

Eurooppalaisten mallien vertailu pienyritysten kyberturvallisuuden tukemisessa



Kaakkois-Suomen
ammattikorkeakoulu

KYMEN
LAAKSON
LIITTO



Euroopan unionin
osarahoittama

CyberCare
Kymi

Tervetuloa!



Raportti on tehty Xamkin toteuttamassa CyberCare Kymi –hankkeessa, jota rahoittaa Kymenlaakson liitto Euroopan Unionin Oikeudenmukaisen siirtymän rahastosta (JTF).

Lisätietoa hankkeen palveluista:
<https://kyberasema.fi>

Laita meille viestiä: cybercare@xamk.fi

Sisällysluettelo

Johdanto	1
Mitä voimme oppia muista Euroopan maista	3
Belgia	5
Ranska	9
Suomi	12
Vertailu ja suositukset Suomelle	16
Lähteet	17



Johdanto

Tämä raportti on osa CyberCare Kymi -hankkeen työpakettia 3, jossa keskitytään kyberturvallisuuden kehittämiseen erityisesti sosiaali- ja terveysalan mikro- ja pienyritysten näkökulmasta. Digitalisaation nopea eteneminen, potilastietojen käsittelyn vaatimukset, sekä uusi EU:n NIS2-direktiivi tuovat mukanaan uusia velvoitteita ja haasteita myös niille toimijoille, joilla ei ole omaa IT-henkilöstöä tai aikaisempaa osaamista kyberturvasta.

Tässä raportissa vertaillaan Suomen kyberturvallisuuden tukirakenteita kahteen Euroopan maahan: Belgiaan ja Ranskaan. Molemmat tarjoavat esimerkkejä konkreettisista toimintamalleista, jotka soveltuvat myös Suomen kontekstiin. Belgia erottuu vaiheistetulla ja visuaalisella itsearviointilla, kun taas Ranska korostaa sektorikohtaisuutta ja reaaliaikaista tukea. Vertailun perusteella esitetään kehitysehdotuksia, joiden tavoitteena on parantaa suomalaisen sote-sektorin pienyritysten kybervalmiuksia.

Raportin rakenne seuraa maakohtaista esittelyä ja päättyy vertailuun sekä suosituksiin. Jokaisessa luvussa tuodaan esiin käytännön työkalut, tukitoiminnot ja ohjausmallit, joita Suomessa voitaisiin soveltaa tai kehittää edelleen.

Huomio: Tämä raportti on suunnattu erityisesti julkisille päättäjille, sote-sektorin tukiorganisaatioille, mikroyrityksille sekä kaikille, jotka osallistuvat kyberturvallisuuden kehittämiseen paikallisesti tai valtakunnallisesti.



Mitä voimme oppia muista Euroopan maista?



Kaakkois-Suomen
ammattikorkeakoulu

KYMEN
LAAKSON
LIITTO



Euroopan unionin
osarahoittama

CyberCare
Kymi



Miksi vertailemme Suomea muihin maihin?

Kyberturvallisuus on yleistyvän digitalisaation myötä noussut kriittiseksi osaksi myös sosiaali- ja terveysalan arkea. Erityisesti pienet yritykset kohtaavat haasteita, koska niillä ei useinkaan ole erillistä IT-henkilöstöä tai resursseja seurata jatkuvasti muuttuvaa kyberuhkien kenttää. Tämä tekee niistä erityisen haavoittuvaisia sekä teknisten riskien että sääntelyvaatimusten noudattamisen kannalta.

Vertailu muiden Euroopan maiden, kuten Belgian ja Ranskan, kanssa tarjoaa meille arvokkaita näkökulmia siitä, miten eri tavoin maiden julkiset toimijat, viranomaiset ja tukiorganisaatiot ovat lähestyneet näitä ongelmia. Nämä maat ovat ottaneet erilaisia, mutta toisiaan täydentäviä lähestymistapoja erityisesti pienyritysten tukemiseksi. Ne tarjoavat konkreettisia esimerkkejä hyvistä käytännöistä ("best practices"), joita voidaan arvioida ja soveltaa Suomen kontekstiin.





Miksi vertailemme Suomea muihin maihin?

