EUROOPAN TILINTARKASTUS-TUOMIOISTUIN

FI

Lausunto 02/2023

(annettu Euroopan unionin toiminnasta tehdyn sopimuksen 322 artiklan 1 kohdan nojalla)

ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten

[toimielinten välinen asiakirja 2023/0109(COD), 18. huhtikuuta 2023]

Sisällys

	Kohta
Johdanto	01–03
Yleiset huomautukset	04–05
Erityiset huomautukset	06–40
Vaikutustenarviointi puuttuu	06–08
Rahoituksesta annettavat tiedot ovat osittaisia	09–12
Rahoituksesta ja henkilöstötarpeista annettavat tiedot ovat osittaisia	09–10
Kyberturvallisuuden eurooppalaista suojakilpeä koskevasta rahoitusjärjestelystä annetaan osittaista tietoa	11–12
Kyberturvallisuuden eurooppalaiseen suojakilpeen liittyvät riskit	13–26
Toimien monimutkaistuminen ja kerrosten lisääntyminen	13–20
Tietojenvaihto	21–26
Kyberhätätilanteiden mekanismiin liittyvät riskit	27–34
EU:n kyberturvallisuusreservin käyttöönotto	27–29
Poikkeaminen talousarvion vuotuisperiaatteesta	30–34
Kyberturvallisuuspoikkeamien jälkitarkastelumekanismiin liittyvät riskit	35–36
Tuloksellisuuden seuranta ja toimintapolitiikan arviointi	37–40
Loppuhuomautukset	41–43
Liite – Euroopan kyberturvallisuusgalaksi	

Johdanto

01 Komissio julkaisi 18. huhtikuuta 2023 ehdotuksen Euroopan parlamentin ja neuvoston asetukseksi toimenpiteistä solidaarisuuden ja valmiuksien vahvistamiseksi unionissa kyberturvallisuusuhkien ja -poikkeamien havaitsemista sekä niihin varautumista ja reagoimista varten (EU:n kybersolidaarisuussäädös).

02 Ehdotetussa EU:n kybersolidaarisuussäädöksessä säädetään toimenpiteistä kyberturvallisuusuhkien ja -poikkeamien havaitsemiseksi, niihin varautumiseksi ja niihin reagoimiseksi erityisesti seuraavin keinoin:

- **kyberturvallisuuden eurooppalainen suojakilpi**, jotta voidaan kehittää ja tehostaa koordinoituja havaitsemis- ja tilannetietoisuusvalmiuksia
- **kyberhätätilanteiden mekanismi**, jolla tuetaan jäsenvaltioita merkittäviin ja laajamittaisiin kyberturvallisuuspoikkeamiin varautumisessa ja reagoimisessa sekä palautumisessa niiden jälkeen
- **kyberturvallisuuspoikkeamien jälkitarkastelumekanismi**, jonka avulla voidaan tarkastella ja arvioida merkittäviä tai laajamittaisia poikkeamia.

03 Komission ehdotuksen oikeusperustan mukaan Euroopan tilintarkastustuomioistuimen kuuleminen on pakollista[1]. Euroopan parlamentti pyysi tilintarkastustuomioistuimelta kannanottoa 2. kesäkuuta 2023 ja neuvosto 7. kesäkuuta 2023. Kuulemisvaatimus täytetään tällä lausunnolla.

[1] Sopimus Euroopan unionin toiminnasta, 322 artiklan 1 kohta.

Yleiset huomautukset

04 EU:n jäsenvaltiot ovat päävastuussa siitä, että niiden alueella tapahtuvia kyberturvallisuuspoikkeamia ja -kriisejä ehkäistään ja niihin varaudutaan ja reagoidaan. Euroopan unionista tehdyn sopimuksen 4 artiklan 2 kohdan mukaisesti kansallinen turvallisuus on edelleen yksinomaan kunkin jäsenvaltion vastuulla. Merkittävien tai laajamittaisten kyberturvallisuuspoikkeamien mahdollinen vaikutus merkitsee kuitenkin sitä, että nämä EU:n tason yhteiset toimet saattavat olla tarpeen.

05 Tilintarkastustuomioistuin suhtautuu myönteisesti ehdotuksen tavoitteisiin vahvistaa EU:n kollektiivista kyberuhkien sietokykyä. Käsillä olevassa lausunnossa tilintarkastustuomioistuin esittää erityisiä huomautuksia ehdotetun EU:n kybersolidaarisuussäädöksen kolmesta osa-alueesta ja tuo esiin joitakin havaitsemiaan riskejä, jotka liittyvät vaikutustenarvioinnin puuttumiseen, taloudellisiin näkökohtiin ja siihen, miten ehdotuksessa esitetyt toimenpiteet voitaisiin panna täytäntöön. Tilintarkastustuomioistuin korostaa erityisesti, että ehdotettu asetus saattaa tehdä koko EU:n kyberturvallisuusgalaksista monimutkaisemman, ja ehdottaa keinoja tämän riskin lieventämiseksi (ks. kohdat ***13***–***20***).

Erityiset huomautukset

Vaikutustenarviointi puuttuu

06 Komission paremman sääntelyn suuntaviivoissa ehdotetaan vaikutustenarviointien ja sidosryhmien kuulemisen käyttöä osana toimintapolitiikkojen suunnittelu- ja täytäntöönpanovaihtoehtojen kattavaa analyysia. Tilintarkastustuomioistuin pitää kattavia vaikutustenarviointeja olennaisena välineenä pyrittäessä arvioimaan, ovatko EU:n toimet tarpeen. Niiden avulla voidaan myös analysoida käytettävissä olevien ratkaisujen mahdollisia vaikutuksia ennen ehdotusten hyväksymistä.

