Co-funded by the European Union

HYVIEN KÄYTÄNTÖJEN OPAS PK-YRITYKSILLE

CYBER AGENT 06.2026

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

Euroopan unionin rahoittama. Esitetyt näkemykset ja mielipiteet ovat ainoastaan tämän tekstin laatijoiden näkemyksiä eivätkä välttämättä vastaa Euroopan unionin tai Euroopan koulutuksen ja kulttuurin toimeenpanovirasto (EACEA) kantaa. Euroopan unioni ja EACEA eivät ole vastuussa niistä.

www.cyberagents.eu

Työpaketti 6: Tulosten jakaminen ja hyödyntäminen

Toimitettava 6.4: Hyvien käytäntöjen opas pk-yrityksille

Työpaketin 6 vetäjä: Women4Cyber Foundation

SISÄLTÖ

TAULUKOIDEN LUETTELO

JOHDANTO

CyberAgent-projekti kehitettiin kolmen vuoden aikana kahdeksassa Euroopan maassa: Romaniassa, Belgiassa, Norjassa, Espanjassa, Turkissa, Puolassa, Liettuassa ja Suomessa. CyberAgent-hanke perustettiin kehittämään ja testaamaan modulaarista, helposti saatavilla olevaa kyberturvallisuuskoulutusohjelmaa pk-yritysten työntekijöille, ammatillisen koulutuksen opiskelijoille sekä korkeakouluopiskelijoille. Tämän työn keskeinen tulos on ”kyberturvallisuuden muutosagentti”: koulutettu, ei-asiantuntija-taustainen työntekijä, joka toimii organisaationsa sisäisenä yhteyshenkilönä kyberturvallisuustietoisuuden edistämisessä.

Tässä oppaassa hankkeen toteutuskokemukset on muunnettu käytännön ohjeiksi pk-yrityksille. Siinä selitetään, mikä on muutosagenttirooli, miten sopiva henkilö tunnistetaan ja nimitetään, miten hänen koulutustaan tuetaan ja miten varmistetaan, että sukupuolten tasa-arvo otetaan huomioon prosessissa alusta alkaen. Oppaan lopussa oleva tarkistuslista auttaa pk-yrityksiä varmistamaan, että oikeat edellytykset ovat olemassa jokaisessa vaiheessa.

1. MIKSI KYBERTURVALLISUUS ON TÄRKEÄÄ JOKAISELLE PK-YRITYKSELLE

ENISA:n Threat Landscape 2025 -raportin mukaan kyberrikolliset teollistavat hyökkäyksiään, mikä tekee pk-yrityksistä arvokkaita kohteita niiden koosta ja toimialasta riippumatta. Yleisimmät uhat, joihin organisaatiot nykyään joutuvat, ovat kiristyshaittaohjelmat, tietojenkalastelu ja tietoturvaloukkaukset. Kiristyshaittaohjelmat ja tietoturvaloukkaukset muodostavat jo suurimman osan EU:n organisaatioihin kohdistuvista kyberrikoksista, ja kiristyshaittaohjelmien osuus rikoksista on yli 80 prosenttia. Näiden hyökkäysten teollistuminen, erityisesti ”Ransomware-as-a-Service” -malli, on madaltanut hyökkääjien kynnystä, jolloin jopa pienimmät organisaatiot ovat tulleet kannattaviksi kohteiksi.

Erityisesti pk-yrityksille kyberhyökkäyksen seuraukset eivät rajoitu vain väliaikaisiin häiriöihin. ENISA:n mukaan kyberturvallisuushyökkäyksillä on vakavia kielteisiä vaikutuksia 90 %:n pk-yritysten liiketoimintaan jo viikon kuluttua tapahtumasta. Tästä riskialttiudesta huolimatta pk-yrityksillä on harvoin omaa IT- tai tietoturvahenkilöstöä, eikä niiden työntekijöille järjestetä juurikaan järjestelmällistä kyberturvallisuuskoulutusta. Euroopan pk-yritykset työllistävät noin 100 miljoonaa ihmistä ja tuottavat yli puolet Euroopan BKT:stä. Siksi pk-yritysten kyberturvallisuusvaje on taloudellinen ja yhteiskunnallinen riski.

Suurin osa kyberhyökkäyksistä onnistuu inhimillisten tekijöiden vuoksi, kuten phishing-linkin klikkaamisen, heikkojen salasanojen tai vahvistamattomien sähköpostiviestien vuoksi. Tämä tarkoittaa, että ensimmäinen puolustuslinja ei ole tekninen työkalu, vaan asiantunteva ja tietoinen työntekijä, joka tietää, mitä varoa ja mitä tehdä, kun jokin menee pieleen. Juuri tätä roolia hoitaa kyberturvallisuuden muutosagentti.

2. KYBERTURVALLISUUDEN MUUTOSAGENTTI

Kyberturvallisuuden muutosagentti -konsepti on CyberAgent-projektin ytimessä. Tässä osiossa selitetään, mikä rooli on kyseessä, miksi se kehitettiin ja miltä se näyttää käytännössä pienissä ja keskisuurissa yrityksissä (pk-yrityksissä).

2.1. MIKÄ SE ON JA MIKSI SITÄ TARVITAAN

Pk-yritykset ovat Euroopan talouden selkäranka, mutta ne kuuluvat edelleen organisaatioihin, jotka ovat kaikkein alttiimpia kyberturvallisuusuhille. Toisin kuin suuryrityksissä, useimmilla pk-yrityksillä ei ole erillistä IT- tai tietoturvaosastoa, ja niiden työntekijät saavat harvoin järjestelmällistä kyberturvallisuuskoulutusta. Tämä johtaa jatkuvaan eroon pk-yritysten kohtaamien kyberriskien ja niiden torjumiskykyjen välillä.

CyberAgent-hanke ja kyberturvallisuuden muutosagentti -rooli on suunniteltu korjaamaan tätä aukkoa rakentamalla uudenlaista osaamista olemassa oleviin tiimeihin. Kyberturvallisuuden muutosagentti on koulutettu, ei-tekninen työntekijä, joka toimii sisäisenä asiantuntijana kyberturvallisuustietoisuudessa, kannustaa turvallisempaan käyttäytymiseen, tunnistaa yleisiä riskejä ja ottaa käyttöön parempia kyberturvallisuuskäytäntöjä organisaatiossa. Tämä henkilö toimii myös kollegoiden oppaana, joka ohjaa heidät asianmukaiseen tukeen tietoturvaloukkausten sattuessa.