Tämän vertailun tarkoituksena ei ole pelkästään tunnistaa puutteita vaan ennen kaikkea tunnistaa kehityskohteita ja ratkaisuja, joita voidaan mukauttaa suomalaiseen lainsäädäntöön, toimintaympäristöön ja sote-alan rakenteisiin. Erityisen keskeistä on tarkastella:

- Miten pienyrityksiä on tuettu konkreettisilla työkaluilla?
- Millaisia sektori- ja toimialakohtaisia ohjelmia ovat kehitetty?
- Miten sääntelyn noudattamista on helpotettu?
- Millaisia viestintä- ja tukikanavia muilla EU-mailla on tarjolla?

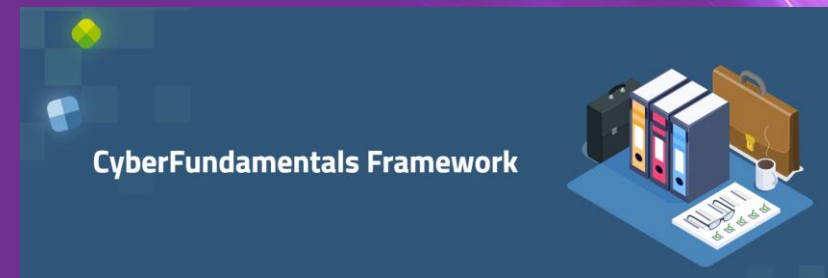
Kansainvälisestä vertailusta voi nousta esiin myös piirteitä, joita Suomessa ei vielä ole hyödynnetty: esimerkiksi visuaaliset itsearviointityökalut, sektorikohtaiset riskikirjastot tai keskitetyt tukialustat. Nämä voivat madaltaa kynnystä ryhtyä kyberturvallisuuden kehittämiseen.

Tämä raportti esittelee Belgian ja Ranskan ratkaisumalleja ja tuo niiden pohjalta esiin johtopäätöksiä ja kehitysehdotuksia Suomen sote-alan kyberturvatyöhön.





Belgia



Belgia oli ensimmäinen EU-maa, joka implementoi NIS2-direktiivin kansalliseen lainsäädäntöön huhtikuussa 2024. Jo tämä kertoo maan ennakoivasta ja suunnitelmallisesta otteesta kyberturvallisuuteen. Erityisesti pienyritysten tukemiseksi Belgia loi keskitetyn verkkoalustan, josta löytyvät kaikki keskeiset tiedot, ohjeet, lomakkeet ja itsearviointityökalut NIS2-vaatimusten täyttämiseen.

Belgian keskeinen työkalu on CyberFundamentals Framework (CyFun), joka jakaa kyberturvatoimenpiteet neljään tasoon: Small, Basic, Important ja Essential. Tämä jaottelu auttaa eri kokoisia ja eri kypsyystason yrityksiä valitsemaan realistisen ja hallittavan etenemiseen. Etenkin mikro- ja pienyritykset voivat aloittaa matalan kynnyksen toimenpiteistä ja laajentaa sitä mukaa miten osaaminen, resurssit ja riskienhallinnan tarpeet kasvavat.

Yksi erityisesti pienyrityksille suunnattu innovaatio on CyFun-merkki. Kyseessä on vapaaehtoinen sertifiointimalli, joka osoittaa yrityksen kyberturvavalmiuden. Sertifikaatin saaminen perustuu itsearviointiin ja tiettyjen minimikriteerien täyttämiseen. Näin yritykset voivat sekä parantaa omaa turvallisuuttaan että viestiä siitä asiakkailleen ja yhteistyökumppaneilleen.

Kuva: [CyberFundamentals Framework](#) | [CCB Safeonweb](#)





Belgia

Belgian itsearviointimalli perustuu viisiportaiseen kypsyystasomalliin. Itsearviointin tulokset esitetään visuaalisesti, esim. hämähäkkikaavioina, jotka vertaavat yrityksen tilannetta vaatimuksiin. Tämä auttaa tunnistamaan kehityskohteet nopeasti ja tekee tuloksista helposti ymmärrettäviä myös teknisesti kokemattomille käyttäjille.

