LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTRAS

ĮSAKYMAS
DĖL NACIONALINIO KIBERNETINIO SAUGUMO CENTRO REAGAVIMO Į KIBERNETINIUS INCIDENTUS VALSTYBĖS INFORMACINIUOSE IŠTEKLIUOSE IR YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE TVARKOS APRAŠO PATVIRTINIMO

2016 m. sausio 6 d. Nr. V-11
Vilnius

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo 4 straipsnio 2 dalimi,

t v i r t i n u Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose tvarkos aprašą (pridedama).

Krašto apsaugos ministras Juozas Olekas

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2016 m. sausio 6 d.
įsakymu Nr. V-11

NACIONALINIO KIBERNETINIO SAUGUMO CENTRO REAGAVIMO Į KIBERNETINIUS INCIDENTUS VALSTYBĖS INFORMACINIUOSE IŠTEKLIUOSE IR YPATINGOS SVARBOS INFORMACINĖSE INFRASTRUKTŪROSE TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose tvarkos aprašas (toliau – Aprašas) nustato Nacionalinio kibernetinio saugumo centro (toliau – NKSC) reagavimo į kibernetinius incidentus procedūras, viešųjų elektroninių ryšių paslaugų teikimo laikinojo, bet ne ilgesnio negu 48 valandos, apribojimo pagrindus ir tokio apribojimo panaikinimo procedūras.

2. Apraše vartojamos sąvokos:

2.1. **duomenų perdavimo tinkas** (toliau – tinklas) – elektroninių ryšių tinklas, sujungiantis kompiuterius, procesų automatizavimo valdymo sistemas (SCADA) ar kitą informacinių ir ryšių technologijų įrangą;

2.2. **įvykis** – duomenų perdavimo tinklo, tinklo įrenginio, tarnybinės ar darbo stoties sutrikimas arba veikimas, neatitinkantis numatytų funkcijų vykdymo, arba kokia nors forma gautas pranešimas apie užfiksuotus elektroninių paslaugų veikimo sutrikimus, informacinės sistemos valdytojo kibernetinio saugumo teisės aktų pažeidimus;

2.3. **NKSC incidentų valdymo sistema (toliau – IVS)** – tai NKSC turimų (valdomų) priemonių visuma, skirta įvykiams ir kibernetiniams incidentams registruoti ir valdyti, taip pat informacijai apie juos dokumentuoti ir archyvuoti;

2.4. **automatizuotos duomenų perdavimo tinklo stebėjimo priemonės (toliau – ADPTSP)** – tai priemonės, skirtos kibernetiniams incidentams automatizuotai aptikti ir į juos reaguoti;

2.5. **automatizuota kibernetinio saugumo sistema** – fizinis ar loginis įrenginys, veikiantis tinkle, kurio paskirtis – automatiškai reaguoti ir apsaugoti nuo kibernetinių incidentų;

2.6. **formalizuotas kibernetinis incidentas** – automatizuotos kibernetinio saugumo sistemos užfiksuotas įvykis, su kuriuo susijusi informacija jau pateikta IVS arba yra išspręstų kibernetinių incidentų duomenų bazėje;

2.7. **pradinis reagavimo laikas** – laikas, per kurį NKSC imasi kibernetinio incidento valdymo priemonių (pvz., pateikia nurodymus valstybės informacinių išteklių (toliau – VII) ir ypatingos svarbos informacinės infrastruktūros (toliau – YSII) valdytojo atsakingam asmeniui, laikinai apriboja paslaugų teikimą ir kt.) po to, kai buvo užfiksuotas kibernetinis incidentas;

2.8. **laikinasis viešųjų elektroninių ryšių paslaugų teikimo apribojimas** – tarnybinės arba darbo stoties ir (arba) naudotojo paskyros prieigos prie VII ar YSII išteklių ar viešųjų tinklų laikinas apribojimas Lietuvos Respublikos kibernetinio saugumo įstatymo nustatyta tvarka;

2.9. **saugumo pranešimas** – informacinis pranešimas VII ar YSII valdytojams (raštu arba žodžiu), kuriame pateikiama aktuali su kibernetiniu saugumu susijusi informacija (kibernetinių incidentų atpažinimo požymiai, saugumo gerinimo rekomendacijos ir kt.), nurodoma pateikiamos informacijos svarba (didelė, vidutinė, maža) ir rekomenduojami arba privalomi VII ir YSII valdytojų veiksmai;

2.10. kitos Apraše vartojamos sąvokos atitinka Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatyme ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme vartojamas sąvokas.

