

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
VIEŠOJO VALDYMO GRUPĖ

PAŽYMA

**DĖL LIETUVOS RESPUBLIKOS KIBERNETINIO SAUGUMO ĮSTATYMO NR.XII-1428
1, 2, 6, 8, 13 STRAIPSNIŲ IR PRIEDO PAKEITIMO IR PAPILDYMO IV¹ SKYRIUMI BEI
17 STRAIPSNIU ĮSTATYMO IR LIETUVOS RESPUBLIKOS ADMINISTRACINIŲ
NUSIŽENGIMŲ KODEKSO PAPILDYMO 480¹ STRAIPSNIU IR 589 STRAIPSNIO BEI
PRIEDO PAKEITIMO ĮSTATYMO PROJEKTŲ (toliau – Projektai)
TAP Nr. 20-2202(2); NR.20-2203(2); TAIS Nr. 20-12300(3); NR. 20-12302(3)**

2021-03-17 Nr. NV-473

Vilnius

Projektų rengėjas. Krašto apsaugos ministerija.

Projekto tikslas. Kurti saugesnę kibernetinę erdvę Lietuvos Respublikoje, įgyvendinti Europos Sąjungos teisinį reglamentavimą kibernetinio saugumo srityje.

Dabartinė situacija.

- 2019 m. balandžio 17 d. Europos parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013 (toliau – Kibernetinio saugumo aktas) nustato, kad atitinkami nacionalinės teisės pakeitimai turi būti atlikti iki 2021 birželio 28 d. Įgyvendinant Kibernetinio saugumo akto įpareigojimus reikia paskirti nacionalinę kibernetinio saugumo sertifikavimo instituciją ir nustatyti jos funkcijas, bei atsakomybę už kibernetinio saugumo sertifikavimo pareigų atlikimo pažeidimus.
- Šiuo metu nacionaliniu mastu informacinių sistemų spragų atskleidimo tvarka nėra nustatyta. Bet koks spragų aptikimas, be išankstinio informacinių sistemos valdytojo leidimo, traktuojamas kaip nusikalstama veika, todėl asmenys, aptikę pažeidžiamumą, paprastai pasirenka laikyti tai paslapyje. Sudarius galimybę saugumo pažeidžiamumą suradusiam asmeniui bendradarbiauti su kibernetinio saugumo subjektais, būtų sudarytos sąlygos šį pažeidžiamumą ištaisyti.
- Kibernetinio saugumo įstatyme nėra apibrėžiamos techninės kibernetinio saugumo priemonės, nors Nacionalinis kibernetinio saugumo centrai yra numatyta pareiga diegti ir valdyti technines kibernetinio saugumo priemones.
- Kibernetinio saugumo įstatyme nepakankamai pilnai reglamentuota Kibernetinio saugumo informacinio tinklo paskirtis, jo naudojimo sąlygos, jame tvarkomų duomenų apimtis bei jų teikimo sąlygos. Šiame tinkle saugoma jautri informacija, kuri neturėtų būti teikiama tretiesiems asmenims

Projektų esmė. Siūloma keisti Kibernetinio saugumo įstatymą.

- Įgyvendinant Kibernetinio saugumo aktą siūloma:
 - paskirti Nacionalinį kibernetinio saugumo centrą vykdyti nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas;

- nustatyti nacionalinės kibernetinio saugumo sertifikavimo institucijos funkcijas (stebėti kaip informacinių ir ryšių technologijų gamintojai ir paslaugų teikėjai vykdo su ES nustatytus reikalavimus ir užtikrinti jų vykdymą, nustatyti įgaliojimus atitikties vertinimo įstaigoms, padėti nacionalinėms akreditacijos įmonėms vykdyti stebėsenos ir priežiūros veiklą, stebėti svarbius pokyčius kibernetinio saugumo sertifikavimo srityje, nagrinėti fizinių ir juridinių asmenų pateiktus skundus susijusius su kibernetinio saugumo sertifikavimu, bendradarbiauti su kitų valstybių narių nacionalinėmis kibernetinio saugumo sertifikavimo institucijomis, dalinantis informacija apie produktų, paslaugų ir procesų neatitiktį Kibernetinio saugumo akto reikalavimams).
- numatyti atsakomybę už kibernetinio saugumo sertifikavimo tvarkos pažeidimus (papildyti Administracinių nusižengimų kodeksą).
- Siūloma nustatyti apribojimus, kurių laikantis informacinių sistemų spragų ieškojimas ir atskleidimas laikomas teisėtu.
- Siūloma pavesti karšto apsaugos ministrui tvirtinti informacinių sistemų spragų atskleidimo tvarką.
- Nustatyti Krašto apsaugos ministerijai naują funkciją – tvirtinti techninių kibernetinio saugumo priemonių sąrašą, kuriame nurodoma kibernetinio saugumo priemonių paskirtis ir tvarkomi duomenys.
- Patikslinti reglamentavimą susijusį su Kibernetinio saugumo informaciniu tinklu, nustatyti, kad šio tinklo duomenys susiję su kibernetiniais incidentais yra konfidencialūs ir nurodyti, kokiais atvejais šie duomenys galėtų būti teikiami.

Derinimas. Projektas suderintas su visomis ministerijomis, Generaline prokuratūra, Ryšių reguliavimo tarnyba, Nacionaline teismų administracija, Policijos departamentu, Valstybine duomenų apsaugos inspekcija, asociacija „Infobalt“. Projektai tikslinti pagal Vyriausybės kanceliarijos Teisės grupės pastabas.

Projektų įgyvendinimo kaštai ir nauda. Naujai paskirtų nacionalinės kibernetinio saugumo sertifikavimo institucijos priežiūros funkcijų vykdymui nuo 2022 m. reikės po 200 tūkst. eurų per metus. 2021 m. lėšų poreikis bus mažesnis, nes Projektais teikiami įstatymai įsigalios nuo metų vidurio ir Krašto apsaugos ministerija lėšų poreikį padengs iš vidinių resursų.

Įgyvendinus Projektus bus sudarytos prielaidos kurti saugesnę kibernetinę erdvę Lietuvos Respublikoje, bus įvykdyti ES reglamento reikalavimai.

Atitiktis Vyriausybės programai. Projektai įgyvendina Vyriausybės programos nuostatų įgyvendinimo plano 11.3.2 veiksmo nuostatas. Projektas įtrauktas į Vyriausybės teisėkūros 2021 m. Seimo pavasario sesijos planą.

Dalykinio vertinimo išvada. Siūlome Projektą svarstyti tarpinstituciniame pasitarime.

Viešojo valdymo grupės patarėjas

Valdas Kiveris

Valdas Kiveris, tel. 870661805, el. p. valdas.kiveris@lr.lt