Belgian verkkopalveluissa on myös kattava kirjasto selkokielisiä mallipohjia, muun muassa seuraaviin osa-alueisiin:

- Omaisuusluettelo (Asset Management)
- Salasanapolitiikka (Password Policy)
- Ohjelmistojen päivityskäytännöt
- Henkilöstön tietoturvakoulutus

Lisäksi yritykset voivat tarkistaa, kuuluvatko ne NIS2-sääntelyn soveltamisalueelle. Näin sääntely ei jää epäselväksi, vaan jokaisella yrityksellä on mahdollisuus arvioida tilannettaan konkreettisten kriteerien perusteella.





Belgia

Belgian CyFun-malli toimii esimerkkinä siitä, miten eri tasoiset yritykset voivat arvioida tilannettaan ja kehittyä vaiheittain.

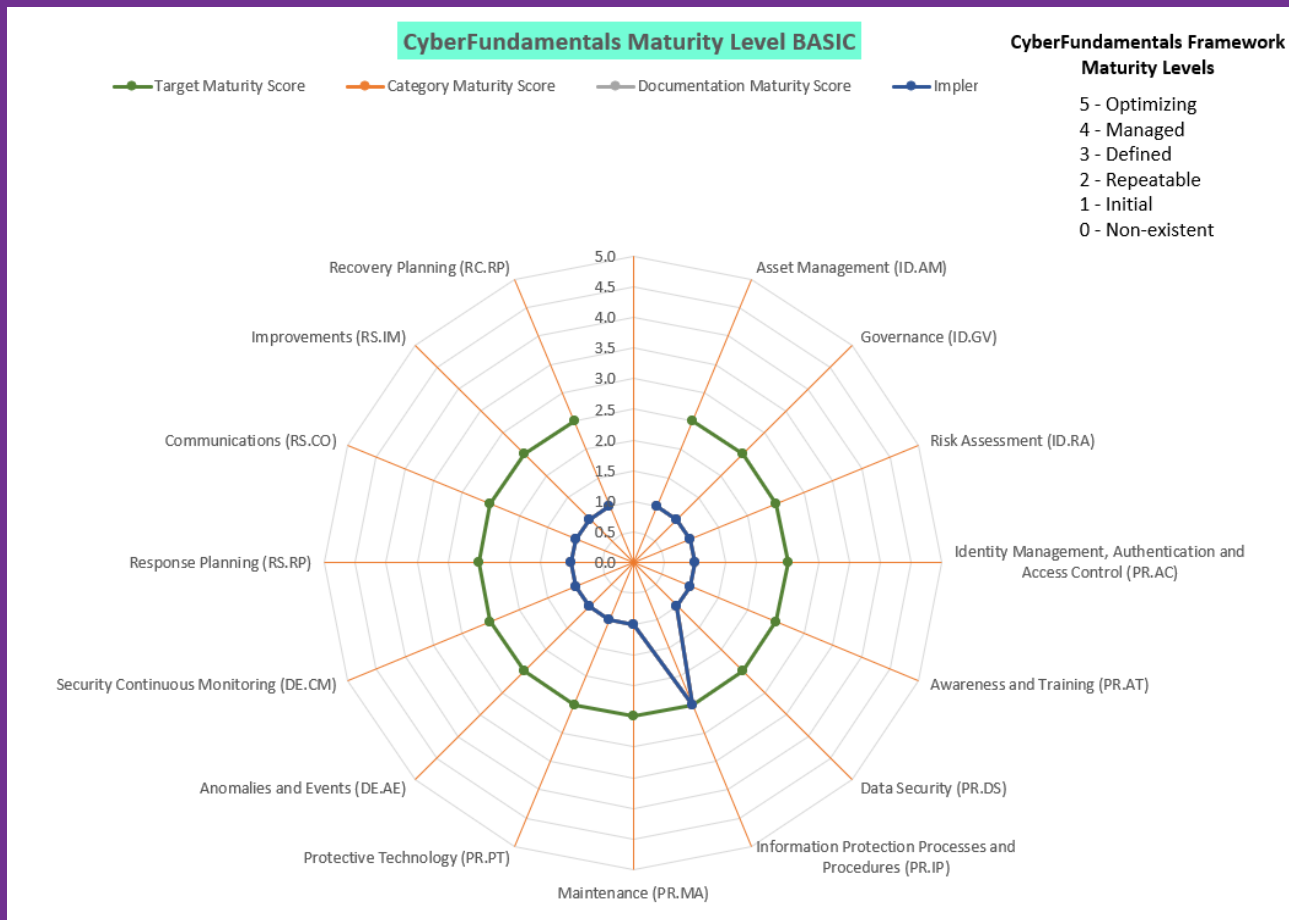
Tämän lisäksi voidaan esittää esimerkkiyrityksen itsearviointikaavio ennen ja jälkeen kehitystoimenpiteet (esim. 6 kk kuluttua).

