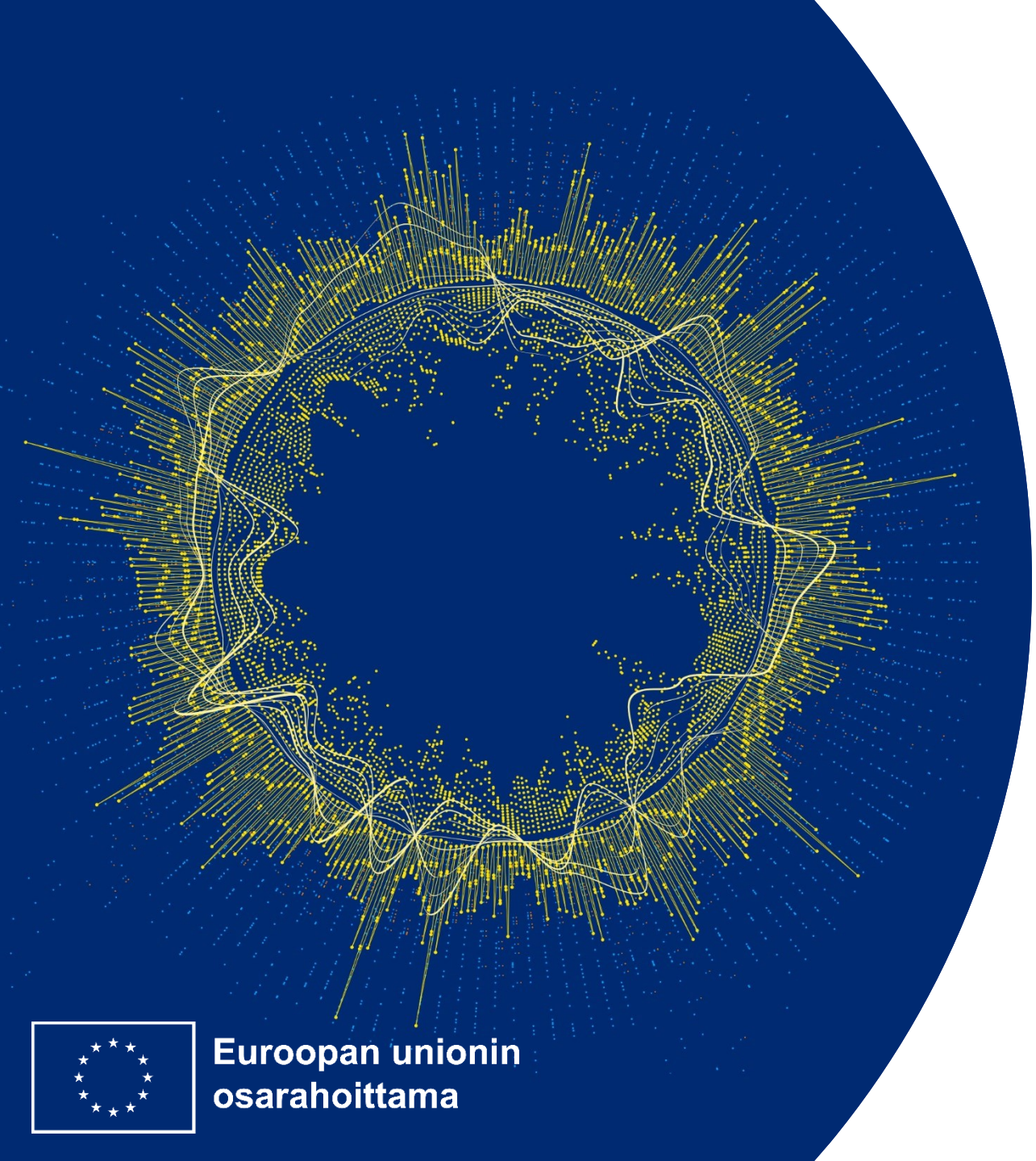


Euroopan unionin osarahoittama

TRAFICOM
Liikenne- ja viestintävirasto

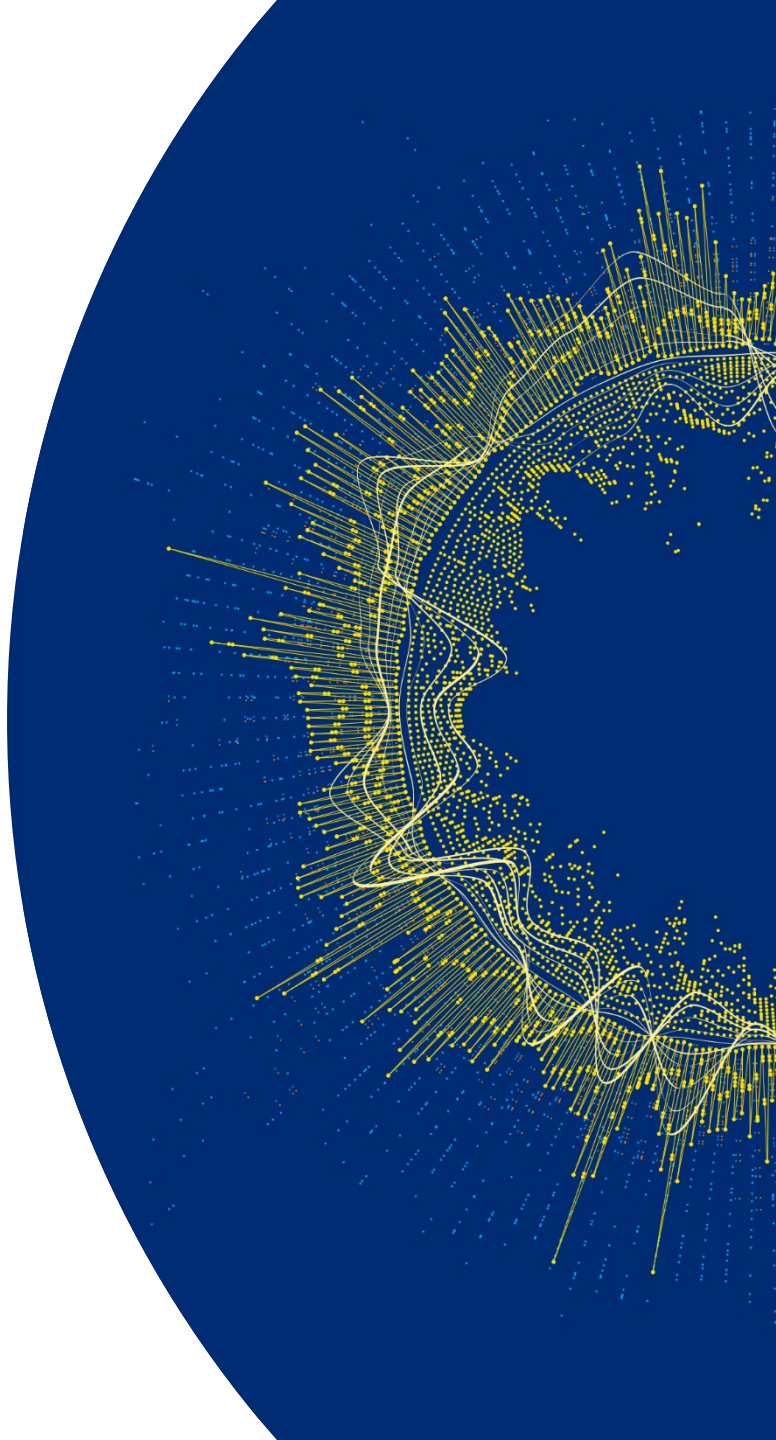
NCC-FI
KYBERTURVALLISUUDEN KANSALLINEN KOORDINOINTIKESKUS

Rahoitustuki kyberturvallisuuslain toimeenpanemisen tukemiseksi -webinaari

4.9.2025 klo 9:00–10:30

Ohjelma

- 9:02 Kyberturvallisuuslain yleisesittely + Q&A (Kalle Varjola, Kyberturvallisuuskeskus)
- 9:30 Rahoitustuki kyberturvallisuuslain toimeenpanemisen tukemiseksi + Q&A (Annalotta Saarikoski, Kyberturvallisuuskeskus)
- 10:00 Tauko 5–10 min
- 10:05 Suositus kyberturvallisuuden riskienhallinnan toimenpiteistä + Q&A (Topi Talikka, Kyberturvallisuuskeskus)
- 10:30 Päättäminen



TRAFICOM

TRAFICOM
Liikenne- ja viestintävirasto

Kyberturvallisuuslain keskeiset velvoitteet

Kalle Varjola
Erityisasiantuntija
Kyberturvallisuuskeskus

Esityksen sisältö

1) Soveltamisala
2) NIS2- toimialat ja valvovat viranomaiset
3) Keskeiset velvoitteet
   - Riskienhallinta
   - Ilmoitusvelvollisuus merkittävistä poikkeamista
   - Toimijaluetteloon ilmoittautuminen

Soveltamisala

- Oikeushenkilö tai luonnollinen henkilö (*toimija*), joka:
  - Harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on niissä tarkoitettu toimija JA
    - A) Täyttää tai ylittää keskisuuren toimijan määritelmän
    - B) Koosta riippumatta, jos toimija on
      - Yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoaja
      - Luottamuspalvelun tarjoaja, aluetunnusrekisterin ylläpitäjä tai DNS-palveluntarjoaja
      - Yhteiskunnan kriittisen infrastruktuurin suojaamisesta ja häiriönsietokyvyn parantamisesta annetun lain (310/2025) nojalla määritetty kriittinen toimija muulla kuin julkishallinnon toimialalla
      - Palvelun tarjoaja kuuluu erityisluokkiin, esim. toimija tarjoaa ainoana palvelua, joka on yhteiskunnan tai talouden kriittisten toimintojen ylläpitämisen kannalta keskeinen.

