KOMISSION VASTAUKSET

EUROOPAN TILINTARKASTUSTUOMIOISTUIMEN ERITYISKERTOMUKSEEN

EU:n toimielinten, elinten ja virastojen kyberturvallisuus: valmiustaso ei yleisesti ottaen ole oikeassa suhteessa uhkiin

Sisällysluettelo

I. KOMISSION VASTAUKSET LYHYESTI 2

a) Johdanto 2

b) Komission kanta tilintarkastustuomioistuimen keskeisiin huomautuksiin ja suosituksiin 2

c) Viimeaikainen kehitys ja seuraavat vaiheet 3

II. KOMISSION VASTAUKSET TILINTARKASTUSTUOMIOISTUIMEN KESKEISIIN HUOMAUTUKSIIN 3

1. EU:n toimielinten, elinten ja virastojen kybervalmiuden taso 3

2. EU:n toimielinten, elinten ja virastojen yhteistyömekanismit 4

3. Tietojen jakaminen merkittävistä poikkeamista tai haavoittuvuuksista 5

III. KOMISSION VASTAUKSET TILINTARKASTUSTUOMIOISTUIMEN PÄÄTELMIIN JA SUOSITUKSIIN 5

Suositus 1 – Parannetaan kaikkien EU-elinten kyberturvallisuusvalmiuksia yhteisillä sitovilla säännöillä ja lisäämällä CERT-EU:n resursseja 5

Suositus 2 – Edistetään EU-elinten välisiä lisäsynergioita tietyillä osa-alueilla 6

Suositus 3 – Lisätään CERT-EU:n ja ENISAn keskittymistä niihin EU:n toimielimiin, elimiin ja virastoihin, joiden kybervalmiuksissa on parantamisen varaa 7

Tässä asiakirjassa esitetään Euroopan komission vastaukset Euroopan tilintarkastustuomioistuimen erityiskertomuksen huomautuksiin varainhoitoasetuksen 259 artiklan mukaisesti, ja se julkaistaan yhdessä erityiskertomuksen kanssa.

I. KOMISSION VASTAUKSET LYHYESTI

a) Johdanto

Kyberturvallisuudesta on tullut Euroopan komission ensisijainen poliittinen ja operatiivinen painopiste. Covid-19-kriisi on lisännyt riippuvuuttamme digitaalisista palveluista (pilvipalvelut, mobiililaitteet, tekoäly). Kahden viime vuoden aikana valtava määrä ihmisiä on siirtynyt etätyöhön. Tämä tarkoittaa, että sekä kyberrikollisuus että kybervakoilu, jotka ovat kaksi merkittävintä Euroopan unionin toimielimin, elimiin ja virastoihin kohdistuvaa uhkaa, ovat myös lisääntyneet verkossa huomattavasti. Komissio tiedostaa tämän suuntauksen. Se on osoittanut johdonmukaista ja päättäväistä johtajuutta kyberturvallisuuden alalla. Vuonna 2019 voimaan tulleella kyberturvallisuusasetuksella muun muassa laajennettiin ENISAn toimeksiantoa ja tehtiin siitä pysyvä. Asetuksella myös käynnistettiin virallinen yhteistyö ENISAn ja CERT-EU:n (EU:n toimielinten, elinten ja virastojen tietotekniikan kriisiryhmä) välillä. Komissio ehdotti vuonna 2020 verkko- ja tietoturvadirektiivin vahvistamista, ja lainsäädäntöprosessissa ollaan jo lähellä hyväksyntää.

Vuoden 2020 kyberturvallisuusstrategiaan sisältyi myös kolme EU:n toimielinten, elinten ja virastojen kyberturvallisuuteen liittyvää toimea. Strategiassa ilmoitettiin tietoturvaa EU:n toimielimissä, elimissä ja virastoissa koskevasta asetuksesta ja EU:n toimielinten, elinten ja virastojen yhteisiä kyberturvallisuussääntöjä koskevasta asetuksesta sekä aikomuksesta luoda uusi oikeusperusta CERT-EU:lle sen toimeksiannon ja rahoituksen vahvistamiseksi, jotta voidaan varmistaa, että CERT-EU:lla on riittävät resurssit kasvaviin uhkiin, riskeihin ja vaaratilanteisiin vastaamiseksi.

