



SAJUNGOS
PADĖTIS
2018



Europos kibernetinio saugumo didinimas

#SOTEU

2018 m. rugsėjo 12 d.

„Kibernetinių išpuolių nesustabdo sienos, tačiau reagavimo pajėgumai įvairiose valstybėse labai skiriasi ir taip atsiranda spragų, kai dėl silpnųjų grandžių dar labiau padidėja išpuolių grėsmė. ES reikia tvirtesnių ir veiksmingesnių struktūrų, kurios užtikrintų didesnę kibernetinį atsparumą ir reagavimą į kibernetinius išpuolius. Esant šiai pasaulinei grėsmei nenorime būti silpniausia grandis.“

Jeanas-Claude'as Junckeris, Talino aukščiausiojo lygio susitikimas skaitmeniniais klausimais, 2017 m. rugsėjo 29 d.



Siekdamos, kad Europa turėtų tinkamų priemonių apsiginti nuo nuolat kintančios kibernetinės grėsmės, 2017 m. Europos Komisija ir vyriausioji įgaliotinė pasiūlė įvairių ES kibernetinio saugumo stiprinimo priemonių rinkinį. Šias pastangas dabar papildo pasiūlymas, padėsiantis ES sutelkti išteklius ir praktinę patirtį mokslinių tyrimų bei inovacijų srityje ir tapti naujos kartos kibernetinio saugumo ir skaitmeninių technologijų srities lydere.

Dabartinės kibernetinės grėsmės



2016 m. per dieną buvo įvykdoma **daugiau kaip 4 000 išpuolių naudojant išpirkos reikalaujančią programinę įrangą.**



80 proc. Europos bendrovių praėjusiais metais patyrė bent vieną kibernetinio saugumo incidentą.



Saugumo incidentų skaičius visose pramonės šakose **išaugo 38 proc.** – tai didžiausias augimo mastas per pastaruosius 12 metų.



Kai kuriose valstybėse narėse kibernetiniai nusikaltimai sudaro **50 proc. visų padarytų nusikaltimų.**



Per 2017 m. gegužės mėn. įvykdytą išpuolį „Wannacry“ nukentėjo **daugiau kaip 150 šalių ir per 230 000** įvairiuose sektoriuose ir šalyse veikiančių **sistemų** – reikšmingas poveikis padarytas prie interneto prisijungusiems esminių paslaugų teikėjams, įskaitant ligonines ir greitosios pagalbos tarnybas.

Atsparumo kibernetiniams išpuoliams didinimas

Komisija jau remia ES gebėjimo atgrasyti nuo kibernetinių išpuolių stiprinimą, atsparumo jiems didinimą ir tinkamesnį reagavimą į juos, ir imasi šių veiksmų:

Remia veiksmingą pirmojo ES kibernetinio saugumo teisės akto – Tinklų ir informacinių sistemų saugumo direktyvos – įgyvendinimą šiomis priemonėmis:



DIDESNIAIS PAJĖGUMAIS

Valstybės narės turi padidinti kibernetinio saugumo pajėgumus.



BENDRADARBIAVIMU

Intensyvesnis bendradarbiavimas ES lygmeniu.



RIZIKOS PREVENCIJA

Svarbiausiuose sektoriuose (pvz., energetikos, transporto, sveikatos priežiūros) veikiantys subjektai įpareigoti įdiegti rizikos prevencijos priemones ir kibernetinių incidentų valdymo priemones.

Bendradarbiauja su valstybėmis narėmis šiais klausimais:



ES KIBERNETINIO SAUGUMO AGENTŪRA

Stiprinti Europos sąjungos kibernetinio saugumo agentūrą, kad būtų galima geriau padėti valstybėms narėms.



ES SERTIFIKAVIMO SISTEMA

Turėti visoje ES veikiančią sertifikavimo sistemą produktų ir paslaugų kibernetiniam saugumui užtikrinti.



KOORDINUOTAS ATSAKAS

Užtikrinti greitą ir koordinuotą atsaką į didelio masto kibernetinius išpuolius.

Europos Sąjungos tinklų ir informacijos apsaugos agentūra (ENISA) padeda valstybių narių kibernetinio saugumo institucijoms geriau apsaugoti ES nuo kibernetinių išpuolių.

Išteklių ir kibernetinio saugumo srities praktinės patirties sutelkimas

Be jau egzistuojančių ES kibernetinio saugumo iniciatyvų, Komisija šiandien siūlo imtis papildomų priemonių: įsteigti Kompetencijos centrų tinklą ir Europos kibernetinio saugumo pramonės, technologijų ir mokslinių tyrimų kompetencijos centrą, kad būtų rengiamos ir diegiamos priemonės bei technologijos, reikalingos siekiant suspėti laiku reaguoti į nuolat kintančias grėsmes.

Europos centras kartu su valstybėmis narėmis bus atsakingas už būsimame ilgalaikiame ES biudžete kibernetiniam saugumui numatytų lėšų kuo tikslingesnio naudojimo koordinavimą. Tai Europai padės sukurti naujų kibernetinių pajėgumų.

Europoje jau sukaupta daug praktinės patirties – visoje ES yra daugiau nei **660 kibernetinio saugumo kompetencijos centrų**. Kad būtų galima veiksmingai remtis ir pasinaudoti jų sukaupta praktine patirtimi, Komisija siūlo mechanizmą, padėsiantį:



Sutelkti, dalytis ir užtikrinti galimybę naudotis sukaupta praktine patirtimi



Diegti ES kibernetinio saugumo produktus ir sprendimus



Užtikrinti ilgalaikį strateginį pramonės įmonių, mokslinių tyrimų bendruomenių ir vyriausybių bendradarbiavimą



Bendrai investuoti ir dalytis brangia infrastruktūra



Europos kompetencijos centras

Koordinuos būsiamame ilgalaikiame 2021–2027 m. ES biudžete kibernetiniam saugumui numatytų lėšų naudojimą pagal programas „Skaitmeninė Europa“ ir „Europos horizontas“. Centras padės Tinklui ir bendruomenei vykdyti **kibernetinio saugumo** mokslinius tyrimus ir inovacijas. Jis taip pat organizuos **bendras** ES, valstybių narių ir pramonės **investicijas**. Pavyzdžiui, pagal programą „Skaitmeninė Europa“ **2 mlrd. EUR** bus investuoti į ES skaitmeninės ekonomikos, visuomenės ir demokratijos apsaugą. To bus siekiama stiprinant ES kibernetinio saugumo pramonę, finansuojant pažangiausią kibernetinio saugumo įrangą ir infrastruktūrą.



Nacionalinių koordinavimo centrų tinklas

Tinklui vadovauti kiekviena valstybė narė paskirs po vieną nacionalinį koordinavimo centrą, kuris dalyvaus kuriant naujus kibernetinio saugumo pajėgumus ir ugdant platesnes kompetencijas. Tinklas padės nustatyti ir remti svarbiausius kibernetinio saugumo projektus valstybėse narėse.



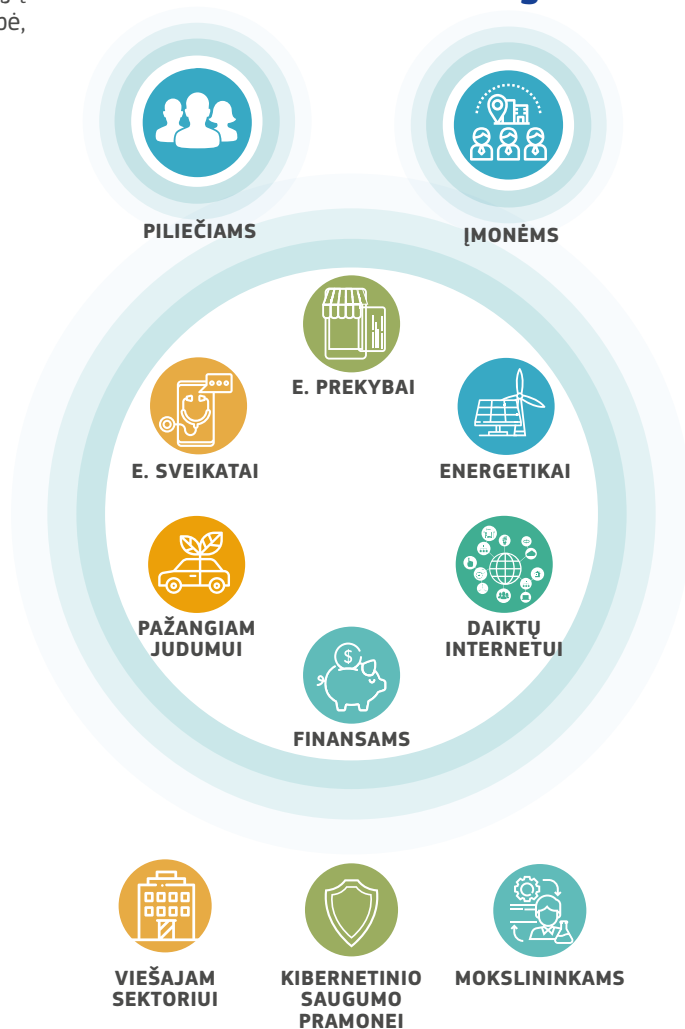
Kompetencijos bendruomenė

Didelė, atvira ir įvairi kibernetinio saugumo srities suinteresuotųjų šalių iš mokslinių tyrimų ir privataus bei viešojo sektorių grupė, įskaitant atstovus iš civilinių ir gynybos institucijų.

Kas pagerės?

- Darbas bus geriau koordinuojamas;
- galimybė pasinaudoti praktine patirtimi;
- prieiga prie bandymų ir eksperimentinės įrangos;
- produktų kibernetinio saugumo vertinimas;
- galimybė naudotis kibernetinio saugumo produktais ir sprendimais;
- parama diegiant produktus ir paslaugas rinkoje;
- didesnis matomumas galimiems investuotojams ir verslo partneriams;
- sutaupoma bendrai investuojant su kitomis valstybėmis narėmis;
- ES galės savarankiškai apsaugoti savo ekonomiką ir demokratiją;
- ES taps pasauline kibernetinio saugumo srities lydere.

Kam tai bus naudinga?





■ **Leidinių biuras**

Print	ISBN 978-92-79-92496-5	doi:10.2775/599558	NA-04-18-693-LT-C
PDF	ISBN 978-92-79-92492-7	doi:10.2775/928356	NA-04-18-693-LT-N