KIBERNETINIO SAUGUMO IR TELEKOMUNIKACIJŲ TARNYBA
PRIE KRAŠTO APSAUGOS MINISTERIJOS
NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

2016 METŲ NACIONALINIO KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

Vilnius

2017 m.

TURINYS

KAS YRA NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Lietuvos Nacionalinis kibernetinio saugumo centras (toliau – NKSC) oficialiai savo veiklą pradėjo 2015 m. sausio 1 d., įsigaliojus Lietuvos Respublikos kibernetinio saugumo įstatymui (2014 m. gruodžio 11 d. Nr. XII-1428)[1]. NKSC, pagal kompetenciją įgyvendindamas kibernetinio saugumo politiką ir vykdydamas valstybės informacinių išteklių (toliau – VII) ir ypatingos svarbos informacinių infrastruktūrų (toliau – YSII[2]) kibernetinių incidentų valdymo padalinio veiklą, rengia ir teikia pasiūlymus krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų VII ir YSII, atlieka šių subjektų atitikties organizaciniams ir techniniams kibernetinio saugumo reikalavimams stebėseną. NKSC turi pareigą teikti konsultacijas ir rekomendacijas VII ir YSII valdytojams kibernetinio saugumo klausimais, analizuoti nacionalinę kibernetinio saugumo situaciją ir rengti nacionalinio kibernetinio saugumo būklės ataskaitas. Vienas NKSC uždavinių – rūpintis, kad YSII valdytojai turėtų kibernetinės gynybos planus ir gebėtų juos vykdyti. NKSC prioritetas – svarbiausių Lietuvai VII ir YSII atsparumo kibernetinėms grėsmėms didinimas ir neatidėliotinas profesionalus kolektyvinės gynybos principais paremtas reagavimas į VII ir YSII vykstančius kibernetinius incidentus.

Šių svarbių nacionalinių funkcijų vykdymui užtikrinti buvusi Ryšių ir informacinių sistemų tarnyba 2015 metais buvo reorganizuota į Kibernetinio saugumo ir telekomunikacijų tarnybą, jai pavedant vykdyti ir NKSC funkcijas. Šis sprendimas leido NKSC veiklą pradėti turint patyrusių specialistų būrį – Lietuvos Respublikos krašto apsaugos sistemos profesionalus, nuo 2008 m. užtikrinančius krašto apsaugos sistemos informacinių sistemų ir telekomunikacijų kibernetinį saugumą.

NKSC keliami dideli tikslai, kurių vienas – sparčiai išvystyti gebėjimus kibernetinio saugumo situacijai Lietuvoje stebėti ir grėsmėms aptikti. Šie gebėjimai turi leisti centro analitikams laiku gauti tikslią informaciją apie svarbių šalies informacinių infrastruktūrų kibernetinę būklę – nustatyti, ar infrastruktūra nėra pažeista virusų ir veikiama kibernetinių nusikaltėlių, aptikti ir prognozuoti kibernetinių atakų vektorius, grėsmių šaltinius ir potencialius atakų taikinius. Kaip

[1] https://www.e-tar.lt/portal/lt/legalAct/5468a25089ef11e4a98a9f2247652cf4

[2] *Ypatingos svarbos informacinė infrastruktūra (YSII) Kibernetinio saugumo įstatyme apibrėžta kaip privataus ar viešojo administravimo subjekto valdoma informacinė infrastruktūra, kurioje įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams. Iki šiol YSII dar nėra identifikuota, o jos sąrašas patvirtintas Lietuvos Respublikos Vyriausybės, tačiau, atsižvelgus į Vidaus reikalų ministerijos ir Krašto apsaugos ministerijos sprendimus, NKSC rūpinasi įmonių ir organizacijų, kurios potencialiai yra YSII, kibernetiniu saugumu.*

2015 metais, taip ir 2016-taisiais, NKSC diegė technines kibernetinės erdvės stebėsenos priemones ir stebimą erdvę išplėtė iki daugiau kaip dvidešimties skirtingų įstaigų ar organizacijų informacinės infrastruktūros. Stebėsenos sistemos plėtra davė akivaizdžių rezultatų – tapo žinoma reali kibernetinio saugumo padėtis nemažoje dalyje valstybės institucijų, o per 2016 metus rasta ir neutralizuota daugiau nei 120 kitomis priemonėmis neaptinkamos žalingos programinės įrangos, tame tarpe ir tokios, kuri siejama su užsienio žvalgybų tarnybų veikla.

Per praėjusius metus NKSC toliau formavo kompetentingą komandą – išplėtė padalinius, taip padidindama analitinį NKSC pajėgumą. Kolektyvo branduolį sudaro kibernetinio saugumo strategai, analitikai ir techniniai ekspertai, išmanantys naujausias informacines technologijas, kibernetinę gynybą ir kibernetinių įvykių tyrimus. 2016 metų pabaigoje NKSC sukūrė ir su kitomis organizacijomis testuoja Kibernetinio saugumo informacinį tinklą, skirtą organizacijoms – tinklo nariams – keistis aktualia kibernetinių incidentų užkardymo ir valdymo informacija.

NKSC ryšių informacija pateikiama svetainėje www.nksc.lt.

SANTRAUKA

Šios ataskaitos tikslas – vykdyti Kibernetinio saugumo įstatyme numatytą NKSC pareigą informuoti krašto apsaugos ministrą apie kibernetinio saugumo būklę Lietuvoje.

Kibernetinio saugumo būklė Lietuvoje vertinama analizuojant įvairių organizacijų pateiktą informaciją, NKSC techninėmis stebėsenos priemonėmis surinktus duomenis, iš kitų šaltinių gautą informaciją apie kibernetines grėsmes VII ir YSII, taip pat kovos su šiomis grėsmėmis Lietuvoje būdus ir jų efektyvumą.

Lietuvos kibernetinio saugumo būklė – įvertinimas, kuriame atsispindi santykis tarp patiriamos žalos ar potencialiai žalą galinčių sukelti grėsmių ir atsako, kurį Lietuvos ūkio subjektai formuoja kibernetinėms grėsmėms atremti.

2016 metais Lietuvoje įvyko keliolika rezonansinių kibernetinių išpuolių, **NKSC fiksavo 3 kartus daugiau nei 2015 metais standartinėmis priemonėmis neaptinkamų kibernetinių incidentų organizacijų kompiuterių tinkluose, net 5 kartus suintensyvėjusią tinklų išorinio perimetro kibernetinę žvalgybą** ir išaugusias grėsmes, susijusias su kompiuterių naudotojų apsilankymais žalingą kodą platinančiose užvaldytose interneto svetainėse. Didžioji dauguma incidentų kilo dėl elementarios kibernetinės higienos nesilaikymo, vadybos ir saugos standartų ar gerosios pasaulyje pripažintos praktikos bei naujai išleistų kibernetinio saugumo klausimus apibrėžiančių LR norminių aktų nesilaikymo. Pažymėtina, kad kaip ir 2015 metais, tik pavienės didelės organizacijos turėjo tinkamus ir pakankamus pajėgumus, galinčius valdyti kibernetiniam saugumui kylančias grėsmes.