Näiden ehdotusten valmistelutyö on edistynyt. Vaikka kollegio ei ole vielä hyväksynyt niitä, on odotettavissa, että ne hyväksytään vuoden 2022 ensimmäisellä neljänneksellä. Toimielinten tässä valmisteluvaiheessa käsittelemät tärkeät kysymykset koskevat ehdotuksen oikeusperustaa sekä kaikkien EU:n toimielinten, elinten ja virastojen talousarvioresursseja, joilla ne voivat sekä rahoittaa omat kyberturvallisuustarpeensa että löytää tarvittavat resurssit CERT-EU:n, talousarvion ja erityisesti virkojen tukemiseksi.

EU:n toimielinten, elinten ja virastojen kyberturvallisuusvalmiuksien taso vaihtelee. Useiden EU:n toimielinten, elinten ja virastojen kyberturvallisuusvalmiuksien taso on vahva, ja niiden olisi edelleen toimittava johtajina ja kannustaa ja innostaa kyberturvallisuusympäristön edistämiseen ja lisäparannuksiin. Mitattavissa olevan edistyksen saavuttamiseksi on tärkeää tunnustaa EU:n toimielinten, elinten ja virastojen erilaiset valmiustasot ja painopisteasettelu suuntaamalla parannustoimet ensisijaisesti niihin EU:n toimielimiin, elimiin ja virastoihin, joissa havaitut puutteet aiheuttavat suurimman riskin.

b) Komission kanta tilintarkastustuomioistuimen keskeisiin huomautuksiin ja suosituksiin

Komissio suhtautuu myönteisesti tilintarkastustuomioistuimen kertomukseen EU:n toimielinten, elinten ja virastojen kyberturvallisuudesta. Komissio panee merkille, että kertomuksessa korostetaan kaikkien EU:n toimielinten, elinten ja virastojen yhteisten tietoturvaa ja kyberturvallisuutta koskevien oikeudellisten kehysten merkitystä kyberturvallisuuden yleisen tason parantamisen kannalta. Komissio toteaa, että tilintarkastustuomioistuimen tärkeimmät huomautukset ja suositukset eivät sinänsä koske komission omaa operatiivista kyberturvallisuutta

vaan komission poliittista roolia lainsäädännön ehdottamisessa EU:n toimielinten, elinten ja virastojen kybervalmiuden kehittämiseksi.

Tulevissa tietoturvaa EU:n toimielimissä, elimissä ja virastoissa koskevassa asetuksessa ja EU:n toimielinten, elinten ja virastojen yhteisiä kyberturvallisuussääntöjä koskevassa asetuksessa vahvistetaan yhteiset säännöt korkeatasoisen tietoturvan ja kyberturvallisuuden saavuttamiseksi, mutta kukin EU:n toimielin, elin ja virasto vastaa itsenäisesti niiden täytäntöönpanosta omassa organisaatio- ja toimintaympäristössään (erityisesti uhka- ja riskiprofiilien osalta). Ehdotettuun kyberturvallisuutta koskevaan asetukseen liittyy noudattamista koskevat mekanismit, jotka ovat asianmukaisia ja oikeassa suhteessa uusien sääntöjen tavoitteeseen ja soveltamisalaan, sanotun kuitenkaan rajoittamatta toimielinten, elinten ja virastojen riippumattomuutta.

Komissio toimii tällä hetkellä digitaalista muutosta käsittelevän toimielinten välisen komitean (ICDT) kyberturvallisuuden alaryhmän puheenjohtajana. Puheenjohtajuus on kiertävä (kausi enintään kaksi vuotta). On huomattava, että alaryhmän työhön ei ole osoitettu erityisiä resursseja: osallistujat toteuttavat kaikki parhaaksi katsomansa toimet vapaaehtoisuuden pohjalta.

Komissio kannattaa CERT-EU:n resurssien ja toimeksiannon yleistä vahvistamisesta.

Näin ollen komissio tukee kertomuksen keskeisiä havaintoja ja suosituksia. Komission kanta esitetään yksityiskohtaisesti III jakson lisähuomautuksissa. Komissio hyväksyy suositukset 1 a, b, c, d, e, f, g ja 2 a, b ja c.

c) Viimeaikainen kehitys ja seuraavat vaiheet

EU:n toimielinten, elinten ja viraston johtajien tasolla on saatu päätökseen virallinen kuuleminen (tietoturvallisuutta ja kyberturvallisuutta koskevien) asetusten konsolidoiduista luonnoksista. Saatua palautetta arvioidaan parhaillaan, ja tämän jälkeen paketti on tarkoitus saada valmiiksi ja kollegion on tarkoitus hyväksyä se vuoden 2022 ensimmäisen neljänneksen aikana.

