EUROOPAN UNIONIN KYBERTURVALLISUUSVIRASTO

LUOTETTAVA JA KYBERTURVALLINEN EUROOPPA

ENISAn strategia

Kesäkuu 2020

LUOTETTAVA JA KYBERTURVALLINEN EUROOPPA

EUROOPAN UNIONIN KYBERTURVALLISUUSVIRASTO

ALKUSANAT

EU:n tavoitteena on vahvistaa digitaalista luottamusta ja turvallisuutta koko Euroopassa yhdessä jäsenvaltioiden ja EU:n toimielinten ja virastojen kanssa. Euroopan unionin kyberturvallisuusvirasto ENISAlla on ollut tavoitteen täyttämisessä keskeinen rooli jo yli 15 vuoden ajan. ENISA on pystynyt vahvistamaan Euroopan valmiutta ja kykyä reagoida kyberturvallisuuden häiriötilanteisiin tuomalla yhteisöjä yhteen.

Talous ja yhteiskunta digitalisoituvat nopeasti. Se on käynyt poikkeuksellisella tavalla ilmi covid-19-kriisin aikana, kun useiden toimien jatkuminen edellytti turvautumista tietotekniikan etäratkaisuihin laajamittaisesti ja yleisesti. Tämä kriisi on havainnollistanut, miten paljon kyberhyökkääjät pystyvät hyödyntämään riippuvaisuuttamme näistä teknologioista. Se on myös paljastanut, että kyberuhkien luonne on laajentunut kohdennetuista hyökkäyksistä miljoonia yrityksiä ja kansalaisia koskeviin uudenlaisiin joukkouhkiin, muun muassa yhä yleisempiin kehittyneisiin kiristyshaittaohjelmiin. Digitaalisten tuotteiden ja palvelujen – esimerkiksi pilvipalvelujen, videokokousten, 5G-teknologian ja tekoälyn – nopea kehitys on myös tuonut uusia haasteita, jotka on havaittava ja joihin on puututtava.

ENISAn on entistä tärkeämpää toimia edelläkävijänä ja auttaa EU:ta ja sen jäsenvaltioita vastaamaan näihin haasteisiin, kun kyberturvallisuudelle koittaa uusi aikakausi Euroopassa. Tämän se tekee pysyvän toimeksiantonsa ja laajennettujen tehtäviensä ja valmiuksiensa avulla.

ENISA pyrkii ennakoimaan merkityksellisiä suuntauksia sekä kerää uusinta asiantuntemusta ja tietämystä ja jakaa sitä kaikille. Se tukee Euroopan komissiota ja jäsenvaltioita, kun ne auttavat julkisia ja yksityisiä toimijoita ja kansalaisia ehkäisemään ja hallitsemaan kybertapahtumiin liittyviä riskejä. Kyberturvallisuuden sertifiointikehyksen täytäntöönpanon myötä ENISA edistää ajattelutavan muutosta parantamalla Euroopassa käyttöön otettavien digitaalisten ratkaisujen turvallisuustasoa. Niin tehdessään se lisää kaikkien valinnanmahdollisuuksia ja edistää luottamusta. Virasto tukee myös aktiivisesti Euroopan kyberturvallisuuden operatiivista yhteisöä tekemällä tiivistä yhteistyötä ja valmistautumalla yhteiseen reagointiin, kun seuraava laajan mittakaavan kyberturvallisuushäiriö iskee Eurooppaan.

Kun ENISA ottaa vastaan uudet tehtävänsä, sen päivittäisen toiminnan keskeisiä liikkeellepanevia voimia ovat avoimuus, ketteryys ja luotettavuus. Lisäksi se tiivistää yhteistyötään jäsenvaltioiden ja Euroopan komission kanssa sovittamalla toimintamalleja yhteen. ENISA pyrkii myös parantamaan ympäristövaikutustaan meneillään olevan ilmastokriisin yhteydessä ja tarjoamaan yhteiskuntavastuullisen ja osallistavan työympäristön.

Koko ENISAn henkilöstö, hallintoneuvoston jäsenet ja neuvoa-antava ryhmä ovat osallistuneet tämä strategia-asiakirjan laadintaan yhteistyöhön perustuvassa ja osallistavassa prosessissa. Siinä asetetaan selkeät tavoitteet, jotka ohjaavat ENISAn työtä tulevina vuosina useiden edessä olevien haasteiden kohtaamisessa.

