LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
NACIONALINIO SAUGUMO IR KRIZIŲ VALDYMO SKYRIUS

PAŽYMA
DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL TIPINIO KIBERNETINIŲ INCIDENTŲ VALDYMO YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANO PATVIRTINIMO“ PROJEKTO (TAP NR. 16-960(2); TAIS NR. 16-1251(4))

2016-07-08 Nr. NV-2220
Vilnius

1. **Projekto rengėjas:**

Krašto apsaugos ministerija

2. **Projekto tikslas, esmė:**

Nutarimo projekto (toliau – Projektas) tikslas – įgyvendinant Lietuvos Respublikos kibernetinio saugumo įstatymo 5 straipsnio 5 punktą, patvirtinti Tipinį kibernetinių incidentų valdymo planą (toliau – Planas) ir jo rengimo taisykles. Vadovaudamiesi Plano nuostatomis, ypatingos svarbos informacinės infrastruktūros valdytojai privalės parengti kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus.

3. **Derinimas:**

Projektas suderintas su Energetikos ministerija, Finansų ministerija, Susisiekimo ministerija, Vidaus reikalų ministerija, Ūkio ministerija, Ryšių reguliavimo tarnyba, Valstybine duomenų apsaugos inspekcija ir Teisingumo ministerija. Nutarimo projektas patikslintas pagal ministerijų atstovų 2016 m. birželio 21 d. pasitarime pateiktas Vyriausybės kanceliarijos Teisės departamento pastabas. Dėl pastabų, į kurias neatsižvelgta arba atsižvelgta iš dalies, pateikta derinimo pažyma.

4. **Dalykinio vertinimo išvada:**

Teikiamas Projektas atitinka Vyriausybės darbo reglamento reikalavimus.

Nacionalinio saugumo ir krizių
valdymo skyriaus vedėjas Dalius Labanauskas

Dalius Labanauskas, tel. 8 706 61 814, el. p. dalius.labanauskas@lrv.lt

VYRIAUSYBĖS TEISĖS AKTO (SPRENDIMO) PROJEKTAS
Nr. TAP-16-960(2)

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
2016-07-05 data
S-8253 Nr.

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

2016-07-05 Nr. 12-01-1233

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO PROJEKTO

Krašto apsaugos ministerija, įgyvendindama Lietuvos Respublikos kibernetinio saugumo įstatymo (toliau – Įstatymas) 5 straipsnio 5 punktą, teikia Lietuvos Respublikos Vyriausybės nutarimo „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“ projektą (toliau – Nutarimo projektas).

Nutarimo projekto tikslas – įgyvendinant Įstatymą nustatyti Tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą, kuriuo vadovaudamiesi ypatingos svarbos informacinės infrastruktūros valdytojai rengs kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus, ir jo rengimo taisykles.

Nutarimo projekto numatomo teisinio reguliavimo poveikis aprašytas vertinimo pažymoje.

Nutarimo projektas neperkelia Europos Sąjungos teisės aktų ir atitinka Lietuvos Respublikos Vyriausybės programą.

Nutarimo projektas paskelbtas Lietuvos Respublikos Seimo teisės aktų informacinėje sistemoje.

Nutarimo projektas suderintas su Energetikos ministerija, Finansų ministerija, Susisiekimo ministerija, Vidaus reikalų ministerija, Ūkio ministerija, Ryšių reguliavimo tarnyba, Valstybine duomenų apsaugos inspekcija, Teisingumo ministerija.

Nutarimo projektas patikslintas pagal ministerijų atstovų 2016 m. birželio 21 d. pasitarime pateiktas Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamento pastabas. Dėl pastabų, į kurias neatsižvelgta arba atsižvelgta iš dalies, teikiama derinimo pažyma.

Nutarimo projektą parengė Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento (direktorius Arvydas Plėštys, tel. +370 706 80 800) Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus (vedėjas plk. ltn. Artūras Litvaitis, tel. +370 706 80 806) vyriausiasis specialistas Miroslavas Tribockis (tel. +370 706 80 807, el. paštas miroslavas.tribockis@kam.lt).

PRIDEDAMA:

1. Nutarimo projektas, 11 lapų.
2. Nutarimo projekto numatomo teisinio reguliavimo poveikio vertinimo pažyma, 1 lapas.
3. Nutarimo projekto derinimo pažyma, 2 lapai.

Krašto apsaugos ministras Juozas Olekas

Miroslavas Tribockis, tel. +370 706 80 807, el. p. miroslavas.tribockis@kam.lt

Projektas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS DĖL TIPINIO KIBERNETINIŲ INCIDENTŲ VALDYMO YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANO PATVIRTINIMO

2016 m. d. Nr.
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 5 straipsnio 5 punktu Lietuvos Respublikos Vyriausybė n u t a r i a:

1. Patvirtinti Tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą.

2. Nustatyti, kad ypatingos svarbos informacinės infrastruktūros valdytojai pagal kompetenciją:

2.1. ne vėliau kaip per 4 mėnesius nuo Lietuvos Respublikos Vyriausybės patvirtinto ypatingos svarbos informacinės infrastruktūros ir (arba) šios infrastruktūros valdytojų sąrašo įsigaliojimo dienos pagal Tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą parengia ir patvirtina kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus ir patvirtintus planus pateikia Nacionaliniam kibernetinio saugumo centrui;

2.2. kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus gali papildyti ir detalizuoti atsižvelgdami į tarptautinius arba Lietuvos standartus, reglamentuojančius kibernetinių incidentų valdymą, šios srities gerąją praktiką ir veiklos specifiką.

Ministras Pirmininkas

Krašto apsaugos ministras

Krašto apsaugos ministerijos
Teisės departamento direktorė
Julita Nagienė

Juozas Olekas
Krašto apsaugos ministras

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2016 m. d. nutarimu
Nr.

TIPINIS KIBERNETINIŲ INCIDENTŲ VALDYMO YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano (toliau – Planas) tikslas – nustatyti tipines ypatingos svarbos informacinės infrastruktūros valdytojo (toliau – valdytojas) procedūras, siekiant tinkamai valdyti kibernetinius incidentus, nustatytus ypatingos svarbos informacinėje infrastruktūroje (toliau Plane ir prieduose – YSII).

2. Pateikiamas trumpas YSII aprašymas.

3. YSII architektūra, konfigūracija, nustatymai ir kita aprašyta valdytojo patvirtintuose YSII kibernetinį saugumą reglamentuojančiuose teisės aktuose, o už šių dokumentų saugojimą ir atnaujinimą atsakingų asmenų kontaktinė informacija ir funkcijos nurodytos 1 priede.

4. YSII veiklos sutrikdymas daro tiesioginį ir netiesioginį poveikį valstybei, visuomenei arba valdytojui.

5. Didžiausias leistinas YSII veiklos sutrikimo terminas nustatytas valdytojo patvirtintuose YSII veiklą reglamentuojančiuose teisės aktuose.

6. Planas parengtas vadovaujantis:

6.1. Lietuvos Respublikos kibernetinio saugumo įstatymu;

6.2. Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimu Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ (toliau Plane ir prieduose – Nacionalinis kibernetinių incidentų valdymo planas);

6.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ (toliau Plane ir prieduose – Organizaciniai ir techniniai kibernetinio saugumo reikalavimai).

7. Plane vartojamos sąvokos atitinka sąvokas, apibrėžtas ir vartojamas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės

informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Nacionaliniame kibernetinių incidentų valdymo plane, Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose.

II SKYRIUS
KIBERNETINIO INCIDENTO VALDYMO ORGANIZAVIMAS

8. Asmenų, dalyvaujančių kibernetinio incidento valdymo veikloje, kontaktinė informacija ir funkcijos nurodytos 1 priede.