Tämän roolin tarpeellisuus vahvistuu CyberAgent-pilottihankkeen aikana kerätyillä havainnoilla. Kahdeksassa kumppanimaassa koulutukseen osallistui 594 rekisteröitynyttä osallistujaa, joihin kuului pk-yritysten työntekijöitä sekä korkeakoulujen ja ammatillisen koulutuksen opiskelijoita. Pk-yritysten työntekijät tunnistetaan yleisesti kohderyhmäksi, jota on vaikeinta tavoittaa ja pitää mukana koulutustilanteissa, pääasiassa aikarajoitteiden ja työvelvollisuuksien vuoksi. Siitä huolimatta pk-yritysten työntekijöiden korkea kurssin suorittamisaste heijastaa kyberturvallisuustietoisuuden todellista merkitystä heidän päivittäisessä työssään.

2.2. KESKEISET VASTUUALUEET

Kyberturvallisuuden muutosagentti ei ole vastuussa kyberturvallisuusongelmien ratkaisemisesta yksin. Rooli perustuu tietoisuuden lisäämiseen, viestintään ja koordinointiin: hän on organisaatiossa se henkilö, joka pitää kyberturvallisuuden esillä ja auttaa työtovereita suoriutumaan siitä päivittäisessä työssään. Mikään tästä ei vaadi teknistä asiantuntemusta. Sen sijaan tarvitaan luotettava henkilö, jolla on hyvät yhteydet organisaatiossa ja joka on motivoitunut tekemään kyberturvallisuudesta luonnollisen osan tiimin työskentelyä.

Käytännössä rooli tarkoittaa joukkoa toistuvia, kevyitä toimintoja, jotka eivät vaadi paljon aikaa, mutta joilla on merkittävä vaikutus organisaation tietoturvakulttuuriin:

- **Säännöllinen tietoisuuden lisääminen**. Muutosagentti jakaa säännöllisesti kollegoille tiedotteita yleisimmistä uhkista, kuten phishing-sähköposteista, heikoista salasanoista, vaarallisesta tietojen käsittelystä ja epäilyttävistä linkeistä, pitäen kyberturvallisuuden esillä ilman, että siitä tulee taakka. Tämä voi olla niin yksinkertaista kuin kuukausittainen viesti tiimin chatissa, lyhyt muistutus ennen kiireistä jaksoa tai tiedote alalla leviävästä uudesta huijausmuodosta. Muoto on vähemmän tärkeää kuin säännöllisyys.

- **Kyberturvallisuuden pitäminen kokousten esityslistalla**. Muutosagentti nostaa kyberturvallisuuteen liittyviä aiheita esiin tiimikokouksissa lyhyiden, käytännönläheisten keskustelujen kautta. Kyse ei ole pitkistä esityksistä tai virallisista koulutustilaisuuksista. Viiden minuutin keskustelu äskettäisestä tietojenkalasteluyrityksestä tai muistutus salasanojen päivittämisestä riittää pitämään tietoisuuden yllä ja viestittämään, että kyberturvallisuus on koko organisaation yhteinen vastuu, ei pelkästään tietotekniikan henkilöstölle tarkoitettu tehtävä.

- **Kannustetaan ilmoittamaan tietoturvaloukkauksista**. Yksi kyberturvallisuuden muutosagenttien tärkeimmistä tehtävistä on luoda kulttuuri, jossa työntekijät uskaltavat ilmoittaa epäilyttävistä tilanteista, kuten epätavallisesta sähköpostista, järjestelmän odottamattomasta käyttäytymisestä tai siitä, että kollega on napsauttanut jotain, mitä hänen ei olisi pitänyt. Monet kyberturvallisuusloukkaukset kärjistyvät, koska työntekijät eivät ilmoita varhaisista varoitusmerkeistä pelätessään nöyryytystä tai syyllistämistä. Muutosagentti auttaa normalisoimaan ilmoittamisen olemalla lähestyttävä ja selventämällä prosessia selkeästi.

- Uusien työntekijöiden **perehdyttämisen tukeminen**. Uudet työntekijät kuuluvat kyberturvallisuuden näkökulmasta organisaation haavoittuvimpiin jäseniin, koska he eivät tunne sisäisiä menettelytapoja, luottavat todennäköisemmin odottamattomiin pyyntöihin eivätkä usein ole vielä saaneet koulutusta perusturvallisuuskäytännöistä. Muutosagentilla on tärkeä rooli kyberturvallisuuden perusteiden esittelyssä perehdyttämisen aikana, jolloin varmistetaan, että hyvät tavat vakiintuvat ensimmäisestä päivästä lähtien sen sijaan, että niitä jouduttaisiin korjaamaan jälkikäteen.

- **Toimiminen sisäisenä yhteyshenkilönä**. Kyberturvallisuuden muutosagentti on henkilö, johon kollegat kääntyvät, kun heillä on kyberturvallisuuteen liittyvä kysymys tai he eivät ole varmoja siitä, miten tietyssä tilanteessa tulisi toimia. Tämä tarkoittaa, että he tietävät, mistä agentin löytää, kenelle asia tulisi eskaloida ja miten ohjata kollega oikean tuen pariin. Pk-yrityksissä, joissa ei ole erillistä IT-henkilöstöä, tämä rooli täyttää aukon, joka muuten jättäisi työntekijät ilman selkeää yhteyshenkilöä.

- **Koulutuksen ja jatkuvan oppimisen edistäminen**. Muutosagentti kannustaa työtovereita hyödyntämään käytettävissä olevia koulutusresursseja, mukaan lukien CyberAgent-moduulit, ja pysyy ajan tasalla organisaation toimialaan ja toimintaan liittyvistä kyberturvallisuusalan kehityksistä.

- **Palautteen kerääminen ja välittäminen eteenpäin**. Muutosagentti kerää organisaation sisällä palautetta kyberturvallisuuteen liittyvistä huolenaiheista: siitä, mikä työntekijöiden mielestä on epäselvää, mitä käytäntöjä ei noudateta ja mitkä riskit tuntuvat kiireellisimmiltä, ja välittää nämä havainnot johdolle. Juuri tämän palautekierron ansiosta organisaatio voi parantaa turvallisuuskulttuuriaan ajan myötä.