Hallintoneuvoston puolesta

Jean-Baptiste Demaison
Hallintoneuvoston puheenjohtaja

Krzysztof Silicki
Hallintoneuvoston varapuheenjohtaja

TAVOITTEEMME

Luotettava ja kyberturvallinen Eurooppa

TEHTÄVÄMME

Euroopan unionin kyberturvallisuusviraston (ENISA) tehtävänä on saavuttaa koko EU:ssa korkea kyberturvallisuuden taso yhteistyössä laajemman yhteisön kanssa. Virasto toteuttaa tämän toimimalla kyberturvallisuuden osaamiskeskuksena, keräämällä ja tarjoamalla jäsenvaltioille ja EU:n elimille riippumatonta, laadukasta teknistä neuvontaa ja apua kyberturvallisuuden alalla. Se osallistuu unionin kyberpolitiikan kehittämiseen ja täytäntöönpanoon.

Viraston tavoitteena on vahvistaa luottamusta verkottuneeseen talouteen, lisätä unionin infrastruktuurin ja palvelujen sietokykyä ja luottamusta niihin sekä suojata yhteiskunnan ja kansalaisten digitaalista turvallisuutta. Se pyrkii olemaan ketterä, ympäristön ja yhteiskunnan kannalta vastuullinen ja ihmiskeskeinen organisaatio.

ARVOT

Yhteisöllinen ajattelutapa
ENISA työskentelee yhteisöjen kanssa, kunnioittaa niiden osaamista ja asiantuntemusta ja edistää yhteisvaikutuksia ja luottamusta voidakseen toteuttaa tehtävänsä mahdollisimman hyvin.

Huippuosaaminen
ENISA pyrkii työssään huipputason asiantuntemukseen. Se noudattaa toiminnassaan erittäin korkeita laatuvaatimuksia sekä arvioi suorituskykyään ja pyrkii parantamaan sitä jatkuvasti innovoinnin ja ennakoinnin avulla.

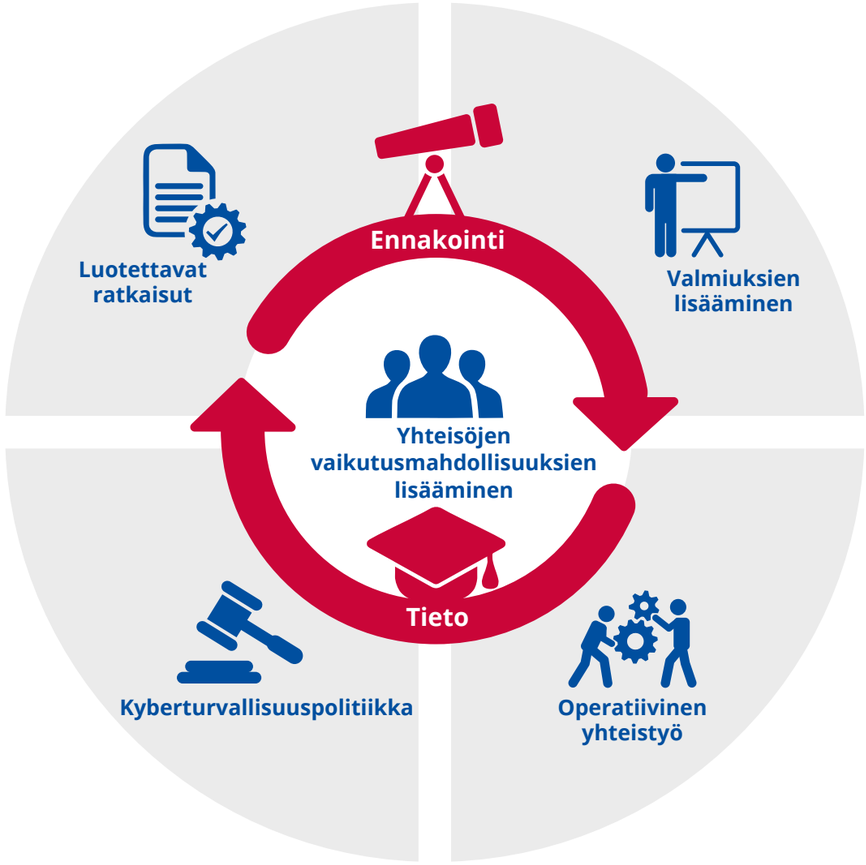
Rehellisyys/etiikka
ENISA noudattaa eettisiä periaatteita ja EU:n asiaankuuluvia sääntöjä ja velvoitteita sekä takaa oikeudenmukaisuuden ja osallisuuden palveluissaan ja työskentely-ympäristössään.

