Euroopa Liidu
Nõukogu

Brüssel, 21. juuni 2022
(OR. en)

10504/22

CYBER 232
TELECOM 288
CSC 286
CSCI 96
FIN 689

MENETLUSE TULEMUS

Saatja:	Nõukogu peasekretariaat
Kuupäev:	21. juuni 2022
Saaja:	Delegatsioonid
Eelmise dok nr:	9716/22
Teema:	Nõukogu järeldused, milles käsitletakse Euroopa Kontrollikoja eriaruannet nr 05/2022 „ELi institutsioonide, organite ja asutuste küberturvalisus: üldine valmisoleku tase ei vasta ohtudele“ – Nõukogu järeldused, mille nõukogu kiitis heaks 21. juuni 2022. aasta istungil

Delegatsioonidele edastatakse lisas eespool nimetatud nõukogu järeldused, mille nõukogu kiitis heaks 21. juuni 2022. aasta istungil.

LISA

NÕUKOGU JÄRELDUSED,

milles käsitletakse Euroopa Kontrollikoja eriaruannet nr 05/2022 „ELi institutsioonide, organite ja asutuste küberturvalisus: üldine valmisoleku tase ei vasta ohtudele“

EUROOPA LIIDU NÕUKOGU,

TULETADES MEELDE oma järeldusi kontrollikoja poolt koostatud eriaruannete läbivaatamise parandamise kohta seoses eelarve täitmisele heakskiidu andmise menetlusega[1];

1. VÕTAB TEADMISEKS Euroopa Kontrollikoja eriaruande nr 05/2022 „ELi institutsioonide, organite ja asutuste küberturvalisus: üldine valmisoleku tase ei vasta ohtudele“[2];

2. RÕHUTAB, kui oluline on kiiresti tugevdada küberturvalisust ELi institutsioonides, organites ja asutustes, võttes arvesse digiülemineku hiljutist intensiivistumist institutsioonides, nende töödeldavat tundlikku teavet, ELi institutsioonide, organite ja asutuste vastu suunatud rünnakute üha suurenevat arvu ja tõsidust ning neid mõjutava ohu taset;

3. TULETAB MEELDE Euroopa Ülemkogu 20. juuni 2019. aasta järeldusi,[3] milles Euroopa Ülemkogu kutsus ELi institutsioone koos liikmesriikidega üles tegema tööd meetmetega, mille eesmärk on suurendada ELi vastupanuvõimet ja parandada selle julgeolekukultuuri seoses väljastpoolt ELi pärinevate küber- ja hübriidohtudega ning paremini kaitsta ELi info- ja sidevõrke ning ELi otsustusprotsesse igasuguse pahatahtliku tegevuse eest;

---

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

4. TULETAB MEELDE nõukogu 10. detsembri 2019. aasta järeldusi vastupanuvõime suurendamiseks ja hübriidohtudega võitlemiseks tehtavate täiendavate jõupingutuste kohta,[4] milles kutsuti ELi institutsioone, organeid ja asutusi üles tagama liikmesriikide toetusel liidu võime kaitsta oma terviklikkust ning suurendada ELi info- ja sidevõrkude ning otsustusprotsessi turvalisust igat liiki pahatahtliku tegevuse vastu, tuginedes põhjalikule ohuhinnangule. Järeldustes märgiti, et selleks peaksid institutsioonid, organid ja asutused liikmesriikide toetusel välja töötama ja rakendama tervikliku meetmekogumi oma julgeoleku tagamiseks kooskõlas 2019. aasta juuni Euroopa Ülemkogult saadud volitustega[5];

5. TULETAB MEELDE nõukogu 22. märtsi 2021. aasta järeldusi, milles käsitletakse Euroopa Liidu küberturvalisuse strateegiat digikümnendi jaoks,[6] kus rõhutati, et küberturvalisus on väga oluline avaliku halduse ja institutsioonide toimimiseks nii riiklikul kui ka ELi tasandil ning meie ühiskonna ja majanduse jaoks tervikuna;

6. TULETAB MEELDE nõukogu 23. mai 2022. aasta järeldusi Euroopa Liidu kübervaldkonna positsiooni arendamise kohta,[7] milles kutsuti ELi institutsioone, organeid ja asutusi üles osalema olemasolevate kübervaldkonna turvalise side vahendite kaardistamises, mida hakatakse arutama asjaomastes nõukogu organites ja asjakohaste koostöörühmade, näiteks CIRTSide võrgustiku ja EU - CyCLONe'ga;

7. RÕHUTAB vajadust tegeleda süsteemse riskiga, mis seisneb selles, et vaatamata oma institutsioonilisele sõltumatusele ja halduslikule autonoomiale on ELi institutsioonid, organid ja asutused omavahel tihedalt seotud;

---

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

8. VÕTAB TEADMISEKS eriaruande tähelepanekud, nimelt selle, et ELi institutsioonid, organid ja asutused ei ole saavutanud ohtudele vastavat küberturvalisuse alast valmisolekut ning nende küberturvalisuse alase küpsuse tase on erinev; TUNNISTAB, et ELi institutsioonide, organite ja asutuste küberturvalisuse alast valmisolekut ning nendevahelist koostoimet tuleks parandada;

9. SOOVITAB seepärast TUNGIVALT ELi institutsioonidel, organitel ja asutustel oma valmisoleku taseme suurendamiseks jätkata selliste küberriskide juhtimise meetmete rakendamist, mis tagavad küberturvalisuse asjakohase taseme, nagu on ette nähtud kavandatavas direktiivis, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus, ning millega tunnistatakse kehtetuks direktiiv (EL) 2016/1148;

10. KUTSUB ELi institutsioone, organeid ja asutusi ÜLES suurendama nii oma jõupingutusi, et kaitsta end küberohtude eest, kui ka omavahelist koostööd ühtsete standardite ja spetsifikatsioonide kehtestamisel, eelkõige küberturvalisusega seotud hangete, projektide ja teenuste puhul, ning suurendama oma IT-süsteemide koostalitlusvõimet, sealhulgas eesmärgiga tagada salastamata sisu turvaline edastamine;

11. KUTSUB Euroopa Liidu Küberturvalisuse Ametit (ENISA) ning ELi institutsioonide ja ametite infoturbeintsidentidega tegelevat rühma (CERT-EU) ÜLES tihendama oma pädevuse piires koostööd, et toetada ELi institutsioone, organeid ja asutusi nende küberturvalisuse alastes jõupingutustes, eelkõige seoses nende ELi institutsioonide, organite ja asutuste suutlikkuse suurendamisega, kelle küberturvalisuse küpsuse tase on madalam;

12. VÕTAB TEADMISEKS eriaruande järeldused ja soovitused ning TUNNISTAB, et ELi institutsioonide, organite ja asutuste küberturvalisuse alast valmisolekut ning nendevahelist koostoimet tuleks märkimisväärselt parandada. ELi institutsioonidel, organitel ja asutustel peaks olema terviklik küberturvalisuse riskijuhtimise raamistik, nad peaksid tegema korrapäraseid riskihindamisi ja auditeid, tuginedes ühisele või tuntud metoodikale ja rahvusvahelistele standarditele, ning nad peaksid süstematiseerima töötajate küberturvalisuse alase teadlikkuse suurendamise ja koolitusprogrammid;

13. TOONITAB samuti, et ELi institutsioonid, organid ja asutused peaksid eraldama eelarvest piisavad vahendid, et tagada küberohtude vastaste kaitsemeetmete rakendamine, järgides samal ajal mitmeaastast finantsraamistikku, ning VÕTAB TEADMISEKS eriaruandes esitatud soovituse, mille kohaselt tuleks määrata kõigi ELi institutsioonide, organite ja asutuste esindusorgan, millele antakse asjakohased volitused ja vahendid küberturvalisuse valdkonna ühiste eeskirjade järgimise jälgimiseks;

14. TUNNISTAB, et CERT-EUd tuleks viivitamata teavitada olulistest küberintsidentidest ELi institutsioonides, organites ja asutustes ning selleks tuleks rühmale eraldada piisavad vahendid, mis on prognoositavad ja kohandatud praegusele ohutasemele ning ELi institutsioonide, organite ja asutuste vajadustele, eelkõige personali, tehnilise varustuse ja taristu osas;

15. MÄRGIB, et küberturvalisuse alast koostööd ja teabevahetust ning turvaliste sidekanalite koostalitlusvõimet ELi institutsioonide, organite ja asutuste vahel tuleks tugevdada ja süstematiseerida; KUTSUB ÜLES kaasama sellisesse koostöösse ja teabevahetusesse ka liikmesriikide avaliku sektori asutused, mis vastutavad küberturvalisuse eest;

16. VÕTAB TEADMISEKS eriaruandele lisatud komisjoni, CERT-EU ja ENISA vastused;

17. KUTSUB komisjoni ÜLES võtma arvesse eriaruandes esitatud soovitusi ning tegutsema ambitsioonikalt ELi institutsioonide, organite ja asutuste küberturvalisuse põhimõtete kujundamisel ning edendama nendevahelist koostoimet.