Ks. tarkemmin:
https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/TRAFICOM_NIS2_taulukko_08042025.pdf

Kokokriteeri

- **Komission suosituksen 2003/361/EY kynnysarvot**
- Keskisuuri toimija (täyttää keskisuuren toimijan määritelmän)
  - Yritys, jonka palveluksessa on vähintään 50 työntekijää tai jonka vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa. Eli muu kuin suosituksessa tarkoitettu mikro- tai pienyritys (soveltamisen kokokriteeri)
- Keskisuuren toimijan kynnysarvon ylittävä yritys
  - Yritys, jonka palveluksessa on vähintään 250 työntekijää tai jonka vuosiliikevaihto ylittää 50 miljoonaa euroa ja taseen loppusumma ylittää 43 miljoonaa euroa (keskeisen toimijan kokokriteeri)

Energia

Liikenne

Pankkitoiminta

Finanssimarkkinoiden infrastruktuuri

Terveys

Juomavesi

Jätevesi

Digitaalinen infrastruktuuri

TVT-palvelujen hallinta (yritysten välinen)

Julkishallinto

Avaruus

Posti- ja kuriiripalvelut

Jätehuolto

Kemikaalien valmistus, tuotanto ja jakelu

Elintarvikkeiden tuotanto, jalostus ja jakelu

Valmistus

Digitaalisen palvelun tarjoajat

Tutkimustoiminta

NIS2-toimialat ja valvovat viranomaiset

Valvovat viranomaiset
Traficom
Energiavirasto
Finanssivalvonta
Valvira
Tukes
Fimea
Ruokavirasto
Etelä-Savon ELY-keskus

Ks. tarkemmin: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis-2-euroopan-unionin-kyberturvallisuusdirektiivi/tarkeaa-tietoa?toggle=Valvovat%20viranomaiset%20vastuusektoreineen%20on%20listattu%20alla

Kyberturvallisuuskeskus NIS2-valvojana

Digitaalinen infrastruktuuri

- Internetin yhdysliikennepisteiden ylläpitäjät
- Aluetunnusrekisterit (.fi)
- Pilvipalvelujen tarjoajat
- Datakeskuspalvelujen tarjoajat
- Sisällönjakeluverkkojen tarjoajat
  - Lisätiedot: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/digitaalinen-infrastruktuuri-digitaaliset-palvelut-ja-tvt-palvelut
- Yleisten sähköisten viestintäverkkojen tarjoajat
- Yleisesti saatavilla olevien sähköisten viestintäpalveluiden tarjoajat
  - Lisätiedot: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/saantelyn-kohteet
  - Yhteystiedot: nis.valvonta.ktk(at)traficom.fi
- Luottamuspalvelujen tarjoajat
  - Lisätiedot: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/sahkoinen-allekirjoitus-ja-muut-eidas-palvelut
  - Yhteystiedot: eidas(at)traficom.fi

ICT-/TVT-palveluiden hallinta

- Hallintapalvelujen tarjoajat (MSP)
- Tietoturvapalveluntarjoajat (MSSP)
  - Lisätiedot: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/digitaalinen-infrastruktuuri-digitaaliset-palvelut-ja-tvt-palvelut

Digitaalisen palvelun tarjoat

- Markkinapaikat
- Hakukonepalvelut
- Verkkoyhteisöalustat
  - Lisätiedot: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/digitaalinen-infrastruktuuri-digitaaliset-palvelut-ja-tvt-palvelut#11759-1
  - Yhteystiedot: nis.valvonta.ktk(at)traficom.fi

Julkishallinto ja tutkimustoiminta

- Keskus- ja aluetason toimijat sekä VTT Oy
  - Lisätiedot: https://www.kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/julkishallinto-ja-tutkimusorganisaatiot
  - Yhteystiedot: nis.valvonta.ktk(at)traficom.fi

Traficomin liikennesektorin NIS2-valvontatehtävät

Yhteystiedot:

kyberturvallisuus.liikenne@traficom.fi

Liikenne

- **Ilmaliikenne**:
  - Lentoliikenteen harjoittajat, joiden toiminta on kaupallista
  - Lentoaseman pitäjät
  - Lennonjohtopalvelua tarjoavat lennonjohtopalvelun tarjoajat
    - Lisätietoja: https://www.traficom.fi/fi/liikenne/ilmailu/ilmailun-kyberturvallisuus
- **Raideliikenne**:
  - Rataverkon haltijat
  - Rautatieyritykset, mukaan lukien palvelupaikan ylläpitäjät
    - Lisätietoja: https://www.traficom.fi/fi/liikenne/raideliikenne/raideliikenteen-kyberturvallisuus
- **Vesiliikenne**:
  - Sisävesillä, merillä ja rannikoilla matkustaja- ja rahtiliikennettä hoitavat yhtiöt
  - Satamien hallinnointielimet ja satamarakenteet, sekä toimijat, jotka huolehtivat rakenteista ja varusteista satamien alueella
  - Alusliikennepalvelujen tarjoajat
    - Lisätietoja: https://www.traficom.fi/fi/liikenne/merenkulku/merenkulun-kyberturvallisuus
- **Tieliikenne**:
  - Liikenteenhallinnasta vastaavat tieviranomaiset
  - Älykkäiden liikennejärjestelmien ylläpitäjät
    - Lisätietoja: https://www.traficom.fi/fi/liikenne/tieliikenne/muut-tieliikenteen-toimijat/tieliikenteen-ohjaus-ja-hallintapalvelujen-ja

Traficomin liikennesektorin NIS2-valvontatehtävät

Yhteystiedot:

kyberturvallisuus.liikenne@traficom.fi

Liikenteen valmistus

- **Moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus**:
  - NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 29 tarkoitettua taloudellista toimintaa harjoittavat toimijat
    - Moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistus
    - Moottoriajoneuvojen korien valmistus
    - Osien ja tarvikkeiden valmistus moottoriajoneuvoihin
    - Sähkö- ja elektroniikkalaitteiden valmistus moottoriajoneuvoihin
    - Muiden osien ja tarvikkeiden valmistus moottoriajoneuvoihin
      - Lisätietoja: https://traficom.fi/fi/liikenne/tieliikenne/muut-tieliikenteen-toimijat/kyberturvallisuusvaatimukset-kulkunevojen-ja
- **Muiden kulkuneuvojen valmistus**:
  - NACE Rev. 2 -luokituksen C jakson kaksinumerotasossa 30 tarkoitettua taloudellista toimintaa harjoittavat toimijat
    - Laivojen, veneiden ja kelluvien rakenteiden rakentaminen
    - Huvi- ja urheiluveneiden rakentaminen
    - Raideliikenteen kulkuneuvojen valmistus
    - Ilma- ja avaruusalusten ja niihin liittyvien koneiden valmistus
    - Taisteluajoneuvojen valmistus
    - Muualla luokittelematon kulkuneuvojen valmistus
    - Moottoripyörien valmistus
    - Polkupyörien ja invalidiajoneuvojen valmistus
    - Muiden muualla luokittelemattomien kulkuneuvojen valmistus

Traficomin Tieto ja Tulevaisuuden yhteydet-toimiala NIS2-valvojana

- **Traficom / Avaruus**
  - **Tehtävä:** Valvonta satelliittien maa-asemien kyberturvallisuudelle NIS2 osalta
  - **Kotisivu jossa tietoa toimijoille:** ei ole julkaistu, tiedot jaetaan suoraan toimijoille
  - **Yhteydenottojen sähköposti:** maa-asemat(at)traficom.fi
  - **Lisätietoja antaa:** Erityisasiantuntija Marko Saarela, marko.saarela(at)traficom.fi

- **Traficom / Verkkotunnukset**
  - **Tehtävä:** Valvonta DNS-palveluntarjoajien ja fi-verkkotunnusvälittäjien osalta
  - **Kotisivu jossa tietoa toimijoille**: https://www.traficom.fi/fi/viestinta/fi-verkkotunnukset/fi-verkkotunnuksen-hakijalle-ja-kayttajalle/nis-2
  - **Lisätietoja saa:** Yhteydenottolomakkeella, https://traficom.fi/fi/traficom/yhteystiedot/asiakaspalvelu/fi-verkkotunnusten-asiakaspalvelu/yhteydenottolomake-fi

- **Traficom / Posti- ja kuriiripalvelut**
  - Tehtävä: Valvonta posti- ja kuriiritoimijoiden osalta
  - **Kotisivu jossa tietoa toimijoille:** ei ole julkaistu, tiedot jaetaan suoraan toimijoille
  - **Yhteydenottojen sähköposti:** NIS2.postijakuriiri(at)traficom.fi
  - **Lisätietoja antaa:** Erityisasiantuntija Tero Ilvonen**,** tero.ilvonen(at)traficom.fi

NIS2-direktiivi finanssialalla

- Finanssivalvonta on finanssisektorin valvova viranomainen
  - sähköpostiosoite kirjaamo(at)finanssivalvonta.fi

- NIS2-direktiivin liitteessä I tarkoitettuja pankkitoiminnan ja finanssimarkkinoiden infrastruktuurin toimijoita (pankit ja pörssi) koskee kyberturvallisuuslakia vastaavien velvoitteiden osalta DORA-asetus (Digital Operational Resiliency Act) ja sitä täydentävä kansallinen sääntely

- ICT- ja tietoturvariskien hallinnan valvonta
  - Toimiluvan myöntämisen yhteydessä selvitetään miten toimija tulee noudattamaan velvoitteita
  - Jatkuvassa valvonnassa arvioidaan velvoitteiden noudattamista. Valvottavien toimittamat ICT-häiriöilmoitukset ovat merkittävässä roolissa, kun valvontaa tehdään.
  - Yksityiskohtaisesti velvoitteiden noudattamista arvioidaan toimijakohtaisilla tarkastuksilla tai useampaan toimijaan kohdistuvilla teema-arvioilla

