmistoa työssäni.
- Tiedän mistä löydän salausohjelmiston käyttöohjeet.

Koulutuksen toteutukseen liittyvät kysymykset

- Koulutuksen sisältö vastasi odotuksia.

- Kouluttaja ilmaisi asiat ymmärrettävästi.
- Koulutuksen toteutus tuki oppimistani.

5.4 Vaihe 4 – koulutuksen vaikuttavuuden arviointi

Seuraavaksi organisaatio arvioi koulutuksesta saatuja tuloksia ja koulutuksen vaikuttavuutta. Arviointia voidaan suorittaa koulutuksen jälkeen sekä ns. myöhennettynä arviointina. Näin pystytään paremmin arvioimaan koulutuksen vaikutusta henkilöiden toimintaan ja asenteisiin.

Esimerkkikoulutus 1

Osana verkkokoulutusta on osiokohtaiset testikysymykset ja koulutuksen lopputestit. Niiden tuloksia tarkastelemalla saadaan selville mm. kysymykset, joihin on vastattu eniten väärin tai, kuinka monta yrityskertaa keskimäärin on vaadittu lopputestin läpäisemiseen. Lisäksi saadaan selville lopputestin läpäisseiden lukumäärä. Ko. tietojen sekä loppukyselyn koulutuksen sisältöön kohdistuvien vastausten avulla pystytään arvioimaan koulutuksen sisältöä ja kehittämään sitä. Esimerkiksi onko koulutuksessa käsitelty jotakin asiaa liian vähän, jos joku tietty kysymys vaatii useampia vastauskertoja ennen kuin se menee oikein.

Koulutuksen vaikuttavuutta voidaan arvioida osittain vertaamalla lähtötilanteen kartoituksen tuloksia koulutuksen loppukyselyn vastaaviin tuloksiin. Näin saadaan selville, onko koulutukselle asetettuja tavoitteita saavutettu, varsinkin tietoisuuden kasvun osalta. Sitä, että siirtyvätkö opitut asiat ja tiedot henkilöiden toimintaan, ei vielä tiedetä tai pystytä näillä tiedoilla arvioimaan.

Esimerkkikoulutuksessa 1 koulutettujen asioiden ja toimintatapojen siirtymistä käytäntöön voidaan arvioida pidemmällä aikavälillä vaiheessa 1 tunnistettujen mittareiden avulla. Esimerkiksi ovatko tehdyt tietoturvahavainnot lisääntyneet henkilöstön koulutuksen myötä ja ovatko henkilöstön aiheuttamat tietoturvatapahtumat vähentyneet?

Vaikutusta käyttäytymiseen voidaan arvioida myöhennettynä arviointina kyselyn avulla. Kyselyn kysymyksen voivat olla esimerkiksi:

- Olen työssäni päässyt hyödyntämään kurssilla oppimaani.
- Koulutuksessa oppimastani on ollut minulle hyötyä työssäni.

Esimerkkikoulutus 2

Vastaavalla tavalla kuin esimerkkikoulutuksen 1 arvioinnissa, voidaan esimerkkikoulutuksen 2 sisältöä arvioida koulutuksen sisältöön kohdistettujen kysymysten avulla. Lisäksi lähtötilanteen kartoituksen avulla voidaan arvioida koulutuksen vaikuttavuutta heti koulutuksen jälkeen. Myöhennetty arviointi voidaan toteuttaa kyselylomakkeen sijaan osallistujien haastattelulla osallistujien vähyyden vuoksi. Haastattelun kysymykset voisivat olla:

- Koitko koulutuksen hyödylliseksi?
- Oletko päässyt hyödyntämään oppimaasi käytännössä?
- Jos olet, miten koulutus tuki siinä?
- Jos et ole, niin mikä on ollut syynä?

6 Yhteenveto

Käsite tietoturvallisuuskoulutus on selkeä ja yksinkertainen mutta sitä tarkemmin tarkasteltaessa huomataan, että se sisältää organisaatioissa erilaisia tasoja. Ajatus siitä, että ”Yksi tietoturvallisuuskoulutus koko henkilöstölle kerran kolmessa vuodessa riittää”, ei täytä vaatimuksia organisaatioiden nykyisissä toimintaympäristöissä. Uusia tieto- ja kyberuhkia ilmaantuu jatkuvasti ja organisaatioiden henkilöstö on eturintamassa kohtaamassa näitä uhkia. Organisaation tietoturvallisuuskoulutuksen on siis oltava jatkuvaa ja suunnitelmallista sekä tehtävien mukaisesti kohdennettua. Lisäksi on huomioitava, että koulutusten vaikuttavuus osittain jopa luodaan sekä sitä parannetaan muilla koulutusta tukeville toimenpiteillä.

