Valstybinio audito ataskaitos santrauka

KIBERNETINIO SAUGUMO APLINKA LIETUVOJE

2015 m. gruodžio 9 d. Nr. VA-P-90-4-16

Su valstybinio audito ataskaita galima susipažinti Valstybės kontrolės interneto puslapyje adresu www.vkontrole.lt

SANTRUMPOS IR SĄVOKOS

Vartojamos sąvokos[1]:

Elektroninė informacija – informacinėje sistemoje tvarkomi duomenys, dokumentai ir informacija.

Elektroninės informacijos sauga – elektroninės informacijos konfidencialumo (su tvarkoma elektronine informacija gali susipažinti tik įgalioti asmenys), vientisumo (elektroninė informacija nebuvo atsitiktinai ar neteisėtai pakeista ar sunaikinta) ir prieinamumo (elektroninė informacija gali būti tvarkoma reikiamu metu) užtikrinimas.

Ypatingos svarbos informacinė infrastruktūra – elektroninių ryšių tinklas ar jo dalis, informacinė sistema ar jos dalis, informacinių sistemų grupė ar pramoninių procesų valdymo sistema ar jos dalis, nepaisant to, ar jos valdytojas yra privatus ar viešojo administravimo subjektas, kuriuose įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams.

Kibernetinė erdvė – aplinka, kurioje pavieniuose kompiuteriuose ar kitoje informacinėje ir ryšių technologijų įrangoje sukuriama elektroninė informacija ir (arba) perduodama per elektroninių ryšių tinklu sujungtus kompiuterius ar kitą informacinių ir ryšių technologijų įrangą.

Kibernetinis incidentas – įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenims.

Kibernetinis saugumas – visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.

Šioje audito ataskaitoje **kibernetinis saugumas** suprantamas plačiau nei apibrėžia Kibernetinio saugumo įstatymas ir apima taip pat Tarptautinės standartizacijos organizacijos (ISO) standartuose[2] ir Šiaurės Atlanto Sutarties Organizacijos (NATO) Kibernetinės gynybos tobulinimo kompetencijos centro pateiktose rekomendacijose[3] priskiriamus elementus (el. informacijos, taikomųjų programų, tinklų, interneto ir ypatingos svarbos informacinės infrastruktūros saugą).

[1] Sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, 2014-12-11 Nr. XII-1428, 2 str., Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, 2011-12-15 Nr. XI-1807, 2 str. ir Lietuvos Respublikos Vyriausybės 2013-07-24 nutarimu Nr. 716 patvirtintame Bendrųjų elektroninės informacijos saugos reikalavimų apraše, 4 p.

[2] ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.

[3] NATO Cooperative Cyber Defence Centre of Excellence National Cyber Security Framework Manual 2012 m.

Santrumpos:

CERT – Elektroninių ryšių tinklų ir informacijos saugumo tyrimo padalinys.

ES – Europos Sąjunga.

IRD – Informatikos ir ryšių departamentas prie Vidaus reikalų ministerijos.

IVPK – Informacinės visuomenės plėtros komitetas prie Susisiekimo ministerijos.

KAM – Krašto apsaugos ministerija.

KSĮ – Kibernetinio saugumo įstatymas.

KS taryba – Kibernetinio saugumo taryba.

LRS – Lietuvos Respublikos Seimas.

LRV – Lietuvos Respublikos Vyriausybė.

NATO – Šiaurės Atlanto Sutarties Organizacija.

NKSC – Nacionalinis kibernetinio saugumo centras.

PAGD – Priešgaisrinės apsaugos ir gelbėjimo departamentas prie Vidaus reikalų ministerijos.

PD – Policijos departamentas prie Vidaus reikalų ministerijos.

RRT – Ryšių reguliavimo tarnyba.

SM – Susisiekimo ministerija.

SVDPT – Saugus valstybinis duomenų perdavimo tinklas.