9. Kibernetinio incidento valdymo metu informacija keičiamasi YSII valdytojo naudojamomis informacijos perdavimo priemonėmis, pavyzdžiui, el. paštu, telefonu.

10. Kibernetinių incidentų kategorijos nustatomos pagal kibernetinių incidentų grupes ir kriterijus, nustatytus Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose.

11. YSII valdytojo paskirtas kompetentingas asmuo arba padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą (toliau Plane ir prieduose – atsakingasis valdytojo darbuotojas), gavęs iš Nacionalinio kibernetinio saugumo centro (toliau Plane ir prieduose – Centras) informacijos apie kibernetinio incidento kategorijos patvirtinimą arba patikslinimą, toliau valdo kibernetinį incidentą. Jei Centras informuoja, kad perima kibernetinio incidento valdymą, atsakingasis valdytojo darbuotojas atlieka veiksmus vadovaudamasis Planu, taip pat Nacionaliniu kibernetinių incidentų valdymo planu ir vykdo Centro nurodymus dėl kibernetinio incidento valdymo.

12. Atsakingasis valdytojo darbuotojas kreipiasi pagalbos į Centrą naudodamasis 2 priede pateiktais kontaktiniais duomenimis, jeigu nustatoma, kad YSII valdytojas negalės savarankiškai suvaldyti kibernetinio incidento per didžiausią leistiną YSII sutrikimo terminą.

13. Jei Policijos departamentas prie Vidaus reikalų ministerijos (toliau Plane ir prieduose – Policija) ir (arba) Valstybinė duomenų apsaugos inspekcija (toliau Plane ir prieduose – Inspekcija) paprašo patikslinti arba papildyti informaciją apie kibernetinį incidentą, atsakingasis valdytojo darbuotojas organizuoja papildomos informacijos surinkimą ir pateikimą informacijos prašančiai institucijai jos nustatytu laiku.

14. Kibernetinio incidento valdymo schema pateikta 3 priede.

III SKYRIUS
KIBERNETINIO INCIDENTO NUSTATYMAS

15. Pagrindiniai šaltiniai, kuriais naudojantis gali būti įvykdytas kibernetinis incidentas ir sutrikdyta YSII veikla, nurodyti 4 priede.

16. Informacija apie galimą kibernetinį incidentą gali būti gauta iš įvairių informacijos šaltinių, pavyzdžiui, valdytojo darbuotojo, kuris atlieka kibernetinių incidentų stebėseną, automatizuotų kibernetinių incidentų aptikimo priemonių, kompetentingų valstybės institucijų, kitų juridinių arba fizinių asmenų, taip pat kitų valstybių, tarptautinių organizacijų arba institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, ir pan.

17. Informacija apie galimą kibernetinį incidentą pirmiausia turi būti pateikta atsakingajam valdytojo darbuotojui, kuris pagal kompetenciją nedelsdamas įvertina informaciją apie galimą kibernetinį incidentą ir patvirtina arba paneigia kibernetinio incidento nustatymo faktą.

18. Atsakingasis valdytojo darbuotojas, patvirtinęs kibernetinio incidento nustatymo faktą:

18.1. per kaip galima trumpesnį laiką užregistruoja kibernetinį incidentą užpildydamas kibernetinio incidento elektroninę registravimo formą (5 priedas) ir apie nustatytą kibernetinį incidentą informuoja 1 priede nurodytus asmenis (jei jiems būtina žinoti pagal atliekamas funkcijas);

18.2. remdamasis 2 priede pateiktais kontaktiniais duomenimis apie nustatytą kibernetinį incidentą praneša Centrui Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose nustatyta tvarka;

18.3. remdamasis 2 priede pateiktais kontaktiniais duomenimis pagal kompetenciją informuoja apie šį faktą Policiją ir (arba) Inspekciją šių institucijų nustatyta tvarka ir sąlygomis.

19. Jei kibernetinio incidento buvimo faktas paneigiamas, kibernetinio incidento valdymas baigiamas ir apie tai atsakingasis valdytojo darbuotojas informuoja Centrą (jei kibernetinio incidento informacijos šaltinis yra Centras).

IV SKYRIUS
KIBERNETINIO INCIDENTO VERTINIMAS

20. Kibernetinio incidento vertinimo metu apie kibernetinį incidentą surenkama informacija, nustatyta Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose.

21. Atsakingasis valdytojo darbuotojas kibernetinio incidento vertinimo metu imasi veiksmų užtikrinti kibernetinio incidento įrašų išsaugojimą, jų patikimumą, vientisumą ir pasiekiamumą.

22. Jei kibernetinis incidentas priskirtas vidutinės arba didelės reikšmės kibernetinių incidentų kategorijai, atsakingasis valdytojo darbuotojas:

22.1. įvertinęs kibernetinį incidentą ir apibendrinęs visą surinktą informaciją, per kaip galima trumpesnį laiką ją pateikia 1 priede nurodytiems asmenims (jei jiems būtina žinoti pagal atliekamas funkcijas);

22.2. pateikia vertinimą Centrui, vadovaudamasis Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose nustatyta tvarka.

V SKYRIUS
KIBERNETINIO INCIDENTO STABDYMAS IR ŠALINIMAS

23. Siekiant suvaldyti kibernetinį incidentą ir atkurti įprastą YSII veiklą, imamasi visų galimų organizacinių, techninių ir teisinių priemonių, pavyzdžiui, išjungiama YSII arba jos dalis, išjungiamos tam tikros YSII funkcijos, YSII arba jos dalis išjungiama iš tinklo ir pan.

24. Pagrindiniai kriterijai, kuriais vadovaujantis priimamas sprendimas dėl kibernetinio incidento stabdymo priemonių:

24.1. 1 priede nurodytų asmenų pasiūlymai dėl kibernetinio incidento stabdymo;

24.2. numatytas galimas poveikis, nurodytas Plano 4 punkte;

24.3. kibernetinio incidento įrašų išsaugojimo, jų patikimumo, vientisumo ir pasiekiamumo užtikrinimas;

24.4. didžiausias leistinas YSII veiklos sutrikimo terminas, nurodytas Plano 5 punkte;

24.5. kibernetinio incidento stabdymo sprendimui įgyvendinti reikalingas laikas ir ištekliai;

24.6. numatoma kita žala, kurią gali padaryti kibernetinis incidentas, priėmus jo stabdymo sprendimą.

25. Jei kibernetinis incidentas priskirtas nereikšmingų kibernetinių incidentų kategorijai, atsakingasis valdytojo darbuotojas, atsižvelgdamas į kibernetinio incidento tipą ir galimas jo stabdymo priemones, parenka ir taiko efektyviausią galimą kibernetinio incidento suvaldymo priemonę.

26. Jei kibernetinis incidentas priskirtas vidutinės ir didelės reikšmės kibernetinių incidentų kategorijai:

26.1. atsakingasis valdytojo darbuotojas informuoja 1 priede nurodytus asmenis (jei jiems būtina žinoti pagal atliekamas funkcijas) apie galimas kibernetinio incidento stabdymo ir šalinimo priemones;

26.2. 1 priede nurodyti asmenys, iš atsakingojo valdytojo darbuotojo gavę detalią informaciją apie galimas kibernetinio incidento stabdymo ir šalinimo priemones, per kuo trumpesnį laiką įvertina padėtį ir priima sprendimą dėl efektyviausių ir mažiausiai žalos padarysiančių kibernetinio incidento stabdymo ir šalinimo priemonių taikymo;

26.3. atsakingasis valdytojo darbuotojas nedelsdamas per kaip galima trumpesnį laiką taiko Plano 233 punkte nustatytas priemones kibernetiniam incidentui sustabdyti ir pašalinti;

26.4. sustabdžius ir pašalinus kibernetinį incidentą, atsakingasis valdytojo darbuotojas apie kibernetinio incidento stabdymo ir šalinimo rezultatus informuoja 1 priede nurodytus asmenis (jei jiems būtina žinoti pagal atliekamas funkcijas);

26.5. atsakingasis valdytojo darbuotojas per kaip galima trumpesnį laiką nuo kibernetinio incidento sustabdymo imasi priemonių, kad pažeidžiamumas, dėl kurio įvyko kibernetinis incidentas, būtų pašalintas.

