FINNISH
GOVERNMENT

Tervetuloa

FINNISH GOVERNMENT

NIS2-direktiivin kansallinen toimeenpano

Sidosryhmätilaisuus 9.10.2023, klo 8.45 – 11.00.

Ohjelma

8.45	**Kahvitarjoilu**
9.00	**Tilaisuuden avaus** *LVM, yksikön päällikkö Maija Ahokas*
9.05	**Hallituksen esitys NIS2 direktiivin kansalliseksi täytäntöönpanemiseksi** *LVM, hallitussihteeri Veikko Vauhkonen*
9.30	**NIS2-direktiivin täytäntöönpano julkishallinnossa** *VM, lainsäädäntöneuvos Eeva Lantto*
9.45	**Liikenne- ja viestintävirasto NIS2- direktiivin täytäntöönpanossa** *Liikenne ja viestintävirasto Traficom, Kyberturvallisuuskeskus, erityisasiantuntija Kalle Varjola*
10.00	**Selvitys NIS2-direktiivin riskienhallintavelvoitteiden taloudellisista vaikutuksista elintarvike- ja valmistussektorille** *Insta Group Oy, Senior Privacy Consultant Jassi Saurio ja Senior Security Advisor Kimmo Pajunen*
10.20 – 11.00	**Kysymykset ja yhteinen keskustelu**

VALTIONEUVOSTO
STATSRÅDET

FINNISH
GOVERNMENT

Tilaisuuden avaus

LVM yksikön päällikkö Maija Ahokas

Hallituksen esitys NIS2-direktiivin kansalliseksi täytäntöönpanemiseksi

Kuulemistilaisuus 9.10.2023

Hallitussihteeri Veikko Vauhkonen
Tieto- ja turvallisuusosasto
Turvallisuusyksikkö