07 Tästä asetusehdotuksesta ei tehty vaikutustenarviointia. Komissio selitti perustelujen 3 kohdassa, että se oli päättänyt olla tekemättä tällaista arviointia ”*ehdotuksen kiireellisyyden*” vuoksi. Se totesi myös, että ehdotetulla asetuksella käyttöön otettuja toimenpiteitä tuetaan Digitaalinen Eurooppa -ohjelmasta ja että toimenpiteet ovat Digitaalinen Eurooppa -ohjelmasta annetun asetuksen mukaisia. Sen osalta oli tehty erityinen vaikutustenarviointi vuonna 2018. Komissio selitti lisäksi, että ehdotetut toimenpiteet perustuivat aiempiin toimiin, jotka oli valmisteltu tiiviissä yhteistyössä tärkeimpien sidosryhmien ja jäsenvaltioiden kanssa; toimenpide-ehdotuksissa oli otettu huomioon saadut kokemukset.

08 Tilintarkastustuomioistuin panee kuitenkin merkille, että Digitaalinen Eurooppa -ohjelman vaikutustenarviointi ei kata asetusehdotukseen sisältyviä uusia toimenpiteitä. Käytettävissä olevista toimintavaihtoehdoista ja ehdotukseen liittyvistä kustannuksista on näin ollen vain vähän tietoa.

Rahoituksesta annettavat tiedot ovat osittaisia

Rahoituksesta ja henkilöstötarpeista annettavat tiedot ovat osittaisia

09 EU:n kybersolidaarisuussäädöksessä säädettyjen toimenpiteiden rahoitus saadaan Digitaalinen Eurooppa -ohjelmasta. Komissio totesi perustelujensa 4 kohdassa, että kyberturvallisuuden eurooppalaiselle suojakilvelle oli jo myönnetty 115 miljoonaa euroa pilottihankkeiden muodossa vuosina 2021–2022. Se totesi myös, että ehdotuksella lisättäisiin Digitaalinen Eurooppa -ohjelman kyberturvallisuutta ja luottamusta koskevaan erityistavoitteeseen vuosina 2025–2027 osoitettavia

743 miljoonan euron määrärahoja 100 miljoonalla eurolla. Tämä tapahtuisi kohdentamalla rahoitusta sisäisesti uudelleen.

10 Uudelleenkohdentamisen jälkeen kyberturvallisuuteen käytettävissä oleva EU:n rahoitus on 843 miljoonaa euroa vuosina 2023–2027. Tilintarkastustuomioistuin panee merkille, että tämä määrä ei kata ainoastaan ehdotetussa asetuksessa säädettyjä toimia, vaan myös muita Digitaalinen Eurooppa -ohjelman kyberturvallisuustoimia (kuten teollisuuden tai standardoinnin tukemisen). Ehdotuksessa ei esitetä arviota ehdotettujen toimenpiteiden perustamiseen ja täytäntöönpanoon liittyvistä odotetuista kokonaiskustannuksista. Ehdotettuja toimenpiteitä ovat kyberturvallisuuden eurooppalainen suojakilpi, kyberhätätilanteiden mekanismi (mukaan lukien EU:n kyberturvallisuusreservi ja kyberturvallisuuspoikkeamien jälkitarkastelumekanismi. Koska ehdotukseen ei liity vaikutustenarviointia, tilintarkastustuomioistuin ehdottaa, että komissio asettaa nämä kustannusarviot saataville läpinäkyvyyden lisäämiseksi.

Kyberturvallisuuden eurooppalaista suojakilpeä koskevasta rahoitusjärjestelystä annetaan osittaista tietoa

11 Asetusehdotuksen II luvussa perustetaan ns. kyberturvallisuuden eurooppalainen suojakilpi, joka koostuu kansallisista ja rajojen yli toimivista turvaoperaatiokeskuksista. Asetusehdotuksessa säädetään, että tukikelpoiset kansalliset turvaoperaatiokeskukset voivat saada EU:n rahoitustukea, joka kattaa enintään 50 prosenttia keskusten välineistön ja infrastruktuurien hankintakustannuksista ja enintään 50 prosenttia keskusten toimintakustannuksista. Rajojen yli toimivien turvaoperaatiokeskusten kohdalla EU:n osarahoitus kattaa enintään 75 prosenttia välineistön ja infrastruktuurien hankintakustannuksista ja enintään 50 prosenttia toimintakustannuksista. Asetusehdotuksessa ei täsmennetä, miksi rajojen yli toimivissa turvaoperaatiokeskuksissa tarvitaan enemmän ja suuremmalla osarahoitusosuudella tuettua välineistöä ja infrastruktuureja kuin yhteenliittyminä toimivilla kansallisilla turvaoperaatiokeskuksilla on käytettävissään.

12 Asetusehdotuksessa ei myöskään tarkenneta, kuinka kauan EU osarahoittaa kansallisten ja rajojen yli toimivien turvaoperaatiokeskusten toimintakustannuksia. Tämä aiheuttaa riskin, että kyberturvallisuuden eurooppalaisen suojakilven toiminta ja kestävyys ovat jatkossa riippuvaisia EU:n rahoituksesta.