Energiavirasto

- Energia-alalta kyberturvallisuuslain piiriin kuuluu sähkön, kaukolämmityksen ja –jäähdytyksen, kaasun, öljyn sekä vedyn toimijoita
  - Energia-alan valvonta on jaettu Energiaviraston ja Turvallisuus- ja kemikaaliviraston (Tukes) välillä. Tarkempi jaottelu löytyy kyberturvallisuuslaista ja Energiaviraston ohjeesta.
- Energiaviraston koostamia ohjeita sekä lisätietoa energia-alan kyberturvallisuusvelvoitteista löytyy Energiaviraston nettisivuilta: https://energiavirasto.fi/kyberturvallisuus
  - Liity samalla myös Energiaviraston kyberturvallisuus-uutiskirjeen vastaanottajaksi
- Ilmoittautuminen toimijaluetteloon tapahtuu VERTTI-valvontatietojärjestelmässä: https://vertti.energiavirasto.fi/
- Yhteys: varautuminen(at)energiavirasto.fi

energiavirasto

tukes

Turvallisuus- ja kemikaalivirasto Tukes

- **https://tukes.fi/kyberturvallisuus** sivustolle on kerätty tiedot velvoitteista, ilmoittautumisesta, yhteystiedoista ja toimialakohtaiset ohjeet
- Tukesin valvomat toimialat
  - Energia
    - Öljynjalostus ja jakeluterminaalit
    - Vedyn tuotantoa ja varastointia harjoittavat toimijat
    - Kaasualan toimijoihin kuuluvat
      - metaanin tuotanto-, varastointi-, käsittely-, jalostus- ja nesteytyslaitteistojen haltijat sekä tätä toimintaa harjoittavat yritykset ja
      - edellä mainittujen toimijoiden kaupallisista-, teknisistä- ja ylläpitotehtävistä vastaavat toimijat
  - Kemikaalien valmistus, tuotanto ja jakelu
  - Valmistava teollisuus (NACE Rev. C26-28 tarkoittamaa valmistusta harjoittavat yritykset)
    - tietokoneet sekä elektroniset ja optiset tuotteet (C26), sähkölaitteet (C27), muut koneet ja laitteet (C28)
- Toimijaluetteloon ilmoittaudutaan **sähköisessä asiointipalvelussa**, https://sahkoinenasiointi.ahtp.fi/fi/palvelut?tyyppi=tukes_NIS2_toimijarekisteriin_ilmoittautuminen
- Mahdolliset yhteydenotot: **kyberturvallisuus(at)tukes.fi**

TRAFICOM

Ruokavirasto elintarviketoimialan valvovana viranomaisena

- Elintarvikeyritykset, jotka harjoittavat tukkukauppaa sekä teollista tuotantoa ja jalostusta.
  - Soveltamisalaan eivät kuulu esim. alkutuotanto, rehutuotanto, vähittäiskauppa, varastointi, kuljetus, elintarvikekontaktimateriaalitoiminta ja ruokapalvelutoiminta.
- Lisätietoa:
  - Ruokaviraston nettisivut, https://www.ruokavirasto.fi/elintarvikkeet/elintarvikeala/elintarvikeyrityksen-perustaminen-ja-omavalvonta/kyberturvallisuusdirektiivi-nis2-elintarviketoimialalla/
  - NIS2.kyberturvallisuus(at)ruokavirasto.fi

Lääkealan turvallisuus- ja kehittämiskeskus Fimea

- Fimea valvoo erityisesti **suuria ja keskisuuria yrityksiä** seuraavilla toimialoilla:
  - **Lääke- ja lääkeainetehtaat**
  - **Veripalvelu**
  - **Apteekit**
  - **Lääkinnällisten laitteiden valmistajat**
  - **Ihmisille tarkoitettujen lääkkeiden tutkimus- ja kehitysorganisaatiot**
  - Lisäksi myöhemmin **CER-lainsäädännön perusteella** yhteiskunnan häiriönsietokyvyn kannalta kriittiset toimijat, em. lisäksi myös **lääketukkukaupat**
- Lisätietoja Fimean kyberturvallisuusvalvonnasta löytyy Fimean verkkosivuilta: https://fimea.fi/valvonta/kyberturvallisuuden-ja-hairionsietokyvyn-valvonta/kyberturvallisuus **ja** https://fimea.fi/valvonta/kyberturvallisuuden-ja-hairionsietokyvyn-valvonta/usein-kysytyt-kysymykset-kyberturvallisuudesta
- Valvontaa toteutetaan osana muuta Fimean toiminnan valvontaa, ja tarkastajia on käytännössä viidellä eri substanssivalvontasektorilla Fimeassa
- Asiointisähköposti: **NIS2-CER(at)fimea.fi**

fimea

Terveydenhuoltosektori Valvira

- Kyberturvallisuuslain velvoitteet koskevat hyvinvointialueita ja kaikkia terveydenhuollon organisaatioita, jotka työllistävät vähintään 50 henkilöä tai joiden vuosiliikevaihto ja taseen loppusumma ylittää 10 miljoonaa euroa.
- Lisätietoja ja ilmoittautumislomake toimijaluetteloon:
  - https://valvira.fi/sosiaali-ja-terveydenhuolto/kyberturvallisuuslaki
  - Jos organisaation kokorajat täyttyvät, muista ilmoittautua!
  - Lisätietoja antaa yli-insinööri Antti Härkönen, antti.harkonen(at)valvira.fi, 0295 209 530
- Asiakastietolakiin perustuvat velvoitteet ja poikkeamailmoitusmenettely säilyvät ennallaan.

Valvira

Etelä-Savon ELY-Keskus

Elinkeino-, liikenne- ja ympäristökeskus

- **Vesihuolto**
  - Juomavesi ja jätevesi
  - Noin 30 vesihuoltolaitosta, myös monialayhtiöitä (esim. vesi + energia)
  - kyberturvallisuus.vesihuolto(at)ely-keskus.fi
- **Jätehuolto**
  - Jätteenkäsittely (mukaan lukien kierrätys)
  - Noin 50 toimijaa: kierrätyslaitoksia, jätekuljetuksia, polttolaitoksia yms.
  - kyberturvallisuus.jatehuolto(at)ely-keskus.fi
- Kyberturvallisuuslaki ja NIS2-Direktiivi
  - https://www.ely-keskus.fi/kyberturvallisuus-kyberturvallisuuslaki-ja-nis2-direktiivi-

Riskienhallinta

Toimijalla on oltava käytössään ajantasainen kyberturvallisuuden riskienhallinnan toimintamalli, jossa

- Tunnistetaan verkko- ja tietojärjestelmiin kohdistuvia ennakoitavissa olevia riskejä
- Määritetään ja kuvataan toimenpiteet, joilla viestintäverkkoja ja tietojärjestelmiä ja niiden fyysistä ympäristöä suojataan riskeiltä ja poikkeamilta (hallintatoimenpiteet).

Riskienhallintatoimenpiteet

- Toimija määrittää ja toteuttaa, valvova viranomainen valvoo.
- Kyberturvallisuuslain 9 §:ssä ja tiedonhallintalain 18 c §:ssä vähimmäisosa-alueet, jotka huomioitava toimintamallissa ja hallintatoimenpiteissä.
- Suhteutettava toiminnan laatuun ja laajuuteen, poikkeamista kohtuudella ennakoitavissa oleviin välittömiin vaikutuksiin, viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeaman todennäköisyyteen ja vakavuuteen, toimenpiteistä aiheutuviin kustannuksiin ja ajantasaisiin teknisiin mahdollisuuksiin torjua uhka.
- Johto vastaa kyberturvallisuuden riskienhallinnan toteuttamisesta ja valvonnan järjestämisestä
- Otettava huomioon myös EU:n komission täytäntöönpanoasetus (2024/2690), https://eur-lex.europa.eu/legal-content/FI/TXT/?uri=CELEX%3A32024R2690&qid=1741615462589

TRAFICOM

Kyberturvallisuuden riskienhallinnan toimintamallissa ja siihen perustuvissa hallintatoimenpiteissä huomioitavat osa-alueet

1. kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi;
2. viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;
3. viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;
4. toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;
5. omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;
6. henkilöstöturvallisuus ja kyberturvallisuuskoulutus;
7. pääsynhallinnan ja todentamisen menettelyt;
8. salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;
9. poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;
10. varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;
11. perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä
12. toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Toimijaluetteloon ilmoittautuminen

- Toimijoiden on ilmoittauduttava omalle valvovalle viranomaiselleen.
  - Mikäli toimija kuuluu useaan eri toimialaan, tulee ilmoittautua jokaiselle toimialakohtaiselle valvovalle viranomaiselle.
- Toimijoiden on ilmoitettava oman toimialansa valvovalle viranomaiselle seuraavat tiedot:
  1. Toimijan nimi
  2. Yhteystiedot, kuten osoite, sähköposti ja puhelinnumero
  3. IP-osoitealueensa