Tietoturvallisuuskoulutuksen tavoitteena on lisätä henkilöstön osaamista sekä tukea heidän tietoturvallisuustaitoja ja -osaamista, joita organisaatio haluaa heidän käyttävän työtehtävissään. Arvioitaessa koulutuksen vaikuttavuutta arvioidaan koulutukselle asetettujen tavoitteiden ja tehtävien täyttymistä. Koulutuksen arvioinnilla halutaan varmistaa opitun asian sisäistämistä ja siirtymistä käytäntöön sekä osoittaa sen hyötyä organisaatiolle. Myös koulutuksen kehittäminen on syy arviointien toteuttamiselle.

Jotta tietoturvallisuuskoulutuksen vaikuttavuuden arviointia pystytään toteuttamaan kattavasti, on se huomioitava koulutuksen kaikissa vaiheissa. Vaikuttavuuden arviointi on siis kiinteä osa koulutusta, ei irrallinen ja suunnittelemattomasti toteutettava toiminne. Vaikuttavuuden arviointi alkaa koulutuksen suunnitteluvaiheessa, jossa tunnistetaan koulutuksen tavoitteet, määritellään mihin arvioinnin tuloksia käytetään ja miten arviointia eri vaiheissa suoritetaan ja millä tasoilla. Arviointia on suoritettava jo koulutuksen aikana eikä ainoastaan koulutuksen jälkeen.

Koulutuksen vaikuttavuutta voidaan arvioida neljällä eri tasolla: reaktiot, oppiminen, käyttäytyminen ja tulokset. Eri tasojen arviointia voidaan suorittaa

osittain samanaikaisesti ja samoilla menetelmillä. Arvioimalla koulutusta kaikilla tasoilla organisaation on mahdollista sekä saada kattava kuva koulutuksen vaikuttavuudesta organisaatiossa että vaikuttaa koulutuksen suunnitteluun ja toteutukseen mahdollistaen entistä parempi käytännön vaikuttavuus.

Teoriassa sekä käytännössä tietoturvallisuuskoulutusten vaikuttavuuksien arviointi on monivaiheinen ja resursseja sitova prosessi, joka vaatii organisaatiolta hyvää ennakkosuunnittelua. Arviointityöstä saatavaa hyötyä organisaatiolle voi olla vaikea todentaa. Toteutettavia tietoturvallisuuskoulutuksia on organisaatiossa yleensä useita eri laajuisia ja eri kohderyhmille. Kaikkien näiden koulutusten vaikuttavuuden arviointi käytännössä ei liene mahdollista; niiden kustannukset voivat olla saatuja hyötyjä suuremmat. Organisaation onkin mietittävä ja suunniteltava etukäteen, mitä koulutuksia ja miten niiden vaikuttavuutta on tarkoituksenmukaista arvioita. Tarkoituksenmukaisuus vaihtelee organisaatioittain.

6.1 Vastaukset työn tutkimuskysymyksiin

Lopputyölle asetetut tutkimuskysymykset ovat:

1. Mitä tietoturvallisuuskoulutuksella tarkoitetaan?
2. Miten tietoturvallisuuskoulutuksen vaikuttavuutta voidaan arvioida?

Kuten lopputyön luvussa kolme on kuvattu, tietoturvallisuuskoulutuksella tarkoitetaan toimenpiteitä, joilla henkilöstölle luodaan heidän tarvitsemansa tietoturvallisuustietämys ja -osaaminen, joka vaihtelee työtehtäväkohtaisesti. Voidaankin käyttää termiä roolipohjainen tietoturvallisuuskoulutus. Luvuissa 3.1-3.4 kuvataan tarkemmin käsitettä tietoturvallisuuskoulutus ja sen suhdetta käsitteeseen tietoturvatietoisuus.

Toiseen tutkimuskysymykseen vastataan luvussa 4. Tietoturvallisuuskoulutuksen vaikuttavuutta voidaan arvioida Kirkpatrickin mallin mukaisesti neljällä eri tasolla: reaktiot, oppiminen, käyttäytyminen ja tulokset. Jokaista tasoa tarkastellaan tarkemmin alaluvuissa 4.2.1-4.2.4

7 Lähdeviitteet ja kirjallisuusluettelo

Amankwa Eric, Loock, Marianne, Kritzinger Elmarie 2014. A conceptual analysis of information security education, information security training and information security awareness definitions, The 9th International Conferense for Internet Technology and Secured Transactions (ICITST-2014), https://doi.org/10.1109/ICITST.2014.7038814.

Da Veiga, Adéle 2015. An information Security Training and Awareness approach (ISTAAP) to Instil an Information Security – Positive Culture, Proceedings of the Ninth International Symposium on Human Aspects of Information Security & Assurance (HAISA 2015), July 2015. Saatavissa: https://www.researchgate.net/publication/280532849_An_Information_Security_Training_and_Awareness_Approach_ISTAAP_to_Instil_an_Information_Security-_Positive_Culture.

Dhakal, Roshna 2018. Measuring the Effectivenes of an Information Security Training and Awareness Program, Doctoral Thesis, Charles Sturt University, Australia 2018. Saatavissa: https://researchoutput.csu.edu.au/en/publications/measuring-the-effectiveness-of-an-information-security-training-a.

