LIETUVOS RESPUBLIKOS
RYŠIŲ REGULIAVIMO TARNYBOS
DIREKTORIUS

ĮSAKYMAS
DĖL NACIONALINIO ELEKTRONINIŲ RYŠIŲ TINKLŲ IR INFORMACIJOS SAUGUMO INCIDENTŲ TYRIMŲ PADALINIO VEIKLOS NUOSTATŲ PATVIRTINIMO

2009 m. kovo 20 d. Nr. 1V- 348
Vilnius

Vadovaudamasis Lietuvos Respublikos ryšių reguliavimo tarnybos nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2004 m. rugpjūčio 19 d. nutarimu Nr. 1029 (Žin., 2004, Nr. 131-4734; 2008, Nr. 82-3257), 8.43 punktu:

1. T v i r t i n u Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinio veiklos nuostatus.
2. N u r o d a u paskelbti šį įsakymą oficialiame leidinyje „Valstybės žinios“.

Direktorius Tomas Barakauskas

PATVIRTINTA
Lietuvos Respublikos ryšių
reguliavimo tarnybos direktoriaus
2009 m. kovo 20 d. įsakymu Nr. 1V- 348

NACIONALINIO ELEKTRONINIŲ RYŠIŲ TINKLŲ IR INFORMACIJOS SAUGUMO INCIDENTŲ TYRIMŲ PADALINIO VEIKLOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinio veiklos nuostatai (toliau – Nuostatai) reglamentuoja Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Tarnyba) vykdomos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinio veiklos tikslą, uždavinius, Tarnybos funkcijas ir teises, taip pat nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinio veiklos organizavimo tvarką, teikėjų teises ir pareigas užtikrinant elektroninių ryšių tinklų ir informacijos saugumą.

2. Nuostatuose vartojamos sąvokos:

2.1. **Elektroninės paslaugos trikdymo ataka** (angl. *DoS*) – tai veiksmas, kuriuo siekiama sutrikdyti elektroninių ryšių tinklo ir (ar) informacinės sistemos darbą arba elektroninių ryšių tinklu teikiamas paslaugas.

2.2. **Elektroniniai duomenys** – duomenys, pateikti tokia forma, kuri tinkama juos tvarkyti informacinėje sistemoje.

2.3. **Elektroninių duomenų klastojimas** – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.

2.4. **Elektroninių ryšių tinklų ir informacijos saugumo incidentas** (toliau – incidentas) – įvykis, veiksmas ar neveikimas, kuris sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (įskaitant valdymo perėmimą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims.

2.5. **Elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimų padalinys** (angl. *Computer Emergency Response Team*) (toliau – CERT padalinys) – asmuo ar jų grupė, kurių pagrindinis tikslas yra operatyviai reaguoti į incidentus informacinėse sistemose ar elektroninių ryšių tinkluose, vykdyti incidentų tyrimus ir atlikti jų šalinimo veiksmus bei skelbti informaciją paslaugų gavėjams apie incidentus bei jų prevenciją.

2.6. **Elektroninių ryšių tinklų ir informacijos saugumo valdymo taisyklės** – dokumentų visuma, nustatanti technines ir organizacines priemones elektroninių ryšių tinklų ir informacijos saugumui užtikrinti.

2.7. **Kenkėjiškas adresas** – elektroninių ryšių tinklo identifikatorius, kurį naudojant vykdoma veikla, kelianti grėsmę elektroninių ryšių tinklų ir informacijos saugumui.

2.8. **Kenkėjiška programinė įranga** – programinė įranga ar jos dalis, specialiai sukurta neteisėtai prisijungti ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (įskaitant perimti valdymą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip panaudoti neviešus elektroninius duomenis tokios teisės neturintiems asmenims.

2.9. **Manipuliacija elektroniniais duomenimis** – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.

2.10. **Neleidžiamasis naudojimasis informacinės sistemos ištekliais –** neteisėtas informacinės sistemos išteklių naudojimas.

2.11. **Neleidžiamasis prisijungimas** – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo.

