Co-funded by the European Union

PK-YRITYSTEN KYBERTURVALLISUUDEN MUUTOSAGENTIT KOULUTUS TARVITSEE KARTOITUSRAPORTIN

CYBER AGENT 10.2023

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Työpaketti 2: CyberAgent-lähestymistapa ja rakenteen suunnittelu

Tuotos 2.2: Pk-yritysten kyberturvallisuuden muutosagentit Koulutus tarvitsee kartoitusraportin

WP2:n johtaja – Olemisen Balanssia ry
Suorituksen johtaja 2.2 – Olemisen Balanssia ry

SISÄLTÖ

JOHDANTO

Tämän hankeraportin tarkoituksena on analysoida ja kartoittaa koulutustarpeita pk-yritysten kyberturvallisuuden muutosagentin edellyttämien asianmukaisten pätevyyksien määrittämiseksi. Laatimalla kattavan uudelleentarkastelun nykyisistä koulutustarjonnoista ja ymmärtämällä pk-yritysten kyberturvallisuuskysymyksiä koskevat mieltymykset tällä kertomuksella pyritään kuromaan umpeen nykyisten taitojen välistä kuilua ja määrittelemään vaadittavat ihanteelliset taidot.

Koska kyberuhat lisääntyvät kehittyneisyydessä, pk-yritysten on varmistettava, että niillä on riittävästi koulutettua henkilöstöä näiden uhkien torjumiseksi. Muutosagentit kyberturvallisuuden alalla ovat tässä yhteydessä keskeisessä asemassa. Tässä hankeraportissa analysoidaan kyberturvallisuusympäristöä eri näkökulmien kautta: Koulutus, sukupuolten tasa-arvo sekä pk-yritysten ja koululaitosten nykytilanne.

1. MENETELMÄ

Tässä kartoitusprosessissa käytimme yhdistelmälähestymistapaa, jossa yhdistettiin työpöytä- ja kenttätutkimus.

Asiakirjatutkimuksessa tehtiin kattava kirjallisuuskatsaus, jonka tarkoituksena oli:

- Tarkastellaan uudelleen nykyisiä ja kehitteillä olevia koulutussäännöksiä ammatillisen koulutuksen ja korkeakoulutuksen tasolla kyberturvallisuuden alalla kussakin kumppanimaassa. Kyberturvallisuuskoulutuksen sisältöön ja tarpeisiin liittyvien artikkelien, valkoisten kirjojen, tutkimusten ja raporttien hankkiminen ja kokoaminen.
- Analysoida ammatillisen koulutuksen ja korkeakoulutuksen kursseja, niiden opetussuunnitelmia ja niiden merkitystä todellisten kyberturvallisuushaasteiden kannalta.

Tavoitteena oli

- Yksilöidään kunkin maan ammatillisen koulutuksen ja korkeakoulutuksen tasolla tarjottavien kyberturvallisuuskurssien nykyiset opetussuunnitelman osat.
- Arvioida, miten nämä opetussuunnitelmat vastaavat kyberturvallisuushaasteita.
- Selvitetään, onko olemassa erityisiä strategioita tai ohjelmia, joilla lisätään naisten osallistumista kyberturvallisuustutkimuksiin.

Kenttätutkimuksen aikana suoritimme kaksi tutkimusta. Yksi niistä on suunniteltu opettajille ja kouluttajille sekä ammatillisen koulutuksen että korkeakoulutuksen luokista kustakin maasta, jotta voidaan ymmärtää nykyisten koulutussäännösten vivahteet. Toinen räätälöidään pk-yrityksille saadakseen käsityksen ja käsityksen yritysten tilanteesta kyberturvallisuuden osalta: Miten työntekijät osallistuvat näihin aiheisiin, haasteisiin ja tarpeisiin. Alan tutkimuksessa keskityttiin myös määrittämään ominaispiirteet, koulutustarpeet ja oppimismieltymykset, erityisesti korostamalla naisten tarpeita kyberturvallisuuden alalla.

Saimme huomattavan määrän vastauksia molempiin kyselyihin. 190 opettajaa ja kouluttajaa ammatillisesta koulutuksesta ja korkeakouluista ja 176 pk-yritysten työntekijää.

Tutkimus 1: Pk-yritysten kyberturvallisuuden muutosagenttien koulutustarpeiden kartoitus – ammatillinen **koulutus ja korkeakoulututkimus.**

Laitoksen tyyppi	**Vastauksia**	**Naaras**	**Uros**	**Mieluummin olla sanomatta**
Korkeakoulut (korkea-asteen oppilaitokset)	104	28	73	3
Ammatillinen koulutus (ammatillinen koulutus)	86	36	48	2
Yhteensä	**190**	**64**	**121**	**5**

Tutkimus 2: Pk-yritysten kyberturvallisuuden muutosagenttien koulutustarpeiden **kartoitus.**

Vastausten määrä	**Laske**
Pk-yritykset	176
Yhteensä	**176**

Kyselylomakkeet ja täydelliset tiedot löytyvät liitteestä C & D.

2. TUTKIMUS (KAIKKI KUMPPANIT)

2.1. NYKYISET KOULUTUSTA KOSKEVAT SÄÄNNÖKSET

Tässä osiossa esitellään tutkimusta ja esitetään asiakirjatutkimuksista ja kyselytutkimuksista saatuja näkemyksiä, joissa tuodaan esiin kumppanimaiden nykyisen koulutusinfrastruktuurin vahvuuksia ja puutteita.

2.1.1. VET & HEI CYBERSECURITY EDUCATION YLEISKATSAUS

Saavutimme laajan analyysin kyberturvallisuuden koulutusympäristöstä kaikissa kumppanimaissa kuvaillaksemme sen nykytilaa ja käynnistääksemme kyberturvallisuuskoulutuksen asiaankuuluvat näkökohdat.

Liettuassa AIKOS-1 tietokannasta tehty haku paljasti yhteensä kuusi Liettuan laitosten tarjoamaa virallista kyberturvallisuuskoulutusohjelmaa, jotka kattavat sekä kandidaatin että maisterin tasot:

Tutkimuksen suunta	Ohjelma	Toimielin	ECTS	Tutkinto
Tietotekninen tekniikka	Tieto- ja tietotekniikkaturvallisuus[2]	Kaunasin teknillinen yliopisto	120	Tietojenkäsittelytieteen maisteri
Johto	Kyberturvallisuuden hallinta3	Mykolas Romeris -yliopisto	90	Master of Business Management
Tietotekninen tekniikka	Tieto- ja tietotekniikkaturvallisuus[4]	Vilna Gediminasin teknillinen yliopisto	120	Tietojenkäsittelytieteen maisteri
Tietotekninen tekniikka	Tietojärjestelmät ja kyberturvallisuus[5]	Vilnan yliopisto	210	Tietojenkäsittelytieteen kandidaatti
Tietotekninen tekniikka	Tietojärjestelmien ja kyberturvallisuuden teknologiat[6]	Marijampole College	180	Tietojenkäsittelytieteen ammatillinen kandidaatti
Tietotekninen tekniikka	Kyberjärjestelmät ja turvallisuus[7]	Kaunas College	180	Tietojenkäsittelytieteen ammatillinen kandidaatti

[1] Ohjelmien hakuun käytettyjä avainsanoja olivat *kyberturvallisuus*, *turvallisuus* ja niiden muunnelmat. Lähde: https://www.aikos.smm.lt/Puslapiai/Pradinis.aspx
[2] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=8618_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[3] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2845&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[4] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=1442_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[5] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=9664&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[6] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2775&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[7] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=3797&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d

Master-tason kyberturvallisuusohjelmat ovat erillisiä mutta toisiaan täydentäviä lähestymistapoja. Kaunasin yliopisto korostaa tutkimusmenetelmiä, tietoturvamenetelmiä ja sähköisen tilan oikeudellisia näkökohtia keskittyen turvallisen IT-järjestelmän suunnittelu- ja toteutustaitojen kehittämiseen. Vilnan Gediminasin teknillinen yliopisto asettaa etusijalle asiantuntijoiden muodostamisen systemaattisella lähestymistavalla tietoturvakysymyksiin, yhdistämällä tieteellistä tietoa menetelmiin ja teknologioihin tietoturvan varmistamiseksi sekä edistämään kriittistä ajattelua ja johtajuutta. Mykolas Romeris University kuitenkin nojaa kyberturvallisuuden hallintaan, jonka tavoitteena on tuottaa asiantuntijoita, jotka ovat taitavia nykyaikaisten IT-ympäristöjen ja monimutkaisten kyberturvallisuustehtävien valvonnassa painottaen voimakkaasti strategista johtamista dynaamisissa teknologisissa yhteyksissä.

Kandidaatin tason kyberturvallisuuden opinto-ohjelmat jakavat keskeisen painopisteen tietotekniikan ja kyberturvallisuuden osaavien ammattilaisten kehittämisessä, mutta jokaisella on selkeät painotukset. Vilnan yliopiston ohjelma on suunnattu tarjoamaan kattavan perustan tietotekniikassa, keskittyen turvallisten tietojärjestelmien analysointiin, suunnitteluun, kehittämiseen ja ylläpitoon. Marijampole College, joka pyrkii myös tuottamaan päteviä tietotekniikan asiantuntijoita, korostaa vahvemmin käytännön näkökohtia, kuten tietokoneverkkojen ja -järjestelmien luomista, ylläpitoa ja hallinnointia. Kaunas College erottuu pyrkimällä valmistamaan asiantuntijoita, joilla on kykyjä paitsi kyberjärjestelmien suunnittelussa ja toteuttamisessa myös johtavissa tiimeissä, ymmärtää eettisiä, oikeudellisia ja sosiaalisia vaikutuksia ja työskennellä tehokkaasti monikulttuurisissa ympäristöissä. Vaikka kaikkien kolmen laitoksen tavoitteena on antaa opiskelijoille teknisiä taitoja kyberturvallisuuden alalla, niiden tavoitteet vaihtelevat teknisestä osaamisesta (Vilnius University), käytännön sovelluksista ja pehmeiden taitojen kehittämisestä (Marijampole College), teknisten, johtajuuden ja eettisten näkökohtien yhdistelmään (Kaunas College)

Haussa paljastui myös neljä rekisteröityä epävirallista aikuiskoulutusohjelmaa kyberturvallisuuden alalla, joista kukin keskittyy kyberhyökkäysten tunnistamiseen, tutkimiseen ja ehkäisemiseen liittyviin taitoihin, erityisesti salauksen avulla. Vaikka kaikki ohjelmat jakavat tämän ydintavoitteen, niiden lähestymistavat ja soveltamisalat eroavat toisistaan. Jotkut keskittyvät kyberturvallisuuteen ja ennaltaehkäiseviin strategioihin, kun taas toiset tarjoavat laajemman opetussuunnitelman, mukaan lukien ohjelmointi, joka kattaa muun muassa sosiaalisen suunnittelun, identiteetinhallinnan ja riskienhallinnan. Erityisesti useat ohjelmat alkavat perusohjelmointi ja edistyminen kehittyneisiin kyberturvallisuusaiheisiin, jotka sopivat aloittelijoille. Yksi standout-ohjelma, yhteistyössä Cybintin kanssa, palvelee niitä, joilla on rajallinen tietotekninen tietämys, joka tarjoaa käytännöllisiä, reaalimaailman taitoja sekä kokopäiväisissä että osa-aikaisissa muodoissa. Nämä ohjelmat pyrkivät yhdessä kehittämään erilaisia kyberturvallisuustaitoja, jotka vaihtelevat perustavasta ohjelmoinnista syvälliseen, sovelluskeskeiseen oppimiseen.

Useat Suomen kansallisen turvallisuuden ja puolustuksen vahvistamiseen tähtäävät linjaukset ovat vaikuttaneet kyberturvallisuuteen liittyviin koulutusohjelmiin. On ollut yhä enemmän tutkimus- ja kehitysaloitteita, koulutusohjelmia ja sertifioituja ammattilaisia kyberturvallisuuden alalla. Kyberturvallisuusstrategiassa (2019) (https://turvallisuuskomitea.fi/en/finlands-cyber-

security-strategy-2019/) ja kyberturvallisuuden kehittämisohjelmassa (2021) korostetaan kansallisen kyberturvallisuusosaamisen kehittämisen merkitystä koulutuksen ja tutkimuksen avulla. Koulujärjestelmän tavoitteena on antaa opiskelijoille taitoja ja tietoja, joilla he voivat navigoida digitaalisessa maailmassa turvallisesti ja tietoisuus kyberuhkista ja suojatoimenpiteistä **Lehto-IWS-018.pdf (jyu.fi).**

Suomalaisessa ammatillisessa koulutuksessa kyberturvallisuutta ei ole nimenomaisesti korostettu erillisenä tai erikoistuneena painopisteenä useimmissa materiaaleissa. Tämä ei kuitenkaan välttämättä tarkoita sitä, että kyberturvallisuus puuttuu kokonaan ammatillisen koulutuksen ohjelmista. Koska digitaalisen lukutaidon ja kyberturvallisuuden merkitys kasvaa kaikilla aloilla, nämä aiheet on sisällytetty laajempiin tietoteknisiin ja teknisiin koulutusohjelmiin. On tärkeää huomata, että ammatillisen koulutuksen tarjoajat Suomessa voivat itsenäisesti järjestää koulutustarjontansa alueellisten ja alakohtaisten vaatimusten mukaisesti. Suomalaisessa ammatillisessa koulutuksessa on viime aikoina tehty laajin uudistus lähes 20 vuoteen. Vuoden 2018 uudistuksen tavoitteena oli luoda tehokkaampi ja joustavampi, osaamisperusteisempi ja asiakaslähtöisempi ammatillisen koulutuksen järjestelmä, parantaa sen tehokkuutta ja sovittaa pätevyydet paremmin työmarkkinoiden tarpeisiin. Tämä tapahtuu pääasiassa vähentämällä sääntelyä ja lisäämällä ammatillisen koulutuksen tarjoajien riippumattomuutta ja vastuuta. (Lähde: **https://www.cedefop.europa.eu/files/8133_en.pdf)** Tämä tarkoittaa sitä, että jotkin laitokset saattavat tarjota erikoistuneempia moduuleja kyberturvallisuuden kaltaisilla aloilla riippuen paikallisen teollisuuden vaatimuksista ja kumppanuuksista. Lehdon tutkimuksen perusteella kyberturvallisuus ei ole erillinen aihe, vaan se on integroitu eri aiheisiin, erityisesti tieto- ja viestintätekniikan (ICT) yhteydessä. Opetuksen vastuu perustuu siihen, että opettajat sisällyttävät kyberturvallisuuskoulutuksen oppiaineisiinsa. Tämä lähestymistapa johtaa vaihteluun siinä, miten tämä toteutetaan eri kouluissa ja eri luokissa, ja korostaa, että kyberturvallisuuden opetuksessa tarvitaan jäsennellympiä ja johdonmukaisempia lähestymistapoja, mukaan lukien mahdollisesti erillinen aihe tai tieto- ja viestintätekniikan koulutuksen näkyvämpi osa.

Korkeakoulutasolla suomalaiset yliopistot tarjoavat kattavia kyberturvallisuuden tutkinto-ohjelmia. Nämä ohjelmat on suunniteltu antamaan opiskelijoille kehittyneitä tietoja ja taitoja eri aloilla kyberturvallisuuden. Monet tarjoavat maisterin tutkinnon tietoturvasta ja tietotekniikasta keskittyen näiden käsitteiden todellisiin vaikutuksiin ja sovelluksiin. Ne ovat saatavilla paikan päällä ja etänä.

Belgian kyberturvallisuussektorilla on yhä suurempi pyyntö saada ammattitaitoisia ammattilaisia, ja noin 4000 avointa kyberturvallisuuspaikkaa on avoinna (marraskuusta 2022). Maan kyberturvallisuusosaamisen kehittämiseksi on otettu käyttöön useita aloitteita ja koulutusohjelmia, joissa tunnustetaan kiireellisyys ja tarve korjata tämä puute. Lukuisat laitokset Belgiassa, kuten KU Leuven, Solvay Business School, Howest University of Applied Sciences, ja monet muut ovat kehittäneet erikoistuneita ohjelmia englanniksi, ranskaksi ja hollanniksi, jotka pystyvät saavuttamaan laajan yleisön. Belgialaisen Agoria-organisaation tutkimuksessa korostettiin kuitenkin tarvetta täydennyskoulutukseen myös sellaisten ammattilaisten keskuudessa, jotka eivät enää osallistu yliopistoon, jotta he voivat pitää heidät ajan tasalla

kyberturvallisuuden alasta ja sen uhkista. Belgian kyberturvallisuusstrategiassa vuosiksi 2021–2025 tunnustetaan kyberturvallisuuden korkeatasoinen integrointi maan akateemiseen ympäristöön ja korostetaan yliopistojen ja muiden oppilaitosten keskeistä roolia alan tutkimus- ja kehitystoimien edistämisessä. CBB: n (Centre for Cybersecurity Belgium) tietokannan mukaan Belgiassa on 33 korkeakoulujen tarjoamaa kurssia (kandidaatin, maisterin ja sertifikaatit), jotka täydentävät erilaisia ammatillisen koulutuksen ohjelmia sekä julkisella että yksityisellä sektorilla. CBB on elin, joka valvoo, koordinoi ja seuraa Belgian kyberturvallisuusstrategian täytäntöönpanoa ja kehittää parhaillaan ilmaista työntekijöiden kyberturvallisuustietoisuutta koskevaa koulutusta belgialaisille työntekijöille, jotta kyberturvallisuusosaamista voidaan levittää entistä enemmän väestön keskuudessa. Yleisesti ottaen Belgian kyberturvallisuusstrategiassa korostetaan kyberturvallisuustietojen ja -taitojen levittämisen merkitystä koulutuksen avulla ja sitoudutaan laajentamaan akateemisia kursseja, edistämään alan tutkimusta, kannustamaan STEM-aineiden koulutusta ja tarjoamaan käytännön koulutusmahdollisuuksia, joilla vastataan ammattilaisten kasvavaan kysyntään Belgian kyberturvallisuusympäristössä.

Norjassa kyberturvallisuus ei ole pääaine, jota voi opiskella ammatillisen koulutuksen tasolla. Ohjelman elementit sisältyvät ammatillisen koulutuksen ohjelmaan nimeltä ”Tietokone ja elektroniikka”. Kyberturvallisuutta koskevaa opetusministeriön kehystä ei ole, vaan siinä mainitaan vain yleisessä digitaalisen lukutaidon perustaidot kaikessa koulutuksessa, että opiskelijoiden olisi voitava käyttää ja navigoida digitaalisia resursseja verkoissa ja niiden ulkopuolella sekä turvata tieto- ja tietoturva.

Kyberturvallisuusosaamista koskevassa kansallisessa strategiassa korostetaan 14.11.2023, että ammatillisen koulutuksen opiskelijat oppivat kyberturvallisuudesta. Monissa ammatillisissa oppiaineissa tämä on erittäin tärkeää ja merkityksellistä. Ammatillisissa kursseissa ei ole kyberturvallisuuden oppimateriaaleja, ja opettajilla ei ole taitoja opettaa erityisesti yksityisyyden, älykkään kodin teknologian ja esineiden internetin kaltaisilla aloilla. Nykyiset kyberturvallisuuskoulutuksen ohjelmat, kuten GenCyber ja CyberFirst, eivät erityisesti käsittele tämän ammatillisen ohjelman tarpeita. (**lähde 1 –2**)

UiO:n, NTNU:n ja valittujen ammatillisten oppilaitosten opettajien yhteistyön avulla on tarkoitus kehittää kyberturvallisuuden oppimateriaalia, joka on myöhemmin saatavilla kansallisella oppimisalustalla NDLA **(National Digital Learning Arena)**.

Korkeakoulutuksessa löydät sekä yhden vuoden ohjelman digitaalisen turvallisuuden kulttuurissa että kandidaatin ohjelmissa kyberturvallisuudessa. Aihe sisältyy myös useisiin datatieteiden ja tietotekniikan maisteriohjelmiin. On olemassa erilaisia erityisiä kyberturvallisuustutkimuksia soveltavana tietokone- ja tietotekniikkana, Bachelor in Cyber Security, Bachelor in Digital Forensics, Digitaalinen infrastruktuuri ja kyberturvallisuus, digitaalinen turvallisuuskulttuuri ja kokemuspohjainen päällikkö tietoturvassa. On myös tutkimuksia, joissa kyberturvallisuus sisältyy HSE-kulttuuriin ja johtaviin, kunnallisiin hätävalmiusosuuskuntiin ja hallitustyöhön käytännössä ja vuositutkimukseen kriisinhallinnassa.

Puolassa kybertutkimukset ovat lisääntyneet viime vuosina. Yhä useammat kyberkurssit avautuvat yliopistoissa, ja samalla ammatillisen koulutuksen kurssien määrä kasvaa. Kyberammatteihin liittyvä kysyntä on kasvanut Puolassa viime vuosina, ja tietoisuus kybertoiminnasta on lisääntynyt myös Puolan valtuuskunnassa, joka kannustaa yrityksiä palkkaamaan kyberasiantuntijoita ja suojaamaan tietoja.
Puolassa, kuten useimmissa Euroopan maissa, akateemista tutkintoa pidetään pakollisena ja siksi kyberkurssit ovat usein lisätutkimus tutkinnon jälkeen. Koska suurin osa akshmi-tutkimuksista on pidempiä, mutta teoreettisesti. On olemassa verkkokursseja, jotka ovat lyhyitä, mutta useimmat niistä keskittyvät käytännön oppimiseen, joka valmistautuu todelliseen työhön.
Kyberalan opiskelijan suuri haaste on, että suurimmalla osalla ammatillisista oppilaitoksista ei ole omaa rahoitusta, joten tarvitaan rahoitusratkaisu, joten tämä vaihtoehto ei aina sovellu kiinnostuneille.

Vaikka kyberturvallisuus olisi asetettava etusijalle kaikilla toiminta-aloilla, Romanian ammatillisen koulutuksen järjestelmä ei ole vielä valmis varmistamaan, että opiskelijat ovat päteviä tällä alalla. Analysoitaessa opetussuunnitelmaa lykeumin alemman syklin – teknologian alalla – millä tahansa ammatillisen koulutuksen alalla, teknisen kulttuurin opetussuunnitelma ei tarjoa tietoverkkoturvallisuutta koskevia oppimistuloksia. Joitakin alan erityistaitoja löytyy yleisen tietämyksen opetussuunnitelmasta, tieto- ja viestintätekniikan kurinalaisuudesta, 9. luokan opetussuunnitelmasta. Nämä ovat:

1. Internetin käytön turvatoimien kuvaus ja soveltaminen:

- Internetin älykäs käyttö
- Tiedonsiirron salauksen merkitys
- Digitaalisen allekirjoituksen käyttö
- Suojautumiskeinot viruksia vastaan

2. Chat-palvelun käyttäminen:

- Videoneuvottelujen yhteistyösovellusten esittely
- IRC-verkkosääntöjen esittely

Lukion ylempi sykli, 11 luokka, vain ammatillisen koulutuksen alalla Electronic Automation erikoisalojen Televiestintäteknikko, Tietokoneoperaattori teknikko, Telematiikka operaattorin teknikko, tarjoaa joitakin sisältöä asentamiseen turvallisuussovelluksia. 12. luokalla, vain Computer Technician erikoistuminen, erikoistunut moduuli sisältää sisältöä, kuten:

- Tietojärjestelmien ja tietoverkkojen turvallisuuden perusperiaatteet
- Verkon turvallisuuspolitiikan kehittäminen
- Verkkojen turvallisuusuhat
- Internet-selailusuoja
- Virukset ja tietoturvasovellukset

Koskien HEI, Transilvania University of Brasov osoittaa vahvaa sitoutumista kyberturvallisuus koulutukseen, joka tarjoaa kattavan maisteriohjelman kyberturvallisuuden suoritetaan kokonaan Englanti. Yliopiston omistautuminen asiantuntemuksen edistämiseen tällä kriittisellä alalla näkyy ohjelman laajassa opetussuunnitelmassa.

Tämä maisteriohjelma Transilvania University on erinomainen tilaisuus opiskelijoille, jotka etsivät monipuolista koulutusta kyberturvallisuudesta kansainvälisessä akateemisessa ympäristössä. Vankan opetussuunnitelman ja englanninkielisen opetuksen yhdistelmä suorittaa tutkinnon menestystä dynaamisella ja haastavalla kyberturvallisuuden alalla.

Babes-Bolyai University Cluj-Napocassa matematiikan ja tietotekniikan tiedekunnan kautta on aloittanut lukuvuodesta 2023–2024 englanninkielisen kyberturvallisuuden maisteriohjelman, jonka tarkoituksena on valmistella tulevia asiantuntijoita tällä alalla, jolla on elintärkeä merkitys tietoyhteiskuntaan siirtymisen yhteydessä. Uuden ohjelman kurssit alkavat tämän vuoden lokakuussa yhdessä lukuvuoden 2023–2024 kanssa, jolloin kilpailu ylittää odotukset. Yli 40 opiskelijaa, myös ulkomailta, hyväksytty ohjelmaan tulee asiantuntijoita alalla Cyber Security, hyväksytyt ehdokkaat voivat jopa päättää opiskella lukuvuoden muissa tunnetuissa yliopistoissa Euroopassa.

Matematiikan ja tietojenkäsittelytieteen tiedekunnassa Master Program *Internet Technologies* (englanniksi) tarjoaa myös ensimmäisen vuoden jälkipuoliskolla kryptografian *ja järjestelmäturvallisuuden kurssin, joka* esittelee opiskelijat kyberturvallisuuden ja tietojen salauksen erityismenetelmiin.

Lisäksi Master Program Modern Technologies in Software System Engineering tarjoaa toisen vuoden alkupuoliskolla valinnaisen kurssin nimeltä IT-järjestelmien turvallisuus, joka keskittyy kyberturvallisuuden tärkeimpiin haasteisiin.

Molemmat kurssit antavat matematiikan ja tietotekniikan tiedekunnan maisteriopiskelijoille mahdollisuuden saada tietoa ja asiantuntemusta tästä aiheesta, joka todellisessa kansainvälisessä kontekstissa on elintärkeää, ja saada tieto nykyaikaisten järjestelmien salauksen ja turvallisuuden haasteista.