Taulukko 1. Teknisten työntekijöiden tehtävien ja muutosagenttien tehtävien ero

IT-ASIANTUNTIJA (tekninen rooli)	KYBERTURVALLISUUDEN MUUTOSAGENTTI (johtava ja kulttuurinen rooli)
Määrittää palomuurit ja tietoturvajärjestelmät	Jakaa räätälöityjä tietoisuutta lisääviä viestejä ja tietoturvavaroituksia työtovereille
Hallinnoi ohjelmistopäivityksiä, korjauspäivityksiä ja teknisiä määrityksiä	Pitää kyberturvallisuuden jatkuvasti sisäisen tiimin kokousten esityslistalla
Reagoi käynnissä oleviin kyberturvallisuusuhkiin ja teknisiin tietoturvaloukkauksiin	Kannustaa kollegoita ilmoittamaan epäilyttävistä toiminnoista aktiivisesti ja avoimesti
Valvoo verkkoliikennettä, turvallisuuslokeja ja teknisiä vaatimustenmukaisuusparametrejä	Tukee uusia työntekijöitä organisaation perehdytysprosessin aikana kyberhygienian perusperiaatteiden osalta
Ottaa käyttöön teknisiä turvallisuustoimenpiteitä ja hallinnoi infrastruktuurin käyttöoikeuksia	Kerää jatkuvasti palautetta henkilöstöltä ja välittää järjestelmälliset huolenaiheet johdolle tai IT-osastolle

3. KYBERTURVALLISUUDEN MUUTOSAGENTTIEN VALINTA JA NIMEAMINEN

Oikean henkilön löytäminen kyberturvallisuuden muutosagentiksi ja hänelle menestymisen edellytysten luominen ovat ratkaisevia päätöksiä, kun roolia otetaan käyttöön organisaatiossa. CyberAgent-pilotti osoitti, että rooli toimii parhaiten, kun sen täyttää henkilö, jota pidetään luotettavana, joka tuntee yrityksen menettelytavat ja jota johto tukee. Tässä osiossa annetaan käytännön ohjeita siitä, miten rooli määritellään selkeästi pitkän aikavälin menestyksen varmistamiseksi ja miten oikea ehdokas löydetään.

3.1. KUINKA LÖYTÄÄ OIKEA EHDOKAS

CyberAgent-pilottihankkeen tulosten perusteella tehokkaimmat kyberturvallisuuden muutosagentit eivät välttämättä ole henkilöitä, joilla on aiempaa teknistä taustaa. Kahdeksassa pilottimaassa ne pk-yritysten edustajat, jotka osallistuivat koulutukseen aktiivisimmin ja osoittivat suurinta potentiaalia, olivat niitä, joilla oli sekä organisaatiotuntemusta että viestintätaitoja sekä aitoa motivaatiota saada aikaan muutosta työpaikallaan. Pilottihankkeen kokemusten perusteella seuraavat ominaisuudet tukevat yleensä menestystä tässä roolissa:

- Organisaation sisäisten prosessien ja tietojenkäsittelykäytäntöjen tuntemus.
- Hyvät viestintä- ja vuorovaikutustaidot.
- Johdon tuki

Tärkeää on, että rooli ei vaadi teknistä tai IT-taustaa. Siksi hallinnollisissa tehtävissä, henkilöstöhallinnossa, operatiivisissa tehtävissä ja johdossa työskentelevät työntekijät voivat hoitaa muutosagenttitehtävää tehokkaasti, edellyttäen että he saavat riittävää koulutusta ja tukea. Teknisten edellytysten poistaminen on tietoinen suunnitteluvalinta, joka laajentaa merkittävästi sopivien ehdokkaiden joukkoa ja avaa oven sukupuolten monimuotoisuudelle, kuten pilottiprojekti osoitti.

Kun ehdokas on löydetty, rooli on saatava näkyväksi ja vakiinnutettavaksi organisaation sisällä. Roolin laajuus tulisi tiedottaa koko organisaatiolle, ja se tulisi määritellä selkeästi: mistä kyberturvallisuuden muutosagentti on vastuussa, kenelle hän raportoi ja mitä hänen ei odoteta tekevän.

3.2. ROOLIN KÄYTTÖÖNOTTO

Seuraava vaihe on roolin käyttöönotto organisaatiossa. Seuraavat vaiheet perustuvat suoraan CyberAgent-pilottihankkeesta kumppanimaissa saatuihin oppeihin, ja ne on suunniteltu sopiviksi kaiken kokoisille pk-yrityksille.

3.2.1. VALITSE JA KOULUTA KYBERTURVALLISUUDEN MUUTOSAGENTTI

Tunnista organisaatiostasi sopivin henkilö ja anna hänelle pääsy CyberAgent-koulutusohjelmaan. Ohjelma koostuu yhdeksästä moduulista, jotka kattavat tietoturvaohjelman hallinnan (M1), järjestelmänhallinnan (M2), analyysityökalut (M3), tietoturvatoiminnot (M4), tietoturvan hallinnon ja politiikan (M5), kyberturvallisuussuunnittelun (M6), riskienhallinnan (M7), liiketoiminnan jatkuvuuden (M8) sekä kyberturvallisuusalan uran edistämisen (M9). Nämä yhdeksän moduulia on virallisesti koottu kahteen viralliseen projektituotokseen: D3.1, joka kattaa korkeakoulujen opetussuunnitelman, ja D3.2, joka kattaa ammatillisen koulutuksen opetussuunnitelman. Tässä oppaassa mainitut moduulit vastaavat siten suoraan D3.1:ssä ja D3.2:ssa kuvattua sisältöä, ja niihin pääsee CyberAgent-alustan kautta riippumatta oppijan oppilaitoksesta. Lisäksi opetussuunnitelma on sovitettu pk-yritysten työntekijöille tarkoitettuihin EQF-tasoihin 4–6, ja se tarjoaa kyberturvallisuuden perustaitoja ja -tietoja, joita voidaan soveltaa käytännössä teknisillä, analyyttisillä, riskienhallinnan ja organisaation osaamisalueilla.

Koulutus on omaan tahtiin suoritettavaa ja saatavilla verkossa, mikä tarkoittaa, että valittu työntekijä voi suorittaa sen joustavasti nykyisten työtehtäviensä ohella. Kun moduuli on suoritettu ja tietotesti läpäisty vähintään 75 prosentin tuloksella, muutosagentti saa kyseisen moduulin kurssin suorittamistodistuksen, joka toimii virallisena todisteena hankituista osaamisista ja jota voidaan käyttää muutosagentin koulutuksen dokumentointiin organisaatiossa.

3.2.2. MÄÄRITÄ VASTUUT JA INTEGROI NE OLEMASSA OLEVIIN RAKENTEISIIN

Kun koulutus on käynnissä tai saatu päätökseen, organisaation tulisi määritellä virallisesti kyberturvallisuuden muutosagentti roolin vastuut ja integroida rooli olemassa oleviin rakenteisiin. Tämä tarkoittaa sitä, että sovitaan siitä, mitä muutosagentti tekee, kuinka paljon aikaa hän käyttää rooliin ja kenen kanssa hän koordinoi toimintaansa, sekä viestitään tästä koko tiimille.