2.12. **Nepageidaujamas elektroninis paštas** – elektroninio pašto laiškų tiesioginės rinkodaros tikslais siuntimas be elektroninio pašto naudotojo ir (ar) abonento išankstinio sutikimo, galintis turėti neigiamos įtakos elektroninio pašto informacinių sistemų funkcionalumui Lietuvos Respublikoje.

2.13. **Teikėjas** – ūkio subjektas, teikiantis viešuosius ryšių tinklus, viešąsias elektroninių ryšių paslaugas ir (ar) informacinės visuomenės tarpines paslaugas, teikiamas viešaisiais ryšių tinklais.

3. Kitos Nuostatuose vartojamos sąvokos suprantamos taip, kaip jos yra apibrėžtos Lietuvos Respublikos elektroninių ryšių įstatyme (Žin., 2004, Nr. 69-2382), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme (Žin., 1996, Nr. 63-1479; 2008, Nr. 22-804), Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme (Žin., 2006, Nr. 65-2380) ir kituose teisės aktuose.

II. NACIONALINIO CERT PADALINIO VEIKLOS TIKSLAS IR UŽDAVINIAI

4. Tarnybos vykdomos nacionalinio CERT padalinio veiklos pagrindinis tikslas – elektroninių ryšių tinklų ir informacijos saugumo stiprinimas ir paslaugų gavėjų pasitikėjimo elektronine erdve didinimas.

5. Tarnybos svarbiausieji uždaviniai, vykdant nacionalinio CERT padalinio veiklą, yra šie:

5.1. koordinuoti CERT padalinių ir teikėjų veiksmus Lietuvos Respublikoje stabdant incidentų plitimą, šalinant incidentų padarinius viešuosiuose ryšių tinkluose ir informacinėse sistemose;

5.2. pagal kompetenciją vykdyti incidentų tyrimus viešuosiuose ryšių tinkluose ir informacinėse sistemose;

5.3. vykdyti incidentų prevenciją viešuosiuose ryšių tinkluose ir informacinėse sistemose;

5.4. pagal kompetenciją atstovauti Lietuvos Respublikai santykiuose su užsienio valstybių incidentų tyrimo institucijomis ir CERT padaliniais.

III. TARNYBOS FUNKCIJOS VYKDANT NACIONALINIO CERT PADALINIO VEIKLĄ

6. Tarnyba, vykdydama šių Nuostatų 5 punkte nurodytus uždavinius:

6.1. registruoja ir pagal kompetenciją tiria incidentus, įvykusius viešuosiuose ryšių tinkluose ir informacinėse sistemose Lietuvos Respublikoje;

6.2. susidarius ypatingai situacijai viešuosiuose ryšių tinkluose ir informacinėse sistemose, siekdama sustabdyti incidento plitimą bei sumažinti jo neigiamas pasekmes, derina CERT padalinių ir teikėjų veiksmus bei teikia jiems reikalingą pagalbą;

6.3. perduoda institucijoms pagal kompetenciją incidento tyrimo medžiagą, jeigu incidento tyrimas nepriklauso Tarnybos kompetencijai;

6.4. pagal kompetenciją skatina naujų CERT padalinių steigimą Lietuvos Respublikoje;

6.5. atlieka elektroninių ryšių tinklų ir informacijos saugumo būsenos stebėseną Lietuvos Respublikos viešuosiuose ryšių tinkluose ir informacinėse sistemose;

6.6. bendradarbiauja su užsienio valstybių incidentų tyrimo institucijomis, CERT padaliniais ir veikia kaip kontaktinis CERT padalinys Lietuvos Respublikoje;

6.7. pagal kompetenciją dalyvauja Europos Sąjungos institucijų, komitetų ir grupių veikloje, prireikus deleguoja ekspertus dalyvauti atitinkamų komitetų ir grupių veikloje;

6.8. viešai skelbia įspėjimus apie galimas incidentų grėsmes ir rengia rekomendacijas teikėjams, CERT padaliniams ir paslaugų gavėjams apie apsaugą nuo incidentų;

6.9. kas ketvirtį rengia ir viešai interneto tinklalapyje www.cert.lt skelbia įvykusių incidentų statistiką;

6.10. teikia pasiūlymus dėl teisės aktų, susijusių su elektroninių ryšių tinklų ir informacijos saugumu;

6.11. pagal galimybes ir poreikius rengia seminarus ir mokymus teikėjams, CERT padaliniams.

