EUROPOS SĄJUNGOS KIBERNETINIO SAUGUMO AGENTŪRA

# PATIKIMA IR KIBERNETIŠKAI SAUGI EUROPA

## ENISA strategija

2020 m. birželis

# PATIKIMA IR KIBERNETIŠKAI SAUGI EUROPA

EUROPOS SĄJUNGOS KIBERNETINIO SAUGUMO AGENTŪRA

# PRATARMĖ

**Daugiau nei 15 metų ENISA – ES kibernetinio saugumo agentūra – drauge su valstybėmis narėmis ir ES institucijomis bei agentūromis atlieka pagrindinį vaidmenį sudarydama sąlygas ES siekti plataus masto tikslų, susijusių su skaitmeninio pasitikėjimo ir saugumo visoje Europoje stiprinimu. Suvienijusi bendruomenes, ENISA sėkmingai prisidėjo prie geresnės Europos parengties ir stipresnių gebėjimų reaguoti į kibernetinius incidentus.**

Tuo pat metu drastiškai padidėjo mūsų ekonomikos ir visuomenės skaitmeninimas – tai paaiškėjo per COVID-19 krizę, kai kolektyvinis ir masinis naudojimasis nuotoliniais IT sprendimo būdais buvo esminis veiksnys, nulėmęs pačios įvairiausios veiklos tęstinumą. Ši krizė išryškino, kokiu mastu kibernetiniai užpuolikai pasinaudoja mūsų priklausomybe nuo šių technologijų. Ji taip pat atskleidė išsiplėtusį kibernetinių grėsmių spektrą, kuris apima tiek tikslinius išpuolius, tiek naujos formos masines grėsmes milijonams įmonių ir piliečių, įskaitant didėjantį sudėtingų incidentų naudojant išpirkos reikalavimo programinę įrangą skaičių. Dėl sparčios skaitmeninių produktų ir paslaugų plėtros, pradedant debesija ir vaizdo konferencijomis ir baigiant 5G ir dirbtiniu intelektu, taip pat kilo naujų sunkumų, susijusių su trūkumų nustatymu ir šalinimu.

Atsižvelgiant į ENISA nuolatinius įgaliojimus ir įvairiapusiškesnes užduotis bei gebėjimus, ji kaip niekad anksčiau turi imtis pagrindinio vaidmens padėdama ES ir jos valstybėms narėms spręsti šiuos sunkumus artėjant naujai kibernetinio saugumo erai Europoje.

Kad tai padarytų, ENISA imsis veiksmų siekdama numatyti atitinkamas tendencijas, rinks ir su visais subjektais dalysis naujausia patirtimi ir žiniomis. Ji rems Europos Komisiją ir valstybes nares, padėdama viešiems ir privatiems dalyviams ir piliečiams užkirsti kelią su kibernetiniais incidentais susijusiai rizikai ir ją valdyti. Įgyvendindama kibernetinio saugumo sertifikavimo sistemą, ENISA didins Europoje įdiegtų skaitmeninių sprendimo būdų saugumo lygį ir taip padės pakeisti paradigmą. Tai darydama ENISA didins visų dalyvių gebėjimą pasirinkti ir pasitikėjimą. Glaudžiai bendradarbiaudama ir pasirengdama kartu reaguoti į kitą didelio masto kibernetinį incidentą Europoje, agentūra taip pat aktyviai rems Europos kibernetinio saugumo operatyvinę bendruomenę.

ENISA imantis savo naujo vaidmens, atvirumas, gyvybingumas ir patikimumas bus pagrindiniai jos kasdienės veiklos aspektai, be to, agentūra glaudžiau bendradarbiaus su valstybėmis narėmis ir Europos Komisija, kad suderintų požiūrį. Atsižvelgdama į dabartinę klimato krizę, ENISA taip pat stengsis siekti geresnio poveikio aplinkai, būti socialiai atsakinga ir užtikrinti įtraukią darbo aplinką.

Šiame strategijos dokumente, kuris parengtas taikant bendradarbiavimu grindžiamą ir įtraukų procesą, kuriame dalyvavo visi ENISA darbuotojai, jos valdančiosios tarybos nariai ir jos patariamoji grupė, nustatyti aiškūs uždaviniai, kurie artimiausiais metais nulems ENISA darbo kryptis siekiant įveikti daugybę būsimų iššūkių.