Kyberturvallisuuden eurooppalaiseen suojakilpeen liittyvät riskit

Toimien monimutkaistuminen ja kerrosten lisääntyminen

13 Tilintarkastustuomioistuin totesi katsauksessaan 02/2019[2], että EU:n kyberturvallisuusympäristö on monimutkainen ja -kerroksinen. Mukana on lukuisia yksityisiä ja julkisia siviilialan toimijoita alueellisella, kansallisella ja EU:n tasolla. Toimijoihin lukeutuvat esimerkiksi lainvalvontaviranomaiset ja rahanpesun selvittelykeskukset. Kyberturvallisuus on myös keskeinen osa kansallista turvallisuutta ja puolustusta. Käsillä olevan lausunnon ***liitteessä*** esitetään kartta EU:n uudesta kyberturvallisuusgalaksista. Kartassa on laatikko, johon on merkitty eri sävyillä kaikki ehdotuksessa esitetyt mekanismit ja komponentit. Kartta kuvastaa asetuksella käyttöön otettavan järjestelmän monimutkaisuutta ja -kerroksisuutta.

14 Asetusehdotuksen II luvussa perustettavan kyberturvallisuuden eurooppalaisen suojakilven tavoitteena on kehittää EU:lle edistykselliset valmiudet havaita, analysoida ja käsitellä kyberuhkia ja -poikkeamia koskevaa dataa. Siitä muodostuu yhteenliitetty yleiseurooppalainen infrastruktuuri kansallisille ja rajojen yli toimiville turvaoperaatiokeskuksille.

15 Voidakseen osallistua kyberturvallisuuden eurooppalaisen suojakilven toimintaan jäsenvaltion on nimettävä vähintään yksi kansallinen turvaoperaatiokeskus, jonka on oltava julkinen elin. Kansallisten turvaoperaatiokeskusten olisi puolestaan perustettava rajojen yli toimivia turvaoperaatiokeskuksia, jotka ovat vähintään kolmen jäsenvaltion turvaoperaatiokeskusten muodostamia yhteenliittymiä. Yhteenliittymät ovat sitoutuneet tekemään yhteistyötä ja koordinoimaan kyberturvallisuuspoikkeamien havaitsemista ja kyberuhkien seurantaa koskevia toimiaan.

16 EU on viime vuosina vahvistanut kyberturvallisuuden sääntelykehystään. Yksi sen keskeisistä välineistä ovat vuonna 2016 annettu verkko- ja tietoturvadirektiivi (NIS-direktiivi) ja siihen vuonna 2022 tehty tarkistus (ns. NIS 2 -direktiivi). NIS 2 -direktiivin nojalla jäsenvaltioiden on perustettava yksi tai useampi kansallisella tasolla toimiva tietoturvaloukkauksiin reagoiva ja niitä tutkiva yksikkö (CSIRT). EU:n tasolla NIS 2 -direktiivillä perustetaan myös verkko- ja tietoturva-alan yhteistyöryhmä, CSIRT-yksiköiden verkosto ja Euroopan kyberkriisien yhteysorganisaatioiden verkosto (EU-CyCLONe).

---

[2] Katsaus 2/2019,*EU:n kyberturvallisuuspolitiikan vaikuttavuuteen liittyvät haasteet*.

17 EU perusti vuonna 2021 Euroopan kyberturvallisuuden tutkimus- ja osaamiskeskuksen. Tätä toukokuussa 2023 avattua keskusta tukee 27 kansallisen koordinointikeskuksen verkosto, johon kuuluu yksi keskus kustakin jäsenvaltiosta. Näistä keskuksista osa on myös kansallisia turvaoperaatiokeskuksia. Keskus vastaa Digitaalinen Eurooppa -ohjelman kyberturvallisuuskomponentin täytäntöönpanosta, lukuun ottamatta EU:n kyberturvallisuusreserviä. Komissio vastaa reservin täytäntöönpanosta, mutta ENISAlle voidaan antaa vastuu sen toiminnasta ja hallinnosta.

18 Komissio on myös perustanut yhteisen kyberturvallisuusyksikön. Tästä yksiköstä ilmoitettiin vuonna 2020 EU:n kyberturvallisuusstrategiassa, ja se määriteltiin tarkemmin komission suosituksessa vuonna 2021.

19 Komissio ilmoitti huhtikuussa 2023 kyberturvallisuusakatemian käynnistämisestä. Kyseessä on uusi aloite, jolla pyritään kuromaan umpeen kyberturvallisuuteen liittyvä osaamisvaje ja lisäämään EU:n kyberalan työvoimaa.

20 Tätä taustaa vasten tilintarkastustuomioistuin katsoo, että ehdotettu asetus saattaa tehdä koko EU:n kyberturvallisuusgalaksista monimutkaisemman. Nykyisen CSIRT-yksiköiden verkoston ja turvaoperaatiokeskusten välillä voi olla päällekkäisyyksiä. Komissio totesi perustelujensa 1 kohdassa, että rajojen yli toimivien turvaoperaatiokeskusten foorumien on tarkoitus luoda uusi valmius, joka täydentää CSIRT-yksiköiden verkostoa. Tilintarkastustuomioistuin panee kuitenkin merkille, että jotkin kansallisten turvaoperaatiokeskusten, rajojen yli toimivien turvaoperaatiokeskusten, CSIRT-yksiköiden ja CSIRT-yksiköiden verkoston tehtävistä ja tavoitteista ovat samankaltaisia. Tällaisia ovat esimerkiksi uhkien havaitseminen ja niiden torjuminen, uhkatiedustelutieto ja tilannetietoisuus. Periaatteessa tätä riskiä voitaisiin lieventää konsolidoimalla asianomaisia rakenteita asteittain erityisesti kansallisten turvaoperaatiokeskusten ja CSIRT-yksiköiden sekä rajojen yli toimivien turvaoperaatiokeskusten kohdalla. Ehdotuksessa olisi myös selvennettävä näiden rakenteiden keskinäistä vuorovaikutusta vahvistamalla selkeät hallintojärjestelyt ja vastuualueet, jotta voidaan varmistaa vaikuttava koordinointi ja saada aikaan synergioita.