Kunnioitus
ENISA kunnioittaa kaikissa palveluissaan ja työskentely-ympäristössään EU:n perusoikeuksia ja -arvoja sekä sidosryhmiensä odotuksia.

Vastuullisuus
ENISA toimii vastuullisesti ja huolehtii yhteiskuntaan ja ympäristöön liittyvien ulottuvuuksien sisällyttämisestä viraston käytäntöihin ja menettelyihin.

Avoimuus
ENISAn menettelyt, rakenteet ja prosessit ovat avoimia, tosiasioihin perustuvia ja riippumattomia, mikä ehkäisee puolueellisuutta, moniselitteisyyttä, vilpillisyyttä ja läpinäkymättömyyttä viraston toiminnassa.

STRATEGISET TAVOITTEET



SO1

Strateginen osatavoite

VOIMAKKAAT JA SITOUTUNEET YHTEISÖT KOKO KYBERTURVALLISUUDEN EKOSYSTEEMISSÄ

Taustaa

Kyberturvallisuus on yhteinen asia. EU:n tavoitteena on saada aikaan sektorien välinen kokonaisvaltainen yhteistyökehys. ENISAlla on keskeinen rooli aktiivisen yhteistyön lisäämisessä kyberturvallisuuden sidosryhmien välillä jäsenvaltioissa sekä EU:n toimielimissä ja virastoissa. Virasto pyrkii varmistamaan yhteisten toimenpiteiden täydentävyyden tuomalla lisäarvoa sidosryhmille, selvittämällä yhteisvaikutuksia ja hyödyntämällä rajallisesti käytettävissä olevaa kyberturvallisuuden asiantuntemusta ja resursseja tehokkaasti. Yhteisöillä pitäisi olla valta ja kyky laajentaa kyberturvallisuusmallia.

Tavoitteet

- Kyberturvallisuuden käsitteitä ja käytäntöjä koskeva EU:n laajuinen huipputason tietämyspohja, jossa hyödynnetään yhteistyötä kyberturvallisuuden keskeisten toimijoiden keskuudessa, edistetään saatuja kokemuksia ja EU:n asiantuntemusta ja luodaan uusia yhteisvaikutuksia.
- Voimakas kyberekosysteemi, johon kuuluvat jäsenvaltioiden viranomaiset, EU:n toimielimet, virastot ja elimet, yhdistykset, tutkimuskeskukset ja korkeakoulut, yritykset, yksityiset toimijat ja kansalaiset, jotka kaikki tekevät osansa kyberturvallisen Euroopan puolesta.

SO2

Strateginen osatavoite

> KYBERTURVALLISUUS EROTTAMATTOMANA OSANA EU:N POLITIIKKAA

Taustaa

Kyberturvallisuus on digitalisaation kulmakivi, ja sitä tarvitaan kaikilla sektoreilla. Siksi se on otettava huomioon monilla eri politiikanaloilla ja aloitteissa. Kyberturvallisuusasioiden käsittelyä ei pidä rajoittaa teknisten kyberasiantuntijoiden asiantuntijayhteisöön. Kyberturvallisuus on sen sijaan juurrutettava kaikkiin EU:n politiikanaloihin. Kunkin alan erityisominaisuudet on otettava huomioon, mutta on ratkaisevan tärkeää välttää hajanaisuutta ja noudattaa johdonmukaista toimintamallia.

Tavoitteet

- Ennakoiva neuvonta ja tuki kaikille asianomaisille EU:n tason toimijoille, jotta kyberturvallisuutta koskeva ulottuvuus saadaan politiikan kehittämisen elinkaareen luotettavien ja kohdennettujen teknisten ohjeiden avulla.
- Kyberturvallisuuden riskinhallintakehykset, jotka ovat käytössä kaikilla sektoreilla ja joita noudatetaan koko kyberturvallisuuskäytäntöjen elinkaaren ajan.