CyFun-työkalu ei vaadi teknistä erityisosaamista, vaan on suunniteltu tukemaan juuri niitä yrityksiä, jotka ovat vasta kyberturvallisuusmatkansa alussa. Tämä tekisi mallista erityisen soveltuvan Suomen mikroyrityksille, jotka kaipaavat ohjattua ja selkokieleistä tukea.





Belgia

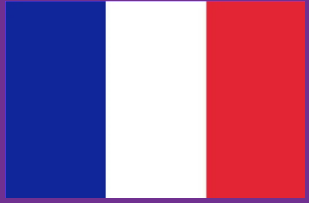


Pääkohdat Belgian mallista:

- Erittäin strukturoitu ja vaiheittain etenevä
- Yhteensopiva eri kokoisten yritysten tarpeisiin
- Selkokieli ja visuaaliset esitykset
- Sertifiointimahdollisuus (CyFun-merkki)
- Keskitetty tietopankki ja mallit

Kuva näyttää itsearviointityökalun kyberturvallisuuden kypsyystason.

Kuva: <https://atwork.safeonweb.be/sites/default/files/2024-11/CyFun%20Self-Assessment%20tool%20V2024-11-05.xlsx>



Ranska



Maaliskuussa 2025 Ranskan senaatti hyväksyi lakiluonnoksen NIS2-direktiivin toimeenpanemiseksi. Se myös julkaisee työkaluja, jotka auttavat / tukevat eri toimialoja soveltamaan sääntelyä omalle alalleen ja vahvistamaan alan kyberturvavalmiuksia.

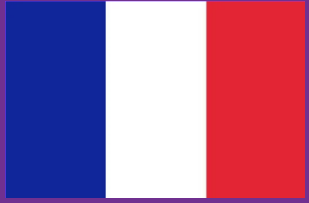
Ranskan kyberturvallisuuskeskus ANSSI on keskeinen toimija, joka tukee pienyrityksiä NIS2-vaatimuksiin valmistautumisessa. ANSSI toimii hallinnon asiantuntijaelimenä. He ovat julkaisseet työkaluja, jotka tukevat eri toimialoja ymmärtämään sääntelyä ja vahvistamaan kyberturvavalmiuksiaan.

Ranska kehitti kansallista verkkopohjaista työkalua nimeltään MonEspaceNIS2, jonka tarkoituksena on tukea yrityksiä NIS2-vaatimuksien täyttämisessä. Alustan sisällön tavoitteena on tarjota:

- Selkeää ohjeistusta ja taustatietoa direktiivistä.
- Itsearviointia tukevia työkaluja.
- Käytännön suosituksia ja dokumenttipohjia.

Kuva: [MonEspaceNIS2 - Accueil](#)





Ranska

Ranskalaiset ovat aloittaneet toimialakohtaisten kyberturvatoimien kehittämisen osana sosiaali- ja terveysalan digitalisaatiota. Tavoitteena on luoda järjestelmiä, jotka tukevat eri kokoisia palveluntuottajia. Tämä osallistava kehittämistapa tähtää siihen että ratkaisut sopivat sekä pienille että suurille toimijoille.

Kyberturvallisuus on Ranskassa sisällytetty osaksi laajempaa France 2030 –ohjelmaa, jossa painotetaan innovaatioita, digitalisaatioita ja sähköisten terveyspalveluiden kehittämistä (mm. Tekoälydiagnostiikka, etävastaanotot ja potilastietojen sähköiset järjestelmät). Nämä kehityssuunnat asettavat uusia vaatimuksia myös kyberriskien hallinnalle.

Kuvassa näkyy verkkosivu, jolla yritykset voivat testata, koskeeko NIS2 heitä.

