LIETUVOS RESPUBLIKOS VYRIAUSYBĖ

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

2016 m. liepos 20 d. Nr. 746
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 Algirdas Butkevičius

Užsienio reikalų ministras, pavaduojantis
krašto apsaugos ministrą Linas Antanas Linkevičius

PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2016 m. liepos 20 d. nutarimu Nr. 746

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, atliekamas siekiant tinkamai valdyti kibernetinius incidentus, nustatytus ypatingos svarbos informacinėje infrastruktūroje.

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

3. Ypatingos svarbos informacinės infrastruktūros neveikimo sukeliamas poveikis ir žala, taip pat didžiausias leistinas ypatingos svarbos informacinės infrastruktūros neveikimo terminas nustatytas valdytojo patvirtintuose ypatingos svarbos informacinės infrastruktūros 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 ypatingos svarbos informacinės infrastruktūros 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. Ypatingos svarbos informacinės infrastruktūros 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. Jeigu 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 ypatingos svarbos informacinės infrastruktūros valdytojas negalės savarankiškai suvaldyti kibernetinio incidento per didžiausią leistiną ypatingos svarbos informacinės infrastruktūros neveikimo terminą, nustatytą valdytojo patvirtintuose ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą reglamentuojančiuose teisės aktuose ar kituose valdytojo vadovo patvirtintuose dokumentuose.

11. Jeigu 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 sukeltas kibernetinis incidentas ir sutrikdyta ypatingos svarbos informacinės infrastruktūros 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 kitų.

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 kuo trumpesnį laiką užregistruoja kibernetinį incidentą, užpildydamas kibernetinio incidento elektroninę registravimo formą (5 priedas), ir apie nustatytą kibernetinį incidentą informuoja 1 priede nurodytus asmenis (jeigu jiems tai 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. Jeigu kibernetinio incidento buvimo faktas paneigiamas, kibernetinio incidento valdymas baigiamas ir apie tai atsakingasis valdytojo darbuotojas informuoja Centrą (jeigu 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 kibernetinio incidento įrašų išsaugojimui, jų patikimumui, vientisumui ir pasiekiamumui užtikrinti.

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

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

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

V SKYRIUS
KIBERNETINIO INCIDENTO SUVALDYMAS

21. Siekiant suvaldyti kibernetinį incidentą ir atkurti įprastą ypatingos svarbos informacinės infrastruktūros 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. nurodytų 1 priede 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 ypatingos svarbos informacinės infrastruktūros neveikimo terminas, nustatytas valdytojo patvirtintuose ypatingos svarbos informacinės infrastruktūros 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. Jeigu 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. Jeigu kibernetinis incidentas priskirtas vidutinės ir didelės reikšmės kibernetinių incidentų kategorijai:

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

24.2. nurodyti 1 priede asmenys, iš atsakingojo valdytojo darbuotojo gavę išsamią 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 incidento suvaldymo rezultatus informuoja 1 priede nurodytus asmenis (jeigu jiems tai būtina žinoti pagal atliekamas funkcijas);

24.4. atsakingasis valdytojo darbuotojas per kuo trumpesnį laiką nuo kibernetinio incidento sustabdymo imasi priemonių pažeidžiamumui, dėl kurio įvyko kibernetinis incidentas, pašalinti;

24.5. apie kibernetinio incidento suvaldymą atsakingasis valdytojo darbuotojas per kuo trumpesnį laiką informuoja Centrą, policiją ir Inspekciją pagal kompetenciją ir praneša apie taikytas kibernetinio incidento valdymo priemones.

VI SKYRIUS
YPATINGOS SVARBOS INFORMACINĖS INFRASTRUKTŪROS VEIKLOS ATKŪRIMAS

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

26. Prieš atkurdamas ypatingos svarbos informacinės infrastruktūros veiklą, atsakingasis valdytojo darbuotojas įsitikina, ar pašalintas pažeidžiamumas, dėl kurio įvyko kibernetinis incidentas.

27. Atsakingasis valdytojo darbuotojas apie atkurtą ypatingos svarbos informacinės infrastruktūros 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 perduoda ją 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 valdytojo vadovui pasiūlymus dėl Plano ir kitų ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą reglamentuojančių teisės aktų ar kitų valdytojo vadovo patvirtintų dokumentų pakeitimo, kibernetinio saugumo būklės gerinimo ir papildomų kibernetinio saugumo priemonių įsigijimo.

