Elektroninio dokumento nuorašas

LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTRAS

ĮSAKYMAS DĖL NACIONALINĖS RYŠIŲ IR INFORMACINIŲ SISTEMŲ SPRAGŲ ATSKLEIDIMO TVARKOS APRAŠO PATVIRTINIMO

2021 m. d. Nr. V-

Vilnius

Vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo 6 straipsnio 13 punktu,

t v i r t i n u Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašą (pridedama).

Krašto apsaugos ministras Arvydas Anušauskas

PATVIRTINTA
Lietuvos Respublikos
krašto apsaugos ministro
2021 m. d.
įsakymu Nr.

NACIONALINĖS RYŠIŲ IR INFORMACINIŲ SISTEMŲ SPRAGŲ ATSKLEIDIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašas (toliau – Aprašas) nustato ryšių ir informacinių sistemų spragų (toliau – spraga) atskleidimo Nacionaliniam kibernetinio saugumo centrui tvarką, Nacionaliniam kibernetinio saugumo centrui teikiamos informacijos apie spragų paieškos rezultatus turinį bei informacijos apie aptiktą spragą atskleidimo kitiems asmenims terminų nustatymo tvarką.

2. Apraše vartojamos sąvokos apibrėžtos Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos informacinės visuomenės paslaugų įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme ir Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme.

3. Aprašas taikomas asmenims, atlikusiems spragų paiešką kibernetinio saugumo subjektų ryšių ir informacinėse sistemose ir pasirinkusiems informaciją apie spragų paieškos rezultatus teikti Nacionaliniam kibernetinio saugumo centrui.

4. Asmenų, atlikusių spragų paiešką, asmens duomenys, nurodyti Aprašo 13.1.5 papunktyje, tvarkomi šių asmenų identifikavimo ir informavimo apie spragos valdymą tikslais, vadovaujantis 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentu (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas). Informacija apie asmens duomenų tvarkymą krašto apsaugos sistemoje pateikiama Asmens duomenų tvarkymo ir duomenų subjektų teisių įgyvendinimo taisyklėse, patvirtintose Lietuvos Respublikos krašto apsaugos ministro 2015 m. gruodžio 3 d. įsakymu Nr. V-1253 „Dėl Asmens duomenų tvarkymo ir duomenų subjektų teisių įgyvendinimo krašto apsaugos sistemoje taisyklių patvirtinimo“, ir Krašto apsaugos ministerijos interneto svetainės www.kam.lt skiltyje ,,Asmens duomenų tvarkymas“.

II SKYRIUS
SPRAGŲ ATSKLEIDIMAS NACIONALINIAM KIBERNETINIO SAUGUMO CENTRUI

5. Asmuo, atlikęs spragų paiešką, per Kibernetinio saugumo įstatymo 17 straipsnio 2 dalies 3 punkte nustatytą terminą Nacionaliniam kibernetinio saugumo centrui turi pateikti Aprašo 13 punkte nurodytą informaciją apie spragų paieškos rezultatus (toliau – pranešimas) bent vienu iš šių būdų:

5.1. el. laišku adresu cert@nksc.lt (informaciją teikiant šifruotu pranešimu, naudojamas Nacionalinio kibernetinio saugumo centro viešasis raktas 0x3956D9B5);

5.2. užpildant Nacionalinio kibernetinio saugumo centro interneto svetainėje publikuojamą atsakingo atskleidimo formą (https://www.nksc.lt/pranesti-spraga.html).

6. Nacionalinis kibernetinio saugumo centras, gavęs pranešimą:

6.1. ne vėliau kaip per 3 darbo dienas nuo pranešimo gavimo dienos informuoja pranešimą pateikusį asmenį (toliau – pranešėjas) apie pranešimo gavimą;

6.2. prašo iš pranešėjo papildomos informacijos, jeigu pranešime pateikta ne visa Aprašo 10 punkte nurodyta informacija arba pateiktos informacijos nepakanka patvirtinti spragos egzistavimą.

7. Nacionalinis kibernetinio saugumo centras, gavęs pranešimą, kuriame pateikiama informacija apie kibernetinio saugumo subjektų ryšių ir informacinėje sistemoje aptiktą spragą, atlieka spragos analizę (įvertina pateiktos informacijos patikimumą ir pakankamumą, nustato spragos paplitimą, paveiktus asmenis ir galimo kibernetinio incidento grėsmę) ir ne vėliau kaip per 3 darbo dienas nuo pranešimo gavimo dienos pateikia šiam kibernetinio saugumo subjektui spragos analizės rezultatus, susijusius su jo ryšių ir informacinėje sistemoje aptikta spraga, kartu su nurodymais:

7.1. patvirtinti spragos analizės rezultatų gavimą;

7.2. patvirtinti arba paneigti spragos egzistavimą;

7.3. informuoti, ar kibernetinio saugumo subjektas ketina taisyti spragą, jeigu spragos egzistavimas patvirtinamas;

7.4. informuoti apie spragos galimai paveiktus naudotojus;

7.5. neatskleisti informacijos apie spragą, jeigu atlikus spragos analizę nustatoma, kad informacijos apie spragą atskleidimas gali sukelti grėsmę kitiems asmenims.