Kuva: [MonEspaceNIS2 - Suis-je concerné ? - Pour bien débuter](#)

Mon entité est-elle concernée ?

Déterminez si votre entité est régulée par la directive NIS 2

Pour bien débuter

Ce test permet de cerner si votre entité sera concernée par la directive NIS 2, et ce dès 2024. Nous le tiendrons à jour au fil des précisions apportées par la transposition en droit français.

Si votre entité appartient à un groupe d'entreprises aux activités variées, ce test peut être réalisé pour chaque entreprise filiale, ou pour le groupe si celui-ci mène une activité économique.





Ranska

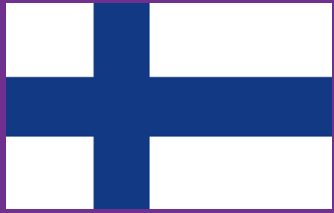
24/7 –tukipalvelu kyberhäiriöihin

Ranska tarjoaa valtakunnallisen kyberturvatuspalvelun, johon yritykset voivat olla yhteydessä sähköpostitse tai puhelimitse ympäri vuorokauden. ANSSI:n ylläpitämä palvelu tarjoaa tukea esim. seuraaviin tilanteisiin:

- Kyberhyökkäykset
- Tietomurrot
- Ohjelmistohaavoittuvuudet
- Uhat tai poikkeamat tietojenkäsittelyssä

Tämä palvelu on erityisen merkittävä niille pienille sosiaali- ja terveysalan toimijoille, joilla ei ole omaa IT-henkilöstöä tai ulkoistettua tukea. ANSSI myös julkaisee kyberturvavaroituksia ja -ohjeistuksia, jotka ovat julkisesti saatavilla heidän verkkosivuillaan.





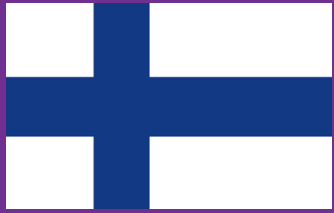
Suomi

Suomi on implementoinut NIS2-direktiivin kansalliseen lainsäädäntöön 8.4.2025. Vaikka lainsäädännöllinen pohja on nyt olemassa, käytännön tukirakenteet pienille ja keskisuurille yrityksille – erityisesti sosiaali- ja terveysalalla – ovat edelleen hajanaisia ja vaikeasti saavutettavia.

Peruspalvelut yrityksille ja yksityishenkilöille

Liikenne- ja viestintäviraston Kyberturvallisuuskeskus tarjoaa ilmoituslomakkeen, jonka kautta sekä yritykset että yksityishenkilöt voivat raportoida kyberhäiriöistä. Ilmoittaminen onnistuu sähköisesti ja kattaa erilaiset tietoturvaloukkaukset, kuten tietojenkalastelun ja palvelunestohyökkäykset. Ilmoitus voi johtaa viranomaisyhteydenottoon ja mahdolliseen tukeen, mutta vastauksen nopeus ja saatavuus riippuvat Kyberturvallisuuskeskuksen resurssitilanteesta





Suomi

Kybermittari

Yksi Suomessa käytettävissä oleva työkalu on Cybermittari, joka on kehitetty kyberturvallisuuden arviointiin ja kehittämiseen. Cybermittari on suunnattu yleisesti organisaatioiden johdolle ja tietoturva-ammattilaisille, eikä se ole erityisesti suunniteltu pienyritysten tai vähäresurssisten toimijoiden tarpeisiin. Työkalu edellyttää usein teknistä ymmärrystä ja ulkopuolista asiantuntemusta.

Kuva: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Kybermittarin%20arviointity%C3%B6kalu_v2.1_20230829.xlsx

KYBERMITTARI

2.1

Tiedon luokittelu

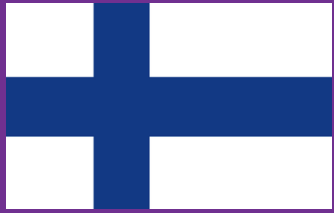
TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kybermittari versio 2.1, 29.08.2023
<https://www.kybermittari.fi>
Palaute ja kysymykset: [kybermittari\(at\)traficom.fi](mailto:kybermittari(at)traficom.fi)

Materiaali on käytettävissä Creative Commons Nimeä 4.0 / CC BY 4.0 lisenssiehtojen mukaisesti.
Cybermittari on rekisteröity tavaramerkki (sanamerkki).

