Euroopan komissio

UNIONIN TILA
2018

Vahvan kyberturvallisuuden rakentaminen EU:lle

#SOTEU

12. syyskuuta 2018

”Kyberhyökkäykset eivät tunne rajoja, mutta valmiutemme vastata niihin vaihtelevat suuresti eri maissa. Tämä luo aukkoja, joiden heikkoudet houkuttelevat entistä enemmän hyökkäyksiä. EU:ssa tarvitaan kestävämpiä ja tehokkaampia rakenteita, jotta voidaan vahvistaa kyberhyökkäysten sietokykyä ja reagoida kyberhyökkäyksiin. Emme halua olla heikoimpia lenkkejä vastattaessa tähän maailmanlaajuiseen uhkaan.”

Jean-Claude Juncker, Tallinnan digitaalihuippukokous, 29. syyskuuta 2017

Jotta Euroopalla olisi oikeat välineet vastata alati muuttuvaan kyberuhkaan, Euroopan komissio ja korkea edustaja ehdottivat vuonna 2017 laajaa toimenpidekokonaisuutta vahvan kyberturvallisuuden rakentamiseksi EU:lle. Näitä toimia täydennetään nyt ehdotuksella, joka auttaa EU:ta kokomaan yhteen resursseja ja osaamista tutkimuksen ja innovoinnin alalla ja jonka avulla se pystyy saavuttamaan johtoaseman seuraavan sukupolven kyberturvallisuus- ja digitaaliteknologioissa.

Nykyiset kyberuhat

Yli 4 000 kiristyshaittaohjelmilla tehtyä hyökkäystä päivittäin vuonna 2016

80 % Euroopan yrityksistä koki viime vuonna vähintään yhden kyberturvallisuuspoikkeaman

Tietoturvapoikkeamat lisääntyivät eri toimialoilla **38 %**, mikä on suurin lisäys 12 vuoteen

Joissakin jäsenvaltioissa **50 % kaikista rikoksista** on kyberrikoksia

Toukokuussa 2017 tapahtunut Wannacry-hyökkäys kohdistui **yli 150 maahan ja yli 230 000 tietojärjestelmään** eri aloilla ja sai aikaan laajat vaikutukset internetiin liitetyissä keskeisissä palveluissa, kuten sairaaloissa ja ambulanssipalveluissa.

Kyberhyökkäysten sietokyvyn vahvistaminen

Komissio tukee jo EU:n kyberpelotteen ja kyberhyökkäysten sietokyvyn ja reagointivalmiuksien parantamista muun muassa seuraavin tavoin:

EU:n ensimmäisen kyberturvallisuussäädöksen (verkko- ja tietoturvadirektiivin) tehokkaan täytäntöönpanon tukeminen, mihin sisältyvät:

PAREMMAT VALMIUDET

Jäsenvaltioiden on parannettava kyberturvallisuusvalmiuksiaan.

YHTEISTYÖ

Tiiviimpi EU-tason yhteistyö

RISKIEN EHKÄISEMINEN

Keskeisten alojen toimijoiden on otettava käyttöön toimenpiteitä riskien ehkäisemiseksi ja kyberturvallisuuspoikkeamien käsittelemiseksi

Yhteistyö jäsenvaltioiden kanssa:

EU:N KYBERTURVALLISUUSVIRASTO

Euroopan unionin kyberturvallisuusviraston vahvistaminen, jotta jäsenvaltioita voidaan avustaa paremmin

EU:N SERTIFIOINTIKEHYS

EU:n laajuinen sertifiointikehys, jolla varmistetaan tuotteiden ja palvelujen kyberturvallisuus

KOORDINOITU REAGOINTI

Nopean ja koordinoidun reagoinnin varmistaminen laajamittaisiin kyberhyökkäyksiin

Euroopan unionin verkko- ja tietoturvavirasto (ENISA) avustaa jäsenvaltioiden kyberturvallisuusviranomaisia, jotta EU voi suojautua paremmin kyberhyökkäyksiltä.

Kyberturvallisuusteknologiaan liittyvien resurssien ja osaamisen kokoaminen yhteen

Olemassa olevien kyberturvallisuusaloitteiden lisäksi komissio ehdottaa nyt, että näitä toimia täydennetään perustamalla osaamiskeskusten verkosto ja Euroopan kyberturvallisuuden teollisuus-, teknologia- ja tutkimusosaamiskeskus, jotka auttavat kehittämään ja ottamaan käyttöön välineitä ja teknologiaa, joiden avulla voidaan pysyä alati muuttuvan uhkan tasalla.

Euroopan osaamiskeskus vastaa siitä, että EU:n seuraavassa pitkän aikavälin talousarviossa kyberturvallisuuteen osoitettuja varoja koordinoidaan mahdollisimman hyvin kohdennetulla tavalla yhdessä jäsenvaltioiden kanssa.. Tämä auttaa luomaan uusia eurooppalaisia kybervalmiuksia.

Euroopassa on jo runsaasti alan osaamista, sillä eri puolilla EU:ta on yli **660 kyberturvallisuuden osaamiskeskusta**. Jotta tämä osaaminen saataisiin tehokkaasti käyttöön, komissio ehdottaa mekanismia, jossa

Olemassa oleva osaaminen kootaan yhteen ja jaetaan ja varmistetaan sen saatavuus

Helpotetaan EU:n kyberturvallisuustuotteiden ja -ratkaisujen käyttöönottoa

Varmistetaan pitkäaikainen strateginen yhteistyö teollisuudenalojen, tutkimusyhteisöjen ja hallintojen välillä

Huolehditaan kalliiden infrastruktuurien yhteisistä investoinneista ja yhteisestä käytöstä

Euroopan osaamiskeskus:

Koordinoi niiden varojen käyttöä, jotka on osoitettu kyberturvallisuuteen Digitaalinen Eurooppa -ohjelmassa ja Euroopan horisontti -ohjelmassa EU:n seuraavassa pitkän aikavälin talousarviossa vuosille 2021–2027. Osaamiskeskus tukee verkostoa ja osaamisyhteisöä **kyberturvallisuusalan** teknologian ja innovoinnin edistämiseksi. Se organisoi myös EU:n, jäsenvaltioiden ja teollisuuden **yhteisiä investointeja**. Esimerkiksi Digitaalinen Eurooppa -ohjelmassa investoidaan **2 miljardia euroa** EU:n digitaalisen talouden, yhteiskunnan ja demokratian suojelemiseen vahvistamalla EU:n kyberturvallisuusalaa ja rahoittamalla alan viimeisintä kehitystä edustavia kyberturvallisuuslaitteita ja -infrastruktuuria.

Kansallisten koordinointikeskusten verkosto:

Kukin jäsenvaltio nimeää yhden kansallisen koordinointikeskuksen johtamaan verkostoa, joka osallistuu uusien kyberturvallisuusvalmiuksien ja laajemman osaamisen kehittämiseen. Verkosto auttaa määrittelemään tarkoituksenmukaisimmat kyberturvallisuushankkeet jäsenvaltioissa ja tukee näitä hankkeita.

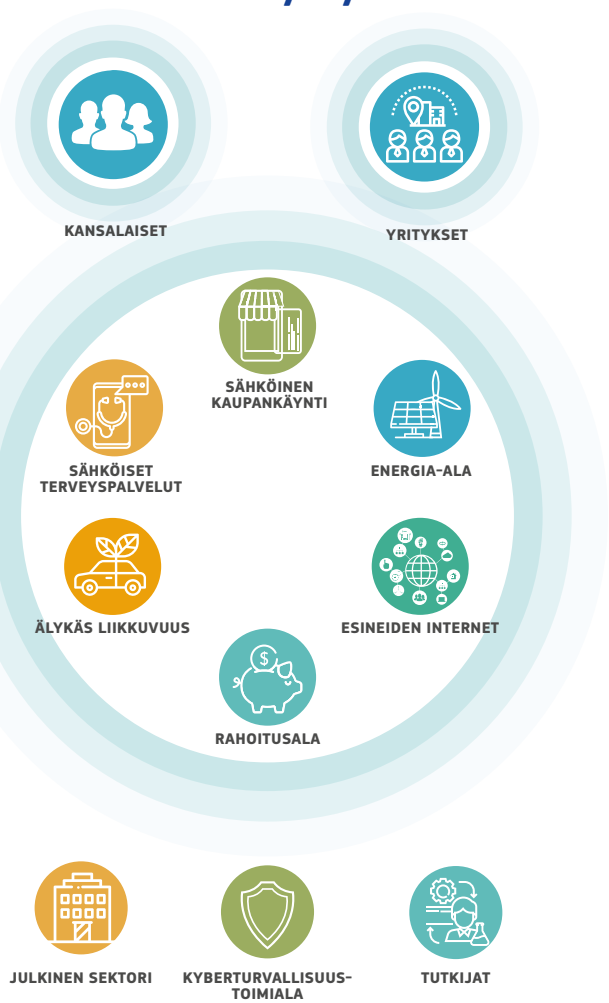
Osaamisyhteisö:

Laaja, avoin ja moninainen joukko kyberturvallisuusalan sidosryhmiä tutkimuksen alalta sekä yksityiseltä ja julkiselta sektorilta, mukaan lukien siviili- ja puolustusviranomaiset.

Mikä paranee?

- toimien koordinointi
- osaamisen saatavuus
- mahdollisuus saada käyttöön testaus- ja kokeilujärjestelyjä
- tuotteiden kyberturvallisuuden arviointi
- innovatiivisten kyberturvallisuustuotteiden ja -ratkaisujen saatavuus
- tuotteiden ja palvelujen markkinoille saattamisen tukeminen
- suurempi näkyvyys mahdollisten investoijien ja liikekumppaneiden suuntaan
- kustannusten säästäminen yhteisillä investoinneilla muiden jäsenvaltioiden kanssa
- EU:n kyky turvata itsenäisesti taloutensa ja demokratiansa
- EU:n asema maailmanlaajuisena johtajana kyberturvallisuuden alalla

Ketkä hyötyvät?



Julkaisutoimisto

Print ISBN 978-92-79-92501-6 doi:10.2775/167357 NA-04-18-693-FI-C
PDF ISBN 978-92-79-92463-7 doi:10.2775/417696 NA-04-18-693-FI-N