26.6. jei kibernetinis incidentas laikomas suvaldytu, apie tai atsakingasis valdytojo darbuotojas per kaip galima trumpesnį laiką informuoja Centrą, Policiją, ir Inspekciją pagal kompetenciją ir praneša apie pritaikytas kibernetinio incidento valdymo priemones.

VI SKYRIUS
YSII VEIKLOS ATKŪRIMAS

27. Atsakingasis valdytojo darbuotojas pagal kompetenciją įvertina YSII būklę, nustato YSII pažeistas dalis ir per kuo trumpesnį laiką imasi veiksmų pažeistoms dalims atkurti arba pakeisti ir (arba) teikia 1 priede nurodytiems asmenims (jei jiems būtina žinoti pagal atliekamas funkcijas) siūlymus dėl pažeistų dalių atkūrimo arba pakeitimo, jei to negali padaryti savo jėgomis.

28. Prieš atkurdamas YSII veiklą, atsakingasis valdytojo darbuotojas įsitikina, ar pašalintas pažeidžiamumas, dėl kurio įvyko kibernetinis incidentas.

29. Atsakingasis valdytojo darbuotojas apie atkurtą YSII veiklą ir pašalintą pažeidžiamumą informuoja Centrą.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

30. Plano veiksmingumo išbandymą organizuoja atsakingasis valdytojo darbuotojas. Bandymo dieną imituojamas kibernetinis incidentas, kurio metu kibernetinio incidento valdymo veikloje dalyvaujantys asmenys atlieka būtinus tokiomis aplinkybėmis veiksmus. Atsakingasis valdytojo darbuotojas parengia bandymo ataskaitą ir ją perduoda Centrui.

31. Atsižvelgdami į gautus Plano bandymų rezultatus, Plano veiksmingumo išbandymo veikloje dalyvavę asmenys, taip pat kibernetinio incidento valdymo veikloje dalyvavę asmenys, įvertinę kibernetinio incidento valdymo metu įgytą patirtį ir nustatę galimus teisinio reguliavimo trūkumus, pateikia pasiūlymus valdytojo vadovui dėl Plano ir kitų valdytojo tvirtinamų kibernetinį saugumą reglamentuojančių teisės aktų pakeitimo, dėl kibernetinio saugumo situacijos gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo.

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Juozas Olekas
Krašto apsaugos ministras

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
1 priedas

ASMENŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA IR FUNKCIJOS

Vardas, pavardė	**Kontaktinė informacija (telefono numeris, el. pašto adresas ir pan.)**	**Funkcijos**
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*

Juozas Olekas
Krašto apsaugos ministras

Krašto apsaugos ministerijos
teisės departamento direktorė
Judita Nagienė

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
2 priedas

INSTITUCIJŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA

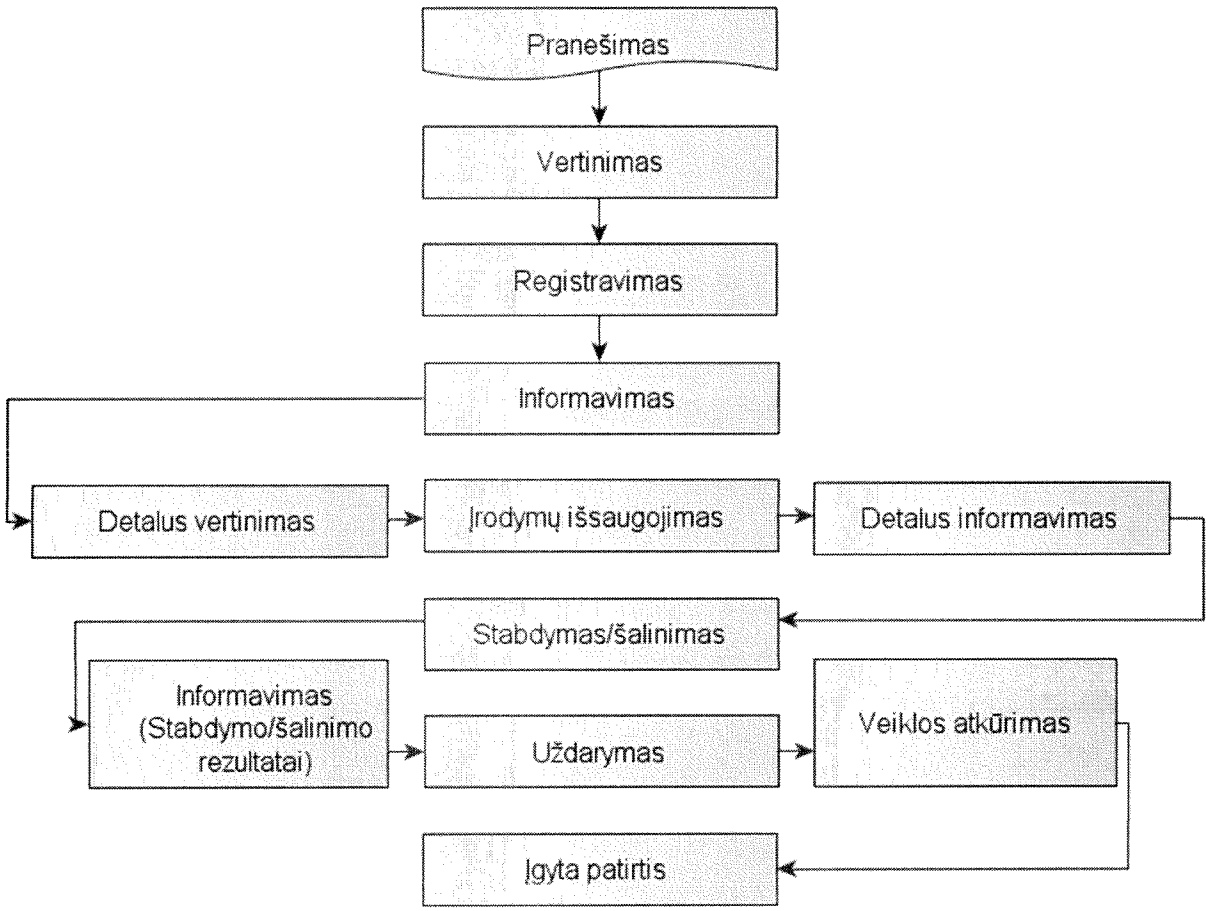
Institucija	**Kontaktinė informacija (telefono numeris, el. pašto adresas ir pan.)**	**Pastabos**
Centras	+370 5 210 3849, el. paštas cert@nksc.lt	Centro budėtojas
	El. paštas info@nksc.lt	Korespondencijai ir paklausimams
Policija	*Kontaktinės informacijos turinys*	*Pastabos turinys*
Inspekcija	*Kranto informacijos turinys*	*Pastabos turinys*

Krašto apsaugos ministerijos
teisės departamento direktorė
Judita Nagienė

Juozas Olekas
Krašto apsaugos ministras

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
3 priedas

KIBERNETINIO INCIDENTO VALDYMO SCHEMA



Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Juozas Olekas
Krašto apsaugos ministras