Pilotti osoitti, että kyberturvallisuuden muutosagenttirooli on kestävimmillään, kun se liitetään johonkin organisaatiossa jo olemassa olevaan rakenteeseen sen sijaan, että se toimisi erillisenä. Tämä voi tarkoittaa sen liittämistä säännöllisen tiimikokouksen esityslistalle tai yhdistämistä olemassa olevaan työterveys- ja turvallisuus- tai sääntöjen noudattamisen rakenteeseen. Tavoitteena on tehdä kyberturvallisuustietoisuudesta normaali osa päivittäistä työtä ja yhteinen organisaation vastuu, ei erillinen toiminta.

3.2.3. LISÄÄ SISÄISTÄ TIETOISUUTTA ROOLISTA

Muutosagentti ei voi toimia tehokkaasti, jos kollegat eivät tiedä, kuka hän on tai mitä hän tekee. Jotta valitulle työntekijälle voidaan antaa toimimiseen tarvittava organisaation tuki, on välttämätöntä lähettää selkeä sisäinen tiedote, jossa kuvataan hänen roolinsa ja vastuualueensa, sekä järjestää säännöllisiä kokouksia, joissa työntekijät voivat esittää kysymyksiä.

Alkuilmoituksen lisäksi muutosagenttia tulisi kannustaa pitämään kyberturvallisuus näkyvänä organisaatiossa säännöllisten tapaamisten avulla. Tämä ei tarkoita pitkiä koulutustilaisuuksia tai muodollisia esityksiä. Pk-yrityksissä tämä voitaisiin toteuttaa lyhyiden aktiviteettien muodossa, jotka liittyvät suoraan tilanteisiin, jotka työntekijät tunnistavat päivittäisestä työstään.

3.2.4. SÄÄNNÖLLINEN ARVIOINTI JA YLLÄPITO PITKÄLLÄ AIKAVÄLILLÄ

Jotta kyberturvallisuuden muutosagenttirooli voisi tuottaa kestävää vaikutusta, organisaation on luotava edellytykset sen jatkumiselle ja kehittymiselle. Tämä tarkoittaa vähintään kerran vuodessa toteutettavan arviointiprosessin rakentamista, jotta voidaan arvioida, mikä toimii, mitä puutteita on jäljellä ja tarvitseeko muutosagentti lisäkoulutusta tai tukea.

Pilottikokeilun tulokset osoittavat, että sitoutumisen ylläpitäminen vaatii enemmän kuin alkuperäisen koulutuksen. Pk-yritysten osallistujat tarvitsevat jatkuvasti joustavia määräaikoja, muistutuksia ja satunnaista tukea, jotta vauhti säilyy. Yksinkertaisen vuosittaisen arvioinnin sisällyttäminen prosessiin ja sen varmistaminen, että muutosagentilla on jatkuva pääsy resursseihin ovat vähimmäisedellytykset roolin tehokkuuden säilyttämiselle pitkällä aikavälillä.

4. SUKUPUOLTEN TASAPAINO JA OSALLISTAVUUS

Kyberturvallisuus on edelleen yksi Euroopan talouden miesvaltaisimmista aloista. Naiset edustavat noin 20 prosenttia kyberturvallisuusalan työvoimasta EU:ssa, ja sama epätasapaino näkyy myös kyberturvallisuuskoulutukseen osallistumisessa. Samalla ala kärsii jatkuvasta osaaja- ja osaamisvajeesta. Kun merkittävä osa potentiaalisesta työvoimasta jää hyödyntämättä, alan on vaikea vastata nykyisen uhkaympäristön edellyttämään kasvavaan kysyntään.

CyberAgent-hanke suunniteltiin siten, että sukupuolten osallistaminen oli nimenomainen tavoite, ei jälkikäteen lisätty ajatus. Alalla, jolla naiset muodostavat tyypillisesti pienen vähemmistön koulutukseen osallistujista, naisten suuri osuus pilottihankkeessa on merkittävä tulos, joka syntyi kohdennettujen tiedotusstrategioiden ja osallistavan lähestymistavan ansiosta.

4.1. MIKSI TÄMÄ ON TÄRKEÄÄ PK-YRITYKSILLE

Erityisesti pk-yrityksille kyberturvallisuuden sukupuolinäkökulma on sekä työvoimakysymys että organisaatiokulttuurikysymys. Useimmilla pk-yrityksillä ei ole erillistä kyberturvallisuushenkilöstöä. Niiden kyberresilienssi riippuu kaikkien työntekijöiden tietoisuudesta ja käyttäytymisestä, erityisesti hallinto-, henkilöstö-, talous- ja operatiivisten tehtävien parissa työskentelevien. Siksi naisten sulkeminen pois kyberturvallisuustietoisuuskoulutuksesta on turvallisuusaukko.

Samalla kyberturvallisuuden muutosagenttirooli tarjoaa konkreettisen mahdollisuuden puuttua kyberturvallisuuden sukupuolten epätasapainoon pk-yritysten sisältä käsin. Koska rooli perustuu viestintätaitoihin, organisaatiotietoisuuteen ja hallintotapaan pikemminkin kuin tekniseen asiantuntemukseen, se sopii hyvin monenlaisille ammattiprofiileille ja tarjoaa ei-teknisissä tehtävissä työskenteleville naisille tunnustetun polun kyberturvallisuusvastuuseen ilman, että se edellyttää uranvaihtoa tai teknistä pätevyyttä.

4.2. KÄYTÄNNÖN TOIMENPITEET NAISTEN JA ALIEDUSTETTUJEN RYHMIEN TAVOITTAMISEKSI

Seuraavat käytännön toimet perustuvat CyberAgent-pilottihankkeen kokemuksiin, ja ne on suunniteltu siten, että ne ovat toteutettavissa kaikenkokoisissa pk-yrityksissä.

Belgialainen pilottihanke osoitti, että naisten osallistumista voidaan lisätä kanavoimalla tiedotusta verkostojen kautta, joihin naiset jo luottavat, kuten ammattijärjestöt ja naisyrittäjien verkostot. Käytännössä tämä tarkoittaa, että kun pk-yritys etsii ehdokkaita kyberturvallisuuden muutosagentiksi, sen tulisi ottaa aktiivisesti yhteyttä alalleen tai alueelleen relevantteihin naisten ammattiverkostoihin sen sijaan, että se luottaisi pelkästään julkisiin ilmoituksiin.