II SKYRIUS
KIBERNETINIŲ INCIDENTŲ KLASIFIKAVIMAS

3. NKSC, vadovaudamasis Lietuvos Respublikos Vyriausybės nustatyta Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, tvarka, vertina savo turimomis (valdomomis) ADPTSP priemonėmis fiksuotus įvykius ar kitų subjektų, turinčių įtakos VII ir YSII valdytojų informacinių sistemų veikimui ir saugumui, pateiktą informaciją apie įvykius, ir nusprendžia, ar priskirti juos atitinkamos kategorijos ir grupės kiberenetiniams incidentams ar ne.

4. ADPTSP fiksuojami įvykiai priskiriami formalizuotiems kibernetiniams incidentams.

5. Jei pagal kibernetinių incidentų kategoriją įvykį galima priskirti kelioms kibernetinio incidento kategorijoms arba VII ar YSII valdytojas negali nustatyti kibernetinio incidento grupės ir kategorijos, pirminę kibernetinio incidento grėsmės kategoriją nustato NKSC budėtojas.

6. NKSC, per laiką, nustatytą Lietuvos Respublikos Vyriausybės patvirtintuose Organizaciniuose ir techniniuose kibernetinio saugumo reikalavimuose, taikomuose ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, negavęs VII ar YSII valdytojo pranešimo apie priemones, skirtas kibernetiniam incidentui valdyti, kibernetiniam incidentui gali suteikti aukštesnę kategoriją.

7. Jeigu NKSC nustato, kad kurios nors kategorijos kibernetinio incidento mastas yra didesnis, vėluojama jį suvaldyti ar kelia didesnę grėsmę nei buvo manyta pradėjus reaguoti, kibernetiniam incidentui suteikia aukštesnę kategoriją.

III SKYRIUS
REAGAVIMAS Į KIBERNETINIUS INCIDENTUS

8. NKSC reaguoja į įvykius, kuriuos aptinka ADPTSP ar fiksuoja kitos automatinio stebėjimo sistemos (saugasienės, el. pašto apsaugos sistemos ir kt.), apie kuriuos, naudodamiesi IVS, praneša VII ar YSII valdytojų asmenys, atsakingi už VII ar YSII organizacinių ir kibernetinių saugumo reikalavimų įgyvendinimo organizavimą (toliau – kontaktiniai asmenys), taip pat apie kuriuos informacija gaunama iš kitų subjektų, turinčių įtakos VII ir YSII valdytojų informacinių sistemų veikimui ir saugumui.

9. Gavęs informaciją apie įvykį šio Aprašo 8 punkte nurodytu būdu, NKSC budėtojas:

9.1. vertina, ar įvykis priskirtinas kibernetiniam incidentui, ir, jei priskirtinas, priskiria jam kibernetinio incidento kategoriją ir grupę, o IVS sukuria jo kortelę;

9.2. valdo kibernetinį incidentą ir informuoja NKSC atsakingą asmenį, kuris, atsižvelgdamas į kibernetinio incidento kategoriją ir grupę, kibernetinio incidento poveikį VII ir YSII, informuoja NKSC vadovą;

9.3. nedelsdamas informuoja NKSC vadovą, jei įvykį priskiria didelės svarbos kibernetiniam incidentui;

9.4. nedelsdamas per IVS siunčia YSII ar VII kontaktiniams asmenims saugumo pranešimus, informaciją apie kibernetiniam incidentui priskirtą kategoriją ir grupę.

10. NKSC vadovas, kilus didelės reikšmės incidentui (klasifikacija incidentams suteikiama vadovaujantis Lietuvos Respublikos Vyriausybės nustatyta Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, tvarka), informuoja krašto apsaugos ministrą ir viceministrą, kuruojantį įstaigos, vykdančios NKSC funkcijas, veiklą.

11. Jei YSII ar VII valdytojas buvo pradėjęs IS techninio gedimo šalinimo darbus, kurie gali pakenkti kibernetinio incidento tyrimui, NKSC gali duoti nurodymus stabdyti pradėtus darbus iki 48 valandų, kad būtų išsaugota su incidentu susijusi informacija.