Tietojenvaihto

21 Tilintarkastustuomioistuin havaitsi erityiskertomuksessaan 05/2022[3], että EU:n toimielimet, elimet ja virastot eivät jakaneet järjestelmällisesti keskeisiä kyberturvallisuustietoja keskenään, vaikka niiden olisi pitänyt tehdä niin. Tehokasta tietojenvaihtoa heikensivät entisestään yhteentoimivuuteen liittyvät ongelmat, jotka haittasivat turvallista viestintää. Vaikka tilintarkastustuomioistuimen havainnot liittyivät tähän suhteellisen pieneen ja homogeeniseen EU:n toimijoiden ryhmään, tilintarkastustuomioistuin katsoo, että tämä haaste tulee yhä relevantimmaksi monimutkaisemmassa ja monimuotoisemmassa kyberturvallisuusgalaksissa jäsenvaltioiden tasolla.

22 Asetusehdotuksen 4 artiklassa todetaan, että kansallisten turvaoperaatiokeskusten olisi toimittava kansallisella tasolla ”viitetahona ja yhdyskäytävänä”, joka kerää ja analysoi muille julkisille ja yksityisille organisaatioille kyberturvallisuusuhkia ja -poikkeamia koskevia tietoja. Tällä hetkellä EU:n tasolla ei kuitenkaan ole asetettu vaatimuksia, joiden mukaan julkisten ja yksityisten organisaatioiden olisi raportoitava kansallisille turvaoperaatiokeskuksille. Tällaisia organisaatioita ovat kansalliset CSIRT-yksiköt, yksityiset turvaoperaatiokeskukset ja toisen verkko- ja tietoturvadirektiivin mukaiset ”keskeiset ja tärkeät toimijat”. Näin ollen on olemassa riski, että kansalliset turvaoperaatiokeskukset eivät saa riittävästi dataa ja tietoja tarpeidensa täyttämiseksi.

23 Ehdotuksen liitteenä olevan rahoitusselvityksen 2.2.2 kohdassa komissio yksilöi riskin siitä, että jäsenvaltiot eivät jaa riittävästi kyberuhkia koskevia asiaankuuluvia tietoja rajojen yli toimivien turvaoperaatiokeskusten foorumeilla tai rajat ylittävien foorumien ja muiden asiaankuuluvien tahojen välillä EU:n tasolla. Tällainen tietojenvaihdon puute saattaa heikentää kyberturvallisuuden eurooppalaisen suojakilven vaikuttavuutta ja lisäarvoa.

24 Tilintarkastustuomioistuin suhtautuukin myönteisesti siihen, että ehdotuksen 4, 5 ja 6 artiklaan sisältyy erityisiä säännöksiä, joiden tarkoituksena on tietojenvaihtoon liittyvän riskin lieventäminen. Ehdotuksen mukaan kansalliset turvaoperaatiokeskukset voivat saada EU:n rahoitusta vain, jos ne sitoutuvat osallistumaan rajojen yli toimivan turvaoperaatiokeskuksen toimintaan. Tilintarkastustuomioistuin panee kuitenkin merkille, että kahden ensimmäisen vuoden aikana saatua taloudellista tukea ei tarvitse maksaa takaisin, jos kansallinen turvaoperaatiokeskus ei liity rajojen yli toimivaan

---

[3] Erityiskertomus 05/2022,EU:n toimielinten, elinten ja virastojen kyberturvallisuus: valmiustaso ei kokonaisuutena ole oikeassa suhteessa uhkiin.

turvaoperaatiokeskukseen. Asetusehdotuksessa edellytetään myös, että rajojen yli toimivien turvaoperaatiokeskusten jäsenet sitoutuvat jakamaan ”merkittävän tietomäärän” keskenään ja luovat hallintokehyksen kirjallisessa yhteenliittymäsopimuksessa.

25 Lisäksi ehdotuksen 7 artiklassa todetaan, että rajojen yli toimivien turvaoperaatiokeskusten on toimitettava EU-CyCLONelle, CSIRT-verkostolle ja komissiolle ”viipymättä” asiaankuuluvat tiedot mahdollisesta tai käynnissä olevasta laajamittaisesta kyberturvallisuuspoikkeamasta. Tilintarkastustuomioistuin korostaa tarvetta varmistaa tämän säännöksen asianmukainen täytäntöönpano.