Valdančiosios tarybos vardu

**Jean-Baptiste Demaison**
Valdančiosios tarybos pirmininkas

**Krzysztof Silicki**
Valdančiosios tarybos pirmininko pavaduotojas

# VIZIJA

**Patikima ir kibernetiškai saugi Europa**

# MISIJA

Europos Sąjungos kibernetinio saugumo agentūros (ENISA) misija – pasiekti aukštą bendrą kibernetinio saugumo lygį visoje Sąjungoje šiuo tikslu bendradarbiaujant su platesne bendruomene. Ji tai daro veikdama kaip kibernetinio saugumo kompetencijos centras, rinkdama ir teikdama valstybėms narėms ir ES įstaigoms nepriklausomas, kokybiškas technines konsultacijas ir pagalbą kibernetinio saugumo klausimais. Agentūra prisideda prie Sąjungos kibernetinės politikos rengimo ir įgyvendinimo.

Mūsų tikslas – stiprinti pasitikėjimą sujungtos ekonomikos sąlygomis, didinti Sąjungos infrastruktūros ir paslaugų atsparumą ir pasitikėjimą jomis ir išlaikyti mūsų visuomenės ir piliečių skaitmeninį saugumą. Siekiame būti gyvybinga, aplinkos ir socialiniu požiūriu atsakinga ir į žmones orientuota organizacija.

# VERTYBĖS

**Bendruomeniška mąstysena**
ENISA dirba su bendruomenėmis, gerbia jų kompetenciją ir patirtį, ir skatina sinergiją bei pasitikėjimą, kad kuo geriau vykdytų savo misiją.

**Kompetencija**
ENISA savo darbe siekia vadovautis naujausia patirtimi, laikosi aukščiausių veiklos kokybės standartų ir, pasitelkdama inovacijas ir įžvalgas, įvertina savo veiklos rezultatus siekdama nuolat tobulėti.

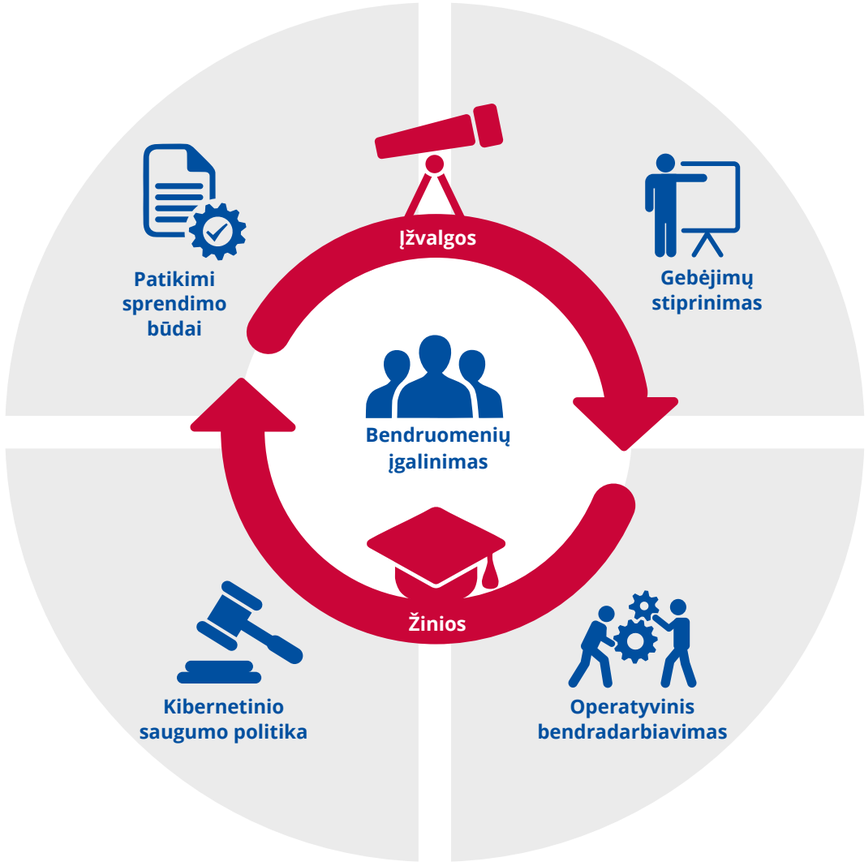
**Sąžiningumas ir etika**
ENISA laikosi etikos principų ir atitinkamų ES taisyklių ir pareigų ir užtikrina, kad teikiamos paslaugos ir darbo aplinka būtų sąžiningos ir įtraukios.

