

Valtioneuvoston kirjelmä kybersolidaarisuus-säädöksestä ja muutoksista kyberturvallisuusasetukseen, U 20/2023 vp

Hallintovaliokunta
5.10.2023

Erityisasiantuntija Emma Hokkanen
Turvallisuusyksikkö
Liikenne- ja viestintäministeriö

LIIKENNE- JA VIESTINTÄMINISTERIÖ

U-kirjelmän valmistelu

- **Komissio antoi 18.4. uuden kyberpaketin, joka sisälsi:**
  - Ehdotuksen kybersolidaarisuussäädökseksi
  - Ehdotuksen muutoksista kyberturvallisuusasetukseen
  - Tiedonannon Cybersecurity Skills Academysta (OKM)

- U-kirjelmä on käsitelty viestintäjaostossa (EU-19) ja hybridiuhat ja kriisivarautuminen-jaostossa (EU-13)
- Ehdotuksesta järjestettiin kuulemistilaisuudet viranomaisille ja yksityiselle sektorille
- Neuvotteluiden odotetaan käynnistyvän Espanjan kuluvalla puheenjohtajakaudella. Espanjan tavoitteena on yleisnäkemys puheenjohtajakautensa loppuun mennessä.



Ehdotuksen tausta ja tavoitteet

- Ehdotuksen taustalla on muuttunut kybertoimintaympäristö ja lisääntyneet kyberuhat unionin alueella. Kyberhäiriötilanteiden uhka kriittisille infrastruktuureille vaatii parempaa varautumista ja yhteistyötä kaikilla EU:n kyberturvallisuusekosysteemin tasoilla.
- Ehdotuksen yleisenä tavoitteena on vahvistaa EU:n yhteistä kyberhäiriöiden havainnointia, tilannekuvaa sekä kyvykkyyttä vastata kyberhäiriöihin.
- Toisena tavoitteena on vahvistaa kriittisten toimijoiden valmiuksia koko EU:ssa, vahvistaa solidaarisuutta kehittämällä yhteisiä toimintavalmiuksia merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien varalle, mukaan lukien tarjoamalla kyberhäiriötilanteiden hallintaan liittyvää tukea kolmansille maille.
- Tavoitteena on myös edistää Euroopan teknologista riippumattomuutta kyberturvallisuuden alalla



Kybersolidaarisuussäädös

- Ehdotuksessa esitetään:
  - yleiseurooppalaisen turvaoperaatiokeskusten (Security Operations Center, SOC) infrastruktuurin **(Kybersuojakilpi, European Cyber Shield)** käyttöönottoa yhteisten havainnointi- ja tilannekuvavalmiuksien rakentamiseksi ja tehostamiseksi.
  - **Kyberhätätilanteiden mekanismin** ja luotettavista yksityisen sektorin palveluntarjoajista koostuvan **kyberturvallisuusreservin perustamista** jäsenvaltioiden tukemiseksi merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa, niihin vastaamisessa ja niistä välittömästi toipumisessa.
  - **kyberturvallisuuspoikkeamien arviointimekanismin** perustamista tiettyjen merkittävien tai laajamittaisten poikkeamien tarkastelua ja arviointia varten.
- Kybersuojakilpeä, kyberhätätilanteiden mekanismia sekä kyberturvallisuusreserviä esitetään tuettavaksi Digitaalinen Eurooppa-rahoituksesta, johon esitetään myös muutoksia



Ehdotuksen keskeinen sisältö (1)

I Yleiset säännökset	• Ehdotuksen sisältö, ehdotuksen tavoitteet • Määritelmät
II Eurooppalainen kybersuojakilpi	• Kansalliset SOCit • Rajat-ylittävät SOCit • SOCien välinen tiedonvaihto ja yhteistyö • Tiedonjako unionin toimijoille • SOCien turvallisuus
III Kyberhätätilanteiden mekanismi	• Tuettavat toiminnot reservistä • Koordinoidut varautumistestaukset • Reservin perustaminen ja reserville esitettävät tukipyynnöt • Koordinaatio kriisinhallintamekanismien kanssa • Luotettavat palveluntarjoajat, tuki kolmansille maille

Ehdotuksen keskeinen sisältö (2)

IV Kyberhäiriöiden arviointimekanismi	• Arviointimekanismin toiminta, ENISAn tehtävät
V Loppusäännökset	• Muutokset DEP-sääntelyyn, DEP-hankkeen 3. tavoitteen osalta lisätään kaksi uutta alatavoitetta: EU cyber shield:in kehittäminen ja cyber emergency mechanism:in perustaminen • Ohjelmassa osoitettujen budjettien leikkaukset • Cyber shield ja cyber emergency –mekanismit sovitetaan osaksi Digitaalinen Eurooppa –hanketta
Kyberturvallisuusasetuksen muuttaminen	• Lukuisia muutoksia, siten että tietoturvapalvelujen tarjoajat tulisi mukaan asetuksen soveltamisalaan. Tietoturvapalveluidentarjoajille luotaisiin vaatimuksia mm. palveluiden laadulle

Ehdotuksen vaikutukset

- Kyberhäiriöiden parempi havainnointi unionissa voi vähentää kyberhäiriöistä aiheutuvia haittoja ja kustannuksia. Varautumistestaukset kriittisille toimialoille voivat parantaa kyberturvallisuutta, kun yritysten kybersuojauksista voidaan tunnistaa puutteita ennakollisesti. Nopea reagointi kyberhäiriöihin parantaa koko unionin kyberturvallisuutta ja ehkäisee häiriöiden leviämistä.
- Rajojen yli toimivaan turvaoperaatiokeskusten yhteenliittymään osallistuminen voisi mahdollisesti tuoda Suomelle hankintoihin liittyviä säästöjä ja parantaa tehokkuutta pidemmällä aikavälillä.
- Ehdotus voi aiheuttaa joitain kansallisia lainsäädäntömuutoksia sekä tarpeen nimetä kansallinen turvaoperaatiokeskus sekä kansallisen CSIRT-toimijan toimimista kyberreservin palveluiden yhteyspisteenä.
- Komissio ei tehnyt ehdotuksesta vaikutustenarviota, jonka vuoksi ehdotusten kaikkien vaikutusten arviointi on haastavaa. Komission mukaan Digitaalinen Eurooppa-ohjelmaan tehty vaikutustenarviointi soveltui myös tähän ehdotukseen.
- Kyberturvallisuusasetukseen ehdotetut muutokset voisivat yhdenmukaistaa tietoturva-alan laatu- ja turvallisuusvaatimuksia ja parantaa eurooppalaisten tietoturva-alan yritysten kilpailukykyä. Sertifiointikehys voisi kuitenkin lisätä pk-yritysten hallinnollista ja taloudellista taakkaa ja heikentää niiden liiketoimintamahdollisuuksia.



Keskeiset näkemykset valtioneuvoston kannasta

- Ehdotuksen tavoitetta kannatetaan. Suomen edun mukaista on vahvistaa kyberturvallisuutta myös EU:n yhteisillä toimilla. EU:n kriisinkestävyyden kokonaisvaltaista kehittäminen on keskeisenä.
- Ehdotuksen yhteyttä teollisuuteen ja lainsäädännön lähentämiseen tulisi tarkentaa. Ehdotuksen suhdetta kansalliseen turvallisuuteen pitää arvioida tarkemmin. Tiedonvaihtoon, jolla voisi olla negatiivisia vaikutuksia kansalliseen turvallisuuteen, suhtaudutaan varauksellisesti. Turvaoperaatiokeskuksen nimeämisessä ei tulisi rajoittaa jäsenvaltioiden hallinnollista autonomiaa.
- Uusien mekanismien luomisessa tulee välttää päällekkäisyyksiä ja varoa olemassa olevien toimivien ratkaisujen muuttamista.
- Kyberhätätilanteiden mekanismin osalta erityisesti ennakolliset varautumistestaukset ovat kannatettavia.
- Tulee myös varmistaa, ettei rahoitusinstrumenttien avulla luoda sellaisia kannustimia, jotka heikentävät jäsenmaiden omien kyberturvallisuuskyvykkyyksien kehittämistä
- Suomalaisten tietoturva-alan toimijoiden markkina-asemasta tulee huolehtia
- Euroopan kyberturvallisuusvirasto ENISAn resursoinnista tulee huolehtia eikä ENISAlle kuuluvia tehtäviä kuulu ensisijaisesti luovuttaa komissiolle
- DEP-ohjelman rahoitukseen kohdistuvia muutoksia tulee analysoida tarkemmin. Varainhoitoasetuksen vuotoisuusperiaatteesta luopumiseen suhtaudutaan varauksellisesti.





Kiitos!

lvm.fi Twitter: @lvmfi

LIIKENNE- JA VIESTINTÄMINISTERIÖ