VDAI – Valstybinė duomenų apsaugos inspekcija.

VIIV taryba – Valstybės informacinių išteklių valdymo taryba.

VRM – Vidaus reikalų ministerija.

SANTRAUKA

Lietuvos Respublikos Vyriausybė 2006 m. nustatė[4], kad galiojantis el. informacijos saugos (kibernetinio saugumo) srities reglamentavimas nepakankamas, todėl nutarė parengti el. ryšių tinklų ir informacijos saugumo įstatymą, o 2011 m. patvirtinto El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programą[5]. Tačiau ji vykdoma nerezultatyviai, o minėtas įstatymas taip ir nebuvo priimtas.

Taigi kibernetinio saugumo sritis iki 2015 m. rėmėsi teisės aktais, kuriuose nebuvo aiškiai nustatytų šios srities politiką formuojančių ir įgyvendinančių institucijų, kibernetinio saugumo dalyvių pareigų, atsakomybės, organizacinių ir techninių kibernetinio saugumo reikalavimų ir kibernetinio saugumo užtikrinimo priemonių.

2014 m. pabaigoje įvyko esminiai kibernetinio saugumo reglamentavimo pokyčiai: priimtas Kibernetinio saugumo įstatymas[6], nustatantis kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžiantis kibernetinio saugumo ir kitas pagrindines šios srities sąvokas. Įsigaliojus įstatymui (nuo 2015 m.), Krašto apsaugos ministerijai suteikti įgaliojimai formuoti kibernetinio saugumo politiką, organizuoti, kontroliuoti ir koordinuoti jos įgyvendinimą, Kibernetinio saugumo ir telekomunikacijų tarnyboje prie Krašto apsaugos ministerijos įsteigtas Nacionalinis kibernetinio saugumo centras[7], sudaryta Kibernetinio saugumo taryba[8].

Vidaus reikalų ministerija, iki 2015 m. turėjusi įgaliojimus formuoti valstybės politiką el. informacijos saugos, kibernetinio saugumo srityje, organizuoti, koordinuoti ir kontroliuoti jos įgyvendinimą[9], nuo 2015 m. politiką valstybės informacinių išteklių saugos srityje įgaliota formuoti tiek, kiek tai neapima kibernetinio saugumo[10] ir kartu su Nacionaliniu kibernetinio saugumo centru, Ryšių reguliavimo tarnyba, Valstybine duomenų apsaugos inspekcija ir Policijos departamentu pagal kompetenciją įgyvendinti kibernetinio saugumo politiką[11].

Kibernetinis saugumas Lietuvoje neatsiejamas nuo ES Kibernetinio saugumo strategijos, Komisijos direktyvos pasiūlymo dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti[12] ir susijęs su ES strategijos „Europa 2020“ dalimi

[4] Lietuvos Respublikos Vyriausybės 2006-12-06 nutarimu Nr. 1211 patvirtinta Lietuvos Respublikos elektroninių ryšių tinklų ir informacijos saugumo įstatymo koncepcija.

[5] Lietuvos Respublikos Vyriausybės 2011-06-29 nutarimu Nr. 796 patvirtinta Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa.

[6] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428.

[7] Lietuvos Respublikos krašto apsaugos ministro 2014-12-29 įsakymu Nr. V-1321 patvirtinti Kibernetinio saugumo ir telekomunikacijų tarnybos prie Krašto apsaugos ministerijos nuostatai.

[8] Lietuvos Respublikos Vyriausybės 2015-04-23 nutarimu Nr. 422 patvirtinta Kibernetinio saugumo taryba ir jos reglamentas.

[9] Lietuvos Respublikos Vyriausybės 2001-03-14 nutarimu Nr. 291 patvirtinti Lietuvos Respublikos vidaus reikalų ministerijos nuostatai 8.6. p.