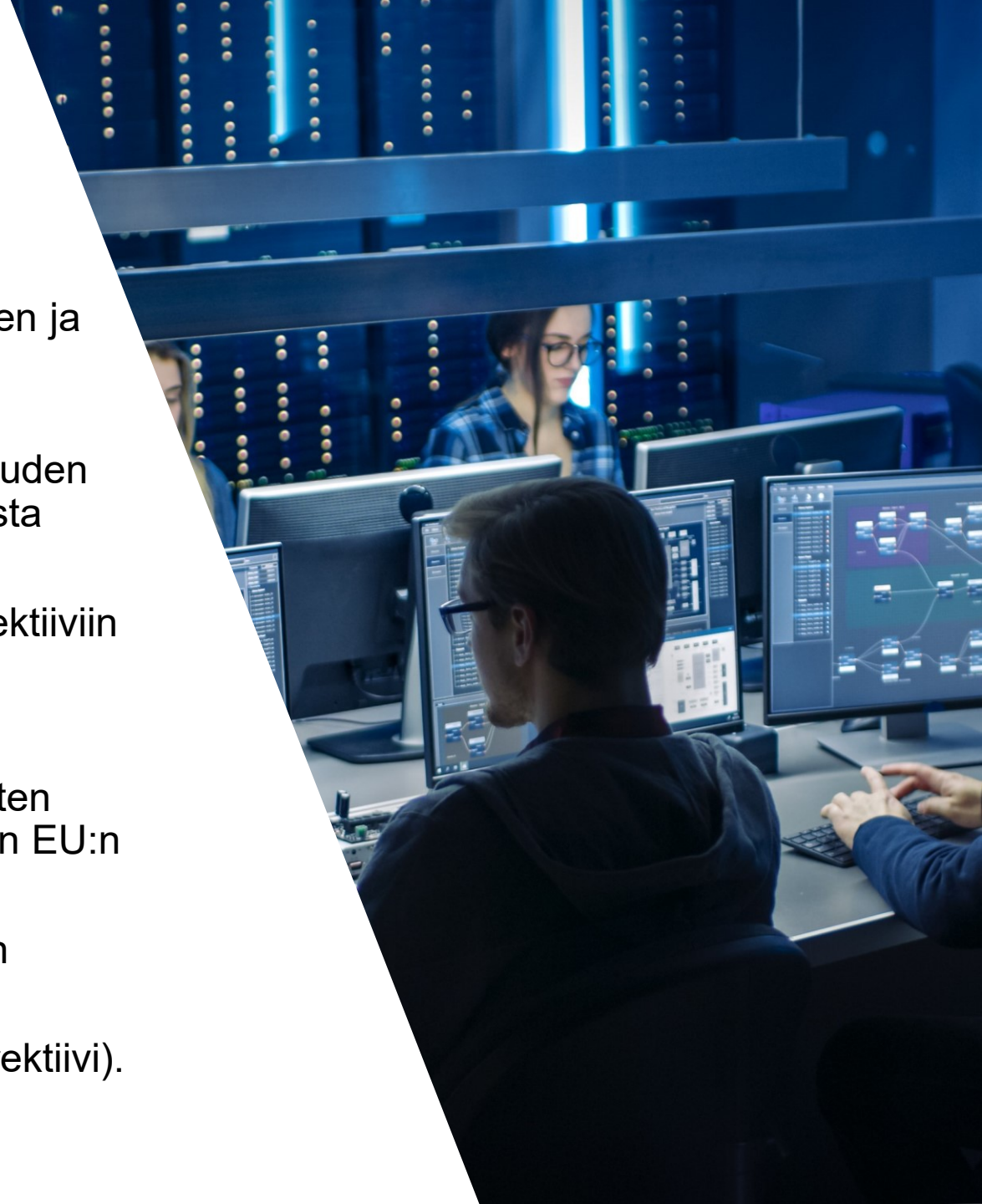
LIIKENNE- JA VIESTINTÄMINISTERIÖ

Esityksen valmistelu

- Direktiivi julkaistiin joulukuussa 2022, toimeenpanon määräaika 17.10.2024.
- Hanke käynnistettiin virallisesti tammikuussa 2023.
- Työryhmärakenne koostuu päätyöryhmästä (LVM pj.) ja julkishallinnon sektoria koskevasta alatyöryhmästä (VM pj.). Työryhmissä poikkihallinnollinen kokoonpano.
  - Päätyöryhmässä on kuultu keskeisten etujärjestöjen edustajia keväällä 2023. Lisäksi valmistelua on yhteensovitettu CER- ja DORA-valmistelun kanssa ja keskusteltu EU:n komission kanssa.
  - Vaikutustenarviointiselvityksen hankinta keväällä 2023.
  - Sidosryhmäkuulemisia valmistelun aikana:
    - Yleinen sidosryhmätilaisuus 30.3.2023
    - Julkishallinnon webinaari 4.5.2023
    - Yleinen sidosryhmätilaisuus 9.10.2023
- Lausuntokierros 3.10. – 29.11.2023.
- Lausuntopalautteen läpikäynti ja jatkovalmistelu 11/2023 alkaen.
- Tavoitteena HE eduskunnalle kevättalvella 2024 ja voimaan 18.10.2024.

Kyberturvallisuusdirektiivi eli NIS2-direktiivi

- Tavoitteena on vahvistaa ja yhdenmukaistaa jäsenvaltioiden ja EU:n yhteistä kyberturvallisuustasoa tietyillä yhteiskunnan sektoreilla.
- Horisontaaliset vähimmäistason velvoitteet kyberturvallisuuden riskienhallinnasta ja merkittävien poikkeamien raportoinnista soveltamisalaan kuuluville toimijoille.
- Velvoitteet tarkentuvat ja soveltamisala laajenee NIS1-direktiiviin verrattuna.
- Toimijoiden jaottelu keskeisiin ja tärkeisiin toimijoihin.
- Lisäksi direktiivissä on EU:n jäsenvaltioiden ja viranomaisten väliseen yhteistyöhön liittyvää sääntelyä ja siinä säädetään EU:n CyCLONe-verkoston tehtävistä.
- Direktiivin mukaisia velvoitteita on sovellettava viimeistään 18.10.2024 alkaen.
- Kumoaa aiemman verkko- ja tietoturvadirektiivin (NIS1-direktiivi).



Keskeiset ehdotukset

- Uusi laki kyberturvallisuuden riskienhallinnasta
  - Toimijoihin kohdistuvista velvoitteista ja niiden valvonnasta sekä muista direktiivin edellyttämistä viranomaistehtävistä säätäminen keskitetysti.
  - Lähtökohtana kansallisen liikkumavaran hyödyntäminen täysimääräisesti velvoitteiden soveltamisalassa, laajuudessa ja valvonnassa.
  - Sektorikohtaista sääntelyä voi soveltaa ensisijaisesti, jos se täyttää velvoitteet korkeatasoisemmin, esim. finanssisektorilla DORA-asetus.
- Julkishallinnon täytäntöönpano tiedonhallintalaissa
- Sähköisen viestinnän palveluista annetun lain muutoksia aluetunnusrekisteriä ja verkkotunnusvälittäjiä koskevan artiklan johdosta.
- NIS1-täytäntöönpanosäännösten kumoaminen sektorikohtaisista laeista.
- Valvonta toimialakohtaisesti ja seuraamusmaksulautakunta.
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimisi tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä.
- Kyberturvallisuustietojen vapaaehtoiset jakamisjärjestelyt.
- Kyberturvallisuusstrategian hyväksyminen ja sisältö.
- Ei kansallisia lisävaatimuksia sertifioitujen tuotteiden tai –palveluiden käytölle.

Soveltamisala

Oikeushenkilö tai luonnollinen henkilö, joka:

Harjoittaa liitteessä I tai II tarkoitettua toimintaa tai on siinä tarkoitettua toimijatyppiä JA

A) Täyttää tai ylittää keskisuuren toimijan määritelmän; tai

B) Koosta riippumatta, jos toimija on

- Yleisten sähköisten viestintäverkkojen tai yleisesti saatavilla olevien sähköisten viestipalvelujen tarjoaja
- Luottamuspalvelun tarjoaja
- Aluetunnusrekisteri tai DNS-palveluntarjoaja
- Palvelun tarjoaja kuuluu erityisluokkiin ja säädetty soveltamisesta asetuksella koosta riippumatta: yhteiskunnan kriittisten toimintojen ylläpitäminen, häiriön merkittävä vaikutus yl. järjestykseen, yl. turvallisuuteen tai kansanterveyteen, häiriön merkittävä systeeminen riski (rajat ylittävin vaikutuksin) taikka erityisen suuri merkitys kansallisella tai alueellisella tasolla.

On CER-direktiivin nojalla määritelty kriittinen toimija

Kokokriteeri

Komission suosituksen 2003/361/EY kynnysarvot

Keskisuuri toimija

= 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)

Suosituksessa olevaa julkisomisteisuuden rajausta ei sovelleta.