_____

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 panašiai)	Funkcijos
Vardenis Pavardenis	*kontaktinės informacijos turinys*	*atliekamų funkcijų aprašymas*
Vardenis Pavardenis	*kontaktinės informacijos turinys*	*atliekamų funkcijų aprašymas*
Vardenis Pavardenis	*kontaktinės informacijos turinys*	*atliekamų funkcijų aprašymas*
Vardenis Pavardenis	*kontaktinės informacijos turinys*	*atliekamų funkcijų aprašymas*
Vardenis Pavardenis	*kontaktinės informacijos turinys*	*atliekamų funkcijų aprašymas*

_____

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
2 priedas

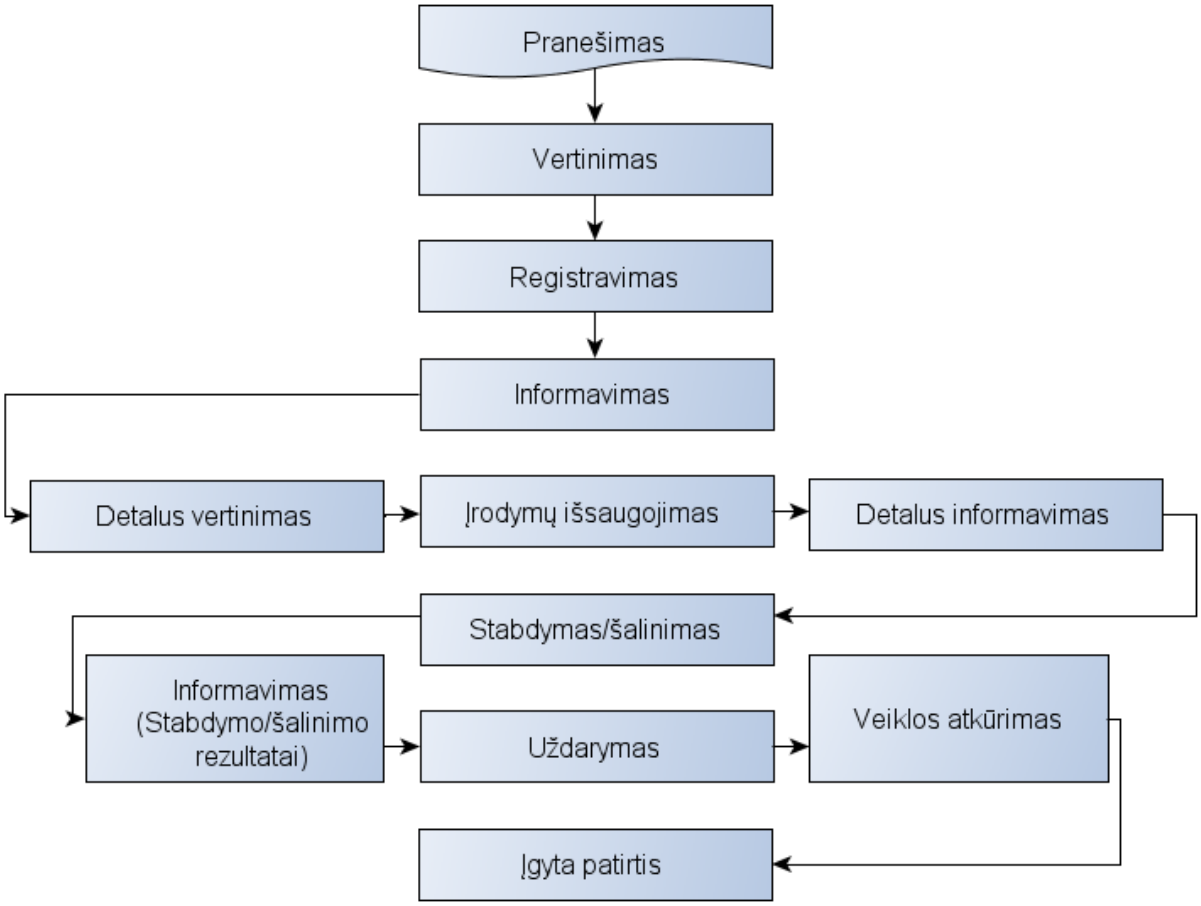
INSTITUCIJŲ, DALYVAUJANČIŲ KIBERNETINIO INCIDENTO VALDYMO VEIKLOJE, KONTAKTINĖ INFORMACIJA

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*

_____

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
3 priedas

KIBERNETINIO INCIDENTO VALDYMO SCHEMA



_____

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
4 priedas

PAGRINDINIAI ŠALTINIAI, KURIAIS NAUDOJANTIS GALI BŪTI SUKELTAS 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*

_____

Tipinio kibernetinių incidentų valdymo
ypatingos svarbos informacinėse
infrastruktūrose plano
5 priedas

KIBERNETINIO INCIDENTO ELEKTRONINĖ REGISTRAVIMO FORMA

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

_____