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
4 priedas

PAGRINDINIAI ŠALTINIAI, KURIAIS NAUDOJANTIS GALI BŪTI ĮVYKDYTAS KIBERNETINIS INCIDENTAS, IR JŲ APRAŠYMAS

Kibernetinio incidento šaltinis	Aprašymas
Išorinės kompiuterinės laikmenos	*Aprašymo turinys*
Internetas	*Aprašymo turinys*
Interneto svetainių pagrindu veikianti programinė įranga	*Aprašymo turinys*
Prarasta įranga	*Aprašymo turinys*
Kiti kibernetinių incidentų šaltiniai	*Aprašymo turinys*

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Juozas Olekas
Krašto apsaugos ministras

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
5 priedas

KIBERNETINIO INCIDENTO REGISTRAVIMO FORMA

Informacija apie kibernetinį incidentą	
Registruojama minimali žinoma informacija apie kibernetinį incidentą, surenkama vertinant kibernetinį incidentą pagal Organizacinius ir techninius kibernetinio saugumo reikalavimus	

Krašto apsaugos ministerijos
Teisės departamento direktorė
Judita Nagienė

Juozas Olekas
Krašto apsaugos ministras

NUMATOMO TEISINIO REGULIAVIMO POVEIKIO VERTINIMO PAŽYMA

Projekto pavadinimai	Lietuvos Respublikos Vyriausybės nutarimo „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“ projektas (toliau – Nutarimo projektas).
Projekto rengėjas	Krašto apsaugos ministerija.
Projekto tikslas	Nutarimo projekto tikslas – įgyvendinant Lietuvos Respublikos kibernetinio saugumo įstatymą, nustatyti Tipinį kibernetinių incidentų valdymo planą, kuriuo vadovaudamiesi ypatingos svarbos informacinės infrastruktūros valdytojai rengs kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus.
	Siūlomo projekto poveikio įvertinimas (teigiamos ir (arba) neigiamos pasekmės)
Poveikis atitinkamai sričiai	Priėmus Nutarimo projektą, bus patvirtintas Tipinis kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planas (toliau – Planas), kuriuo vadovaudamiesi ypatingos svarbos informacinės infrastruktūros valdytojai rengs kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus, ir jo rengimo taisyklės. Plane nustatoma kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planų struktūra ir preliminarus turinys, o plano rengimo taisyklėse detalizuojamos kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano rengimo nuostatos. Kadangi kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planai bus rengiami pagal patvirtintą Planą, tai užtikrins, kad į paminėtus planus bus įtrauktos ir aprašytos visos nuostatos, susijusios su kibernetinio incidento valdymu, ir tai palengvins kibernetinio incidento valdymą ypatingos svarbos informacinėse infrastruktūrose. Priėmus Nutarimo projektą, neigiamų pasekmių nenumatoma.
Poveikis valstybės finansams	Priėmus Nutarimo projektą, poveikio valstybės finansams nebus.
Poveikis administracinei naštai	Nutarimo projektas įgyvendina Kibernetinio saugumo įstatymo nuostatas. Poveikis administracinei naštai buvo įvertintas rengiant Kibernetinio saugumo įstatymo projektą. Priėmus Nutarimo projektą, administracinė našta nepadidės.

Kita svarbi informacija Nėra.

Informacija apie asmenį ir instituciją, atsakingus už poveikio vertinimą

Vardas ir pavardė	Miroslavas Tribockis
Pareigos	Vyriausiasis specialistas
Institucija (padalinys)	Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento Kibernetinio saugumo ir elektroninės informacijos saugos skyrius
Telefono numeris ir elektroninio pašto adresas	Tel. +370 06 80 807, el. paštas miroslavas.tribockis@kam.lt

Juozas Olekas
Krašto apsaugos ministras

LIETUVOS RESPUBLIKOS TEISINGUMO MINISTERIJA

Biudžetinė įstaiga, Gedimino pr. 30, LT-01104 Vilnius,
tel. (8 5) 266 2984, faks. (8 5) 262 5940, el. p. rastine@tm.lt,
atsisk. sąskaita LT267044060000269484 AB SEB bankas, banko kodas 70440.
Duomenys kaupiami ir saugomi Juridinių asmenų registre, kodas 188604955

Lietuvos Respublikos krašto apsaugos ministerijai 2016-05-06 Nr. (1.8)2T-556
| 2016-04-13 Nr. 12-01-645

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO PROJEKTO

Lietuvos Respublikos teisingumo ministerija, išnagrinėjusi pateiktą išvadai gauti Lietuvos Respublikos Vyriausybės nutarimo „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“ projektą (toliau – Nutarimo projektas), teikia šias pastabas ir pasiūlymus:

1. Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano projekto (toliau – Plano projektas) 22, 23 punktuose nustatyta, kad atsakingasis darbuotojas Nr. 2, siekdamas, jog būtų užtikrintas kibernetinio incidento įrašų ir jo įrodymų išsaugojimas, taip pat jų patikimumas, vientisumas ir pasiekiamumas, atlieka šiuos veiksmus: *pirmas veiksmas*; *antras veiksmas; kt.* Jeigu atsakingojo darbuotojo Nr. 2 veiksmai, nustatyti Plano projekto 22 punkte, yra neefektyvūs, jis turi imtis papildomų veiksmų, kad būtų užtikrintas kibernetinio incidento įrašų ir jo įrodymų išsaugojimas, taip pat jų patikimumas, vientisumas ir pasiekiamumas.

Vadovaujantis Kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano rengimo taisyklių projekto (toliau – Taisyklių projektas) 4 punktu, valdytojas, rengdamas Planą, Tipiniame kibernetinių incidentų YSII plane pasviruoju šriftu pateiktą tekstą turi pakeisti, atsižvelgdamas į savo situaciją.

Atkreipiame dėmesį, kad Taisyklių projekto 8.1 papunktis atkartoja Plano projekto 22, 23 punktuose nurodytą informaciją, tačiau nepaaiškina, kokius veiksmus reikia nurodyti, kad būtų užtikrintas tinkamas kibernetinio incidento įrašų ir jo įrodymų išsaugojimas, jų patikimumas, vientisumas ir pasiekiamumas. Nusikalstamos veiklos atvejais įrodymai gali būti naudojami teismo procesuose, o netinkamas jų rinkimas, saugojimas ir kitoks tvarkymas įrodymų vientisumui ir autentiškumui gali turėti neigiamų pasekmių, nes įrodymai gali būti pripažinti netinkamais teismo procesuose, todėl siekiant teisinio aiškumo, siūlome Plano projekto 22, 23 punktuose reglamentuoti konkrečius kibernetinio incidento įrašų ir jo įrodymų išsaugojimo veiksmus arba Taisyklių projekto 8.1 papunktyje nurodyti pagrindinius kibernetinio incidento įrašų ir jo įrodymų išsaugojimo

principus (pavyzdžiui, įrodymai turi būti saugomi atsižvelgiant į teisės aktuose nustatytus senaties terminus, įrašai negali būti pakeisti originalioje laikmenoje, kurioje jie buvo įrašyti, taip pat turi būti patvirtintas naudojamos techninės įrangos patikimumas, programinės įrangos, naudojamos įrašų analizei, patikimumas ir kiti principai).

2. Siūlome tikslinti Plano projekto 30.7 papunkčio formuluotę ir aiškiai nurodyti, kokiais atvejais, kokiai institucijai ir ką reikia pateikti.

3. Reikėtų Planą sukonkretinti, nurodant, kiek įmanoma konkretesnius ar siektinus rodiklius, bendrus visiems ypatingos svarbos informacinės infrastruktūros valdytojams. Tai ypač taikytina terminų nustatymui. Dabar dėl terminų nustatymo tam tikriems veiksmams atlikti Plane paliekama teisė spręsti pačiam ypatingos svarbos informacinės infrastruktūros valdytojui. Tačiau atsižvelgiant į tai, kad šis Planas nebus derinamas su jokia institucija, tik pateikiamas NKSC, pažymėtina, kad skirtingų ypatingos svarbos informacinės infrastruktūros valdytojų numatomi terminai gali labai skirtis, o Planai gali nebūti veiksmingi įvykus kibernetiniam incidentui.

Teisingumo ministras Juozas Bernatonis

Sigita Panovienė, (8 5) 266 2955, el. p. sigita.panoviene@tm.lt.
Andrius Petukauskas, (8 5) 266 2953, el. p. andrius.petukauskas@tm.lt

Originalas nebus siunčiamas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
TEISĖS DEPARTAMENTAS

IŠVADA

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL TIPINIO KIBERNETINIŲ INCIDENTŲ VALDYMO YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANO PATVIRTINIMO“ PROJEKTO

(toliau – Nutarimo projektas)
(TAP NR. 16-960(2); TAIS NR. 16-1251(4)

2016-07-12 Nr.NV-2266

Vilnius

Įvertinę Nutarimo projekto, patikslinto pagal 2016 m. birželio 21 d. ministerijų atstovų (viceministrų, ministerijų kanclerių) pasitarime pateiktas pastabas ir pasiūlymus, atitiktį įstatymams, Vyriausybės nutarimams bei teisės technikos reikalavimams, teikiame šias pastabas ir pasiūlymus:

1. Nutarimo projekto 1 punkte po žodžio „planą“ siūlome įrašyti žodį skliaustuose „pridedama“, Nutarimo projekto 2.1 papunktyje siūlome išbraukti perteklinius žodžius „parengia ir“ ir 2.2 papunktyje nurodyti, kieno veiklos specifika turima omenyje.

2. Nutarimo projekte tvirtinamo Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano (toliau – Planas) 1, 11 ir kituose punktuose, 6.2 papunktyje siūlome išbraukti žodžius „ir prieduose“, nes šiuose punktuose ir papunktyje įsivesti trumpiniai nevartojami prieduose. Be to, kadangi priedai yra sudėtinė Plano dalis šie žodžiai yra pertekliniai.

3. Siūlome apjungti Plano 2 ir 3 punktų nuostatas, o Plano 2 punkte atsisakyti perteklinio žodžio „pateikiamas“.

4. Siūlome suvienodinti Plano 3, 5 ir 31 punktuose nurodytų teisės aktų pavadinimus.

5. Siekiant aiškumo siūlome tikslinti Plano 4 punkto nuostatą, nes neaišku, ką ja norima nustatyti ir kokia šios nuostatos reikšmė ją įrašius į Nutarimo projekto 2.1 papunktyje nurodytus kibernetinių incidentų valdymo ypatingos svarbos informacinės infrastruktūros (toliau – YSII) planus (atsižvelgiant į Plano 4 punkto patikslinimą esant poreikiui taip pat siūlome tikslinti Plano 24.2 papunktį, kuriame duodama nuoroda į Plano 4 punktą).

6. Plano 11 punkte nurodyta, kad atsakingasis valdytojo darbuotojas atlieka veiksmus vadovaujantis Planu, tačiau neaišku, kokius veiksmus jis atlieka, todėl siekiant aiškumo siūlome sukonkretinti duodamą nuorodą į Plano konkrečius punktus.

7. Siekiant aiškumo Plano 12 punkte siūlome nurodyti, kur nustatytas didžiausias leistinas YSII sutrikimo terminas. Be to, Plano 5 punkte kalbama apie YSII *veiklos* sutrikimo terminą, todėl siūlome suvienodinti šiuose Plano punktuose vartojamas formuluotes.

8. Plano 13 punkte siūlome vartoti oficialų Policijos departamento prie Lietuvos Respublikos vidaus reikalų ministerijos pavadinimą.

9. Siekiant aiškumo siūlome Plano 17 ir 23 punktuose nurodyti, kas atlieka šiuose punktuose nuodytus veiksmus.

10. Plano 24.4 papunktyje siūlome tikslinti duodamą nuorodą į Plano 5 punktą, nes jame nėra nurodytas YSII veiklos sutrikdymo terminas, o tik duodama nuoroda į teisės aktus, kuriuose šis terminas nustatytas.

11. Plano 26.3 papunktyje tikslintina duodama nuoroda į Plano 233 punktą, nes tokio punkto nėra.

12. Siūlome tikslinti Plano 26.6 papunktį, nes jis nesiderina su Plano 26 punkto pirmąja pastraipa.

13. Siekiant išvengti dažno teisės aktų keitimo, svarstytina, ar Plano 2 priede nereikėtų atsisakyti konkretaus telefono numerio ir elektroninių paštų nurodymo, nes juos pakeitus reikės keisti ir Plano priedus.

Teisės departamento direktoriaus pavaduotojas Aleksandr Radčenko

Aida Gritienė, tel. 870663839, el. p. aida.gritiene@lrv.lt

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO „DĖL TIPINIO KIBERNETINIŲ INCIDENTŲ VALDYMO YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANO PATVIRTINIMO“ DERINIMO PAŽYMA

Institucijos pavadinimas, rašto data, numeris	**Pasiūlymai ir pastabos**	**Žyma apie pritarimą pastaboms ir pasiūlymams**
Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamentas, 2016-06-08, Nr. NV-1859	1. <...> Taip pat neaišku, kodėl Projekte siūloma patvirtinti Tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą, nors pagal Įstatymo 5 straipsnio 5 dalį Vyriausybei pavesta nustatyti tipinius <...> planus, ar tai nereiškia, kad atskiroms kibernetinių incidentų kategorijoms turėtų būti nustatomi skirtingi tipiniai planai.	Manytina, kad Lietuvos Respublikos kibernetinio saugumo įstatymo (toliau – Įstatymas) leidėjas, pasirinkdamas daugiskaitinę formą (rengiami „tipiniai <...> planai“), siekė suteikti Įstatymą įgyvendinančiai institucijai galimybę prireikus patvirtinti kelis tipinius planus. Vis dėlto įstatymų leidėjas nenustatė kriterijų, kuriais remiantis būtų tvirtinami ne vienas, o keli tipiniai planai, tad manytina, kad Įstatymo tikslai pasiekiami tvirtinant vieną tipinį planą, kuris apima visas galimas kibernetinių incidentų situacijas. Pažymėtina, kad Lietuvos Respublikos Vyriausybės nutarimo „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“ projektu (toliau – Nutarimo projektas) teikiamo tvirtinti Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano turinys aprėpia visų kibernetinių incidentų kategorijų, nustatytų Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimu Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“, valdymą, o vadovaujantis Nutarimo projekto 2.2 papunkčiu, ypatingos svarbos infrastruktūros valdytojai, rengdami kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus, gali juos papildyti ir detalizuoti atsižvelgdami į tarptautinius ar Lietuvos standartus, reglamentuojančius kibernetinių incidentų valdymą, šios srities gerąją praktiką ir veiklos specifiką, taip išspręsdami galimų skirtumų

		valdant kibernetinius incidentus pagal veiklos specifiką problemą.
	3.<...> Taip pat nepagrįstas šiame punkte nustatomas 6 mėnesių terminas.	**Atsižvelgta iš dalies.** Terminas patikslintas vietoj 6 mėnesių nustatant 4 mėnesius. Terminas nustatytas atsižvelgiant į Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarime Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ nustatytą 4 mėnesių terminą, per kurį ypatingos svarbos infrastruktūros valdytojai turi įgyvendinti organizacinius kibernetinio saugumo reikalavimus, tarp jų ir patvirtinti kibernetinį saugumą reglamentuojančius teisės aktus. Taip pat pažymėtina, kad už Įstatymo įgyvendinamuosiuose teisės aktuose nustatytų reikalavimų pažeidimus numatyta administracinė atsakomybė. Siekiant, kad Nutarimo projektas, kuriuo tvirtinamas Tipinis kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planas, būtų aiškus ne tik turinio požiūriu, bet ir kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planų parengimo ir tvirtinimo termino prasme, Nutarimo projekte paliekamos nuostatos, susijusios su kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planų parengimo ir tvirtinimo terminais.