NIS2 toimialat (uudet punaisella)

Liite I

- Energia (vety- ja latauspisteiden palveluntarjoajat)
- Liikenne
- Pankkitoiminta
- Finanssimarkkinoiden infrastruktuuri
- Terveys
- Juomavesi
- Jätevesi
- Digitaalinen infrastruktuuri (tele, luottamuspalvelut, CDN, konesalit)
- TVT-palvelujen hallinta (yritysten välinen)
- Julkishallinto
- Avaruus

Liite II

- Posti- ja kuriiripalvelut
- Jätehuolto
- Kemikaalien valmistus, tuotanto ja jakelu
- Elintarvikkeiden tuotanto, jalostus ja jakelu
- Valmistus (mm. lääkinnälliset laitteet, tietokoneet sekä elektroniset ja optiset laitteet, sähkölaitteet, muut koneet ja laitteet sekä kulkuneuvot)
- Digitaalisen palvelun tarjoajat (verkkoyhteisöalustojen tarjoajat)
- Tutkimustoiminta

Keskeiset velvoitteet toimijoille

Riskienhallinta

Raportointi merkittävistä poikkeamista

Toimijaluetteloon ilmoittautuminen

Riskienhallinta

Kyberturvallisuuden riskienhallinta: tavoitteena estää tai minimoida kyberuhkien tai poikkeamien vaikutus toimintaan, sen jatkuvuuteen palveluiden vastaanottajiin ja muihin palveluihin.

Yleinen riskienhallintavelvoite:

Toimijan

- on tunnistettava, arvioitava ja hallittava riskejä, joita kohdistuu sen toiminnoissa tai palveluntarjonnassa käytettävien viestintäverkkojen ja tietojärjestelmien turvallisuudelle.
- on toteutettava turvallisuus- ja riskienhallintatoimenpiteet, jotka ovat ajantasaisia, oikeasuhtaisia ja riittäviä suhteessa riskeihin sekä viestintäverkon tai tietojärjestelmän merkitykseen toimijan toiminnan ja palveluntarjonnan kannalta.
- johto vastaa riskienhallinnan toteuttamisesta.

Riskienhallinta

Riskienhallinnan toimintamalli

Toimijalla on oltava käytössään ajantasainen 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.
- 9 §: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.
- Valvova viranomainen voisi antaa tarkempia teknisiä määritelmiä riskienhallinnasta.
- Noudatettava lisäksi komission NIS2-direktiivin nojalla antamia täytäntöönpanosäädöksiä.

Riskienhallinta

Toimintamallissa ja hallintatoimenpiteissä on huomioitava:

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 menettelyt haavoittuvuuksien käsittelyyn ja julkistamiseen;

4) toimitusketjun toimittajien tuotteiden ja palveluntarjoajien palvelujen yleinen laatu ja häiriönsietokyky, tuotteisiin ja palveluihin sisällytetyt kyberturvallisuusriskien hallintatoimenpiteet sekä toimittajien ja palveluntarjoajien kyberturvallisuuskäytännöt;

5) omaisuudenhallinta ja turvallisuuden kannalta tärkeiden toimintojen tunnistaminen;

6) henkilöstöturvallisuus ja kyberturvallisuuskoulutus;

7) pääsynhallinnan ja todentamisen menettelyt;

8) salausmenetelmien käyttämistä koskevat toimintaperiaatteet sekä tarvittaessa toimenpiteet suojatun sähköisen viestinnän käyttöön;

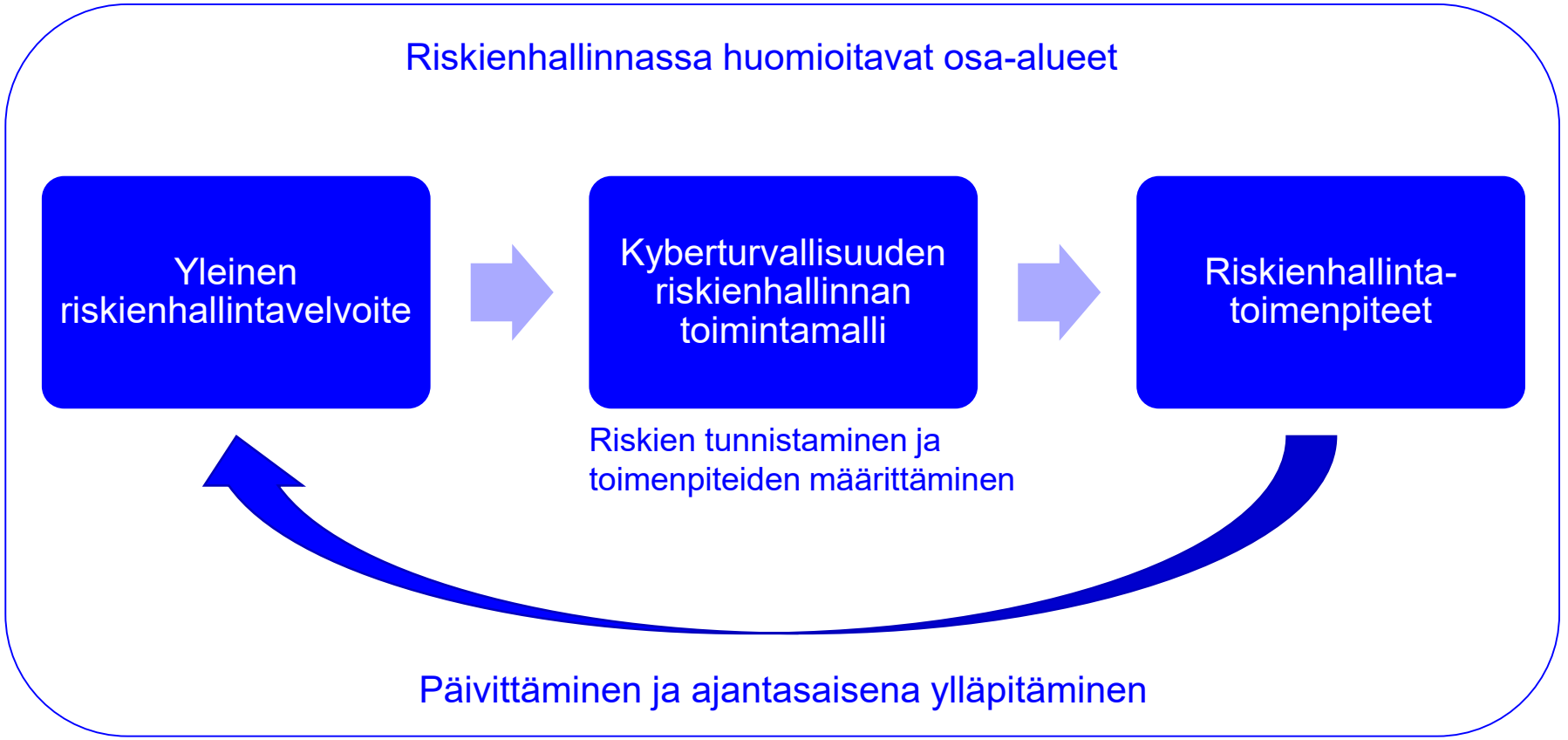
9) poikkeamien havainnointi ja käsittely turvallisuuden ja toimintavarmuuden palauttamiseksi ja ylläpitämiseksi;