7. Tarnyba atlieka kitas Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatytas funkcijas, kiek tai susiję su elektroninių ryšių tinklų ir informacijos saugumu.

IV. TARNYBOS TEISĖS VYKDANT NACIONALINIO CERT PADALINIO VEIKLĄ

8. Tarnyba, vykdydama nacionalinio CERT padalinio veiklą, turi teisę:

8.1. teikti rekomendacijas teikėjams dėl techninių ir organizacinių reikalavimų, skirtų incidentų prevencijai užtikrinti ir užkirsti kelią incidentams plisti;

8.2. nurodyti teikėjams laikinai apriboti viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų, informacinės visuomenės tarpinių paslaugų teikimą ar nurodyti teikėjams taikyti priemones, stabdančias incidento plitimą ar šalinančias incidento priežastis, ar taikyti kitas laikinąsias poveikio priemones;

8.3. gauti iš teikėjų, CERT padalinių ir valstybės institucijų visą informaciją, susijusią su incidentais;

8.4. keistis incidentų tyrimo informacija su kitais CERT padaliniais, teikėjais, išskyrus informaciją, kuri teisės aktų numatytais atvejais yra viešai neskelbtina;

8.5. sudaryti kenkėjiškų adresų sąrašą, nustatyti kenkėjiškų adresų įtraukimo į tokį sąrašą atvejus, tvarką ir sąlygas;

8.6. gavus išankstinį teikėjo sutikimą, prisijungti prie viešųjų ryšių tinklų ar informacinių sistemų ir išbandyti jų saugumą; elektroninių ryšių tinklų ir informacijos saugumo stebėsenos metu gauta informacija naudojama tik Tarnybos vykdomai nacionalinio CERT padalinio veiklai.

9. Tarnyba turi ir kitų teisių, susijusių su nacionalinio CERT padalinio veiklos vykdymu, kurias jai suteikia įstatymai ir kiti teisės aktai.

V. INCIDENTŲ TYRIMO TVARKA

10. Teikėjai ir CERT padaliniai privalo pranešti Tarnybai apie šiuos incidentus:

10.1. elektroninės paslaugos trikdymo atakas;

10.2. neleidžiamuosius prisijungimus;

10.3. neleidžiamuosius naudojimusis informacinės sistemos ištekliais;

10.4. manipuliacijas elektroniniais duomenimis;

10.5. kenkėjišką programinę įrangą;

10.6. nepageidaujamą elektroninį paštą;

10.7. elektroninių duomenų klastojimą.

11. Teikėjų pranešimai apie incidentus turi būti pateikiami Tarnybai:

11.1. nedelsiant po to, kai teikėjai nustato incidentą, jeigu incidentas kelia grėsmę paties teikėjo viešojo ryšių tinklo ir (ar) viešųjų elektroninių ryšių paslaugų ar informacinių sistemų saugumui, o teikėjas savo techninėmis ir organizacinėmis priemonėmis negali jo pašalinti pats, ir jeigu incidentas kelia grėsmę kitų teikėjų viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų ar informacinių sistemų saugumui;

11.2. per 4 darbo valandas nuo incidento nustatymo momento, jeigu incidentas kelia grėsmę paties teikėjo viešojo ryšių tinklo ir (ar) viešųjų elektroninių ryšių paslaugų ar informacinių sistemų saugumui, o teikėjas savo techninėmis ir organizacinėmis priemonėmis negali jo pašalinti pats;

11.3. kiekvieno mėnesio antrą darbo dieną už praėjusį mėnesį įvykusius incidentus, jeigu teikėjas įgyvendino tinkamas technines bei organizacines priemones ir incidentai buvo pašalinti.