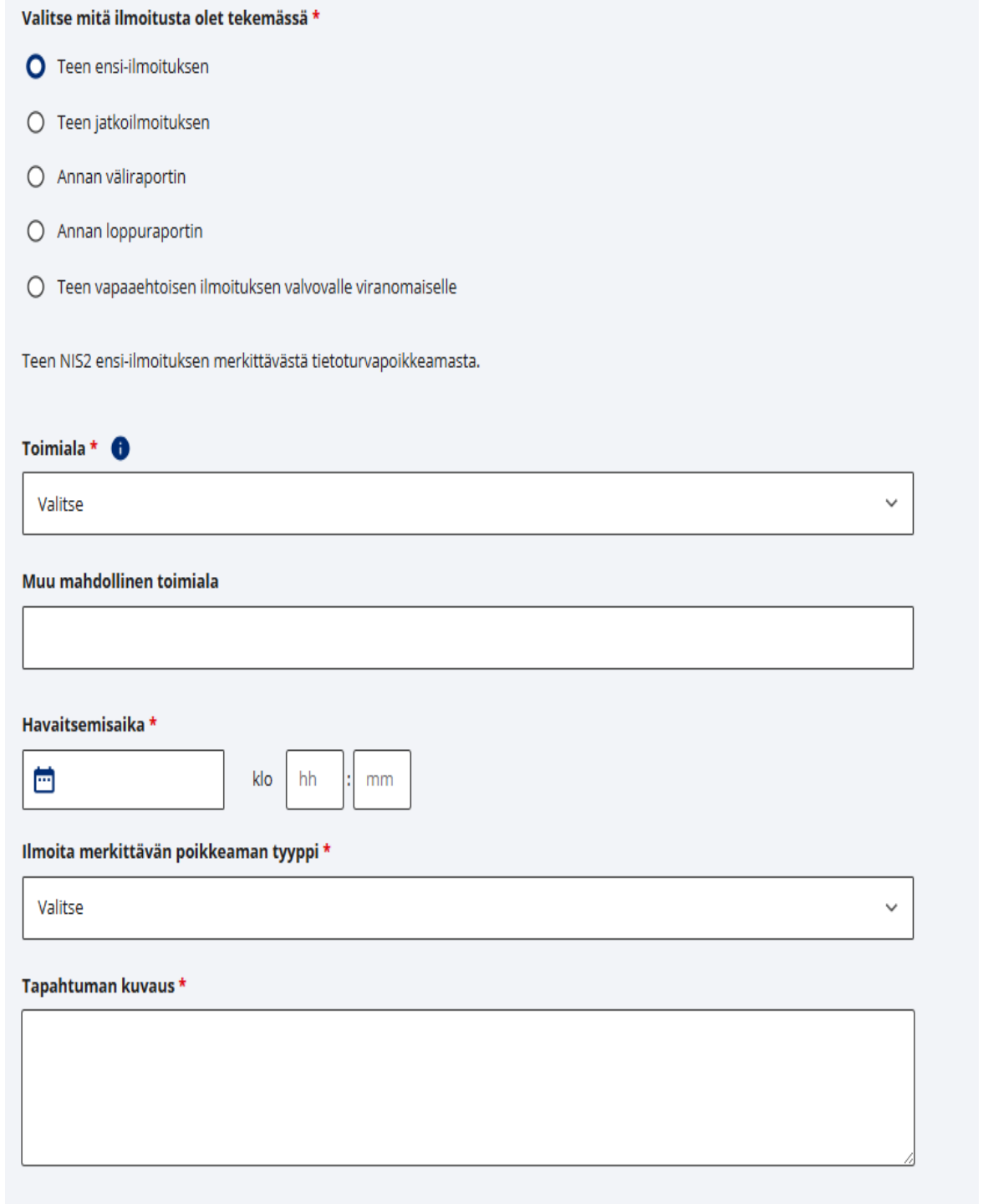
     Ks. ohje IP-osoitealueiden ilmoittamisesta toimijaluetteloon

     https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/IP-osoitteiden%20ilmoittaminen%20NIS2.pdf
  4. NIS 2 -direktiivin liitteessä I tai II tarkoitettu asiaankuuluva toimialansa ja sen osa
  5. Onko toimija keskeinen toimija
  6. EU:n jäsenvaltiot, joissa toimija tarjoaa palvelujaan
  7. Osallistuminen kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn

- DNS-palveluntarjoajien, aluetunnusrekisterin ylläpitäjien, pilvipalvelujen tarjoajien, datakeskuspalvelujen tarjoajien, sisällönjakeluverkkojen tarjoajien, hallintapalvelun tarjoajien, tietoturvapalveluntarjoajien, verkossa toimivien markkinapaikkojen tarjoajien, verkossa toimivien hakukoneiden tarjoajien ja verkkoyhteisöalustojen tarjoajien on ilmoitettava lisäksi:
  - NIS 2 -direktiivin liitteessä I tai II tarkoitettu toimijatyyppinsä
  - Päätoimipaikkansa ja muiden Euroopan unionin jäsenvaltiossa sijaitsevien laillisten toimipaikkojensa osoite tai, jos toimija ei ole sijoittautunut Euroopan unioniin, sen Euroopan unioniin nimetyn edustajan osoite, sähköpostiosoite, puhelinnumero ja muut ajantasaiset yhteystiedot
  - Luettelo Euroopan unionin jäsenvaltioista, joissa toimija tarjoaa palveluita.

Merkittävästä poikkeamasta ilmoittaminen

- Keskitetysti Kyberturvallisuuskeskuksen verkkosivuilta löytyvällä NIS2-poikkeamailmoitussovelluksella.
  - https://kyberturvallisuuskeskus.fi/fi/toimintamme/saantely-ja-valvonta/nis2-euroopan-unionin-kyberturvallisuusdirektiivi
  - Sovellus välittää ilmoituksen oikealle valvovalle viranomaiselle ja Kyberturvallisuuskeskuksen CSIRT-yksikölle, jolta toimija voi myös halutessaan pyytää apua ns. lisälomakkeella.
- Ilmoittaminen palvelujen vastaanottajille (ks. kyberturvallisuuslaki 14 § ja tiedonhallintalaki 18 g §).



Merkittävästä poikkeaman ilmoittaminen

Kaikkien NIS2-toimijoiden on aina ilmoitettava merkittävästä poikkeamasta valvovalle viranomaiselle.

24 h kuluessa ensi-ilmoitus

- Havainto merkittävästä poikkeamasta
- epäilläänkö, että kyseessä on rikos tai vihamielinen teko
- Rajat ylittävien vaikutusten mahdollisuus

72 h kuluessa jatkoilmoitus

- Arvio poikkeaman laadusta, vakavuudesta ja vaikutuksista
- Vaarantumis-indikaattorit (IOC), jos mahdollista
- Mahdolliset täydennykset

Mahdollinen väliraportti

1 kk kuluessa loppuraportti

- Yksityiskohtainen kuvaus poikkea-masta, sen vakavuudesta ja vaikutuksista
- Poikkeaman arveltu aiheuttaja
- Toimenpiteet tilanteen hoitamiseksi
- Mahdolliset rajat ylittävät vaikutukset

TRAFICOM

TRAFICOM
Liikenne- ja viestintävirasto

Kiitos

kalle.varjola(a)traficom.fi

TRAFICOM
Liikenne- ja viestintävirasto

Rahoitustuki kyberturvallisuuslain toimeenpanemisen tukemiseksi

Annalotta Saarikoski
Erityisasiantuntija
Kyberturvallisuuskeskus/NCC-FI

Kansallisen koordinointikeskuksen rahoitustuki kolmansille osapuolille

- Kyberturvallisuuden tutkimuksen, kehityksen ja innovaatioiden kansallinen koordinointikeskus (NCC-FI) myöntää rahoitustukea kolmansille osapuolille ns. kaskadirahoituksena omasta EU-projektirahoituksesta
- EU-projektin aikana (2025–2029) tavoitteena on vahvistaa kansallista ja EU:n kyberturvallisuuskapasiteettia myöntämällä rahoitustukea modernien kyberturvallisuusratkaisujen käyttöönottoon ja levittämiseen etenkin pk-yrityksissä
- Auki olevista hauista viestitään: koordinointikeskus.fi, haeavustuksia.fi, EU Funding and Tenders Portal ja koordinointikeskuksen uutiskirje.

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

NCC-FI
KYBERTURVALLISUUDEN KANSALLINEN KOORDINOINTIKESKUS

Euroopan unionin osarahoittama

TRAFICOM

Rahoitustukihaku kyberturvallisuuslain (124/2025) toimeenpanemisen tukemiseksi

- Haku auennut 15.8. ja päättyy 16.10.2025 klo 16:15
- Rahoitustukea myönnetään yhteensä enintään 2 MEUR
- Rahoitustukea voidaan myöntää 1.1.–31.12.2026 syntyviin kustannuksiin.
- Rahoitustuki on de minimis -muotoista. Yksi yritys voi saada de minimis -tukea kuluvan kolmen vuoden aikana enintään 300 000 euroa.
- Enintään 100 000 euroa ja vähintään 10 000 euroa per hakija ja hanke.
- Omavastuuosuusvaatimus 50 % hankkeen kokonaiskustannuksista.

Hakukelpoisuus 1/2

- Rahoitustukea voivat hakea kyberturvallisuuslain 3 §:n mukaisesti lain soveltamisalaan kuuluvat mikrokokoiset, pienet ja keskisuuret oikeushenkilöt ja luonnolliset henkilöt (toimijat), jotka ovat ilmoittautuneet oman toimialansa valvovan viranomaisen ylläpitämään toimijaluetteloon.
  - Suuret yritykset, julkisen hallinnon tiedonhallinnasta annetun lain (906/2019) piiriin kuuluvat organisaatiot ja toimijaluetteloon ilmoittautumatta jättäneet toimijat **eivät ole** hakukelpoisia.
- Hakijan koon määritelmässä sovelletaan mikroyritysten sekä pienten ja keskisuurten yritysten määritelmästä annetun komission suosituksen 2003/361/EY liitettä kyberturvallisuuslain tarkoittamalla tavalla
  - ”Mikroyritysten sekä pienten ja keskisuurten yritysten (pk-yritysten) luokka koostuu yrityksistä, joiden palveluksessa on vähemmän kuin 250 työntekijää ja joiden vuosiliikevaihto on enintään 50 miljoonaa euroa tai taseen loppusumma on enintään 43 miljoonaa euroa.”
  - Kuten kyberturvallisuuslaissa, suosituksen liitteen 3 artiklan 4 kohtaa ei sovelleta. Näin ollen myös julkisyhteisön tai -laitoksen omistuksessa olevat toimijat voivat olla hakijoina ja heidän osalta rahoitustuen hakijan koon määritelmässä huomioidaan vain kyberturvallisuuslain liitteessä tarkoitettu toiminta. Koon määrittelyssä ei tällöin huomioida julkisyhteisön tai -laitoksen, kuten kunnan henkilöstön määrää, liikevaihtoa ja tasetta (tai äänioikeudelle asetettuja rajoituksia).