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

11) perustason kyberhygieniakäytännöt

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

Riskienhallinta – mitä esitys edellyttäisi?



Keskeiset velvoitteet toimijoille

Riskienhallinta

Raportointi merkittävistä poikkeamista

Toimijaluetteloon ilmoittautuminen

Raportointi merkittävistä poikkeamista

Raportointivelvoite merkittävistä poikkeamista viipymättä valvovalle viranomaiselle

Poikkeama:

tapahtuma, joka vaarantaa viestintäverkoissa tai tietojärjestelmissä tarjottavien tai niiden välityksellä saatavilla olevien tallennettujen, siirrettyjen tai käsiteltyjen tietojen taikka palvelujen saatavuuden, aitouden, eheyden tai luottamuksellisuuden.

Merkittävä poikkeama:

poikkeama, joka on aiheuttanut tai voi aiheuttaa palvelujen vakavan toimintahäiriön tai asianomaiselle toimijalle taloudellisia tappioita taikka poikkeama on vaikuttanut tai voi vaikuttaa muihin luonnollisiin henkilöihin tai oikeushenkilöihin aiheuttamalla huomattavaa aineellista tai aineetonta vahinkoa.

Vapaaehtoinen ilmoittaminen muista kuin merkittävistä poikkeamista, kyberuhkista ja läheltä piti – tilanteista valvovalle viranomaiselle.

Raportointi merkittävistä poikkeamista

Ensi-ilmoitus 24h kuluessa → Jatkoilmoitus 72h kuluessa → Mahdollinen väliraportti → Loppuraportti 1kk kuluessa

- Ensi- ja jatkoilmoitus 24/72h kuluessa poikkeaman havaitsemisesta, loppuraportti 1kk kuluessa jatkoilmoituksesta.
- Ilmoitukset sähköisen asiointipalvelun kautta.
- Valvova viranomainen välittää raportin CSIRT-yksikölle (Kyberturvallisuuskeskus) ja antaa toimijalle vastauksen viivytyksettä.
- CSIRT-yksikkö antaa toimijan pyynnöstä ohjeita tai operatiivisia neuvoja merkittävän poikkeaman vaikutuksia lieventävistä toimenpiteistä.
- Toimijan on ilmoitettava palvelujen vastaanottajille, jos poikkeama todennäköisesti haittaa palvelujen tarjoamista.
- Toimijan on ilmoitettava kyberuhkasta ja sen hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujensa vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa.
- Valvova viranomainen voisi määräyksellä tarkentaa poikkeaman merkittävyyttä ja siitä ilmoittamista.