8. Skaitmeninių paslaugų teikėjams Aprašo 7 punkte nustatyta tvarka teikiami spragos analizės rezultatai, tačiau nurodymai neteikiami.

9. Jeigu spragos analizės metu nustatoma, kad spraga galimai egzistuoja ir kitų, nei nurodyta 7 punkte, kibernetinio saugumo subjektų ryšių ir informacinėse sistemose, Nacionalinis kibernetinio saugumo centras apie galimą spragą informuoja šiuos kibernetinio saugumo subjektus ir teikia Aprašo 7 punkte numatytus nurodymus.

10. Nacionalinis kibernetinio saugumo centras, gavęs kibernetinio saugumo subjekto patvirtinimą dėl spragos egzistavimo arba spragos egzistavimo paneigimą, ne vėliau kaip per 3 darbo dienas nuo patvirtinimo arba paneigimo gavimo dienos perduoda šią informaciją pranešėjui.

11. Nacionalinis kibernetinio saugumo centras periodiškai, bet ne rečiau kaip kas 60 kalendorinių dienų nuo pranešimo gavimo teikia pranešėjui apibendrintą informaciją apie pranešime nurodytos spragos valdymą, iki kol spraga yra pašalinama, nustatoma, kad spraga neegzistuoja arba gaunama informacijos, kad kibernetinio saugumo subjektas atsisako taisyti spragą. Ši pareiga netaikoma dėl spragų, kurių valdymas tęsiasi ilgiau kaip 180 kalendorinių dienų nuo pranešimo gavimo datos.

12. Nacionalinis kibernetinio saugumo centras, spragos analizės metu nustatęs galimus nusikalstamos veikos ar Bendrojo duomenų apsaugos reglamento pažeidimo požymius, ne vėliau kaip per dvidešimt keturias valandas nuo šių aplinkybių nustatymo apie tai informuoja atitinkamai Lietuvos policiją ar Valstybinę duomenų apsaugos inspekciją.

III SKYRIUS
NACIONALINIAM KIBERNETINIO SAUGUMO CENTRUI TEIKIAMOS INFORMACIJOS APIE SPRAGŲ PAIEŠKOS REZULTATUS TURINYS

13. Nacionaliniam kibernetinio saugumo centrui teikiamos informacijos apie spragų paieškos rezultatus turinys:

13.1. informacija, kuri privalo būti teikiama:

13.1.1. ryšių ir informacinė sistema, kurioje buvo (yra) vykdoma spragų paieška (URL adresas ir (arba) IP adresas, prievadas (-ai));

13.1.2. data ir laikas, kai buvo pradėta spragų paieška;

13.1.3. data ir laikas, kai spragų paieška buvo baigta (jeigu spragų paieška jau baigta);

13.1.4. IP adresas, iš kurio buvo vykdoma spragų paieška;

13.1.5. pranešėjo kontaktinė informacija:

13.1.5.1. vardas, pavardė;

13.1.5.2. elektroninio pašto adresas;

13.1.5.3. viešasis raktas (jeigu naudojama);

13.2. informacija, kuri teikiama tik tais atvejais, jei spragų paieškos metu buvo aptikta spraga, ir tik tokia apimtimi, kiek žinoma pranešėjui:

13.2.1. informacija, reikalinga spragai nustatyti ir išanalizuoti:

13.2.1.1.pagrindinė informacija: laikas, konkreti vieta/sistema (URL adresas ir (arba) IP adresas, prievadas (-ai), pažeidžiamos programinės ar techninės įrangos pavadinimas ir versija);

13.2.1.2.papildoma techninė informacija, reikalinga spragai atkartoti (konkretūs žingsniai, kaip buvo atrasta spraga, angl. *proof of concept*);

13.2.1.3.pasinaudojimo spraga kodas (angl. *exploit code*);

13.2.1.4.kita informacija, galinti padėti identifikuoti spragą (ekrano vaizdai, video, naudoti įrankiai ir kt.);

13.2.2. ar pranešėjas pats aptiko spragą, ar apie tai sužinojo iš kitų šaltinių. Jeigu egzistuoja šaltinis, pateikti į jį nuorodą;

13.2.3. informacija apie aktyvų naudojimąsi spraga;

13.2.4. tikėtinos pasekmės, jeigu spraga būtų pasinaudota (pavyzdžiui, perimti/sunaikinti duomenys, sutrikdyta sistema ir pan.);

13.2.5. kitos ryšių ir informacinės sistemos, produktai, organizacijos, vartotojai, kurie gali būti paveikti šios spragos;

13.2.6. ar galima perduoti pranešėjo kontaktus kibernetinio saugumo subjektui;

13.2.7. ar pranešėjas planuoja atskleisti informaciją apie spragą viešai;

13.2.8. kokie pranešėjo asmens duomenys galėtų būti paviešinti, jeigu bus publikuojamas kibernetinio saugumo subjekto ir (arba) Nacionalinio kibernetinio saugumo centro viešas spragos atskleidimas.

