Euroopan unionin
neuvosto

Bryssel, 21. kesäkuuta 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

YHTEENVETO ASIAN KÄSITTELYSTÄ

Lähettäjä:	Neuvoston pääsihteeristö
Päivämäärä:	21. kesäkuuta 2022
Vastaanottaja:	Valtuuskunnat
Ed. asiak. nro:	9716/22
Asia:	Neuvoston päätelmät Euroopan tilintarkastustuomioistuimen erityiskertomuksesta nro 5/2022 "EU:n toimielinten, elinten ja virastojen kyberturvallisuus: valmiustaso ei ole yleisesti ottaen oikeassa suhteessa uhkiin" – Neuvoston istunnossaan 21. kesäkuuta 2022 hyväksymät neuvoston päätelmät

Valtuuskunnille toimitetaan oheisena edellä mainitut, neuvoston istunnossaan 21. kesäkuuta 2022 hyväksymät neuvoston päätelmät.

NEUVOSTON PÄÄTELMÄT

Euroopan tilintarkastustuomioistuimen erityiskertomuksesta nro 5/2022 "EU:n toimielinten, elinten ja virastojen kyberturvallisuus: valmiustaso ei ole yleisesti ottaen oikeassa suhteessa uhkiin"

EUROOPAN UNIONIN NEUVOSTO, joka

PALAUTTAA MIELEEN antamansa päätelmät tilintarkastustuomioistuimen laatimien erityiskertomusten tarkastelun parantamisesta vastuuvapauden myöntämisen yhteydessä[1],

1. PANEE MERKILLE Euroopan tilintarkastustuomioistuimen erityiskertomuksen nro 5/2022 "EU:n toimielinten, elinten ja virastojen kyberturvallisuus: valmiustaso ei ole yleisesti ottaen oikeassa suhteessa uhkiin"[2].

2. KOROSTAA, että on tärkeää ja kiireellistä vahvistaa kyberturvallisuuden tasoa EU:n toimielimissä, elimissä ja virastoissa, kun otetaan huomioon digitalisaatiovauhdin viimeaikainen kiihtyminen toimielimissä, niiden käsittelemät arkaluonteiset tiedot, EU:n toimielimiin, elimiin ja virastoihin kohdistuvien hyökkäysten määrän kasvu ja vakavuus sekä niihin kohdistuvan uhkan taso.

3. MUISTUTTAA Eurooppa-neuvoston 20. kesäkuuta 2019 antamista päätelmistä[3], joissa Eurooppa-neuvosto kehotti EU:n toimielimiä yhdessä jäsenvaltioiden kanssa kehittämään toimenpiteitä, joilla voidaan parantaa EU:n sietokykyä ja turvallisuuskulttuuria EU:n ulkopuolelta tulevia kyber- ja hybridiuhkia vastaan, sekä suojaamaan paremmin EU:n tieto- ja viestintäverkkoja ja sen päätöksentekoprosessia kaikenlaisilta haitallisilta toimilta.

---

1 7515/00 + COR 1.
2 8040/22.
3 EUCO 9/19.

4. MUISTUTTAA neuvoston 10. joulukuuta 2019 antamista päätelmistä, jotka koskevat täydentäviä pyrkimyksiä parantaa selviytymiskykyä ja torjua hybridiuhkia[4] ja joissa neuvosto kehotti EU:n toimielimiä, elimiä ja virastoja varmistamaan jäsenvaltioiden tuella unionin valmiudet suojella koskemattomuuttaan ja parantaa EU:n tieto- ja viestintäverkkojen ja päätöksentekoprosessien turvallisuutta torjumalla kaikenlaista haitallista toimintaa kattavan uhka-arvion pohjalta. Päätelmissä todettiin, että tätä varten toimielinten, elinten ja virastojen olisi jäsenvaltioiden tukemana kehitettävä ja pantava täytäntöön kattava toimenpidekokonaisuus turvallisuutensa varmistamiseksi kesäkuussa 2019 kokoontuneen Eurooppa-neuvoston toimeksiannon mukaisesti[5].

5. MUISTUTTAA 22. maaliskuuta 2021 EU:n kyberturvallisuusstrategiasta digitaaliselle vuosikymmenelle antamistaan päätelmistä[6], joissa se korosti, että kyberturvallisuus on elintärkeää julkishallinnon ja instituutioiden toiminnalle niin kansallisella kuin EU:n tasolla sekä yhteiskunnallemme ja taloudellemme kokonaisuudessaan.

6. MUISTUTTAA 23. toukokuuta 2022 Euroopan unionin kybertoimien kehittämisestä antamistaan päätelmistä[7], joissa EU:n toimielimiä, elimiä ja virastoja kannustettiin osallistumaan kyberalan suojatun viestinnän nykyisiä välineitä koskevaan kartoitukseen, josta keskustellaan asiaankuuluvissa neuvoston elimissä ja asiaankuuluvien yhteistyöryhmien, kuten CSIRT-yksiköiden verkoston ja EU-CyCLONen, kanssa.