II. KOMISSION VASTAUKSET TILINTARKASTUSTUOMIOISTUIMEN KESKEISIIN HUOMAUTUKSIIN

1. EU:n toimielinten, elinten ja virastojen kybervalmiuden taso

Komissio on samaa mieltä siitä, että EU:n toimielinten, elinten ja virastojen kyberturvallisuusmenojen tasoa tarkasteltaessa on tärkeää ottaa huomioon uhat ja riskit.

Myös EU:n toimielinten, elinten ja virastojen henkilöstöresurssien vakauteen vaikuttavat useat tekijät. Kyberturvallisuusasiantuntijoiden rekrytointimarkkinat ovat yhä monimutkaisemmat. Monissa tapauksissa henkilöstösääntöjä ei ole mukautettu erityisasiantuntijan tehtäviin (palvelukseenotto, urakehitys, koulutus). Lisäksi budjettivallan käyttäjän EU:n toimielinten, elinten ja virastojen henkilöstömääriin kohdistama yleinen paine merkitsee, että kyberturvallisuuden

kaltaisilla uusilla painopistealoilla ei edelläänkään ole riittävästi virkoja, etenkään sisäisissä operatiivisissa yksiköissä.

Hallinnon ja riskinhallinnan edistymisen osalta olisi otettava huomioon, että vaatimustenmukaisuuden seuranta on nyt siirtymässä pilottivaiheesta täysimittaiseen täytäntöönpanoon. Näin ollen on normaalia, että kattavuus on toistaiseksi melko alhainen. Tämä vaatimustenmukaisuutta koskeva hanke on seuraava vaihe kybervalmiuksien parantamiseen tähtäävässä pitkän aikavälin prosessissa, joka alkoi yhteisen riskimenetelmän määrittelyllä, yhteisten työkalujen kehittämisellä, haavoittuvuuksien hallinnan käyttöönotolla sekä resurssien inventoinnin seurannalla, testauksella ja validoinnilla. Tällä pitkällä tiellä on edistytty siitä huolimatta, että komission resurssipohja on monimutkainen, sillä yli 1 000 tietojärjestelmän hallinnoinnista vastaa yli 50 pääosastoa ja toimeenpanovirastoa.

2. EU:n toimielinten, elinten ja virastojen yhteistyömekanismit

CERT-EU on ilmiömäinen menestystarina sekä EU:n toimielinten, elinten ja virastojen välisen että Euroopan tason yhteistyön edistämisessä, koska se osallistuu täysvaltaisena jäsenenä verkko- ja tietoturvadirektiivillä perustettuun CSIRT-verkostoon. CERT-EU on näin ollen esimerkkitapaus siitä, miten yhteistyötä ja kyberturvallisuuspalveluja voidaan parantaa. Tilintarkastustuomioistuimen CERT-EU:ta koskevat huomautukset osoittavat hyvin selvästi, että CERT-EU tekee erinomaista työtä yhä uhkaavammassa kyberturvallisuustilanteessa, jossa resurssit ovat jatkuvasti liian alhaiset.

Nykyisen toimielinten välisen sopimuksen mukaan ENISA edustaa virallisesti EU:n erillisvirastoja ja yhteisyrityksiä CERT-EU:n johtokunnassa. Lisäksi niiden näkemykset esittää johtokunnan kokouksissa tieto- ja viestintätekniikan neuvoa-antavan komitean (ICTAC) edustaja, joka voi osallistua kokouksiin ENISAn avustamiseksi virastojen edustamisessa mutta jolla ei ole virallista asemaa eikä äänioikeutta. Virastojen riittävää edustusta CERT-EU:n johtokunnassa parannetaan asetusehdotuksessa lisäämällä johtokunnan kokoonpanoon enintään kolme edustajaa, jotka unionin virastojen verkosto (EUAN) nimittää tieto- ja viestintätekniikan neuvoa-antavan komiteansa ehdotuksesta.

Kukin EU:n toimielin, elin ja virasto osallistuu ICDT:n kyberturvallisuuden alaryhmään parhaansa mukaan ja päättää itse sitoumuksensa tasosta. Uuden kyberturvallisuutta koskevan puitesopimuksen valmistelun yhteydessä käsitellään parannuksia hankintoja koskevaan tietojenvaihtoon, joka on tärkeä aihe kyberturvallisuuden alaryhmän työryhmän 2 toiminta-alalla.