Juozas Olekas
Krašto apsaugos ministras

20

5

Siūlau įtraukti į Vyriausybės posėdžio (pasitarimo) darbotvarkės projektą

2016-07-13

Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo (TAP-16-960(2)(16-1251(2)))

Pranešėjas: krašto apsaugos ministras J.Olekas

Dalyvauja: KAM Kibernetinio saugumo ir informacinių technologijų departamento Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus vyr.specialistas M.Tribockis

Klausimo kuratorius: N.Makštelienė

2016 06 09

Apsvarstyta ministerijų atstovų pasitarime 2016-06-21 (data)	Ministerijų atstovų pasitarimo protokolo išrašas 1. Pasiūlyti KAM atsižvelgti į TD ir Nacionalinio saugumo ir krizių valdymo skyriaus pastabas. 2. Projektą patikslinus svarstyti Vyriausybės posėdžio B dalyje.
Informacija apie projekto svarstymą Vyriausybės pasitarime ar/ir Vyriausybės posėdyje	Papildoma informacija

14 B

prie 22 kl. LRV posė-dis)

VYRIAUSYBĖS TEISĖS AKTO (SPRENDIMO) PROJEKTAS
Nr. TAP-16-960(3)

Patikslintas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖS KANCELIARIJA
2016-07-15 S-8779
data Nr.

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 2016-07-15 Nr. 12-01-1296

DĖL LIETUVOS RESPUBLIKOS VYRIAUSYBĖS NUTARIMO PROJEKTO

Teikiame Lietuvos Respublikos Vyriausybės nutarimo „Dėl Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano patvirtinimo“ projektą (toliau – Nutarimo projektas), patikslintą pagal Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamento 2016 m. birželio 12 dienos išvadoje Nr. NV-2266 pateiktas redakcinio pobūdžio pastabas. Nutarimo projektas darbo tvarka suderintas su Lietuvos Respublikos Vyriausybės kanceliarijos Teisės departamentu.

Nutarimo projektą parengė Krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamento (direktorius Arvydas Plėštys, tel. +370 706 80 800) Kibernetinio saugumo ir elektroninės informacijos saugos skyriaus (vedėjas plk. ltn. Artūras Litvaitis, tel. +370 706 80 806) vyriausiasis specialistas Miroslavas Tribockis (tel. +370 706 80 807, el. p. miroslavas.tribockis@kam.lt).

PRIDEDAMA. Nutarimo projektas, 11 lapų.

Krašto apsaugos ministras Juozas Olekas

Miroslavas Tribockis, tel. +370 706 80 807, el. p. miroslavas.tribockis@kam.lt

Projektas

LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

NUTARIMAS DĖL TIPINIO KIBERNETINIŲ INCIDENTŲ VALDYMO YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANO PATVIRTINIMO

2016 m. d. Nr.
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 5 straipsnio 5 punktu, Lietuvos Respublikos Vyriausybė n u t a r i a:

1. Patvirtinti Tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą (pridedama).

2. Nustatyti, kad ypatingos svarbos informacinės infrastruktūros valdytojai pagal kompetenciją:

2.1. ne vėliau kaip per 4 mėnesius nuo Lietuvos Respublikos Vyriausybės patvirtinto ypatingos svarbos informacinės infrastruktūros ir (arba) šios infrastruktūros valdytojų sąrašo įsigaliojimo dienos pagal Tipinį kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planą patvirtina kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus ir juos pateikia Nacionaliniam kibernetinio saugumo centrui;

2.2. kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose planus gali papildyti ir detalizuoti atsižvelgdami į tarptautinius arba Lietuvos standartus, reglamentuojančius kibernetinių incidentų valdymą, šios srities gerąją praktiką ir ypatingos svarbos informacinės infrastruktūros valdytojo veiklos specifiką.

Ministras Pirmininkas

Krašto apsaugos ministras

Teisės departamento
Teisėkūros skyriaus vedėja

Inga Šilinytė

Juozas Olekas
Krašto apsaugos ministras

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2016 m. d.
nutarimu Nr.

TIPINIS KIBERNETINIŲ INCIDENTŲ VALDYMO YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tipinio kibernetinių incidentų valdymo ypatingos svarbos informacinėse infrastruktūrose plano (toliau – Planas) tikslas – nustatyti tipines ypatingos svarbos informacinės infrastruktūros valdytojo (toliau – valdytojas) procedūras, siekiant tinkamai valdyti kibernetinius incidentus, nustatytus ypatingos svarbos informacinėje infrastruktūroje (toliau – YSII).

2. Trumpas YSII aprašymas. YSII architektūra, konfigūracija, nustatymai ir kita aprašyta valdytojo patvirtintuose YSII kibernetinį saugumą reglamentuojančiuose teisės aktuose, o už šių dokumentų saugojimą ir atnaujinimą atsakingų asmenų kontaktinė informacija ir funkcijos nurodytos 1 priede.

3. YSII neveikimo sukeliamas poveikis ir žala, taip pat didžiausias leistinas YSII neveikimo terminas nustatytas valdytojo patvirtintuose YSII kibernetinį saugumą reglamentuojančiuose teisės aktuose ar kituose valdytojo vadovo patvirtintuose dokumentuose.

4. Planas parengtas vadovaujantis:

4.1. Lietuvos Respublikos kibernetinio saugumo įstatymu;

4.2. Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimu Nr. 87 „Dėl Nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“ (toliau – Nacionalinis kibernetinių incidentų valdymo planas);

4.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“ (toliau – Organizaciniai ir techniniai kibernetinio saugumo reikalavimai).

5. Plane vartojamos sąvokos atitinka sąvokas, apibrėžtas ir vartojamas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės

informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, Nacionaliniame kibernetinių incidentų valdymo plane, Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose.

II SKYRIUS
KIBERNETINIO INCIDENTO VALDYMO ORGANIZAVIMAS

6. Asmenų, dalyvaujančių kibernetinio incidento valdymo veikloje, kontaktinė informacija ir funkcijos nurodytos 1 priede.

7. Kibernetinio incidento valdymo metu informacija keičiamasi YSII valdytojo naudojamomis informacijos perdavimo priemonėmis (el. paštu, telefonu ar kitomis).

8. Kibernetinių incidentų kategorijos nustatomos pagal kibernetinių incidentų grupes ir kriterijus, nustatytus Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose.

9. YSII valdytojo paskirtas kompetentingas asmuo arba padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą (toliau – atsakingasis valdytojo darbuotojas), gavęs iš Nacionalinio kibernetinio saugumo centro (toliau – Centras) informacijos apie kibernetinio incidento kategorijos patvirtinimą arba patikslinimą, toliau valdo kibernetinį incidentą. Jei Centras informuoja, kad perima kibernetinio incidento valdymą, atsakingasis valdytojo darbuotojas atlieka Plano V ir VI skyriuose nurodytus veiksmus, taip pat vadovaujasi Nacionaliniu kibernetinių incidentų valdymo planu ir vykdo Centro nurodymus dėl kibernetinio incidento valdymo.