IV SKYRIUS
INFORMACIJOS APIE APTIKTĄ SPRAGĄ ATSKLEIDIMO KITIEMS ASMENIMS TERMINŲ NUSTATYMAS

14. Trumpesni, negu nurodyta Kibernetinio saugumo įstatymo 17 straipsnio 5 dalyje, informacijos apie aptiktą spragą atskleidimo kitiems asmenims, negu nurodyti Kibernetinio saugumo įstatymo 17 straipsnio 2 dalies 3 punkte, terminai nustatomi pranešėjo prašymu arba Nacionalinio kibernetinio saugumo centro iniciatyva.

15. Nacionalinis kibernetinio saugumo centras, gavęs pranešėjo prašymą, nustato trumpesnį, negu nurodyta Kibernetinio saugumo įstatymo 17 straipsnio 5 dalyje, informacijos apie aptiktą spragą atskleidimo kitiems asmenims, negu nurodyti Kibernetinio saugumo įstatymo 17 straipsnio 2 dalies 3 punkte, terminą, esant bent vienai iš šių aplinkybių:

15.1. jeigu kibernetinio saugumo subjektas paneigė informaciją apie spragos egzistavimą, o Nacionalinis kibernetinio saugumo centras, įvertinęs spragos analizės rezultatus, nenumato galimų informacijos apie aptiktą spragą atskleidimo neigiamų pasekmių;

15.2. kibernetinio saugumo subjektas raštu išreiškė sutikimą, kad informacijos apie aptiktą spragą atskleidimo kitiems asmenims terminas būtų sutrumpintas, o Nacionalinis kibernetinio saugumo centras, įvertinęs spragos analizės rezultatus, nenumato galimų informacijos apie aptiktą spragą atskleidimo neigiamų pasekmių. Tokiu atveju informacijos apie spragą atskleidimo terminas negali būti trumpesnis nei sutarta su kibernetinio saugumo subjektu.

16. Nacionalinis kibernetinio saugumo centras nustato trumpesnį, negu nurodyta Kibernetinio saugumo įstatymo 17 straipsnio 5 dalyje, informacijos apie aptiktą spragą atskleidimo kitiems asmenims, negu nurodyti Kibernetinio saugumo įstatymo 17 straipsnio 2 dalies 3 punkte, terminą savo iniciatyva, jeigu apie spragą yra informuojama visuomenė.

_____

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Krašto apsaugos ministerija 188602751, Vilnius, Totorių g. 25
Dokumento pavadinimas (antraštė)	DĖL NACIONALINĖS RYŠIŲ IR INFORMACINIŲ SISTEMŲ SPRAGŲ ATSKLEIDIMO TVARKOS APRAŠO PATVIRTINIMO
Dokumento registracijos data ir numeris	2021-07-09 Nr. V-484
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	ARVYDAS ANUŠAUSKAS, Ministras
Sertifikatas išduotas	ARVYDAS ANUŠAUSKAS, Lietuvos Respublikos krašto apsaugos ministerija LT
Parašo sukūrimo data ir laikas	2021-07-09 09:37:21
Parašo formatas	XAdES-X-L
Laiko žymoje nurodytas laikas	2021-07-09 09:37:38
Informacija apie sertifikavimo paslaugų teikėją	ADIC CA-B, Asmens dokumentu israsymo centras prie LR VRM LT
Sertifikato galiojimo laikas	2020-12-11 - 2023-12-11
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA, VI Registru centras - i.k. 124110246 LT" išduotą sertifikatą "Dokumentų valdymo sistema DokVIS, Lietuvos Respublikos krašto apsaugos ministerija, į.k.188602751 LT", sertifikatas galioja nuo 2018-12-27 iki 2021-12-26
Pagrindinio dokumento priedų skaičius	1
Pagrindinio dokumento pridedamų dokumentų skaičius	-
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	Dokumentų valdymo sistema Avilys, versija 3.5.45.2
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2021-07-11)
Paieškos nuoroda	https://www.e-tar.lt/portal/legalAct.html?documentId=270e6bd1e08911eb866fe2e083228059
Papildomi metaduomenys	Nuorašą suformavo 2021-07-11 01:26:13 TAIS