Hakukelpoisuus 2/2

- Rahoitustukea hakeva harjoittaa toimintaansa Suomessa Suomeen rekisteröidyllä y-tunnuksella. Yksi hakija/y-tunnus voi jättää yhden hakemuksen hakukierrosta kohti.
- Tukea ei myönnetä yhteisesti usealle hakijalle, esimerkiksi konsortiolle tai konsernin yrityksille. Tukea ei myönnetä muiden kuin saajan itsensä käytettäväksi.
- Tukea ei myönnetä esim. jos
  - EU:n tai ETA:n ulkopuolella toimiva taho käyttää hakijaan suoraa tai epäsuoraa määräysvaltaa Kirjanpitolain (1336/1997) 5 §:ssä tarkoitetulla tavalla,
  - Hakijalla on suurempia kuin vähäisiä velkoja ulosotossa tai velkoja, jotka on palautettu ulosotosta varattomuusestetodistuksin
  - ... (kattava lista löytyy hakuilmoituksesta)

Käyttötarkoitus

- Rahoitustukea voidaan myöntää kyberturvallisuuslain 9 §:n vaatimuksia mukaileviin arviointi- ja kehittämistoimenpiteisiin.
- Toimenpiteillä on määrä arvioida ja kehittää tapoja, joilla toimija hallitsee riskejä ja estää tai minimoi haitallisia vaikutuksia, jotka kohdistuvat viestintäverkkojen ja tietojärjestelmien turvallisuuteen.
- Toimenpiteet on suhteutettava toiminnan laatuun ja laajuuteen, toimijan viestintäverkkojen ja tietojärjestelmien riskialttiuteen, poikkeamien todennäköisyyteen ja vakavuuteen sekä ajantasainen kehitys huomioon ottaen käytettävissä oleviin teknisiin mahdollisuuksiin torjua uhka.

Kyberturvallisuuslain 9 §:n vaatimuksia mukailevat arviointi- ja/tai kehittämistoimenpiteet

1) kyberturvallisuutta koskevan riskienhallinnan toimintaperiaatteet ja hallintatoimenpiteiden vaikuttavuuden arviointi;

2) viestintäverkkojen ja tietojärjestelmien turvallisuutta koskevat toimintaperiaatteet;

3) viestintäverkkojen ja tietojärjestelmien hankinnan, kehittämisen ja ylläpidon turvallisuus sekä tarvittavat menettelyt haavoittuvuuksien käsittelemiseksi ja julkistamiseksi;

4) toimitusketjun välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;

5) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;

6) henkilöstöturvallisuus ja kyberturvallisuusosaaminen;

7) pääsynhallinnan ja todentamisen menettelyt;

8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttämiseksi;

9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;

10) varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan jatkuvuuden hallinta ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö;

11) perustason tietoturvakäytännöt toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi; sekä

12) toimenpiteet viestintäverkkojen ja tietojärjestelmien fyysisen ympäristön ja tilaturvallisuuden sekä välttämättömien resurssien varmistamiseksi.

Hyväksyttävät kustannukset

- Palkkakustannukset
  - Lasketaan hakuilmoituksessa osoitetulla kaavalla
  - Loppuselvityksessä osoitettava, mikä on kunkin henkilön hankkeen aikana tehdyn työajanosuus kokonaistyöajasta
- Ostopalvelut
- Ostot
- Vuokrat ja lisenssit
- Sisäiseen viestintään liittyvät kustannukset
- Kohtuulliset matkakustannukset
- Hankkeen raportointiin liittyvät kustannukset
- Yleisiä kuluja 7 %

Muuta hyväksyttävistä kustannuksista

- Kustannukset hyväksytään ja maksetaan loppuselvityksessä raportoitujen toteutuneiden kustannusten perusteella.
- Hankkeen kustannusten täytyy syntyä ja kohdistua tukea myönnettävälle organisaatiolle niihin toimintoihin tai toimintayksikköihin, joihin kyberturvallisuuslain velvoitteet ulottuvat.
- Kustannukset hyväksytään lähtökohtaisesti arvonlisäverottomina.
- Intressiyrityksiltä ostetut palvelut eivät ole hyväksyttäviä kustannuksia.
- Ehdot koskevat myös omavastuuosuudella rahoitettavia kustannuksia.

Tukihakemus jätetään sähköisellä hakulomakkeella

- Lomakkeelle tunnistaudutaan vahvalla sähköisellä tunnistusvälineellä.
- Hakulomakkeen liitteenä toimitettava hankesuunnitelma tulee tehdä hakusivulla olevaan hankesuunnitelmapohjaan.
- Hakulomakkeen täyttävällä henkilöllä täytyy olla hakijaorganisaation puolesta perusrekisteriin, kuten kaupparekisteriin merkitty organisaation edustamiseen oikeuttava rooli tai Suomi.fi -valtuutus ('Tietoturvan kehittämisen tuen hakeminen') hakea rahoitustukea organisaation puolesta.

Rahoitustuki on harkinnanvaraista

- Rahoitustukea myönnetään hakukelpoisuuskriteerit täyttäville sekä parhaiten hakemusten arvioinnissa menestyville hakijoille.
- Hakemukset arvioidaan ensin hakukelpoisuuskriteerejä vasten. Kriteerit täyttävät hakemukset siirtyvät arviointivaiheeseen, jossa arvioidaan hankkeen tarkoituksenmukaisuutta, toimeenpantavuutta ja vaikuttavuutta.
- Arviointiin vaikuttavat esimerkiksi hakemuksessa annettujen tietojen riittävyys, ymmärrettävyys, selkeys, johdonmukaisuus ja uskottavuus.

Arviointikriteerit

- Tarkoituksenmukaisuus (painoarvo 30 %)
  - Miten hyvin hanke toteuttaa rahoitustuen käyttötarkoitusta ja tavoitteita
  - Missä määrin hanke tukee hakijan kyberturvallisuutta koskevassa riskienhallinnan toimintamallissa määritettyjen riskienhallinnan tavoitteiden toteutumista
- Toimenpantavuus (painoarvo 40 %)
  - Hankesuunnitelman laatu
  - Kustannuserittelyn laatu
  - Hankesuunnitelman tehokkuus ja toimeenpantavuus hankkeelle varattuihin resursseihin ja aikaan nähden
- Vaikuttavuus (painoarvo 30 %)
  - Millainen vaikuttavuus hankkeella on hakijan kyberturvallisuuden lähtötasoon nähden
  - Missä määrin hankkeen tulokset vahvistavat hakijan kykyä suojata hakijan ylläpitämiä yhteiskunnan kannalta keskeisiä ja tärkeitä viestintäverkkoja ja/tai tietojärjestelmiä ja/tai niiden fyysistä ympäristöä kyberturvallisuusuhkilta ja -poikkeamilta
  - Missä määrin hanke ennaltaehkäisee ja rajoittaa yhteiskunnan toimintaan kohdistuvia häiriöitä ja vaikutuksia

Hakuprosessi ja aikataulu

Aika	Vaihe
16.10.2025 klo 16:15	Haun päättyminen
Q4/2025	Hakukelpoisuuden tarkistus ja arviointi
Q1/2026	Rahoitustukipäätösten antaminen, tuen 1. osan maksu ja tiedotus myönnetyistä rahoitustuista koordinointikeskuksen verkkosivuilla
Q1/2027	Loppuselvitysten jättäminen
Q1/2027	Toteutuneiden kustannusten hyväksyminen ja tuen loppuosan maksu
2027	Vaikuttavuuden arviointi

Lisätietoja

- Koordinointikeskus.fi
  - Hakuohjeet ja hakemuksen jättäminen
  - Usein kysytyt kysymykset ja vastaukset
- kyber.rahoitustuki(at)traficom.fi

- Huom! Hakemusten käsittelyn aikana hakemuksen tietoihin ilmenevistä muutoksista on viipymättä ilmoitettava kyber.rahoitustuki(at)traficom.fi

TAUKO

Jatkamme hetken kuluttua

TRAFICOM
Liikenne- ja viestintävirasto

Suositus kyberturvallisuuden riskienhallinnan toimenpiteistä

Topi Talikka
Tietoturva-asiantuntija
Kyberturvallisuuskeskus

Suositus **valvoville viranomaisille** NIS2-direktiivin mukaisista kyberturvallisuuden riskienhallinnan toimenpiteistä.

Suositus voi tukea myös **toimijoiden** kyberturvallisuuden **riskienhallinnan suunnittelua**.

Suositukseen on koottu **tietoa ja käytännön esimerkkejä** siitä, millaisia toimenpiteitä laissa säädettyihin **vaatimuksiin** voi kuulua.

Suosituksessa kuvataan myös erilaisia **keinoja**, joita valvova viranomainen voi harkintansa ja arvionsa mukaan käyttää **ohjaus- ja valvontatehtävissään**.