**Pagarba**
ENISA gerbia pagrindines Europos teises ir vertybes, susijusias su visomis jos paslaugomis ir darbo aplinka, taip pat paiso savo suinteresuotųjų subjektų lūkesčių.

**Atsakomybė**
ENISA prisiima atsakomybę ir taip užtikrina socialinių ir aplinkos aspektų integravimą į praktiką ir procedūras.

**Skaidrumas**
ENISA nustato atviras, faktines ir nepriklausomas procedūras, struktūrą ir procesus ir taip riboja galimybes atsirasti šališkumui, dviprasmiškumui, sukčiavimui ir neaiškumui.

# STRATEGINIAI UŽDAVINIAI



# SU 1

## Strateginis uždavinys

# ĮGALINTOS IR BENDRADARBIAUJANČIOS BENDRUOMENĖS KIBERNETINIO SAUGUMO EKOSISTEMOJE

## Aplinkybės

Kibernetinis saugumas yra bendros atsakomybės sritis. Europa stengiasi sukurti tarpsektorinę bendradarbiavimo sistemą, kurioje dalyvautų visi dalyviai. ENISA atlieka pagrindinį vaidmenį skatindama aktyvų kibernetinio saugumo suinteresuotųjų subjektų bendradarbiavimą valstybėse narėse ir ES institucijose bei agentūrose. Ji stengiasi užtikrinti bendrų pastangų papildomumą sukurdama vertę suinteresuotiesiems subjektams, nagrinėdama sinergiją ir veiksmingai panaudodama ribotą patirtį ir išteklius kibernetinio saugumo srityje. Bendruomenes reikėtų įgalinti, kad jos prisitaikytų prie kibernetinio saugumo modelio.

## Ką norime pasiekti?

- Mūsų tikslas – ES masto naujausios žinios apie kibernetinio saugumo koncepcijas ir praktiką, kuriomis grindžiamas pagrindinių kibernetinio saugumo srities dalyvių bendradarbiavimas, skatinama įgyta patirtis, ES kompetencija ir sukuriamos naujos sinergijos sritys.
- Siekiame sukurti įgalintą kibernetinę ekosistemą, kuri apima valstybių narių institucijas, ES institucijas, agentūras ir įstaigas, asociacijas, mokslinių tyrimų centrus ir universitetus, pramonę, privačius dalyvius ir piliečius, kurie visi atlieka savo vaidmenį užtikrinant Europos kibernetinį saugumą.

# SU 2

## Strateginis uždavinys

# KIBERNETINIS SAUGUMAS KAIP SUDEDAMOJI ES POLITIKOS DALIS

## Aplinkybės

Kibernetinis saugumas yra kertinis skaitmeninės transformacijos pagrindas ir toks saugumas reikalingas visuose sektoriuose, todėl į jį reikia atsižvelgti pačiose įvairiausiose politikos srityse ir iniciatyvose. Kibernetinis saugumas negali apimti tik specializuotos techninių kibernetinių ekspertų bendruomenės. Todėl kibernetinis saugumas turi būti integruotas į visas ES politikos sritis. Fragmentiškumo vengimas yra tiek pat svarbus kaip ir poreikis užtikrinti nuoseklų požiūrį kartu atsižvelgiant į kiekvieno sektoriaus ypatumus.

## Ką norime pasiekti?

- Užtikrinti aktyvias konsultacijas ir paramą visiems ES lygmens dalyviams, kurie kibernetinio saugumo aspektą į politikos formavimo gyvavimo ciklą integruoja pasitelkdami patikimas ir tikslines technines gaires.
- Sukurti kibernetinio saugumo rizikos valdymo sistemas, kurios veiktų visuose sektoriuose ir kurių būtų paisoma per visą kibernetinio saugumo politikos gyvavimo ciklą.