SO3

Strateginen osatavoite

TEHOKAS YHTEISTYÖ EU:N OPERATIIVISTEN TOIMIJOIDEN KESKEN LAAJAMITTAISISSA KYBERTURVALLISUUDEN HÄIRIÖTILANTEISSA

Taustaa

Kyberturvallisuus on edellytys sille, että kaikki Euroopan digitaalitalouden ja -yhteiskunnan tarjoamat hyödyt voidaan saavuttaa. Kyberhyökkäyksillä ei ole rajoja. Ne voivat vaikuttaa kaikkiin yhteiskunnan kerroksiin, ja EU:n on oltava valmis vastaamaan suuriin (laajamittaisiin ja rajatylittäviin) kyberhyökkäyksiin ja kyberkriisiin. Rajatylittävät keskinäiset riippuvuudet ovat korostaneet sitä, että jäsenvaltioiden ja EU:n toimielinten välillä tarvitaan tehokasta yhteistyötä, jotta kaikilla tasoilla (strategisella, operatiivisella, teknisellä ja viestinnän tasolla) voidaan reagoida aiempaa nopeammin ja koordinoida toimia asianmukaisesti.

Tavoitteet

- Jatkuva rajatylittävä ja eri kerrosten välinen tuki yhteistyölle jäsenvaltioiden välillä sekä EU:n toimielinten kanssa. Etenkin mahdollisissa laajamittaisissa häiriöissä ja kriiseissä tuki teknisen, operatiivisen, poliittisen ja strategisen yhteistyön laajentamiselle keskeisten operatiivisten toimijoiden keskuudessa, jotta voidaan reagoida ajoissa, jakaa tietoa, tiedottaa tilanteesta ja harjoittaa kriisiviestintää koko EU:ssa.
- Jäsenvaltioiden pyynnöstä tehtävä kokonaisvaltainen ja nopea tekninen käsittely, jotta voidaan täyttää tekniset ja operatiiviset tarpeet häiriöiden ja kriisien hallinnassa.

SO4

Strateginen osatavoite

KYBERTURVALLISUUDEN HUIPPUTASON OSAAMINEN JA VALMIUDET KOKO EU:SSA

Taustaa

Kyberhyökkäykset lisääntyvät ja monimutkaistuvat jatkuvasti. Samalla myös yksityishenkilöiden, organisaatioiden ja yritysten tieto- ja viestintäteknisten infrastruktuurien ja -teknologioiden käyttö lisääntyy nopeasti. Kysyntä kyberturvallisuuden tietämyksestä ja osaamisesta ylittää niiden tarjonnan. EU:n on investoitava kyberturvallisuuden valmiuksien ja osaamisen kehittämiseen kaikilla tasoilla tavallisista käyttäjistä korkeasti koulutettuihin ammattilaisiin asti. Investoinneissa ei pitäisi keskittyä pelkästään kyberturvallisuustaitojen lisäämiseen jäsenvaltioissa vaan myös sen varmistamiseen, että erilaisilla operatiivisilla yhteisöillä on hallussaan asiaankuuluvat valmiudet monenlaisten kyberuhkien hallitsemiseksi.

Tavoitteet

- Yhdenmukaistetut kyberturvallisuusvalmiudet, ammatillinen kokemus ja koulutusrakenteet, joilla voidaan vastata kasvavaan kysyntään kyberturvallisuuden tietämyksestä ja osaamisesta EU:ssa.
- Korkea perustaso kyberturvallisuutta koskevassa tietoisuudessa ja osaamisessa koko EU:ssa ja kyberasioiden ottaminen huomioon kaikilla uusilla aloilla.
- Hyvin valmistellut ja testatut valmiudet sekä asianmukaiset voimavarat kehittyvään uhkaympäristöön vastaamiseksi koko EU:ssa.

SO5

Strateginen osatavoite

VAHVA LUOTTAMUS TURVALLISIIN DIGITAALISIIN RATKAISUIHIN

Taustaa

Digitaaliset tuotteet ja palvelut tuovat mukanaan sekä etuja että riskejä. Nämä riskit on tunnistettava ja niiden vaikutuksia lievennettävä. Kun arvioidaan digitaalisten ratkaisujen turvallisuutta ja varmistetaan niiden luotettavuus, on olennaisen tärkeää omaksua yhteinen toimintamalli, jonka tavoitteena on saada aikaan tasapaino yhteiskunnan, markkinoiden, talouden ja kyberturvallisuuden tarpeiden välillä. Avoimesti toimiva neutraali yhteisö lisää asiakkaan luottamusta digitaalisiin ratkaisuihin ja laajempaan digitaaliseen ympäristöön.

Tavoitteet

- Koko EU:n laajuinen kyberturvallinen digitaalinen ympäristö, jossa kansalaiset voivat luottaa tieto- ja viestintätekniikan tuotteisiin, palveluihin ja prosesseihin ja joka saadaan aikaan ottamalla sertifiointijärjestelmät käyttöön keskeisillä teknologisilla aloilla.