Valitse kieli / Välj språk / Choose language

Suomi



Suomi

Ohjeistukset ja oppaat

Kyberturvallisuuskeskus on julkaissut oppaita eri kokoisille yrityksille. Esimerkiksi pienyrityksille suunnattu opas sisältää ohjeita muun muassa:

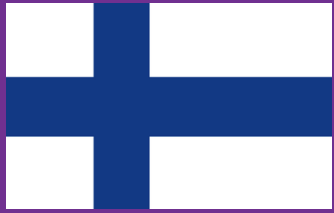
- tietojenkalastelun tunnistamiseen
- kiristysohjelmien torjuntaan
- suojautumiskeinoihin ja toimintamalleihin

Oppaat ovat hyödyllisiä, mutta käytännön soveltaminen jää yritysten vastuulle.

Harjoitusskenaariot ja valmistautuminen

Kyberturvallisuuskeskuksen tarjoama kyberharjoitusskenaarioiden kirjasto on avoin kaikille. Sen tarkoituksena on auttaa organisaatioita valmistautumaan kyberuhkiin simuloimalla erilaisia häiriötilanteita. Harjoitukset tukevat kyberturvavalmiutta ja palautumiskykyä.

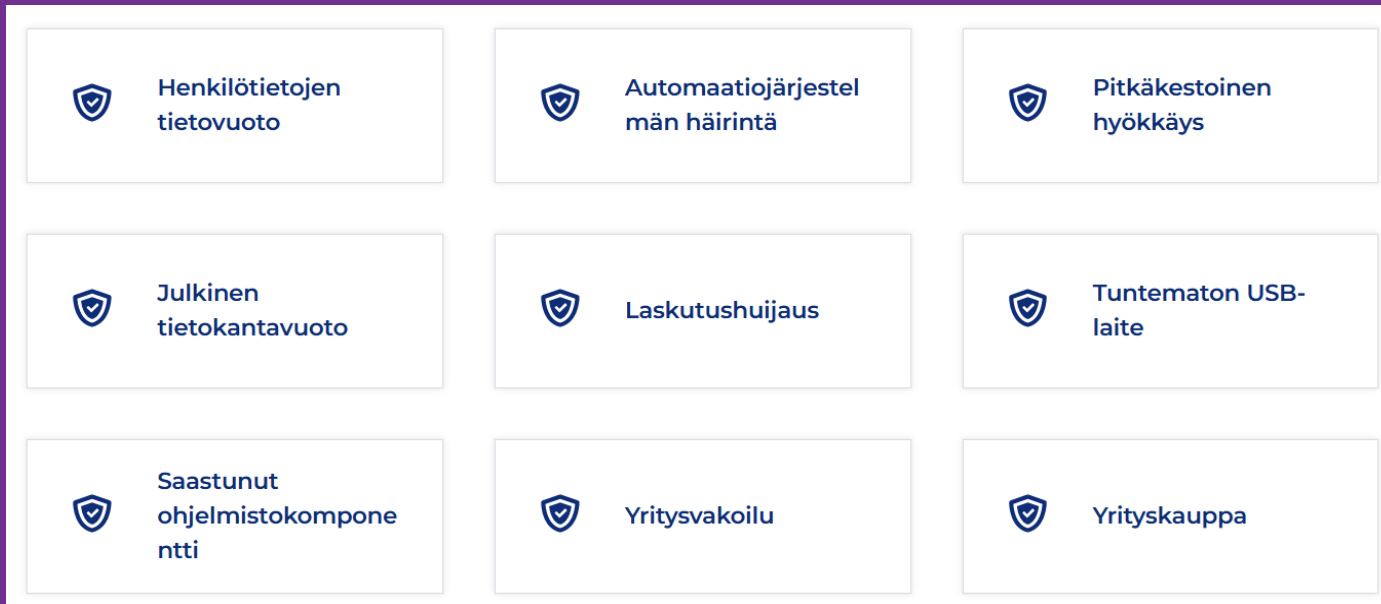




Suomi

Harjoitusskenaariot ja valmistautuminen

Kyberturvallisuuskeskuksen tarjoama kyberharjoitusskenaarioiden kirjasto on avoin kaikille. Sen tarkoituksena on auttaa organisaatioita valmistautumaan kyberuhkiin simuloimalla erilaisia häiriötilanteita. Harjoitukset tukevat kyberturvavalmiutta ja palautumiskykyä.