Suosituksen soveltamisesta

- Ei sido viranomaisia eikä toimijoita. Sitovat velvoitteet säädetään:
  - Laeissa,
  - Euroopan komission antamassa tarkentavassa sääntelyssä ja
  - toimialakohtaisen viranomaisen määräyksissä.
- Toimialakohtaiset määräykset tai muu erityissääntely voi sisältää suosituksesta poikkeavia, tiukempia vaatimuksia.
  - Valvova viranomainen ratkaisee, millaiset toimenpiteet täyttävät säädetyt vaatimukset kullakin toimialalla.
  - Suosituksen mukaisten käytäntöjen toteuttaminen ei takaa sitä, että toimija täyttäisi kansallisen sääntelyn edellyttämät vaatimukset.

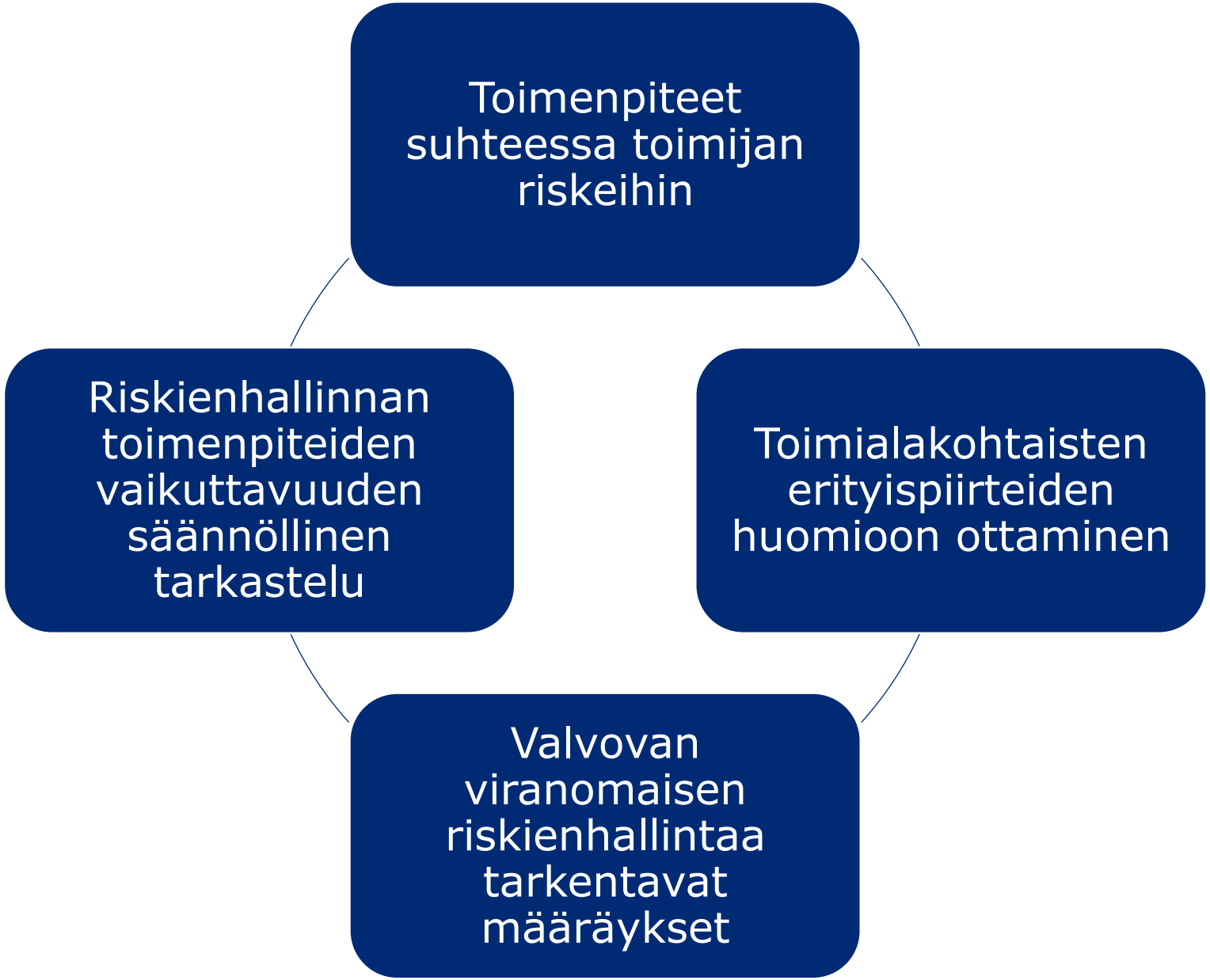
Suosituksen sisällöstä

- Toimijalle asetetaan **riskienhallintavelvoite** kyberturvallisuuslain 2 luvussa 7-10 §:ssä.
  - Suositus keskittyy lain 9 §:ssä säädettyihin **kyberturvallisuuden riskienhallinnan toimenpiteisiin**.
- Suositukseen on koottu yleisimmin käytetyt kyberturvallisuuden **riskienhallintakeinot**.
  - Esimerkkejä toteutuksista, joita valvova viranomainen saattaa kohdata valvonnan yhteydessä.
  - Esimerkkejä todennusmenetelmistä ja viittaukset yleisimpiin kansallisiin ja kansainvälisiin viitekehyksiin.

Riskiperustainen lähestymistapa

Toimijan on toteutettava riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa toiminnassa käytettäville viestintäverkoille ja tietojärjestelmille aiheutuviin riskeihin ja viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.

Kyberturvallisuuslaki 7 § 2 mom.



Kaikki vaaratekijät huomioiden

- Riskien tunnistamisessa huomioidaan internet-välitteisen uhkan lisäksi fyysinen uhka. Tahallinen tai tahaton tapahtuma. Ulkoisen uhkan lisäksi sisäinen uhka.
- Toimijan on huomioitava riskienhallinnassaan teknisen tietoturvallisuuden lisäksi myös verkko- ja tietojärjestelmiensä fyysisen ympäristönsä suojaus.

Kyberturvallisuuden riskienhallinnan toimenpiteet

1. Kyberturvallisuuden **riskienhallinnan toimintaperiaatteet** ja riskienhallinnan toimenpiteiden vaikuttavuuden arviointi

2. Viestintäverkkojen ja tietojärjestelmien **turvallisuutta koskevat toimintaperiaatteet**

3. Viestintäverkkojen ja tietojärjestelmien **hankinnan, kehittämisen ja ylläpidon turvallisuus** sekä tarvittavat menettelyt **haavoittuvuuksien** käsittelyyn ja julkistamiseen

4. **Toimitusketjun** välittömien toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja **häiriönsietokyky**, niihin sisällytetyt hallintatoimenpiteet sekä välittömien toimittajien ja palveluntarjoajien **kyberturvallisuuskäytännöt**

5. **Omaisuudenhallinta** ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen

6. **Henkilöstöturvallisuus ja kyberturvallisuuskoulutus**

7. **Pääsynhallinnan ja todentamisen** menettelyt

8. **Salausmenetelmien** käyttämistä koskevat toimintaperiaatteet ja menettelyt sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön

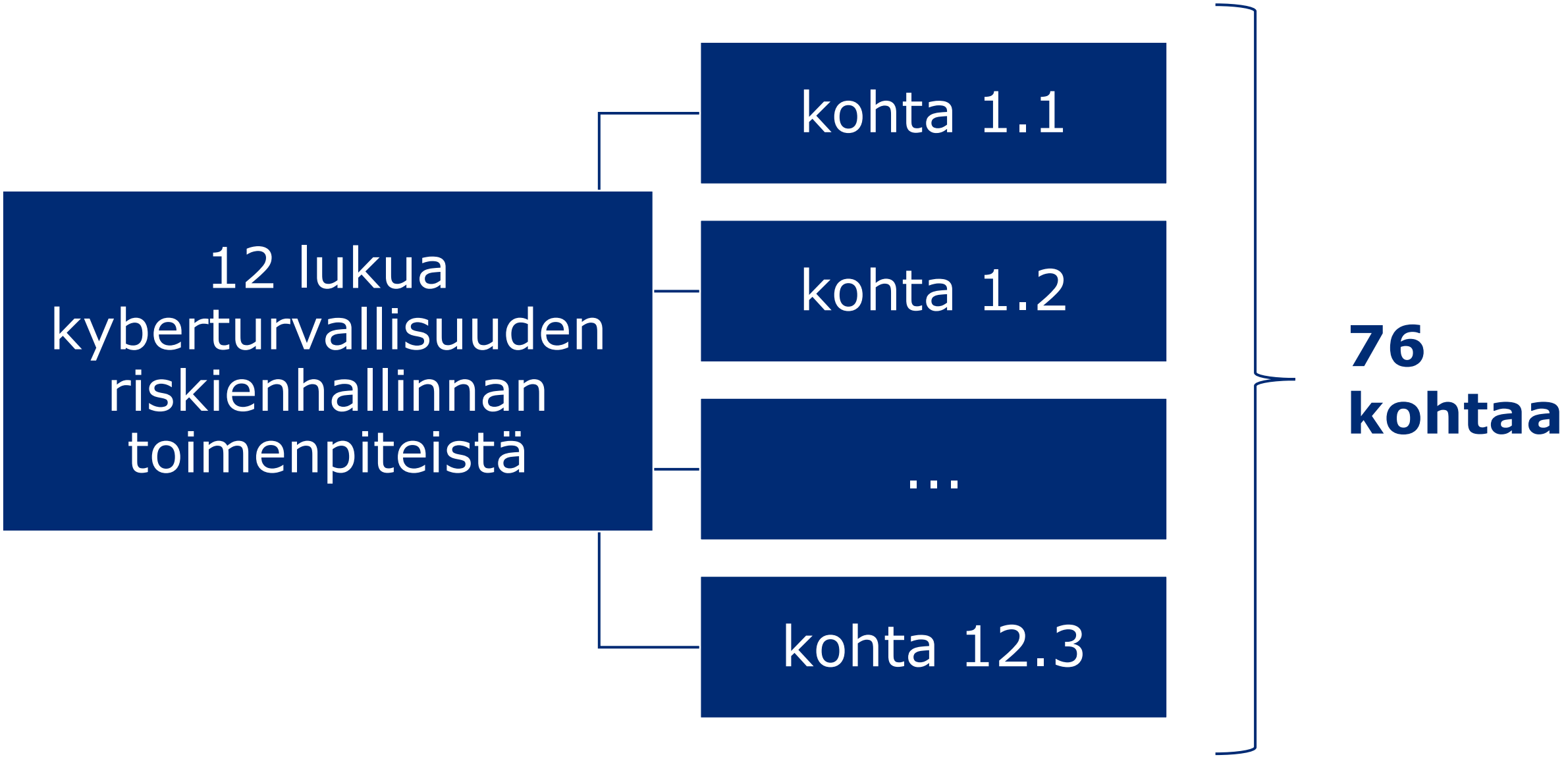
9. **Poikkeamien havainnointi ja käsittely** turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi

10. Varmuuskopiointi, palautumissuunnittelu, kriisinhallinta ja muu toiminnan **jatkuvuuden hallinta** ja tarvittaessa suojattujen varaviestintäjärjestelmien käyttö

11. **Perustason tietoturvakäytännöt** toiminnan, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden ja tietoaineistoturvallisuuden varmistamiseksi

12. Toimenpiteet viestintäverkkojen ja tietojärjestelmien **fyysisen ympäristön** ja tilaturvallisuuden sekä **välttämättömien resurssien** varmistamiseksi

Kyberturvallisuuslaki 9 §
Tiedonhallintalaki 18 c §


12 lukua kyberturvallisuuden riskienhallinnan toimenpiteistä
kohta 1.1
kohta 1.2
...
kohta 12.3
76 kohtaa

Esimerkki suosituksen kohdasta

10.3 Palautustestaus ja varmuuskopioiden suojaaminen

Toteutusesimerkki

Tämä kohta laajentaa perustason tietoturvakäytäntöjen kohtaa 11.11.

- Varmuuskopioiden palautusta ja varajärjestelmien toimivuutta tulisi testata säännöllisesti, ensisijaisesti automaattisesti. Testauksessa pitäisi tarkastaa myös varmuuskopioiden eheys. Varmuuskopioiden palautustestaus on tehtävä turvallisesti niin, ettei se vaaranna tuotantojärjestelmää.
- Varmuuskopioita on säilytettävä turvallisessa tilassa, joka on toimijan riskienhallinnan perusteella riittävän eriytettynä varmuuskopioitavasta järjestelmästä. Tämä voi tarkoittaa esimerkiksi muuta toimitilaa tai erillistä palotilaa. Varmuuskopioita voi säilyttää tarvittaessa useassa muodossa, joiden palautusnopeuksissa voi olla eroa, kuten levylle otetut varmistukset sekä erilliset pitkäaikaisarkistot.
- Varmuuskopioiden suojaamisessa voidaan ottaa huomioon niiden eheyden, saatavuuden ja luottamuksellisuuden tarpeet. Tämä tarkoittaa esimerkiksi riittävää fyysistä suojausta ja muita kontrolleja, kuten salausta.

Todennus

1. Valvova viranomainen todentaa, että toimija on mahdollisuuksien ja tarpeen mukaan määrittänyt toimenpiteet, joilla varmuuskopioiden ja varajärjestelmien toimivuutta testataan säännöllisesti, esimerkiksi kerran viikossa. Tämä voi olla automatisoitua tai manuaalista. Keskeistä on, että mekaanisen palautuksen lisäksi tarkastetaan myös se, että tieto saadaan palautettua eheänä ja käyttökelpoisena, sekä mahdollinen varajärjestelmä pystytettyä oikealla tiedolla. Valvovan viranomainen todentaa, että varmuuskopiot on suojattu riittävästi. Esimerkiksi arkkitehtuurikuvauksissa, järjestelmädokumentaatiossa tai vastaavassa pitäisi olla kuvattuna se, miten varmuuskopiojärjestelmä tai sen osa on eriytetty muusta järjestelmästä. Tämän pitäisi varmistaa se, että jos esimerkiksi viestintäverkkoon ja tietojärjestelmään pääsee hyökkääjä, ei tämä voi päästä käsiksi kaikkiin varmistuksiin.
2. Valvova viranomainen todentaa katselmoinneilla ja haastatteluilla, miten toimija testaa varmuuskopioiden toimivuutta mahdollisuuksien ja tarpeen mukaan. Tästä tulisi käydä ilmi esimerkiksi suoritetut toimenpiteet varmuuskopioiden eheyden varmistamiseksi sekä testauksen säännöllisyys. Valvova viranomainen voi tarvittaessa hyödyntää myös fyysisiä katselmointeja sen varmistamiseksi, että varmuuskopioita on eriytetty muusta järjestelmästä riittävästi. Katselmoinnissa tulisi varmistua esimerkiksi siitä, että uhkat kuten tulipalo, tulvat ja henkilöuhka, eivät koske sekä varmistettavaa järjestelmää että varmuuskopioita.
3. Jos kyseessä on fyysisen erottelun sijaan perusteltu looginen erottelu, voi valvova viranomainen hyödyntää esimerkiksi toimijan tekemiä skannauksia ja yhteydenottoyrityksiä sen varmistamiseksi, että eriytettyyn varmuuskopiointijärjestelmään ei pääse käsiksi varmistettavan viestintäverkon ja tietojärjestelmän puolelta.

Perustelut

Poikkeamatilanteista palautumisen yhteydessä tapahtuu liian usein niin, että palautus ei onnistu tai hyökkääjä onnistuu tuhoamaan sekä tietojärjestelmän että varmuuskopiot. Tämän vuoksi palautuksen kattava ja säännöllinen testaaminen sekä palautusjärjestelmän suojaaminen voivat olla toiminnan kannalta elintärkeitä.

Viitteet

ISO/IEC 27002:2022 (5.33, 8.13, 8.14, 8.24)

IEC 62443-2-1:2010 (4.3.4.3.9)

IEC 62443-2-1:2024 (DATA 1.1, DATA 1.2, DATA 1.5, DATA 1.6, DATA 1.7, AVAIL 1.2, AVAIL 2.3)

IEC 62443-2-4:2024 (SP.12.01, SP.12.02, SP.12.03, SP.12.04, SP.12.05, SP.12.06, SP.12.07)

NIST CSF 1.1 (PR.IP-4, RC.RP-1, RC.IM-1, RC.IM-2)

NIST CSF 2.0 (PR.DS-11, RC.RP-01, RC.RP-05, ID.IM-03)

NIS CG Reference document (3.12.2 Backup and redundancy management)

Työkalut

Julkri (TEK-20, VAR-09)

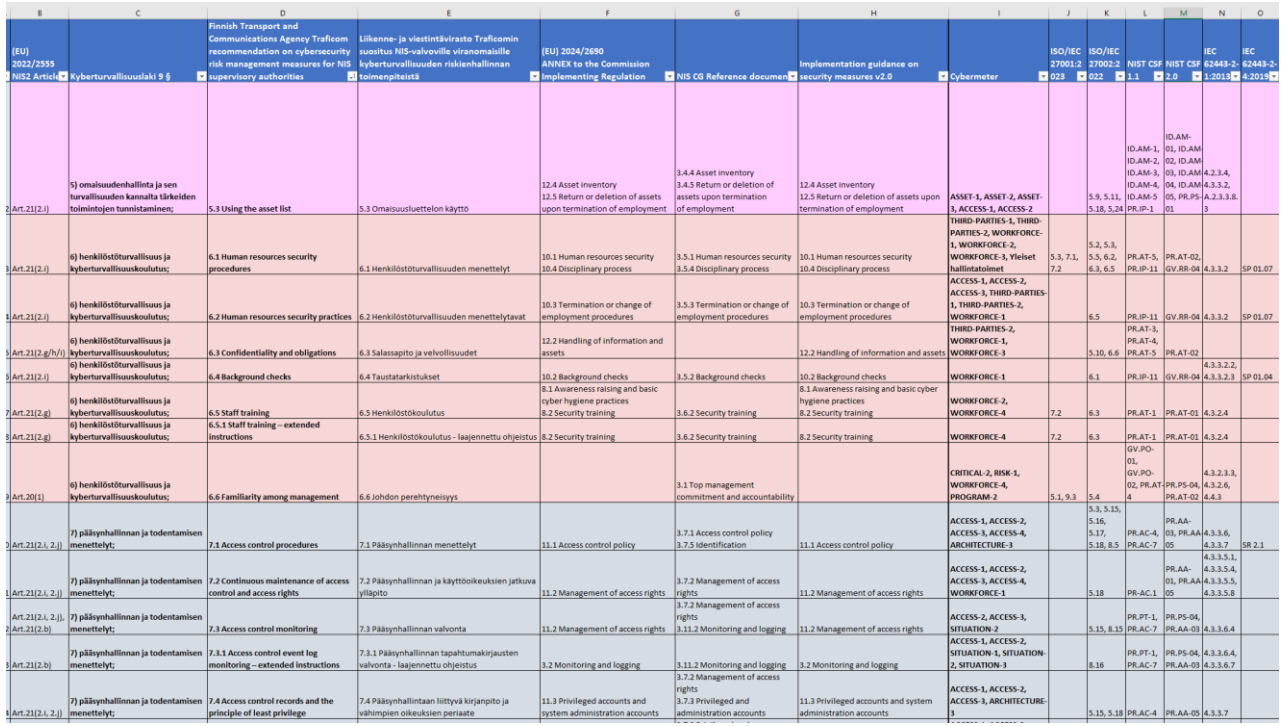
Kybermittari (RESPONSE-4, ARCHITECTURE-1, ARCHITECTURE-5)

Perustason tietoturvakäytännöt

- Antaa yleiskuvan toimijan toteuttamista teknisistä hallintakeinoista
- Asettavat perustason käytännöt, joiden avulla toimija pystyy torjumaan suurimman osan yleisimmistä tietoturvauhkista
- Parantavat yksinään organisaation kypsyystasoa ja kyberturvallisuuden tilaa

Ristiinviittaustaulukko

- Suosituksen liitteenä on julkaistu ristiinviittaustaulukko, josta kaikki suosituksessa käytetyt standardiviittaukset löytyvät taulukkomuodossa.
- Muista riskiperustainen lähestymistapa!
- Laki ei velvoita minkään standardin käyttöä, mutta ne voivat antaa lisätukea riskienhallinnan suunnitteluun.
- Standardit voivat sisältää laista poikkeavia vaatimuksia.