NKSC, analizuodama interneto svetainių saugos problematiką, atkreipia dėmesį, kad interneto **svetainės paprastai yra silpnai dokumentuotos, todėl, kaip ir ankstesniais metais, saugos prasme yra prižiūrimos nepatenkinamai.** Siūlytina teisės aktais reglamentuoti interneto svetainių gyvavimo ciklo formalizavimą, kad organizacijos, kurios yra svetainių turinio savininkės, privalėtų įteisinti valdomas interneto svetaines, nusistatant tvarkas, kurios reglamentuoja svetainių kūrimo, eksploatavimo bei modernizavimo procesus bei parengti saugos politiką apibrėžiančius dokumentus, kaip tai privalu daryti steigiant informacines sistemas.

NKSC ir toliau masiškai aptinka tinkluose veikiančius kompiuterius, kurie naudoja pasenusią operacinę ir taikomąją programinę įrangą, apie kurios pažeidžiamumus, leidžiančius įsibrauti į organizacijų kompiuterių tinklus pačiais paprasčiausiais būdais yra visuotinai žinoma.

2016 metais pastebėta, kad lyginat su 2015 metais, kelis kartus padidėjo bandymai įsilaužti į organizacijų tinklus pasinaudojant kompiuterių naudotojų naivumu ir jiems siunčiamuose laiškuose esančiomis nuorodomis nukreipti juos į užkratą turinčias svetaines, iš kurių šis užkratas automatiškai užkrečia naudotojų kompiuterius. Toks užkrato infiltravimo būdas yra itin efektyvus, tad artimiausioje ateityje ši metodika bus ir toliau naudojama piktavalių.

Praėjusiais metais Lietuvoje vyko eilė elektroninių paslaugų trikdymo kibernetinių atakų. Nors paviršutiniškai vertinant tai atrodė kaip įprastinis svetainių pasiekiamumo trikdymas, tačiau **NKSC, remdamasi įvairiais požymiais, tai įvertino, kaip specifinę Lietuvos elektroninių ryšių tinklų infrastruktūros atsparumo žvalgybą rengiantis didesnio masto kibernetinėms operacijoms**.

2016 metais NKSC savo stebimoje Lietuvos kibernetinės erdvės dalyje aptiko **kelis kompiuterių užkrėtimo specializuota šnipinėjimui naudojamos programinės įrangos atvejus** (angl. Advanced Persistant Threat, APT), siejamus su užsienio valstybių žvalgybos tarnybomis ir joms dirbančiomis stipriomis ir gerai finansuojamomis programišių grupėmis.

NKSC, siekdama įvertinti valstybės informacinių išteklių valdytojų požiūrį į naujai priimtus kibernetinį saugumą reglamentuojančius teisės aktus, vykdė elektroninę valstybinių įstaigų apklausą kibernetinio saugumo tema. Ši apklausa, išryškino rimtą problemą - **įstaigos ignoruoja Lietuvos teisės aktų reikalavimus,** juos mažai nagrinėja, netaiko veikloje ir net neplanuoja vyriausybės nustatytais terminais įgyvendinti nustatytų kibernetinio saugumo reikalavimų. Antra, ne mažesnės svarbos identifikuota problema - įvairių dydžių, brandos, išteklių ir galimybių **valstybinėms įstaigoms yra sudėtinga įgyvendinti visą šiuo metu teisės aktais nustatytą kibernetinio saugumo reikalavimų aibę**.

Pažymėtina, kad Lietuvoje iki 2016 metų pabaigos nebuvo patvirtintas ypatingos svarbos informacinės infrastruktūros ir jų valdytojų sąrašas. Todėl **ypatingos svarbos paslaugas teikiančios Lietuvos privataus kapitalo įmonės ir organizacijos neturėjo prievolės vykdyti Lietuvos Vyriausybės nustatytų privalomųjų kibernetinio saugumo reikalavimų.**

Kibernetinio saugumo būklė Lietuvoje stiprinama ne tik diegiant kibernetinio saugumo organizacines ir technines priemones, bet ir vykdant tikslines pratybas. 2016 metais buvo surengtos

pirmosios nacionalinės kibernetinio saugumo pratybos "Kibernetinis skydas", kuriose dalyvavo daugiau nei 40 Lietuvos valstybės bei kitų institucijų, įskaitant akademinės bendruomenės atstovus..

Nepaisant kai kurių pozityvių kibernetinio saugumo tendencijų , NKSC manymu, **kibernetinio saugumo lygis Lietuvoje yra nepatenkinamas**. NKSC prognozuoja, kad kibernetinių incidentų nemažės, o tikslinių kibernetinių atakų skaičius vien didės. Ypač nerimą kelia stebimas kibernetinių išpuolių sukeliamas vis didėjantis efektas fizinėje plotmėje, kai paveikiami pramoniniai procesai, nuo kurių priklauso gyventojų kasdieninė veikla ir ūkio subjektų teikiamos paslaugos.

NKSC vertinimu, siekiant užkardyti didelio masto ir rimtą žalą sukeliančias kibernetines atakas, Lietuvos įmonės ir organizacijos turėtų skirti daugiau dėmesio kibernetiniam saugumui, kibernetinio saugumo politiką nustatančioms institucijoms būtina suformuluoti bei patvirtinti šiuolaikinius iššūkius atitinkančią **Lietuvos kibernetinio saugumo strategiją**, kuri apimtų ir visos Lietuvos kibernetinės erdvės gynybos nuo kibernetinių išpuolių aspektą. Kibernetinio saugumo politiką įgyvendinančios institucijos bei ypatingos svarbos informacinių infrastruktūrų valdytojai turėtų daugiau dėmesio skirti ne tik techninei kibernetinio saugumo bazei stiprinti, bet **pasitelkus informacinės saugos ir kibernetinio saugumo specialistus, intensyviau tobulinti kibernetinių grėsmių aptikimo pajėgumus**.