Kuva: [2020 | Kyberharjoitusskenaariot](#)





Vertailu

Belgian ja Ranskan esimerkit osoittavat, kuinka eri tavoin EU-maat voivat tukea pieniä sosiaali- ja terveysalan yrityksiä kyberturvallisuuden kehittämisessä. Vertailun perusteella on mahdollista tunnistaa konkreettisia kehityskohteita, joita Suomessa voitaisiin toteuttaa.

Vertailutaulukko: Belgia – Ranska – Suomi

Ominaisuus	Belgia	Ranska	Suomi
Lainsäädäntö	NIS2 implementoitu 4/2024	NIS2 implementoitu ennen kesää	NIS2 implementoitu 8.4.2025
Tuki pienyrityksille	CyFun-Label, matalan kynnyksen alusta	MonEspaceNIS2, sektorikohtainen ohjaus	Kybermittari, Traficom ohjeet, harjoitukset
Sertifiointi	Kyllä, vapaaehtoinen (CyFun)	Ei	Ei
Reaaliaikainen tuki	Ei erillistä hotline-palvelua	Kyllä, 24/7-palvelu	Ei
Toimialakohtainen ohjaus	Osittain, kypsyystasomalli	Kyllä, selkeästi sektorikohtainen	Ei
Visuaaliset työkalut	Hämähäkkikaaviot, Excel-mallit	Ohjattu eteneminen alustalla	Ei



Suosituksset Suomelle

Kehitä sektoriin kohdennettu, matalan kynnyksen alusta

Suomi tarvitsee Belgian tapaan keskitetyn verkkopalvelun, joka kokoaa yhteen ohjeet, mallipohjat, itsearviointit ja raportointikanavat. Alustan tulisi olla helposti käytettävä myös ilman teknistä osaamista.

Mahdollista vapaaehtoinen sertifiointi

CyFun-sertifikaatti toimii motivaattorina. Samankaltainen tunnustus Suomessa voisi lisätä asiakkaiden luottamusta ja helpottaa julkisiin hankintoihin osallistumista.

Ota käyttöön visuaaliset arviointimenetelmät

Hämähäkkikaaviot ja pisteytykset auttavat hahmottamaan kehityskohteet selkeästi. Visualisointi alentaa osallistumiskynnystä.





Suosituksset Suomelle

Perusta kansallinen kyberneuvontapalvelu

ANSSI:n malli osoittaa, että jatkuva puhelin- ja sähköpostituki voi olla ratkaisevaa pienyrityksille, joilla ei ole IT-tukea.

Sisällytä kyberturva osaksi yrityksen muita tukirakenteita

Kyberturvallisuus tulisi linkittää osaksi tietosuojasuunnitelmia ja laadunhallintaa. Tämä integrointi tuo suojautumisen osaksi jokapäiväistä toimintaa.

Lähteet

CyberFundamental Framework. Safeonweb. Verkkosivu. Saatavissa: <https://atwork.safeonweb.be/tools-resources/cyberfundamentals-framework>

CyberFundamentals Self-Assessment Tool – User Instructions. 2024. Centre for Cybersecurity Belgium. PDF-dokumentti. Saatavissa: [CyFun_Self Assessment user instructions_Jan2024.pdf](#)

Directive NIS 2. République Française. Verkkosivu. Saatavissa: <https://monespacenis2.cyber.gouv.fr/>

French Healthcare. 2024. 40th Annual J.P. Morgan Healthcare Conference – France 2030 Strategy and Digital Health Investment. PDF-dokumentti. Saatavissa: <https://frenchhealthcare.com/app/uploads/2021/12/catalogue-JP-Morgan-12.01.2022.pdf>

Pienyritysten kyberturvallisuusopas. 2020. Traficom. PDF-dokumentti.

Saatavissa: https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Pienyritysten_kyberturvallisuusopas_9_2020.pdf