26 Asetusehdotuksen 6 artiklassa säädetään, että komissio voi täytäntöönpanosäädöksillä täsmentää rajojen yli toimivien turvaoperaatiokeskusten yhteentoimivuuden edellytykset. Ehdotuksen 8 artiklassa säädetään, että komissio voi myös hyväksyä täytäntöönpanosäädöksiä, joissa vahvistetaan tekniset vaatimukset, joiden mukaisesti jäsenvaltioiden on varmistettava tietosuojan ja infrastruktuurin korkea fyysisen turvallisuuden taso. Näistä ehdoista ja vaatimuksista olisi sovittava nopeasti, jotta vältetään yhteensopimattomien järjestelmien kehittäminen rinnakkain ja pystytään vähentämään kustannuksia.

Kyberhätätilanteiden mekanismiin liittyvät riskit

EU:n kyberturvallisuusreservin käyttöönotto

27 Tilintarkastustuomioistuin totesi erityiskertomuksessaan 05/2022, että EU:n oma tietotekniikan kriisiryhmä CERT-EU, joka tarjoaa EU:n toimielimille, elimille ja virastoille kriisitilanteisiin reagoimista koskevaa tukea, ei toiminut tarkastuksen ajankohtana ympärivuorokautisesti.

28 Asetusehdotuksen 14 artiklassa säädetään, että komissio arvioi EU:n kyberturvallisuusreservistä haettavaa tukea koskevat pyynnöt ENISAn tuella ja että vastaus toimitetaan ”viipymättä”. Koska priorisointia voivat edellyttää useat samanaikaiset pyynnöt, asetusehdotuksessa vahvistetaan joitakin päätöksentekoperusteita. Ehdotuksen 13 artiklassa täsmennetään, että komissio voi täytäntöönpanosäädöksillä täsmentää yksityiskohtaisia järjestelyjä EU:n kyberturvallisuusreservin tukipalvelujen kohdentamiseksi.

29 Tilintarkastustuomioistuin pitää ratkaisevan tärkeänä, että aikaan, joka kuluu EU:n kyberturvallisuusvarauksesta annettavaa tukea koskevan pyynnön ja komission

vastauksen välillä, ei liity viivästyksiä pyynnön ajoituksen vuoksi. Ehdotuksessa ei kuitenkaan tarkenneta ennalta vahvistettua määräaikaa, eikä siinä kehoteta organisaatioita toteuttamaan tarvittavia toimia tällaisen määräajan saavuttamiseksi.

Poikkeaminen talousarvion vuotuisperiaatteesta

30 Yksi EU:n talousarvion perusperiaatteista on vuotuisperiaate, joten talousarvioon otetut määrärahat hyväksytään varainhoitovuodeksi, joka päättyy 31. joulukuuta. Käyttämättä jääneitä maksusitoumuksia ja maksumäärärahoja ei siirretä ilman eri toimenpiteitä seuraavalle varainhoitovuodelle. Tämä periaate on vahvistettu varainhoitoasetuksen 2 luvussa.

31 Ehdotetun asetuksen 19 artiklassa poiketaan tästä periaatteesta kyberhätätilanteiden mekanismin alaisuudessa toteutettavien toimien rahoituksen osalta. Artiklassa säädetään, että maksusitoumus- ja maksumäärärahat, jotka ovat jääneet käyttämättä varautumiseen, uhkiin reagoimiseen ja keskinäiseen avunantoon liittyviä toimia varten, siirretään ilman eri toimenpiteitä ja ne voidaan sitoa ja maksaa enintään seuraavan varainhoitovuoden joulukuun 31 päivään asti. Komissio selitti perustelujensa 2 jaksossa, että tämä budjettihallinnon joustavuus oli tarpeen *kyberturvallisuusympäristön ja kyberuhkien ennakoimattoman, poikkeuksellisen ja erityisen luonteen vuoksi*.

32 Varautumisen osalta tilintarkastustuomioistuin katsoo, että toimijoiden varautumisen koordinoitu testaus olisi sisällytettävä suunniteltuihin toimiin, joten testaukset eivät yleensä ole ennalta arvaamattomia eivätkä poikkeuksellisia. Tilintarkastustuomioistuin katsoo, että tällaiset suunnitellut toimet eivät edellytä poikkeamista vuotuisuuden perusperiaatteesta.

33 Sen sijaan EU:n kyberturvallisuusreserviä ja keskinäistä avunantoa käytetään kuitenkin vain ennalta arvaamattomien tapahtumien yhteydessä. Siksi tilintarkastustuomioistuin katsoo, että poikkeukset ovat perusteltuja vain niiden kohdalla.

34 Selkeyden vuoksi ja ottaen huomioon muiden asetusten, kuten unionin pelastuspalvelumekanismia tai naapuruus-, kehitys- ja kansainvälisen yhteistyön välinettä – Globaali Eurooppa koskevien asetusten sisällön, tilintarkastustuomioistuin katsoo myös, että ehdotetussa asetuksessa olisi täsmennettävä, että käyttämättömien sitoumusten siirto ilman eri toimenpiteitä olisi rajoitettava seuraavaan vuoteen.

Kyberturvallisuuspoikkeamien jälkitarkastelumekanismiin liittyvät riskit

35 Ehdotetun asetuksen 18 artiklassa säädetään, että ENISAn on komission, EU-CyCLONen tai CSIRT-verkoston pyynnöstä tarkasteltava ja arvioitava tiettyyn merkittävään tai laajamittaiseen kyberturvallisuuspoikkeamaan liittyviä uhkia, haavoittuvuuksia ja lieventämistoimia. Tehtyään yhteistyötä kaikkien relevanttien sidosryhmien kanssa ENISAn on laadittava jälkitarkasteluraportti, joka kattaa tärkeimmät syyt, haavoittuvuudet ja saadut kokemukset.