Määrittele rooli organisaation kannalta merkittävän vaikutuksen perusteella, ei teknisen asiantuntemuksen perusteella. Ei-teknisissä tehtävissä työskentelevät naiset ovat todennäköisemmin kiinnostuneita kyberturvallisuuskoulutuksesta ja ottavat muutosagenttitehtävän vastaan, kun rooli esitetään sen organisaatiolle tuoman arvon perusteella eikä teknisten taitojen perusteella. Tehtävä voidaan määritellä rooliksi, joka suojaa yritystä, tukee kollegoita ja edistää hallintoa. Sisäisessä viestinnässä, työnkuvauksissa ja rekrytointimateriaaleissa käytetyllä kielellä on merkitystä.

5. PARHAAT KÄYTÄNNÖT

Kyberturvallisuuden muutosagenttiin nimittäminen on tärkeä ensimmäinen askel, mutta rooli voi tuottaa kestävää vaikutusta vain, jos se toimii organisaatiokulttuurissa, joka tukee sitä aktiivisesti. Seuraavat parhaat käytännöt on suunniteltu auttamaan pk-yrityksiä luomaan oikeat olosuhteet, jotta muutosagentti voi menestyä ja kyberturvallisuustietoisuus voi tulla luonnolliseksi osaksi organisaation toimintaa.

- **Kannusta avoimeen viestintään**. Työntekijöiden tulisi voida ilmoittaa virheistä, epäilyttävistä tilanteista tai tietoturvaan liittyvistä huolenaiheista ilman pelkoa syyllistämisestä tai nöyryytyksestä. Monissa organisaatioissa kyberturvallisuusvälikohtaukset kärjistyvät juuri siksi, että työntekijät epäröivät ilmoittaa asioista, joista he eivät ole varmoja tai joista he tuntevat olevansa vastuussa.

- **Pidä asiat yksinkertaisina ja integroi ne päivittäisiin rutiineihin**. Kyberturvallisuustietoisuuden ei tarvitse ilmetä virallisten koulutustilaisuuksien tai pitkien työpajojen muodossa. Lyhyet, käytännönläheiset muistutukset, jotka on integroitu olemassa oleviin rutiineihin, ovat usein tehokkaampia kuin satunnaiset intensiivikoulutukset. Tavoitteena on tehdä kyberturvallisuudesta taustalla toimiva tapa pikemminkin kuin jaksottainen tapahtuma.

- **Dokumentoi jokainen vaihe**. Yksi käytännöllisimmistä toimista, joihin pk-yritys voi ryhtyä, on kirjata ylös perustason kyberturvallisuuskäytännöt: miten salasanoja hallitaan, miten arkaluontoisia tietoja säilytetään ja jaetaan, mitä tehdä, kun epäilyttävä sähköposti saapuu, ja keneen ottaa yhteyttä, jos tapahtuu tietoturvaloukkaus. Näiden ei tarvitse olla virallisia ohjeistuksia. Yhden sivun pituinen ohje, joka on kaikkien työntekijöiden saatavilla riittää.

- **Aloita ylhäältä**. Johtajien ja johdon on näkyvästi näytettävä esimerkkiä siitä käyttäytymisestä, jota työntekijöiltä odotetaan. Jos johto ei noudata perusturvallisuuskäytäntöjä, se viestittää, että nämä käytännöt ovat vapaaehtoisia. Muutosagenttien uskottavuus organisaatiossa riippuu osittain siitä, tukeeko ympäröivä kulttuuri sitä, mitä he yrittävät edistää.

- **Tietoisuuden lisääminen on jatkuvaa työtä**. Kyberturvallisuusuhkat kehittyvät jatkuvasti, ja yksittäinen koulutustilaisuus vanhenee nopeasti. Tietoisuuden lisäämistä on pidettävä jatkuvana prosessina eikä kertaluonteisena toimena. Tämä tarkoittaa säännöllisiä yhteydenottoja, jaksottaisia kertauskursseja sekä kyberturvallisuuden muutosagenttia, joka pysyy ajan tasalla ja tuo jatkuvasti ajankohtaista tietoa organisaatioon.

5.1. KANSALLISTEN PILOTTIPROJEKTIEN LAADULLINEN PALAUTE

Laadullisen palautteen perusteella osallistujat suhtautuivat koulutukseen yleisesti ottaen myönteisesti, ja monet totesivat, ettei merkittäviä parannuksia tarvittu. Avoimissa vastauksissa (D5.3 – CyberAgentin osaamisen kehittämiskoulutusohjelman arviointi) toistuvimmat teemat olivat: alustan käytettävyys, navigointi tai arviointiprosessi; tekniset saatavuus- tai luotettavuusongelmat; saavutettavuuden, joustavuuden ja laajan tietämyksen tuoma positiivinen arvo; toiveet käytännönläheisemmistä tapauksista, käytännön harjoituksista tai todellisista pk-yritysten esimerkeistä; sisällön tiheys, rakenne tai oppimispolkujen eriyttäminen.

Erityisesti kolmanneksi useimmin mainittu aihe (saavutettavuuden, joustavuuden ja laajan tietämyksen tuoma positiivinen arvo) heijastaa niiden osallistujien arvostusta, jotka totesivat, ettei parannuksia tarvita, ja korostivat ohjelman vahvuuksia spontaanisti. Tämä on merkityksellinen signaali: avoimessa tekstikentässä, joka oli tarkoitettu kritiikin keräämiseen, lähes neljännes laadullisista vastauksista ilmaisi tyytyväisyyttä koulutuksen saavutettavuuteen ja laajuuteen.

5.2. TOIMENPITEET KOULUTUKSEN TOTEUTTAMISEKSI JA HALLINNOIMISEKSI PK-YRITYKSISSÄ

CyberAgent-alustan laajamittainen pilotointi kahdeksassa Euroopan maassa tarjosi tärkeitä oivalluksia siitä, miten pienet ja keskisuuret yritykset omaksuvat ja ylläpitävät kyberturvallisuuden osaamisen kehittämistä. Lopullisessa koulutuksen arviointiraportissa (D5.3) dokumentoitujen sekamenetelmällä kerättyjen todisteiden ja oppijoiden kohtaamien esteiden perusteella yritysjohtajille suositellaan seuraavien sisäisten hallinnollisten, teknisten ja strategisten toimien toteuttamista koulutuksen organisatorisen vaikutuksen optimoimiseksi.