10. Atsakingasis valdytojo darbuotojas kreipiasi pagalbos į Centrą naudodamasis 2 priede pateiktais kontaktiniais duomenimis, jeigu nustatoma, kad YSII valdytojas negalės savarankiškai suvaldyti kibernetinio incidento per didžiausią leistiną YSII neveikimo terminą, nustatytą valdytojo patvirtintuose YSII kibernetinį saugumą reglamentuojančiuose teisės aktuose ar kituose valdytojo vadovo patvirtintuose dokumentuose.

11. Jei Policijos departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Policija) ir (arba) Valstybinė duomenų apsaugos inspekcija (toliau – Inspekcija) paprašo patikslinti arba papildyti informaciją apie kibernetinį incidentą, atsakingasis valdytojo darbuotojas organizuoja papildomos informacijos surinkimą ir pateikimą informacijos prašančiai institucijai jos nustatytu laiku.

12. Kibernetinio incidento valdymo schema pateikta 3 priede.

III SKYRIUS
KIBERNETINIO INCIDENTO NUSTATYMAS

13. Pagrindiniai šaltiniai, kuriais naudojantis gali būti įvykdytas kibernetinis incidentas ir sutrikdyta YSII veikla, nurodyti 4 priede.

14. Informacija apie galimą kibernetinį incidentą gali būti gauta iš įvairių informacijos šaltinių: valdytojo darbuotojo, kuris atlieka kibernetinių incidentų stebėseną, automatizuotų kibernetinių incidentų aptikimo priemonių, kompetentingų valstybės institucijų, kitų juridinių arba fizinių asmenų, taip pat kitų valstybių, tarptautinių organizacijų arba institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, ir kita.

15. Atsakingasis valdytojo darbuotojas, gavęs informacijos apie galimą kibernetinį incidentą, pagal kompetenciją ją įvertina ir patvirtina arba paneigia kibernetinio incidento nustatymo faktą.

16. Atsakingasis valdytojo darbuotojas, patvirtinęs kibernetinio incidento nustatymo faktą:

16.1. per kaip galima trumpesnį laiką užregistruoja kibernetinį incidentą užpildydamas kibernetinio incidento elektroninę registravimo formą (5 priedas) ir apie nustatytą kibernetinį incidentą informuoja 1 priede nurodytus asmenis (jei jiems būtina žinoti pagal atliekamas funkcijas);

16.2. remdamasis 2 priede pateiktais kontaktiniais duomenimis apie nustatytą kibernetinį incidentą praneša Centrui Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose nustatyta tvarka;

16.3. remdamasis 2 priede pateiktais kontaktiniais duomenimis pagal kompetenciją informuoja apie šį faktą Policiją ir (arba) Inspekciją šių institucijų nustatyta tvarka ir sąlygomis.

17. Jei kibernetinio incidento buvimo faktas paneigiamas, kibernetinio incidento valdymas baigiamas ir apie tai atsakingasis valdytojo darbuotojas informuoja Centrą (jei kibernetinio incidento informacijos šaltinis yra Centras).

IV SKYRIUS
KIBERNETINIO INCIDENTO VERTINIMAS

18. Kibernetinio incidento vertinimo metu apie kibernetinį incidentą surenkama informacija, nustatyta Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose.

19. Atsakingasis valdytojo darbuotojas kibernetinio incidento vertinimo metu imasi veiksmų užtikrinti kibernetinio incidento įrašų išsaugojimą, jų patikimumą, vientisumą ir pasiekiamumą.

20. Jei kibernetinis incidentas priskirtas vidutinės arba didelės reikšmės kibernetinių incidentų kategorijai, atsakingasis valdytojo darbuotojas:

20.1. įvertinęs kibernetinį incidentą ir apibendrinęs visą surinktą informaciją, per kaip galima trumpesnį laiką ją pateikia 1 priede nurodytiems asmenims (jei jiems būtina žinoti pagal atliekamas funkcijas);

20.2. pateikia kibernetinio incidento vertinimą Centrui, vadovaudamasis Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose nustatyta tvarka.

V SKYRIUS
KIBERNETINIO INCIDENTO SUVALDYMAS

21. Siekiant suvaldyti kibernetinį incidentą ir atkurti įprastą YSII veiklą, 1 priede nurodyti asmenys, atlikdami savo funkcijas, imasi visų galimų organizacinių, techninių ir teisinių priemonių (toliau – kibernetinio incidento valdymo priemonės).

22. Pagrindiniai kriterijai, kuriais vadovaujantis priimamas sprendimas dėl kibernetinio incidento valdymo priemonių:

22.1. 1 priede nurodytų asmenų pasiūlymai dėl kibernetinio incidento valdymo;

22.2. numatytas galimas poveikis ir žala, nurodyti Plano 3 punkte;

22.3. kibernetinio incidento įrašų išsaugojimo, jų patikimumo, vientisumo ir pasiekiamumo užtikrinimas;

22.4. didžiausias leistinas YSII neveikimo terminas, nustatytas valdytojo patvirtintuose YSII kibernetinį saugumą reglamentuojančiuose teisės aktuose ar kituose valdytojo vadovo patvirtintuose dokumentuose;

22.5. kibernetinio incidento valdymo sprendimui įgyvendinti reikalingas laikas ir ištekliai;

22.6. numatoma kita žala, kurią gali padaryti kibernetinis incidentas, priėmus jo valdymo sprendimą.

23. Jei kibernetinis incidentas priskirtas nereikšmingų kibernetinių incidentų kategorijai, atsakingasis valdytojo darbuotojas, atsižvelgdamas į kibernetinio incidento tipą ir galimas jo valdymo priemones, parenka ir taiko efektyviausią galimą kibernetinio incidento valdymo priemonę.

24. Jei kibernetinis incidentas priskirtas vidutinės ir didelės reikšmės kibernetinių incidentų kategorijai:

24.1. atsakingasis valdytojo darbuotojas informuoja 1 priede nurodytus asmenis (jei jiems būtina žinoti pagal atliekamas funkcijas) apie galimas kibernetinio incidento valdymo priemones;

24.2. 1 priede nurodyti asmenys, iš atsakingojo valdytojo darbuotojo gavę detalią informaciją apie galimas kibernetinio incidento valdymo priemones, per kuo trumpesnį laiką įvertina padėtį ir priima sprendimą dėl efektyviausių ir mažiausiai žalos padarysiančių kibernetinio incidento valdymo priemonių taikymo ir jas taiko;

24.3. suvaldžius kibernetinį incidentą, atsakingasis valdytojo darbuotojas apie kibernetinio suvaldymo rezultatus informuoja 1 priede nurodytus asmenis (jei jiems būtina žinoti pagal atliekamas funkcijas);

24.4. atsakingasis valdytojo darbuotojas per kaip galima trumpesnį laiką nuo kibernetinio incidento sustabdymo imasi priemonių, kad pažeidžiamumas, dėl kurio įvyko kibernetinis incidentas, būtų pašalintas;

24.5. apie jo suvaldymą atsakingasis valdytojo darbuotojas per kaip galima trumpesnį laiką informuoja Centrą, Policiją, ir Inspekciją pagal kompetenciją ir praneša apie pritaikytas kibernetinio incidento valdymo priemones.

VI SKYRIUS
YSII VEIKLOS ATKŪRIMAS

25. Atsakingasis valdytojo darbuotojas pagal kompetenciją įvertina YSII būklę, nustato YSII pažeistas dalis ir per kuo trumpesnį laiką imasi veiksmų pažeistoms dalims atkurti arba pakeisti ir (arba) teikia 1 priede nurodytiems asmenims (jei jiems būtina žinoti pagal atliekamas funkcijas) siūlymus dėl pažeistų dalių atkūrimo arba pakeitimo, jei to negali padaryti savo jėgomis.

