LIIKENNE- JA VIESTINTÄMINISTERIÖ
KOMMUNIKATIONSMINISTERIET

U 17 / 2026 vp Valtioneuvoston kirjelmä komission ehdotuksista EU:n kyberturvallisuusasetukseksi (CSA2) ja NIS 2 -muutosdirektiiviksi

Liikenne- ja viestintävaliokunta 24.3.2026
Neuvotteleva virkamies Marième Korhonen-Cara, LVM (CSA2)
Hallitussihteeri Veikko Vauhkonen, LVM (NIS2)

Ehdotusten pääasiallinen sisältö (CSA2 ja NIS 2)

- **EU:n kyberturvallisuusasetusehdotus (CSA2)**
- Ehdotus koostuu kolmesta osa-alueesta:

1. EU:n kyberturvallisuusviraston (ENISA) mandaatin uudistaminen
2. Eurooppalainen kyberturvallisuuden sertifiointikehys
3. NIS2-direktiivin toimialojen ICT-toimitusketjujen *ei-teknisten* riskien hallinta

- Tavoitteena on EU:n kyberturvallisuuden kyvykkyyksien ja resilienssin lisääminen sekä sisämarkkinoiden pirstaloitumisen ehkäiseminen. Ehdotus kumoaisi voimassa olevan asetuksen.

- **Komission ehdotus NIS 2 -direktiivin muutoksiksi**
- Annettu samassa yhteydessä CSA2-ehdotuksen kanssa.
- Kohdennettuja muutoksia, joiden tavoitteena on tukea CSA2-ehdotuksen tavoitteita sekä samalla selventää soveltamisalaa, edistää direktiivin yhdenmukaista täytäntöönpanoa, helpottaa vaatimustenmukaisuuden osoittamista ja alentaa sääntelystä toimijoille aiheutuvia kustannuksia.
- Ehdotukset liittyvät pääosin CSA2-ehdotuksiin.

1. Euroopan kyberturvallisuusvirasto ENISA:n mandaatin uudistaminen (CSA2-ehdotus)

- Ehdotuksessa esitetään ENISA:n nykyisten tehtävien täydentämistä mm.
  - **Operatiivisella toiminnalla** kyberuhkien torjunnassa jäsenmaiden ja EU-instituutioiden tukena, ml. antamalla varhaisia varoituksia ja avustamalla kiristyshaittaohjelmahyökkäyksissä
  - Monialaisen **tilannekuvan tuottamisella**
  - **Tietojärjestelmien haavoittuvuuksiin liittyvillä palveluilla**
  - **Kyberosaamiseen** liittyvien sertifikaattien kehittämiseen ja myöntämiseen liittyvillä tehtävillä
- ENISA voisi jatkossa myös kerätä toiminnastaan maksuja (osaamistodistukset, työkalujen käyttö)
- Ehdotus kasvattaisi merkittävästi ENISA:n budjettia ja henkilömäärää:
  - Vuodesta 2031 eteenpäin ENISA:n henkilömäärä kasvaisi n. 131 → **260 htv**
  - ENISA:n budjetti kasvaisi vuoden 2026 tasosta (26 me) yhteensä noin **49 miljoonaan euroon**.
- Jäsenmaiden tulisi nimetä 2 kansallista asiantuntijaa ENISA:n toiminnan tueksi. Tämä nostaisi ENISA:n SNE-asiantuntijoiden määrän 40-60 htv.
  - **Jäsenmaat vastaisivat SNE-asiantuntijoiden palkkakuluista**
- Komissio esittää itselleen myös lisävaltuuksia ENISA:n päätöksentekoelimiin

2. Eurooppalainen kyberturvallisuuden sertifiointikehys (CSA2-ehdotus)

- Asetusehdotuksessa esitetään uudistuksia eurooppalaisen kyberturvallisuuden sertifiointiin koskevaan sääntelyyn. Asetuksella säädettäisiin sertifiointien kehittämisestä ja käytöstä. Asetuksella ei asetettaisi sertifiointivelvollisuuksia. Sertifikaattien hakeminen ja käyttö olisi edelleen vapaaehtoista.
- EU:n laajuisella kyberturvallisuussertifikaatilla voisi osoittaa, että sertifioinnin kohde täyttää soveltuvassa sertifiointijärjestelmässä määritellyt tekniset kyberturvallisuusvaatimukset. Sertifikaatti ja osoitus vaatimustenmukaisuudesta tunnustettaisiin kaikissa jäsenvaltioissa.
- **Keskeisimmät muutokset:**
  - Yhteistyötä ja toiminnan läpinäkyvyyttä lisätään komission, ENISA:n ja jäsenvaltioiden välillä.
  - Organisaatioiden kybertaso (*cyber posture*) ja EU-sääntelyn vaatimustenmukaisuus (*compliance*) sertifioinnin piiriin.
  - Jokaisella sertifiointijärjestelmällä tulee olla ylläpitostrategia ja sen mukaiset ylläpitokeinot.
  - ENISA:n tulee valmistella sertifiointijärjestelmä (skeema) 12 kuukauden kuluessa komission pyynnöstä.

3. NIS2-direktiivin toimialojen ICT-toimitusketjujen ei-teknisten riskien hallinta (CSA2-ehdotus)

- Ehdotuksessa esitetään NIS2-direktiivin toimialoille velvoitteita ICT-toimitusketjujen *ei-teknisten* riskien hallitsemiseksi.
- Tavoitteena on ei-teknisten riskien hallintatoimien yhdenmukaistaminen unionissa, joilla varmistettaisiin sisämarkkinoiden toiminta, edistettäisiin EU:n teknologista suvereniteettia ja vahvistettaisiin EU:n kyberturvallisuuden ja resilienssin tasoa.
- NIS2-direktiivin valvovat viranomaiset valvoisivat CSA2-asetusehdotuksen ICT-toimitusketjujen riskienhallintatoimenpiteiden noudattamista ja voisivat tarvittaessa määrätä toimijoille seuraamusmaksuja, joiden suuruusluokka vaihtelee rikotun velvoitteen mukaan (enintään 1%, 2% tai 7% vuosittaisesta maailmanlaajuisesta liikevaihdosta).

1. Jäsenvaltiot ja komissio arvioisivat yhteisessä riskiarvioinnissa NIS2-toimialan ICT-toimitusketjujen **ei-teknisiä** riskejä.
2. Komissio voisi tämän pohjalta tunnistaa kriittiset ICT-osat sekä kyberturvallisuushuolia aiheuttavat kolmannet maat ja niiden korkean riskin toimittajat.
3. Komissio voisi sitten täytäntöönpanoasetuksella kieltää toimialoja käyttämästä ja asentamasta tällaisten toimittajien ICT-komponentteja. Komissio voisi täytäntöönpanoasetuksilla määritellä siirtymäajat kiellettyjen ICT-komponenttien vaihtamiselle.

Viestintäverkkojen osalta (matkaviestintäverkot, kiinteä verkko, satelliittiverkko) asetusehdotus velvoittaisi suoraan korkean riskin toimittajien ICT-komponenttien vaihtamisen, kun komissio on julkaissut edellä todetun listan korkean riskin toimittajista. *Matka*viestintäverkkojen osalta asetusehdotus määrittelee suoraan 36 kuukauden siirtymäajan kiellettyjen ICT-komponenttien vaihtamiseksi. Siirtymäaika alkaisi korkean riskin toimittajien listauksen julkaisusta.

4. NIS 2 –muutosdirektiivi

- Annettu samassa yhteydessä CSA2-ehdotuksen kanssa. Kohdennettuja muutosehdotuksia, joiden tavoitteena yksinkertaistaa vaatimustenmukaisuutta ja tukea direktiivin täytäntöönpanoa. Lisäksi tavoitteena on sujuvoittaa sääntelyä, keventää yrityksille aiheutuvia kustannuksia ja tukea CSA2-ehdotuksen tavoitteita.
- Soveltamisala:
  - Uusina toimijoina EU:n ID-lompakoiden ja yrityslompakoiden tarjoajat, merenalaisen infrastruktuurin palveluntarjoajat ja kaksikäyttöinfrastruktuuri.
  - Tarkennuksia ja rajauksia toimijatyyppeihin mm. energia- ja terveyssektorilla.
  - Keskeisen toimijan kokorajaa korotettaisiin ”small midcap” –yrityksen tasolle.
- Eurooppalaisen kyberturvallisuussertifioinnin hyödyntäminen vaatimustenmukaisuuden osoittamiseen.’
- Komission riskienhallintatoimia koskevat täytäntöönpanoasetukset olisivat jatkossa täysharmonisoivia.
- ENISA:lle eräitä tehtäviä rajat ylittävien riskien arvioinnista ja valvovien viranomaisten tukemisesta.
- Kiristyshaittaohjelmaan ja -lunnaisiin liittyvien tietojen ilmoittaminen silloin kun se on aiheuttanut merkittävän poikkeaman.
- Kansallisissa kyberturvallisuusstrategioissa on huomioitava kvantinkestävän salauksen (PQC) käyttöönottopolitiikat.
- Muutokset saatettava osaksi kansallista lainsäädäntöä 12 kuukauden kuluessa niiden voimaantulosta.

Keskeiset kannat valtioneuvoston kirjelmästä

- Valtioneuvosto katsoo, että ENISA:n toiminnan tulee olla tehokasta, priorisoitua ja läpinäkyvää. ENISA:n toiminnan ja tehtävien tulisi ensisijaisesti täydentää jäsenmaiden viranomaisten kyberturvallisuustehtäviä.
- Jäsenmaiden tulee itse voida päättää viraston toimielimiin nimitettävistä edustajista sekä virastoon lähetettävistä asiantuntijoista.
- Valtioneuvosto pitää tärkeänä, että tällä asetuksella ei ennakoida tulevan rahoituskehyksen sisältöä. EU:n toimielinten ja virastojen hallintomenojen taso sekä henkilöstömäärä on pidettävä maltillisena.
- Valtioneuvosto tukee yleisesti eurooppalaisen kyberturvallisuuden sertifiointikehyksen uudistamista, tehostamista ja selkeyttämistä.
- Valtioneuvosto pitää kannatettavana, että EU:ssa haetaan yhteisiä ICT-toimitusketjuja koskevia ratkaisuja, jotka vahvistavat näiden turvallisuutta, edistävät sisämarkkinoiden toimintaa ja EU:n teknologista suvereniteettia. Toimenpiteiden tulee olla ennakoitavia ja hallittuja sekä perustua asianmukaiseen kuulemiseen ja vaikutusarviointiin. Valtioneuvosto katsoo, että ehdotuksessa esitettyjen toimenpiteiden tulee olla myös oikeasuhtaisia ja riskiperustaisia.
- Valtioneuvosto suhtautuu myönteisesti NIS 2 -direktiivin muutosehdotuksiin, jotka yksinkertaistavat sääntelyä, alentavat kustannuksia ja turvaavat kyberturvallisuuden korkeaa tasoa. Valtioneuvosto suhtautuu myönteisesti soveltamisalaa ja kyberturvallisuussertifiointien hyödyntämistä koskeviin ehdotuksiin.
- Valtioneuvosto pitää tärkeänä, että NIS 2 -vaatimukset ovat oikeasuhtaisia ja riskiperusteisia. Valtioneuvosto suhtautuu alustavan varauksellisesti ehdotukseen komission täysharmonisoivista täytäntöönpanosäädöksistä riskienhallinnassa.

LIIKENNE- JA VIESTINTÄMINISTERIÖ
KOMMUNIKATIONSMINISTERIET

Kiitos!

Ylitarkastaja Eevi Vuorinen, LVM (vastuuvalmisteljia), eevi.vuorinen@gov.fi, p. 0295 342 080
Neuvotteleva virkamies Emma Hokkanen, LVM (CSA2), emma.hokkanen@gov.fi, p. 0295 342 106
Neuvotteleva virkamies Marième Korhonen-Cara, LVM (CSA2), marieme.korhonen-cara@gov.fi, p. 0295 342 134
Hallitussihteeri Veikko Vauhkonen, LVM (NIS2), veikko.vauhkonen@gov.fi, p. 0295 342 168