36 Tilintarkastustuomioistuin katsoo, että tämä on tärkeä palautemekanismi, jolla vahvistetaan jatkuvasti EU:n havaitsemis-, varautumis- ja reagointivalmiuksia kyberturvallisuusuhkien ja -poikkeamien varalta. Tilintarkastustuomioistuin ehdottaa kuitenkin, että asetusehdotuksessa olisi asetettava enimmäisaika ENISAn raportin toimittamiselle mahdollisten poikkeamien jälkeen, jotta voidaan varmistaa, että palaute annetaan hyvissä ajoin. Lisäksi ehdotuksessa todetaan, että raportissa olisi tarvittaessa annettava suosituksia unionin kyberturvallisuuden tason parantamiseksi. Ehdotuksessa ei kuitenkaan täsmennetä, miten niiden toteuttamista seurattaisiin.

Tuloksellisuuden seuranta ja toimintapolitiikan arviointi

37 Ehdotetun asetuksen 19 artiklalla muutetaan Digitaalinen Eurooppa -ohjelmaa koskevan asetuksen liitettä II ottamalla käyttöön uusi mitattavissa oleva indikaattori eli *niiden toimien lukumäärä, joilla tuetaan kyberturvallisuuspoikkeamiin varautumista ja reagoimista kyberhätätilanteiden mekanismin puitteissa*. Tämä indikaattori täydentää kahta olemassa olevaa indikaattoria, joiden tarkoituksena on seurata edistymistä Digitaalinen Eurooppa -ohjelman kyberturvallisuutta ja luottamusta koskevan erityistavoitteen saavuttamisessa ja raportoida siitä: *yhteisesti hankittujen kyberturvallisuusinfrastruktuurien tai -työkalujen tai molempien lukumäärä* ja *niiden käyttäjien ja käyttäjäyhteisöjen lukumäärä, joilla on pääsy eurooppalaisiin kyberturvallisuusvalmiuksiin*.

38 Tilintarkastustuomioistuin katsoo, että ehdotetulla uudella indikaattorilla mitataan vain tuotoksia, ja se antaa vain vähän tietoa kyberturvallisuuden eurooppalaisen suojakilven ja kyberhätätilanteiden mekanismin käytöstä ja tuloksista.

39 Ehdotuksen 20 artiklassa edellytetään, että komissio toimittaa Euroopan parlamentille ja neuvostolle kertomuksen asetuksen arvioinnista ja uudelleentarkastelusta neljän vuoden kuluttua sen soveltamispäivästä.

40 Tilintarkastustuomioistuin katsoo, että arvioinnin olisi perustuttava riittäviin ja luotettaviin tietoihin, mutta nopeasti muuttuva uhkaympäristö edellyttää jatkuvaa mukautumista ja innovointia EU:lta ja jäsenvaltioilta. Tilintarkastustuomioistuin katsoo näin ollen, että tämänhetkisen ehdotuksen mukainen arvioinnin ajankohta saattaa olla uuden ohjelmakauden kannalta liian myöhäinen. Lisäksi koko Digitaalinen Eurooppa -ohjelman kyberturvallisuutta ja luottamusta koskevaan erityistavoitteeseen budjetoitu määrä on sidottu vuoden 2027 loppuun mennessä.

Loppuhuomautukset

41 Ehdotetussa EU:n kybersolidaarisuussäädöksessä säädetään toimenpiteistä kyberturvallisuusuhkien ja -poikkeamien havaitsemiseksi, niihin varautumiseksi ja niihin reagoimiseksi. Tilintarkastustuomioistuin suhtautuu myönteisesti ehdotuksen tavoitteeseen vahvistaa EU:n kollektiivista kyberuhkien sietokykyä.

42 Tässä lausunnossa tuodaan esille joitakin tilintarkastustuomioistuimen havaitsemia riskejä. Lausunnossa otetaan kantaa myös siihen, miten ehdotus voitaisiin panna täytäntöön. Tilintarkastustuomioistuin korostaa erityisesti seuraavia riskejä: kyberturvallisuuden eurooppalaisen suojakilven toiminta ja kestävyys saattavat olla tulevaisuudessa riippuvaisia EU:n rahoituksesta; toimintaa saattaa vaikeuttaa se, ettei tietoja jaeta; ehdotukseen sisältyvät toimenpiteet tekevät koko EU:n kyberturvallisuusgalaksista monimutkaisemman.

43 Käytyään lainsäädäntöehdotuksen läpi tilitarkastustuomioistuin ehdottaa, että **komissio ja lainsäätäjät harkitsevat seuraavaa**:

— asetetaan ehdotettujen toimenpiteiden laadintaan ja täytäntöönpanoon liittyvät kustannusarviot saataville läpinäkyvyyden edistämiseksi (ks. kohta ***10***)

— selvennetään, miten kansallisten turvaoperaatiokeskusten, rajojen yli toimivien turvaoperaatiokeskusten, CSIRT-yksiköiden ja CSIRT-verkoston olisi oltava vuorovaikutuksessa; vahvistetaan tätä varten selkeät hallintojärjestelyt ja vastuualueet vaikuttavan koordinoinnin varmistamiseksi ja synergioiden aikaansaamiseksi (kohta ***20***)