[10] Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas, 2011-12-15 Nr. XI-1807 (akto redakcija, galiojanti nuo 2015-01-01 su paskutiniu pakeitimu, atliktu 2014-11-06 įstatymu Nr. XII-1302), 5 str. 4 d.

[11] Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014-12-11 Nr. XII-1428, 4 str. 2 ir 3 d.

[12] Europos Sąjungos vyriausiojo įgaliotinio užsienio reikalams 2013-02-07 bendras komunikatas JOIN (2013) 1 final Europos Parlamentui, Tarybai, Europos ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos Sąjungos kibernetinio saugumo strategija“ kartu su Europos Komisijos pasiūlymu dėl Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti COM(2013) 48 final.

„Europos skaitmeninė darbotvarkė“ [13], kurioje pabrėžiama, jog visos suinteresuotosios šalys turi kartu stengtis užtikrinti informacinių ir ryšių technologijų infrastruktūros saugumą ir atsparumą, daugiausia dėmesio skiriant prevencijai, parengčiai ir informuotumui, kad būtų sukurti veiksmingi ir suderinti reagavimo į naujas ir vis sudėtingesnes kibernetines atakas ir el. nusikaltimus mechanizmai.

Valstybės mastu nėra sukaupta tikslių duomenų apie kibernetinio saugumo ir el. informacijos saugos priemonėms įgyvendinti naudojamas lėšas. Valstybinių auditorių vertinimu, 2011–2014 m. kibernetinio saugumo ir el. informacijos saugos priemonėms įgyvendinti panaudota apie 20,9 mln. EUR, o nuo 2015 m. iki 2020 m. planuojama panaudoti dar apie 15,6 mln. EUR valstybės biudžeto asignavimų, ES ir kitos tarptautinės finansinės paramos lėšų.

Audito tikslas – įvertinti, ar užtikrinamas kibernetinis saugumas Lietuvoje. Tikslui pasiekti vertinome, ar:

- sukurta veiksminga kibernetinio saugumo sistema;
- užtikrinamas kibernetinis saugumas valstybinėse įstaigose.

Audito metu analizavome esamą kibernetinio saugumo ir el. informacijos saugos teisinį reguliavimą, strateginį planavimą, valdymo praktiką, šiai sričiai skiriamas ir naudojamas lėšas. Vertinome, ar pasiekti planavimo dokumentuose nustatyti kibernetinio saugumo ir el. informacijos saugos rezultatai ir kaip valstybės įstaigos užtikrina kibernetinį saugumą, ar tinkamai taiko kibernetinio saugumo technines ir organizacines priemones.

Auditą atlikome Vidaus reikalų ministerijoje ir Krašto apsaugos ministerijoje. Duomenis ir informaciją rinkome iš šių ministerijų valymo srities įstaigų, kitų ministerijų, Vyriausybės kanceliarijos, Ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Valstybės saugumo departamento, Lietuvos mokslo ir studijų institucijų kompiuterinio tinklo (LITNET) tarybos atstovų ir Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos. Bendravome su asociacijos „INFOBALT“ kibernetinio saugumo specialistais. Audito metu aštuoniolikoje įstaigų atlikome patikras vietoje. Analizavome užsienio šalių patirtį, gerąją praktiką, mokslinių tyrimų duomenis ir visuomenės informavimo priemonėse skelbiamą informaciją, susijusią su audituojama sritimi.

Audituojamas laikotarpis – 2011–2015 m. I pusmetis. Pokyčių analizei buvo naudojami ankstesnių laikotarpių duomenys.

Nustatėme, kad iki šiol valstybėje nepakankamai efektyviai sprendžiami kibernetinio saugumo ir jo atsparumo didinimo klausimai. Akcentuojant tik reagavimą į incidentus ir jų užkardymą kibernetinėje erdvėje, pamirštami tradiciniai el. informacijos saugos valdymo klausimai (informacijos konfidencialumas, vientisumas, prieinamumas) ir nuo 2015 m. neskiriama pakankamai dėmesio šios srities plėtrai, teisės aktų rengimui, organizacinės struktūros tobulinimui ir kt.

Be to, viešajame sektoriuje įgyvendinamos nepakankamos šios srities organizacinės ir techninės priemonės. Valstybinės įstaigos savo veikloje nepakankamai dėmesio skiria kibernetiniam saugumui užtikrinti, o naujai priimtas Kibernetinio saugumo įstatymas neišsprendžia visų su kibernetiniu saugumu susijusių grėsmių. Šis įstatymas bus veiksmingas tiek, kiek bus veiksmingi jį lydintieji teisės aktai, įstaigų praktinė patirtis ir gebėjimai valdyti kibernetinį saugumą ir el. informacijos saugą, parinkti efektyvias reikalavimų įgyvendinimo kontrolės priemones, spręsti

[13] Europos Komisijos 2010-08-26 komunikato KOM(2010) 245 galutinis/2 Europos Parlamentui, Tarybai, Europos Ekonomikos ir socialinių reikalų komitetui ir Regionų komitetui „Europos Skaitmeninė darbotvarkė“ 2.3 dalis.

šios srities specialistų kompetencijos problemas. Nepašalinus šių trūkumų gali nukentėti ne tik administracinės ir viešosios paslaugos, informacija, bet ir kiekvienas pilietis, šalies prestižas, pasitikėjimas naujomis technologijomis.

Siekiant tobulinti kibernetinio saugumo reglamentavimo kokybę, spręsti esamas planavimo ir finansavimo problemas, pasiūlėme Vyriausybei nustatyti bendras kibernetinio saugumo, el. informacijos saugos strategines kryptis ir joms pasiekti būtinas priemones, konsoliduoti el. informacijos saugos valdymą. Skirti įstaigą, kuri koordinuotų šios srities reikalavimų rengimą, jų suvienijimą ir nustatyti lėšų skyrimo, panaudojimo prioritetus ir kriterijus.

Krašto apsaugos ir Vidaus reikalų ministerijoms rekomendavome peržiūrėti esamus kibernetinio saugumo, el. informacijos saugos reikalavimus, juos suderinti, patvirtinti šios srities trūkstamas nuostatas, metodinius dokumentus ir numatyti priemones, skirtas konsultuoti ir informuoti kibernetinį saugumą, el. informacijos saugą užtikrinančius subjektus aktualiais šios srities klausimais.

Įvertinę audito metu surinktus įrodymus, pateikiame valstybinio audito išvadas ir rekomendacijas.

IŠVADOS

1. Kibernetinio saugumo ir el. informacijos saugos sritys Lietuvoje atskirtos įstatymų lygiu, tačiau juos įgyvendinti nėra lengva, o bendra valstybės saugumo būklė šiose srityse kol kas negerėja, nes:

   1.1. El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa, kurioje planuota pasiekti daugiausia rezultatų šioje srityje, vykdoma nerezultatyviai (bendras programos tikslų įgyvendinimas 2015 m. rugsėjo mėn. siekia 21 proc.). Nustatyti ne visi su kibernetinio saugumo ir el. informacijos sauga susijusių planavimo dokumentų tarpusavio ryšiai, vėluojama įgyvendinti planavimo dokumentuose numatytas priemones (1.1 poskyris, 11–14 psl.);

   1.2. laiku neparengti teisės aktai, reglamentuojantys kibernetinį saugumą, nėra sprendimo dėl el. informacijos saugos, kibernetinio saugumo ir kitų su informacijos sauga susijusių sričių reikalavimų peržiūrėjimo ir suderinimo (1.2 poskyris, 15–17 psl.);

   1.3. 2015 m. pradėjusi veikti kibernetinio saugumo valdymo sistema nesudaro visų su el. informacijos sauga susijusių sričių darnaus valdymo sąlygų: neišvengiama dalinio įstaigų veiklos dubliavimo, trūksta kompetencijos atskyrimo formuojant ir įgyvendinant kibernetinio saugumo ir el. informacijos saugos politiką (1.3 poskyris, 18–19 psl.);

   1.4. kibernetiniam saugumui ir el. informacijos saugai reikalingų lėšų skyrimas ir panaudojimas (suplanuota 2015–2020 m. 15,6 mln. EUR) vykdomas šių sričių politiką formuojančioms Krašto apsaugos ir Vidaus reikalų ministerijoms nenustačius lėšų skyrimo prioritetų ir kriterijų, neturint duomenų apie faktinę įstaigų kibernetinio saugumo ir el. informacijos saugos būklę, panaudotas lėšas (2011–2014 m. 20,9 mln. EUR) ir jų poveikį (1.4 poskyris, 19–22 psl.).

2. Kibernetinio saugumo ir el. informacijos saugos techninių ir organizacinių priemonių įgyvendinimas viešajame sektoriuje nepakankamas, netinkamai pasiruošta reaguoti į kibernetinėje erdvėje kylančias grėsmes, nes tikrintos įstaigos:

   2.1. vidutiniškai taiko 25 proc. šiai sričiai užtikrinti rekomenduojamų organizacinių priemonių, pagrindiniai trūkumai susiję su saugumo valdymo sistemos kūrimu, incidentų valdymu, veiklos tęstinumo užtikrinimu, personalo kompetencijos tobulinimu ir išoriniu bendradarbiavimu;

   2.2. tinkamai įgyvendina tik 39 proc. rekomenduojamų techninių priemonių ir lieka pažeidžiamos dėl netinkamo saugios konfigūracijos nustatymo, el. ryšių tinklų, mobilių ir kitų technologijų valdymo (2 skyrius, 23–26 psl.).

REKOMENDACIJOS

Lietuvos Respublikos Vyriausybei:

1. Siekiant užtikrinti kibernetinį saugumą ir jo atsparumo didinimą, tobulinti esamą planavimą, teisinį reguliavimą ir finansų valdymą:

   1.1. nustatyti bendras kibernetinio saugumo, el. informacijos saugos strategines kryptis ir joms pasiekti būtinas priemones (1.1 išvada);

   1.2. skirti įstaigą, kuri valstybės mastu koordinuotų kibernetinio saugumo, el. informacijos saugos reikalavimų rengimą, jų suvienijimą (1.2 išvada);

   1.3. konsoliduoti el. informacijos saugos valdymą (1.3 ir 2 išvados);

   1.4. valstybės mastu nustatyti kibernetiniam saugumui, el. informacijos saugai reikalingų lėšų skyrimo ir panaudojimo prioritetus, kriterijus, stebėsenos ir kontrolės mechanizmą (1.4 išvada).

Lietuvos Respublikos krašto apsaugos ir vidaus reikalų ministerijoms:

2. Siekiant gerinti kibernetinio saugumo reglamentavimo kokybę ir efektyvumą, mažinti administracinę naštą šiuos reikalavimus įgyvendinančioms ir jų įgyvendinimą stebinčioms įstaigoms:

   2.1. peržiūrėti esamus kibernetinio saugumo, el. informacijos saugos reikalavimus, juos suderinti ir (arba) patvirtinti trūkstamas nuostatas ir metodinius dokumentus (1.2 ir 2 išvados);

   2.2. užtikrinti įstaigų konsultavimą ir informavimą kibernetinio saugumo ir el. informacijos saugos (valdymo sistemos kūrimas, incidentų valdymas, veiklos tęstinumo užtikrinimas, personalo kompetencijos tobulinimas, išorinis bendradarbiavimas, saugios konfigūracijos nustatymas, tinklo saugumas, mobilių ir kitų technologijų valdymas) klausimais (2 išvada).

Rekomendacijų įgyvendinimo priemonės ir terminai pateikti 1 priede.