Laadunhallintaa koskevia neuvoja

CyberAgent-oppimateriaalit sisältävät huomattavan määrän operatiivista ja strategista tietoa. Johtajien tulisi välttää koko opetussuunnitelman antamista kerralla; sen sijaan modulaarisen aikataulun laatiminen ehkäisee kognitiivista väsymystä ja varmistaa osaamisen sujuvamman siirtymisen osaksi yrityksen päivittäisiä rutiineja.

Tekniseen integrointiin liittyvät suositukset

Pilottivaiheen alustavat havainnot osoittivat, että tekniset käyttöönottoon liittyvät haasteet, kuten viivästyneet tai roskapostisuodattimien estämät rekisteröitymisen vahvistusviestit, voivat hidastaa koulutuksen käyttöönottoa ja osallistujien sitoutumista sen alkuvaiheessa. Ennen käyttäjien rekisteröimistä koulutusalustalle organisaation johdon tulisi varmistaa yhdessä IT-ylläpidon kanssa, että ulkoisiin verkko-oppimisympäristöihin liittyvä liikenne ja sähköpostit sallitaan asianmukaisesti. Lisäksi henkilöstöä on hyvä ohjeistaa tarkistamaan myös roskapostikansionsa rekisteröitymisprosessin aikana.

Strategista käyttöönottoa koskevat suositukset

Kansalliset pilottitiedot paljastivat, että korkeamman tason strategiset moduulit – erityisesti M6 (kyberturvallisuussuunnittelu) ja M8 (liiketoiminnan jatkuvuus) – vaativat vankkaa taustakokemusta, jotta niitä voidaan hyödyntää täysimääräisesti. Välittömän liiketoiminnallisen arvon maksimoimiseksi nämä moduulit tulisi kohdistaa erityisesti henkilöstölle, jolla on johtamis-, operatiivisia tai liiketoiminnan hallintovastuita.

5.2.1. MUUTOSAGENTTIEN NÄKEMYKSIÄ

Pilottivaiheessa, johon kertyi 272 kattavaa kyselyvastausta kahdeksasta Euroopan maasta, paljastui kolme kohderyhmiin vaikuttavaa monialaista vaikutusta.

Joustava toteutus ja työn sekä opiskelun yhteensovittaminen

Peräti 86,0 % vastaajista oli samaa mieltä tai täysin samaa mieltä siitä, että asynkroninen, omaan tahtiin suoritettava muoto oli riittävän joustava integroitavaksi saumattomasti heidän ammatillisiin ja akateemisiin aikatauluihinsa, mikä antoi pk-yritysten työntekijöille mahdollisuuden tasapainottaa osaamisen kehittämistä päivittäisten operatiivisten tehtävien kanssa.

Menetelmällinen merkitys ei-tekniselle henkilöstölle

Pilottivaiheen tulokset vahvistavat CyberAgent-opetussuunnitelman keskeisen koulutussuunnittelun ja osoittavat, että tehokas organisaation kyberresilienssi ei vaadi edistyneitä teknisiä tai IT-ohjelmointitaitoja. D5.3:n vaikutustenarviointitietojen mukaan 77,2 % osallistujista ilmoitti, että koulutuksen ansiosta he pystyivät selvästi ymmärtämään, miten heidän omat ammatilliset roolinsa vaikuttavat ja suojaavat yrityksen päivittäisiä tietoturvakäytäntöjä.

Mitattava tietojen lisääntyminen ei-asiantuntijoiden lähtötasosta

Alustan analytiikka osoittaa, että 89,3 % kaikista osallistujista saavutti todennetun kasvun kyberturvallisuustietämyksessään. Ratkaisevaa on, että tämä kehitys oli näkyvintä aivan aloittelijoiden keskuudessa: 90,9 % oppijoista, jotka arvioivat alkuperäisen ymmärryksensä ”erittäin heikoksi” ennen ohjelmaa, ilmoitti merkittävän parannuksen tietämyksessään ja luottamuksessaan tunnistaa yrityksen kyberriskit.

5.2.2. ”MITÄ TEHDÄ JA MITÄ VÄLTTÄÄ”

Pilottimaista saadun ”oppimispolkujen eriyttämistä” koskevan palautteen perusteella esitämme suosituksia yrityksille:

Taulukko 2 ”Mitä tehdä ja mitä välttää”

ÄLÄ (pk-yritysten sudenkuopat)	SUOSITELTAVAA (parhaat käytännöt)
Odottaa, että työntekijä kuuntelee kaikki 8 moduulia epärealistisen tiiviissä aikataulussa (esim. viikon tai kuukauden kuluessa). Pilottitutkimukset (D5.3) paljastivat, että päivittäisistä työtehtävistä johtuva ajanpuute oli pk-yritysten työntekijöiden suurin este, mikä johti alhaisempaan kokeen läpäisyasteeseen.	Laaditaan joustava, yksilöllinen oppimisaikataulu työntekijän tarpeiden ja aikataulun mukaan soveltaen mikro-oppimisen periaatteita. Annetaan oppijoille mahdollisuus keskittyä moduuleihin, jotka parantavat suoraan heidän työtehtäviensä vaikutusaluetta.
Odottaa, että koulutettu kyberturvallisuuden muutosagentti korvaisi erikoistuneen IT-insinöörin tai ratkaisisi itsenäisesti monimutkaisia kyberturvallisuusvälikohtauksia. Ydinteknisen infrastruktuurin odotusten siirtäminen ei-tekniselle henkilöstölle aiheuttaa suurta roolien epäselvyyttä.	Muutosagenttia kannustetaan toimimaan sisäisenä tietoturvakoordinaattorina ja tietoisuuden lisääjänä. He ovat tehokkaimmillaan edistettäessä turvallisuuskulttuuria, muistuttaessa sisäisistä koulutuksista ja esittäessä lyhyitä päivityksiä tiimikokouksissa.
E-oppimisprosessin jättäminen täysin valvomatta toimimaan automaattisesti ilman yrityksen näkyvyyttä. Yksi rekisteröitymislinkki ei takaa pitkäaikaista organisaatiolle koituvaa arvoa.	Käytetään jäsenneltyä seurantakehystä (kuten taulukko 3) virstanpylväiden seuraamiseen ja sisäisen mentoroinnin osoittamiseen. Pilottiarvioinnin (D5.3) havainnot vahvistavat, että nimetyn esimiehen tai mentorin olemassaolo korreloi selvästi testin vahvistetun loppuun saattamisen kanssa.