LIETUVOS KIBERNETINIŲ GRĖSMIŲ ŽEMĖLAPIS

NKSC savo veikloje, kaip ir ankstesniais metais, prioritetą teikia didžiausią žalą Lietuvai galinčių sukelti kibernetinių grėsmių prevencijai ir aptikimui. NKSC išskiria tokias 2016 metais Lietuvoje dominavusias kibernetines grėsmes ir tendencijas lyginant su 2015 metais (1 pav.):

	• **pažeidžiamos interneto svetainės;**
	• **elektroninių ryšių tinklų žvalgyba;**
	• **elektroninių paslaugų trikdymas (DDoS);**
	• **žalingos programinės įrangos plitimas;**
	• **nesaugi tinklo įrenginių komunikacija;**
	• **neatnaujinta operacinių sistemų ir taikomoji programinė įranga;**
	• **socialinė inžinerija;**
	• **pramoninių procesų valdymo sistemų sąsaja su internetu.**

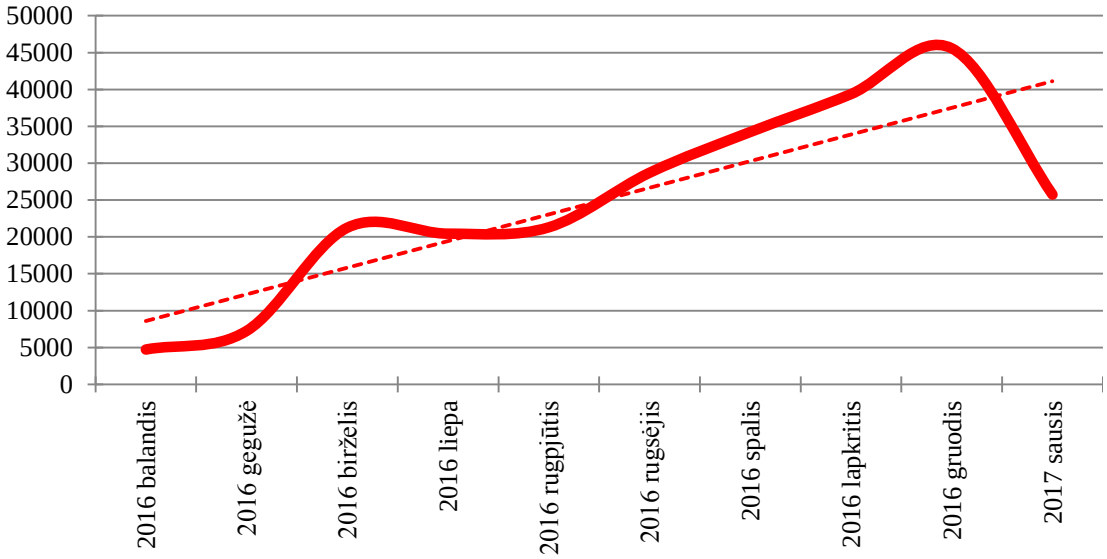
1 pav. Kibernetinės grėsmės 2016 m. ir tendencijos, lyginant su 2015 m.

Apibendrinant, NKSC 2016 metais stebėjo šiek tiek mažėjantį itin pažeidžiamų Lietuvos svetainių skaičių, sumažėjusį kiekį atmestinai valdomų tinklo įrenginių viešuose elektroniniuose tinkluose ir kiek sumažėjusį internetu valdomų pramoninių procesų sistemų kiekį. Kitų grėsmių dinamika augo. Lyginant su 2015 metais, padaugėjo rezonansinių kibernetinių incidentų, kai buvo trikdomos elektroninės paslaugos paslaugų atkirtimo kibernetinėmis atakomis.

ELEKTRONINIŲ RYŠIŲ TINKLŲ ŽVALGYBA

Prievadų skenavimas iš užsienio valstybių išaugo net 5 kartus.

2016 metais NKSC stebėjo ir sekė elektroninių ryšių tinklų skenavimo tendencijas. Dalį tinklų skenavimo atvejų, dėl specifinės skenuojančių šaltinių elgsenos, NKSC priskyrė kibernetinei žvalgybai. 2016 metais prie interneto prijungtų įrenginių prievadų skenavimas, lyginant su 2015 metais, nepasižymėjo ypatingais bruožais, išskyrus kelis atskirus aktyvumo epizodus. Prievadų skenavimo, kaip paprastos, tačiau efektyvia išliekančios kibernetinės žvalgybos priemonės panaudojimo apimtys nuolat augo. **Per 2016 metus NKSC stebimoje kibernetinėje erdvėje prievadų skenavimas iš užsienio valstybių išaugo net 5 kartus** (2 pav.).

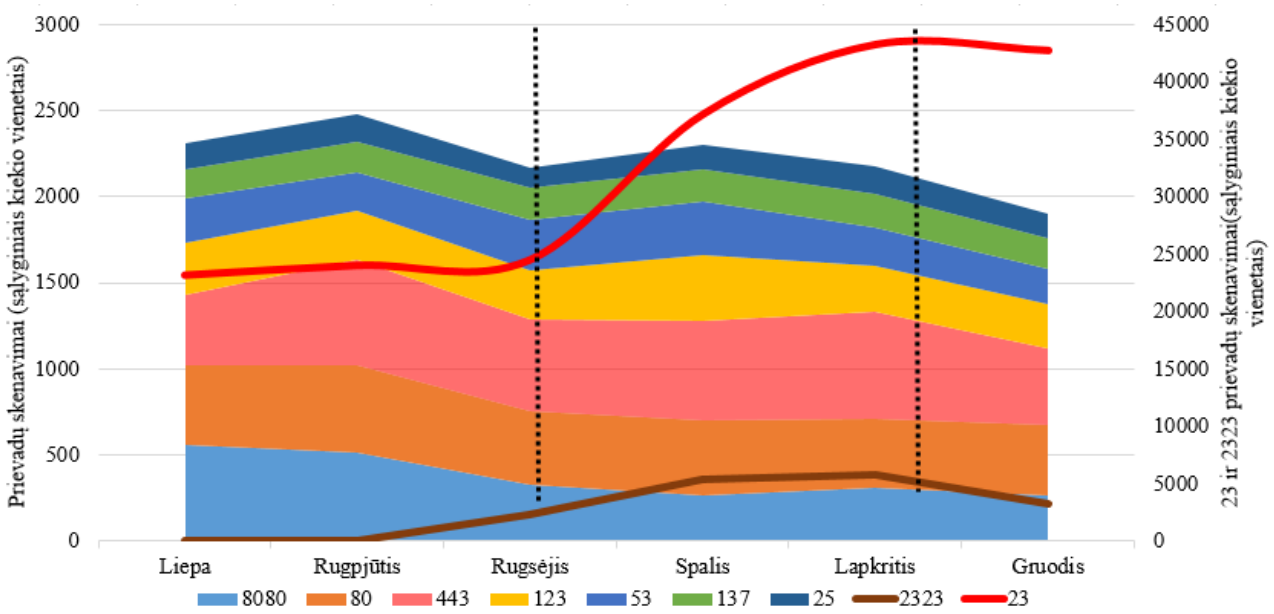


2 pav. Vienos organizacijos IP adresų aibės skenavimo statistika.

Ši dinamika parodo, kad, visų pirma, skenavimas ir toliau išlieka populiariu būdu sužinoti elektroninių tinklų infrastruktūroje veikiančių tinklo įrenginių atvirus prievadus, kurių specifinė informacija leidžia spręsti apie įrenginio tipą, veikiančią programinę įrangą ir galimas saugumo spragas, kurias išnaudojant galima nesankcionuotai pasiekti informacinius išteklius, valdyti prie tinklo prijungtą techninę įrangą ar kontroliuoti elektroninius valdiklius.

Išanalizavus stebimos kibernetinės erdvės skenavimo foną, pastebėta, kad kintant skenavimo dinamikai, smarkiai nekito atskirų prievadų skenavimo apimtys. 2016 metais piktavaliai internete tradiciškai ieškojo spragų, kurios leistų privilegijuotą prieigą prie įrenginių ir informacinių išteklių

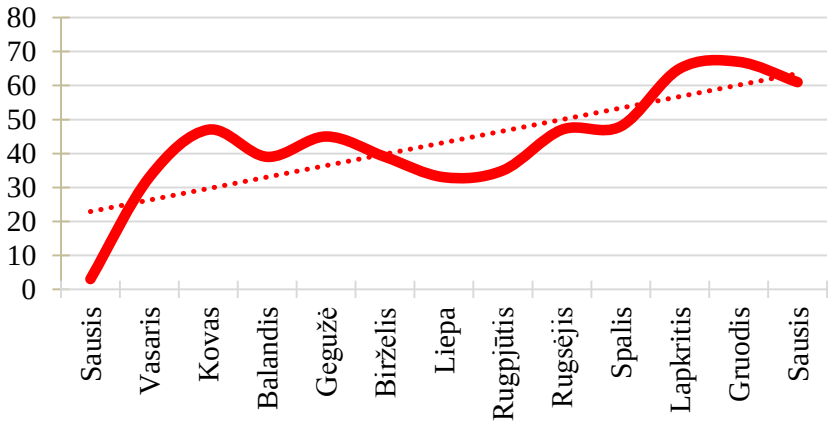
(pvz., tinklo maršrutizatoriaus valdymo ar interneto svetainės turinio administravimo posistemio).2016 metų skenavimo išskirtinumas – suaktyvėjusi prisijungimo prie įrenginių, kurie gali būti valdomi nuotoliniu būdu, įsk. interneto daiktų įrenginius[3], būdų paieška. Paprastai domėjimasis įrenginiais, kurie gali būti valdomi nuotoliniu būdu 23-čiu prievadu, yra dešimt kartų didesnis, lyginant šio ir kitų prievadų skenavimo apimtis, tačiau 2016 metų rugsėjo – lapkričio mėnesiais toks skenavimas ženkliai išaugo. NKSC vertinimu, tai susiję su Mirai botneto (išnaudojančio IoT pažeidžiamumus) veikla[4]. Tiesa, su šio rezonansinį atgarsį sukėlusio botneto veikimu susijusių prievado (2323 ir 7547[5]) skenavimo aktyvumas ypatingai nekito (3 pav.)



3 pav. 2016 metų antrojo pusmečio prievadų skenavimo statistika, išskirianti specifinę elektroninių ryšių tinklų kibernetinę žvalgybą

2016 metais NKSC stebėjo nežymų specializuotų įrenginių – pramoninių procesų valdymo įrangos (SCADA, PLC[6]) žvalgymo augimą. Kaip ir 2015 metais, Lietuvos interneto erdvėje buvo galima aptikti tokių įrenginių, kurie neturėtų būti pasiekiami internetu. Šių įrenginių žvalgymo tendenciją iliustruoja vienos Lietuvos organizacijos, kuri naudoja SCADA įrangą, IP adresų aibės specifinis skenavimas. Grafike (4 pav.) pavaizduota auganti SCADA prievadų skenavimo tendencija ženkliai nesiskiria nuo bendros tinklų žvalgybos intensyvėjimo dinamikos.

[3] *(angl., Internet of Things, IoT – prie interneto prijungtos vaizdo stebėjimo kameros, spausdintuvai, išmanieji televizoriai ir pan.)*
[4] *Heightened DDoS Threat Posed by Mirai and Other Botnets, https://www.us-cert.gov/ncas/alerts/TA16-288A*
[5] *Mirai Evolving: New Attack Reveals Use of Port 7547, https://securityintelligence.com/mirai-evolving-new-attack-reveals-use-of-port-7547/*
[6] *SCADA - angl. Supervisory control and data acquisition - kompiuterizuota, tinklais valdoma programuojama pramoninių procesų valdymo įranga; PLC - angl. Programmable Logic Controller - programuojami valdikliai (laiko rėlės, kiti procesą logiškai valdantys elementai).*



4 pav. Pramoninių procesų valdymo įrangos žvalgymo tinkluose dinamika 2016 metais.

Lietuvos interneto erdvė yra žvalgoma iš įvairių geografinių vietų. Dažniausiai fiksuojamos šalys – JK, Rusijos Federacija, Kinija. Žemiau pateikiamoje lentelėje (5 pav.) atsispindi vienos Lietuvos didelės valstybinės organizacijos kibernetinio perimetro žvalgymo statistika pagal šalis, kuriose registruoti žvalgyme dalyvavę IP adresai. NKSC rekomenduoja organizacijoms, neteikiančioms tarptautinių paslaugų savo interneto prieigoje, blokuoti aktyviausiai žvalgyboje dalyvaujančių valstybių IP adresus.

IP adresas	%	Regionas		Šalis	Laiko juosta
185.116.2XX.XXX	22	Europa		JK	GMT+0
195.182.1XX.XXX	7	Europa		Rusijos Federacija	GMT+3
192.099.0XX.XXX	7	Šiaurės amerika		Kanada	EST
198.252.1XX.XXX	7	Azija		Singapūras	GMT+8
183.060.0XX.XXX	5	Azija		Kinija	GMT+8
185.094.1XX.XXX	5	Europa		Rusijos Federacija	GMT+7
005.045.0XX.XXX	4	Europa		Nyderlandai	
217.160.0XX.XXX	4	Europa		Vokietija	GMT+1
180.097.2XX.XXX	4	Azija		Kinija	GMT+8
184.168.1XX.XXX	4	Šiaurės amerika		JAV	MST
188.214.1XX.XXX	4	Europa		Rumunija	GMT+2
121.153.1XX.XXX	3	Azija		Korėja	GMT+9
199.189.0XX.XXX	3	Šiaurės amerika		JAV	CST
208.043.0XX.XXX	3	Šiaurės amerika		JAV	EST
109.236.0XX.XXX	3	Europa		Nyderlandai	GMT+1
080.082.0XX.XXX	3	Europa		Nyderlandai	GMT+1
195.154.1XX.XXX	3	Europa		Prancūzija	GMT+1
061.240.1XX.XXX	3	Azija		Hong Kongas	GMT+8
217.117.1XX.XXX	3	Europa		Rusijos Federacija	GMT+7
125.137.1XX.XXX	3	Azija		Korėja	GMT+9

5 pav. Lietuvos valstybinės organizacijos tinklų žvalgymas pagal šaltinius - šalis.

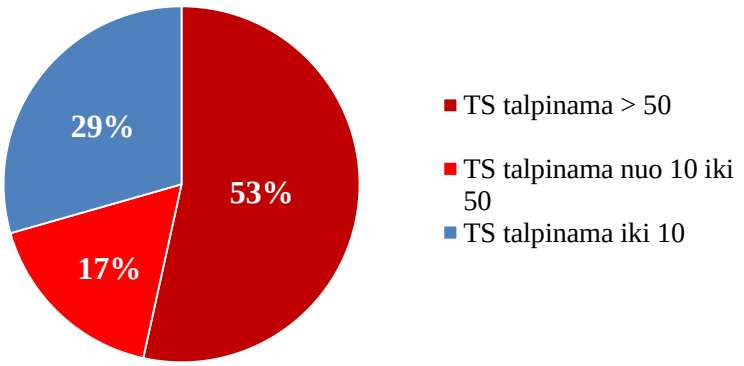
PAŽEIDŽIAMOS INTERNETO SVETAINĖS

2016 metais NKSC išanalizavo virš 800 Lietuvos viešojo sektoriaus interneto svetainių, kurias aptarnauja virš 450 tarnybinių stočių. Nustatyta, kad nemaža dalis įstaigų visiškai nesirūpina savo svetainių saugumu: egzistuoja tokių svetainių, kurių programinė įranga nėra atnaujinama daugiau kaip 10 metų. Tokios svetainės turi daugybę pažeidžiamumų, jos kelia grėsmę ir kitoms svetainėms, kurios talpinamos toje pačioje tarnybinėje stotyje.

Kaip ir 2015 metais, į penktadalį Lietuvos interneto svetainių ir toliau galima įsilaužti turint žemą kvalifikaciją ir be papildomų išteklių.

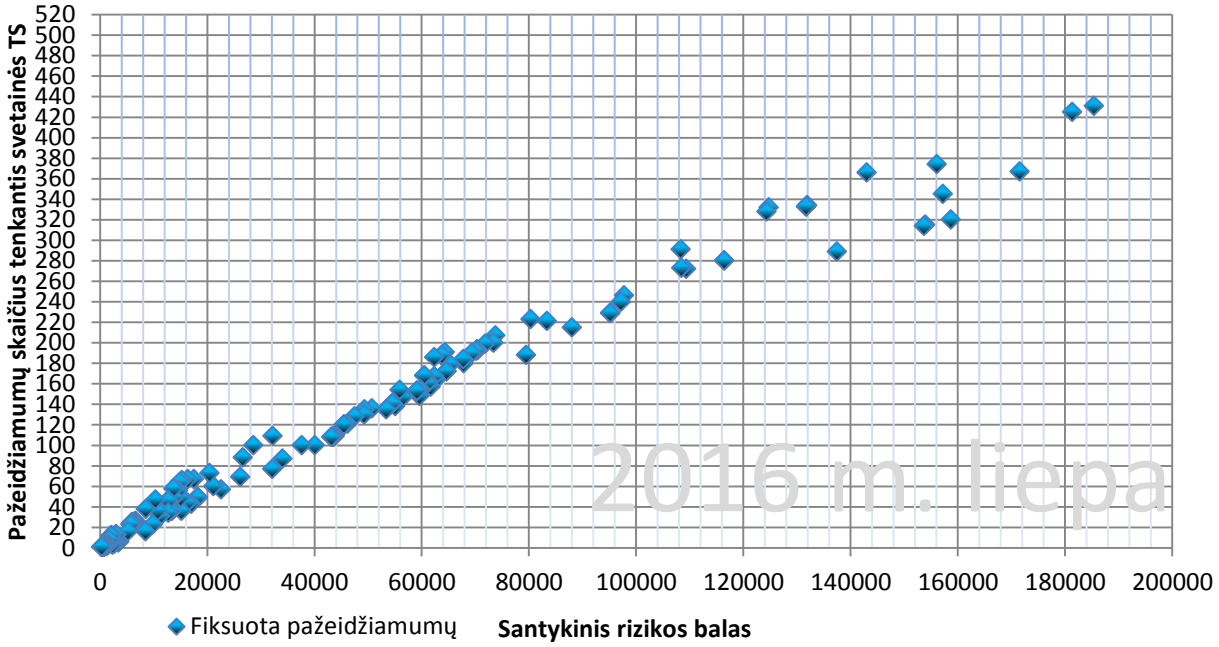
Talpinimo paslaugą perkančiai organizacijai pirkimo dokumentuose nenurodžius, kad svetainę aptarnaujanti tarnybinė stotis negali teikti kitų, su perkančiąja organizacija nesuderintų paslaugų, neapibrėžus, kokį lankytojų srautą patalpinta svetainė privalo būti pajėgi aptarnauti, talpinimo paslaugas teikiančios įmonės, mažindamos paslaugos savikainą, į tą pačią tarnybinę stotį talpina kiek įmanoma didesnį svetainių kiekį. Valstybės institucijų, politinių organizacijų ir privačių verslo subjektų tinklalapiai talpinami kartu.

Atlikus analizę matyti, kad Lietuvoje didelė dalis interneto prieglobos tarnybinių stočių aptarnauja daugiau nei 50 svetainių (6 pav.). Dėl šios priežasties svetainės tampa labiau pažeidžiamos, išauga įsilaužimo grėsmė. Įsilaužus į bent vieną tarnybinėje stotyje talpinamą svetainę, didėja tikimybė įsilaužti ir į kitas. Be to, nusikaltėliai gali įsigyti talpinimo paslaugą toje pačioje tarnybinėje stotyje ir savo svetainę panaudoti kibernetinei atakai prieš kitas svetaines ar tarnybinę stotį. Esant dideliam talpinamų interneto svetainių kiekiui, bet kurios iš svetainių pažeidžiamumo tikimybė didėja.