Bukarestin yliopisto, matematiikan ja tietotekniikan tiedekunta, tarjoaa Master Program Security and Applied Logic (englanniksi), joka tarjoaa sarjan kursseja omistettu salaus ja järjestelmän turvallisuus. Opiskelijat voivat hankkia tietoa käyttöjärjestelmän turvallisuuden, salauksen, verkkoturvallisuuden ja kyberturvallisuuden aloilla, joten he ovat valmiita vastaamaan tämän alan haasteisiin.

Espanjassa suurin osa kyberturvallisuuden opinnoista on korkea-asteen, tutkintojen tai maisterin tutkinto. Espanjan kansallisen kyberturvallisuusinstituutin keräämien tietojen mukaan:

- Noin 87 kyberturvallisuuden maisterin tutkintoa, joita julkiset ja yksityiset yliopistot ja muut korkeakoulut tarjoavat.
- 4 erikoisalat, enimmäkseen erikoistuminen tietokoneen rikostekniseen.

- 3 korkeakoulututkintoa, jotka kaikki tarjoavat yksityisen sektorin.

Ammatillisen koulutuksen osalta espanjalaisissa ammatillisissa oppilaitoksissa on tarjolla noin 60 kurssia. Kaikkia niistä säännellään samalla opetussuunnitelmalla, jonka opetusministeriö hyväksyi toukokuussa 2020 *kuninkaallisella asetuksella 479/2020, 7. huhtikuuta, joka vahvistaa kyberturvallisuuden erikoistumiskurssin tietotekniikan ympäristöissä*.

Nykyisistä ohjelmista huolimatta lisäponnistelujen tarve tunnustetaan. Espanja on pannut täytäntöön useita suunnitelmia, kuten kansallista digitaalitaitosuunnitelmaa, pk-yritysten digitalisointisuunnitelmaa 2021–2025 ja Espanjan digitaalista 2025 -suunnitelmaa. Niissä keskitytään erityisesti uusien lahjakkuuksien luomiseen, jotta voidaan vastata digitaalisten taitojen kasvavaan kysyntään erityisesti kyberturvallisuuden alalla.

Türkiyessä kyberturvallisuuden tarve on kasvanut nopeasti ja tullut erittäin tärkeäksi maassamme ja kaikkialla maailmassa, erityisesti viime vuosina. Samanaikaisesti teknologisen kehityksen kanssa kyberriskit ja -uhat ovat myös muuttuneet samaan tahtiin ja muuttuneet monimutkaisiksi. Kyberriskit ja -uhat ovat saavuttaneet potentiaalin aiheuttaa paljon kattavampia ja kielteisiä seurauksia kuin fyysiset hyökkäykset. Rahoituksen, sähköisen viestinnän, energian, liikenteen ja ilmailun kaltaisilla aloilla, jotka tarjoavat palveluja turvallisessa digitaalisessa ympäristössä, kansallisesta kyberturvallisuudesta on tullut yksi maamme tärkeimmistä painopisteistä. Tässä yhteydessä tutkimukset jatkavat ammatillisen ja korkea-asteen koulutuksen kyberturvallisuuskoulutuksen levittämistä alan tarpeiden mukaisesti sekä koulutussisällön kehittämistä ja rikastamista.

Näiden opintojen puitteissa ammatillisessa koulutuksessa: Kyberturvallisuuden perusteet verkkotoiminnassa tietotekniikan alalla. Tietoverkkoturvallisuuden, ohjelmoinnin perustekijöiden, järjestelmän turvallisuuden, verkkoteknologioiden, turvallisten ohjelmistojen kehittämisen, tunkeutumistestauksen ja kyberhäiriöiden torjunnan, tietokonerikostutkinnan jne.

Korkeakoulutuksessa ”Cyber-Turvallisuusanalyytikko ja Operaattori” -tutkinto-ohjelma kyberturvallisuuden ammatillisissa oppilaitoksissa, oikeuslääketieteen tietotekniikan perustutkinto-ohjelma yliopistoissa ja asiaankuuluvat maisteriohjelmat tarjotaan yliopistoissa.

Lisäksi korkeakoulujen täydennyskoulutuskeskukset, kuntien julkiset koulutuskeskukset, viralliset laitokset, kuten TÜBİTAK, TSE ja yksityiset oppilaitokset tarjoavat myös kyberturvallisuuskoulutusta.

2.1.2. KYBERTURVALLISUUSHAASTEET JA TEOLLISUUDEN TARPEET

Perusteellisen kirjallisuuskatsauksen perusteella olemme listanneet pk-yritysten kohtaamia kyberturvallisuushaasteita hankkeen maissa. Kyberturvallisuuden muuttuvassa toimintaympäristössä pienet ja keskisuuret yritykset (pk-yritykset) kohtaavat Liettuassa useita kyberturvallisuushaasteita. Koska nämä yritykset luottavat toiminnassaan yhä enemmän digitaaliteknologiaan, ne ovat alttiimpia kyberuhkien kirjolle, mikä edellyttää kattavaa ymmärrystä ja strategista lähestymistapaa näiden riskien hallitsemiseksi tehokkaasti.

Vuoden 2022 tutkimuksessa Bukauskas et al. erottivat[8] erilaisia organisaatiotyyppejä kyberturvallisuuden kypsyys- ja osaamistarpeidensa perusteella. Tutkimuksen mukaan pienet organisaatiot ovat verrattavissa yhteiskunnan yksittäisiin henkilöihin, sillä digitaalisen työtilan turvallisuuden tärkein parametri on kyberhygienian taso, johon vaikuttaa kyberturvallisuusuhkien yleinen ymmärrys. Tällä tasolla kyberturvallisuutta koordinoidaan sisäisesti organisaation sisällä, mikä johtaa mahdollisiin tietoturvaloukkauksiin liiketoimintaprosesseissa. Myös keskikokoisissa yrityksissä kyberturvallisuuden hallintaa ja sääntelyä koordinoidaan heikosti. Reagointi poikkeamiin tai muihin kyberturvallisuustoimiin ei myöskään korostu organisaatiossa. Liettuan pienyritysten osuus kaikista yrityksistä on 97 prosenttia, Bukauskas et al. (2022) totesi, että tietotekniikka-asiantuntijoille, jotka tarjoavat tietoteknisiä palveluja, kuulevat käyttäjiä ja joiden työtehtäviin kuuluu kyberturvallisuuden perusperiaatteiden varmistaminen, on merkittävä tarve. He korostivat myös, että uhkatiedustelussa ja tieteellisessä tutkimuksessa havaitaan huomattavaa puutetta ja että kyberturvallisuuden asiantuntijoita tarvitaan näkyvästi turvallisuussuunnittelun ja järjestelmien elinkaaren aikana.

Muutama vuosi aiemmin ”Luo Liettualle” -ohjelma järjesti yhteistyössä kansallisen puolustusministeriön kanssa julkisen kuulemisen kyberturvallisuustietoisuuden lisäämisestä pienten ja keskisuurten yritysten keskuudessa[9]. Aloitteessa päädyttiin myös siihen, että on ilmeistä, että Liettuan pk-yritysten kyberturvallisuustietoisuuden taso ei ole korkea ja että pienet yritykset eivät ole saavuttaneet riittävää kyberresilienssitasoa digitaalisten riskien puutteellisen ymmärtämisen vuoksi. Lisäksi aloitteessa todettiin, että yli puolet (57 prosenttia) yritysten johtajista totesi, että heillä ei ole tai ei ole varma, onko heillä riittävästi tietoa kyberturvallisuusratkaisujen valitsemiseksi, ja yli kolme neljäsosaa työntekijöistä oli sitä mieltä, että heillä ei ole helposti ymmärrettävää tietoa.

Vertailu Bukauskas et al. (2022) ja aiempi ”Create for Lithuania” -aloite (2019), on ilmeistä, että Liettuan pk-yritysten kyberturvallisuustilanne on osoittautunut vähäiseksi. Molemmissa tutkimuksissa korostetaan jatkuvaa puutetta kyberturvallisuuden perustietämyksestä ja -valmiudesta näissä yrityksissä. Vaikka riippuvuus digitaaliteknologioista on lisääntynyt, pk-yrityksissä on edelleen haavoittuvuuksia, jotka johtuvat riittämättömästä kyberuhkien

[8] Bukauskas, L., Brilingaitė, A., Lepaitė, D., Juozapavičius, A., Ikamas, K., 2022. ”Projekto ”Kibernetinio saugumo kompetencijp žemėlapio kūrimas” ataskaita”, Vilniaus universitetas Informatikos institutas. Saatavilla osoitteessa: https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf [Accessed 12. tammikuuta 2024]. DOI: https://doi.org/10.15388/CIBERSEK.2022.

[9] Luo Liettualle ja puolustusministeriölle 2019. SVV Kibernetinio saugumo Apklausos Apžvalga. [online] Saatavana osoitteessa: http://kurklt.lt/wp-content/uploads/2019/12/SVV-kibernetinio-saugumo-apklausos-ap%C5%BEvalga-Kurk-Lietuvai.pdf

sietokyvystä ja siitä, että digitaalisista riskeistä ei yleisesti ymmärretä. Tämä jatkuva haaste korostaa kiireellistä tarvetta parantaa kyberturvallisuutta koskevaa tietoisuutta ja koulutusta pk-yritysten keskuudessa. Tämä on kriittinen ala, joka muodostaa suurimman osan Liettuan liiketoimintaympäristöstä.

Suomessa Elinkeinoelämän tutkimuslaitoksen (Elinkeinoelämän tutkimuslaitos) tutkimuksessa korostettiin, että suomalaisten yritysten, myös pk-yritysten, tietoturvaloukkausten määrä on kaksinkertaistunut kahden vuoden aikana. Suomalaiset yritykset ilmoittivat tietoturvaloukkauksista kolme kertaa enemmän kuin Euroopan keskiarvo vuonna 2019, ja useimmat tapaukset liittyivät huijauksiin, tietojenkalasteluhyökkäyksiin, tietomurtoihin, haittaohjelmiinja haavoittuvuuksiin. Tutkimuksessa korostetaan myös osaavien kyberturvallisuusammattilaisten puutetta suomalaisten pk-yritysten suurimpana haasteena. **https://www.etla.fi/en/publications/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/**

Kansallinen kyberturvallisuuskeskus (NCSC-FI) (**https://www.kyberturvallisuuskeskus.fi/en**) on Suomen hallituksen johtama aloite. Se toimii osana Liikenne- ja viestintävirastoa (Traficom), joka vastaa viestinnän ja liikenteen sääntelystä Suomessa. Ne antavat tietoa kyberturvallisuuden nykytilasta ja tarjoavat ohjeita ja työkaluja sekä yksilöille että organisaatioille kyberturvallisuuskäytäntöjensä parantamiseksi. Keskus osallistuu myös kansallisiin kyberturvallisuusaloitteisiin, kuten haavoittuvuushälytyksiin, ja edistää tietoisuutta ja varautumista kyberuhkia vastaan.

Niiden viikoittaiset katsaukset antavat hyvän kuvan pk-yritysten kohtaamista haasteista. Opimme, että suomalaiset pk-yritykset, kuten monet muutkin, ovat kohdanneet samoja turvallisuusongelmia, joita ETLA-instituutti on kuvaillut monien tietojenkalastelu- ja huijausviestien kohteena. Näitä ovat yritykset esittää Suomi.fi:n kaltaisia laillisia palveluita tietojenkalasteluun tai muuhun arkaluontoiseen tietoon. Pk-yritysten taloudelliset resurssit voivat rajoittaa nykyaikaisten kyberturvallisuusratkaisujen käyttöönottoa kyberuhkilta suojautumiseksi. Samalla tavoin jo varustetuilla pk-yrityksillä on vaikeuksia pysyä ajan tasalla uusien kyberturvallisuusuhkien varalta.

Pyrkiessämme ymmärtämään pk-yritysten kyberturvallisuustilannetta Belgiassa teimme perusteellisen tutkimuksen. Tilintarkastustuomioistuin piti kuitenkin haastavana saada kattavia tietoja tai lähteitä, jotka käsittelevät tätä kriittistä ongelmaa. Tiedon puute vaikeuttaa sellaisten tehokkaiden strategioiden ja ratkaisujen luomista, jotka voivat auttaa pk-yrityksiä suojelemaan digitaalisia resurssejaan kyberuhkilta.

Pystyimme tavoittamaan ammattilaisia, jotka ovat aktiivisesti mukana kyberturvallisuuden alalla Belgiassa, kiitos Women4Cyber-säätiön laajan verkoston. Nämä asiantuntijat antoivat meille tärkeitä näkemyksiä ja näkökulmia, jotka auttoivat meitä ymmärtämään pk-yritysten erilaisia kyberturvallisuuteen liittyviä haasteita. Saimme näkemyksiä Iva Tashevalta, merkittävältä Women4Cyber Belgiumin jäseneltä, joka jakoi laajan kokemuksensa ja tietämyksensä haasteista, joita pk-yritykset kohtaavat yrittäessään suojata digitaalista infrastruktuuriaan kyberuhkilta.

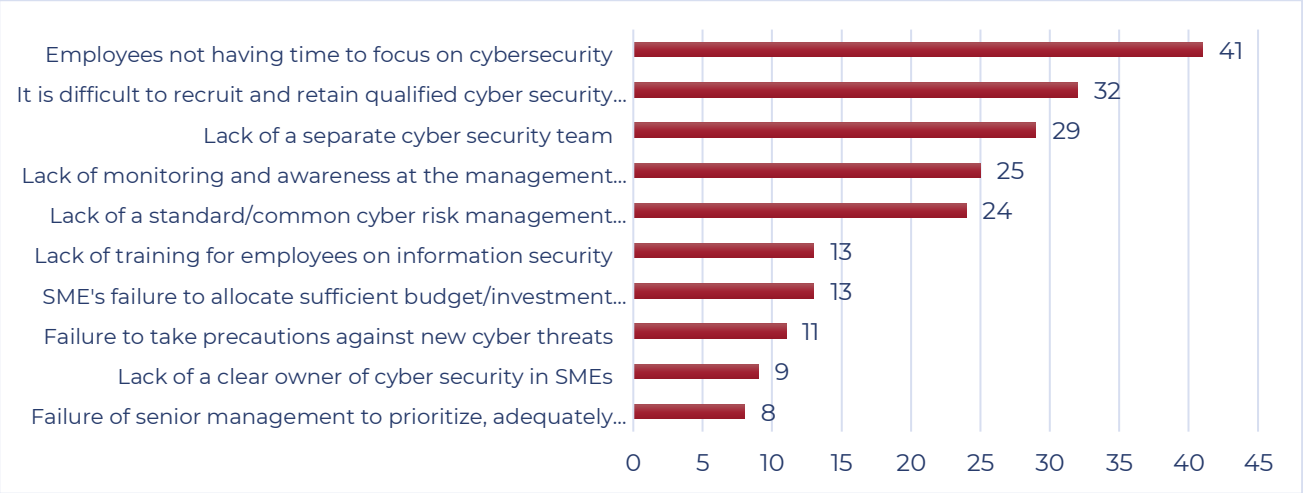
Pk-yrityksillä on useita kyberturvallisuushaasteita, kuten vaikeudet saada tapauskohtaista tukea, henkilöllisyyksien ja pääsynhallintakoulutuksen puute henkilöstölleen sekä rajallinen ymmärrys pilvipalvelujen rooleista ja vastuualueista. Lisäksi pk-yrityksillä on rajalliset mahdollisuudet käyttää kohtuuhintaisia haavoittuvuusskannausratkaisuja ja seurantavälineitä, minkä vuoksi ne ovat alttiimpia kyberuhkille. Liiketoimintaympäristöjen kokonaisvaltainen hyperyhteys altistaa pk-yritykset identiteettivarkauksille ja petollisille toiminnoille, kun taas tietojenkalastelu ja huijaukset aiheuttavat jatkuvia riskejä. Näihin haasteisiin vastaamiseksi pk-yritysten on toteutettava ennakoivia toimenpiteitä, pantava täytäntöön vankat turvallisuuskäytännöt ja tarjottava työntekijöille kattavaa koulutusta osaamisensa vahvistamiseksi ja suojautumiseksi mahdollisilta rikkomuksilta ja taloudellisilta tappioilta.

Kyberturvallisuudesta on tullut yksi tärkeimmistä prioriteeteista Espanjassa toimiville yrityksille, myös pienille ja keskisuurille yrityksille (pk-yritykset). Etätyöskentelyn ja verkkokurssien lisääntyminen on johtanut muun muassa etätyöpöytätoimintojen, pilvipalvelujen ja yhteistyövälineiden laajamittaiseen käyttöön, mikä on lisännyt riskejä ja tietokonehyökkäyksiä. Kansallisen kryptologisen keskuksen (CCN-CERT) raportissa yhdistetään etätyön lisääntyminen ja teknologian käyttö näiden riskien lisääntymiseen. Yleisimpiä yritysten kärsimiä hyökkäyksiä ovat kiristysohjelmat ja etäkäyttöjärjestelmiin kohdistuvat hyökkäykset. Kyberuhkien lisääntyminen on johtanut siihen, että yritykset ovat lisänneet kyberturvallisuusryhmiin osoitettujen henkilöiden määrää joko sisäisesti tai ulkoisesti. Tästä huolimatta yritykset ulkoistavat edelleen noin 50 prosenttia näistä toiminnoista.

Lisäksi Espanjassa on edelleen 21 prosenttia yrityksistä, joilla ei ole turvallisuusoperaatiokeskuksia häiriötilanteiden käsittelyä varten. Liiketoimintaympäristön kyberturvallisuuskoulutuksen osalta Deloitten analyysissa korostetaan, että analysoitujen organisaatioiden työntekijöiden kyberturvallisuutta koskevan verkkokoulutuksen tuntimäärä kasvoi vuonna 2022 lähes 30 prosenttia vuoden 2021 tietoihin verrattuna. Lähes 50 prosentilla espanjalaisista yrityksistä ei kuitenkaan ole kyberturvallisuussertifiointia, mikä on selkeä haaste tulevaisuudelle.

Espanjalaisten yritysten suurin haaste on kuitenkin edelleen kyberturvallisuuden lahjakkuuden puute. ObservaCiberin laatiman raportin ”Analysis and Diagnosis of Cybersecurity Talent in Spain” mukaan Espanjassa oli vuonna 2021 osaamisvaje arviolta 24.119. Vuonna 2024 on arvioitu, että Espanja tarvitsee yli 83.000 asiantuntijaa, mikä nostaa osaamisvajeen 57,5 prosenttiin.

Vaikuttaa siltä, että heikoin yhteys, joka saa pk-yritykset kohtaamaan kyberturvallisuuteen liittyviä haasteita, on inhimillinen tekijä. Pk-yritysten suurin haaste on se, että kyberturvallisuudesta vastaava henkilöstö ei pysty varaamaan riittävästi aikaa kyberturvallisuuden alalle, koska sillä on vastuualueita useammalla kuin yhdellä alueella. Tähän liittyen erillisen kyberturvallisuustiimin puuttuminen sijoittuu kolmanneksi pk-yritysten kyberturvallisuuden hallinnassa kohtaamien vaikeuksien listalle. Pk-yrityksillä on vaikeuksia rekrytoida ja ylläpitää päteviä kyberturvallisuuden työntekijöitä.



Kuva – 1 pk-yritysten haasteet – Türkiye-tutkimus.

Romaniassa verkkoympäristö tarjoaa liiketoimintamahdollisuuksia ja yhteyksiä, jotka voivat auttaa pk-yrityksiä kehittymään, mutta se sisältää myös monia riskejä.

Kyberturvallisuus ei ole enää tarina, se on todellisuutta myös Romaniassa, vaikka tähän asti meillä ei ole ollut merkittävää kyberhyökkäystä.

Käytetty tietolähde on VERIZONin raportti kyberuhkista vuonna 2023 – pk-yritysten tärkeimmät keskeiset kohdat (DATA BREACH INVESTIGATIONS REPORT – DBIR), joka perustuu 16,312 tietoturvahäiriöön, joista 5199 on vahvistettu tietoturvaloukkauksiksi.

Pk-yritysten kiinnostuksen kohteet:

- Pk-yritysten ja yritysten hyökkäyspinnat ovat samankaltaiset, koska ne käyttävät pilvipohjaisia ohjelmistoja. Luvaton tunkeutuminen järjestelmään, sosiaalisen suunnittelun tekniikat ja verkkosovellusten perushyökkäykset muodostavat 92 prosenttia kaikista pk-yritysten havaitsemista hyökkäyksistä (85 prosenttia yrityksistä).
- ransomware 24 % tapauksista (tiedot varastetaan ennen salausta)
- luvaton tunkeutuminen järjestelmään – monimutkaiset hyökkäykset, jotka perustuvat haittaohjelmiin ja/tai hakkerointiin tavoitteidensa saavuttamiseksi.
- Ulkoiset hyökkääjät muodostavat suurimman uhan, joka aiheuttaa 83 prosenttia nykyisistä tietoturvaloukkauksista ja on 94 prosenttia pk-yritysten hyökkäyksistä. 94 prosenttia uhkien leviämiseen osallistuvista toimijoista on ulkoisia, kun taas suurten organisaatioiden tapauksessa vastaava luku on 89 prosenttia, ja 98 prosenttia rikkomuksista on taloudellisesti perusteltuja, kun taas yritysten tapauksessa vastaava luku on 97 prosenttia.
- Taloudelliset motiivit ovat ykkönen 95 prosentissa tapauksista, ja pk-yrityksiin kohdistuvissa hyökkäyksissä osuus nousee 98 prosenttiin. Vain yksi prosentti on motivoitunut vakoilusta.
- Työntekijät ovat heikko lenkki turvallisuusketjussa – 74 prosenttia kaikista tapauksista (huono tietoisuus kyberuhkista). Pääasiallinen tunkeutumismenetelmä voi johtua varastettujen valtakirjojen käytöstä – 49 % ja tietojenkalastelu – 12 % tai muista menetelmistä, kuten väärin konfiguroinnista tai arkaluonteisten tietojen virheellisestä lähettämisestä.

- Yrityssähköpostien vaarantaminen – uhri huijataan siirtämään suuria summia hyökkääjien tileille.

Norjassa pienet ja keskisuuret yritykset (pk-yritykset) kohtaavat merkittäviä kyberturvallisuuteen liittyviä haasteita. Monilta puuttuu syvällinen ymmärrys asiaan liittyvistä riskeistä, mikä johtaa mahdollisiin haavoittuvuuksiin. Työntekijöiden tehokkaassa kyberturvallisuuskoulutuksessa on huomattava aukko, mikä tekee inhimillisestä virheestä yhteisen riskitekijän. Pk-yrityksillä, erityisesti niillä, joilla on rajalliset resurssit, on usein vaikeuksia investoida kehittyneisiin kyberturvallisuustoimenpiteisiin ja ammattitaitoiseen henkilöstöön. Niiden on myös navigoitava monimutkaisia tietosuojalakeja, mikä lisää vaatimusten noudattamisen varmistamisen monimutkaisuutta ja suojaa arkaluonteisia tietoja. Verkkourkintahyökkäysten ja sosiaalisen suunnittelun lisääntyminen osoittaa edelleen niiden haavoittuvuuden, samoin kuin riittämätön verkkoturvallisuus ja sisäisten uhkien riski. Näiden riskien hallinta on ratkaisevan tärkeää, mutta pk-yritykset pitävät usein tehokasta riskinarviointia ja hallintaa haastavana. Lisäksi riippuvuus kolmansien osapuolten toimittajista tuo mukanaan toisen monimutkaisuuden tason, mikä saattaa altistaa pk-yrityksille uusia kyberturvallisuusuhkia.

2.2. NAISET KYBERTURVALLISUUDESSA

Tilintarkastustuomioistuin analysoi naisten koulutus- ja tukitarpeita, naisten nykyisiä pätevyyksiä ja pätevyyksiä kyberturvallisuuden alalla sekä suosituksia lisätä naispuolisten työntekijöiden osallistumista kyberturvallisuushaasteisiin.

Microsoft teki tutkimuksen 35 Euroopan maassa, joissa alle yksi viidestä tietojenkäsittelytieteen tutkinnon suorittaneesta oli naisia. Kiinnostus tieteeseen, teknologiaan, insinööritieteeseen ja matematiikkaan (STEM-aineet) nousee aivan liian aikaisin. OECD:n kansainvälisen opiskelijoiden arviointiohjelman (PISA) mukaan pojat ovat tyttöjä todennäköisemmin kuvittelemaan olevansa tieto- ja viestintätekniikan ammattilaisia, tutkijoita tai insinöörejä. (Microsoft, 2017).

Kun tarkastellaan naisten osuutta tieto- ja viestintätekniikan asiantuntijoista työelämässä, EU27:ssä vuonna 2020 vain 18,5 prosenttia kaikista tieto- ja viestintätekniikan asiantuntijoista oli naisia. Naisten osuus oli suurin Bulgariassa – 28,2 prosenttia, Kreikassa – 26,6 prosenttia ja Romaniassa – 26,2 prosenttia (ks. kuvio 5 (Naiset menevät teknologiaan, 2021)). Pohjoismaiden ja Baltian maat olivat myös etupäässä listan kärjessä lukuun ottamatta Norjaa, joka sijoittui maan keskipisteeseen. (Naiset menevät tekniikkaan, 2021).

Liettuan tasavallan tilasto-osaston mukaan vuoden 2022 viimeisellä neljänneksellä tiedotus- ja viestintäryhmässä oli 29,4 tuhatta miestä ja 21,5 tuhatta naista. Vuoden 2023 ensimmäisellä neljänneksellä se oli 34,6 tuhatta miestä ja 20,7 tuhatta naista. Vuoden 2023 toisella neljänneksellä miehiä oli 36,8 tuhatta ja naisia 14,8 tuhatta, ja vuoden 2023 kolmannella neljänneksellä miehiä oli 34,5 tuhatta miestä ja 18,0 tuhatta naista. Naispuolisten työntekijöiden määrä väheni huomattavasti vuoden 2023 ensimmäisestä neljänneksestä vuoden 2023 toiseen neljännekseen, minkä jälkeen se kasvoi vuoden 2023 kolmannella neljänneksellä (Rodiklia duomenp Bazė – Oficialiosios Statistikos Portalas, n.d.).

Kun jopa 11 prosenttia naisista työskentelee kyberturvallisuuden parissa, tehtiin kyselytutkimus, jossa selvitettiin kansalaisten näkemyksiä naisten näkökulmista tällä alalla. Riita-asioissa 44,4 prosenttia vastaajista vastasi, että kyberturvallisuuden alalla naisia pitäisi olla 30–60 prosenttia. Suurin osa vastaajista vastasi, että naisten osuus naisammattilaisista olisi 30–60 prosenttia (35,2 prosenttia). Kun analysoidaan vastauksia sukupuolen ja ikäryhmän mukaan, voidaan havaita, että naiset, erityisesti nuoremmat (alle 25 ja 25–45), ajattelevat useimmiten, että naisten määrän pitäisi olla noin puolet. Nuorten miesten (alle 25-vuotiaiden) mielestä jopa 30 prosenttia naisista olisi naisia. Voidaan havaita, että naisilla itsellään on tapana nähdä paljon enemmän naisia kyberturvallisuuden alalla kuin tällä hetkellä markkinoilla. Tämä on hyvä uutinen, sillä naisten houkutteleminen alalle auttaisi paitsi korjaamaan ammattihenkilöiden puutetta, myös lisäämään organisaatioiden turvallisuutta. (Bukauskas et al., 2022).

Suomessa, kuten monissa Euroopan maissa, vallitsee yhteisymmärrys sukupuolten epätasapainosta kyberturvallisuuden ja tietotekniikan alalla yleensä. Aloitteet ja toimet, joilla tuetaan naisia kyberturvallisuuden alalla ja edistetään heidän osallistumistaan kyberturvallisuushaasteiden ratkaisemiseen, ovat lisääntyneet. Suurinta osaa niistä tukevat voittoa tavoittelemattomat järjestöt.

Kyberturvallisuusalalla on toteutettu useita aloitteita koulutus- ja urapolkujen, koulutusohjelmien ja verkostoitumistapahtumien kehittämiseksi. Strategia perustuu myös roolimallien edistämiseen korostamalla naisten menestyksekästä urapolkua kyberturvallisuuden alalla ja jakamalla heidän tarinoitaan innostaakseen useampia naisia jatkamaan uraa tällä alalla. Women4Cyber ja luetellut aloitteet korostavat monimuotoisuuden ja osallisuuden merkitystä sukupuolten epätasa-arvoon puuttumiseksi ja kyberturvallisuusalan yleisen vahvuuden ja häiriönsietokyvyn edistämiseksi. Myös julkiset ja yksityiset laitokset tukevat tätä strategiaa sisällyttämällä tämän sukupuolten tasa-arvon tärkeimpänä painopisteenä kaikkiin aloitteisiinsa.

Women4Cyber Finland (W4CFI)

Elokuussa 2021 perustettu W4CFI on voittoa tavoittelematon järjestö, jonka tavoitteena on lisätä suomalaisen kyberturvallisuuden alalla työskentelevien naisten määrää. Se on osa laajempaa EU:n laajuista Women4Cyber-aloitetta ja keskittyy tukemaan monipuolisempaa ja osallistavampaa teollisuutta Suomessa. W4CFI osallistuu erilaisiin toimiin, mukaan lukien ohjeiden antaminen, tietämyksen vaihto ja tietoisuuden lisääminen, jotta voidaan lisätä ja tukea naisten osallistumista kyberturvallisuuteen. **Women4Cyber Suomi**

Liikenne- ja viestintäministeriö ja Aalto-yliopisto -hanke

Liikenne- ja viestintäministeriö kehittää yhteistyössä Aalto-yliopiston kanssa koulutuspakettia, jolla kyberturvallisuudesta tehdään kansalaisosaamista koko Euroopan unionissa. Aloitteessa korostetaan kyberturvallisuuden kasvavaa merkitystä jokapäiväisessä elämässä ja kaikkien kansalaisten, myös naisten, tietoisuuden ja taitojen tarvetta. Siinä korostetaan oppilaitosten roolia esteettömän kyberturvallisuuskoulutuksen tarjoamisessa, mikä on ratkaisevan tärkeää naisten vaikutusmahdollisuuksien lisäämiseksi alalla. Suomi edistää kyberturvallisuusosaamista koskevaa koulutusta EU:ssa. **Digitaalisten taitojen ja työpaikkojen foorumi** (europa.eu)

”Mimmit koodaa” (Naisten koodi) -liike

Tämä aloite tarjoaa työpajoja, koulutusta, verkostoitumismahdollisuuksia, webinaareja ja uratukea. Siinä keskitytään haastaviin stereotypioihin ja kannustetaan useampia naisia tutkimaan uraa tekniikassa, mukaan lukien kyberturvallisuus. Tämän organisaation tavoitteena on luoda polkuja, joilla naiset voivat tulla kyberturvallisuuden alalle ja menestyä siellä. **Mimmit koodaa**

Belgian kyberturvallisuusympäristössä naisten osuus työvoimasta on 19 prosenttia Agorian vuonna 2022 julkaiseman ensimmäisen Belgian kyberturvallisuusalaa koskevan sosioekonomisen tutkimuksen mukaan. Belgian talousministeriön (FPS Belgium) koordinoimana Belgian toimivaltaiset poliittiset toimijat ovat laatineet viisivuotissuunnitelman naisille digitaalialalla nimeltä ”Naiset digitaalisessa – kansallinen ja intersektionaalinen strategia 2021–2026”. Viisivuotissuunnitelmaan sisältyy yhteinen ja monialainen strategia, joka perustuu viiteen strategiseen tavoitteeseen, jotka ovat hyödyllisiä ennakkoluulojen torjumiseksi ja sellaisten rakenteellisten esteiden poistamiseksi, jotka estävät naisia osallistumasta digitaalitalouteen. Nämä viisi tavoitetta ovat seuraavat:

1. Varmistetaan, että naisia valmistuu enemmän digitaalialalla; 2. Kannustetaan kaikkia naisia osallistumaan digitaalisille työmarkkinoille ja/tai digitaalialalle; 3. Parannetaan naisten pysymistä digitaalialalla; 4. Uusien kuvien luominen naisten aseman edistämiseksi kentällä (näytöllä ja sen ulkopuolella) 5. Tiettyjen kohderyhmien välisen sukupuolten välisen kuilun kurominen umpeen (**yhteys strategiaan**).

Brysselissä toimiva Women4Cyber-säätiö järjestää ja tukee monenlaisia toimia, jotka on suunnattu naisille, jotka työskentelevät tai aloittavat uransa kyberturvallisuuden alalla Belgiassa ja Euroopassa. Belgiassa säätiö tukee Belgian kansallista lukua (Women4Cyber**Belgium**) ja tekee yhteistyötäsen kanssa. Belgian kansalliseen lukuun kuuluu noin 20 aktiivista jäsentä, jotka työskentelevät aloitteiden parissa. Luvun järjestämiä toimia, tapahtumia ja ohjelmia ovat muun muassa seuraavat: verkostoitumiskokoukset ja -tapahtumat (virtuaaliset ja henkilökohtaiset), kuten ”virtuaalinen kahvi”, jossa W4C Belgia -luku kutsuu keskustelemaan kyber- ja tietoturva-alan eri alojen asiantuntijoista; webinaarit ja tiedotustilaisuudet; mentorointiohjelmat, joiden tarkoituksena on auttaa naisia parantamaan taitojaan ja edistämään kyberturvallisuusuraansa kaikilla tasoilla; hankkeet ja tapahtumat yhteistyössä Belgian kyberturvallisuuskoalition kanssa (kuten **kansainvälisen naistenpäivän järjestäminen 2023**); edistetään stipendejä verkkoihin liittyviin koulutusohjelmiin, kuten Solvay Brussels School of Economics & Managementin järjestämiin koulutusohjelmiin.

Norjassa sukupuolten välisen kuilun poistaminen kyberturvallisuudessa on ratkaisevan tärkeää selviytymiskykyisen ja monipuolisen työvoiman rakentamiseksi. Naisten osuus IT:stä on vain 29 prosenttia. Pieni määrä on vahvasti yhteydessä niiden naisten määrään, jotka valitsevat matemaattisia ja teknisiä aiheita toissijaisella tasolla.

Koulutus- ja tukitarpeet ja suositukset naisten osallistamiseksi

Tarvitaan räätälöityjä kyberturvallisuusohjelmia, jotka on erityisesti suunniteltu kannustamaan naisten osallistumista. Näissä ohjelmissa olisi tasapainotettava tekniset näkökohdat organisatorisiin ja ihmiskeskeisiin kyberturvallisuuskysymyksiin. Alalla on useita teknisiä lisäkoulutuksia, kun taas tyypillisimmissä naisammateissa (pedagogisissa – terveysalan ammateissa) tarjottavat lisäkoulutustarjoukset eivät sisällä tällaisia tarjouksia, ja näihin ammatteihin liittyvän kyberturvallisuuden lyhyemmän koulutustarjonnan kehittäminen voisi tavoittaa enemmän naisia. Tätä tukee myös itse ala, jonka mukaan moninaisuus voi tuoda ainutlaatuisia näkökulmia kyberturvallisuushaasteisiin. Naisten tietoisuutta sisäisestä kyberturvallisuusurasta voitaisiin lisätä järjestämällä kouluissa ja yliopistoissa työpajoja, seminaareja ja kohdennettuja tiedotusohjelmia, jotka voivat innostaa useampia naisia tulemaan tälle alalle.

Toinen lähestymistapa, jota monet nimetyistä 50 parhaasta norjalaisesta naisesta 2022 ehdotti, on perustaa mentorointiohjelmia ja verkostoitumismahdollisuuksia naisille kyberturvallisuuden alalla, jotta he voivat tarjota olennaista ohjausta ja tukea sekä auttaa heitä navigoimaan ja etenemään tällä alalla.

Kyberturvallisuusala itse ehdottaa, että organisaatioiden olisi pantava täytäntöön osallistavia työhönottokäytäntöjä ja -politiikkoja, joilla kannustetaan aktiivisesti naisten rekrytointia ja pysymistä kyberturvallisuustehtävissä. 32 % naisista teknisissä rooleissa on usein ”ainoa nainen huoneessa” McKinseyn raportin mukaan ”Women in the Workplace 2022**.**

Lisäksi naisten edistäminen kyberturvallisuuden johtotehtävissä voi tarjota roolimalleja ja innostaa muita naisia toimimaan samanlaisilla poluilla, kuten esimerkiksi **Mia Landsem**.

Romaniassa kyberturvallisuus on edelleen yksi dynaamisimmista ja jännittävimmistä teknologian aloista. Tämä ala tarvitsee kuitenkin systeemistä muutosta naisten edustuksessa ja korvauksissa. Vaikka kiinnostus kyberturvallisuuteen on lisääntynyt, sukupuolten välinen ero on edelleen olemassa. Naiset ovat edelleen erittäin aliedustettuina, kun taas useimmat työpaikat ovat pääasiassa miehiä. Kyberturvallisuuden tulevaisuuteen vaikuttaa kyky houkutella, säilyttää ja edistää kyberalan ammattilaisia, myös enemmän naisia.

On tehty monia tutkimuksia, joiden tarkoituksena on osoittaa, miten aliarvioidut naiset ovat ympäri maailmaa, mutta myös saada kaikki ymmärtämään naisten merkitys kaikilla aloilla ja erityisesti kyberturvallisuudessa. Äärimmäinen sukupuoliero kyberturvallisuuden työntekijäpohjan välillä osoittaa, että muut työvoimat eivät ole tasa-arvoisia. Naisten osuus koko työvoimasta on 39 prosenttia. Niiden osuus STEM-alan työntekijöistä on 38 prosenttia, mutta vain noin 25 prosenttia kyberturvallisuusalan työntekijöistä Cybersecurity Venturesin mukaan.

On olemassa useita esteitä, jotka pitävät naiset poissa kyberturvallisuudesta. Kyberturvallisuuskoulutukseen ja -sertifiointiin keskittyvän voittoa tavoittelemattoman järjestön (ISC)2 tekemän tutkimuksen mukaan suurin osa alalla työskentelevistä naisista ilmoittaa sukupuoleen perustuvasta syrjinnästä. Lähes kaikki naiset (87 %) ilmoittivat kokeneensa tiedostamatonta syrjintää, kun taas 19 % ilmoitti joutuneensa avoimen syrjinnän kohteeksi. Naiset mainitsivat myös selittämättömiä viivästyksiä uralla etenemisessä (53 %) ja liioiteltuja vastauksia virheisiin (29 %).

Syrjintä ilmenee myös korvausvajeena. (ISC) 2 -tutkimus osoittaa, että 32 % kyberturvallisuuden parissa työskentelevistä miehistä ansaitsee keskimäärin 50,000–100,000 dollaria vuodessa, kun taas vain 18 % kyberturvallisuuden naisista käyttää samaa tuloluokkaa. Ja 25 % miehistä ja 20 % naisista ansaitsevat 100,000–500,000 dollaria vuodessa.

Naisten määrän lisäämiselle kyberturvallisuuden alalla on vahvoja perusteita, kuten monimuotoisuuden, innovoinnin, emotionaalisen empatian ja puolueettoman näkökulman edut, jotka kaikki ovat arvokkaita taitoja kyberturvallisuustyöpaikalle.

Women in Cybersecurity Boardin jäsen Jay Koehler antoi toisen käsityksen: ”Naiset putoavat pois, koska se on ”poikien” klubi, ja yhteenkuuluvuuden tunne on alhainen.” Tähän ongelmaan voidaan puuttua sitoutumalla ja vastuullisesti tarjoamaan psykologista turvallisuutta ja sukupuoliystävällistä työpaikkaa ja luomalla naisten verkostoja.

On toivoa, että kyberturvallisuus ei enää ole ”miesvaltainen ammatti”, vaan se on täynnä lahjakkaita ihmisiä, jotka edustavat kaikkia sukupuolia ja taustoja.

Kirjallisuutta naisten osallistumisesta kyberturvallisuuteen Espanjassa on niukasti. Suurin osa nykykirjallisuudesta osoittaa, että sukupuolten välinen epätasapaino laajemmassa tiedeyhteisössä, mukaan lukien STEM-alat, on selvästi vähentynyt naisten etenemisessä uran korkeammalle tasolle, jota pidetään yleisesti ”pipeline-ilmiönä”. Korkea-asteen koulutuksen osalta sukupuolten välinen ero on edelleen huomattava, sillä vain 18 prosenttia näiden aineiden opintoja suorittaneista on naisia. Naiset, jotka työskentelevät pk-yrityksissä I+D:hen liittyvissä tehtävissä, ovat edelleen hyvin pieniä, mutta eivät kansallisen tilastokeskuksen tietojen mukaan edes 30 prosenttia. Espanjassa toimivien korkea-asteen oppilaitosten kyberturvallisuutta käsittelevien naistutkijoiden osalta hyvin harvat heistä osoittavat, että henkilöstö on sukupuolijakaumaltaan tasapainoinen. *Fundación Alternativasin tarkastamista 31 korkeakoulusta 11:llä* ei ole naisia tutkimusryhmiinsä, ja vain viidessä heistä on tasa-arvoisempi työvoima. Näihin haasteisiin vastaamiseksi koulutus- ja tukitarveanalyysissa yksilöidään keskeiset parannuskohteet. Olisi kehitettävä aloitteita, joilla kannustetaan useampia naisia jatkamaan tohtoriopintoja ja varmistetaan tasapuolinen edustus koko koulutusketjun ajan. On ratkaisevan tärkeää puuttua vääristymiin urakehityksen prosesseissa, ja mentorointiohjelmilla voi olla keskeinen rooli naisten ohjaamisessa kyberturvallisuusalan monimutkaisuuden läpi. Lisäksi suositellaan yhteistyötä yksityisten teollisuuden organisaatioiden kanssa, jotta voidaan tutkia urapolkuja ja edistää naisten osallistumista kyberturvallisuusrooleihin yksityisellä sektorilla. Tutkintojen ja pätevyyksien arviointi korostaa räätälöityjen koulutusohjelmien merkitystä korostaen erityisiä kyberturvallisuustaitoja ja -osaamista.

2.3. ESCO-AMMATTIEN ANALYSOINTI

Tulkitsemme nykyistä ESCO-luokitusta (eurooppalainen monikielinen taito-, osaamis- ja ammattiluokitus), joka koskee tunnistettuja oppimistuloksia, mukaan lukien tiedot, taidot ja osaaminen. Tavoitteena on

- Analysoida kyberturvallisuuteen liittyviä ESCO:n nykyisiä ammatteja.
- Kartoitetaan yksilöidyt oppimistulokset ESCOn ammatteihin tietojen, taitojen, pätevyyksien jne. osalta.

Jokaisessa ammatissa on joukko osaamista, taitoja ja tietoja. Alla on lueteltu määritelmät ja esimerkkejä pätevyydestä, taidoista, tiedoista ja arvosta.

Osaamisella tarkoitetaan yksilön kykyä suorittaa tietty tehtävä tai tehtävä tehokkaasti. Se käsittää yhdistelmän tietoja, taitoja ja käyttäytymistä, joita sovelletaan suorituskyvyn parantamiseen. Esimerkki: Projektinhallinnan osaaminen edellyttää organisaatiotaitojen yhdistelmää, projektinhallintaprosessien tuntemusta ja kykyä kommunikoida tehokkaasti tiimin jäsenten kanssa.

Taidot ovat erityisiä kykyjä tai kykyjä, jotka on hankittu käytännön, koulutuksen tai kokemuksen avulla, joiden avulla yksilö voi suorittaa tehtäviä. Esimerkki: Penetraatiotestaustaidot, kyky käyttää kyberturvallisuustyökaluja ja -ohjelmistoja, ohjelmointitaidot sekä kyky analysoida ja reagoida uhkiin reaaliajassa.

Tieto viittaa tosiasioihin, tietoon ja ymmärrykseen, jotka on opittu koulutuksen tai kokemuksen kautta. Siihen sisältyy teoreettinen ymmärrys tosiasioista ja periaatteista, jotka liittyvät tiettyyn alaan. Esimerkki: Ymmärrys siitä, miten erilaisia kyberhyökkäyksiä tehdään (esim. tietojenkalastelu, kiristysohjelmat, DDoS-hyökkäykset) tai tietämys erilaisista salausmenetelmistä ja tieto kyberturvallisuuden uusimmista trendeistä ja kehityksestä.

Analyysi jakautuu kahteen vaiheeseen:

Vaihe 1: ESCO-ammattien tarkastelu ja valinta

ESCO-portaalin kuuleminen kyberturvallisuuteen liittyvien ammattien suodattamiseksi ja kunkin ammatin seuraavassa osiossa olevien asiakirjojen suodattamiseksi kiinnittäen erityistä huomiota lueteltuihin taitoihin, pätevyyteen ja tietämykseen.

ESCO:n ammattinimike	Tietämys	Taidot	Toimivalta
3512.3 – Tieto- ja viestintätekniikan turvallisuusteknikko	• Tieto- ja viestintätekniikan verkottuminen • laitteistohyökkäysvektorit • kyberhyökkäysten vastatoimet • ICT:n käyttöjärjestelmien hankinta • verkkolaitteet	• ratkaise ongelmat kriittisesti • tieto- ja viestintätekniikan järjestelmän analysointi • asiakirjojen asianmukaisen hallinnan varmistaminen	• integroi järjestelmäkomponentit • teknisen dokumentaation toimittaminen • ratkaise tieto- ja viestintätekniikan järjestelmäongelmia • käytä

	• Web-sovellus • turvallisuusuhat	• suorita ohjelmistotestejä tunnistaa tieto- ja viestintätekniikan järjestelmän heikkoudet	kulunvalvontaohjelmistoa
2529.1 – Tieto- ja viestintätekniikan turvallisuuspäällikkö – Sisältää yrityksen turvallisuustoimintoja suorittavat henkilöt.	• Tieto- ja viestintätekniikan verkkoturvallisuusriskit • Tieto- ja viestintätekniikan turvallisuutta koskeva lainsäädäntö • Tieto- ja viestintätekniikan turvallisuusstandardit • hyökkäysvektorit • tarkastustekniikat • kyberhyökkäysten vastatoimet • kyberturvallisuus • tietosuoja • päätöksenteon tukijärjestelmät • tietojen luottamuksellisuus • tietoturvastrategia • sisäinen riskienhallintapolitiikka • organisaation häiriönsietokyky	• kouluttaa tietojen luottamuksellisuutta • organisaation tieto- ja viestintätekniikan standardien noudattamisen varmistaminen • varmistetaan lakisääteisten vaatimusten noudattaminen • varmistetaan osastojen välinen yhteistyö • tietosuojan varmistaminen • tieto- ja viestintätekniikan turvallisuusriskien tunnistaminen • tieto- ja viestintätekniikan riskienhallinnan toteuttaminen • tieto- ja viestintätekniikan turvallisuuspolitiikan täytäntöönpano • toteuta hallinnointi- ja ohjausjärjestelmä	• johtaa katastrofien toipumisharjoituksia • ylläpidettävä suunnitelma toiminnan jatkuvuudesta • IT-turvallisuusvaatimusten hallinta • hallinnoi katastrofien toipumissuunnitelmia • asiantuntija-alan kehityksen seuranta • seuraa teknologian trendejä hyödynnä päätöksenteon tukijärjestelmää
2529.2 – digitaalisen rikostutkinnan asiantuntija – hakee ja analysoi tietoja tietokoneista ja muuntyyppisistä tiedontallennuslaitteista; tutkii digitaalista mediaa, joka on saattanut olla piilossa, salattu tai vahingoittunut, rikosteknisellä tavalla tarkoituksena tunnistaa, säilyttää, palauttaa, analysoida ja esittää tosiasioita ja mielipiteitä digitaalisesta tiedosta.	• Tieto- ja viestintätekniikan verkkoturvallisuusriskit • Tieto- ja viestintätekniikan turvallisuusstandardit • tietokoneiden rikostekninen tutkimus • kyberhyökkäysten vastatoimet • tietojen luottamuksellisuus • penetraatiotestaustyökalu • hakukielet • Resurssikuvauskehyskyselyn kieli	• soveltaa käänteissuunnittelua • kehittää tietoturvastrategiaa • kouluttaa tietojen luottamuksellisuutta • tietojen kerääminen rikosteknisiin tarkoituksiin • tieto- ja viestintätekniikan turvallisuusriskien tunnistaminen • tunnista tieto- ja viestintätekniikan järjestelmän heikkoudet • tieto- ja viestintätekniikan verkkodiagnostiikkatyöka	• IT-turvallisuusvaatimusten hallinta • oikeudellisten asioiden tietojen hallinta • suorita digitaalisten laitteiden rikosteknisiä säilömyksiä

		lujen käyttöönotto • antaa tieto- ja viestintätekniikan konsultointineuvontaa • suojaa arkaluontoiset asiakkaan tiedot • käytä komentosarjaohjelmointia • käytä ohjelmistoja tietojen säilyttämiseen • suorita tieto- ja viestintätekniikan turvallisuustestaus	
2529.3 – sulautettujen järjestelmien tietoturvainsinööri – sulautettujen järjestelmien tietoturvainsinöörien painopiste on verkkoon liitetyissä tuotteissa ja niitä tukevissa verkoissa ja vähemmän organisatorisessa tietoturvassa, kuten tieto- ja viestintätekniikan tietoturvainsinöörissä.	• Tieto- ja viestintätekniikan verkkoturvallisuusriskit • Tieto- ja viestintätekniikan turvallisuusstandardit • Esineiden internet • tietokoneohjelmointi • kyberhyökkäysten vastatoimet • sulautetut järjestelmät • tietoturvastrategia • ohjelmistojen poikkeamat	• tieto- ja viestintätekniikan järjestelmän analysointi • luo vuokaaviokaavio • määritä turvallisuuskäytännöt • kehitä tieto- ja viestintätekniikan laiteohjainta • kehitä ohjelmistoprototyyppiä • suorita ohjelmistotestejä • tieto- ja viestintätekniikan turvallisuusriskien tunnistaminen • tunnista tieto- ja viestintätekniikan järjestelmän heikkoudet • teknisten tekstien tulkinta • antaa tieto- ja viestintätekniikan konsultointineuvontaa • suorita tieto- ja viestintätekniikan turvallisuustestaus • teknisen dokumentaation toimittaminen	• pysy ajan tasalla uusimmista tietojärjestelmäratkaisuista • IT-turvallisuusvaatimusten hallinta • seuraa järjestelmän suorituskykyä • riskianalyysin tekeminen • raportti testituloksista käyttää ohjelmistosuunnittelumalleja • käytä ohjelmistokirjastoja • tietokoneavusteisten ohjelmistojen suunnittelutyökalujen hyödyntäminen • määritä tekniset vaatimukset
2529.4 – eettinen hakkeri – suorittaa turvallisuuden haavoittuvuusarviointeja ja tunkeutumistestejä alan hyväksymien menetelmien ja protokollien	• hyökkäysvektorit • tietokoneiden rikostekninen tutkimus • kyberhyökkäysten vastatoimet • etiikkaa • Tieto- ja viestintätekniikan tuotteiden oikeudelliset vaatimukset	• suorita tieto- ja viestintätekniikan turvallisuustestaus • teknisen dokumentaation toimittaminen • kehitä koodin hyödyntämistä • TVT-auditointien	• ratkaise ongelmat kriittisesti • organisaation kontekstin analysointi • seuraa järjestelmän suorituskykyä

mukaisesti; analysoi järjestelmiä sellaisten mahdollisten haavoittuvuuksien varalta, jotka voivat johtua järjestelmän epäasianmukaisista konfiguraatioista, laitteisto- tai ohjelmistovirheistä tai toiminnallisista heikkouksista.	• penetraatiotestaustyökalu • ohjelmistojen poikkeamat • ICT-testiautomaation työkalut • Web-sovellusten turvallisuusuhat	toteuttaminen • suorita ohjelmistotestejä • tieto- ja viestintätekniikan turvallisuusriskien tunnistaminen • tunnista tieto- ja viestintätekniikan järjestelmän heikkoudet	
2529.5 – Tieto- ja viestintätekniikan häiriönsietokyvyn johtaja – tutkii, suunnittelee ja kehittää malleja, toimintaperiaatteita, menetelmiä, tekniikoita ja välineitä, jotka parantavat organisaation kyberturvallisuutta, selviytymiskykyä ja palautumista katastrofista	• Tieto- ja viestintätekniikan talteenottotekniikat • kyberturvallisuus sisäinen • riskienhallintapolitiikka • organisaation häiriönsietokyky • järjestelmän varmuuskopiointi paras käytäntö	• valmiussuunnitelmien laatiminen hätätilanteita varten • kehittää tietoturvastrategiaa • TVT-auditointien toteuttaminen • tieto- ja viestintätekniikan turvallisuusriskien tunnistaminen • ICT-elvytysjärjestelmän käyttöönotto • tieto- ja viestintätekniikan riskienhallinnan toteuttaminen	• liiketoimintaprosessien analysointi • organisaation kontekstin analysointi • noudata lakisääteisiä määräyksiä • johtaa katastrofien toipumisharjoituksia • IT-turvallisuusvaatimusten hallinta • hallinnoi katastrofien toipumissuunnitelmia • järjestelmän turvallisuuden hallinta • suorita tieto- ja viestintätekniikan turvallisuustestaus
2529.6 – Tieto- ja viestintätekniikan turvallisuusvastaava – suunnittelee ja toteuttaa turvatoimia tietojen ja tietojen suojaamiseksi luvattomalta käytöltä, tahalliselta hyökkäykseltä, varkauksilta ja korruptiolta.	• Tieto- ja viestintätekniikan verkkoturvallisuusriskit • Esineiden internet • kyberhyökkäysten vastatoimet • tietokannan kehittämistyökalut • internetin hallinto • mobiililaitteiden hallinta • käyttöjärjestelmät • organisaation häiriönsietokyky • laadunvarmistusmenetelmät • järjestelmän varmuuskopiointi paras käytäntö	• tunnista tieto- ja viestintätekniikan järjestelmän heikkoudet • teknisten tekstien tulkinta • ylläpitää ICT-identiteetin hallintaa • ylläpidä tietokannan turvallisuutta	• noudata yrityksen käytäntöjä • huolehdi tieto- ja viestintätekniikan järjestelmien laadusta • asiakirjojen asianmukaisen hallinnan varmistaminen • ICT-tietoarkkitehtuurin hallinta • IT-turvallisuusvaatimusten hallinta • suorita tieto- ja viestintätekniikan vianmääritys • ratkaise tieto- ja viestintätekniikan järjestelmäongelmia
2529.7 – Tieto- ja viestintätekniikan tietoturvainsinööri – neuvoo ja toteuttaa ratkaisuja, joilla hallitaan tietojen ja ohjelmien	• Tieto- ja viestintätekniikan turvallisuutta koskeva lainsäädäntö • Tieto- ja viestintätekniikan turvallisuusstandardit • hyökkäysvektorit • liiketoiminta-analyysi	• kehittää tietoturvastrategiaa • kouluttaa tietojen luottamuksellisuutta • tietoturvan varmistaminen • TVT-auditointien	• määritä tietojen laatukriteerit • määritä tekniset vaatimukset • pidä tehtävätietueita • pysy ajan tasalla uusimmista

saatavuutta ja varmistetaan organisaation tehtävien ja liiketoimintaprosessien suojaaminen.	• kyberhyökkäysten vastatoimet • kyberturvallisuus • kehitteillä olevat teknologiat • tietoarkkitehtuuri • tietoturvastrategia • käyttöjärjestelmät • organisaation häiriönsietokyky • riskienhallinta • strukturoimaton data	toteuttaminen • suorita ohjelmistotestejä • tieto- ja viestintätekniikan turvallisuusriskien tunnistaminen • tunnista tieto- ja viestintätekniikan järjestelmän heikkoudet • tieto- ja viestintätekniikan riskienhallinnan toteuttaminen • antaa tieto- ja viestintätekniikan konsultointineuvontaa • tieto- ja viestintätekniikan järjestelmän analysointi • määritä turvallisuuskäytännöt	tietojärjestelmäratkaisuista • IT-turvallisuusvaatimusten hallinta • hallinnoi katastrofien toipumissuunnitelmia • seuraa järjestelmän suorituskykyä • suorita tietojen analysointi • riskianalyysin tekeminen • raportoi testitulosten vianmääritys • tarkista viralliset tieto- ja viestintätekniikan eritelmät
2529.8 – Tieto- ja viestintätekniikan turvallisuuspäällikkö – ehdottaa ja toteuttaa tarvittavat tietoturvapäivitykset; neuvoo, tukee, informoi ja tarjoaa koulutusta ja turvallisuutta koskevaa tietoisuutta ja ryhtyy suoraan toimiin koko verkossa tai järjestelmässä tai sen osassa.	• Tieto- ja viestintätekniikan ongelmanhallintatekniikat • Tieto- ja viestintätekniikan projektinhallinta • Tieto- ja viestintätekniikan laatupolitiikka • Tieto- ja viestintätekniikan turvallisuusstandardit • Tieto- ja viestintätekniikan järjestelmän käyttäjävaatimukset • Esineiden internet • hyökkäysvektorit • tietokoneiden rikostekninen tutkimus • tietoturvastrategia • sisäinen riskienhallintapolitiikka • internetin hallinto • Tieto- ja viestintätekniikan tuotteiden oikeudelliset vaatimukset	• määritä turvallisuuskäytännöt • kehittää tietoturvastrategiaa • laaditaan tieto- ja viestintätekniikan turvallisuusehkäisysuunnitelma • tieto- ja viestintätekniikan riskienhallinnan toteuttaminen	• johtaa katastrofien toipumisharjoituksia • ylläpitää ICT-identiteetin hallintaa • IT-turvallisuusvaatimusten hallinta • hallinnoi katastrofien toipumissuunnitelmia • ratkaise tieto- ja viestintätekniikan järjestelmäongelmia
2529.9 – Tietoinsinööri – integroi jäsennellyn tiedon tietojärjestelmiin (tietopohjat) monimutkaisten ongelmien ratkaisemiseksi, jotka yleensä edellyttävät korkeatasoista	• liiketoimintatiedustelu • liiketoimintaprosessien mallintaminen • tietokannan kehittämistyökalut • tiedonhaku • tietorakenteen luonnollisen kielen käsittely • tekoälyn periaatteet	• käytä sovelluskohtaista rajapintaa • tietokantojen käyttö • käytä merkintäkieliä	• analysoida liiketoiminnan vaatimuksia • soveltaa ICT-järjestelmien teoriaa • TVT-osaamisen arviointi • luo semanttisia puita • määritä tekniset vaatimukset • hallitse tieto- ja viestintätekniikan

inhimillistä asiantuntemusta tai tekoälymenetelmiä.	• Resurssikuvauskehyskyselyn kieli • järjestelmien kehittäminen elinkaari • systeemiteoria • tehtävien algoritmisointi • Web-ohjelmointi		semanttista integraatiota • hallitse liiketoiminnan osaamista • hallinnoi tietokantaa

Vaihe 2: ESCO Ammatti- ja oppimistulosten kartoitus

Edellisessä taulukossa analysoimme dokumentoituja ammatteja ja yksilöimme kuhunkin rooliin liittyvät oppimistulokset. Käytimme ESCO-kehystä luokitellaksemme nämä tulokset tietoiksi, taidoiksi ja kompetensseiksi.

Oppimistulos on selkeä ja täsmällinen lausunto, joka kuvaa, mitä opiskelijoiden odotetaan oppivan ja kykenevän tekemään opetusjakson päätyttyä. Lausunto sisältää tietoa, taitoja ja asenteita.

ESCO-ammattiluokittelijan osio Tieto- ja viestintätekniikan ammattilaiset jakautuvat kahteen alajaksoon: Ohjelmistojen ja sovellusten kehittäjät ja analyysit sekä tietokannan ja verkon ammattilaiset. Viimeinen ryhmä koostuu neljästä ryhmästä: Tietokanta- ja verkkoammattilaiset, järjestelmien ylläpitäjät, tietokoneverkon ammattilaiset sekä tietokannan ja verkon ammattilaiset, jotka eivät ole muualla luokiteltuja. Kaikki taulukossa esitetyt kyberturvallisuusammatit löytyivät tästä yksiköstä. Konserniin kuuluu esimerkiksi tieto- ja viestintätekniikan tietoturva-asiantuntijoita.

Tällaisissa tapauksissa tehtäviin kuuluisi:

a) sellaisten suunnitelmien laatiminen, joilla suojataan tietokonetiedostot vahingossa tapahtuvalta tai luvattomalta muuttamiselta, tuhoamiselta tai luovuttamiselta ja vastataan kiireellisiin tietojenkäsittelytarpeisiin.

b) käyttäjien kouluttaminen ja tietoturvatietoisuuden edistäminen järjestelmän turvallisuuden varmistamiseksi sekä palvelinten ja verkon tehokkuuden parantamiseksi.

C) antamalla käyttäjille mahdollisuus keskustella esimerkiksi tietokoneen datan käyttötarpeista, tietoturvaloukkauksista ja ohjelmointimuutoksista.

D) tietokoneviruksia koskevien nykyisten raporttien seuranta sen määrittämiseksi, milloin virustorjuntajärjestelmiä päivitetään.

(E) tietokoneen suojaustiedostojen muokkaaminen uuden ohjelmiston sisällyttämiseksi, virheiden korjaaminen tai yksittäisen käyttöoikeuden tilan muuttaminen.

F) tietotiedostojen käytön seuranta ja tietojen suojaaminen tietokonetiedostoissa.

g) riskinarviointien tekeminen ja tietojenkäsittelyjärjestelmän testien suorittaminen tietojenkäsittelytoimien ja turvatoimien toimivuuden varmistamiseksi.

h) salataan tiedonsiirtoja ja asennetaan palomuureja luottamuksellisten tietojen salaamiseksi, kun niitä lähetetään, ja väärien digitaalisten siirtojen estämiseksi.

Kuvaus kunkin ammatin oppimistuloksista:

Miehitys	Oppimistulokset
Tieto- ja viestintätekniikan turvallisuusteknikko (3512.3)	• Osoittaa kattava ymmärrys tieto- ja viestintätekniikan verkkojen, laitteisto-hyökkäysten vektoreista, kyberhyökkäysten vastatoimista ja käyttöjärjestelmistä. • Analysoida ja diagnosoida kriittisesti tieto- ja viestintäteknisten järjestelmien haavoittuvuuksia järjestelmän turvallisuuden parantamiseksi. • Toteuttaa ja hallita vankkoja asiakirjojen hallintastrategioita, jotka noudattavat tieto- ja viestintätekniikan turvallisuusprotokollia. • Kehittää ja toteuttaa yksityiskohtaisia ohjelmistotestaussuunnitelmia ohjelmiston haavoittuvuuksien tunnistamiseksi ja korjaamiseksi. • Integroi järjestelmäkomponentit ja käytä kulunvalvontaohjelmistoa turvallisten ja tehokkaiden tieto- ja viestintäteknisten järjestelmien rakentamiseksi.
Tieto- ja viestintätekniikan turvallisuuspäällikkö (2529.1)	• Ymmärtää ja analysoida tieto- ja viestintätekniikan tietoturvariskejä, lainsäädäntöä ja standardeja organisaation tietojen suojaamiseksi. • Kehittää ja toteuttaa tietoturvastrategioita ja sisäisiä riskienhallintakäytäntöjä. • Johtaa katastrofien toipumisharjoituksia ja ylläpitää toiminnan jatkuvuutta koskevia suunnitelmia. • Koulutetaan henkilöstöä tietojen luottamuksellisuudesta ja varmistetaan osastojen välinen yhteistyö turvallisuuskäytäntöjen parantamiseksi.
Digitaalisen rikostutkinnan asiantuntija (2529.2)	• Analysoida ja testata sulautettujen järjestelmien turvallisuutta, erityisesti esineiden internetin (IoT) ympäristössä. • Ohjelmistojen prototyyppien ja testien kehittäminen ja toteuttaminen sekä tietokonevasteisten ohjelmistojen suunnittelutyökalujen hyödyntäminen. • Hallitse tietoturvavaatimusten noudattamista ja suorita riskianalyysi ja järjestelmän suorituskyvyn seuranta. • Määritellä ja toteuttaa sulautettujen järjestelmien turvallisuuskäytäntöjä ja teknisiä vaatimuksia.
Sulautettujen järjestelmien turvallisuusinsinööri	• Analysoida ja testata sulautettujen järjestelmien turvallisuutta, erityisesti esineiden internetin

(2529.3)	(IoT) ympäristössä. • Ohjelmistojen prototyyppien ja testien kehittäminen ja toteuttaminen sekä tietokoneavusteisten ohjelmistojen suunnittelutyökalujen hyödyntäminen. • Hallitse tietoturvavaatimusten noudattamista ja suorita riskianalyysi ja järjestelmän suorituskyvyn seuranta. • Määritellä ja toteuttaa sulautettujen järjestelmien turvallisuuskäytäntöjä ja teknisiä vaatimuksia.
Eettinen hakkeri (2529.4)	• Suorittaa tietoturvahaavoittuvuusarviointeja ja tunkeutumistestausta alan hyväksymin menetelmin. • Tunnistaa ja hyödyntää järjestelmien mahdollisia haavoittuvuuksia turvallisuustoimenpiteiden parantamiseksi. • Kehitetään koodia, jossa hyödynnetään ja toteutetaan tieto- ja viestintätekniikan auditointeja järjestelmän eheyden varmistamiseksi. • Analysoida organisaation kontekstia, jotta turvallisuusstrategiat voidaan räätälöidä tehokkaasti
ICT Resilience Manager (2529.5)	• Laadittava ja pantava täytäntöön valmiussuunnitelmat ja tietoturvastrategiat hätäskenaarioita varten. • Tieto- ja viestintätekniikan hyödyntämisjärjestelmien ja riskienhallintaprosessien toteuttaminen ja hallinta. • Johtaa katastrofien toipumisharjoituksia ja hallita järjestelmän turvallisuutta kriisien aikana. • Analysoi liiketoimintaprosesseja organisaation häiriönsietokyvyn ja lakisääteisten määräysten noudattamisen parantamiseksi.
ICT Security Administrator (2529.6)	• Suunnitella ja toteuttaa turvatoimenpiteitä tietojen suojaamiseksi ja ICT-identiteettijärjestelmien hallinnoimiseksi. • Ylläpidetään tietokantojen turvallisuutta ja varmistetaan järjestelmän eheys ja häiriönsietokyky. • Ratkaista ICT-järjestelmän ongelmia ja suorittaa vianmääritys- ja laadunvarmistusmenetelmiä. • Hallitse tietoarkkitehtuuria ja noudata organisaation tietosuojakäytäntöjä.
Tieto- ja viestintätekniikan turvallisuusinsinööri (2529.7)	• Neuvoo ja toteuttaa ratkaisuja, joilla hallitaan tietojen saatavuutta ja suojataan liiketoimintaprosesseja. • Analysoida tieto- ja viestintäteknisiä järjestelmiä ja määritellä turvallisuuspolitiikat ja tietojen

	laatukriteerit. • Suorita tietojen analysointi ja riskianalyysi ja hallinnoi tietoturvavaatimusten noudattamista ja katastrofien palautumissuunnitelmia. • Pysy ajan tasalla kehittymässä olevista teknologioista ja tietojärjestelmien ratkaisuista
Tieto- ja viestintätekniikan turvallisuuspäällikkö (2529.8)	• Ehdottaa ja toteuttaa tietoturvapäivityksiä ja hallita tieto- ja viestintätekniikan turvallisuutta eri hankkeissa. • Johtaa katastrofien toipumisharjoituksia ja laatia tieto- ja viestintätekniikan turvallisuussuunnitelmia. • Ylläpitää ja hallita ICT-identiteetin hallintajärjestelmiä ja ratkaista monimutkaisia järjestelmäongelmia. • Kehittää ja toteuttaa tietoturvastrategioita ja hallinnoida katastrofien palautumissuunnitelmia.
Tietoinsinööri (2529.9)	• Integroi jäsennelty tieto tietojärjestelmiin käyttämällä kehittyneitä työkaluja, kuten RDF-kyselykieltä ja web-ohjelmointia. • Hallitse semanttisia integraatio- ja tietokantajärjestelmiä liiketoiminnan tietämyksen hallinnan parantamiseksi. • Analysoida liiketoiminnan vaatimuksia ja soveltaa ICT-järjestelmien teoriaa kehittää tehokkaita tietokantoja. • Luodaan semanttisia puita ja arvioidaan tieto- ja viestintätekniikan osaamista monimutkaisten ongelmien ratkaisemiseksi tekoälymenetelmien avulla.

3. ANALYYSIT JA SELVITYKSET

3.1. KENTTÄTUTKIMUKSEN ANALYYSI

Ammatillisen koulutuksen ja korkeakoulun kenttätutkimusanalyysi

Pk-yritysten kyberturvallisuuden muutosagenttien koulutustarpeiden kartoitus (Mapping the Training Needs for SME Cyber Security Change Agents) sisältää useita kysymyksiä, joissa keskitytään kyberturvallisuuskoulutukseen ammatillisen koulutuksen ja korkea-asteen koulutuksen yhteydessä. Keräsimme tietoa kyberturvallisuuskoulutukseen, opetusmenetelmiin, sukupuolen osallistavuuteen ja vastaajien väestökehitykseen liittyvistä aiheista.

Tämän tutkimuksen tavoitteena on analysoida vastauksia, joiden avulla voidaan ymmärtää kyberturvallisuuskoulutuksen nykytila, käytetyt menetelmät sekä käsitykset osallistavuudesta ja tehokkuudesta tällä alalla.

Vastausanalyysi perustuu seuraavaan keskeiseen rakenteeseen:

- Väestö
- Opetussuunnitelma, koulutustarpeet ja oppimismieltymykset
- Osaamisvaatimukset ja tulevaisuuden taidot
- Sukupuolikohtaiset näkemykset

Väestörakenne:

Kyselyyn vastanneiden sukupuolijakauma ammatillisen koulutuksen oppilaitosten ja korkeakoulujen välillä on seuraava:

Vastaajien kokonaismäärä laitostyypeittäin

Laitoksen tyyppi	Vastauksia	Naaras	Uros	Mieluummin olla sanomatta
Korkeakoulut (korkea-asteen oppilaitokset)	104	28	73	3
Ammatillinen koulutus (ammatillinen koulutus)	86	36	48	2
Yhteensä	**190**	**64**	**121**	**5**

Sukupuolten välinen epätasapaino on sekä korkeakouluissa että ammatillisissa oppilaitoksissa, mutta ero on pienempi ammatillisissa oppilaitoksissa. Jotta saadaan selkeämpi kuva sukupuolten edustuksesta suhteessa kunkin toimielimen vastausten kokonaismäärään ja mukautetaan tuloksia vastausten puolueellisuuden osalta, tilintarkastustuomioistuin on laskenut kunkin sukupuolen prosenttiosuuden molemmissa laitostyypeissä.

Vastaajien jakautuminen laitostyypeittäin

Laitoksen tyyppi	Naisten osuus %	Miesten %	En halua sanoa %	Yhteensä
Korkeakoulut (korkea-asteen oppilaitokset)	27	70	3	**100 %**
Ammatillinen koulutus (ammatillinen koulutus)	42	56	2	**100 %**

Vastausharhalla oikaistu analyysi vahvistaa, että vaikka molempien laitostyyppien osuus miesvastaajista on suurempi, ero miesten ja naisten välillä on edelleen pienempi ammatillisen koulutuksen oppilaitoksissa. Syy voi olla monipuolinen (esim. kulttuuriset, rakenteelliset tai poliittiset tekijät, jotka vaikuttavat sukupuolten monimuotoisuuteen kyberturvallisuuskasvatuksessa kaikissa näissä oppilaitoksissa). Naisvastaavien suurempi osuus ammatillisessa koulutuksessa viittaa mahdollisiin aloihin, joilla voitaisiin tutkia tarkemmin käytäntöjä, jotka tukevat sukupuolinäkökohdat huomioon ottavampaa toimintaympäristöä ammatillisessa koulutuksessa kuin korkea-asteen koulutuksessa.

Opetussuunnitelma, koulutustarpeet ja oppimismieltymykset

Korkeakoulujen ja ammatillisen koulutuksen nykyisiin kyberturvallisuuskoulutuksiin sisältyvät aiheet

Aihe	Vastauksia	HEI	ELÄINLÄÄKÄRI
Kyberturvallisuuden perusteet	151	90	61
Verkon turvallisuus	123	72	51
Uhka-analyysi ja -hallinta	99	65	34
Salaus	92	57	35
Häiriötilanteisiin reagoiminen	82	49	33
Riskienhallinta	77	43	34
Kyberturvallisuuslait ja -politiikat	73	42	31
Kehittyneet uhkien lieventämistekniikat	54	33	21

Vaikuttaa siltä, että perustiedot ja taidot sekä verkon turvallisuus ovat etusijalla. Uhka-analyysi ja -hallinta, kryptografia ja vaaratilanteiden reagointi viittaavat siihen, että koulutuksessa käsitellään kattavasti kyberturvallisuusuhkia. Riskienhallintaa ja kyberturvallisuutta koskevat lait ja politiikat, vaikka ne osoittavat, että tarvitaan kokonaisvaltainen lähestymistapa, johon sisältyy oikeudellisen kontekstin ymmärtäminen ja riskien tehokas hallinta, ei aina ole valittu. On mielenkiintoista huomata, että kehittyneitä uhkien lieventämistekniikoita on vähemmän mukana koulutuksissa.

Jotta tulokset saatiin ilman kunkin laitostyypin (korkeakoulujen ja ammatillisen koulutuksen) vastaajien määrää, tiedot normalisoitiin kunkin laitostyypin vastausten kokonaismäärällä. Tämän lähestymistavan avulla voimme nähdä niiden laitosten osuuden, jotka sisällyttävät kunkin aiheen kyberturvallisuutta koskeviin koulutusohjelmiinsa.

Aiheet	HEI Proportion	Ammatillisen koulutuksen osuus
Kyberturvallisuuden perusteet	15,76 %	15,48 %
Verkon turvallisuus	12,61 %	12,94 %
Uhka-analyysi ja -hallinta	11,38 %	8,63 %
Salaus	9,98 %	8,88 %
Häiriötilanteisiin reagoiminen	8,58 %	8,38 %
Riskienhallinta	7,53 %	8,63 %
Kyberturvallisuuslait ja -politiikat	7,36 %	7,87 %
Kehittyneet uhkien lieventämistekniikat	5,78 %	5,33 %

Mielenkiintoista on, että on olemassa samanlaisia prioriteetteja, joissa on pieniä vaihteluja. Sekä korkeakoulut että ammatilliset oppilaitokset korostavat merkittävästi kyberturvallisuuden perusteita ja verkkoturvallisuutta. Tämä osoittaa, että nämä aiheet tunnustetaan kyberturvallisuuskasvatuksen kriittisiksi komponenteiksi. Osuudet vastaavat läheisesti toisiaan, ja korkea-asteen oppilaitoksissa korostetaan hieman enemmän ”kyberturvallisuuden perusteita” kuin ammatillisissa oppilaitoksissa ja ”verkkoturvallisuus” on samanlainen, mutta kuilu on kapeampi.

Erikoistuneiden aiheiden, kuten ”Threat Analysis and Management”, ”kryptografia” ja ”Advanced threat lievitystekniikat”, painotus vaihtelee huomattavasti. Korkea-asteen oppilaitokset kohdistavat yleensä hieman suuremman osan koulutusohjelmistaan näihin aiheisiin kuin ammatilliseen koulutukseen. Tämä selittyy sillä, että korkea-asteen oppilaitokset keskittyvät tarjoamaan kattavampaa ja teoriaan perustuvaa käsitystä kyberturvallisuudesta, johon sisältyy usein laajempi valikoima erikoistuneita aiheita. Vaikka ammatilliset oppilaitokset käsittelevät edelleen monia aiheita, ne voivat asettaa etusijalle käytännön sovellukset ja välittömän työvalmiuden.

Opetusmenetelmät

Opetusmenetelmät	HEI Proportion	Ammatillisen koulutuksen osuus
Tapaustutkimukset	60,91 %	39,09 %
Ryhmähankkeet	58,95 %	41,05 %
Käytännön laboratoriot	59,02 %	40,98 %
Luentoja	56,97 %	43,03 %
Käännetty luokkahuone	34,78 %	65,22 %
Online-simulaatiot	51,35 %	48,65 %

Case Studies, Group Projects, Hands-on Labs, Lectures menetelmiä käytetään laajalti molemmissa laitostyypeissä, ja etusijalla korkeakouluissa kuin ammatillisessa koulutuksessa. Käännetyn luokkahuonemenetelmän osalta se on yleisempää ammatillisessa koulutuksessa (65,22 %) kuin korkeakouluissa (34,78 %), mikä osoittaa, että ammatillisen koulutuksen vuorovaikutteinen oppimismalli on halukas. Käännetyissä luokkahuoneissa asetetaan etusijalle aktiivinen oppiminen ja opiskelijoiden sitoutuminen, jotka sopivat hyvin ammatillisen koulutuksen käytännönläheiseen ja taitoihin perustuvaan lähestymistapaan.

Opetusmenetelmien tehokkuus

Opetusmenetelmä	Laske
Käytännön harjoitukset	141
Henkilökohtaiset työpajat	134
Vuorovaikutteiset simulaatiot	104
Verkkokurssit	100
Opetusvideota	73
Webinaarit	68

Tässä yleiskatsauksessa korostetaan erilaisten opetusmenetelmien moninaisuutta, mutta painotetaan selkeästi käytännöllisiä, vuorovaikutteisia ja joustavia oppimiskokemuksia. Käytännön harjoitteluistunnot ja henkilökohtaiset työpajat ovat erittäin arvostettuja, koska ne tarjoavat interaktiivisen ja käytännöllisen oppimiskokemuksen. Interaktiiviset simulaatiot ja verkkokurssit saivat myös merkittäviä mainintoja esteettömien oppimistapojen merkityksestä.

Koulujen kohtaamat haasteet.

Kun kysytään koulujen suurimmista haasteista, tässä on yhteenveto toistuvimmista aiheista:

- **Osallistujien taitojen ja kokemusten moninaisuus**: Kouluttajilla on vaikeuksia, jotka johtuvat osallistujien erilaisista taustoista ja asiantuntemuksen tasosta. Koulutuksen räätälöinti koko ryhmälle ja sen varmistaminen, että sekä tekniset että ei-tekniset henkilöt voivat hyötyä istunnoista, on haastavaa.
- **Kurssimateriaalin pitäminen ajan tasalla**: Kyberturvallisuusuhkien nopea kehitys edellyttää koulutusmateriaalien ja opetusmenetelmien jatkuvaa päivittämistä relevanssin varmistamiseksi.
- **Käytännön harjoittelun rajoitukset**: Käytännön kokemuksen tarjoamisessa on suuri haaste. Rajoituksia ovat riittämättömät laboratoriotilat, reaalimaailman simulointivalmiuksien puute ja vaikeus luoda realistisia kyberhyökkäysskenaarioita käytännössä.
- **Resurssien rajoitukset**: Kouluttajien on usein kohdattava rajalliset taloudelliset resurssit, pätevän henkilöstön puute, vanhentuneet oppimateriaalit ja riittämättömät laitteisto- ja ohjelmistotyökalut, joita tarvitaan tehokkaaseen koulutukseen.
- **Opiskelijan sitoutuminen ja motivaatio**: Opiskelijoiden huomion säilyttäminen ja motivoiminen osallistumaan aktiivisesti oppimiseen on vaikeaa, varsinkin kun on tarpeen kattaa monimutkainen ja joskus kuiva tekninen sisältö.
- **Opetussuunnitelma ja koulutusrakenne**: Tarvitaan kattavia ja monialaisia opetussuunnitelmia, jotka kattavat kaikki kyberturvallisuuteen liittyvät näkökohdat. Lisäksi kyberturvallisuuden sisällyttäminen opetussuunnitelmaan erityisesti lukion tasolla on edelleen merkittävä haaste.
- **Pääsy ajantasaisiin työkaluihin ja teknologioihin**: Opiskelijoiden pääsy uusimpiin kyberturvallisuustyökaluihin ja -teknologioihin käytännön oppimiseen on usein haastavaa, mikä on ratkaisevan tärkeää käytännön ymmärryksen kannalta.
- **Kieli- ja lokalisointikysymykset**: Kyberturvallisuusresursseja ei välttämättä ole aina saatavilla opiskelijoiden äidinkielillä, mikä lisää monimutkaisuutta koulutukseen muilla kuin englanninkielisillä alueilla.
- **Teollisuuden ja koulutuksen yhteensovittaminen**: Haasteena on tasapainottaa tarve opettaa teoreettista perustaa ja käytännön taitoja, jotka vastaavat alan tarpeita. On myös välttämätöntä valmistaa opiskelijoita työmarkkinoille asiaankuuluvilla taidoilla.

- **Opettajien valmiudet ja kehittäminen**: On ratkaisevan tärkeää mutta haastavaa varmistaa, että opettajilla on ajantasaista tietoa ja että he pystyvät tehokkaasti välittämään moni-mutkaisia käsitteitä.

Mukauttaminen pk-yritysten erityistarpeisiin

Vastausvaihtoehto	Laske
Neutraali	82
Linjassa	67
Hieman linjaamaton	19
Hyvin linjassa	17
Ei sovitettu yhteen	5

Suurin osa vastauksista osoittaa, että yhdenmukaistaminen on neutraalia, mikä viittaa siihen, että tässä kohdassa on parantamisen varaa. Merkittävä määrä vastaajia arvosteli ohjelmiaan yhdenmukaisiksi, kun taas hyvin harvat kouluttajat uskovat, että heidän ohjelmansa ovat hyvin yhdenmukaisia tai eivät ole linjassa alan tarpeiden kanssa. Asteikon alapäässä olevat vastaukset (ei ole yhdenmukaisia ja hieman yhdenmukaisia) heijastavat huolenaiheita tai haasteita, jotka liittyvät koulutussisällön täydelliseen yhdenmukaistamiseen alan kyberturvallisuuden muuttuvan luonteen kanssa. Vastausten jakautuminen osoittaa, että teollisuuden suuntauksiin ja vaatimuksiin mukautetun kyberturvallisuuskoulutuksen varmistaminen on edelleen merkityksellinen. Siinä korostetaan CyberAgent-hankkeen merkitystä, jonka tavoitteena on tarjota jatkuvia opetussuunnitelmien päivityksiä, alan kumppanuuksia ja käytännön koulutusmahdollisuuksia kyberturvallisuuskoulutusohjelmien mukauttamiseksi kyberturvallisuusalan tarpeisiin.

Pk-yrityksiä koskevat erityisaiheet

Aihe/Tiedot	Laske
Pk-yritysten perustason kyberturvallisuus	91
Pk-yritysten tietosuoja ja yksityisyys	75
Ohjelmaan ei sisälly pk-yritysten erityisaiheita tai -taitoja	**64**
Häiriötilanteisiin reagoiminen pk-yrityksille	58
Riskien arviointi ja hallinta pk-yrityksissä	53
Kyberturvallisuuspolitiikan kehittäminen pk-yrityksille	46

Kyberturvallisuuden perusperiaatteita ja tietosuojaa painotetaan voimakkaasti. Useimmin mainitut aiheet, pk-yritysten peruskyberturvallisuus ja pk-yritysten tietosuoja ja yksityisyys, osoittavat, että kouluttajat asettavat etusijalle pk-yritysten osaamisen, jotta ne voivat suojata tietojaan ja ymmärtää kyberturvallisuuden peruskäsitteitä. Luku ”Ei pk-yritysten erityisaiheita tai -taitoja sisälly ohjelmaan” osoittaa, että joissakin kyberturvallisuutta koskevissa koulutusohjelmissa on puutteita pienten ja keskisuurten yritysten (pk-yritysten) räätälöityjen sisältöjen osalta. Siinä korostetaan kriittistä alaa kyberturvallisuuskoulutuksen parantamiseksi, erityisesti kun otetaan huomioon pk-yritysten kohtaamat haasteet ja uhat.

Pk-yritykset toimivat usein rajallisin resurssein, eivätkä ne välttämättä saa käyttöönsä erikoistunutta kyberturvallisuusasiantuntemusta, minkä vuoksi ne ovat erityisen alttiita kyberuhkille. Koska kyberturvallisuuden koulutusohjelmissa ei ole pk-yrityskohtaista sisältöä, näillä ohjelmilla ei ehkä täysin vastata pk-yritysten erityistarpeisiin, mikä saattaa jättää aukkoja niiden valmistautumisessa ja kyberhyökkäyksiä vastaan sietämisessä. Tämän puutteen korjaaminen edellyttää sellaisten aiheiden ja taitojen integrointia, jotka on erityisesti suunniteltu vastaamaan pk-yritysten kyberturvallisuustarpeisiin, kuten pienempiin liiketoimiin räätälöity riskinarviointi, kustannustehokkaat kyberturvallisuuskäytännöt ja strategiat tehokkaan kyberturvallisuuspolitiikan kehittämiseksi rajallisin resurssein.

Pk-yritysten työntekijöiden osaamisvaje

Taito/Topic	Laske
Uhkien havaitseminen ja niihin reagoiminen	103
Pilviturvallisuusosaaminen	87
Häiriötilanteisiin reagoiminen ja toipuminen	69
Tietosuoja ja tietosuoja	67
Riskienhallinta ja analysointi	63
Kehitteillä olevat teknologiat	58
Verkon turvallisuus	41
Vaatimustenmukaisuus ja sääntelyyn liittyvä tietämys	36

Analyysi paljastaa, että työntekijöiltä puuttuu osaamista keskeisiltä alueilta, joissa uhkan havaitseminen ja reagointi yleisimmin mainitaan. Tämä korostaa, että on tärkeää valmistaa opiskelijoita tunnistamaan kyberturvallisuusuhkia ja reagoimaan niihin olennaisena valmiutena alalla. Pilvipalvelujen tietoturvaosaaminen sijoittuu toiseksi, mikä osoittaa riippuvuuden pilvipalveluteknologioista ja erityisosaamisen tarpeesta pilviympäristöjen turvaamiseksi työntekijöiltä. Lisäksi arvostetaan häiriötilanteisiin reagointia ja toipumista, tietosuojaa ja riskienhallintaa ja analysointia. Kehittyvien teknologioiden osalta katsotaan, että tarve pysyä ajan tasalla alan viimeisimmistä edistysaskelista ei ole alijäämäinen. Sama koskee verkon turvallisuutta, joka on perustavaa laatua oleva alue, joka on osa useimpia kyberturvallisuuskoulutusohjelmia. Se osoittaa koulutuksen tehokkuuden tältä osin.

Uhat

Uhat	Laske
Tekoälypohjaiset kyberhyökkäykset	117
Ransomware-hyökkäykset	96
Tietojenkalastelu ja sosiaalinen tekniikka	87
Pilvipalvelun tietoturvaloukkaukset	82
Esineiden internetin haavoittuvuudet	75
Deepfake-uhat	51
Sisäpiirin uhkaukset	25

Analyysi osoittaa, että tekoälyyn perustuviin kyberhyökkäyksiin on keskitytty merkittävästi, sillä ne ovat yleisimmin mainittu kyberturvallisuusuhka, mikä osoittaa huolen tekoälyllä toimivien kyberuhkien hienostumisesta ja monimutkaisuudesta. Ransomware-hyökkäykset sekä tietojenkalastelu ja sosiaalinen suunnittelu olivat myös erittäin tärkeitä, mikä osoitti näiden hyökkäysvektorien läsnäolon pk-yrityksissä. Pilvipalvelujen tietoturvaloukkaukset ja esineiden internetin haavoittuvuudet korostavat pilvipalvelujen turvallisuuteen ja esineiden internetin laajentamiseen liittyviä huolenaiheita, mikä kuvastaa haasteita, jotka liittyvät pk-yritysten erilaisten ja hajautettujen teknologisten ekosysteemien suojeluun. Deepfake-uhkia ja sisäpiiriuhkia ei pidetä suurena uhkavektorina. Koulutusohjelmilla, jotka kattavat viisi tärkeintä aihetta, voidaan antaa opiskelijoille ja pk-yritysten työntekijöille paremmat valmiudet puuttua kohtaamiinsa uhkiin.

Uudet suuntaukset

Alue	Laske
Tekoäly ja koneoppiminen kyberturvallisuudessa	160
Digitaalinen identiteetti ja yksityisyys	96
Eettinen hakkerointi ja puolustava osaaminen	82
Kvanttilaskennan uhkat	67
Hajautetut turvallisuusjärjestelmät (esim. lohkoketju)	52
Keskittyminen pehmeisiin taitoihin ja tieteidenväliseen koulutukseen	47

Tekoälyä ja koneoppimista kyberturvallisuudessa korostetaan voimakkaasti, sillä se on useimmin mainittu ala, mikä kuvastaa näiden teknologioiden merkitystä kyberturvallisuustoimenpiteiden parantamisessa ja näiden alojen ammattilaisten tarvetta. Digitaalinen identiteetti ja yksityisyys ovat toinen merkittävä painopiste, jossa korostetaan digitaalisten identiteettien suojelun ja yksityisyyden turvaamisen merkitystä. Eettiset hakkerointi- ja Defensive Skills -pisteet osoittavat, että tarvitaan käytännön taitoja, joiden avulla ammattilaiset voivat tunnistaa haavoittuvuudet ja puolustaa hyökkäyksiä tehokkaasti. Kvanttilaskennan uhkia, hajautettuja turvallisuusjärjestelmiä, kuten lohkoketjuteknologiaa ja pehmeitä taitoja ja tieteidenvälistä koulutusta, ei pidetty nousevina suuntauksina. Vastausten jakaminen korostaa kyberturvallisuusalan monimuotoisuutta ja sitä, miten tärkeää on valmistella ammattilaisia, joilla on monipuolinen osaaminen ja tietämys nykyisten ja tulevien haasteiden ratkaisemiseksi. AI-aiheena on kuitenkin luottaa listan kärkeen.

Sukupuolten tasa-arvo

Naisten prosenttiosuus	Vastausten määrä
Alle 10 %	57
10–25 %	79
26–50 %	43
51–75 %	8
Yli 75 %	3

Naisten osuus kyberturvallisuutta koskevista koulutusohjelmista paljastaa sukupuolten monimuotoisuuden eroavaisuuksia, ja suurin osa vastauksista osoittaa, että naisten osallistuminen on vähäistä. Yksityiskohtaisesti 79 vastauksesta naisten osuus oli 10–25 prosenttia, ja 57 vastauksen mukaan se oli alle 10 prosenttia. Joissakin ohjelmissa ehdotetaan maltillista sukupuolijakaumaa, ja 43 vastaajaa arvioi, että naisten osallistumisaste on 26–50 prosenttia. Ohjelmat, joissa on suuri osuus naispuolisista osallistujista, ovat kuitenkin erityisen harvinaisia, mistä on osoituksena vain 8 vastausta, jotka viittaavat 51–75 %: iin, ja minimaalinen 3 vastausten määrä arvioi yli 75 %. Nämä tiedot korostavat haastetta sukupuolten monimuotoisuuden saavuttamisessa kyberturvallisuuden koulutusohjelmissa ja korostavat huomattavaa kuilua naisten osallistumisessa useimmissa raportoiduissa ohjelmissa.

Tasa-arvoaloitteet

Vastaus	Vastausten määrä
Kyllä	30
Ei	160

Tiedot osoittavat, että merkittävä enemmistö vastaajista, yhteensä 160, ei käytä erityisiä aloitteita tai strategioita, joilla kannustetaan naisia osallistumaan kyberturvallisuuskoulutukseen. Vain 30 vastaajaa vahvisti tällaisten toimenpiteiden toteuttamisen. Tämä viittaa siihen, että vaikka on olemassa jonkin verran tietoisuutta ja pyrkimyksiä lisätä naisten osallistumista kyberturvallisuuskoulutukseen kohdennetuilla aloitteilla, useimmissa ohjelmissa ei ehkä vielä priorisoida tai panna täytäntöön erityisiä strategioita sukupuolten monimuotoisuuteen puuttumiseksi. Kohdennettujen aloitteiden puute voisi osaltaan vaikuttaa siihen, että naisten osallistuminen on vähäistä, kuten edelliseen kysymykseen annetuissa vastauksissa todettiin.

Sukupuolinäkökulman huomioon ottava koulutus

Vastaus	Vastausten määrä
Kyllä	47
Ei	44
Epävarma	72
Ei ole merkitystä minulle	27

Tulokset viittaavat siihen, että vastaajien mielipide jakautuu sukupuolinäkökohdat huomioon ottavien kyberturvallisuutta koskevien koulutusmoduulien saatavuudesta. Suurin ryhmä, johon kuului 72 vastaajaa, ilmaisi epävarmuutta (”epävarmuus”), mikä viittaa siihen, että sukupuolinäkökohdat huomioon ottavan aineiston esiintymisestä ei ole selkeää yksimielisyyttä tai tietoa. Lähes jopa jakautuu niihin, jotka uskovat, että sukupuolinäkökohdat huomioon ottavia moduuleja on riittävästi (47 vastausta) ja niiden välillä, jotka eivät (44 vastausta). Lisäksi 27 vastaajaa katsoi, että kysymys ei liity heidän kokemuksiinsa tai asiayhteyteensä.

Tämä jako heijastaa käynnissä olevaa keskustelua ja erilaisia käsityksiä kyberturvallisuuskoulutuksen sisällön osallistavuudesta. Epävarmojen vastausten suuri määrä osoittaa, että kyberturvallisuusalan koulutusekosysteemissä saattaa olla puutetta

sukupuolinäkökohdat huomioon ottavien koulutusresurssien tiedostamisessa tai saatavuudessa.

Sukupuolten osallistamisen esteet

Este	Laske
Stereotypiat tai kulttuurinormit	107
Tietämättömyys kyberturvallisuuden mahdollisuuksista	86
Mentoroinnin tai roolimallien puute	74
Työ- ja yksityiselämän tasapainon haasteet	60
Koettu sukupuolten tasa-arvon suosiminen teollisuudessa	58

Merkittävimmät esteet naisten osallistumiselle kyberturvallisuuteen, kuten kyselyyn vastanneet havaitsivat, ovat stereotypiat tai kulttuurinormit (107 mainintaa) ja tietämättömyys kyberturvallisuuden mahdollisuuksista (86 mainintaa). Nämä kaksi estettä viittaavat siihen, että yhteiskunnalliset käsitykset ja riittämättömät tiedot urapoluista haittaavat merkittävästi naisten pääsyä kyberturvallisuusalalle. Mentoroinnin tai roolimallien puute sekä työ- ja yksityiselämän yhteensovittamiseen liittyvät haasteet ovat myös merkittäviä esteitä, mikä korostaa tukiverkostojen ja joustavien työympäristöjen merkitystä naisten osallistumisen edistämisessä. Lisäksi alan kokema sukupuolitaho viittaa siihen, että alalla tarvitaan kulttuurisia ja systeemisiä muutoksia, jotta alasta tulisi miellyttävämpi ja tasa-arvoisempi naisten kannalta.

Erityisohjelma monimuotoisuuden ja osallisuuden edistämiseksi

Vastaus	Vastausten määrä
Kyllä	44
Ei	85
En ole varma	61

Tiedoista käy ilmi, että merkittävällä osalla kyselytutkimuksista, joihin saatiin 85 vastausta, ei ole käytössä erityisiä toimintalinjoja tai ohjelmia, joilla edistettäisiin naisten monimuotoisuutta ja osallisuutta kyberturvallisuuskoulutukseen. Samaan aikaan 44 vastaajaa ilmoitti, että niiden toimielimet toteuttavat tällaisia aloitteita, ja korostivat lähestymistapaa, jolla puututaan sukupuolten monimuotoisuuteen kentällä. Huomattava määrä vastaajista, 61, on kuitenkin epävarma siitä, onko niiden toimielimillä tällaisia toimintalinjoja tai ohjelmia, mikä viittaa mahdolliseen viestinnän tai tietoisuuden puuttumiseen olemassa olevasta monimuotoisuudesta ja osallistamisesta. Tämä sekava vastaus viittaa myös siihen, että vaikka jotkin laitokset toteuttavat toimia kyberturvallisuuskoulutuksen osallistamiseksi, sekä monimuotoisuusohjelmien täytäntöönpanossa että tällaisten aloitteiden tietoisuudessa tiedekunnan, henkilöstön ja opiskelijoiden keskuudessa on edelleen huomattavia eroja.

Parannusehdotus

Ehdotus	Laske
Menestyneiden naispuolisten kyberturvallisuusammattilaisten näkyvyyden lisääminen	95
Lisää naispuolisia kyberturvallisuuden ohjaajia tai koulutushenkilöstöä	89
Tarjota stipendejä tai kannustimia	81
Mentorointimahdollisuudet	49
Koulutussisältöä, joka välttää sukupuoleen liittyviä vinoutumia	33
Päivitetään säännöllisesti toimintalinjoja osallistavuuden tukemiseksi	31
Sukupuolinäkökohdat huomioon ottava tapaustutkimus ja skenaariot	24
Räätälöidyt koulutusohjelmat	21
Enemmän vain naisille suunnattuja koulutustilaisuuksia	18

Vastausten analyysi, joka koskee ehdotuksia kyberturvallisuuskoulutuksen lisäämiseksi sukupuolinäkökulman huomioon ottamiseksi, paljastaa vahvan yksimielisyyden useiden keskeisten strategioiden merkityksestä. Kannattavin ehdotus 95 maininnalla on menestyksekkäiden naispuolisten kyberturvallisuusammattilaisten näkyvyyden lisääminen. Tämä korostaa roolimallien ja kunnianhimoisten lukujen kriittistä roolia naisten kannustamisessa jatkamaan uraa kyberturvallisuuden alalla. Lähellä takana, 89 maininnan, on kehotus lisätä naispuolisia kyberturvallisuuden ohjaajia tai koulutushenkilöstöä, mikä korostaa tarvetta edustukseen opetushenkilöstössä. Stipendejä tai kannustimia, jotka saavat 81 mainintaa, pidetään ratkaisevan tärkeinä alan taloudellisen saatavuuden ja houkuttelevuuden kannalta. 49 vastaajan mukaan mentorointimahdollisuudet korostavat alan kokeneiden ammattilaisten ohjauksen ja tuen merkitystä. Tarve saada koulutussisältöä, jossa vältetään sukupuolten tasa-arvon vääristyminen, ja säännöllisesti päivitettävät toimintapolitiikat, joilla tuetaan osallisuutta, viittaavat siihen, että tarvitaan opetussuunnitelmaa ja politiikan mukautuksia, jotka heijastavat ja edistävät monimuotoisuutta.

Pk-yritysten kenttätutkimusten analyysi

Väestörakenne:

Kyselyyn saatiin vastauksia kumppanimaista. Eniten vastaajia on Romaniassa (28), Norjassa (23) ja Liettuassa, Espanjassa ja Belgiassa 21 vastaajaa. Myös Suomella ja Türkiyellä on merkittävä määrä vastauksia, joista kukin on 20, ja Puola on lähellä jäljessä 19 vastaajaa.

Yrityssektori

Yrityssektori	Laske
SE	18
Koulutus	6
Rakentaminen	4
Konsultointi	4
Kyberturvallisuus	4

Tiedot osoittavat, että tietotekniikka-ala on vahvasti edustettuna, ja 18 vastaajaa määritteli yrityksensä tällä alalla toimivaksi. Koulutus-, rakennus-, konsultointi- ja kyberturvallisuusaloilla on myös merkittäviä edustustoja, joista kukin on 4–6. Viiden parhaan joukossa on useita aloja, joilla on vähemmän osuuksia, mikä kuvastaa tutkimuksen laajaa lähestymistapaa eri toimialoilla.

Vastaajien profiili

Asema yrityksessä	Laske
Esimies	48
Toimitusjohtaja/Omistaja	35
Tekninen (insinööri/kehittäjä/analysaattori)	27
Muu	25
Koordinaattori/Hallinto	8
Myynti/Markkinointi	8
Asiantuntija/asiantuntija	8
Työntekijä	8
Konsultti	3
Koulutus/opetus	2
Rahoitus/kirjanpito	1
Projektinhallinta	1
HR	1
Yhteensä	**175**

On olemassa laaja valikoima työnimikkeitä, joilla on monipuolinen ammattiyleisö ja laaja positiopaneeli, kuten ”työntekijä” ja ”johtaja”, joka osoittaa laajan valikoiman vastaajia, jotka ulottuvat organisaation hierarkioiden eri tasoille. Kyberturvallisuus on monialainen kysymys, joka sitouttaa yksilöitä eri rooleihin ja vastuisiin yrityksissä.

Sukupuoli

Kyselyyn vastanneista sukupuolijakaumasta käy ilmi, että miehillä (102) on suurempi edustus kuin naisilla (69), ja pieni osa vastaajista (4) ei halua julkistaa sukupuoltaan. Tämä jako viittaa siihen, että kyselyn edustamalla alalla on sukupuolten välistä kuilua, joka heijastaa laajempia suuntauksia kyberturvallisuus- ja teknologia-aloilla, joilla miesten määräävä asema on usein raportoitu. Naispuolisten vastaajien merkittävä määrä osoittaa kuitenkin naisten merkityksellisen osallistumisen alalla, mikä viittaa jatkuviin muutoksiin alan sukupuolijakaumassa. Vaikka sukupuolten välinen kuilu on ilmeinen, vastausten moninaisuus viittaa myös siihen, että kyberturvallisuuden toimintaympäristö muuttuu vähitellen.

Sukupuolijakauma maittain

Valtio	Naaras	Uros	Mieluummin olla sanomatta
Belgia	10	10	1
Suomi	9	11	0
Liettua	9	12	0
Norja	8	15	0
Puola	8	9	2
Romania	12	16	0
Espanja	6	14	1
Turkki	7	13	0

Taulukossa esitetään sukupuolten jakautuminen eri maissa. Miesvastaajia on enemmän kuin naisvastaavia kaikissa maissa, mikä vastaa edellä käsiteltyä yleistä sukupuolijakaumaa. Ero vaihtelee kuitenkin maittain: joissakin maissa, kuten Belgiassa, miesten ja naisten vastaajien määrä on yhtä suuri (10 kumpaakin) ja Puolassa miesten (9) ja naisten (8) osuus on suurempi, ja pieni osa vastaajista ei halua sanoa sukupuoltaan (2). Romaniassa ja Norjassa vastaajia on enemmän ja miesten ja naisten välinen suhde on korkeampi. Tämä sukupuolijakauma antaa monipuolisen käsityksen kyselyyn vastanneiden väestörakenteesta ja korostaa sekä sukupuolten välisiä eroja että maantieteellistä monimuotoisuutta kyberturvallisuuden alalla.

Yrityksen koko

Yrityksen koko	Laske
Enintään 10 työntekijää	64
11–50	60
51–250	51

Kyselyyn saadut vastaukset osoittavat, että osallistujista on huomattava määrä pieniä ja keskisuuria yrityksiä. Suurin ryhmä on yrityksiä, joissa on enintään 10 työntekijää (64 vastaajaa), ja niitä, joilla on 11–50 työntekijää (60 vastaajaa), ja sitten 51–250 työntekijää (51 vastaajaa).

Pienten yritysten enemmistö vastaajista korostaa sellaisten räätälöityjen kyberturvallisuusratkaisujen merkitystä, joilla vastataan pk-yritysten erityistarpeisiin ja -rajoitteisiin.

Osaamistaso

Kyberturvallisuuden tietotaso	Laske
Väli	85
Aloittelija	64
Edistynyt	26

Kyselyyn saadut vastaukset osoittavat, että suurin osa vastaajista pitää työntekijöidensä nykyistä kyberturvallisuusosaamista ”välitasona” (85), jota seuraa ne, jotka pitävät sitä ”aloittelijatasolla” (64), ja pienempi osa pitää työntekijöitään ”edistyneenä” kyberturvallisuusosaamisena (26).

Tämä jakautuminen viittaa siihen, että edustettuna olevissa organisaatioissa on merkittäviä kasvu- ja kehittämismahdollisuuksia kyberturvallisuusosaamisessa. Suurin osa ”keskitason” ja ”aloittelijan” tasoista viittaa siihen, että tarvitaan jatkuvaa koulutusta koskevia aloitteita näiden työntekijöiden kyberturvallisuutta koskevan tietopohjan nostamiseksi. Siinä korostetaan mahdollisuutta kohdennettuihin kyberturvallisuuskoulutusohjelmiin, joissa otetaan huomioon erilaiset tietotasot ja varmistetaan, että aloittelijat ymmärtävät hyvin kyberturvallisuuden perusperiaatteet.

Osaavien työntekijöiden läsnäolo, vaikkakin vähemmän, on rohkaisevaa, koska se osoittaa perustavaa laatua olevaa kyberturvallisuusosaamista joissakin organisaatioissa.

Tietotaso perustuu yrityksen kokoon.

Yrityksen koko	Edistynyt	Aloittelija	Väli
Enintään 10 työntekijää	6	25	33
11–50	10	20	30
51–250	10	19	22

Taulukosta käy ilmi, miten kyberturvallisuusosaamisen tasot (Advanced, Beginner, Intermediate) jakautuvat eri yrityskokoihin. Pienet yritykset (enintään 10 työntekijää) näyttävät nojaavan kyberturvallisuusosaamisen ”välitason” tasoon, jota seuraa ”aloittelija”. Tämä viittaa siihen, että vaikka pienyrityksillä saattaa olla jonkin verran ymmärrystä kyberturvallisuudesta, aloittelijatasolla on edelleen merkittävä osa, mikä osoittaa parantamisen varaa ja peruskoulutuksen tarvetta. Keskisuuret yritykset (11–50 työntekijää) jakautuvat tasapuolisesti eri tietotasoille ja suosivat hieman ”välillistä” tietämystä. Tämä voisi heijastaa jäsennellympää lähestymistapaa kyberturvallisuuskoulutukseen hieman suuremmissa organisaatioissa, mutta myös osoittaa sekä kehittyneen ymmärryksen että perustavaa laatua olevien oppimistarpeiden olemassaolon. Suuret pk-yritykset (51–250 työntekijää) noudattavat samaa mallia kuin keskisuuret yritykset, joissa on yhtä paljon kehittyneitä ja aloittelevia tasoja ja hieman vähemmän keskitason osaamista.

Kaikenkokoisissa yrityksissä kyberturvallisuusosaamisen ”väliaikainen” taso on yleisin.

Kyberturvallisuustehtäviä hoitavat työntekijät

Numero	Laske
1–5	88
0	22
6–10	17
21+	12
11–20	5

Kyberturvallisuuden työntekijöiden määrä	Laske
0–4	113
5–9	17
10–14	13
20–24	4
25–50	6
+ 100	9

Taulukoissa esitetään kyberturvallisuuteen liittyvää työtä tekevien työntekijöiden lukumäärän jakautuminen eri organisaatioissa. Se tarjoaa selkeämmän kuvan siitä, miten kyberturvallisuusvastuut jakautuvat eri työntekijämäärille. Suurin osa vastauksista kuuluu 0–4-luokkaan, mikä viittaa siihen, että suuri määrä organisaatioita, joissa on hyvin pieniä kyberturvallisuusryhmiä tai ei edes yhtäkään erityisesti kyberturvallisuudelle omistettua organisaatiota. Taajuudet vähenevät merkittävästi siirtyessämme korkeammille alueille, ja jonkin verran elpyminen organisaatioissa, joissa on yli 100 työntekijää, jotka ovat omistautuneet kyberturvallisuuteen. Tämä selittyy sillä, että kyseiset yritykset työskentelevät kyberturvallisuuden alalla pääasiallisena ammattinaan.

Yksityiskohtaisesti tiedot viittaavat siihen, että kyberturvallisuusryhmien koko on laaja, ja yleisin koko on yksi työntekijä, minkä jälkeen ei ole omistautuneita kyberturvallisuustyöntekijöitä, jotka osoittavat, että monet organisaatiot luottaisivat minimaalisesti tai eivät lainkaan omistautuneeseen kyberturvallisuushenkilöstöön. Tiheys vähenee huomattavasti joukkueen koon kasvaessa.

Jako osoittaa, että kyberturvallisuusalan työvoiman kohdentamisessa saattaa olla puutteita, sillä merkittävällä määrällä pieniä ja keskisuuria yrityksiä (pk-yrityksiä) ei ehkä ole riittäviä resursseja kyberturvallisuuteen, mikä altistaa ne suuremmille riskeille. Suurempien tiimien läsnäolo joissakin organisaatioissa viittaa kyberturvallisuuden merkityksen tunnustamiseen tietyillä aloilla tai suuremmissa yrityksissä.

Naiset kyberturvallisuudessa

Naisten valikoima kyberturvallisuudessa	Laske
0	78
1–5	57
6–10	8
11–15	4
16–20	1

Kyselyn ”Kuinka monet näistä työntekijöistä ovat naisia?” tulokset osoittavat, että pk-yritysten kyberturvallisuushenkilöstössä on merkittävä sukupuolten välinen kuilu. Silmiinpistävin havainto on, että suurin osa yrityksistä, yhteensä 78, ilmoitti, ettei heillä ole lainkaan naisia kyberturvallisuustehtävissään. Tämä viittaa siihen, että naiset ovat aliedustettuina tällä kriittisellä alalla kaikissa tutkituissa pk-yrityksissä. Määrä vähenee asteittain, kun kyberturvallisuusrooleissa olevien naisten määrä kasvaa, ja 31 yrityksessä on yksi nainen

tällaisessa asemassa. Muutamat yritykset, joilla on vähintään 10 naista kyberturvallisuusrooleissa, vaikka ne ovatkin myönteisiä, ovat edelleen poikkeus eikä normi. Nämä tapaukset voivat edustaa organisaatioita, joilla on suurempia kyberturvallisuusryhmiä tai jotka ovat kiinnittäneet erityistä huomiota sukupuolten monimuotoisuuteen kyberturvallisuushenkilöstössään. Siinä korostetaan, että tarvitaan aloitteita, joilla pyritään kannustamaan ja tukemaan naisia kyberturvallisuuden alalla. Niiden yritysten huomattava määrä, joilla ei ole lainkaan naisia kyberturvallisuustehtävissä, korostaa ratkaisevan tärkeää alaa, jolla edistetään sukupuolten monimuotoisuutta ja osallisuutta alalla. Tämän sukupuolten välisen kuilun umpeen kurominen voisi edistää monipuolisempia näkökulmia kyberturvallisuushaasteisiin vastaamisessa.

Ulkoisten palvelujen käyttö

Vastaus	Laske
Ei	115
Kyllä	60

Vastaukset paljastavat merkittävän näkökulman siihen, miten pk-yritykset lähestyvät kyberturvallisuutta. Suurin osa kyselyyn vastanneista yrityksistä, 115 yritystä 175:stä, ilmoittaa, etteivät ne palkkaa ulkoisia palveluja kyberturvallisuustyöhön. Tämä viittaa siihen, että kyberturvallisuuspyrkimyksiä on syytä hallinnoida sisäisesti suuressa osassa pk-yrityksiä. Tähän suuntaukseen voivat vaikuttaa useat tekijät, kuten budjettirajoitukset, kyberturvallisuuskäytäntöjen hallinta tai usko siihen, että niiden nykyiset sisäiset resurssit riittävät vastaamaan niiden kyberturvallisuustarpeisiin. Tämä tilanne tekee CyberAgent-hankkeesta erittäin merkityksellisen, jotta työntekijällä olisi perustavaa laatua olevat taidot ja tiedot.

60 yritystä ilmoitti palkkaavansa ulkoisia palveluja kyberturvallisuustehtäviin. Tämä ryhmä tunnustaa todennäköisesti ulkoistamisen edut, kuten erikoisosaamisen hankkimisen, uusimpien kyberturvallisuusuhkien ja vastatoimien pysymisen ajan tasalla tai sisäisten valmiuksien täydentämisen. Päätös ulkoisten palvelujen palkkaamisesta voisi myös heijastaa ymmärrystä kyberturvallisuusuhkien monimutkaisuudesta, joka voi olla haastavaa hallita täysin yrityksen sisällä, erityisesti pk-yrityksille, joiden resurssit ovat rajalliset.

Tämä jako korostaa pk-yritysten kyberturvallisuusstrategian eroavaisuuksia, sisäisen hallinnoinnin ja kyberturvallisuustoimintojen ulkoisen ulkoistamisen välistä tasapainoa. Siinä korostetaan kyberturvallisuutta koskevan räätälöidyn lähestymistavan merkitystä ja tunnustetaan, että eri organisaatioilla voi olla erilaisia tarpeita, valmiuksia ja resursseja, jotka vaikuttavat niiden päätöksiin hakea ulkoista tukea kyberturvallisuuspyrkimyksille.

Koulutusohjelmien tehokkuus

Vastaus	Laske
1 (tehoton)	8
2	38
3	79
4	39
5 (erittäin tehokas)	11

Vastaukset antavat käsityksen käsityksistä nykyisten koulutusohjelmien tehokkuudesta valmentaa opiskelijoita todellisiin kyberturvallisuushaasteisiin pk-yrityksissä. Suurin osa vastaajista, joilla oli 79 lukua, arvioi nykyisten koulutusohjelmien tehokkuuden ”3”, mikä viittaa neutraaliin tai kohtalaiseen käsitykseen niiden tehokkuudesta. Tämä viittaa siihen, että vaikka näissä ohjelmissa on jonkin verran luottamusta, on myös paljon parantamisen varaa. Vastaukset osoittavat myös suuntausta kohti asteikon alapäätä, jossa ”2” sai 38 laskentaa, mikä osoittaa suhtautuvansa epäilevästi näiden koulutusohjelmien tehokkuuteen. Äärimmäisissä tapauksissa ”1” (tehoton) sai vähiten valituksia (8 kpl) ja ”5” (erittäin tehokas) hieman enemmän (11 laskentaa). Tämä osoittaa, että hyvin harvat vastaajat pitävät nykyisiä koulutusohjelmia joko täysin tehottomina tai erittäin tehokkaina valmistautumaan pk-yritysten kyberturvallisuushaasteisiin. ”4”-vastausten tasapainoinen määrä (39 laskentaa) viittaa siihen, että huomattava osa osallistujista pitää koulutusohjelmia suhteellisen tehokkaina, mutta ei ilman merkittäviä rajoituksia. Vaikka nykyiset koulutusohjelmat tarjoavat jonkin verran valmistautumista todellisiin kyberturvallisuushaasteisiin pk-yrityksissä, tarjotun koulutuksen ja alan tarpeiden välillä on kuilu. Tämä kuilu voi johtua useista tekijöistä, kuten kyberturvallisuusuhkien kehitysvauhdista, taitojen käytännön soveltamisesta tai pk-yritysten kohtaamien haasteiden erityisyydestä.

Kyberturvallisuuskoulutuksen kolme tärkeintä alaa

Luokka	Laske
Uhkien havaitseminen ja niihin reagoiminen	102
Riskienhallinta ja analysointi	81
Häiriötilanteisiin reagoiminen ja toipuminen	72
Tietosuoja ja tietosuoja	68
Pilviturvallisuusosaaminen	51
Verkon turvallisuus	46
Vaatimustenmukaisuus ja sääntelyyn liittyvä tietämys	31
Kehitteillä olevat teknologiat	24

Vastausten analyysistä käy ilmi, että ”uhkien havaitsemista ja reagointia” pidetään kyberturvallisuuskoulutuksen tärkeimpänä alana 102:lla, mikä osoittaa vahvan uskomuksen sen merkitykseen pyrittäessä vastaamaan pk-yritysten todellisiin kyberturvallisuushaasteisiin. Tätä alaa seuraavat tiiviisti ”riskinhallinta ja -analyysi” ja ”Incident response and recovery” (81 ja 72), joissa korostetaan riskien ymmärtämisen arvoa ja kykyä reagoida tehokkaasti poikkeamiin. ”Tietosuoja ja tietosuoja” saavat myös merkittävää painoarvoa, mikä kuvastaa

tietosuojalainsäädännön kasvavaa merkitystä sekä tarvetta suojata henkilökohtaisia ja arkaluonteisia tietoja digitaalisella aikakaudella. ”Pilviturvallisuusosaaminen” tunnistetaan 51 vastaajan avainalueeksi, mikä johtuu todennäköisesti pilvipalvelujen yleistymisestä ja niiden mukanaan tuomista ainutlaatuisista turvallisuushaasteista. Verkkojen turvallisuus, jossa on 46 asiaa, on edelleen perustavanlaatuinen huolenaihe, mikä korostaa, että tarvitaan vahvoja puolustuskeinoja verkkopohjaisia uhkia vastaan. ”Vaatimustenmukaisuus- ja sääntelyosaaminen” ja ”kehittyvät teknologiat” eivät ole yhtä tärkeitä.

Osaaminen ja osaaminen

Osaamisalue ja osaamisalue	Olennainen (%)	Suuri tarve (%)	Kohtalainen tarve (%)	Vähäinen tarve (%)	Ei tarvita (%)
Tietosuoja ja tietosuoja	38.29	38.29	13.14	10.29	0.00*
Riskien arviointi ja hallinta	34.86	36.00	24.00	4.57	0.57
Häiriötilanteisiin reagoiminen ja toipuminen	33.14	38.86	19.43	8.00	0.57
Viestintätaidot	32.57	35.43	22.29	8.00	1.71
Tekninen tietämys	30.29	32.00	26.29	8.57	2.86
Uhkatiedustelu ja -seuranta	29.71	37.14	24.00	8.57	0.57
Politiikan kehittäminen ja täytäntöönpano	24.00	37.14	24.00	12.57	2.29

*: ”Ei tarvita” prosenttiosuutta ”Tietosuoja ja tietosuoja” ei ole saatavilla (NaN), mikä saattaa johtua siitä, että kaikki vastaajat pitävät tätä alaa ainakin jonkin verran, joten sen voidaan katsoa olevan 0 prosenttia.

Taulukossa esitetään kunkin osaamis- ja osaamisalan keskimääräiset pisteet, jotka on saatu kyselyvastauksista, joissa arvioidaan niiden merkitys asteikolla 1 (ei tarvita) viiteen (olennaiseen). Nämä pisteet antavat kvantitatiivisen käsityksen siitä, miten vastaajat priorisoivat eri osa-alueita kentän sisällä.

Tässä taulukossa esitetään selkeä erittely siitä, miten vastaajat arvostavat kutakin osaamis- ja osaamisaluetta. Aloilla, kuten ”Data Privacy and Protection” ja ”Risk Assessment and Management” on suurin prosenttiosuus ”Essential” luokituksista, mikä kuvastaa niiden kriittistä merkitystä alalla. Sen sijaan ”politiikan kehittäminen ja täytäntöönpano” osoittaa vastausten laajemman jakautumisen, mikä viittaa siihen, että niiden merkitys on vaihtelevampi. Tulokset korostavat voimakkaasti teknistä tietämystä, uhkatietoisuutta ja kykyä reagoida poikkeamiin sekä tarvetta tehokkaille viestintä- ja tietosuojakäytännöille.

Uudet kyberturvallisuusuhat

Kehittyvä kyberturvallisuusuhka	Taajuus
Tietojenkalastelu ja sosiaalinen tekniikka	105
Tekoälypohjaiset kyberhyökkäykset	95
Ransomware-hyökkäykset	90
Pilvipalvelun tietoturvaloukkaukset	60
Deepfake-uhat	57
Esineiden internetin haavoittuvuudet	44
Sisäpiirin uhkaukset	31

Verkkourkinta ja sosiaalinen suunnittelu ovat kaikkein kiireellisimpiä uhkia, ja tekoälyyn perustuvat kyberhyökkäykset ja ransomware-hyökkäykset saavat myös merkittävää huomiota. Tämä viittaa siihen, että pk-yritykset ovat hyvin tietoisia tarpeesta suojautua sekä perinteisiltä että kehittyviltä kyberuhkilta. Myös pilvipalvelujen tietoturvaloukkaukset ja deepfake-uhat korostuvat, mikä kuvastaa huolta pilvipalvelujen turvallisuudesta ja tekoälyn mahdollisesta väärinkäytöstä. IoT-haavoittuvuudet ja sisäpiiriuhat tunnistetaan myös, vaikka niitä pidetään vähemmän välittöminä kuin muut kategoriat. On vastauksia, jotka viittaavat siihen, että jotkut vastaajat ovat epävarmoja erityisistä uhkista tai heillä ei ole ideoita liiketoimintatasollaan, mikä viittaa siihen, että joidenkin pk-yritysten tietoisuudessa tai huolenaiheissa on mahdollisesti puutteita.

Kyberturvallisuusosaamisen ja -taitojen puute

Kyberturvallisuusosaamisen ja -taitojen puute	Taajuus
Alhainen uhkatietoisuus	105
Kyberturvallisuutta koskevien määräaikaisten koulutusten alhainen taso	88
Alhainen haavoittuvuusarviointi	80
Alhainen tekninen osaaminen	71
Politiikan ja asetusten alhainen taso	50
Alhainen pehmeiden taitojen taso	37

Merkittävimmät puutteet työntekijöiden kyberturvallisuustietämyksissä tai -taidoissa ovat uhkatietoisuus, säännöllinen kyberturvallisuuskoulutus, haavoittuvuusarviointi, tekniset taidot sekä politiikan ja sääntelyn ymmärtäminen. Näiden vastausten tiheys korostaa, että näitä erityisaloja käsittelevän kattavan kyberturvallisuuskoulutuksen tarve on ratkaisevan tärkeä. Uhkatietoisuus on merkittävin puute, mikä osoittaa, että työntekijät eivät ehkä ole täysin tietoisia kyberturvallisuusuhkista, jotka voivat vaikuttaa heidän organisaatioonsa. Tämä puute korostaa, että on tärkeää tehostaa valistusohjelmia ja koulutusta, jotta työntekijät voivat tunnistaa mahdolliset uhat tehokkaammin. Säännölliset kyberturvallisuuskoulutukset nähdään myös aukona, mikä osoittaa, että tarvitaan jatkuvaa koulutusta ja päivityksiä uusimmista kyberturvallisuuskäytännöistä ja -uhkista kertaluontoisten koulutustilaisuuksien sijaan.

Uudet suuntaukset

Kyberturvallisuuskoulutuksen uudet suuntaukset	Taajuus
Tekoäly ja koneoppiminen kyberturvallisuudessa	134
Digitaalinen identiteetti ja yksityisyys	108
Eettinen hakkerointi ja puolustava osaaminen	86
Keskittyminen pehmeisiin taitoihin ja tieteidenväliseen koulutukseen	54
Kvanttilaskennan uhkat	39
Hajautetut turvajärjestelmät (esim. lohkoketju)	28

Analyysi osoittaa, että tekoälyn ja koneoppimisen merkitys kyberturvallisuudessa korostuu selvästi seuraavien viiden vuoden odotetuimpana trendinä. Tämä osoittaa, että kehittyneiden teknologioiden rooli kyberturvallisuuspuolustuksen parantamisessa ja uusien turvallisuusratkaisujen kehittämisessä tunnustetaan yhä enemmän. Tämän kategorian korkea vastaustiheys viittaa siihen, että koulutusohjelmiin on yhä enemmän sisällytettävä tekoäly- ja koneoppimiskomponentteja kyberturvallisuuden ammattilaisten valmistamiseksi tulevaisuuteen. Digitaalinen identiteetti ja yksityisyyden suoja nousevat toiseksi odotetuimmaksi trendiksi, mikä korostaa henkilötietojen suojaan ja digitaalisten identiteettien hallintaan liittyviä huolenaiheita yhä enemmän verkkomaailmassa. Tämä suuntaus viittaa koulutuksen kysyntään, joka kattaa yksityisyydensuojalakien, tietosuojatekniikoiden ja identiteetinhallintaratkaisujen monimutkaisuuden. Eettiset hakkerointi- ja puolustustaidot tunnistetaan kolmanneksi keskeiseksi trendiksi, mikä kuvastaa ennakoivien puolustusstrategioiden merkitystä kyberturvallisuudessa. Eettisen hakkeroinnin painotus osoittaa siirtymisen kohti koulutusta, jonka avulla kyberturvallisuuden ammattilaiset voivat ajatella hyökkääjien tavoin puolustaakseen organisaatiotaan paremmin.

Koulutusohjelmien riittävyys

Vastaus	Taajuus
Kyllä	81
Ei varmaa	65
Ei	29

Analyysi kysymyksestä, jossa selvitettiin vastaajien näkemyksiä nykyisten kyberturvallisuuskoulutusohjelmien riittävyydestä, paljastaa osallistujien keskuudessa ristiriitaisen näkökulman. Merkittävä osa vastaajista, jotka edustavat suurinta osaa vastaajista, katsoo, että nykyiset kyberturvallisuuskoulutusohjelmat ovat riittäviä, kuten ”kyllä” -vastaukset osoittavat. Tämä viittaa siihen, että monet ihmiset kokevat, että nykyisin saatavilla oleva koulutus vastaa heidän organisaatioidensa tarpeita tai vastaa heidän odotuksiaan siitä, mitä kyberturvallisuuskoulutuksen pitäisi sisältää. Huomattava osa vastaajista ei kuitenkaan ole varma nykyisten koulutusohjelmien riittävyydestä, mikä korostaa jonkinasteista epävarmuutta tai tiedon puutetta käytettävissä olevista koulutusvaihtoehdoista tai niiden tehokkuudesta nykyisiin kyberturvallisuushaasteisiin vastaamisessa. Tämä epävarmuus saattaa johtua kyberuhkien muuttuvasta luonteesta ja siitä, että koulutusohjelmia on vaikea pitää ajan tasalla alan viimeisimmästä kehityksestä. ”Ei”-vastaukset, vaikka ne edustavatkin pienintä ryhmää,

osoittavat selvän huolen siitä, että nykyiset koulutusohjelmat eivät riitä vastaamaan nykyisiin kyberturvallisuustarpeisiin. Tämä ryhmä saattaa havaita puutteita koulutuksen kattavuudessa uusista uhkista, teknologioista tai menetelmistä.

Koulutusohjelmien osallistavuus

Vastaus	Taajuus
Kyllä	81
Ei varmaa	65
Ei	29

Vastausten analyysi osoittaa, että nykyisten sukupuolten tasa-arvoa koskevien kyberturvallisuuskoulutusohjelmien osallistavuus on erilainen. Monet vastaajat katsovat, että nykyinen koulutus on osallistavaa ja vastaa tehokkaasti kaikkien sukupuolten tarpeita, kuten ”kyllä” -vastaukset osoittavat. Tämä viittaa siihen, että merkittävä osa kyberturvallisuusyhteisöstä uskoo, että nykyiset koulutustoimet ovat siirtymässä osallistavuuteen ja sukupuolten tasa-arvoon. Suuri joukko vastaajia ei kuitenkaan ole varma näiden ohjelmien osallistavuudesta, mikä viittaa huomattavaan epävarmuuteen tai tietoisuuteen kyberturvallisuuskoulutuksen sukupuolinäkökohdista. Tämä vastaus voisi tuoda esiin koulutuksen tarjoajien ja osallistujien välisen viestintävajeen tai ehdottaa, että osallistamistoimet eivät ehkä ole niin näkyviä tai vaikuttavia kuin on tarkoitettu. ”Ei” -vastauksissa, jotka edustavat pienintä ryhmää vastaajista, korostetaan kuitenkin kriittistä huolta siitä, että nykyinen kyberturvallisuuskoulutus ei vastaa riittävästi kaikkien sukupuolten tarpeita. Tämä palaute viittaa siihen, että kyberturvallisuuden koulutusohjelmien osallistamispyrkimyksissä on puutteita, mikä viittaa siihen, että tarvitaan enemmän työtä sen varmistamiseksi, että nämä ohjelmat ovat tervetulleita ja räätälöityjä kaikkien sukupuoli-identiteettien yksilöiden tarpeisiin.

3.2. KOULUTUKSEN MIELTYMYKSET JA TARPEET

Kenttätutkimuksen tulosten perusteella tässä on kuvaus havaituista ominaisuuksista ja koulutustarpeista, oppimismieltymyksistä, koulutuksesta ja tuesta kyberturvallisuuteen osallistuville naisille.

Koulutustarpeen tunnistaminen:

Ala 1 – Perustiedot ja taidot

Ensisijaisena tavoitteena kyberturvallisuuskasvatuksessa. Erityisesti kyberturvallisuuden perusasiat ja verkkoturvallisuus. Merkittäviä puutteita esiintyy muun muassa uhkien havaitsemisessa ja reagoinnissa, pilvipalvelujen turvallisuusosaamisessa, häiriötilanteissa reagoinnissa ja palautuksessa, tietosuojassa ja -suojassa sekä riskienhallinnassa ja analysoinnissa. Koulutusohjelmilla on puututtava näihin osaamisvajeisiin. Myös pk-yrityksiin suuntautuneessa sisällössä tarvitaan voimakkaasti kyberturvallisuutta.

Alue 2 – Erikoisalat

Tämä edellyttää koulutusta, joka kattaa laajan kirjon kyberturvallisuusuhkia ja vastatoimia. Joitakin erikoistuneita aiheita, kuten uhka-analyysiä ja -hallintaa, salausta ja kehittyneitä uhkien lieventämistekniikoita, korostettiin. Koulutukseen olisi sisällyttävä sisältöä useimmin mainituista uusista uhkista, kuten tekoälyyn perustuvista kyberhyökkäyksistä, kiristysohjelmahyökkäyksistä, tietojenkalastelusta ja sosiaalisesta suunnittelusta, pilvipalvelujen tietoturvaloukkauksista ja esineiden internetin haavoittuvuuksista.

Ala 3 – Käytännön soveltaminen

Opetusmenetelmien, kuten käytännön laboratorioiden, tapaustutkimusten ja ryhmäprojektien suosiminen korostaa käytännön, vuorovaikutteisen ja reaalimaailman soveltamisen merkitystä kyberturvallisuuskoulutuksessa.

Nykyiset käytännöt:

Opetusmenetelmän osalta voimme huomata erilaisten käytäntöjen käytön, kuten tapaustutkimukset, ryhmäprojektit, käytännön laboratoriot ja luennot. On olemassa sekoitus teoreettisia ja käytännöllisiä lähestymistapoja nykyisissä koulutusohjelmissa.

Nykyiset koulutusohjelmat kattavat useita kyberturvallisuusaiheita, joiden perusaiheet asetetaan etusijalle. Joissakin ohjelmissa on kuitenkin havaittu, että pk-yrityskohtaista sisältöä ei ole.

Osallisuuden ja sukupuolten tasapuolisen edustuksen osalta joissakin ohjelmissa on toteutettu aloitteita, joilla lisätään naisten osallistumista ja luodaan sukupuolinäkökohdat huomioon ottavia koulutusympäristöjä, vaikka nämä toimet näyttävät olevan vähemmistössä.

Haasteet:

Kyberturvallisuuskoulutuksen suurimmat haasteet ovat seuraavat:

- Koulutuksen räätälöinti erilaisiin taustoihin ja osaamistasoihin on haastavaa, koska osaamista ja kokemusta on monenlaisia
- Kurssimateriaalin pitäminen ajan tasalla kyberturvallisuusuhkien nopeasta kehityksestä selviytymiseksi. Se edellyttää koulutusmateriaalien jatkuvaa päivittämistä.
- Käytännön koulutusrajoitukset, jotka johtuvat laboratoriotilojen rajoituksista, reaalimaailman simulointivalmiuksista ja realististen kyberhyökkäysskenaarioiden luomisesta käytännössä
- Opiskelijoiden pitäminen sitoutuneina ja motivoituneina, erityisesti monimutkaisella teknisellä sisällöllä, on vaikeaa.
- Teollisuuden ja koulutuksen yhteensovittaminen teoreettisen perustan tasapainottamiseksi käytännön taitoihin, jotka vastaavat teollisuuden tarpeita, asettavat haasteen.

Ehdotus koulutuksen kehittämiseksi:

- Koulutuksen räätälöinti pk-yritysten tarpeisiin: integroidaan aiheet ja taidot, jotka on erityisesti suunniteltu vastaamaan pk-yritysten kyberturvallisuustarpeisiin.
- Tehostamalla käytännön soveltamista laajentamalla käytännön, vuorovaikutteisten opetusmenetelmien käyttöä käytännön taitojen ja reaalimaailman valmiuden parantamiseksi.
- Sisältää uusia trendejä, kuten tekoälyä ja koneoppimista, digitaalista identiteettiä ja yksityisyyttä sekä eettistä hakkerointia. Niitä pidetään nyt keskeisinä painopisteinä koulutusohjelmissa.
- Osaamisvajeiden korjaaminen keskittymällä aloihin, joilla työntekijöitä ei ole, kuten uhkien havaitseminen ja reagointi, pilvipalvelujen turvallisuus ja reagointi, jotta he voivat valmistautua paremmin haasteisiin ja tulla tehokkaiksi ja häiriönsietokykyisiksi kyberagenteiksi.
- Kehitetään sukupuolten monimuotoisuutta koskevia aloitteita naisten osallistumisen lisäämiseksi kohdennettujen aloitteiden, mentoroinnin ja roolimallien avulla.

4. PK-YRITYKSEN KYBERTURVALLISUUDEN MUUTOSAGENTIN PÄTEVYYSPROFIILI

Pöytä- ja kenttätutkimuksen tulosten perusteella tässä on esimerkki CyberAgentin odotetuista tiedoista, taidoista ja kompetensseista. Nämä tulokset kuvaavat osallistujien odotettuja saavutuksia heidän kyberturvallisuutta koskevien koulutusohjelmiensa lopussa ja varmistavat, että EQF-tason 4/5 perustiedot ja taidot kehittyvät edistyneempiin ja johtajuuteen suuntautuneisiin kykyihin EQF-tasolla 6.

CyberAgentin tutkintoprofiili	**Tietämys**	**Taidot**	**Toimivalta**
EQF:n tasolla 4/5	**Kyberturvallisuuden perusteet** - Kyberturvallisuuden peruskäsitteet - Kyberuhkien tyypit (verkkourkinta, kiristysohjelmat, ddos-hyökkäykset), hyökkäysvektorit - Kyberturvallisuuden merkitys organisaation resurssien suojaamisessa. **Kyberturvallisuutta koskeva lainsäädäntö ja datakehys** - Kyberturvallisuuslainsäädäntö, standardit ja vaatimustenmukaisuusvaatimukset - Tietoturvastrategiat ja -politiikat - Tietosuoja - Riskienhallintaperiaatteet	**Turvallisuus** - Tunnistaa mahdolliset kyberturvallisuusriskit ja haavoittuvuudet - Kyberturvallisuustyökalujen ja -ohjelmistojen käyttö kyberuhkilta suojautumiseen - Edistetään kyberturvallisuuden peruskäytäntöjen käytännön soveltamista, turvallisen salasanan luomista, turvallista selaamista, sähköpostien turvallisuutta ja arkaluonteisten tietojen turvallista käsittelyä.	**Riskienhallinta ja riskien vähentäminen** - Arvioida ja lieventää mahdollisia turvallisuusuhkia **Tehokas viestintä kyberturvallisuuskysymyksistä** - Kyky viestiä tehokkaasti kyberturvallisuuskysymyksistä, - Ilmoittaa uhkista ja rikkomuksista organisaation asianmukaisiin kanaviin.

EQF:n tasolla 6	**Kehittyneet kyberturvallisuuskonseptit** - Ymmärtää kehittyneet kyberturvallisuusperiaatteet, mukaan lukien kehittyneet kyberuhat ja hyökkäysvektorit, - Tietoisuus kyberturvallisuusuhkien ja puolustusmekanismien viimeisimmistä suuntauksista. **Kyberturvallisuuslainsäädäntö ja sen noudattaminen** - Tieto kansallisesta ja kansainvälisestä kyberturvallisuuslainsäädännöstä, -standardeista ja -vaatimuksista sekä muista niiden toimialan kannalta merkityksellisistä vaatimuksista.	**Kehittynyt riskien arviointi ja hallinta** - Kyky tehdä kattavia riskinarviointeja - Kehittyneiden menetelmien ja työkalujen käyttö - Suunnitella ja toteuttaa tehokkaita riskinhallintastrategioita havaittujen riskien lieventämiseksi. **Turvallisuusarkkitehtuurin ja verkkopuolustuksen osaaminen** - Suunnitella, toteuttaa ja arvioida suojattuja verkkoarkkitehtuureja, mukaan lukien palomuurien, tunkeutumisen havaitsemisjärjestelmien (ids) ja tunkeutumisenestojärjestelmien (ips) käyttö. **Häiriötilanteisiin reagoiminen ja toipuminen** - Kyky valmistautua kyberturvallisuuspoikkeamiin, reagoida niihin ja toipua niistä, - Laaditaan elpymistä ja toiminnan jatkuvuutta koskevia suunnitelmia.	**Suunnittelu ja politiikan kehittäminen** - Kyky kehittää ja toteuttaa strategisia kyberturvallisuuspolitiikkoja ja -kehyksiä, jotka vastaavat organisaation tavoitteita ja velvoitteita. **Johtajuus kyberturvallisuusaloitteissa** - Kyberturvallisuushankkeiden ja -tiimien johtaminen ja johtaminen, mukaan lukien kyky inspiroida ja ohjata työntekijöitä kyberturvallisuusstrategioiden täytäntöönpanossa. **Päätöksenteko** - Tee eettisiä päätöksiä kyberturvallisuuskäytännöistä

Eurooppalaisen tutkintojen viitekehyksen tasolla 4/5 mahdolliset oppimistulokset voisivat olla seuraavat:

- Oppijat oppivat kyberturvallisuuden peruskäsitteet, mukaan lukien perusterminologia, kyberuhkien tyypit, kuten tietojenkalastelu, kiristysohjelmat ja DDoS-hyökkäykset, ja niiden hyökkäysvektorit.
- Oppijat pystyvät tunnistamaan mahdolliset kyberturvallisuusriskit ja haavoittuvuudet, käyttämään asiaankuuluvia välineitä ja ohjelmistoja näiden riskien lieventämiseksi ja ottamaan käyttöön kyberturvallisuuden peruskäytäntöjä, kuten turvallisen salasanan luomisen ja turvallisen selailun.
- Oppijat saavat tietoa kyberturvallisuuslainsäädännöstä, standardeista ja vaatimustenmukaisuusvaatimuksista sekä tietoturvaa ja riskinhallintaa koskevista strategioista ja käytännöistä organisaatiossa.
- Oppijat kehittävät osaamista arvioida ja lieventää mahdollisia turvallisuusuhkia tehokkaasti ja viestiä kyberturvallisuuskysymyksistä selkeästi ja tehokkaasti organisaatiossa, mukaan lukien uhkien ja tietoturvaloukkausten raportointi asianmukaisiin kanaviin.

Eurooppalaisen tutkintojen viitekehyksen tasolla 6 mahdolliset oppimistulokset voisivat olla seuraavat:

- Oppijat kehittävät kehittynyttä ymmärrystä kyberturvallisuuden periaatteista, mukaan lukien kyky tunnistaa kehittyneet kyberuhat ja hyökkäysvektorit ja pysyä ajan tasalla kyberturvallisuuspuolustuksen uusimmista trendeistä.
- Oppijat hankkivat kattavan tietämyksen kansallisesta ja kansainvälisestä kyberturvallisuuslainsäädännöstä, standardeista ja vaatimustenmukaisuusvaatimuksista, räätälöiden tämän ymmärryksen toimialansa erityistarpeisiin.
- Oppijat voivat tehdä yksityiskohtaisia riskinarviointeja kehittyneiden menetelmien ja välineiden avulla ja laatia tehokkaita riskinhallintastrategioita näiden riskien lieventämiseksi.
- Oppijat suunnittelevat, toteuttavat ja arvioivat suojattuja verkkoarkkitehtuureja, mukaan lukien kriittisten tietoturvateknologioiden, kuten palomuurien, IDS: n ja IPS: n käytön hallinta.
- Oppijat ovat taitavia suunnittelemaan ja toteuttamaan poikkeamiin reagointi- ja palautumisstrategioita, jotka varmistavat organisaation selviytymiskyvyn tehokkailla elpymis- ja jatkuvuussuunnitelmilla.
- Oppijat osoittavat johtajuutta kyberturvallisuudessa kehittämällä strategisia toimintalinjoja, hallinnoimalla kyberturvallisuushankkeita ja -ryhmiä sekä tekemällä tietoon perustuvia, eettisiä päätöksiä paineen alla.

5. LIITTEET

5.1. LISÄYS A: LUETTELO TARKASTETUISTA KIRJALLISUUDESTA

Ammatillisen koulutuksen ja korkeakoulun kyberturvallisuuskoulutuksen yleiskatsaus

1. https://ccb.belgium.be/en/ict-security-education-belgium
2. https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
3. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
4. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country=fin
5. http://www.anc.edu.ro/standarde-pregatire-profesionala/
6. http://217.73.164.21/index.php/articles/curriculum/c556+592/
7. http://217.73.164.21/index.php/articles/c560/
8. https://www.agerpres.ro/english/2023/09/19/first-master-s-program-in-romania-in-cyber-security-accredited-by-eit-digital-at-ubb-cluj-napoca--1171675
9. https://dnsc.ro/invatamant/vezi/5
10. https://www.linkedin.com/posts/eit-digital_ubb-cluj-joins-eit-digital-adding-cybersecurity-activity-7031990099756081152-Sr77/?originalSubdomain=si
11. https://www.unitbv.ro/documente/curriculum-syllabus/Master/Plan%20inv/MI_master_TIN_2017_2018_PI.pdf
12. https://mateinfo.unitbv.ro/images/2023/planuri_inv/Plan_inv_2023_2025_Tehnologii_moderne_in_ingineria_sistemelor_soft.pdf
13. https://drive.google.com/drive/folders/1h9aC1xwobVtGN4qNukWMvDPXICf62FgF
14. Espanjan kyberturvallisuusosaajien analyysi ja diagnostiikka, maaliskuu 2022, Observaciber, https://www.observaciber.es/
15. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
16. Panoraama todellinen de la Ciberseguridad en Espanaa, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
17. Catálogos de formación en Ciberseguridad, INCIBE, 2023 https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad
18. Plan Nacional de competcias digitales https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/plan-nacional-competencias-digitales.aspx
19. Suunnitelma España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
20. Digitalización de PYMES 2021–2025 -suunnitelma https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
21. Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en Ciberseguridad en ENTORNOS de las tecnologías de la información y se fijan los aspectos básicos del currículo https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963

Kyberturvallisuushaasteet ja teollisuuden tarpeet

1. El estado de la Ciberseguridad en España, Deloitte, 2022 **https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html**
2. Ferreirós Orihuel, Inés (koordinaatti). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa GEOPOLÍTICO de la I+D+i. Fundación Alternativas: 187–206 (2023) **https://digital.csic.es/handle/10261/310469**
3. El reto de la Ciberseguridad en España: YK:n haavoittuvassa asemassa oleva, Telefónica **https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/**
4. Los retos de la Ciberseguridad para las empresas españolas, Byte ti, 11 de enero de 2024 **https://revistabyte.es/tema-de-portada-byte-ti/retos-de-la-ciberseguridad/**
5. La falta de profesionales acentúa la amenaza de los Ciberataques, el Periódico de España, 7 de Marzo de 2023, **https://www.epe.es/es/tecnologia/20230307/falta-profesionales-acentua-amenaza-ciberataques-84230209**
6. Espanjan kyberturvallisuusosaajien analyysi ja diagnostiikka, maaliskuu 2022, Observaciber, **https://www.observaciber.es/**
7. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación **https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf**
8. Panoraama todellinen de la Ciberseguridad en Espana **https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf**
9. Suunnitelma España Digital 2025 **https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx**

10. Digitalización de PYMES 2021–2025 -suunnitelma https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
11. https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
12. http://data.europa.eu/esco/occupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28
13. https://nsm.no/fagomrader/digital-sikkerhet/
14. https://www.bdo.no/nb-no/nyheter/2023/na-jakter-hackerne-de-sma-selskapene
15. https://www.evelon.no/artikler/trussellandskapet-i-europa
16. https://norsis.no/sikkerhetskultur2023/sammendrag/
17. https://serit.no/hva-er-god-datasikkerhet-i-bedriften/
18. https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf

Naiset kyberturvallisuudessa

1. Microsoft. (2017, maaliskuu). Miksi Euroopan tytöt eivät opiskele STEM:ää? Microsoft News. Viitattu 20. tammikuuta 2024, osoitteesta https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf
2. Naiset menevät tekniikkaan. (2021, syyskuu). Tieto- ja viestintätekniikan työvoima Euroopassa ja sen sukupuolihaaste covid-19-pandemian jälkeen. Naiset menevät tekniikkaan. Viitattu 20. tammikuuta 2024, osoitteesta https://womengotech.com/app/uploads/2021/09/ICT-workforce-in-Europe-and-its-gender-challenge.pdf
3. Rodiklia duomena bazė – Oficialiosios statistikos portalas. (n.d.) 1. https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/
4. Bukauskas, Brilingaite, Ikamas, Juozapavicius ja Lepaite. (2022, 5. elokuuta). Ataskaita Lietuvos kibernetinio saugumo kompetencijų žemelapis. Vilnan yliopisto. Viitattu 20. tammikuuta 2024, osoitteesta https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf
5. https://www.digi.no/artikler/debatt-flere-tech-jenter-ma-til-for-a-finne-morgendagens-losninger/535073
6. https://odanettverk.no/2022/03/08/dette-er-norges-50-fremste-tech-kvinner-2022/
7. https://e24.no/naeringsliv/i/k6Goma/etterlyser-flere-kvinner-til-cybersikkerhet
8. https://www.ssb.no/befolkning/artikler-og-publikasjoner/kvinner-velger-fortsatt-kvinneyrker
9. https://live.worldbank.org/en/event/2023/women-business-law-2023
10. https://wbl.worldbank.org/en/data/exploreeconomies/romania/2023
11. https://eige.europa.eu/gender-equality-index/2022/country/RO
12. https://cybernews.com/editorial/cyber-women-grim-statistics-big-opportunities/
13. https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/
14. https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-winFerreirós Orihuel, Inés (koordinaatti). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa GEOPOLÍTICO de la I+D+i. Fundación Alternativas: 187–206 (2023) https://fundacionalternativas.org/publicaciones/iv-informe-sobre-la-ciencia-y-la-tecnologia-en-espana/
15. Mujeres Empleadas en ciencia y tecnología (reparto por sectores). España, UE-27 y UE-28. Serie 2019–2021. https://www.ine.es/jaxi/Tabla.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c02002.px&L=0
16. La mujer en la ciencia española, en datos y gráficos, EpData, 7 de marzo de 2023 https://www.epdata.es/datos/mujer-ciencia-espanola-datos-estadisticas/298
17. Espanjan kyberturvallisuusosaajien analyysi ja diagnostiikka, maaliskuu 2022, Observaciber, https://www.incibe.es/ed2026/talento-hacker/publicaciones/diagnostico-talento-ciberseguridad
18. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
19. Panoraama todellinen de la Ciberseguridad en Espanaa, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

5.2. LISÄYS B: KYSELYLOMAKE

Ammatillisen koulutuksen ja korkeakoulujen kyselylomake

Tämän kyselyn tarkoituksena on kerätä tietoa kyberturvallisuuskoulutuksen nykytilasta ja tulevista tarpeista ja auttaa muokkaamaan tehokasta kyberturvallisuutta koskevaa koulutusohjelmaa, joka on räätälöity pienten ja keskisuurten yritysten (pk-yritysten) kyberturvallisuushaasteisiin.

Kysely on jaettu neljään osaan:

- Väestö
- Opetussuunnitelma, koulutustarpeet ja oppimismieltymykset
- Osaamisvaatimukset ja tulevaisuuden taidot
- Sukupuolikohtaiset näkemykset

Kyselyn suorittaminen kestää noin 8 minuuttia.

VÄESTÖ

Mikä on maasi?
▫ Liettua
▫ Belgia
▫ Norja
▫ Türkiye
▫ Suomi
▫ Romania
▫ Espanja
▫ Puola

Missä oppilaitoksessa opetetaan tällä hetkellä?
▫ ammatillinen koulutus (ammatillinen koulutus)
▫ HEI (korkeakoulu)

Mikä on sukupuolesi?
▫ Mies
▫ Nainen
▫ Ei kannata sanoa

Kuinka monta vuotta olet ollut mukana kyberturvallisuuskoulutuksessa?
▫ Alle 1 vuosi
▫ 1–5 vuotta
▫ 6–10 vuotta
▫ Yli 10 vuotta

OPETUSSUUNNITELMA, KOULUTUSTARPEET JA OPPIMISMIELTYMYKSET

Mitkä seuraavista aiheista sisältyvät kyberturvallisuuskoulutusohjelmaan? (Valitse kaikki, mitä sovelletaan)

▫ Kyberturvallisuuden perusteet
▫ uhkien analysointi ja hallinta
▫ Edistyneet uhkien lieventämistekniikat
▫ Kryptografia
▫ Verkkoturvallisuus
▫ Kyberturvallisuuslait ja -politiikat
▫ Riskienhallinta
▫ Vastaushäiriöihin
▫ Muut: ___

Mitä opetusmenetelmiä käytät ensisijaisesti kyberturvallisuuskoulutuksessasi? (Valitse kaikki, mitä sovelletaan)

▫ Luennot
▫ Hands-on Labs
▫ tapaustutkimukset
▫ Ryhmähankkeet
▫ Verkkosimulaatiot
▫ Flipped Classroom

Muut: ___

Mitkä oppimismuodot olisivat tehokkaimpia kyberturvallisuuskoulutuksessa? (Valitse kaikki, mitä sovelletaan)

▫ Henkilökohtaiset työpajat
▫ Verkkokurssit
▫ Webinaarit
▫ Interaktiiviset simulaatiot
▫ Videotutoriaalit
▫ Hands-on practice -istunnot
▫ Muut: ___

Mitkä ovat suurimmat haasteet tehokkaassa kyberturvallisuuskoulutuksessa?

Avoin kysymys

Asteikolla 1–5, kuinka tehokkaasti nykyiset koulutusohjelmat valmistavat opiskelijoita reaalimaailman pk-yritysten kyberturvallisuushaasteisiin?

▫ Erittäin tehoton
▫ Jotain tehotonta
▫ Neutraali
▫ Jotain tehokasta
▫ Erittäin tehokas

Kuinka hyvin uskotte, että nykyinen kyberturvallisuuskoulutus vastaa pk-yritysten erityistarpeita?

1 (ei tasattu)
2 (hieman tasainen)
3 (yhteensopiva)
4 (No harmonisoitu)
5 (erittäin harmonisoitu)

Onko koulutuksessanne erityisiä aiheita tai taitoja, joilla vastataan pk-yritysten ainutlaatuisiin kyberturvallisuustarpeisiin? (Valitse kaikki, mitä sovelletaan)

▫ Peruskyberturvallisuus pk-yrityksille
▫ Riskien arviointi ja hallinta pk-yrityksissä
▫ Pk-yrityksiä koskevat vaaratilanteet
▫ Pk-yritysten tietosuoja ja yksityisyys
▫ Kyberturvallisuuspolitiikan kehittäminen pk-yrityksille
▫ Muut: ___

Kuinka usein räätälöit tai mukautat kyberturvallisuuskoulutustasi vastaamaan paremmin pk-yrityksiä?

▫ Aina
▫ Usein
▫ Joskus
▫ Harvinaan
▫ Ei koskaan

Saatko palautetta tai oletko yhteydessä pk-yritysten edustajiin tai ammattilaisiin varmistaaksesi, että koulutussisältö vastaa heidän tarpeitaan?

▫ Kyllä, säännöllisesti
▫ Joskus
▫ Harvinaan
▫ Ei koskaan

Kuinka tehokkaasti luulet kokemuksesi perusteella, että nykyinen kyberturvallisuuskoulutus auttaa pk-yritysten ammattilaisia vastaamaan kyberturvallisuushaasteisiin?

▫ Erittäin tehoton
▫ Jotain tehotonta
▫ Neutraali
▫ Jotain tehokasta
▫ Erittäin tehokas

Mitä ehdotuksia teillä on pk-yritysten kyberturvallisuuskoulutuksen tarkoituksenmukaisuuden ja tehokkuuden parantamiseksi?

Avoin kysymys

OSAAMISVAATIMUKSET JA TULEVAISUUDEN TAIDOT

Mitkä ovat mielestäsi suurimmat osaamisvajeet nykyisessä pk-yritysten kyberturvallisuusalan työvoimassa? (Valitse enintään kolme)

- ▫ uhkien havaitseminen ja reagointi
- ▫ Pilviturvallisuusosaaminen
- ▫ vaatimustenmukaisuus ja sääntelyyn liittyvä tietämys
- ▫ Tapaturmareaktio ja toipuminen
- ▫ Riskienhallinta ja analysointi
- ▫ Tietosuoja ja tietosuoja
- ▫ Kehittyvät teknologiat
- ▫ Verkkoturvallisuus

Arvioi osaamis- ja osaamistarpeet asteikosta 1 (ei tarvita) viiteen (erittäin tarpeellinen):

	Luokitus				
Riskien arviointi ja hallinta Ymmärrys riskien ja vaikutusten tyypeistä.					
Tekninen tietämys Kyberturvallisuuden tekniset näkökohdat ja käyttöjärjestelmien tuntemus, verkostoituminen ja tietokantojen hallinta.					
Häiriötilanteisiin reagoiminen ja toipuminen Tietoturvaloukkausten ja -poikkeamien tunnistaminen, niihin vastaaminen ja niistä toipuminen.					
Politiikan kehittäminen ja täytäntöönpano Tehokkaiden turvallisuuspolitiikkojen ja -käytäntöjen kehittäminen ja täytäntöönpano.					
Uhkatiedustelu ja -seuranta Pysyminen ajan tasalla uusimmista kyberturvallisuustrendeistä, uhista ja hyökkäysmenetelmistä.					
Viestintätaidot Tehokas viestintä henkilöstön, johdon ja mahdollisesti asiakkaiden kanssa kyberturvallisuuskysymyksistä.					
Tietosuoja ja tietosuoja Tietosuojan periaatteet ja arkaluonteisten tietojen suojaaminen.					

Onko mielestänne sellaisia olennaisia taitoja ja tietoja, joita ei ole lueteltu edellisessä kysymyksessä ja jotka saattavat olla erittäin tarpeellisia pk-yrityksille?

Avoin kysymys

Mihin uusiin kyberturvallisuusuhkiin pk-yritysten on mielestäsi varauduttava seuraavien viiden vuoden aikana? (Valitse enintään kolme)

- ▫ Ransomware-hyökkäykset
- ▫ IoT-haavoittuvuudet
- ▫ Pilvitietoturvaloukkaukset
- ▫ tekoälypohjaiset kyberhyökkäykset
- ▫ Sisäpiiriuhat
- ▫ Muut: ___

Mitä pidät kyberturvallisuuskoulutuksen kolmena parhaana trendinä seuraavien viiden vuoden aikana? (Valitse jopa 3 vaihtoehtoa)

▫ tekoäly ja koneoppiminen kyberturvallisuudessa
▫ Keskitytään pehmeisiin taitoihin ja tieteidenväliseen koulutukseen
▫ Quantum Computing Threats
▫ Eettinen hakkerointi ja puolustava osaaminen
▫ Digitaalinen identiteetti ja yksityisyys
▫ hajautetut turvajärjestelmät (esim. lohkoketju)
▫ Muut: ___

Onko olemassa erityisiä koulutusmenetelmiä, -työkaluja tai -alustoja, joiden uskot olevan poikkeuksellisen tehokkaita kyberturvallisuuskasvatuksessa?

Avaa teksti

Lisähuomautuksia tai ehdotuksia pk-yritysten kyberturvallisuuskoulutuksen parantamiseksi?

Avaa teksti

SUKUPUOLIKOHTAISET NÄKEMYKSET

Mikä on naisten arvioitu prosenttiosuus kyberturvallisuuskoulutusohjelmiin osallistuneista?

▫ Vähemmän kuin 10 %
▫ 10–25 %
▫ 26–50 %
▫ 51–75 %
▫ Yli 75 %

Onko olemassa erityisiä aloitteita tai strategioita, joilla kannustetaan naisia osallistumaan kyberturvallisuuskoulutukseen?

▫ Kyllä
▫ Ei

Jos vastaus on kyllä, täsmennä: ___

Uskotko, että kyberturvallisuuden alalla on riittävästi sukupuolinäkökohdat huomioon ottavia koulutusmoduuleja?

▫ Kyllä
▫ Ei
▫ Epävarmuutta
▫ Ei koske minua

Mitkä ovat kokemuksesi mukaan tärkeimmät esteet, jotka estävät naisia osallistumasta tai etenemästä kyberturvallisuuskoulutukseen ja -uraan? (Valitse kaikki, mitä sovelletaan)

▫ Tietoisuus kyberturvallisuuden mahdollisuuksista
▫ Stereotypiat tai kulttuurinormit
▫ mentoroinnin tai roolimallien puute
▫ Työ- ja yksityiselämän tasapainon haasteet
▫ Sukupuolten suosiminen teollisuudessa

▫ Muut: ___

Onko oppilaitoksellanne erityisiä toimintalinjoja tai ohjelmia, joilla edistetään erityisesti naisten monimuotoisuutta ja osallisuutta kyberturvallisuuskoulutuksessa?

▫ Kyllä
▫ Ei
▫ Ei ole varmaa

Mikä voisi tehdä kyberturvallisuuskoulutuksesta sukupuolinäkökohdat huomioon ottavampaa? (Valitse enintään kolme)

▫ Lisää naispuolisia kyberturvallisuuden ohjaajia tai koulutushenkilöstöä
▫ Tarjoa stipendejä tai kannustimia
▫ Koulutussisältöä, joka välttää sukupuoleen liittyviä vinoutumia
▫ Menestyneiden naispuolisten kyberturvallisuusammattilaisten näkyvyyden lisääminen
▫ Lisää vain naisille suunnattuja koulutustilaisuuksia
▫ Sukupuolta koskevat tapaustutkimukset ja skenaariot
▫ räätälöidyt koulutusohjelmat
▫ Mentorointimahdollisuudet
▫ Muut: ___

PK-YRITYKSIÄ KOSKEVA KYSELYLOMAKE

Kyselyn tarkoituksena on kartoittaa pk-yritysten kyberturvallisuuden muutosagenttien koulutustarpeet. Vastauksesi auttavat ymmärtämään eri pk-yritysten kyberturvallisuustietojen ja -taitojen nykytilannetta, tunnistamaan kyberturvallisuuskoulutuksen puutteita ja parantamaan tulevien koulutusohjelmien tehokkuutta.

Kysely on jaettu kolmeen osaan:

- Väestö
- Koulutustarpeet
- Osallistavuus ja naisten tarve kyberturvallisuudessa.

Kyselyn suorittaminen kestää noin 5 minuuttia.

VÄESTÖ

Mikä on maasi?

▫ Liettua
▫ Belgia
▫ Norja
▫ Türkiye
▫ Suomi
▫ Romania
▫ Espanja
▫ Puola

Mikä on nykyinen asemasi ja osastosi yrityksessä?

Sijainti: ___
Osasto: ___

Mikä on sukupuolesi?

▫ Mies
▫ Nainen

▫ Ei kannata sanoa

Kuinka monta työntekijää yrityksessä työskentelee?

▫ enintään 10 työntekijää
▫ 11–50
▫ 51–250

Miten arvioisit työntekijöiden nykyistä kyberturvallisuusosaamista ja -taitoja?

▫ Aloittelija
▫ Välituote
▫ Edistynyt

Kuinka moni työntekijä tekee kyberturvallisuuteen liittyvää työtä?

Lisätään numero: ___

Palkkaatko ulkopuolisia palveluita kyberturvallisuustyöhön?

▫ Kyllä
▫ Ei

KOULUTUSTARPEET

Asteikolla 1–5 (erittäin tehokas) kuinka tehokkaasti nykyiset koulutusohjelmat valmistavat opiskelijoita reaalimaailman pk-yritysten kyberturvallisuushaasteisiin?

1- Tehoton
5 Erittäin tehokas

Mitkä ovat mielestäsi suurimmat osaamisvajeet nykyisessä pk-yritysten kyberturvallisuusalan työvoimassa? (Valitse enintään kolme)

▫ uhkien havaitseminen ja reagointi
▫ Pilviturvallisuusosaaminen
▫ vaatimustenmukaisuus ja sääntelyyn liittyvä tietämys
▫ Tapaturmareaktio ja toipuminen
▫ Riskienhallinta ja analysointi
▫ Tietosuoja ja tietosuoja
▫ Kehittyvät teknologiat
▫ Verkkoturvallisuus
▫ Muut: ___

Arvioi asteikosta 1 (ei tarvita) viiteen (olennaiseen) osaamistarpeeseen ja osaamistarpeeseen:

	Luokitus				
Riskien arviointi ja hallinta Ymmärrys riskien ja vaikutusten tyypeistä.					
Tekninen tietämys Kyberturvallisuuden tekniset näkökohdat ja käyttöjärjestelmien tuntemus, verkostoituminen ja tietokantojen hallinta.					
Häiriötilanteisiin reagoiminen ja toipuminen Tietoturvaloukkausten ja -poikkeamien tunnistaminen, niihin vastaaminen ja niistä toipuminen.					
Politiikan kehittäminen ja täytäntöönpano Tehokkaiden turvallisuuspolitiikkojen ja -käytäntöjen kehittäminen ja täytäntöönpano.					
Uhkatiedustelu ja -seuranta Pysyminen ajan tasalla uusimmista kyberturvallisuustrendeistä, uhista ja hyökkäysmenetelmistä.					
Viestintätaidot Tehokas viestintä henkilöstön, johdon ja mahdollisesti asiakkaiden kanssa kyberturvallisuuskysymyksistä.					
Tietosuoja ja tietosuoja Tietosuojan periaatteet ja arkaluonteisten tietojen suojaaminen.					

Onko mielestänne sellaisia olennaisia taitoja ja tietoja, joita ei ole lueteltu edellisessä kysymyksessä ja jotka saattavat olla erittäin tarpeellisia pk-yrityksille?
Avoin kysymys
Mihin uusiin kyberturvallisuusuhkiin pk-yritysten on mielestäsi varauduttava seuraavien viiden vuoden aikana? (Valitse enintään kolme)
▫ Ransomware-hyökkäykset
▫ IoT-haavoittuvuudet
▫ Pilvitietoturvaloukkaukset
▫ tekoälypohjaiset kyberhyökkäykset
▫ Sisäpiiriuhat
▫ Muut: ___
Mitä erityisiä puutteita, jos sinulla on, mielestäsi työntekijän nykyisessä kyberturvallisuustiedossa tai -taidossa?
▫ Matala tekninen osaaminen
▫ Pehmeiden taitojen alhainen taso
▫ Alhaisen haavoittuvuuden arviointi
▫ Poliittisten ja määräysten alhainen ymmärrys
▫ Matala tietoisuus uhkasta
▫ Säännöllisten kyberturvallisuuskoulutusten alhainen taso
▫ Muut: ___
Mitä pidät kyberturvallisuuskoulutuksen kolmena parhaana trendinä seuraavien viiden vuoden aikana? (Valitse jopa 3 vaihtoehtoa)
▫ tekoäly ja koneoppiminen kyberturvallisuudessa
▫ Keskitytään pehmeisiin taitoihin ja tieteidenväliseen koulutukseen
▫ Quantum Computing Threats
▫ Eettinen hakkerointi ja puolustava osaaminen
▫ Digitaalinen identiteetti ja yksityisyys
▫ hajautetut turvajärjestelmät (esim. lohkoketju)
▫ Muut: ___

OSALLISTAVUUS JA NAISTEN TARPEET KYBERTURVALLISUUDESSA
Katsotteko, että nykyinen kyberturvallisuuskoulutus on osallistavaa ja vastaa tehokkaasti kaikkien sukupuolten tarpeisiin?
▫ Kyllä
▫ Ei
▫ Ei ole varmaa
Onko sinulla ollut esteitä tai haasteita pääsyssä kyberturvallisuuskoulutukseen tai -tutkimuksiin osallistumisessa?
▫ Kyllä
▫ Ei
▫ Ei kannata sanoa
▫ Jos kyllä, täsmennä: ___
Oletko tietoinen organisaatiossasi olevista aloitteista tai ohjelmista, jotka erityisesti tukevat tai edistävät naisten osallistumista kyberturvallisuuteen?
▫ Kyllä
▫ Ei
▫ Ei ole varmaa
Minkä tyyppinen tuki tai resurssit kannustaisivat organisaatiossasi useampia naisia osallistumaan kyberturvallisuuskoulutukseen? (Avoin)
Avoin kysymys

Mitä parannuksia tai innovaatioita ehdottaisitte kyberturvallisuuskoulutuksen tehokkuuden parantamiseksi?
Avoin kysymys

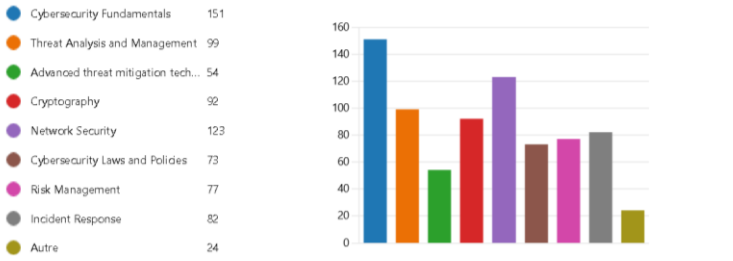
5.3. LISÄYS C: KYSELYN TULOKSET

Ammatillinen koulutus ja korkeakoulut

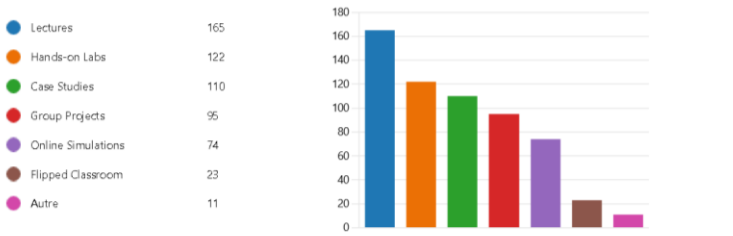
Mapping the training needs for SME Cyber Security Change Agents - VET and HEI survey

190 Responses

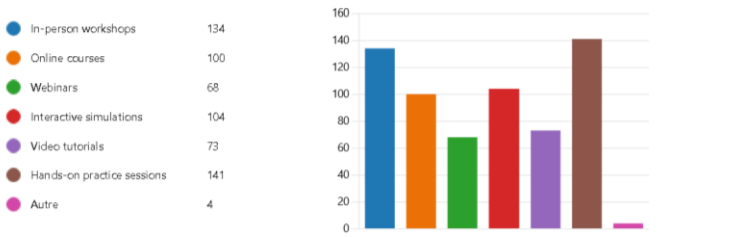
1. **Which of the following topics are included in your cybersecurity training program? (Select all that apply)**



2. **What teaching methods do you primarily use in your cybersecurity training? (Select all that apply)**



3. **What teaching method would be the most effective for cybersecurity training? (Select all that apply)**



4. **What are the biggest challenges you face in delivering effective cybersecurity training?**

190
Réponses

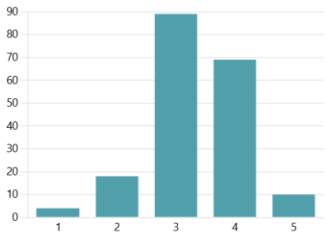
Dernières réponses
"-"
"-"
"keeping up with Technology Changes, Basic knowledge of the students, Soft...

Mettre à jour

34 répondants (**19**%) répondu **students** pour cette question.

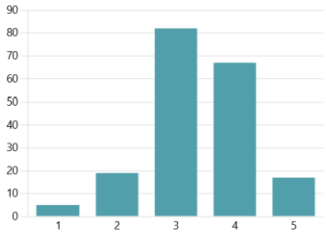
5. **On a scale of 1 (Very Ineffective) to 5 (Very Effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.33
Évaluation moyenne



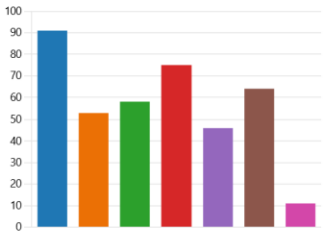
6. **On a scale of 1 (Not aligned) to 5 (Highly aligned), how well do you believe the current cybersecurity training aligns with the specific needs of SMEs?**

3.38
Évaluation moyenne



7. **Are there specific topics or skills that you include in your training to address the unique cybersecurity needs of SMEs? (Select all that apply)**

Basic Cybersecurity for SMEs	91
Risk Assessment and Managem...	53
Incident Response for SMEs	58
Data Protection and Privacy for ...	75
Cybersecurity Policy Developme...	46
No SME's specific topic or skills ...	64
Autre	11



8. **How often do you customize or adapt your cybersecurity training to better cater to SMEs?**

Always	14
Often	60
Sometimes	55
Rarely	47
Never	14

9. **Do you receive feedback or are you in contact with SME representatives or professionals to ensure the relevancy of your training content to their needs?**

Yes, regularly	43
Occasionally	64
Rarely	54
Never	29

10. **Based on your experience, how effective do you believe the current cybersecurity training is in equipping SME professionals to handle cybersecurity challenges?**

Very Ineffective	7
Somewhat Ineffective	21
Neutral	65
Somewhat Effective	88
Very Effective	9

11. **What suggestions do you have for improving the relevance and effectiveness of cybersecurity training for SMEs?**

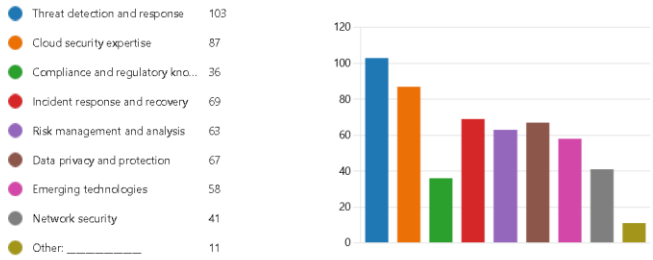
117
Réponses

Dernières réponses
"leverage external expertise, practical hands-on exercises, interactive training...

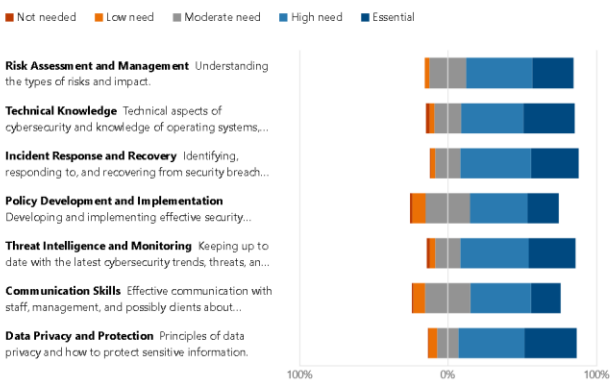
Mettre à jour

36 répondants (**31**%) répondu **trainings** pour cette question.

12. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



13. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



14. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

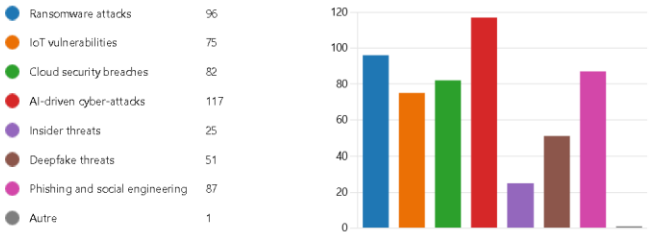
190
Réponses

Dernières réponses
"-"
"-"
"Cloud Security, AI"

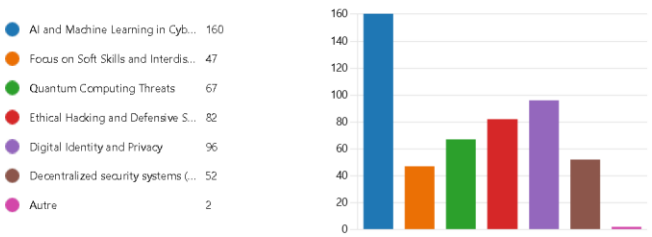
Mettre à jour

10 répondants (**5**%) répondu **skills** pour cette question.

15. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Are there any particular training methods, tools, or platforms that you believe are exceptionally effective for cybersecurity education?**

115
Réponses

Dernières réponses
"TryHackMe, HackTheBox"

Mettre à jour

12 répondants (**11**%) répondu **platform** pour cette question.

18. **Any additional comments or suggestions for improving cybersecurity training for SMEs?**

80
Réponses

Dernières réponses
"Uniform Course material"

Mettre à jour

9 répondants (**11**%) répondu **SMEs** pour cette question.

19. **What is the estimated percentage of women among the participants in your cybersecurity training programs?**

Less than 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
More than 75%	3

20. **Are there any specific initiatives or strategies you employ to encourage women's participation in cybersecurity training?**

Yes	30
No	160

21. **If you replied "Yes" to the previous question, please specify**

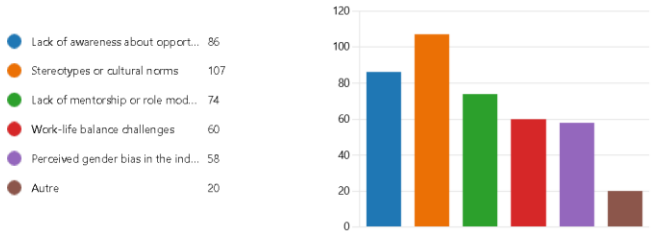
35
Réponses

Dernières réponses

13 répondants (**37**%) répondu **women** pour cette question.

22. **Do you believe there are enough gender-inclusive training modules available in cybersecurity?**

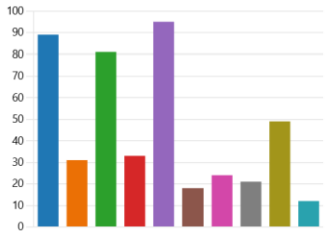
23. **In your experience, what are the primary barriers that prevent women from participating or advancing in cybersecurity training and careers? (Select all that apply)**



24. **Does your institution have specific policies or programs to promote diversity and inclusion, particularly for women, in cybersecurity training?**

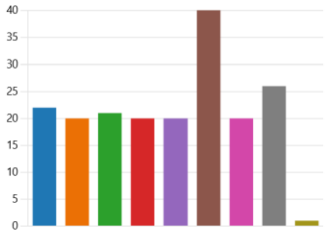
25. **What could make cybersecurity training more gender-inclusive? (Choose up to three)**

More female cybersecurity instr...	89
Regularly update policies to sup...	31
Offer scholarships or incentives	81
Training content that avoids gen...	33
Increased visibility of successful ...	95
More women-only training sessi...	18
Gender-inclusive case studies a...	24
Tailored training programs	21
Mentorship opportunities	49
Autre	12



26. **What is your country?**

Lithuania	22
Belgium	20
Norway	21
Türkiye	20
Finland	20
Romania	40
Spain	20
Poland	26
Azerbaijan	1



27. **In which school institution are you currently teaching?**

VET (Vocational Education and T...	86
HEI (Higher Education (HE) Instit...	104

28. **What is your gender?**

Male	121
Female	64
Prefer not to say	5

29. **How many years have you been involved in cybersecurity training? (Either general, specific, short and long trainings)**

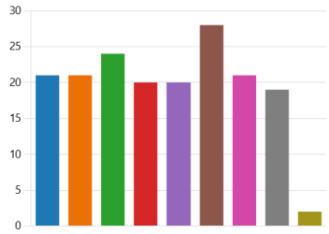
Less than 1 year	21
1-5 years	85
6-10 years	53
More than 10 years	31

Mapping the training needs for SME Cyber Security Change Agents - SMEs survey

176 Responses

1. **What is your country?**

Lithuania	21
Belgium	21
Norway	24
Türkiye	20
Finland	20
Romania	28
Spain	21
Poland	19
Azerbaijan	2



2. **What is your company sector?**

176
Réponses

Dernières réponses
"Consultancy"
"Cyber Security - Management Consultancy"
"Education, VET"

Mettre à jour

13 répondants (**7**%) répondu **education** pour cette question.

3. **What is your current position in the company?**

176
Réponses

Dernières réponses
"Team lead"
"Owner & Director"
"Teacher"

Mettre à jour

43 répondants (**25**%) répondu **Manager** pour cette question.

4. **What is your gender?**

5. **How many employees are working in the company?**

6. **How would you rate employees' current level of cybersecurity knowledge and skills?**

7. **How many employees perform work related to cybersecurity?**

176
Réponses

Dernières réponses
"3"
"2"
"3"

Mettre à jour

36 répondants (**21**%) répondu **1** pour cette question.

8. **How many of these employees are women?**

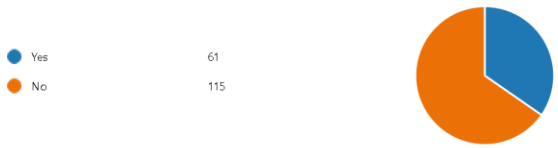
176
Réponses

Dernières réponses
"1"
"1"
"0"

Mettre à jour

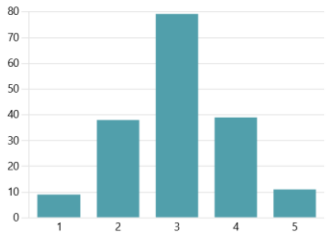
31 répondants (**18**%) répondu **1** pour cette question.

9. **Do you hire external services for cybersecurity work?**



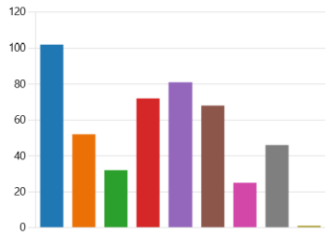
10. **On a scale of 1 (ineffective) to 5 (very effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.03
Évaluation moyenne

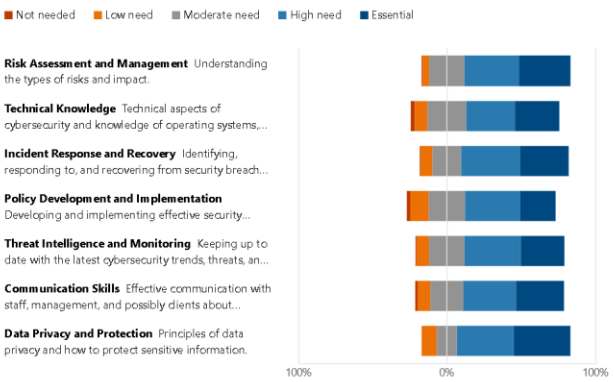


11. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**

Threat detection and response	102
Cloud security expertise	52
Compliance and regulatory kno...	32
Incident response and recovery	72
Risk management and analysis	81
Data privacy and protection	68
Emerging technologies	25
Network security	46
Other: _____	1



12. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



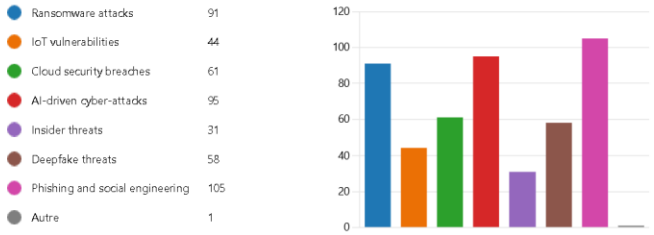
13. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

175
Réponses

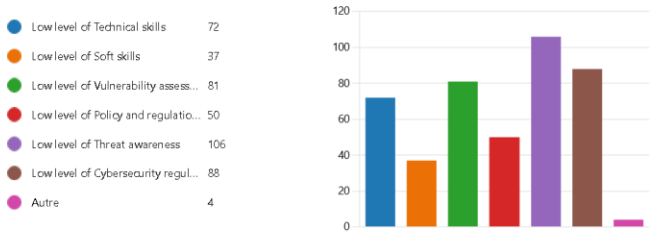
Dernières réponses
"My assumption is that Subject matter experts (SME's) in a big company are ...
"Cyber Security on all these topics arround Generative AI - which is complete...
"Not sure"

4 répondants (**2**%) répondu **skills** pour cette question.

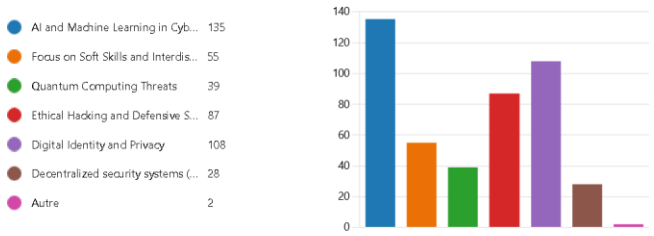
14. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



15. **What specific gaps, if any, do you feel exist in employee's current cybersecurity knowledge or skills status? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**

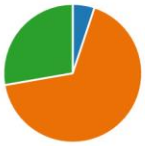


17. **Do you feel that current cybersecurity training is inclusive and addresses the needs of all genders effectively?**

Yes	82
No	29
Not sure	65

18. **If you identify as female, have you faced any barriers or challenges in accessing or participating in cybersecurity training/studies?**

Yes	7
No	92
Prefer not to say	38



19. **If you replied "Yes" to the previous question, please specify**

11
Réponses

Dernières réponses
"I feel that previous question is missing one more answer such as "I'm a male...
"I have to actively look for help and support for us females who work in the C...

Mettre à jour

3 répondants (**30**%) répondu **male** pour cette question.

20. **Are you aware of any initiatives or programs within your organization that specifically support or promote the participation of women in cybersecurity?**

Yes	18
No	158

21. **If you replied "Yes" to the previous question, please specify**

17
Réponses

Dernières réponses
"I am a strong female advocate for Cyber Security, Women Supporting Wom..."

8 répondants (**47**%) répondu **Women** pour cette question.

5.4. LISÄYS D: LUETTELO TARKASTETUISTA ESCO-AMMATEISTA

Viitteet:

2529.1 https://esco.ec.europa.eu/sites/default/files/chief%20ICT%20security%20officer.pdf
2529.2 https://esco.ec.europa.eu/sites/default/files/digital%20forensics%20expert.pdf
2529.3 https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F1c5a896a-e010-4217-a29a-c44db26e25da
2529.4 https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
2529.5 https://esco.ec.europa.eu/sites/default/files/ICT%20resilience%20manager.pdf
2529.6 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20administrator.pdf
2529.7 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20consultant.pdf
2529.8 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20manager.pdf
2529.9 https://esco.ec.europa.eu/sites/default/files/knowledge%20engineer.pdf

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau