



EIROPAS SAVIENĪBAS KIBERDROŠĪBAS AĢENTŪRA

UZTICAMA UN KIBERDROŠA EIROPA

ENISA stratēģija

2020. gada jūnijs



UZTICAMA UN KIBERDROŠA EIROPA

EIROPAS SAVIENĪBAS KIBERDROŠĪBAS AĢENTŪRA



PRIEKŠVĀRDS

Vairāk nekā 15 gadu ES Kiberdrošības aģentūra (ENISA) kopā ar dalībvalstīm un ES iestādēm un aģentūrām ir devusi būtisku ieguldījumu ceļā uz ES vērīgu mērķi pastiprināt digitālo uzticamību un drošību visā Eiropā. ENISA, vienojot kopienas, ir sekmīgi palīdzējusi vairo Eiropas gatavību kiberincidentiem un tās spējas reaģēt uz tiem.

Vienlaikus ir krasi paplašinājusies mūsu ekonomikas un sabiedrības digitalizācija, kā tas pierādījās Covid-19 krīzē, kuras laikā bija būtiski kolektīvi un masveidā sākt izmantot attālinātus IT risinājumus, lai daudzas darbības neapsīktu. Šī krīze izgaismoja to, cik ļoti kibernetiskie izmanto mūsu atkarību no minētajām tehnoloģijām. Tā arī atklāja, kā kibernetiskie draudi ir paplašinājusies no selektīviem uzbrukumiem līdz jaunu veidu milzīgiem draudiem, kas apdraud miljoniem uzņēmumu un iedzīvotāju, tostarp aizvien aug ar sarežģītām izspiedējprogrammatūrām saistītu incidentu skaits. Arī ātrā digitālo produktu un pakalpojumu attīstība, sākot no mākonpakalpojumiem un videokonferencēm un beidzot ar 5G un mākslīgo intelektu, ir nesusi līdzīgas jaunas problēmas, kas vēl jāapzina un jārisina.

Pateicoties savām pastāvīgajām pilnvarām un paplašinātajiem uzdevumiem un spējām, ES Kiberdrošības aģentūrai tagad, kad Eiropā ir sācies jauns kiberdrošības laikmets, ir vēl nepieredzētas iespējas kļūt par vienu no galvenajiem palīgiem ES un tās dalībvalstīm šo problēmu risināšanā.

Šajā nolūkā ENISA darbs būs vērsts uz būtisku tendenču prognozēšanu un jaunāko kompetenču un zināšanu piesaistīšanu un kopīgošanu ar visiem. Tā palīdzēs

Eiropas Komisijai un dalībvalstīm sniegt atbalstu publiskā un privātā sektora dalībniekiem un iedzīvotājiem ar kiberincidentiem saistītu risku novēršanā un pārvaldīšanā. Ar kiberdrošības sertifikācijas satvara ieviešanu ENISA veicinās paradigmas maiņu, paaugstinot Eiropā izmantoto digitālo risinājumu drošības līmeni. Tādējādi tā vairo visu izvēles iespējas un uzticēšanos. Aģentūra arī aktīvi atbalstīs Eiropas kiberdrošības operatīvo dalībnieku kopienas, cieši sadarbojoties ar to un gatavojoties kopīgi reaģēt uz nākamo plašāpmēra kiberincidentu Eiropā, kad tāds notiks.

ENISA savu jauno pienākumu izpildē ļoti svarīga būs atklātība, izveicība un uzticamība ikdienas darbībā, un tā ciešāk sadarbosies ar dalībvalstīm un Eiropas Komisiju, lai saskaņotu pieeju. ENISA arī centīsies mazināt savu ietekmi uz vidi, ņemot vērā pašreizējo klimata krīzi, un būt sociāli atbildīga darbavieta ar iekļaujošu darba vidi.

Šajā stratēģijas dokumentā, kurš tika izstrādāts iekļaujošā sadarbības procesā, piedaloties visiem ENISA darbiniekiem un tās Administratīvās padomes un Padomdevēju grupas locekļiem, ir skaidri izklāstīti mērķi, uz kuriem būs virzīts ENISA darbs nākamajos gados, lai stātos pretī daudzajām gaidāmajām problēmām.

Administratīvās padomes vārdā

Jean-Baptiste Demaison

Administratīvās padomes priekšsēdētājs

Krzysztof Silicki

Administratīvās padomes priekšsēdētāja vietnieks

REDZĒJUMS

Uzticama un kiberdroša Eiropa

UZDEVUMS

Eiropas Savienības Kiberdrošības aģentūras (ENISA) uzdevums ir, sadarbojoties ar plašāku dalībnieku loku, panākt vienādi augstu kiberdrošības līmeni visā Savienībā. Tā šo uzdevumu veic, būdama kiberdrošības kompetences centrs, kas piesaista un nodrošina dalībvalstīm un ES struktūrām neatkarīgas augstas kvalitātes tehniskās konsultācijas un palīdzību kiberdrošības jomā. Tā dod ieguldījumu Savienības kiberdrošības politikas izstrādē un īstenošanā.

Mūsu mērķis ir vairogt uzticību satiklotai ekonomikai, palielināt Savienības infrastruktūras noturību un uzticamību un garantēt mūsu sabiedrībai un iedzīvotājiem digitālo drošību. Mēs vēlamies būt sociālā un vides jomā atbildīga organizācija, kura spēj ātri reaģēt un kuras darbības centrā ir cilvēki.

VĒRTĪBAS

Orientācija uz kopienu

ENISA strādā ar kopienām, ievērojot to kompetenci un speciālās zināšanas, un vairo sinerģiju un uzticību, lai paveiktu savu uzdevumu pēc iespējas labāk.

Izcilība

ENISA mērķis ir savā darbā izmantot visjaunākās speciālās zināšanas, tā strādā pēc visaugstākajiem kvalitātes standartiem un izvērtē savus darbības rezultātus, lai censtos nepārtraukti uzlabot savu darbību ar inovācijām un nākotnes prognozēm.

Godprātība/ētika

ENISA savos pakalpojumos un darba vidē ievēro ētikas principus un attiecīgos ES noteikumus un saistības, nodrošinot taisnīgumu un iekļautību.

Cieņa

ENISA ievēro Eiropas pamattiesības un pamatvērtības visos savos pakalpojumos un darba vidē, kā arī savu ieinteresēto personu gaidas.

Atbildība

ENISA uzņemas atbildību, tādējādi nodrošinot sociālo un vides jautājumu iekļaušanu savā praksē un procedūrās.

Pārredzamība

ENISA izmanto tādas procedūras, struktūras un procesus, kas ir atklāti, faktos balstīti un neatkarīgi, tādējādi ierobežojot neobjektivitāti, neviennozīmību, krāpšanu un necaurredzamību.

STRATĒĢISKIE MĒRĶI



1. SM

Stratēģiskais mērķis

“

AR LIELĀM IESPĒJĀM APVELTĪTAS
UN LĪDZDALĪGAS KOPIENAS
VISĀ KIBERDROŠĪBAS
EKOSISTĒMĀ

Konteksts

Atbildība par kiberdrošību jāuzņemas visiem kopā. Eiropa cenšas ieviest visaptverošu pārnozaru sadarbības sistēmu. ES Kiberdrošības aģentūrai ir būtiska nozīme aktīvas sadarbības stimulēšanā starp kiberdrošībā ieinteresētajām personām dalībvalstīs un ES iestādēm un aģentūrām. Tā cenšas nodrošināt kopīgo centienu papildināmību, radot ieinteresētajām personām pievienoto vērtību, pētot sinerģijas iespējas un efektīvi izmantojot ierobežotos kiberdrošības resursus un ekspertus. Būtu jādod kopienām iespējas izvērst kiberdrošības modeli.

Ko mēs vēlamies panākt

- Mūsdienīgu ES mēroga zināšanu korpusu par kiberdrošības koncepcijām un praksi, kurš veicina sadarbību starp galvenajiem kiberdrošības jomas dalībniekiem, izplata gūtās atziņas un ES speciālās zināšanas un rada jaunas sinerģijas.
- Plašām iespējām apveltītu kiberdrošības ekosistēmu, kas aptver dalībvalstu iestādes, ES iestādes, aģentūras un struktūras, apvienības, pētniecības centrus un universitātes, attiecīgās nozares dalībniekus, privātā sektora dalībniekus un iedzīvotājus, kuri visi sniedz ieguldījumu kiberdrošības panākšanā Eiropā.

2. SM

Stratēģiskais mērķis

“

KIBERDROŠĪBA
KĀ NEATŅEMAMA ES
POLITIKAS DAĻA

Konteksts

Kiberdrošība ir digitālās pārveides stūrakmens un ir vajadzīga visās nozarēs, tāpēc tā ir jāņem vērā daudzās dažādās politikas jomās un iniciatīvās. Kiberdrošības jautājuma risināšanu nedrīkst uzticēt tikai atsevišķai specializētai kopienai — tehniskajiem kiberdrošības ekspertiem, kiberdrošības jautājums ir jāiekļauj visās ES politikas jomās. Ir būtiski izvairīties no sadrumstalotības un izmantot saskaņotu pieeju, tai pašā laikā ņemot vērā katras nozares specifiku.

Ko mēs vēlamies panākt

- Ar praktiski izmantojamām un mērķorientētām tehniskām pamatnostādnēm sniegt proaktīvus padomus un atbalstu visiem attiecīgajiem ES līmeņa dalībniekiem, kas iekļauj kiberdrošības jautājumu politikas izstrādes aprites ciklā.
- Kiberdrošības riska pārvaldības satvarus, kas ir ieviesti visās nozarēs un ko ievēro visā kiberdrošības politikas aprites ciklā.

3. SM

Stratēģiskais mērķis

“

REZULTATĪVA SADARBĪBA STARP
OPERATĪVAJIEM DALĪBNIEKIEM
SAVIENĪBĀ ĀRKĀRTĪGI LIELU
KIBERINCIDENTU GADĪJUMĀ

Konteksts

Eiropas digitālās ekonomikas un sabiedrības sniegtos labumus var pilnvērtīgi izmantot tikai tad, ja ir panākta kiberdrošība. Kiberuzbrukumiem robežu nav. Tie var skart visus sabiedrības slāņus, un Savienībai jābūt gatavai reaģēt uz ārkārtīgi lieliem (plašapmēra un pārrobežu) kiberuzbrukumiem un kiberkrīzi. Savstarpējā pārrobežu atkarība ir likusi apzināties vajadzību pēc rezultatīvas sadarbības starp dalībvalstīm un ES iestādēm, lai varētu ātrāk reaģēt un pienācīgi koordinēt centienus visos līmeņos (stratēģiskajā, operatīvajā, tehniskajā un komunikācijas līmenī).

Ko mēs vēlamies panākt

- Pāri valstu un slāņu robežām sniegt pastāvīgu atbalstu dalībvalstu savstarpējai sadarbībai un to sadarbībai ar ES iestādēm. Jo īpaši, ņemot vērā iespējamus plašapmēra incidentus un krīzes, atbalstīt svarīgāko operatīvo dalībnieku savstarpējās tehniskās, operatīvās, politiskās un stratēģiskās sadarbības izvērsšanu, lai visā Savienībā varētu laikus reaģēt, apmainīties ar informāciju, apzināties situāciju un komunicēt krīžu laikā.
- Pēc dalībvalstu pieprasījuma visaptveroši un ātri risināt tehniskos jautājumus, lai palīdzētu apmierināt tehniskās un operatīvās vajadzības incidentu un krīžu pārvaldības jomā.

4. SM

Stratēģiskais mērķis

“

MODERNĀKĀS KOMPETENCES
UN IESPĒJAS KIBERDROŠĪBAS
JOMĀ VISĀ SAVIENĪBĀ

Konteksts

Kiberuzbrukumu biežums un sarežģītība strauji palielinās, bet tai pašā laikā ātri pieaug arī IKT infrastruktūru un tehnoloģiju izmantojums fizisku personu vidū, organizācijās un nozarēs. Pieprasījums pēc kiberdrošības jomas zināšanām un kompetencēm pārsniedz piedāvājumu. ES ir jāiegulda kompetenču un talantu vairošanā kiberdrošības jomā visos līmeņos, sākot ar darbiniekiem, kas nav eksperti, un beidzot ar augsti kvalificētiem speciālistiem. Ieguldījumi būtu jāvērs ne tikai uz kiberdrošības prasmju kopuma paplašināšanu dalībvalstīs, bet arī uz to, lai nodrošinātu, ka dažādajām operatīvajām kopienām ir pietiekamas spējas, lai tiktu galā ar visu kiberdraudu klāstu.

Ko mēs vēlamies panākt

- Saskaņotas kompetences, profesionālo pieredzi un izglītības struktūras kiberdrošības jomā, lai apmierinātu arvien augošās vajadzības pēc zināšanām un kompetencēm kiberdrošības jomā ES.
- Paaugstinātu kiberdrošības izpratnes un kompetenču pamatlīmeni visā ES un tai pašā laikā kiberdrošības jautājuma iekļaušanu jaunās disciplīnās.
- Pamatīgas un pārbaudītas spējas un pietiekamas iespējas tikt galā ar mainīgajiem draudiem visā ES.

5. SM

Stratēģiskais mērķis

“

AUGSTA LĪMENA
UZTICĪBA DROŠIEM
DIGITĀLAJIEM
RISINĀJUMIEM

Konteksts

Digitālie produkti un pakalpojumi rada gan ieguvumus, gan riskus, un šie riski ir jāapzina un jāmazina. Izvērtējot digitālo risinājumu drošību un raugoties, lai tie būtu uzticami, ir būtiski izmantot vienotu pieeju, lai panāktu līdzsvaru starp sabiedrības, tirgus, ekonomiskajām un kibernetikas vajadzībām. Neitrāla struktūra, kas darbojas pārredzami, vairo klientu uzticību digitālajiem risinājumiem un digitālajai videi kopumā.

Ko mēs vēlamies panākt

- Ieviešot sertifikācijas shēmas svarīgākajās tehnoloģiju jomās, izveidot visā ES kibernetikas digitālo vidi, kurā iedzīvotāji var uzticēties IKT produktiem, pakalpojumiem un procesiem.

6. SM

Stratēģiskais mērķis

“

PROGNOZES PAR
JAUNAJĀM UN GAIDĀMAJĀM
KIBERDROŠĪBAS
PROBLĒMĀM

Konteksts

Daudzām jaunām tehnoloģijām, kas vēl ir attīstības sākumposmā vai drīz tiks ieviestas plašā lietošanā, būtu vērtīgi piemērot prognozēšanas metodes. Strukturētā procesā, kurā varētu notikt dialogs starp ieinteresētajām personām, lēmumu pieņēmējiem un politikas veidotājiem, varētu noteikt agrīnas risku mazināšanas stratēģijas, kas uzlabotu ES noturību pret kibernetikas draudiem, un rast risinājumus jaunu problēmu novēršanai.

Ko mēs vēlamies panākt

- Izprast jaunas tendences un modeļus, izmantojot prognozēšanu un nākotnes scenārijus, kas palīdzētu mazināt ar kibernetiku saistītās problēmas, ar kurām varētu saskarties mūsu ieinteresētās personas.
- Agrīni novērtēt problēmas un riskus, kas varētu rasties, izmantojot gaidāmās nākotnes iespējas un pielāgojoties tām, un tai pašā laikā sadarboties ar ieinteresētajām personām, lai nonāktu pie atbilstīgām problēmu un risku mazināšanas stratēģijām.

7. SM

Stratēģiskais mērķis

“

EFEKTĪVA UN LIETDERĪGA
KIBERDROŠĪBAS JOMAS
INFORMĀCIJAS UN ZINĀŠANU
PĀRVALDĪBA EIROPAS LABĀ

Konteksts

Energija, kas griež kibernetikas ratu, ir informācija un zināšanas. Lai kibernetikas speciālisti varētu efektīvi sasniegt mūsu mērķus, strādāt vienmēr mainīgā vidē, kurā gan attīstās digitālā joma, gan mainās dalībnieki, stāties pretī mūsdienās aktuālajām problēmām, ir pastāvīgi jāvēl, jāorganizē, jāapkopo, jāanalizē, jāziņo un jāuztur kibernetikas informācija un zināšanas. Lai nodrošinātu, ka informāciju un zināšanas kopīgo un izvērs ES kibernetikas ekosistēmā, ir būtiski īstenot visus minētos posmus.

Ko mēs vēlamies panākt

- ES kibernetikas ekosistēmā nodrošināt pieejamu, pielāgotu, savlaicīgu un praktiski īstenojamu kopīgotas informācijas un zināšanu pārvaldību, kam būtu atbilstīga metodika, infrastruktūra un rīki, savienotās un kvalitātes nodrošināšanas metodes, lai pakalpojumus varētu pastāvīgi uzlabot.



PAR ENISA

Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) ir Savienības aģentūra, kuras mērķis ir visā Eiropā panākt vienādi augstu kiberdrošības līmeni. 2004. gadā dibinātā un ar ES Kiberdrošības aktu nostiprinātā Eiropas Savienības Kiberdrošības aģentūra sniedz ieguldījumu ES kiberdrošības politikā, vairo IKT produktu, pakalpojumu un procesu uzticamību ar kiberdrošības sertifikācijas shēmām, sadarbojas ar dalībvalstīm un ES struktūrām un palīdz Eiropai sagatavoties nākotnes izaicinājumiem kiberdrošības jomā. Aģentūra sadarbojas ar savām galvenajām ieinteresētajām personām, daloties zināšanās, veidojot spējas un veicinot izpratni, lai vairotu uzticību satīklotajai ekonomikai, palielinātu Savienības infrastruktūras noturību un galu galā garantētu Eiropas sabiedrībai un iedzīvotājiem digitālo drošību. Sīkāka informācija par *ENISA* un tās darbu ir sniegta tīmekļa vietnē www.enisa.europa.eu.



ENISA

Eiropas Savienības Kiberdrošības aģentūra

Birojs Atēnās

1 Vasilisis Sofias Str

151 24 Marousi, Attiki, Grieķija

Birojs Hēraklejā

95 Nikolaou Plastira

700 13 Vassilika Vouton, Heraklion, Grieķija

enisa.europa.eu