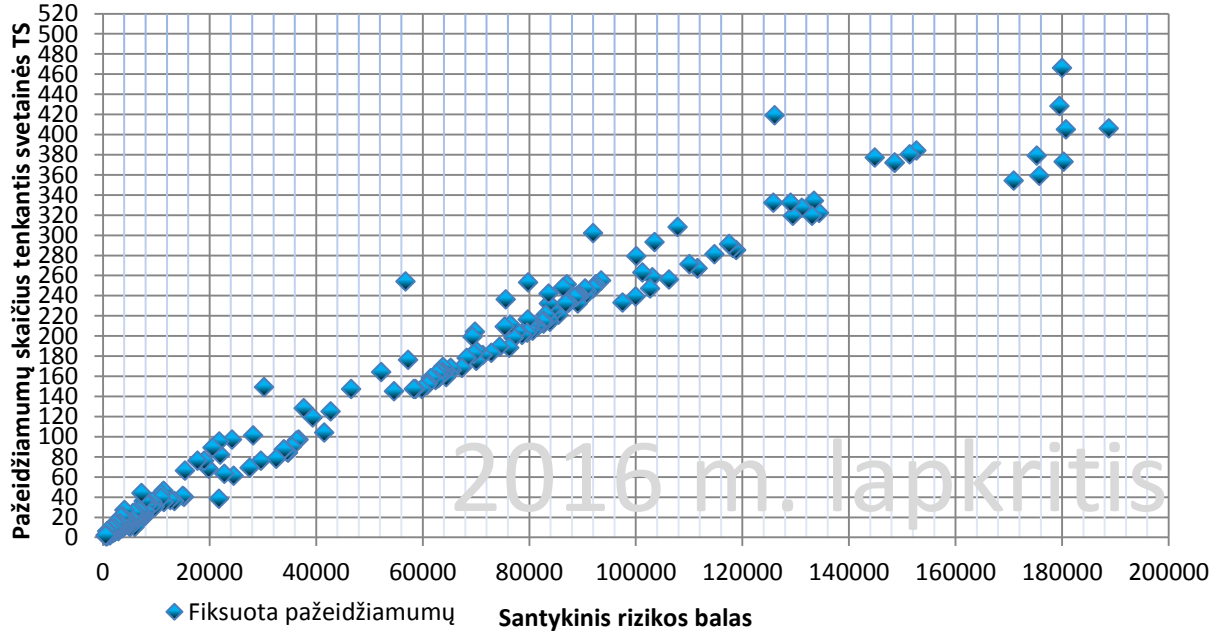


6 pav. Tiriamos imties interneto svetainių skaičius tenkantis atitinkamo apkrovimo TS.

NKSC dukart per 2016 metus atliko svetainių saugumo būklės vertinimą. Naudojant pažeidžiamumų pavojingumo skaičiavimo metodiką, nustatytas suminis pavojingumo įvertis CVSS (angl. *Common Vulnerability Scoring System*). Lyginant liepos ir lapkričio mėnesiais atliktas analizes, nustatyta, kad rimtų pažeidžiamumų turinčių tarnybinių stočių skaičius padidėjo nuo 200 iki 262. Be kita ko, stebimas bendras rizikos laipsnio didėjimas (7 pav. ir 8 pav.). Tikėtina, kad tokia tendencija yra sąlygota laiko faktoriaus, t.y. sena programinė įranga dar labiau paseno ir jai atrasta daugiau pavojingesnių pažeidžiamumų.

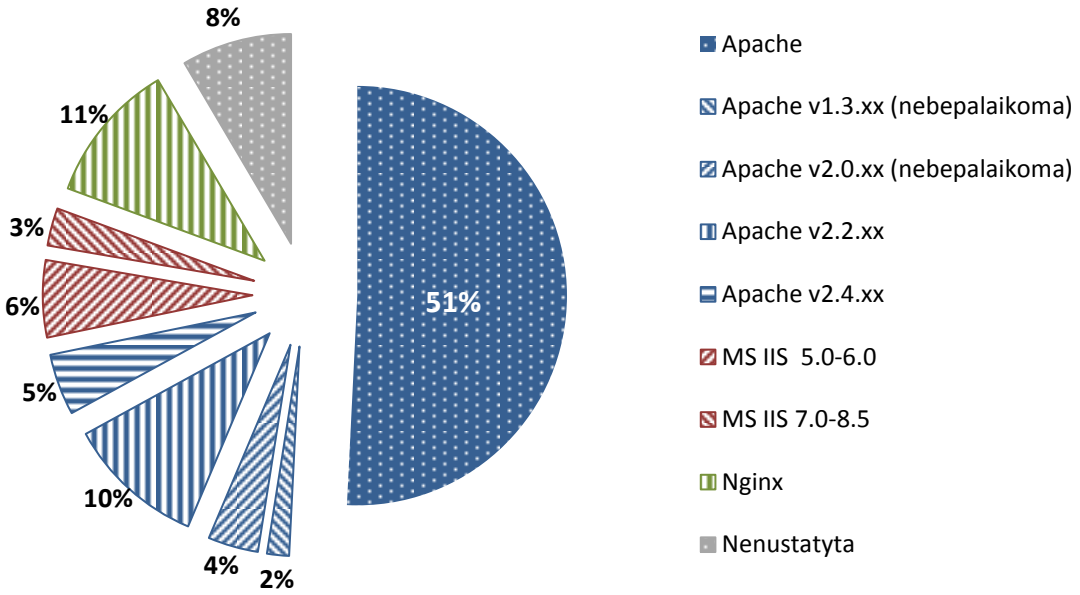


7 pav. Tarnybinei stočiai tenkantys pažeidžiamumai ir santykinis rizikos balas. 2016 metų liepa.



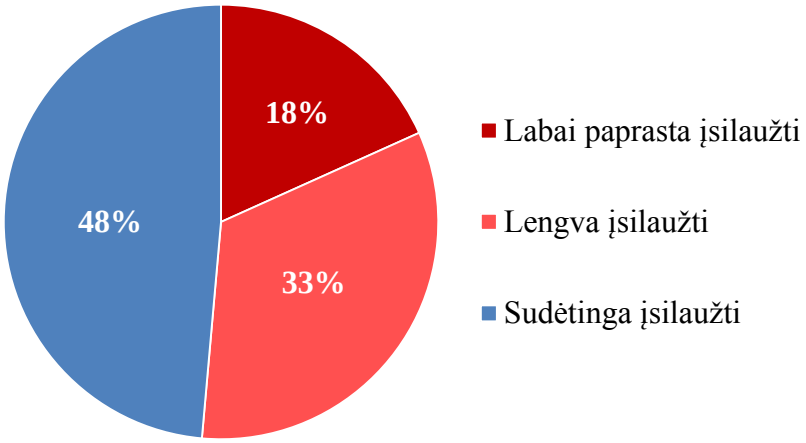
8 pav. Tarnybinei stočiai tenkantys pažeidžiamumai ir santykinis rizikos balas. 2016 metų lapkritis.

NKSC nustatė, kad daugelyje tarnybinių stočių vis dar naudojamos pasenusios, itin daug pažeidžiamumų turinčios HTTP užklausų tarnybos (9 pav.). 6 proc. analizuotų svetainių transliuoja Apache versijas, kurios šiuo metu nebepalaikomos (v.1.3.xx ir v.2.0.xx). Šių versijų atnaujinimai paskutinį kartą išleisti atitinkamai 2010 metų vasario ir 2013 metų liepos mėnesiais. Palaikomas Apache v.2.x.xx versijas naudoja 15 proc. svetainių. Daugiau nei pusei svetainių (51 proc.) buvo nustatytas HTTP užklausų tarnybos tipas (Apache), tačiau versija nustatyta nebuvo. Nesant galimybei paprastais instrumentais nustatyti svetainės naudojamos konkrečios tarnybos versijos, piktavaliui yra apsunkinamos sąlygos pakenkti svetainei pasinaudojant senesnių versijų pažeidžiamumais.



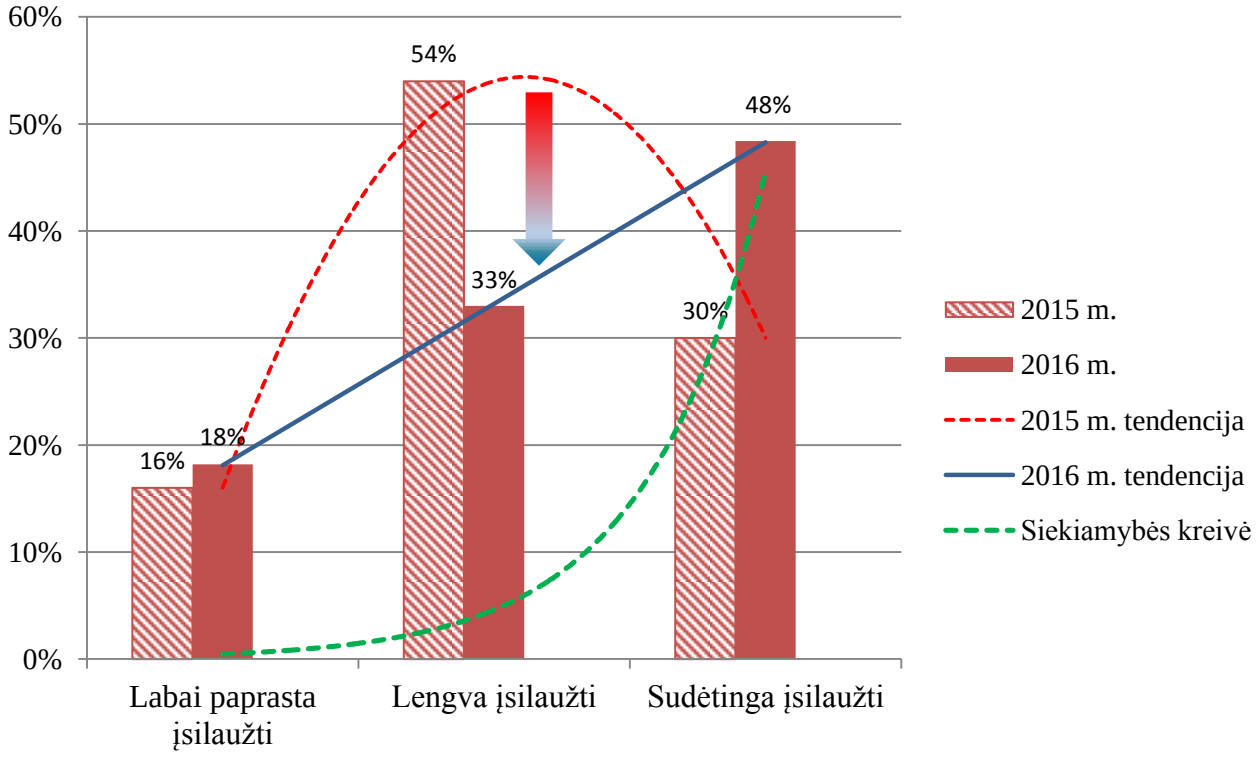
9 pav. Svetainių pasiskirstymas pagal *HTTP* užklausų tarnybos tipą.

Vertinant analizuojamas interneto svetaines pagal pažeidžiamumo išnaudojimo sudėtingumą, **nustatyta, kad į beveik penktadalį (18 proc.) galima įsilaužti neturint gilių techninių žinių ar ypatingų programavimo įgūdžių** (10 pav.**Error! Reference source not found.**). Visa įsilaužimui reikalinga informacija ir instrumentai yra laisvai pasiekiami internete. Į 33 proc. svetainių galima nesunkiai įsilaužti, tačiau reikia turėti gilesnių žinių, gauti informacijos uždarose įsilaužėlių bendruomenėse. Beveik pusė (48 proc.) analizuotų svetainių yra sąlyginai saugios. Įsilaužimui į šias svetaines reikalingos ekspertinės, dažnai ne vieno specialisto žinios, nes pažeidžiamumų išnaudojimo būdas nėra viešai paskelbtas arba yra sudėtingas.



10 pav. Lietuvos interneto svetainių pažeidžiamumas pagal įsilaužimo sudėtingumą.

Sugretinus 2015 ir 2016 metų duomenis, stebimos teigiamos svetainių saugumo būklės tendencijos (11 pav.). Pateiktame grafike matomas svetainių, į kurias lengva įsilaužti, sumažėjimas 21 procentu. Vis dėlto, tokių, į kurias labai paprasta įsilaužti, skaičius nežymiai augo (2 proc.). Pavaizduotos tendencijų kreivės rodo situacijos gerėjimą – 2016 metų kreivė yra artimesnė siekiamybės kreivei, lyginant su 2015 kreive. Apibendrinant galima teigti, kad per metus padidėjo bendras svetainių atsparumas įsilaužimams.



11 pav. Lietuvos interneto svetainių pažeidžiamumas pagal įsilaužimo sudėtingumą ir teigiama tendencija.

Galima numanyti, kad pozityvi tendencija susijusi su tuo, kad dauguma informuotų įstaigų atsižvelgė į NKSC raginimą pašalinti nurodytas saugumo spragas. Kadangi dalis apie saugumo spragas neinformuotų įstaigų svetaines talpina tose pačiose tarnybinėse stotyse, dėl talpinimo paslaugą teikiančių įmonių veiksmų, sauga natūraliai sustiprinta ir kitose svetainėse. Kita dalis informuotų įstaigų pakeitė svetainių talpinimo paslaugos teikėją patikimesniu.

Palyginus organizacijų interneto svetainių programinės įrangos sąrašus su pažeidžiamumų duomenų baze, pastebėti daugybiniai *Apache, Joomla, PHP* pažeidžiamumų atvejai. NKSC stebėtose svetainėse nustatyta net 14 didžiausios rizikos pažeidžiamumų, kurie paskelbti prieš 10 ar daugiau metų (12 pav.).