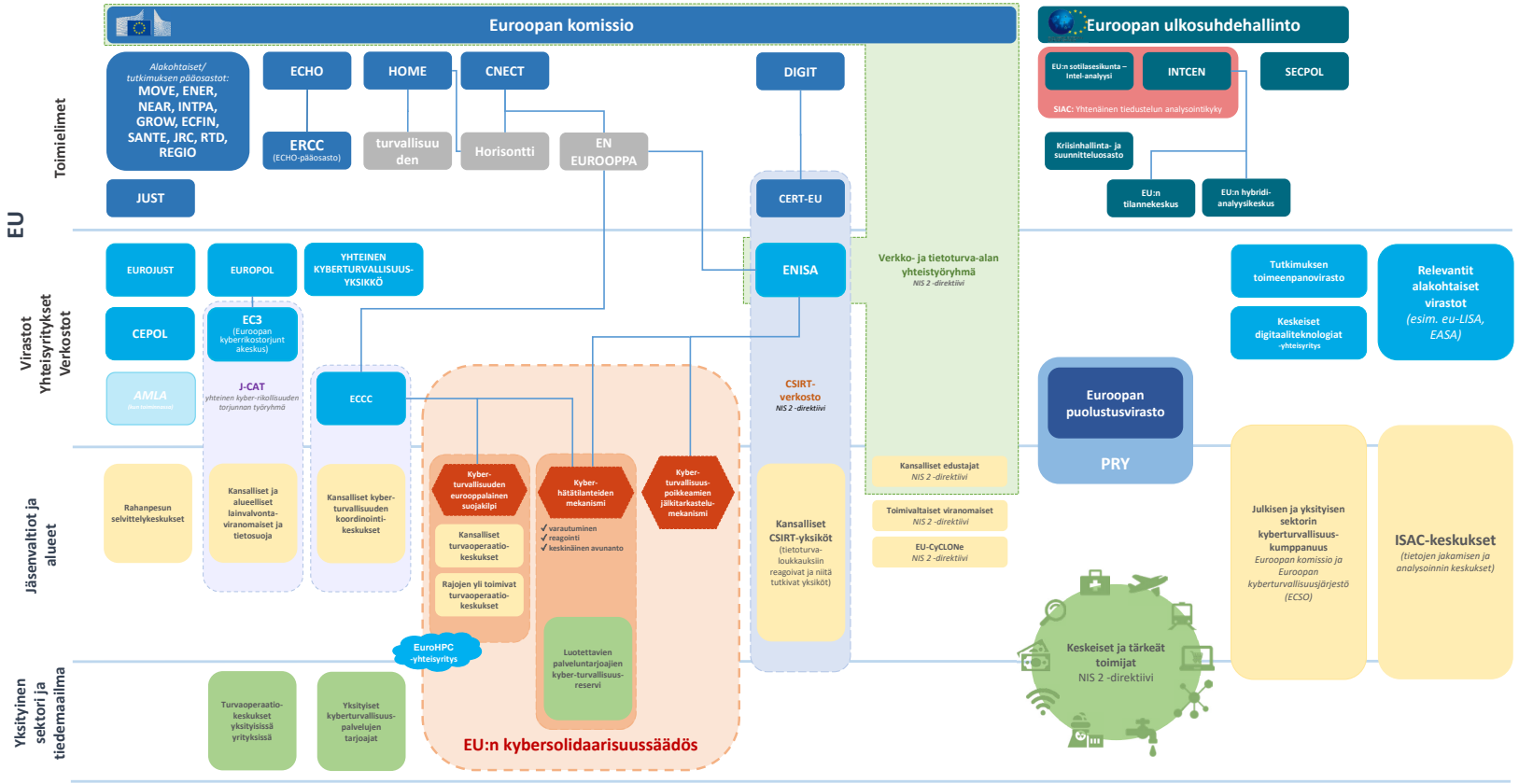
— varmistetaan, että aikaan, joka kuluu tuen saamista kyberturvallisuusvarauksesta koskevan pyynnön ja komission vastauksen välillä, ei liity viivästyksiä pyynnön ajoituksen vuoksi (kohta ***29***)

— rajoitetaan torjuntatoimien ja keskinäisen avunannon yhteydessä poikkeamista vuotuisperiaatteesta ja selvennetään, että käyttämättä jääneisiin sitoumuksiin liittyvien määrien siirrot, jotka tapahtuvat ilman eri toimenpiteitä, olisi rajoitettava seuraavaan vuoteen (kohdat ***32***–***34***)

— asetetaan enimmäisaika ENISAn raportin toimittamiselle mahdollisten häiriöiden jälkeen, jotta voidaan varmistaa, että palaute annetaan hyvissä ajoin (kohta ***36***)

— aikaistetaan määräaikaa, johon mennessä komission on toimitettava kertomus asetuksen arvioinnista ja uudelleentarkastelusta (kohta ***40***).