Sähköpostin ja videoneuvottelun kaltaisiin palveluihin liittyvien yhteisten välineiden osalta on mahdollista käyttää SECEM-2-järjestelmää, jonka komissio on ottanut käyttöön kaikissa EU:n toimielimissä, elimissä ja virastoissa salattuna sähköpostiratkaisuna, joka edellyttää salausavainten ja varmenteiden tehokasta hallinnointia. Lisäksi kehitteillä on SECABC-väline, joka mahdollistaa sähköpostien salauksen toimielinten välillä. Se on tarkoitus tarjota kaikkien kiinnostuneiden EU:n toimielinten, elinten ja virastojen saataville vuoden 2022 aikana. Arkaluonteisia turvallisuusluokittelemattomia tietoja käsitteleviä yksikköjä varten on jo käytössä suojatut videoneuvotteluyhteydet, ja ne voidaan tapauskohtaisesti antaa myös muiden EU:n toimielinten, elinten ja virastojen käyttöön hallinnoimalla kokousten osallistujien henkilöllisyyksiä. Arkaluonteisten tietojen jakamista käsitellään myös ehdotetussa tietoturvaa koskevassa asetuksessa (jossa säädetään yhteisistä merkinnöistä).

3. Tietojen jakaminen merkittävistä poikkeamista tai haavoittuvuuksista

Sitä, että kaikki EU:n toimielimet, elimet ja virastot eivät ilmoita merkittävistä poikkeamista tai haavoittuvuuksista, käsitellään kyberturvallisuutta koskevassa asetusluonnoksessa komission NIS 2 -direktiivissä[1] esittämän ehdotuksen mukaisesti. Täytäntöönpanon taso riippuu siitä, millaisia lisäresursseja riippumattomat EU:n toimielimet, elimet ja virastot tähän tarkoitukseen osoittavat. Mahdollisuudet tällaisten ilmoitusten valvontaan ovat edelleen rajalliset, myös tällä hetkellä suunnitellun asetusehdotuksen mukaan, sillä EU:n toimielimet, elimet ja virastot ovat institutionaalisesti riippumattomia. Ehdotettuun kyberturvallisuutta koskevaan asetukseen liittyy noudattamista koskevat mekanismit, jotka ovat asianmukaisia ja oikeassa suhteessa uusien sääntöjen tavoitteeseen ja soveltamisalaan, sanotun kuitenkaan rajoittamatta toimielinten, elinten ja virastojen riippumattomuutta.

III. KOMISSION VASTAUKSET TILINTARKASTUSTUOMIOISTUIMEN PÄÄTELMIIN JA SUOSITUKSIIN

Suositus 1 – Parannetaan kaikkien EU-elinten kyberturvallisuusvalmiuksia yhteisillä sitovilla säännöillä ja lisäämällä CERT-EU:n resursseja

Ehdotettu asetus sisältää erityisiä toimenpiteitä, joiden tarkoituksena on parantaa yhteistä kyberturvallisuustasoa. Nämä toimenpiteet muunnetaan kyberturvallisuussuunnitelmiksi, jotka määritellään ja pannaan täytäntöön EU:n toimielinten, elinten ja virastojen tasolla niiden oman kyberturvallisuuden hallintokehyksen mukaan.

Komissio hyväksyy tämän suosituksen. Tiettyjen osasuositusten osalta komissio toteaa seuraavaa:

a) Komissio hyväksyy suosituksen 1 a. Asetusehdotukseen sisältyy hallinto- ja valvontakehyksiä koskevia säännöksiä, jotka perustetaan kunkin EU:n toimielimen, elimen tai viraston ylimmän johdon tasolla kaikkien kyberturvallisuusriskien tehokkaan ja järkevän hallinnan varmistamiseksi.
b) Komissio hyväksyy suosituksen 1 b. Asetusehdotuksella vahvistetaan riskiperusteista lähestymistapaa kyberturvallisuuden hallintaan, sillä siinä selvennetään, että toimissa, tietotekniikan turvallisuutta koskevissa suunnitelmissa ja olennaisten valvontatoimien varsinaisessa täytäntöönpanossa olisi noudatettava arviointeja.