# SU 3

## Strateginis uždavinys

# VEIKSMINGAS OPERATYVINIŲ DALYVIŲ BENDRADARBIAVIMAS SĄJUNGOJE MASINIŲ KIBERNETINIŲ INCIDENTŲ ATVEJU

## Aplinkybės

Europos skaitmeninės ekonomikos ir visuomenės privalumus galima visapusiškai pasiekti tik užtikrinus kibernetinį saugumą. Kibernetiniai išpuoliai vykdomi nepaisant sienų. Poveikis gali būti daromas visoms visuomenės grupėms ir Sąjunga turi būti pasirengusi reaguoti į masinius (didelio masto ir tarpvalstybinius) kibernetinius išpuolius ir kibernetinę krizę. Tarpvalstybinė tarpusavio priklausomybė išryškino veiksmingo valstybių narių ir ES institucijų bendradarbiavimo poreikį siekiant greičiau reaguoti ir tinkamai koordinuoti pastangas visais lygmenimis (strateginiu, operatyviniu, techniniu ir komunikacijų).

## Ką norime pasiekti?

- Keliais lygmenimis teikti nuolatinę tarpvalstybinę paramą valstybėms narėms bendradarbiaujant tarpusavyje ir su ES institucijomis. Visų pirma atsižvelgiant į galimus didelio masto incidentus ir krizes, teikti paramą didinant pagrindinių operatyvinių dalyvių techninį operatyvinį, politinį ir strateginį bendradarbiavimą, siekiant sudaryti galimybes laiku reaguoti, dalytis informacija, didinti informaciją apie situaciją ir užtikrinti komunikaciją visoje Sąjungoje krizės metu.
- Vykdyti visapusišką ir greitą techninę priežiūrą valstybių narių prašymu siekiant lengviau patenkinti techninius ir operatyvinius poreikius, susijusius su incidentų ir krizių valdymu.

# SU 4

## Strateginis uždavinys

# PAŽANGIOJI KIBERNETINIO SAUGUMO SRITIES KOMPETENCIJA IR GEBĖJIMAI VISOJE SĄJUNGOJE

## Aplinkybės

Kibernetinių išpuolių dažnumas sparčiai didėja ir jie tampa vis sudėtingesni, tuo pačiu IRT infrastruktūra ir technologijomis vis dažniau naudojasi asmenys, organizacijos ir pramonės įmonės. Kibernetinio saugumo žinių ir kompetencijos poreikis viršija pasiūlą. ES turi investuoti stiprindama kibernetinio saugumo visais lygmenimis kompetenciją ir gabumus, pradedant ne specialistais ir baigiant ypač įgudusiais profesionalais. Investicijos turėtų būti orientuotos ne tik į kibernetinio saugumo įgūdžių rinkinio didinimą valstybėse narėse. Jomis taip pat reikėtų užtikrinti, kad įvairios operatyvinės bendruomenės turėtų tinkamus pajėgumus atsižvelgti į kibernetinės grėsmės aplinkybes.

## Ką norime pasiekti?

- Suderinti kibernetinio saugumo kompetenciją, profesionalią patirtį ir švietimo struktūras, kurios atitiktų nuolat didėjančią kibernetinio saugumo žinių ir kompetencijos Europos Sąjungoje paklausą.
- Siekti didesnio bazinio informuotumo apie kibernetinį saugumą lygį ir didesnės kompetencijos Europos Sąjungoje, kartu integruojant kibernetinį aspektą į naujas disciplinas.
- Turėti geros parengties ir ištestuotus gebėjimus, įskaitant tinkamą gebėjimą spręsti su kintančia grėsme susijusius klausimus visoje Europos Sąjungoje.

# SU 5

## Strateginis uždavinys

“

# DIDELIS PASITIKĖJIMAS SAUGIAIS SKAITMENINIAIS SPRENDIMO BŪDAIS

## Aplinkybės

Skaitmeniniai produktai ir paslaugos suteikia privalumus ir kelia riziką, kurią būtina nustatyti ir sumažinti. Skaitmeninių sprendimo būdų saugumo vertinimo ir jų patikimumo užtikrinimo proceso metu labai svarbu priimti bendrą požiūrį, kuriuo būtų siekiama nustatyti visuomenės, rinkos, ekonomikos ir kibernetinio saugumo poreikių pusiausvyrą. Neutralus ir skaidrus subjektų elgesys padidins klientų pasitikėjimą skaitmeniniais sprendimo būdais ir platesne skaitmenine aplinka.

## Ką norime pasiekti?

- Sukurti kibernetiniu požiūriu saugią skaitmeninę aplinką visoje Europos Sąjungoje, kurioje piliečiai galėtų pasitikėti IRT produktais, paslaugomis ir procesais šiuo tikslu pagrindinėse technologinėse srityse diegiant sertifikavimo schemas.

# SU 6

## Strateginis uždavinys

“

SU NAUJAIS IR BŪSIMAIS KIBERNETINIO SAUGUMO IŠŠŪKIAIS SUSIJUSIOS ĮŽVALGOS

## Aplinkybės

Įžvalgų metodų naudojimas būtų naudingas įvairioms naujoms technologijoms, kurios dar tik pradedamos kurti arba jau yra parengtos diegti plačiu mastu. Pasitelkdami suinteresuotųjų subjektų dialogą įgalinantį struktūrizuotą procesą, sprendimų priėmėjai ir politikos formuotojai turėtų sugebėti apibrėžti ankstyvas rizikos mažinimo strategijas, kurios padidina ES atsparumą kibernetinio saugumo grėsmėms, ir rasti sprendimo būdus, padedančius spręsti naujus iššūkius.

## Ką norime pasiekti?

- Suprasti naujas tendencijas ir būdus pasinaudojant įžvalgomis ir ateities scenarijais, kurie padeda sušvelninti mūsų suinteresuotiesiems subjektams kylančius kibernetinius iššūkius.
- Atlikti ankstyvą iššūkių ir rizikos, kylančių diegiant ir pritaikant naujas ateities alternatyvas, analizę ir bendradarbiauti su suinteresuotaisiais subjektais rengiant rizikos mažinimo strategijas.

# SU 7

## Strateginis uždavinys

# VEIKSMINGAS IR EFEKTYVUS KIBERNETINIO SAUGUMO INFORMACIJOS IR ŽINIŲ VALDYMAS EUROPOJE

## Aplinkybės

Informacija ir žinios – tai esminiai kibernetinio saugumo elementai. Kad kibernetinio saugumo specialistai galėtų veiksmingai siekti mūsų uždavinių, dirbti nuosekliai kintančioje aplinkoje, atsižvelgiant į skaitmeninius pokyčius ir dalyvius, įveikti mūsų laikmečio iššūkius, turime užtikrinti nuolatinį kibernetinio saugumo informacijos ir žinių rinkimo, organizavimo, apibendrinimo, analizavimo, perdavimo ir išlaikymo procesą. Visi etapai yra labai svarbūs siekiant užtikrinti, kad informacija ir žiniomis būtų dalijamasi ir kad jos būtų plečiamos ES kibernetinio saugumo ekosistemoje.

## Ką norime pasiekti?

- Bendrai valdyti informaciją ir žinias ES kibernetinio saugumo ekosistemai prieinama, pritaikyta ir tinkama forma bei laiku, naudojant atitinkamą metodiką, infrastruktūrą ir priemones, įskaitant kokybės užtikrinimo metodus, kad teikiamos paslaugos nuolat tobulėtų.

## APIE ENISA

Europos Sąjungos kibernetinio saugumo agentūra (ENISA) yra Sąjungos agentūra, kurios tikslas – pasiekti bendrą aukštą kibernetinio saugumo lygį visoje Europoje. Europos Sąjungos kibernetinio saugumo agentūra, įkurta 2004 m. ir sustiprinta ES kibernetinio saugumo aktu, prisideda prie ES kibernetinės politikos, didina IRT produktų, paslaugų ir procesų, kuriuose naudojamos kibernetinio saugumo sertifikavimo schemos, patikimumą, bendradarbiauja su valstybėmis narėmis ir ES įstaigomis ir padeda Europai pasirengti būsimiems kibernetiniams iššūkiams. Dalydamasi žiniomis, stiprindama gebėjimus ir didindama informuotumą, agentūra dirba kartu su savo pagrindiniais suinteresuotaisiais subjektais, siekdama stiprinti pasitikėjimą sujungta ekonomika, didinti Sąjungos infrastruktūros atsparumą, užtikrinti Europos visuomenės ir piliečių skaitmeninį saugumą. Daugiau informacijos apie ENISA ir jos darbą galima rasti internete www.enisa.europa.eu.

TP-02-20-759-LT-N

**ENISA**
Europos Sąjungos kibernetinio saugumo agentūra

**Biuras Atėnuose**
1 Vasilissis Sofias Str
151 24 Marousi, Atika, Graikija

**Biuras Heraklione**
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklionas, Graikija

enisa.europa.eu