Keskeiset velvoitteet toimijoille

Riskienhallinta

Raportointi merkittävistä poikkeamista

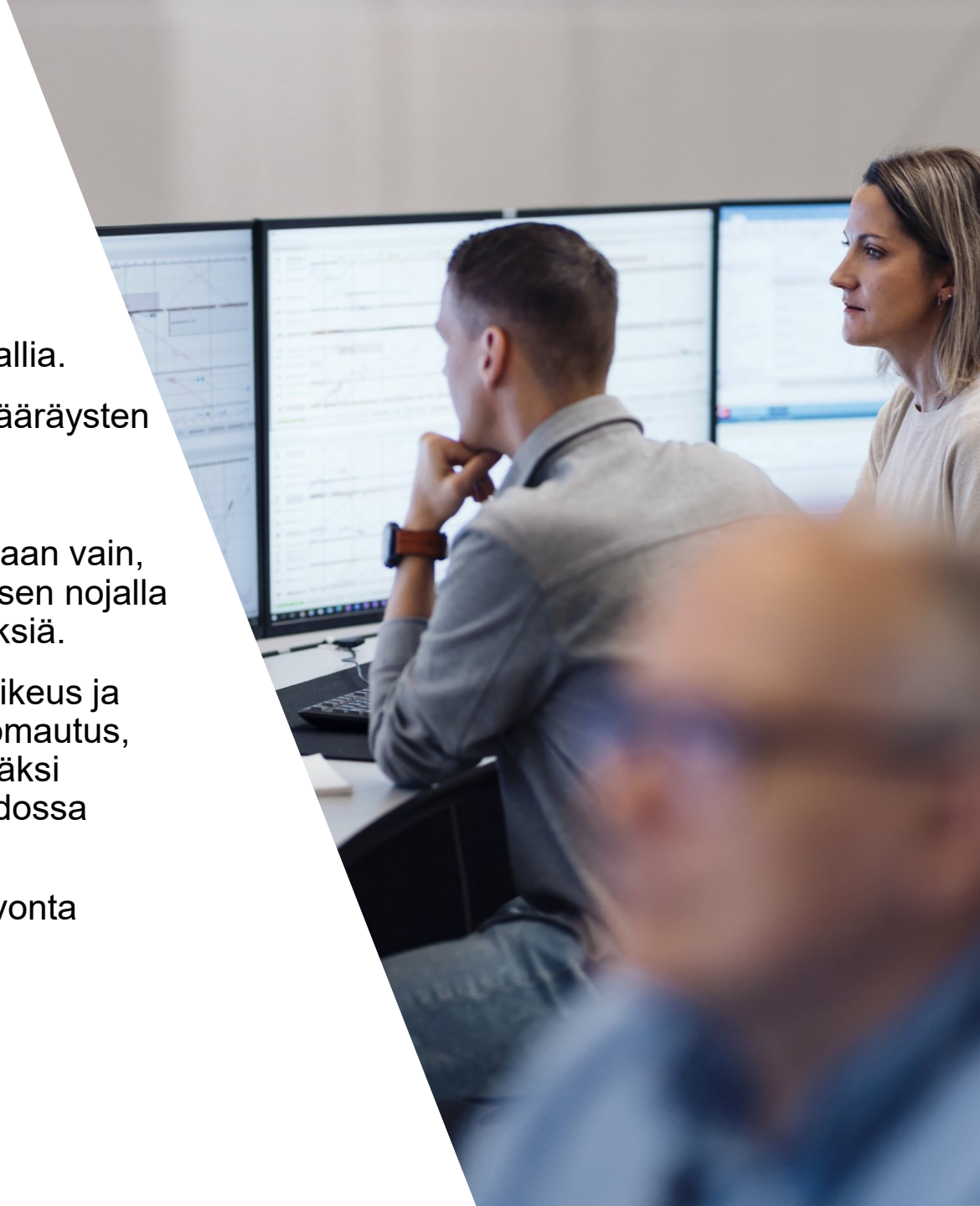
Toimijaluetteloon ilmoittautuminen

Toimijaluetteloon ilmoittautuminen

- Valvova viranomainen ylläpitää valvontatoimialansa osalta toimijaluetteloa.
- Toimijan on ilmoitettava valvovalle viranomaiselle tätä varten:
  - Toimijan nimi ja ajantasaiset yhteystiedot sekä IP-osoitealueet
  - NIS2-direktiivin liitteessä tarkoitettu toimiala ja sen osa
  - Täyttääkö toimija keskeisen toimijan määritelmän
  - Osallistumisesta kyberturvallisuustietojen vapaaehtoiseen jakamisjärjestelyyn.
- Muutoksista tietoihin olisi ilmoitettava viipymättä ja enintään kahden viikon kuluessa muutoksesta.
- Valvova viranomainen voisi antaa teknisiä määräyksiä tietojen ilmoittamisesta.
- Eräiden toimijoiden (mm. digi-infrastruktuuri) olisi lisäksi ilmoitettava päätoimipaikka, luettelo jäsenvaltioista, joissa palveluja tarjotaan, sekä liitteen mukainen toimijatyyppi.
- Voimaan muusta esityksestä poiketen 1.1.2025.

Valvonta

- Valvovan viranomaisen tehtävässä jatkettaisiin NIS1-direktiivin täytäntöönpanossa omaksuttua toimialakohtaisesti hajautettua mallia.
- Valvonnan tarkoituksena varmistaa lain, sen nojalla annettujen määräysten ja NIS2-direktiivin nojalla annettujen säädösten noudattaminen.
- Valvonta kohdistettaisiin riskiperusteisesti keskeisiin toimijoihin. Ennakkovalvontaa voisi kohdistaa muuhun kuin keskeiseen toimijaan vain, jos on perusteltu syy epäillä, että toimija ei ole noudattanut lakia, sen nojalla annettuja määräyksiä, tai NIS2-direktiivin nojalla annettuja säädöksiä.
- Valvovan viranomaisen toimivaltuuksia olisivat mm. tiedonsaantioikeus ja tietopyynnöt, tarkastus, turvallisuusauditoinnin teetättäminen, huomautus, varoitus ja korjaaviin toimiin velvoittaminen uhkasakon uhalla. Lisäksi viimesijainen toimivalta rajoittaa henkilön toimimista yrityksen johdossa sekä rajoittaa tai esittää luvanvaraista toimintaa rajoitettavaksi.
- Jos monialatoimijaa valvoisi useampi kuin yksi viranomainen, valvonta kohdistuu toimialaan ja viranomaisilla yhteistyövelvoite.



Valvonta

Valvova viranomainen (25 §)	Toimiala
Liikenne- ja viestintävirasto	Ilmaliikenne, raideliikenne, vesiliikenne, tieliikenne, avaruus, digitaalinen infrastruktuuri, TVT-palvelujen hallinta, kuriiri- ja postipalvelun tarjoajat, digitaalisen palvelun tarjoajat, valmistus (moottoriajoneuvojen, perävaunujen ja puoliperävaunujen valmistusta harjoittavat toimijat, muiden kulkuneuvojen valmistusta harjoittavat toimijat, tutkimusorganisaatiot, julkishallinto
Energiavirasto	Sähkö, kaukolämmityksen tai kaukojäähdytyksen haltijat, kaasu (jakelu- ja siirtoverkonhaltijat)
Turvallisuus- ja kemikaalivirasto	Kaasu (maakaasun toimittajat, varastointilaitteiston haltijat, maakaasun käsittelylaitteiston haltijat, maakaasualan yritykset sekä maakaasun jalostus- ja käsittelylaitteistojen haltijat), öljy, vedyn tuotantoa, varastointia ja siirtoa harjoittavat toimijat, aineiden valmistusta ja aineiden tai seosten jakelua harjoittavat yritykset sekä yritykset, jotka tuottavat esineitä aineista tai seoksista, tietokoneiden, elektronisten ja optisten laitteiden valmistajat, sähkölaitteiden valmistajat sekä muiden koneiden ja laitteiden valmistajat
Sosiaali- ja terveydenalan lupa- ja valvontavirasto	Terveys
Etelä-Savon ELY-keskus	Juomavesi, jätevesi ja jätehuolto
Ruokavirasto	Elintarvikeyritykset, jotka harjoittavat tukkukauppaa, teollista tuotantoa tai jalostusta
Lääkealan turvallisuus- ja kehittämiskeskus	Lääkinnällisiä laitteita valmistavat toimijat ja In vitro –diagnostiikkaan tarkoitettuja lääkinnällisiä laitteita valmistavat toimijat
Finanssivalvonta	Pankkitoiminta ja finanssimarkkinoiden infrastruktuuri

Esityksen muita ehdotuksia

- Riskienhallinta- ja raportointivelvoitteiden ja toimijaluetteloon ilmoittautumisen laiminlyönnistä voitaisiin määrätä hallinnollinen seuraamusmaksu. Maksun määräisi valvovan viranomaisen esityksestä seuraamusmaksulautakunta.
- Liikenne- ja viestintäviraston Kyberturvallisuuskeskus toimisi tietoturvaloukkauksiin reagoivana ja niitä tutkivana CSIRT-yksikkönä, jonka tehtävistä ja toimivaltuuksista säädettäisiin laissa.
- CSIRT-yksikkö toimisi koordinaattorina koordinoitua haavoittuvuuksien julkaisemista varten Euroopan haavoittuvuustietokantaan.
- Toimijoiden, CSIRT-yksikön ja muiden tahojen välillä voitaisiin muodostaa kyberturvallisuustietojen vapaaehtoisia jakamisjärjestelyitä kyberuhkien ehkäisemiseksi, havaitsemiseksi, poikkeamien hallitsemiseksi ja niistä palautumiseksi tai vaikutusten lieventämiseksi.
- Laissa säädettäisiin kansallisen kyberturvallisuusstrategian hyväksymisestä ja vähimmäissisällöstä. Strategian hyväksyisi valtioneuvosto.
- Laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman laatimisesta vastaisi Liikenne- ja viestintävirasto yhteistoiminnassa valvovien viranomaisten, poliisihallituksen, suojelupoliisin, Puolustusvoimien ja Huoltovarmuuskeskuksen kanssa.

Mitä seuraavaksi?

- Lausuntokierros käynnissä, lausuntoaikaa 29.11.2023 saakka.
- Esitys saatavilla lausuntopalvelu.fi –palvelussa.
- Lausuntopalautteen arviointi ja jatkovalmistelu 11/23 – 01/24.
- Eduskuntakäsittely keväällä 2024.
- LVM:n valmistelijat: Veikko Vauhkonen ja Sonja Töyrylä-Posio.

Lisätietoja:

- Lausuntopalvelu: https://www.lausuntopalvelu.fi/FI/Proposal/Participation?proposalId=4433cf…a-00ca-412e-8f47-20c55031b8dd
- Hankeikkuna: https://valtioneuvosto.fi/hanke?tunnus=LVM027:00/2023
- LVM.fi: https://lvm.fi/-/hallituksen-esitys-kyberturvallisuusdirektiivin-taytantoonpanemiseksi-lausunnoille
- LVM.fi: https://www.lvm.fi/-/kyberturvallisuusdirektiivi-vahvistaa-koko-eu-n-kyberturvallisuustasoa-kansallinen-toimeenpanohanke-kaynnistyi-1903681

Kiitos!

lvm.fi

LIIKENNE- JA VIESTINTÄMINISTERIÖ

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

NIS 2-direktiivin täytäntöönpano julkishallinnon toimialalla

EEVA LANTTO, LAINSÄÄDÄNTÖNEUVOS

NIS2-DIREKTIIVIN KANSALLISEN TOIMEENPANON SIDOSRYHMÄTILAISUUS 9.10.2023

NIS 2 HE-luonnoksesta

- Voimaansaattaminen LVM:n esittelyvastuulla olevalla HE:llä, joka sisältää seuraavat lait:
  - ”NIS 2-yleislaki”, eli laki kyberturvallisuuden riskienhallinnasta
  - Laki tiedonhallintalain muuttamisesta
  - Muiden lakien vähäisiä muutoksia: esim. SVPL, sekä muita toimialakohtaisia lakeja, joiden tietoturvasääntely yhteensovitetaan NIS 2-yleislain kanssa (lähinnä poistetaan päällekkäinen NIS 1 sääntely)

Tiedonhallintalain suhde ns. NIS 2 -yleislakiin

- Tiedonhallintalakiin toimijoiden velvoitteet ja niiden noudattamisen valvonta julkishallinnon toimialalla. Muilla toimialoilla direktiivi saatetaan kokonaisuudessaan voimaan lailla kyberturvallisuuden riskienhallinnasta
- Vain NIS 2-yleislaissa seuraavat asiakokonaisuudet
  - kansallinen kyberturvallisuusstrategia sekä laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallintasuunnitelma
  - CSIRT-yksikkö (Liikenne- ja viestintävirastossa) ja sen tehtävät, mm. haavoittuvuuskartoitukset sekä vapaaehtoiset kyberturvallisuustietojen jakamisjärjestelyt
  - Keskitetty yhteyspiste (Liikenne- ja viestintävirastossa) ja sen tiedonvaihto esim. EU:n suuntaan
  - Liikenne- ja viestintäviraston/valvovien viranomaisten tietojen (toimintaa koskevat ilmoitukset, poikkeamailmoitukset sekä muut valvontatehtävässä saadut tiedot) käsittely sekä yhteistyö muiden viranomaisten kanssa ja Euroopan unionin suuntaan sekä tietojen luovuttaminen niille

Tiedonhallintalain NIS 2-sääntelyn soveltaminen julkishallinnon toimijoihin (vähimmäissoveltamisala)

Sovellettaisiin

- valtion virastoihin ja laitoksiin, valtion liikelaitoksiin, itsenäisiin julkisoikeudellisiin laitoksiin sekä hyvinvointialueisiin, hyvinvointiyhtymiin ja Helsingin kaupunkiin niiden hoitaessa laissa hyvinvointialueiden järjestämisvastuulle säädettyjä tehtäviä.
- [CER-direktiivin] nojalla julkishallinnon toimialan kriittisiksi toimijoiksi määriteltyihin toimijoihin

Ei sovellettaisi

- eduskuntaan tai eduskunnan virastoihin
- tuomioistuimiin tai valitusasioita käsittelemään perustettuihin lautakuntiin
- yliopistoihin tai ammattikorkeakouluihin
- kuntiin tai kuntayhtymiin
- Puolustusvoimiin, Puolustuskiinteistöihin, poliisin hallinnosta annetussa laissa (110/1992) tarkoitettuihin poliisiyksikköihin, Rajavartiolaitokseen, Tullin rikostorjuntaan, Syyttäjälaitokseen, Suomen Pankkiin eikä julkisen hallinnon turvallisuusverkkotoiminnasta annetussa laissa (10/2015) tarkoitettuun turvallisuusverkon palvelutuotantoon ja palvelujen käyttöön.
- muihin kuin viranomaisena toimiviin julkista hallintotehtävää hoitaviin
- valvontaa ei sovellettaisi tasavallan presidentin kansliaan, valtioneuvoston oikeuskanslerin toimintaan eikä Kansaneläkelaitokseen.

Toimijoiden velvoitteet

1. Toimintaa koskeva ilmoitus valvovalle viranomaiselle
2. Kyberturvallisuuden riskienhallintavelvoite
   - Velvollisuus hallita riskejä, riskienhallinnan toimintamalli, riskienhallintatoimenpiteiden toteuttaminen ja dokumentointi riskienhallinnan toimintamalliin, johdon vastuu riskienhallinnasta ja sen toteuttamisen valvonnasta
3. Ilmoitusvelvollisuudet poikkeamista ja kyberuhkista
   - Velvollisuus ilmoittaa merkittävistä poikkeamista valvovalle viranomaiselle
   - Velvollisuus ilmoittaa merkittävästä poikkeamasta palvelujen vastaanottajille ja yleisölle sekä ilmoittaa merkittävästä kyberuhkasta sekä kyberuhkan hallitsemiseksi käytettävissä olevista toimenpiteistä niille palvelujen vastaanottajille, joihin merkittävä kyberuhka saattaa vaikuttaa

Valvonta julkishallinnon toimialalla

- Julkishallinnon toimialan valvova viranomainen (toimivaltainen viranomainen) olisi Liikenne- ja viestintävirasto
  - Antaa ohjausta ja neuvontaa
  - Neuvoo tarvittaessa poikkeamien käsittelyssä (yhteistyö CSIRT:n kanssa)
  - Voi velvoittaa toimijan korjaamaan puutteet sääntelyn noudattamisessa.
  - Tiedonsaanti- ja tarkastusoikeus sekä arvioinnin teettämisoikeus tietyin edellytyksin

  - Julkishallintoon ei sovellettaisi yleislain seuraamusmaksua eikä johdon toiminnan rajoittamiseen liittyvää sääntelyä

Valmistelu ja aikataulu

- LVM:n vetämä päätyöryhmä (yleislaki) ja VM:n vetämä alatyöryhmä (tiedonhallintalaki), hankesivut https://valtioneuvosto.fi/hanke?tunnus=LVM044:00/2022
- Lausuntokierros 3.10. – 29.11.2023
- LVM:n sidosryhmätilaisuus ma 9.10. VM esittelee tilaisuudessa oman osuutensa ja vastaa julkishallinnon toimialan kysymyksiin.
- HE tarkoitus antaa eduskunnalle kevättalvella 2024
- Direktiivin noudattamisen edellyttämät säännökset oltava voimassa viimeistään 18.10.2024.
  - Tarkoitus saada käsiteltyä eduskunnassa kevätistuntokaudella, että toimijoilla ja valvovilla viranomaisilla olisi aikaa valmistautua sääntelyn noudattamiseen.

VALTIOVARAINMINISTERIÖ
FINANSMINISTERIET

Kiitos

EEVA LANTTO, LAINSÄÄDÄNTÖNEUVOS
ETUNIMI.SUKUNIMI@GOV.FI
VM.FI | @VMUUTISET

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Liikenne- ja viestintävirasto Traficom NIS2-toimeenpanossa

LVM:n sidosryhmätilaisuus
9.10.2023

Traficomin NIS2-roolit

CSIRT –toimija (Computer Security Incident Response Team)

- Tehtävinä mm. reagoida poikkeamiin ja avustaa tapauksen mukaan asianomaisia keskeisiä ja tärkeitä toimijoita, kerätä ja analysoida forensisia tietoja ja ylläpitää kyberturvallisuuden tilannekuvaa.

Valvova viranomainen

- Liitteen I toimialat
  - Liikenne, Digitaalinen infrastruktuuri, TVT-palvelujen hallinta, Julkishallinto ja Avaruus
- Liitteen II toimialat
  - Posti- ja kuriiripalvelut, Valmistus (Moottoriajoneuvot, perävaunut ja puoliperävaunut sekä muut kulkuneuvot), Digitaalisten palvelujen tarjoajat ja Tutkimustoiminta.

Koordinointi

- Keskitetty yhteyspiste, kansallisen ja kansainvälisen yhteistyön koordinointi, raportointi EU:n suuntaan, laajamittaisten kyberturvallisuuspoikkeamien ja -kriisien hallinnan koordinointi.

Muita tehtäviä

- Seuraamusmaksulautakunnan pj:n ja varapj:n nimeäminen sekä laajamittaisten kyberturvallisuuspoikkeamien ja –kriisien hallintasuunnitelman laatiminen yhteistyössä muiden viranomaisten kanssa.

Kyberturvallisuuskeskuksen palveluja

Hyökkäyspintakartoitus (Hyöky)

- Hyöky on Liikenne- ja viestintävirasto Traficomin Kyberturvallisuuskeskuksen tuottama kansallinen hyökkäyspintakartoitus kyberturvallisuuden parantamiseksi
- Tällä hetkellä ensisijainen kohde ovat kunnat, mutta tarkoituksena on laajentaa tämän jälkeen muillekin toimijoille.

Kybermittari

- Itsearvioinnin ja kehittämisen työkalu ja käytön tukipalvelu kaikille toimijoille
- Mittari tukee myös NIS2-itsearviointien tekemisessä

HAVARO

- HAVARO on Liikenne- ja viestintävirasto Traficomin tuottama palvelu, joka havainnoi suomalaisiin yrityksiin kohdistuvia vakavia tietoturvauhkia ja varoittaa niistä
- Palvelu suunnattu erityisesti kriittisen infrastruktuurin toimijoille

Kyberturvallisuuskeskuksen tilannekuvatuotteet

- Tuotevalikoimamme sisältää runsaasti tuotteita sekä kansalaisille että yrityksille
- Sektorikohtaiset sähköpostilistat toimivat ensisijaisena tiedottamiskanavana yritysten suuntaan

Kaikki palvelut:
https://www.kyberturvallisuuskeskus.fi/fi/palvelumme/tilannekuva-ja-verkostojohtaminen
https://havaro.fi/fi/havaro-etusivu

TRAFICOM
Liikenne- ja viestintävirasto
Kyberturvallisuuskeskus

Kiitos

Kalle Varjola

etunimi.sukunimi(a)traficom.fi

Selvitys NIS2-direktiivin riskienhallintavelvoitteiden taloudellisista vaikutuksista

LVM:n sidosryhmätilaisuus 9.10.2023

Selvityksen tavoitteet

1. NIS2-direktiivin elintarvike- ja valmistussektoriin kuuluvien, Suomeen sijoittautuneiden yritysten **nykyiset kyberturvallisuuskustannukset**

2. NIS2-direktiivin **riskienhallintavelvoitteista aiheutuvat kustannukset** sekä lyhyellä että pitkällä aikavälillä kyseisillä sektoreilla

3. Velvoitteiden noudattamisesta syntyvät **kustannushyödyt** yritysten kybermaturiteetin parantuessa

Selvityksen toteutustapa ja kattavuus

Selvitys toteutettiin **haastattelemalla** elintarvike- ja valmistussektorin yrityksiä sekä kuulemalla yrityksiä **sähköisen kyselylomakkeen** avulla.

20
Osallistunutta yritystä

15
Suuria yrityksiä

5
Keskisuuria yrityksiä

Selvityksen tulokset

Nykyiset kyberturvallisuuskustannukset ja kustannushyödyt

Instan selvityksessä keskimääräisiksi **nykyisiksi kyberturvallisuus-kustannuksiksi valmistussektorin yritykset arvioivat 0,7 %** ja **elintarvikesektorin yritykset 0,3 % liikevaihdosta.** EU-komission arvion mukaan kyberturvallisuuskustannukset ovat keskimäärin 0,5 % liikevaihdosta.

Kustannushyötyjen euromääräinen arviointi koettiin haastavaksi, mutta **yritykset kokivat kybermaturiteetin parantumisen tuovan kuitenkin useita erilaisia liiketaloudellisia hyötyjä.**

Selvityksen tulokset

Riskienhallintavelvoitteista aiheutuvat kustannukset

Selvityksen perusteella **riskienhallintavelvoitteet tulevat aiheuttamaan merkittävinäkin pidettäviä kustannuksia** elintarvike- ja valmistussektoriin kuuluville yrityksille kertaluonteisesti sekä vuosittain jatkuvaluonteisesti.

Selvityksen perusteella elintarvikesektorille aiheutuu valmistussektoria matalammat kustannukset.

Elintarvikesektori

Kertaluonteiset	Jatkuvaluonteiset
274 000 €	148 000 €

Valmistussektori

Kertaluonteiset	Jatkuvaluonteiset
367 000 €	279 000 €

Selvityksen tulokset

Riskienhallintavelvoitteista aiheutuvat kustannukset

Heikoiten täytetään toiminnan jatkuvuuden hallintaan sekä toimitusketjun turvallisuuteen liittyvät velvoitteet.

Parhaiten täytetään henkilöstöturvallisuuteen, pääsynhallintaperiaatteisiin sekä omaisuudenhallintaan liittyvä velvoite.

Eniten kustannuksia aiheutuu poikkeamien käsittelyyn sekä toimitusketjun turvallisuuteen liittyvistä vaatimuksista.

Kiitos!

Jassi Saurio
SENIOR PRIVACY CONSULTANT
jassi.saurio@insta.fi

insta.fi

Kysymykset ja yhteinen keskustelu

FINNISH GOVERNMENT

Tilaisuus on päättynyt
Kiitos!

FINNISH
GOVERNMENT