[1] Ehdotus Euroopan parlamentin ja neuvoston direktiiviksi toimenpiteistä yhteisen korkean kyberturvatason varmistamiseksi koko unionissa ja direktiivin (EU) 2016/1148 kumoamisesta, COM(2020) 823 final.

c) Komissio hyväksyy suosituksen 1 c. Kyberturvallisuutta koskevat koulutus- ja tiedotusohjelmat mainitaan asetusehdotuksessa osana kyberturvallisuuden perustasoa.
d) Komissio hyväksyy suosituksen 1 d. Komission kokemuksen mukaan säännölliset tarkastukset ja testit ovat välttämättömiä, mutta ne eivät riitä varmistamaan, että edistystä tapahtuu. Näin ollen säännöllinen raportointi ja avoimuus ovat tarvittava osa a kohdan mukaista kyberturvallisuuden hallintokehystä.
e) Komissio hyväksyy suosituksen 1 e. Asetusehdotukseen sisältyy säännöksiä, jotka koskevat EU:n toimielinten, elinten ja virastojen ilmoituksia merkittävistä kyberuhkista, haavoittuvuuksista ja poikkeamista.
f) Komissio hyväksyy suosituksen 1 f. Komissio on samaa mieltä tarpeesta lisätä CERT-EU:n resursseja. Asetusehdotukseen sisällytetään EU:n toimielinten, elinten ja virastojen henkilöstöä ja rahoitusosuuksia koskevia säännöksiä.
g) Komissio hyväksyy suosituksen 1 g. Ehdotettuun asetukseen liittyy vaatimusten noudattamista koskevat mekanismit, jotka ovat oikeassa suhteessa säännösten kohteeseen ja soveltamisalaan ja joissa otetaan huomioon EU:n toimielinten, elinten ja virastojen institutionaalinen riippumattomuus. Tulevan asetuksen sisältö riippuu lainsäädäntömenettelyn tuloksesta ja perustuu EU:n lainsäätäjän päätökseen komission ehdotuksesta.

Suositus 2 – Edistetään EU-elinten välisiä lisäsynergioita tietyillä osa-alueilla

Komissio, joka toimii tällä hetkellä digitaalista muutosta käsittelevän toimielinten välisen komitean (ICDT) kyberturvallisuuden alaryhmän puheenjohtajana, on samaa mieltä suosituksista, joiden mukaan olisi edistettävä ratkaisuja arkaluonteisten tietojen johdonmukaiseen ja turvalliseen jakamiseen, kyberturvallisuushankkeita koskevien tietojen järjestelmälliseen jakamiseen sekä yhteisiin hankintakehyksiin ja kyberturvallisuuspalveluja koskeviin sopimuksiin.

Komissio hyväksyy tämän suosituksen. Tiettyjen osasuositusten osalta komissio toteaa seuraavaa:

a) Komissio hyväksyy suosituksen 2 a. Komissio luo ICDT:n kyberturvallisuuden alaryhmälle teknisiä aloitteita ja palveluja, jotta voidaan edistää ja tukea yhteisiä välineitä arkaluonteisten tietojen jakamiseksi, mikä mahdollistaa sähköpostin ja videoneuvottelujen kaltaiset palvelut. Komissio toteaa myös, että arkaluonteisten turvallisuusluokittelemattomien tietojen yhteisiä merkintöjä ja käsittelyä koskevia yhteisiä sääntöjä käsitellään ehdotetussa tietoturvaa koskevassa asetuksessa.
b) Komissio hyväksyy suosituksen 2 b. ICDT:n kyberturvallisuuden alaryhmän nykyiset työryhmät käsittelevät tätä asiaa, ja sitä kehitetään edelleen. Hankintoja koskevan tietojenvaihdon parantamista käsitellään uuden kyberturvallisuutta koskevan puitesopimuksen valmistelujen yhteydessä.
c) Komissio hyväksyy suosituksen 2 c. EU:n toimielimillä, elimillä ja virastoilla on jo mahdollisuus osallistua komission hallinnoimiin toimielinten välisiin puitesopimuksiin tieto- ja viestintätekniikan alalla. Uuden kyberturvallisuutta koskevan puitesopimuksen valmistelua koordinoidaan ICDT:n kyberturvallisuuden alaryhmän kanssa.

Suositus 3 – Lisätään CERT-EU:n ja ENISAn keskittymistä niihin EU:n toimielimiin, elimiin ja virastoihin, joiden kybervalmiuksissa on parantamisen varaa

Tämä suositus on osoitettu CERT-EU:lle ja ENISAlle.