	B	C	D	E	F	G	H	I	J	K	L	M	N	O
	(EU) 2022/2555 NIS2 Article	Kyberturvallisuuslaki 9 §	Finnish Transport and Communications Agency Traficom recommendation on cybersecurity risk management measures for NIS supervisory authorities	Liikenne- ja viestintävirasto Traficomin suositus NIS-valvoville viranomaisille kyberturvallisuuden riskienhallinnan toimenpiteistä	(EU) 2024/2690 ANNEX to the Commission Implementing Regulation	NIS CG Reference documen	Implementation guidance on security measures v2.0	Cybermeter	ISO/IEC 27001:2 023	ISO/IEC 27002:2 022	NIST CSF 1.1	NIST CSF 2.0	IEC 62443-2-1:2013	IEC 62443-2-4:2015
2	Art.21(2.i)	5) omaisuudenhallinta ja sen turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;	5.3 Using the asset list	5.3 Omaisuusluettelon käyttö	12.4 Asset inventory 12.5 Return or deletion of assets upon termination of employment	3.4.4 Asset inventory 3.4.5 Return or deletion of assets upon termination of employment	12.4 Asset inventory 12.5 Return or deletion of assets upon termination of employment	ASSET-1, ASSET-2, ASSET-3, ACCESS-1, ACCESS-2		5.9, 5.11, 5.18, 5,24	ID.AM-1, ID.AM-2, ID.AM-3, ID.AM-4, ID.AM-5 PR.IP-1	ID.AM-01, ID.AM 02, ID.AM 03, ID.AM 04, ID.AM 05, PR.PS-01	4.2.3.4, 4.3.3.2, A.2.3.3.8, 3	
3	Art.21(2.i)	6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;	6.1 Human resources security procedures	6.1 Henkilöstöturvallisuuden menettelyt	10.1 Human resources security 10.4 Disciplinary process	3.5.1 Human resources security 3.5.4 Disciplinary process	10.1 Human resources security 10.4 Disciplinary process	THIRD-PARTIES-1, THIRD-PARTIES-2, WORKFORCE-1, WORKFORCE-2, WORKFORCE-3, Yleiset hallintatoimet	5.3, 7.1, 7.2	5.2, 5.3, 5.5, 6.2, 6.3, 6.5	PR.AT-5, PR.IP-11	PR.AT-02, GV.RR-04	4.3.3.2	SP 01.07
4	Art.21(2.i)	6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;	6.2 Human resources security practices	6.2 Henkilöstöturvallisuuden menettelytavat	10.3 Termination or change of employment procedures	3.5.3 Termination or change of employment procedures	10.3 Termination or change of employment procedures	ACCESS-1, ACCESS-2, ACCESS-3, THIRD-PARTIES-1, THIRD-PARTIES-2, WORKFORCE-1		6.5	PR.IP-11	GV.RR-04	4.3.3.2	SP 01.07
5	Art.21(2.g/h/i)	6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;	6.3 Confidentiality and obligations	6.3 Salassapito ja velvollisuudet	12.2 Handling of information and assets		12.2 Handling of information and assets	THIRD-PARTIES-2, WORKFORCE-1, WORKFORCE-3		5.10, 6.6	PR.AT-3, PR.AT-4, PR.AT-5	PR.AT-02		
6	Art.21(2.i)	6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;	6.4 Background checks	6.4 Taustatarkistukset	10.2 Background checks	3.5.2 Background checks	10.2 Background checks	WORKFORCE-1		6.1	PR.IP-11	GV.RR-04	4.3.3.2.2, 4.3.3.2.3	SP 01.04
7	Art.21(2.g)	6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;	6.5 Staff training	6.5 Henkilöstökoulutus	8.1 Awareness raising and basic cyber hygiene practices 8.2 Security training	3.6.2 Security training	8.1 Awareness raising and basic cyber hygiene practices 8.2 Security training	WORKFORCE-2, WORKFORCE-4	7.2	6.3	PR.AT-1	PR.AT-01	4.3.2.4	
8	Art.21(2.g)	6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;	6.5.1 Staff training – extended instructions	6.5.1 Henkilöstökoulutus - laajennettu ohjeistus	8.2 Security training	3.6.2 Security training	8.2 Security training	WORKFORCE-4	7.2	6.3	PR.AT-1	PR.AT-01	4.3.2.4	
9	Art.20(1)	6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;	6.6 Familiarity among management	6.6 Johdon perehtyneisyys		3.1 Top management commitment and accountability		CRITICAL-2, RISK-1, WORKFORCE-4, PROGRAM-2	5.1, 9.3	5.4	GV.PO-01, GV.PO-02, PR.AT-4	PR.PS-04, PR.AT-02	4.3.2.3.3, 4.3.2.6, 4.4.3	
10	Art.21(2.i, 2.j)	7) pääsynhallinnan ja todentamisen menettelyt;	7.1 Access control procedures	7.1 Pääsynhallinnan menettelyt	11.1 Access control policy	3.7.1 Access control policy 3.7.5 Identification	11.1 Access control policy	ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, ARCHITECTURE-3		5.3, 5.15, 5.16, 5.17, 5.18, 8.5	PR.AC-4, PR.AC-7	PR.AA-03, PR.AA 05	4.3.3.6, 4.3.3.7	SR 2.1
11	Art.21(2.i, 2.j)	7) pääsynhallinnan ja todentamisen menettelyt;	7.2 Continuous maintenance of access control and access rights	7.2 Pääsynhallinnan ja käyttöoikeuksien jatkuva ylläpito	11.2 Management of access rights	3.7.2 Management of access rights	11.2 Management of access rights	ACCESS-1, ACCESS-2, ACCESS-3, ACCESS-4, WORKFORCE-1		5.18	PR-AC.1	PR.AA-01, PR.AA 05	4.3.3.5.1, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.8	
12	Art.21(2.i, 2.j), Art.21(2.b)	7) pääsynhallinnan ja todentamisen menettelyt;	7.3 Access control monitoring	7.3 Pääsynhallinnan valvonta	11.2 Management of access rights	3.7.2 Management of access rights 3.11.2 Monitoring and logging	11.2 Management of access rights	ACCESS-2, ACCESS-3, SITUATION-2		5.15, 8.15	PR.PT-1, PR.AC-7	PR.PS-04, PR.AA-03	4.3.3.6.4	
13	Art.21(2.b)	7) pääsynhallinnan ja todentamisen menettelyt;	7.3.1 Access control event log monitoring – extended instructions	7.3.1 Pääsynhallinnan tapahtumakirjausten valvonta - laajennettu ohjeistus	3.2 Monitoring and logging	3.11.2 Monitoring and logging	3.2 Monitoring and logging	ACCESS-1, ACCESS-2, SITUATION-1, SITUATION-2, SITUATION-3		8.16	PR.PT-1, PR.AC-7	PR.PS-04, PR.AA-03	4.3.3.6.4, 4.3.3.6.7	
14	Art.21(2.i, 2.j)	7) pääsynhallinnan ja todentamisen menettelyt;	7.4 Access control records and the principle of least privilege	7.4 Pääsynhallintaan liittyvä kirjanpito ja vähimpien oikeuksien periaate	11.3 Privileged accounts and system administration accounts	3.7.2 Management of access rights 3.7.3 Privileged and administration accounts	11.3 Privileged accounts and system administration accounts	ACCESS-1, ACCESS-2, ACCESS-3, ARCHITECTURE-3		5.15, 5.18	PR.AC-4	PR.AA-05	4.3.3.7	

Yhteenveto

- Suositus tarjoaa katalogin erilaisista kyberturvallisuuden riskienhallintatoimenpiteisiin liittyvistä menetelmistä
- Riskien hallinta on jatkuvaa! Riskien tunnistaminen, arviointi ja käsittely sekä hallintatoimenpiteiden ajantasaisuuden varmistaminen ovat riskienhallinnan keskiössä
- Jos kyberturvallisuus ja sen riskienhallinta on organisaatiolle uusi asia, alkuun pääsee parhaiten perustason tietoturvakäytäntöjä soveltamalla
- Ole matalla kynnyksellä yhteydessä omaan valvovaan viranomaiseesi, heiltä saa ohjausta ja tukea kyberturvallisuuslain soveltamiseen

Kiitos!

Tutustu myös Kyberturvallisuuskeskuksen NIS2-teemasivuihin

Lisätietoa

Kyber.rahoitustuki(at)traficom.fi

Kyberturvallisuuskeskus.fi

Koordinointikeskus.fi