26. Prieš atkurdamas YSII veiklą, atsakingasis valdytojo darbuotojas įsitikina, ar pašalintas pažeidžiamumas, dėl kurio įvyko kibernetinis incidentas.

27. Atsakingasis valdytojo darbuotojas apie atkurtą YSII veiklą ir pašalintą pažeidžiamumą informuoja Centrą.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

28. Plano veiksmingumo išbandymą organizuoja atsakingasis valdytojo darbuotojas. Bandymo dieną imituojamas kibernetinis incidentas ir kibernetinio incidento valdymo veikloje dalyvaujantys asmenys atlieka būtinus tokiomis aplinkybėmis veiksmus. Atsakingasis valdytojo darbuotojas parengia bandymo ataskaitą ir ją perduoda Centrui.

29. Atsižvelgdami į gautus Plano bandymų rezultatus, Plano veiksmingumo išbandymo veikloje dalyvavę asmenys, taip pat kibernetinio incidento valdymo veikloje dalyvavę asmenys, įvertinę kibernetinio incidento valdymo metu įgytą patirtį ir nustatę galimus teisinio reguliavimo trūkumus, pateikia pasiūlymus valdytojo vadovui dėl Plano ir kitų YSII kibernetinį saugumą reglamentuojančių teisės aktų ar kitų valdytojo vadovo patvirtintų dokumentų pakeitimo, dėl kibernetinio saugumo situacijos gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo.

Teisės departamento
Teisėkūros skyriaus vedėja

Inga Šilinytė

Juozas Olekas
Krašto apsaugos ministras

7

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
1 priedas

ASMENŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA IR FUNKCIJOS

Vardas, pavardė	**Kontaktinė informacija (telefono numeris, el. pašto adresas ir pan.)**	**Funkcijos**
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*
Vardenis Pavardenis	*Kontaktinės informacijos turinys*	*Vykdomų funkcijų aprašymas*

Teisės departamento
Teisėkūros skyriaus vedėja

Inga Šilinytė

Juozas Olekas
Krašto apsaugos ministr

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
2 priedas

INSTITUCIJŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA

Institucija	**Kontaktinė informacija (telefono numeris, el. pašto adresas ir pan.)**	**Pastabos**
Centras	*Kontaktinės informacijos turinys*	*Pastabos turinys*
Policija	*Kontaktinės informacijos turinys*	*Pastabos turinys*
Inspekcija	*Kontaktinės informacijos turinys*	*Pastabos turinys*

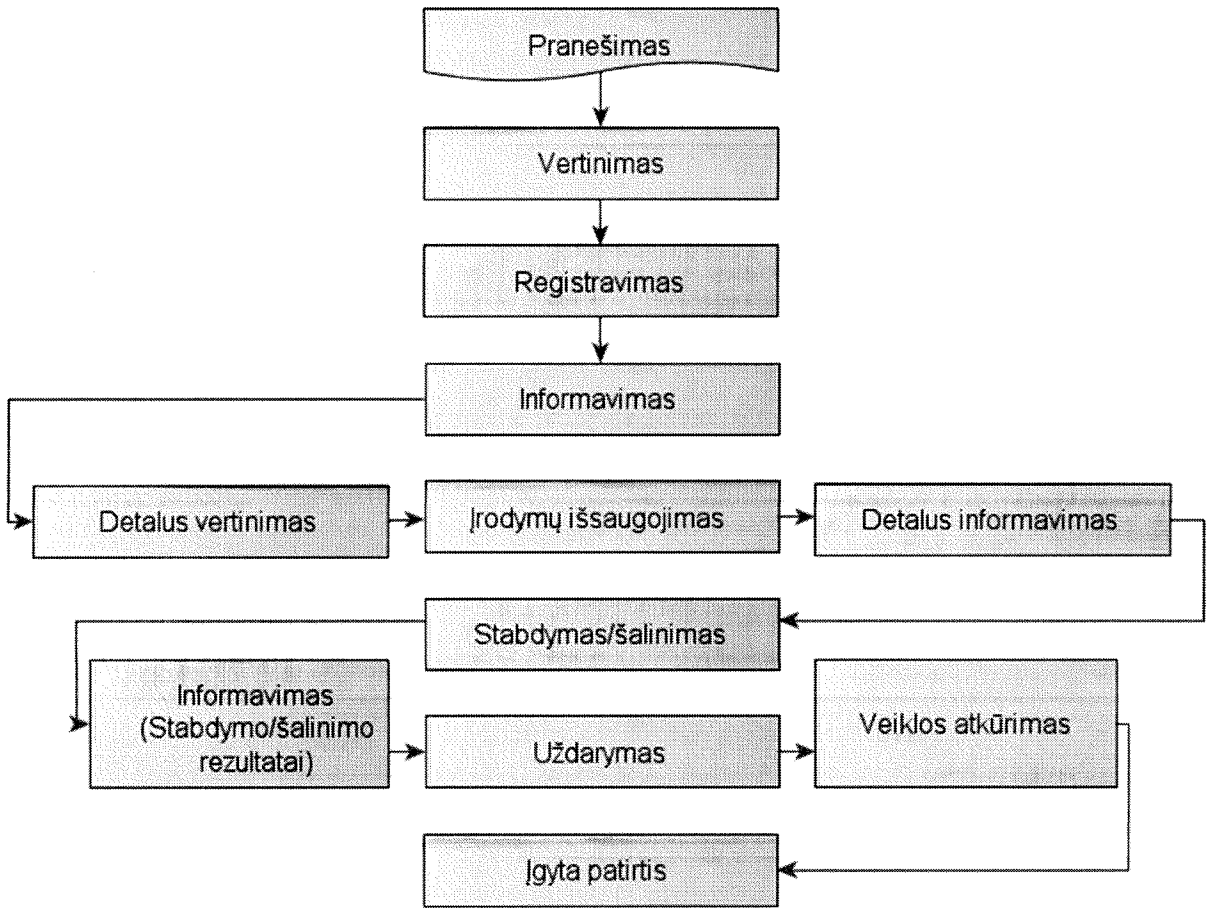
Teisės departamento
Teisėkūros skyriaus vedėja

Inga Šilinytė

Juozas Olekas
Krašto apsaugos ministras

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
3 priedas

KIBERNETINIO INCIDENTO VALDYMO SCHEMA



Teisės departamento
Teisėkūros skyriaus vedėja

Inga Šilinytė

Juozas Olekas
Krašto apsaugos ministras

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
4 priedas

PAGRINDINIAI ŠALTINIAI, KURIAIS NAUDOJANTIS GALI BŪTI ĮVYKDYTAS KIBERNETINIS INCIDENTAS, IR JŲ APRAŠYMAS

Kibernetinio incidento šaltinis	Aprašymas
Išorinės kompiuterinės laikmenos	*Aprašymo turinys*
Internetas	*Aprašymo turinys*
Interneto svetainių pagrindu veikianti programinė įranga	*Aprašymo turinys*
Prarasta įranga	*Aprašymo turinys*
Kiti kibernetinių incidentų šaltiniai	*Aprašymo turinys*

Teisės departamento
Teisėkūros skyriaus vedėja

Inga Šilinytė

Juozas Olekas
Krašto apsaugos ministras

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
5 priedas

KIBERNETINIO INCIDENTO REGISTRAVIMO FORMA

Informacija apie kibernetinį incidentą	
Registruojama minimali žinoma informacija apie kibernetinį incidentą, surenkama vertinant kibernetinį incidentą pagal Organizacinius ir techninius kibernetinio saugumo reikalavimus	

Teisės departamento
Teisėkūros skyriaus vedėja
Inga Šilinytė

Juozas Olekas
Krašto apsaugos ministras