Digi- ja väestötietovirasto (2023): Organisaation Digiturvakysely Raportti ja keskeiset havainnot 30.5.2023. Viitattu 20.8.2023. Saatavissa: Organisaation+digiturvakysely,+raportti+kevät+2023.pdf (dvv.fi).

European Network and Information Security Agency (ENISA). The new user’s guide: How to raise information security awareness. Viitattu 18.8.2023. Saatavissa: The new users’ guide: How to raise information security awareness (EN) — ENISA (europa.eu).

European Network and Information Security Agency (ENISA). Your guide to designing a cyber-awareness programme. Viitattu 18.8.2023. Saatavilla: https://www.enisa.europa.eu/topics/cybersecurity-education/2023-ar-in-a-box-material/cyber-awareness-program_03-online.pdf.

Frisk, Tarja 2005. Koulutuksen arviointi kouluttajan ja henkilöstön kehittäjän työssä, Educa-Instituutti Oy. Suomen Printman Oy. ISBN 952-5047-44-X.

Gumaraes, Johnny 2021. Information Security Awareness: Learning for Effectiveness. St. Thomas University. Miami Gardens, Florida. Saatavilla: https://www.proquest.com/open-view/d2a8de705479ad3be176483b13881c00/1?pq-origsite=gscholar&cbl=18750&diss=y.

ISO/IEC 27001:2022:fi. Tietoturvallisuus, kyberturvallisuus ja tietosuoja. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki: Suomen standardoimisliitto. 45 s.

Kirkpatrick Donald L, Kirkpatrick James D. 2006. Evaluating training programs: the four levels, Berrett-Koehler Publishers, Inc. San Francisco. ISBN-10:1-57675-348-4; ISBN-13: 978-1-57675-348-4.

Kirkpatrick James D, Kayser Kirkpatrick Wendy (2016), Kirkaptrick's Four Levels of Training Evaluation, ATD Press, Versa Press. USA. E-ISBN: 978-1-60728102-3.

Nykänen, Kari 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation käyttäytymiseen, Väitöskirja. Oulun yliopisto, luonnontieteellinen tiedekunta. Oulu. ISBN 978-951-42-9571-3. Saatavissa: http://urn.fi/urn:isbn:9789514295713.

Raivola, Reijo 2000. Tehoa vai laatua koulutukseen?, WSOY. Juva. ISBN: 951-0-23953-4

Sanastokeskus. TEPA-termipankki (erikoisalojen sanastojen ja sanakirjojen kokoelma). Viitattu 18.8.2023. Saatavilla: https://termipankki.fi/tepa/fi/.

SANS 2023. SANS 2023 Security awareness report Managing human risk. Viitattu: 7.10.2023. Saatavilla: https://go.sans.org/lp-wp-2023-security-awareness-report.

SFS-ISO/IEC 27003:2017. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuudenhallintajärjestelmät. Ohjeistusta. Helsinki: Suomen standardoimisliitto. 100 s.

Sydänmaanlakka, Pentti 2012. Älykäs organisaatio. Talentum Media Oy, Hansaprint Oy 2012 Vantaa. ISBN 978-952-14-1940-9.

Toth Patricia, Klein Penny 2014. A Role-Based Model for Federal Information Technology/Cybersecurity Training, NIST Special Publication 800-16 Revision 1 (3rd draft) USA 2014. Saatavilla: https://csrc.nist.gov/files/pubs/sp/800/16/r1/3pd/docs/sp800_16_rev1_3rd-draft.pdf.

Veseli, Ilirjana 2011. Measuring the Effectiveness of Information Security Awareness Program. Master's Thesis. Gjøvik University College, Department of Computer Science and Media Technology. Norway. Saatavilla: https://ntnuopen.ntnu.no/ntnu-xmlui/bitstream/handle/11250/143980/Ilirjana%20Veseli.pdf?sequence=1.

Viitala, Riitta 2013. Henkilöstöjohtaminen – Strateginen kilpailutekijä. Edita Publishing Oy 2014 Helsinki. ISBN 978-951-37-6411-1.

Viitala, Riitta 2021. Henkilöstöjohtaminen Keskeiset käsitteet, teoriat ja trendit. Edita Publishing 2021, Keuruu. ISBN 978-37-7838-5.

Vilander, Jaakko 2021. Bridging the knowing-doing-gap: the role of attitude information security awareness. Master's Thesis. University of Jyväskylä, Faculty of information technology, Jyväskylä. Saatavilla: http://urn.fi/URN:NBN:fi:jyu-202105313312.

Wilson Mark, Hash Joan 2003. Building an Information Technology Security Awareness and Training Program. NIST Special Publication 800-50, USA 2003. https://doi.org/10.6028/NIST.SP.800-50.

Wilson, Mark 1998. Information Technology Security Training Requirements: A Role- and Performance-Based Model, NIST Special Publication 800-16, USA 1998. https://doi.org/10.6028/NIST.SP.800-16.

Haastattelut:

Yritys A:n edustajan haastattelu 19.10.2023

Yritys B:n edustajien (2 henkilöä) haastattelu 17.11.2023

8 Kuvat ja taulukot