12. Teikėjai, pranešdami Tarnybai apie incidentus, nurodytus Nuostatų 11.1 ir 11.2 punktuose, turi pateikti pranešimą apie incidentą pagal Nuostatų priedo formą, o pranešdami Tarnybai apie incidentus, nurodytus Nuostatų 11.3 punkte, turi pateikti pranešimą apie bendrą incidentų statistiką XML (angl. *eXtensible Markup Language*) formatu, aprašytu interneto tinklalapyje www.cert.lt.

13. Lietuvoje veikiančių CERT padalinių, nepriklausančių teikėjams, incidentų statistika už einamųjų metų praėjusį mėnesį įvykusius incidentus, jeigu CERT padalinys įgyvendino tinkamas technines bei organizacines priemones, incidentai buvo pašalinti ir jie nebekelia grėsmės kitų teikėjų viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų ar informacinių sistemų saugumui, turi būti pateikiama Tarnybai kiekvieno mėnesio antrą darbo dieną XML formatu, aprašytu interneto tinklalapyje www.cert.lt.

14. Teikėjai ir CERT padaliniai pranešimus apie incidentus gali pateikti Tarnybai elektroniniu paštu cert@cert.lt ar interneto tinklalapyje www.cert.lt.

15. Incidentų pavojingumo lygiai, kuriuos nustato Tarnyba vykdydama incidentų tyrimus, yra:

15.1. kritinis, t. y. incidentas, kuris gali žymiai pažeisti viešąjį ryšių tinklą ar informacinę sistemą ir kuris padaro žalos daugiau nei 50 proc. atitinkamo teikėjo paslaugų gavėjų arba incidentas, kuris sutrikdo valstybės informacinių sistemų veikimą;

15.2. pavojingas, t. y. incidentas, kuris gali nežymiai pažeisti viešąjį ryšių tinklą ar informacinę sistemą ir kuris padaro žalos daugiau nei 50 proc. atitinkamo teikėjo paslaugų gavėjų, arba incidentas, kuris gali žymiai pažeisti viešąjį ryšių tinklą ar informacinę sistemą ir kuris padaro žalos mažiau nei 50 proc. atitinkamo teikėjo paslaugų gavėjų;

15.3. mažai pavojingas, t. y. incidentas, kuris gali nežymiai pažeisti viešąjį ryšių tinklą ar informacinę sistemą ir kuris padaro žalos iki 10 proc. atitinkamo teikėjo paslaugų gavėjų.

16. Tarnyba, įvertinusi užregistruoto incidento pavojingumo lygį, imasi būtinų veiksmų incidentui ištirti bei visoms teikėjo ir (ar) CERT padalinio pranešimuose nurodytoms aplinkybėms išsiaiškinti:

16.1. incidentų, kurie yra priskirti prie kritinių, tyrimai pradedami nedelsiant po to, kai gaunamas teikėjo ir (ar) CERT padalinio pranešimas;

16.2. incidentų, kurie yra priskirti prie pavojingų, tyrimai pradedami tik atlikus kritinių incidentų tyrimus arba ne vėliau kaip po 3 darbo dienų nuo teikėjo ir (ar) CERT padalinio pranešimo apie incidentą gavimo;

16.3. incidentų, kurie yra priskirti prie mažai pavojingų, tyrimai pradedami tik atlikus kritinių ir pavojingų incidentų tyrimus arba ne vėliau kaip po 5 darbo dienų nuo teikėjo ir (ar) CERT padalinio pranešimo apie incidentą gavimo.

17. Tarnyba užtikrina incidentų tyrimo metu gautos konfidencialios informacijos apsaugą nuo neteisėto šios informacijos paviešinimo, taip pat užtikrina, kad ši informacija nebūtų atskleista, kopijuojama ar naudojama kitiems tikslams, kurie gali sukelti neigiamų padarinių konfidencialią informaciją pateikusiam asmeniui, išskyrus teisės aktuose numatytus atvejus.