12. NKSC, naudodamasis IVS turima informacija, kibernetinių incidento tyrimą atlieka, vadovaudamasis reagavimo į kibernetinius incidentus algoritmu (pridedama).

13. Pasikartojantys kibernetiniai incidentai formalizuojami, sukuriant automatiškai juos fiksuojančias ir apdorojančias priemones.

14. Siekdamas suvaldyti didelės reikšmės kibernetinį incidentą, NKSC gali konsultuotis ir (arba) bendradarbiauti su Ryšių reguliavimo tarnybos reagavimo į kibernetinius incidentus padaliniu, Lietuvos kriminalinės policijos biuro Nusikaltimų elektroninėje erdvėje tyrimo valdyba, NATO Reagavimo į kompiuterių incidentus pajėgomis (angl. NATO Computer Incident Response Capability, NCIRC), interneto paslaugų teikėjais ir kitomis kompetentingomis institucijomis.

15. NKSC didelės svarbos kibernetinį incidentą gali priskirti pavojingo kibernetinio incidento kategorijai, jei didelės svarbos kibernetinis incidentas ir (ar) jo poveikis gali sukelti (sukelia) bent vieną iš padarinių, numatytų Lietuvos Respublikos Vyriausybės patvirtintame Nacionalinio kibernetinių incidentų valdymo plane.

16. NKSC, suvaldęs kibernetinį incidentą, jį dokumentuoja, suformuluoja techninių sprendimų išvadas, kurias įtraukia į išspręstų kibernetinių incidentų duomenų bazę, atlieka įvykusio kibernetinio incidento analizę, kurioje nurodomi veiksmai, kuriuos vykdant būtų siekiama išvengti analogiškų kibernetinių incidentų ateityje, pateikia pasiūlymus VII ir YSII valdytojams dėl techninių ir organizacinių priemonių tobulinimo.

17. Suvaldytų kibernetinių incidentų IVS įvykių kortelės saugomos IVS ne mažiau kaip 3 metus.

18. Kibernetinio incidento valdymo metu arba laikotarpiui, kuris būtinas incidento padariniams ir šalutiniams efektams likviduoti, gali būti laikinai apribotas viešųjų elektroninių ryšių paslaugų teikimas. Paslaugų apribojimas ir atnaujinimas atliekamas vadovaujantis Apašo IV skyriaus nuostatomis.

IV SKYRIUS
LAIKINASIS VIEŠŲJŲ ELEKTRONINIŲ RYŠIŲ PASLAUGŲ TEIKIMO APRIBOJIMAS IR APRIBOJIMO PANAIKINIMAS

19. NKSC turi teisę duoti motyvuotą nurodymą laikinai, bet ne ilgiau negu 48 valandoms, apriboti viešųjų elektroninių ryšių paslaugų teikimą šių paslaugų teikėjui:

19.1. jei kyla grėsmė VII ir YSII paslaugų ar duomenų konfidencialumui, vientisumui ir (ar) pasiekiamumui;

19.2. jei nevykdomi teisėti NKSC nurodymai, susiję su kibernetinių incidentų valdymu ir tyrimu;

19.3. jei kibernetinio incidento valdymo metu neįmanoma susisiekti su VII ir YSII kontaktiniu asmeniu;

19.4. kai nepavyksta suvaldyti didelės svarbos arba pavojingų incidentų kategorijai priskirtų kibernetinių incidentų.

20. NKSC laikinąjį viešųjų elektroninių ryšių paslaugų teikimo apribojimą panaikina, kai kibernetinis incidentas suvaldytas anksčiau nei baigiasi laikinojo apribojimo terminas.

21. Sprendimas duoti motyvuotą nurodymą laikinai apriboti viešųjų elektroninių ryšių paslaugų teikimą ir panaikinti laikinąjį viešųjų elektroninių ryšių paslaugų teikimo apribojimą, įforminamas įstaigos prie Krašto apsaugos ministerijos, vykdančios NKSC funkcijas, vadovo įsakymu.

Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose tvarkos aprašo priedas

REAGAVIMO Į KIBERNETINIUS INCIDENTUS ALGORITMAS