Liite – Euroopan kyberturvallisuusgalaksi



AMLA: Rahanpesuntorjuntaviranomainen
CEPOL: Euroopan unionin lainvalvontakoulutusvirasto
CMPD: Kriisinhallinta- ja suunnitteluosasto
CONNECT-pääosasto: Viestintäverkkojen, sisältöjen ja teknologian pääosasto
ECFIN-pääosasto: Talous- ja rahoitusasioiden pääosasto
ECHO-pääosasto: EU:n pelastuspalveluasioiden ja humanitaarisen avun operaatioiden pääosasto
ENER-pääosasto: Energian pääosasto
GROW-pääosasto: Sisämarkkinoiden, teollisuuden, yrittäjyyden ja pk-yritystoiminnan pääosasto
HOME-pääosasto: Muuttoliike- ja sisäasioiden pääosasto
INTPA-pääosasto: Kansainvälisten kumppanuuksien pääosasto
JUST-pääosasto: Oikeus- ja kuluttaja-asioiden pääosasto
MOVE-pääosasto: Liikenteen ja liikkumisen pääosasto
NEAR-pääosasto: Naapuruuspolitiikan ja laajentumisneuvottelujen pääosasto
REGIO-pääosasto: Alue- ja kaupunkipolitiikan pääosasto
RTD-pääosasto: Tutkimuksen ja innovoinnin pääosasto
SANTE-pääosasto: Terveyden ja elintarviketurvallisuuden pääosasto
DIGIT-pääosasto: Tietotekniikan pääosasto
EASA: Euroopan unionin lentoturvallisuusvirasto
EC3: Euroopan kyberrikostorjuntakeskus
ECCC: Euroopan kybertorvallisuuden tutkimus- ja osaamiskeskus
ECSO: Euroopan kybertorvallisuusjärjestö
EDA: Euroopan puolustusvirasto
EUH: Euroopan ulkosuhdehallinto
ERCC: Hätäavun koordinointikeskus
EU-CyCLONe: Euroopan kyberkriisien yhteysorganisaatioiden verkosto
EuroHPC: Eurooppalainen suurteholaskenta
EUROJUST: Euroopan unionin rikosoikeudellisen yhteistyön virasto
Europol: Euroopan unionin lainvalvontayhteistyövirasto
INTCEN: Euroopan unionin tiedusteluanalyysikeskus
ISF: Sisäisen turvallisuuden rahasto
YTK: Yhteinen tutkimuskeskus
KDT: Keskeiset digitaaliteknologiat
NIS-direktiivi: Verkko- ja tietoturvadirektiivi
PRY: Pysyvä rakenteellinen yhteistyö
SECPOL: Turvallisuuspolitiikka ja konfliktinesto

Lähde: Euroopan tilintarkastustuomioistuin.

Tilintarkastustuomioistuimen III jaosto on tilintarkastustuomioistuimen jäsenen Bettina Jakobsenin johdolla hyväksynyt tämän kertomuksen Luxemburgissa 26. syyskuuta 2023 pitämässään kokouksessa.

Tilintarkastustuomioistuimen puolesta

Tony Murphy
presidentti

TEKIJÄNOIKEUDET

© Euroopan unioni, 2023

Datan ja asiakirjojen uudelleenkäyttöä koskevat Euroopan tilintarkastustuomioistuimen periaatteet vahvistetaan avoimen datan politiikkaa ja asiakirjojen uudelleenkäyttämistä koskevassa Euroopan tilintarkastustuomioistuimen päätöksessä 6-2019.

Ellei toisin ilmoiteta (esimerkiksi yksittäisissä tekijänoikeusilmoituksissa), Euroopan tilintarkastustuomioistuimen sisältöihin, jotka EU omistaa, myönnetään käyttöoikeudet Creative Commons Attribution 4.0 International (CC BY 4.0) licence -käyttöoikeuden nojalla. Yleissääntö siis on, että uudelleenkäyttö on sallittua, jos sisällön tuottaja mainitaan asianmukaisesti ja kaikista sisältöön tehdyistä muutoksista ilmoitetaan. Euroopan tilintarkastustuomioistuimelle kuuluvan sisällön uudelleenkäyttäjä ei saa vääristää asiakirjojen alkuperäistä merkitystä tai sanomaa. Euroopan tilintarkastustuomioistuin ei vastaa mistään seurauksista, jotka johtuvat uudelleenkäytöstä.

Tarvittavat lisäoikeudet on hankittava, jos tietyssä sisällössä (esimerkiksi Euroopan tilintarkastustuomioistuimen henkilöstöstä otetuissa valokuvissa) esitetään tunnistettavissa olevia henkilöitä tai jos sisällössä on mukana kolmansien tahojen töitä.

Jos tällainen lisäoikeus saadaan, se kumoaa ja korvaa yllä mainitun yleisen käyttöoikeuden. Lisäoikeutta koskevassa luvassa on selvästi ilmoitettava käyttöoikeuden rajoitukset.

Jos sisällöt eivät ole EU:n omaisuutta, voi olla, että lupa niiden käyttöön tai jäljentämiseen on pyydettävä suoraan asianomaisilta tekijänoikeuksien haltijoilta.

Tietokoneohjelmistot tai asiakirjat, joihin kohdistuu teollisoikeuksia, kuten patentteja, tavaramerkkejä, rekisteröityjä malleja, logoja ja nimiä, eivät kuulu Euroopan tilintarkastustuomioistuimen uudelleenkäyttöperiaatteiden piiriin.

EU:n toimielinten verkkosivuilla (joiden verkkotunnuksen loppuosa on europa.eu) on linkkejä ulkopuolisille Internet-sivustoille. Koska Euroopan tilintarkastustuomioistuin ei vastaa näistä sivustoista, on suositeltavaa, että tutustutte niiden tietosuoja- ja tekijänoikeusperiaatteisiin.

Tilintarkastustuomioistuimen logon käyttö

Euroopan tilintarkastustuomioistuimen logoa ei saa käyttää ilman tilintarkastustuomioistuimen ennakkosuostumusta.