VI. TEIKĖJŲ TEISĖS IR PAREIGOS UŽTIKRINANT ELEKTRONINIŲ RYŠIŲ TINKLŲ IR INFORMACIJOS SAUGUMĄ

18. Teikėjai privalo:

18.1. įgyvendinti tinkamas technines ir organizacines priemones elektroninių ryšių tinklų ir informacijos saugumui užtikrinti, kiek tai susiję su jų teikiamais viešaisiais ryšių tinklais ir (ar)

viešosiomis elektroninių ryšių paslaugomis, o prireikus – kartu su kitais teikėjais imtis reikiamų saugumo priemonių kitų teikėjų viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų ar informacinių sistemų atžvilgiu;

18.2. turėti savo patvirtintas ir atnaujinamas elektroninių ryšių tinklų ir informacijos saugumo valdymo taisykles ir laikytis jų reikalavimų;

18.3. viešai skelbti paslaugų gavėjams rekomendacijas apie priemones elektroninių ryšių tinklų ir informacijos saugumui užtikrinti naudojantis teikėjų teikiamomis paslaugomis;

18.4. imtis visų priemonių, kad elektroniniai duomenys nebūtų siunčiami ir nebūtų priimami iš elektroninių ryšių tinklų taškų, kurie yra įtraukti į Tarnybos kenkėjiškų adresų sąrašą;

18.5. nedelsdami informuoti paslaugų gavėjus:

18.5.1. apie dėl incidento kilusius ilgalaikius viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų ar informacinių sistemų teikimo sutrikimus;

18.5.2. iškilus kritinio incidento grėsmei ir tais atvejais, kai teikėjo taikomos priemonės nepanaikina grėsmės atsiradimo priežasčių, taip pat informuoti paslaugų gavėjus apie visas įmanomas priemones, kurių paslaugų gavėjai gali imtis šiai grėsmei pašalinti, ir nurodyti tikėtinas išlaidas, susijusias su tokių priemonių panaudojimu;

18.6. pateikti Tarnybai informaciją ryšiams, taip pat ir elektroninio pašto adresą, skirtą apsikeisti duomenimis apie incidentus tarp Tarnybos ir teikėjo.

19. Teikėjai turi teisę:

19.1. imtis neatidėliotinų priemonių ir laikinai apriboti paslaugų gavėjams viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų teikimą, kai yra akivaizdi incidento plitimo grėsmė, ir apie tokius veiksmus nedelsdami informuoti Tarnybą;

19.2. teikti Tarnybai teikėjų nuomone svarbią informaciją apie jiems žinomus incidentus.

VII. BAIGIAMOSIOS NUOSTATOS

20. Tarnybos veiksmai ir neveikimas, susiję su Nuostatų taikymu ir įgyvendinimu, gali būti skundžiami Lietuvos Respublikos įstatymų nustatyta tvarka.

21. Už Nuostatų pažeidimus teikėjai atsako teisės aktų nustatyta tvarka.

_____

Nacionalinio elektroninių ryšių
tinklų ir informacijos saugumo
incidentų tyrimų padalinio
veiklos nuostatų
priedas

PRANEŠIMO APIE ELEKTRONINIŲ RYŠIŲ TINKLŲ IR INFORMACIJOS SAUGUMO INCIDENTĄ FORMA

Lietuvos Respublikos ryšių reguliavimo tarnybai
Algirdo g. 27A, LT-03219 Vilnius
tel. (8 5) 210 5679, faks. (8 5) 216 1564
el. paštas: cert@cert.lt

Informacija ryšiams	Organizacija:
	Asmens vardas, pavardė:
	Pareigos:
	Adresas:
	Telefonas, el. pašto adresas:
Incidento apibūdinimas	Incidento tipas:
	Incidento laikas:
	Pažeistų viešųjų ryšių tinklų ir (ar) viešųjų elektroninių ryšių paslaugų, informacinių sistemų, programinės įrangos ir pan. aprašas:
	Informacija apie incidento priežastis (nustatytas asmuo, IP adresas ar kita):
	Incidento aprašymas (nurodyti kiek įmanoma detalesnę informaciją):
	Paslaugų gavėjų, kuriems incidentas padarė žalos, apytikris skaičius arba išraiška procentais nuo bendro teikėjo paslaugų gavėjų skaičiaus:
Incidento valdymas	Veiksmai, kurių imtasi (arba planuojama imtis) šalinant incidentą:
Kita svarbi informacija	
Data	