SO6

Strateginen osatavoite

KEHITTYVIEN JA TULEVIEN KYBERTURVALLISUUSHAASTEIDEN ENNAKOINTI

Taustaa

Ennakointimenetelmien käytöstä olisi hyötyä useille uusille teknologioille, olivatpa ne edelleen lapsenkengissä tai jo lähellä laajaa käyttöönottoa. Jäsennellyssä prosessissa, jossa sidosryhmät voivat käydä keskenään vuoropuhelua, päätöksentekijät ja lainsäätäjät pystyisivät laatimaan varhaisen riskien lieventämisen strategioita, joilla parannetaan EU:n kyberturvallisuusuhkien sietokykyä ja etsitään ratkaisuja kehittyvien haasteiden käsittelyyn.

Tavoitteet

- Kehittyvien suuntausten ja mallien ymmärtäminen käyttämällä ennakoivia ja tulevaisuutta käsitteleviä skenaarioita, jotka auttavat lieventämään sidosryhmien kyberhaasteita.
- Varhainen arviointi haasteista ja riskeistä, jotka johtuvat kehittyvien tulevien vaihtoehtojen omaksumisesta ja niihin mukautumisesta, sekä asianmukaisten lieventämisstrategioiden osalta sidosryhmien kanssa tehtävä yhteistyö.

SO7

Strateginen osatavoite

TEHOKAS JA VAIKUTTAVA KYBERTURVALLISUUSTIEDON JA -TIETÄMYKSEN HALLINTA EUROOPASSA

Taustaa

Kyberturvallisuusmoottorin polttoaineena ovat tieto ja tietämys. Jotta kyberturvallisuuden ammattilaiset pystyvät saavuttamaan tavoitteemme tehokkaasti, työskentelemään jatkuvasti muuttuvassa ympäristössä – sekä digitaalisen ympäristön että toimijoiden osalta – ja vastaamaan aikamme haasteisiin, kyberturvallisuutta koskevaa tietoa ja tietämystä on kerättävä ja järjestettävä jatkuvasti. Niistä on tehtävä yhteenvetoja ja analyysejä, ja niitä välitettävä eteenpäin ja pidettävä yllä. Kaikki vaiheet ovat olennaisia sen varmistamiseksi, että EU:n kyberturvallisuuden ekosysteemissä jaetaan ja levitetään sekä tietoa että tietämystä.

Tavoitteet

- Tiedon ja tietämyksen yhteinen hallinta EU:n kyberturvallisuuden ekosysteemissä helposti saatavilla olevassa, tarkoitukseensa räätälöidyssä, oikea-aikaisessa ja sovellettavassa muodossa asianmukaisten menetelmien, infrastruktuurien ja työkalujen yhteydessä ja yhdistettynä laadunvarmistusmenetelmiin, jotta palveluja voidaan parantaa jatkuvasti.

TIETOA ENISASTA

Euroopan unionin kyberturvallisuusvirasto, ENISA, on unionin virasto, jonka tarkoituksena on saavuttaa korkea kyberturvallisuuden taso koko EU:ssa. Virasto perustettiin vuonna 2004, ja sitä on myöhemmin vahvistettu EU:n kyberturvallisuusasetuksella. Euroopan unionin kyberturvallisuusvirasto osallistuu EU:n kyberpolitiikan laatimiseen, edistää tieto- ja viestintäteknisten tuotteiden, palvelujen ja prosessien luotettavuutta kyberturvallisuuden sertifiointijärjestelmillä, tekee yhteistyötä jäsenvaltioiden ja EU:n elinten kanssa ja auttaa EU:ta valmistautumaan tulevaisuuden kyberhaasteisiin. Virasto jakaa tietämystä, kehittää valmiuksia ja lisää tietoisuutta sekä tekee yhteistyötä keskeisten sidosryhmiensä kanssa lujittaakseen luottamusta verkottuneeseen talouteen, parantaakseen unionin infrastruktuurin sietokykyä ja ennen kaikkea suojatakseen eurooppalaisen yhteiskunnan ja kansalaisten digitaalista turvallisuutta. ENISAsta ja sen työstä on lisätietoa osoitteessa www.enisa.europa.eu.

TP-02-20-759-FI-N

ENISA
Euroopan unionin kyberturvallisuusvirasto

Ateenan toimisto
1 Vasilissis Sofias Str
151 24 Marousi, Attiki, Kreikka

Heraklionin toimisto
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Kreikka

enisa.europa.eu

ISBN 978-92-9204-358-2