ÄLÄ (pk-yritysten sudenkuopat)	SUOSITELTAVAA (parhaat käytännöt)
Itsenäisen opiskelun salliminen täysin erillisenä, jolloin on vaarana, että yksittäiset oppimisen esteet tai piilevät tekniset vaikeudet jäävät huomaamatta. Ilman vuorovaikutusta aloittelijat usein jumittuvat ja luopuvat ohjelmasta hiljaa, kun he joutuvat pulaan.	Yhdistämällä omaan tahtiin etenevän opiskelun proaktiivisiin operatiivisiin kosketuspisteisiin, kuten lyhyisiin tilannekatsauksiin tai digitaalisiin muistutuksiin. Aktiivinen johdon sitoutuminen poistaa suoraan oppimisen esteitä, nostaa työntekijöiden motivaatiota ja kurssien suoritusastetta.

6. SUUNNITELMA KYBERTURVALLISUUDEN MUUTOSAGENTTIROOLIN KÄYTTÖÖNOTTAMISEKSI

Kyberturvallisuuden muutosagenttiroolin onnistunut käyttöönotto alkaa jo kauan ennen varsinaista nimitystä. Ajan käyttäminen organisaation nykytilan arviointiin, sisäisen tuen rakentamiseen ja roolin selkeään määrittelyyn alusta alkaen lisää merkittävästi pitkän aikavälin menestymisen mahdollisuuksia. Seuraavat vaiheet on suunniteltu opastamaan pk-yrityksiä käytännössä tämän valmisteluvaiheen läpi.

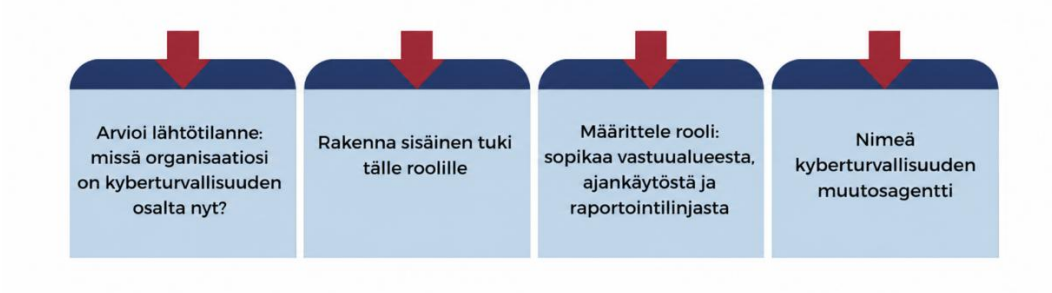
1. Ensimmäinen vaihe on arvioida, missä vaiheessa organisaatio tällä hetkellä on. Tämä tarkoittaa rehellistä tarkastelua jo käytössä olevista – tai puuttuvista – kyberturvallisuuskäytännöistä. Ovatko työntekijät tietoisia perusuhkista, kuten tietojenkalastelusta? Onko epäilyttävien tapahtumien ilmoittamiseen olemassa menettelytapa? Käsitelläänkö arkaluonteisia tietoja yhdenmukaisesti koko tiimissä?

2. Toinen vaihe on luoda sisäistä tukea roolille. Muutosagentti ei voi toimia tehokkaasti ilman johdon tukea. Ennen ehdokkaan valitsemista päätös roolin perustamisesta tulisi keskustella ja sopia johtotasolla, ja siihen tulisi sisältyä selkeä sitoumus ajan varaamiseen, roolin viralliseen tunnustamiseen sekä roolin hoitajan aktiiviseen tukemiseen.

3. Kolmas vaihe on määritellä rooli ennen sen täyttämistä. Tämä tarkoittaa sitä, että sovitaan vastuualueista, odotetusta ajankäytöstä ja siitä, miten rooli sijoittuu olemassa olevaan organisaatiorakenteeseen. Selkeä toimeksianto, vaikka se olisi vain yksinkertainen yhden kappaleen kuvaus, välttää epäselvyyksiä ja antaa tulevalle kyberturvallisuuden muutosagentille tarvittavan legitiimiyden toimia.

Kun nämä kolme vaihetta on toteutettu, organisaatio on valmis tunnistamaan ja nimittämään oikean ehdokkaan. Seuraavassa osiossa esitetään tarkistuslista, joka ohjaa roolin onnistunutta käyttöönottoa.

Kuva1 – Visuaalinen etenemissuunnitelma kyberturvallisuuden muutosagenttitehtävän käyttöönottoon



7. TARKISTUSLISTA

Seuraavaa tarkistuslistaa on tarkoitettu käytettäväksi sen varmistamiseen, että kyberturvallisuuden muutosagentin onnistuneen käyttöönoton keskeiset edellytykset ovat täyttyneet. Se perustuu CyberAgent-pilottihankkeesta saatuihin kokemuksiin.

7.1. JOHTAMINEN

[ ] Muutosagenttiroolista on sovittu virallisesti ja sille on varattu määrärahat

[ ] Selkeä toimeksianto on määritelty: laajuus, ajallinen sitoumus ja raportointisuhteet

[ ] Nimityksestä on tiedotettu koko organisaatiolle

[ ] Roolin arviointi on suunniteltu toteutettavaksi seuraavien 12 kuukauden kuluessa

[ ] Muutosagentti on varannut aikataulussaan aikaa roolinsa hoitamiseen

7.2. HENKILÖSTÖASIAT

[ ] Valintaprosessi oli avoin kaikille, sukupuolesta tai taustasta riippumatta

[ ] Tehtävästä tiedotettiin sen organisaatiovaikutusten, ei teknisen osaamisen, näkökulmasta

[ ] Muutosagenttiin liittyvät vastuut on kirjattu hänen toimenkuvaansa tai tavoitteisiinsa

[ ] Uudet työntekijät tutustuvat kyberturvallisuuden muutosagenttiin perehdyttämisen yhteydessä

[ ] Muutosagenttien koulutuksista ja sertifioinneista pidetään kirjattuna

7.3. KYBERTURVALLISUUDEN MUUTOSAGENTTI

[ ] Rekisteröitynyt CyberAgent-alustalle ja sopinut oppimispolusta

[ ] Suorittanut vähintään yhden moduulin ja saanut todistuksen

[ ] Kollegat tietävät, miten he voivat ottaa yhteyttä muutosagenttiin

[ ] Kyberturvallisuuden peruskäytännöt on dokumentoitu ja ne ovat koko henkilöstön saatavilla

[ ] Säännölliset tiedotustilaisuudet on otettu käyttöön (kokoukset, viestit tai muistutukset)

[ ] Työtovereilla on käytössään selkeä menettely epäilyttävien tilanteiden ilmoittamiseksi

[ ] Kyberturvallisuutta koskevaa palautetta kerätään ja välitetään säännöllisesti johdolle

8. MITEN ONNISTUNUTTA KÄYTTÖÖNOTTOA MITATAAN

Kyberturvallisuuden muutosagenttiroolin toteuttaminen on jatkuva sitoumus. Seuraavat indikaattorit voivat auttaa pk-yrityksiä arvioimaan, onko roolilla todellista vaikutusta ajan mittaan.