7. KOROSTAA tarvetta puuttua järjestelmäriskiin, joka liittyy EU:n toimielinten, elinten ja virastojen välisiin sekä niiden ja jäsenvaltioiden instituutioiden välisiin yhteyksiin näiden tahojen institutionaalisesta ja hallinnollisesta riippumattomuudesta huolimatta.

---

4 14972/19.
5 EUCO 9/19.
6 6722/21.
7 9364/22.

8. PANEE MERKILLE erityiskertomuksen havainnot siitä, että EU:n toimielimet, elimet ja virastot eivät ole saavuttaneet uhkia vastaavaa kybervalmiustasoa ja niiden kyberturvallisuuden kehittyneisyyden taso on erilainen. TOTEAA, että EU:n toimielinten, elinten ja virastojen kyberturvallisuuden valmiustasoa olisi nostettava ja niiden välistä synergiaa parannettava.

9. KANNUSTAA sen vuoksi voimakkaasti EU:n toimielimiä, elimiä ja virastoja jatkamaan valmiustasonsa nostamiseksi sellaisten kyberriskien hallintatoimenpiteiden toteuttamista, joilla varmistetaan uhkia vastaava kyberturvallisuuden taso, kuten todetaan toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta esitetyssä direktiiviehdotuksessa.

10. KEHOTTAA EU:n toimielimiä, elimiä ja virastoja tehostamaan toimiaan kyberuhkilta suojautumiseksi ja yhteistyötään johdonmukaisten standardien ja eritelmien laatimiseksi erityisesti kyberturvallisuuteen liittyviä julkisia hankintoja, hankkeita ja palveluja varten sekä parantamaan tietoteknisten järjestelmiensä yhteentoimivuutta muun muassa turvallisuusluokittelemattoman sisällön turvallisen välityksen varmistamiseksi.

11. KEHOTTAA Euroopan unionin kyberturvallisuusvirastoa (ENISA) ja EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmää (CERT-EU) tehostamaan toimivaltuuksiensa puitteissa yhteistyötään EU:n toimielinten, elinten ja virastojen tukemiseksi niiden kyberturvallisuuspyrkimyksissä, erityisesti niiden EU:n toimielinten, elinten ja virastojen valmiuksien kehittämisessä, joiden kyberturvallisuuden kehittyneisyyden taso on heikompi.

12. PANEE MERKILLE erityiskertomuksen päätelmät ja suositukset ja TOTEAA, että EU:n toimielinten, elinten ja virastojen kyberturvallisuuden valmiustasoa olisi nostettava ja niiden välistä synergiaa parannettava huomattavasti. EU:n toimielimillä, elimillä ja virastoilla olisi oltava kattava kyberturvallisuutta koskeva riskinhallintajärjestelmä, niiden olisi suoritettava säännöllisiä riskinarviointeja ja tarkastuksia, jotka perustuvat yhteisiin tai hyvin tunnettuihin menetelmiin ja kansainvälisiin standardeihin, ja niiden olisi järjestelmällisesti lisättävä henkilöstönsä kyberturvallisuustietoisuutta ja toteutettava koulutusohjelmia.

13. KOROSTAA myös, että EU:n toimielinten, elinten ja virastojen olisi osoitettava riittävästi määrärahoja kyberuhkilta suojautumistoimenpiteiden toteutuksen varmistamiseksi monivuotista rahoituskehystä noudattaen, ja PANEE MERKILLE erityiskertomuksen suosituksen, jonka mukaan olisi nimitettävä kaikkia EU:n toimielimiä, elimiä ja virastoja edustava toimija, jolle olisi annettava riittävät toimivaltuudet ja välineet valvoa yhteisten kyberturvallisuussääntöjen noudattamista.

14. TOTEAA, että CERT-EU:lle olisi ilmoitettava viipymättä merkittävistä kyberturvallisuuspoikkeamista EU:n toimielimissä, elimissä ja virastoissa ja että sillä olisi tätä varten oltava riittävät resurssit, jotka ovat ennakoitavissa ja mukautettuja nykyiseen uhkatasoon ja EU:n toimielinten, elinten ja virastojen tarpeisiin erityisesti henkilöstön, teknisten laitteiden ja infrastruktuurin osalta.

15. TOTEAA, että kyberturvallisuutta koskevaa yhteistyötä ja tietojenvaihtoa sekä EU:n toimielinten, elinten ja virastojen välisten suojattujen viestintäkanavien yhteentoimivuutta olisi vahvistettava ja järjestelmällistettävä. KEHOTTAA ottamaan tällaiseen yhteistyöhön ja tietojenvaihtoon mukaan myös jäsenvaltioiden kyberturvallisuudesta vastaavat viranomaiset.

16. PANEE MERKILLE erityiskertomukseen liitetyt komission, CERT-EU:n ja ENISAn vastaukset.

17. PYYTÄÄ komissiota ottamaan huomioon erityiskertomuksen suositukset ja toimimaan tavoitteellisesti suunnitellessaan EU:n toimielinten, elinten ja virastojen kyberturvallisuuspolitiikkoja ja edistämään niiden välisen synergian lisäämistä.