EUROOPA LIIDU KÜBERTURVALISUSE AMET

USALDUSVÄÄRNE JA KÜBERTURVALINE EUROOPA

ENISA strateegia

Juuni 2020

USALDUSVÄÄRNE JA KÜBERTURVALINE EUROOPA

EUROOPA LIIDU KÜBERTURVALISUSE AMET

EESSÕNA

Üle 15 aasta on Euroopa Liidu Küberturvalisuse Ametil (ENISA) olnud põhiroll ELi ühe eesmärgi – kindlustada digitaalne usaldusväärsus ja turvalisus kogu Euroopas – teostamisel koos liikmesriikide ning ELi institutsioonide ja asutustega. Kogukondi kokku tuues on ENISA edukalt kaasa aidanud Euroopa valmisoleku tugevdamisele küberintsidentideks ja neile reageerimise suutlikkuse tõhustamisele.

Samas on oluliselt suurenenud meie majanduse ja ühiskonna digitaliseeritus, nagu tõendas COVID-19 kriis, kui paljude tegevuste toimimiseks oli oluline ühiselt ja massiliselt üle minna IT-kauglahendustele. Kriis rõhutas, kui palju küberkurjategijad kasutavad ära meie sõltuvust neist tehnoloogiatest. Samuti näitas see küberohtude maastiku laienemist suunatud rünnakutelt uut tüüpi ning miljoneid ettevõtteid ja kodanikke haaravatele massiivsetele ohtudele, sealhulgas sagenevatele keerukatele lunavaraintsidentidele. Digitaaltoodete ja -teenuste kiire areng – pilveteenustest ja videokonverentsidest kuni 5G ja tehisintellektini – on samuti loonud uusi probleeme, mis tuleb leida ja lahendada.

Küberturvalisuse uue ajastu algamisega Euroopas peab ENISA oma alalise mandaadi raames ning tõhustatud ülesannete ja suurema suutlikkusega senisest enam võtma juhtrolli, et aidata ELil ja tema liikmesriikidel nende probleemidega toime tulla.

Selleks tegeleb ENISA oluliste suundumuste prognoosimisega ning kogub ja jagab kõigile tipptasemel eriteavet ja teadmisi. Amet toetab Euroopa Komisjoni ja liikmesriike avaliku ja erasektori osalejate ning kodanike abistamisel küberintsidentidega seotud riskide ennetamisel ja juhtimisel. Küberturvalisuse sertifitseerimise raamistiku rakendamisega aitab ENISA kaasa paradigma muutusele, suurendades Euroopas kasutatavate digilahenduste turvalisust. Sellega suurendab amet ka kõigi võimalusi teha valikuid ja nende usaldusväärsust. Samuti toetab amet aktiivselt Euroopa küberturvalisuse tegevkogukonda, tehes tihedat koostööd ja valmistudes ühiselt reageerima, kui Euroopat tabab järgmine suur küberintsident.

Kui ENISA asub täitma oma uut rolli, on avatus, paindlikkus ja usaldusväärsus tema igapäevase tegevuse põhitegurid, samas teeb ta tihedat koostööd liikmesriikide ja Euroopa Komisjoniga lähenemisviiside ühtlustamisel. Samuti püüab ENISA vähendada jätkuva kliimakriisi kontekstis oma keskkonnamõju ning olla sotsiaalselt vastutustundlik ja kaasav töökeskkond.

Käesolevas strateegias, mis töötati välja kõigi ENISA töötajate, haldusnõukogu ja nõuanderühma liikmete osalemise kaudu kaasavas koostööprotsessis, püstitatakse selged eesmärgid, mis juhivad ENISA tegevust lähiaastatel, et tulla toime paljude tulevikuprobleemidega.

Haldusnõukogu nimel

Jean-Baptiste Demaison
haldusnõukogu esimees

Krzysztof Silicki
haldusnõukogu aseesimees

VISIOON

Usaldusväärne ja küberturvaline Euroopa

MISSIOON

Euroopa Liidu Küberturvalisuse Ameti (ENISA) missioon on saavutada kõrgetasemeline küberturvalisus kogu Euroopa Liidus koostöö kaudu laiema kogukonnaga. Selleks toimib amet küberturvalisuse eksperdikeskusena, kogudes ja pakkudes küberturvalisuse valdkonnas sõltumatut kvaliteetset tehnilist nõu ja tuge liikmesriikidele ja ELi asutustele. Amet aitab kaasa Euroopa Liidu küberturvalisuse poliitika väljatöötamisele ja rakendamisele.

Meie eesmärk on tugevdada usaldust sidusa majanduse vastu, suurendada Euroopa Liidu taristu ja teenuste säilenõtkust ja usaldusväärsust ning tagada meie ühiskonna ja kodanike digitaalne turvalisus. Soovime olla paindlik, keskkonna suhtes ja sotsiaalselt vastutustundlik inimestele keskendunud organisatsioon.