[ ] Kyberturvallisuustietoisuustoimiin osallistuvien työntekijöiden määrä on kasvanut muutoksen edistäjän nimittämisen jälkeen

[ ] Kyberturvallisuudesta keskustellaan säännöllisesti tiimikokouksissa, eikä sitä enää pidetä poikkeuksellisena aiheena

[ ] Työntekijät tietävät, kuka muutosagentti on, ja uskaltavat kääntyä hänen puoleensa kysymyksillä tai huolenaiheilla

[ ] Ilmoitettujen epäilyttävien sähköpostiviestien, tapahtumien tai huolenaiheiden määrä on kasvanut

[ ] Muutosagentti on suorittanut lisäkoulutusmoduuleja nimityksensä jälkeen

[ ] Organisaation sisällä kerätään säännöllisesti henkilöstön palautetta kyberturvallisuudesta ja siihen reagoidaan

8.1. JOHDON OHJEET MALLIPOHJAN MUKAUTTAMISEEN JA RÄÄTÄLÖINTIIN

Jotta kyberturvallisuuden muutosagenttien osaamisen kehittäminen johtaa yrityksen pitkäaikaiseen kestävyyteen, jatkuva rakenteellinen seuranta on välttämätöntä. Taulukossa 3 on käytännöllinen seurantamalli, joka on suunniteltu pk-yritysten johtajille organisaation lähtötason arvioimiseksi ennen koulutusta sekä konkreettisen turvallisuuskulttuurin kehityksen mittaamiseksi 6 ja 12 kuukautta nimeäisen jälkeen.

Johtajien tulisi käsitellä tätä mallia dynaamisena viitekehyksenä. Yrityksenne koon, toimialan ja olemassa olevan infrastruktuurin mukaan teitä kannustetaan mukauttamaan ja laajentamaan tätä matriisia:

- **Asteikkojen mukauttaminen**
  Mikro-pk-yritykset (alle 10 työntekijää) voivat yksinkertaistaa prosenttipohjaisia mittareita suoraan työntekijämääriksi seurannan helpottamiseksi.
- **Indikaattoreiden laajentaminen**
  Yrityksille, jotka toimivat erittäin digitalisoiduissa tai riskialttiissa ympäristöissä, suositellaan lisäämään tavoitteisiin liittyviä rivejä, kuten ”monivaiheista todennusta (MFA) käyttävien työntekijöiden osuus” tai ”keskimääräinen vasteaika simuloituun uhkaan”.
- **Lokalisointi**
  Sovita ”Suositeltu tietolähde” -sarake yrityksesi sisäisiin viestintäkanaviin (esim. seuranta Slackin kautta, MS Teamsin kyselyt tai fyysiset lokit tiimikokouksissa).

Taulukko 3. Nimeämisen jälkeisen seurannan malli pk-yritysten johtajille

Menestysindikaattori	Yksikkö / mitta-asteikko	Lähtötilanne (ennen)	Edistyminen (6 kuukautta)	Tavoite (12 kuukautta)	Suositeltu tietolähde
Työntekijöiden valmius torjua phishing-hyökkäyksiä	Epäilyttäviä sähköposteja luottavaisesti käsittelevien työntekijöiden osuus	%	%	%	Sisäinen pulssikysely tai CyberAgent-alustan tiedot
Kokousten integrointitiheys	Niiden tiimikokousten lukumäärä, joissa kyberturvallisuus otettiin esille	Lukumäärä	Lukumäärä	Lukumäärä	Tiimikokousten pöytäkirjat/esityslistat
Tapahtumien raportointiaktiivisuusaste	Ilmoitettujen ja dokumentoitujen epäilyttävien tapahtumien lukumäärä	Lukumäärä / kuukausi	Lukumäärä / kuukausi	Määrä / kuukausi	Sisäinen turvallisuustapahtumaloki tai IT-palautekierros
Muutosagenttien näkyvyys	Henkilöstön osuus, joka tietää tarkasti, kuka muutosagentti on	%	%	%	Lyhyt sisäinen kysely
Alustan edistymissitoumus	Mikro-oppimiseen aktiivisesti osallistuvien työntekijöiden määrä	Lukumäärä	Lukumäärä	Lukumäärä	CyberAgent-alustan hallinnoijan analytiikkapaneeli

JOHTOPÄÄTÖS

Kyberturvallisuus ei ole enää vain suurten organisaatioiden, joilla on omat IT-osastot, huolenaihe. Uhkaympäristön kehittyessä ja pk-yrityksiin kohdistuvien sääntelyvaatimusten kiristyessä herää kysymys, miten ne voivat puolustautua käytettävissään olevilla resursseilla.

Kyberturvallisuuden muutosagentti -rooli tarjoaa käytännöllisen ja oikeasuhteisen vastauksen tähän kysymykseen. Se ei vaadi asiantuntijan palkkaamista, investointeja kalliisiin työkaluihin tai olemassa olevien prosessien perusteellista uudistamista. Sen sijaan se edellyttää oikean henkilön löytämistä organisaatiosta, hänelle annettavaa koulutusta ja toimivaltuuksia sekä sellaisten olosuhteiden luomista, joissa kyberturvallisuustietoisuus tulee osaksi jokapäiväistä työelämää.

CyberAgent-projekti on osoittanut, että tämä on mahdollista. Kahdeksassa Euroopan maassa pk-yritysten työntekijät, joilla ei ollut teknistä taustaa, suorittivat koulutuksen, ottivat roolin vastaan ja alkoivat vaikuttaa siihen, miten heidän organisaationsa suhtautuivat kyberturvallisuuteen. Todisteet ovat selkeät: kun pääsyn kynnystä madalletaan, kun rooli määritellään organisaatiokulttuurin eikä teknisen asiantuntemuksen pohjalta ja kun osallistaminen nähdään suunnitteluperiaatteena eikä jälkikäteen lisättynä ajatuksena, tulokset seuraavat perässä.

Tämä opas on kutsu ottamaan se ensimmäinen askel. Suunnitelma on valmis. Työkalut ovat käytettävissä. Tehtävä on ulottuvilla jokaiselle pk-yritykselle, joka on valmis panostamaan henkilöstöönsä.

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 Grupo

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

IT Akademija

ProxyLab

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau