



LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTERIJA

Biudžetinė įstaiga, Totorių g. 25, LT-01121 Vilnius, tel.: (8 5) 273 5501 / 262 4821, faks. (8 5) 264 8517, el. p. kam@kam.lt.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188602751, PVM mokėtojo kodas LT100001016116

Lietuvos Respublikos Vyriausybei

2018-09-10-02
Nr. 12-01-1400

DĖL LIETUVOS RESPUBLIKOS ĮSTATYMO PROJEKTO

Lietuvos Respublikos krašto apsaugos ministerija, atsižvelgdama į 2018 m. spalio 1 d. įvykusio susitikimo su asociacijos „Infobalt“ atstovais rezultatus, pakartotinai teikia parengtą Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 5, 6 ir 43 straipsnių pakeitimo ir įstatymo papildymo 43² ir 43³ straipsniais įstatymo projektą (toliau – Projektas). Projektas teikiamas įgyvendinant Nacionalinės kibernetinio saugumo strategijos, patvirtintos Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. posėdyje, nuostatas ir vykdant Lietuvos Respublikos Vyriausybės 2018 m. birželio 20 d. posėdžio protokolo Nr. 27 7 klausimo 2 punkte įtvirtintus pavedimus.

**I. Sprendžiama
problema**

2016 m. NATO viršūnių susitikimo Varšuvoje metu kibernetinė erdvė pripažinta penktuoju kariavimo domenu. Taip dar kartą patvirtinama, kad kibernetinėmis priemonėmis gali būti pažeistas valstybės suverenitetas, panaudojama jėga ar net surengta ginkluota ataka. Kibernetinis saugumas laikytinas esminiu valstybės interesu, nacionalinio saugumo dalimi. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos, Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Lietuvos Respublikos krašto apsaugos ministerijos surinkti duomenys rodo, kad Lietuva nuolat susiduria su įvairaus tipo kibernetiniais incidentais, skirtais valstybės informaciniams ištekliams ir ypatingos svarbos informacinei infrastruktūrai pažeisti, ir prognozuojama, kad ateityje jų skaičius ir mastas nemažės.

2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitos duomenimis, 2017 m. Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apdorojo 54 414 kibernetinių incidentų. 2017 m. kibernetinių incidentų užregistruota dešimtadaliu daugiau nei 2016 m. Lietuvos valstybės informaciniai ištekliai tebėra prioritetas kibernetinio šnipinėjimo taikinys, bet taikomasi ir į privataus sektoriaus ypatingos svarbos informacinę infrastruktūrą, kitas įmones, turinčias strateginę ar svarbią reikšmę nacionaliniam saugumui. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), taikydamas technines kibernetinio saugumo priemones, daugiausia kenkimo programinės įrangos paplitimo atvejų nustatė energetikos (27 proc.), viešojo saugumo ir teisinės tvarkos (22 proc.) bei užsienio

| | |
|--------------------------------|--|
| | <p>reikalų ir saugumo politikos (21 proc.) sektoriuose. Palyginti su 2016 m., kenkimo programinė įranga labiau plito viešojo saugumo ir teisinės tvarkos, užsienio reikalų ir saugumo politikos, energetikos sektoriuose. Šalies kibernetinio saugumo situacijai įtaką daro ir viešojo sektoriaus interneto svetainių būklė, kuri, 2017 m. Nacionalinio kibernetinio saugumo būklės ataskaitos duomenimis, 2017 m. pablogėjo.</p> <p>NKSC parengtoje 2017 m. nacionalinio kibernetinio saugumo būklės ataskaitoje nurodoma, kad nors 2017 m. buvo matyti kylantis kibernetinio saugumo reikalavimų įgyvendinimo lygis valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje, tačiau reikalavimai yra įgyvendinami <i>ad hoc</i>, ne visa apimtimi ir formaliai, o didėjantis fiksuojamų incidentų kiekis ir atlikti tyrimai rodo, kad organizacijos laiku netaiko būtinų priemonių, kad užkardytų žinomus pažeidžiamumus ir grėsmes. Be to, atsižvelgiant į pasaulio ir Lietuvos kibernetinių grėsmių tendencijas, prognozuojama, kad 2018 m. ir toliau bus ieškoma saugumo spragų Lietuvos valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje, kartu toliau didės susidomėjimas technologiniuose procesuose dalyvaujančiais ir turinčiais sąsają su internetu įrenginiais.</p> |
| II. Siūlomos priemonės | <p>Siūloma nustatyti pareigą juridiniams asmenims, atitinkantiems Vyriausybės patvirtintus kriterijus, naudoti saugųjį valstybinį duomenų perdavimo tinklą (toliau – Saugusis tinklas) ir visas jų valdomas informacines sistemas, registrus, juose esančius duomenis laikyti biudžetinių įstaigų patikėjimo teise valdomose patalpose įrengtuose ir biudžetinių įstaigų eksploatuojamuose duomenų centruose (toliau – valstybinis duomenų centras) bei įstatyme įtvirtinti valstybinių duomenų centro sąvoką.</p> |
| III. Priemonių sąnaudos | <p>Saugusis tinklas bus kuriamas remiantis Saugiu valstybiniu duomenų perdavimo tinklu (toliau – SVDPT), kuris jau dabar jungia 1 300 valstybės institucijų ir įstaigų, mokančių už SVDPT paslaugas. SVDPT tvarkytoją valstybės įmonę „Infostruktūra“, įsigaliojus įstatymo pakeitimams, planuojama pertvarkyti į biudžetinę įstaigą. Šios įstaigos teikiamos paslaugos būtų finansuojamos iš Saugiajame tinkle esančių institucijų šiuo metu SVDPT ryšiams skirtų lėšų, perkėlus jas į būsimą biudžetinės įstaigos, administruojančios Saugųjį tinklą, biudžetą. Valstybės duomenų centro Vilniuje, Gedimino pr. 11, investicijų projekto, skirto valstybės duomenų centro patalpoms įrengti, vykdymui lėšos jau paskirtos, ir šis centras planuojamas įrengti 2019 m. pradžioje. Taip pat numatyta skirti patalpas valstybės duomenų centrui Kaune, jam įrengti iki 2020 m. vidurio planuojama panaudoti Europos Sąjungos lėšas.</p> |
| IV. Nauda visuomenei | <p>Įgyvendinus siūlomus pakeitimus, Saugųjį tinklą naudojančiams juridiniams asmenims būtų teikiamas standartizuotas ir saugus paslaugų paketas, užtikrinamas greitesnis ir efektyvesnis reagavimas į kibernetinius incidentus, taupomi kibernetiniam saugumui skiriami ištekliai, nes būtų centralizuojamas saugos užtikrinimas ir sudarytos sąlygos efektyviau taikyti kolektyvinės gynybos priemonės. Nustatę pareigą naudoti valstybinius duomenų centrus sukurtume sąlygas valstybėje taikyti kolektyvines kibernetinio saugumo ir gynybos priemones, taip užtikrindami visos valstybės aukštesnį kibernetinio saugumo lygį, sumažintume valstybei svarbių valstybės informacinių išteklių kibernetinio saugumo pažeidžiamumus ir koordinuotai valdytume valstybės ypatingos svarbos infrastruktūrą.</p> |

Projektą parengė Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento direktorius Jonas Skardinskas (tel. 8 706 80 800, el. p. jonas.skardinskas@kam.lt) ir Krašto apsaugos ministerijos Teisės departamento (direktorė Judita Nagienė, tel. (8 5) 273 5545, el. p. judita.nagiene@kam.lt) Teisėkūros skyriaus (Istaigų teisinės priežiūros skyriaus patarėja, atliekanti Teisėkūros skyriaus viršininko funkcijas, Svetlana Lapėnienė, tel. (8 5) 273 5563, el. p. svetlana.lapeniene@kam.lt) vyr. specialistas Mantas Keliotis (tel. (8 5) 273 5597, el. p. mantas.keliotis@kam.lt).

PRIDEDAMA:

1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 5, 6 ir 43 straipsnių pakeitimo ir Įstatymo papildymo 43² ir 43³ straipsniais įstatymo projektas, 3 lapai.
2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 5, 6 ir 43 straipsnių pakeitimo ir Įstatymo papildymo 43² ir 43³ straipsniais įstatymo projekto lyginamasis variantas, 4 lapai.
3. Lietuvos Respublikos Vyriausybės nutarimo „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo Nr. XI-1807 1, 2, 5, 6 ir 43 straipsnių pakeitimo ir Įstatymo papildymo 43² ir 43³ straipsniais įstatymo projekto pateikimo Lietuvos Respublikos Seimui“, 1 lapas.
4. Aiškinamasis raštas, 9 lapai.
5. Derinimo pažyma, 6 lapai.

Krašto apsaugos ministras



Raimundas Karoblis