VÄÄRTUSED

Kogukonnavaim
ENISA teeb koostööd kogukondadega, võttes arvesse nende pädevusi ja eriteavet, ning soodustab sünergiat ja usaldust, et oma missiooni kõige paremini täita.

Tipptase
ENISA püüdleb oma tegevuses eriteabe tipptaseme saavutamise poole, järgib tegevustes kõige kõrgemaid kvaliteedistandardeid ning hindab oma tegevust, et seda innovatsiooni ja tuleviku-uuringute abil pidevalt täiustada.

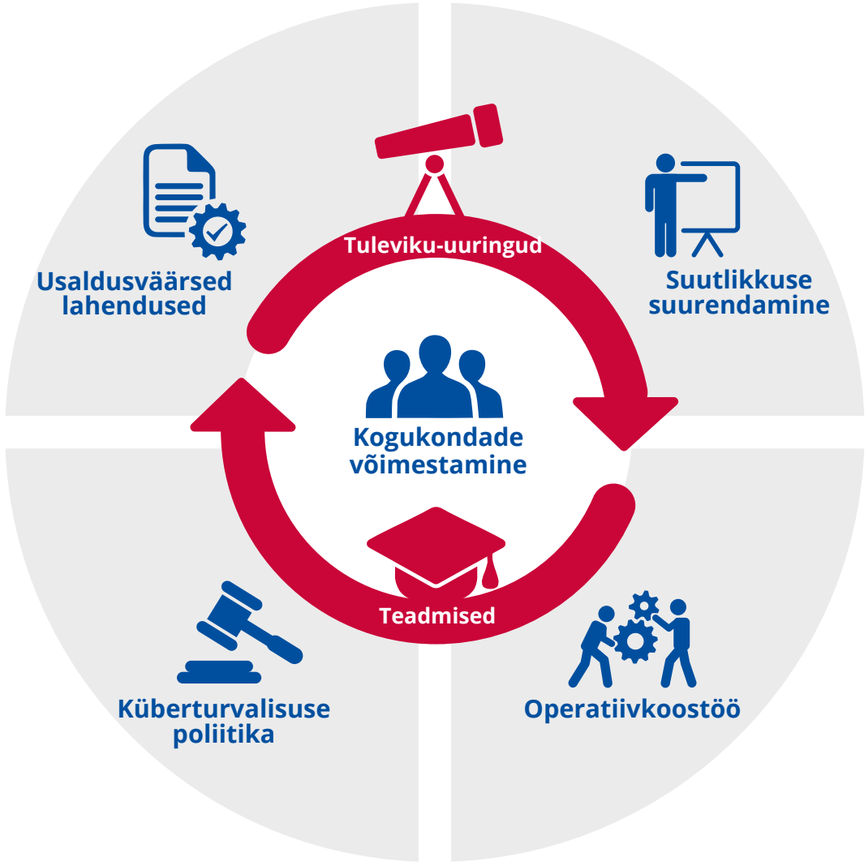
Ausus ja eetika
ENISA järgib oma teenuste ja töökeskkonna osas eetikapõhimõtteid ning asjakohaseid ELi eeskirju ja kohustusi, tagades õigluse ja kaasamise.

Õiguste järgimine
ENISA järgib kõigi oma teenuste ja töökeskkonna osas Euroopa põhiõigusi ja väärtusi ning oma sidusrühmade ootusi.

Vastutus
ENISA võtab vastutuse, tagades seega, et ameti tavadesse ja menetlustesse lõimitakse ühiskondlik ja keskkondlik mõõde.

Läbipaistvus
ENISA kehtestab avatud, faktipõhised ja sõltumatud menetlused, struktuurid ning protsessid, piirates seega kallutatust, mitmetimõistetavust, pettust ja ebaselgust.

STRATEEGILISED EESMÄRGID



SE1

Strateegiline eesmärk

VÕIMEKAD JA KAASATUD KOGUKONNAD KOGU KÜBERTURVALISUSE ÖKOSÜSTEEMIS

Kontekst

Küberturvalisus on jagatud vastutus. Euroopa püüdleb valdkondadeülese ja kõikehõlmava koostööraamistiku poole. ENISA-l on põhiroll liikmesriikides olevate küberturvalisuse sidusrühmade ning ELi institutsioonide ja ametite aktiivse koostöö edendamisel. Amet püüab tagada ühistegevuste vastastikuse täiendavuse, pakkudes sidusrühmadele lisaväärtust, uurides sünergiaid ning kasutades tõhusalt küberturvalisuse piiratud eksperditeadmisi ja ressursse. Kogukondi tuleks võimestada, et laiendada küberturvalisuse mudelit.

Mida soovime saavutada

- Kogu ELi hõlmav tipptasemel küberturvalisuse mõistete ja tavade teadmistekogu, mis toetab küberturvalisuse valdkonnas osalejate koostööd, edendab saadud kogemustest õppimist ja ELi eksperditeadmisi ning loob uusi sünergiaid.
- Võimestatud küberökosüsteem, mis hõlmab liikmesriikide asutusi, ELi institutsioone, ameteid ja asutusi, ühendusi, uurimiskeskusi ja ülikoole, valdkonda, erasektori osalejaid ja kodanikke, kellel kõigil on oma roll Euroopa küberturvaliseks muutmisel.

SE2

Strateegiline eesmärk

KÜBERTURVALISUS KUI ELI POLIITIKA LAHUTAMATU OSA

Kontekst

Küberturvalisus on digitaliseerimise alus ning seda vajatakse kõigis sektorites, mistõttu tuleb seda arvestada väga paljudes poliitikavaldkondades ja -algatustes. Küberturvalisus ei tohi piirduda ainult küberturvalisuse tehnikaekspertide erikogukonnaga. Seepärast tuleb see lõimida kõigisse ELi poliitikavaldkondadesse. On oluline vältida killustatust ning on vaja sidusat lähenemisviisi, arvestades samas iga sektori eripära.

Mida soovime saavutada

- Ennetav nõustamine ja tugi kõigile asjakohastele ELi tasandi osalejatele, mis käsitleb küberturvalisuse mõõdet poliitika arendustsüklis, toimivate ja sihipäraste tehniliste suuniste kaudu.
- Küberturvalisuse riskijuhtimisraamistikud, mis on olemas kõigis sektorites ja mida järgitakse kogu küberturvalisuse poliitika arendustsükli vältel.

SE3

Strateegiline eesmärk

EUROOPA LIIDU TEGEVOSALEJATE TÕHUS KOOSTÖÖ MASSIIVSETE KÜBERINTSIDENTIDE KORRAL

Kontekst

Euroopa digitaalse majanduse ja ühiskonna hüvesid saab täielikult saavutada ainult kübertuvalisuse tingimustes. Küberründed ei tunne piire. Need võivad mõjutada kõiki ühiskonnakihte ning Euroopa Liit peab olema valmis reageerima massiivsetele (suuremahulistele ja piirülestele) küberrünnetele ja küberkriisile. Piiriülene omavaheline seotus on toonud esile liikmesriikide ja ELi institutsioonide tõhusa koostöö vajaduse, et tagada kiirem reageerimine ja tegevuste nõuetekohane koordineerimine kõigil tasanditel (strateegiline, operatiivne, tehniline ja side).

Mida soovime saavutada

- Pidev piiriülene ja eri tasandite ülene tugi liikmesriikide koostööle ja koostööle ELi institutsioonidega. Arvestades eelkõige võimalikke suuremahulisi intsidente ja kriise ning tuge tehnilise, operatiivse, poliitilise ja strateegilise koostöö laiendamisele peamiste tegevosalejate seas, et võimaldada õigeaegset reageerimist, teabe jagamist, olukorrateadlikkust ja kriisiteabevahetust kogu Euroopa Liidus.
- Liikmesriigi nõudmisel terviklik ja kiire tehniline menetlemine, et lihtsustada tehniliste ja operatiivsete vajaduste täitmist intsidendi või kriisi ohjamisel.

SE4

Strateegiline eesmärk

TIPPTASEMEL PÄDEVUS JA SUUTLIKKUS KÜBERTURVALISUSE VALDKONNAS KOGU EUROOPA

Kontekst

Küberrünnete sagedus ja keerukus kasvab kiiresti, kuigi samas suureneb kiiresti ka IKT-taristute ja -tehnoloogiate kasutamine üksikisikute, organisatsioonide ja majandusharude poolt. Vajadus küberturvalisuse teadmiste ja pädevuste järele ületab nende pakkumise. EL peab investeerima küberturvalisuse pädevuste ja talentide arendamisse kõigil tasanditel, alates eriteadmisteta isikutest kuni kõrgelt kvalifitseeritud spetsialistideni. Investeeringud peaksid keskenduma mitte ainult küberturvalisuse oskuste suurendamisele liikmesriikides, vaid ka tagama, et eri tegevkogukondadel oleks asjakohane võimekus tulla toime küberohtude maastikul.

Mida soovime saavutada

- Ühtlustatud küberturvalisuse pädevused, erialased kogemused ja haridusstruktuurid, et täita ELi pidevalt kasvavat vajadust küberturvalisuse teadmiste ja pädevuste järele.
- Küberturvalisuse teadlikkuse ja pädevuste kõrgem lähtetase kogu ELis, lõimides kübervaldkonna aspekte kõigisse uutesse valdkondadesse.
- Hästi ettevalmistatud ja testitud suutlikkus koos asjakohase võimekusega tulla toime areneva ohukeskkonnaga kogu ELis.

SE5

Strateegiline eesmärk

“

TURVALISTE DIGILAHENDUSTE SUUR USALDUSVÄÄRSUS

Kontekst

Digitaaltoodete ja -teenustega kaasnevad peale hüvede ka riskid, mis tuleb tuvastada ja mida tuleb leevendada. Digilahenduste turvalisuse hindamise ja nende usaldusväärsuse tagamise protsessis on oluline rakendada ühist lähenemisviisi, et saavutada ühiskondlike, turupõhiste, majanduslike ja küberturvalisuse vajaduste tasakaal. Läbipaistvalt tegutsev neutraalne üksus suurendab klientide usaldust digilahenduste ja laiema digikeskkonna vastu.

Mida soovime saavutada

- Küberturvaline kogu ELi digikeskkond, milles kodanikud saavad usaldada IKT-lahendusi, -teenuseid ja -protsesse tänu sertifitseerimissüsteemide kasutamisele tehnoloogia põhivaldkondades.

SE6

Strateegiline eesmärk

TEKKIVATE JA TULEVASTE KÜBERTURVALISUSE PROBLEEMIDE TULEVIKU-UURINGUD

Kontekst

Tuleviku-uuringu meetodite kasutamine oleks kasulik arvukate uute tehnoloogiate puhul, mis on alles algetapis või mis võetakse peagi laialdaselt kasutusele. Sidusrühmade, otsustajate ja poliitikakujundajate vahelist dialoogi võimaldava struktureeritud protsessi abil oleks võimalik varakult määratleda leevendusstrateegiad, mis parandaksid ELi säilenõtkust küberturvalisuse ohtude suhtes ja aitaksid leida tekkivate probleemide lahendusi.

Mida soovime saavutada

- Tekkivate suundumuste ja mustrite mõistmine tuleviku-uuringute ja tulevikustsenaariumite abil, mis aitavad leevendada meie sidusrühmade küberprobleeme.
- Tekkivate tulevikuvõimaluste kasutuselevõtmisest ja nendega kohandumisest tulenevate probleemide ja riskide varajane hindamine, tehes samas sidusrühmadega koostööd võimalike leevendusstrateegiate osas.

SE7

Strateegiline eesmärk

KÜBERTURVALISUSE TEABE JA TEADMISTE TÕHUS JA TULEMUSLIK HALDAMINE EUROOPA JAOKS

Kontekst

Küberturvalisus toimib teabe ja teadmiste jõul. Et küberturvalisuse spetsialistid oleksid meie eesmärkide saavutamisel tulemuslikud, tegutsedes digiarengute kui ka osalejate osas pidevalt muutuvas keskkonnas ning lahendades tänapäevaseid probleeme, vajame küberturvalisuse teabe ja teadmiste kogumise, organiseerimise, kokkuvõtmise, analüüsimise, teabevahetuse ja haldamise pidevat protsessi. Kõik etapid on hädavajalikud, et tagada teabe ja teadmiste jagamine ja laiendamine ELi küberturvalisuse ökosüsteemis.

Mida soovime saavutada

- ELi küberturvalisuse ökosüsteemi teabe ja teadmiste jagatud haldus, mis on juurdepääsetavas, kohandatud, õigeaegses ja rakendatavas vormis koos sobivate meetodite, taristute ja vahenditega, mis on seotud kvaliteeditagamise meetoditega, et tagada teenuste pidev täiustamine.

ENISA

Euroopa Liidu Küberturvalisuse Amet (ENISA) on Euroopa Liidu amet, mille eesmärk on saavutada küberturvalisuse kõrge ühistase kogu Euroopas. 2004. aastal asutatud ning ELi küberturvalisuse määrusega tugevdatud Euroopa Liidu Küberturvalisuse Amet osaleb ELi küberpoliitikas, suurendab IKT-toodete, -teenuste ja -protsesside usaldusväärtust küberturvalisuse sertifitseerimissüsteemide abil, teeb koostööd liikmesriikide ja ELi organitega ning aitab Euroopal valmistuda tuleviku küberprobleemideks. Jagades teadmisi, suurendades võimekust ja teadlikkust teeb amet koostööd peamiste sidusrühmadega, et tugevdada usaldust sidusmajanduse vastu, edendada Euroopa Liidu taristu säilenõtkust ning tagada kokkuvõttes Euroopa ühiskonna ja kodanike digitaalne turvalisus. ENISA ja tema töö kohta leiab lisateavet aadressil www.enisa.europa.eu.

TP-02-20-759-ET-C

ENISA
Euroopa Liidu Küberturvalisuse Amet

Ateena büroo
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Kreeka

Heraklioni büroo
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Kreeka

enisa.europa.eu