Pažeidžiamumo pavadinimas (CVSS > 7.5)	Pažeidžiamumo publikavimo data	Vėluojama atnaujinti metų
Apache HTTPD: Apache Chunked encoding vulnerability (CVE-2002-0392)	2002-07-03	14
PHP Vulnerability: CVE-2003-0863	2003-11-17	13
PHP Multiple Vulnerabilities	2005-01-10	11
PHP Vulnerability: CVE-2005-3391	2005-11-01	11
PHP Vulnerability: CVE-2005-3392	2005-11-01	11
PHP CURL/GD Module 'safe_mode'/'open_basedir' Bypass Vulnerability	2005-11-01	11
PHP Vulnerability: CVE-2005-3390	2005-11-01	11
PHP GLOBALS Variable Overwriting Vulnerability	2005-11-01	11
PHP 'virtual()' Safe Mode/Open_basedir Bypass Vulnerability	2005-11-01	11
PHP 'mb_send_mail()' Header Injection Vulnerability	2005-11-29	11
PHP HTTP Response Splitting Vulnerability	2006-01-13	10
PHP Safe Mode Bypass 2	2006-04-10	10
Apache HTTPD: mod_rewrite off-by-one error (CVE-2006-3747)	2006-07-28	10
PHP "ecalloc" Integer Overflow Vulnerability	2006-10-10	10

12 pav. Užfiksuoti pavojingi pažeidžiamumai, publikuoti prieš 10 ir daugiau metų.

Kaip ir ankstesniais metais, **svetainių priežiūrai ir kibernetinio saugumo būklei neigiamą įtaką darė nedarnios interneto svetainės saugos lygį lemiančių trijų subjektų pastangos**: svetainės ir jos turinio savininkas (valdytojas), svetainės turinio valdymo sistemos kūrėjas (integratorius) ir svetainės prieglobos paslaugos teikėjas kibernetinio saugumo priemonių nenustatė ar netaikė, ar taikė nekvalifikuotai, su kitais dviem subjektais nederinta apimtimi. 2016 metais NKSC tyrė keletą incidentų, iš esmės kilusių dėl duomenų apdorojimo sprendimus diegusių turinio valdymo sistemos kūrėjų atsainaus požiūrio į LR vyriausybės patvirtintų saugos reikalavimų įgyvendinimą. Nereti atvejai, kai pirkimo dokumentuose nurodomi gana išsamūs ir teisingi saugos reikalavimai, tačiau juos įgyvendinti pavedama ne turinio valdymo sistemos kūrėjui, o tik svetainės

prieglobos paslaugos tiekėjui. Dėl neteisingo atsakomybių paskirstymo sukuriama situacija, kai tiekėjas, net ir norėdamas, negali pilna apimtimi užtikrinti svetainės saugos, nes negali taisyti ne jo kompetencijoje esančio produkto saugumo spragų.

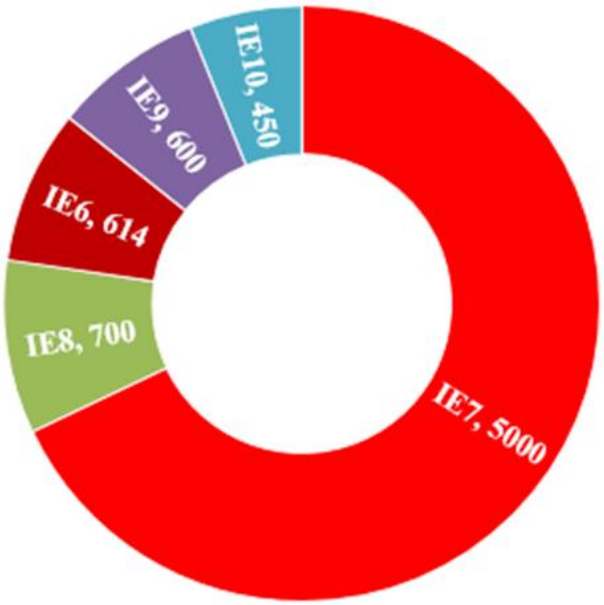
Dar viena problema, daranti įtaką svetainių kibernetinio saugumo būklei, yra tai, kad ne visos organizacijos yra įsteigusios savo svetaines kaip informacines sistemas. Dėl to, kad svetainės nėra laikomos informacinės sistemos objektu, nėra reguliariai atliekama jų rizikos analizė, nėra aptinkamos ir šalinamos saugumo spragos. Todėl organizacija, kuri yra svetainės turinio savininkė, turėtų įteisinti valdomas interneto svetaines, nusistatant tvarkas, kurios reglamentuoja svetainių kūrimo, eksploatavimo bei kibernetinio saugumo užtikrinimo procesus.

OPERACINIŲ SISTEMŲ IR TAIKOMOSIOS PROGRAMINĖS ĮRANGOS SAUGUMO SPRAGOS

Aptikta beveik 2000 kompiuterių su gamintojo nebepalaikoma ir nesaugia operacine sistema.

NKSC 2016 metais elektroninių valstybės informacinių išteklių tinkluose aptiko didelį skaičių ypač pavojingo žalingo kodo (*angl., malware*) naudojimo atvejų, kurių nefiksavo informacinių sistemų valdytojų įdiegti technologiniai saugumo sprendimai. Konstatuotina, kad kaip ir 2015 metais, viena pagrindinių saugumo problemų yra pavėluotas operacinių sistemų ir taikomosios programinės įrangos naujinimas. Saugumo spragos, sudarančios sąlygas įsilaužti, lieka neužtaisytos metus ir ilgiau, naudojamos pasenusios ir gamintojo nebepalaikomos, todėl nesaugios operacinės sistemos, neatnaujinama populiari programinė įranga (Adobe produktai, Java, interneto naršyklės ir pan.), kurios pažeidžiamumai nuolat išnaudojami laužiantis į organizacijų tinklus.

Lietuvoje 2016 metais situacija, lyginant su 2015-aisiais, negerėjo. Populiariausios programinės įrangos, kurios pažeidžiamumai buvo dažniausiai išnaudojami kibernetinių atakų metu, atnaujinimas smarkiai vėlavo. Pvz., 2016 m. pabaigoje patikrinus, kokios operacinės sistemos įdiegtos organizacijų kompiuteriuose, kuriais naršoma internete, aptikta beveik 2000 kompiuterių su gamintojo nebepalaikoma ir nesaugia operacine sistema Windows XP bei apie 7500 kompiuterių, kuriuose įdiegtos ir internetui naršyti naudojamos pasenusios (pažeidžiamos) interneto naršyklės (13 pav.).



13 pav. Aptiktų kompiuterių, kuriais naršoma internete pasenusiomis IE naršyklėmis, skaičius (vnt.). 2016 metų pabaigoje duomenys.

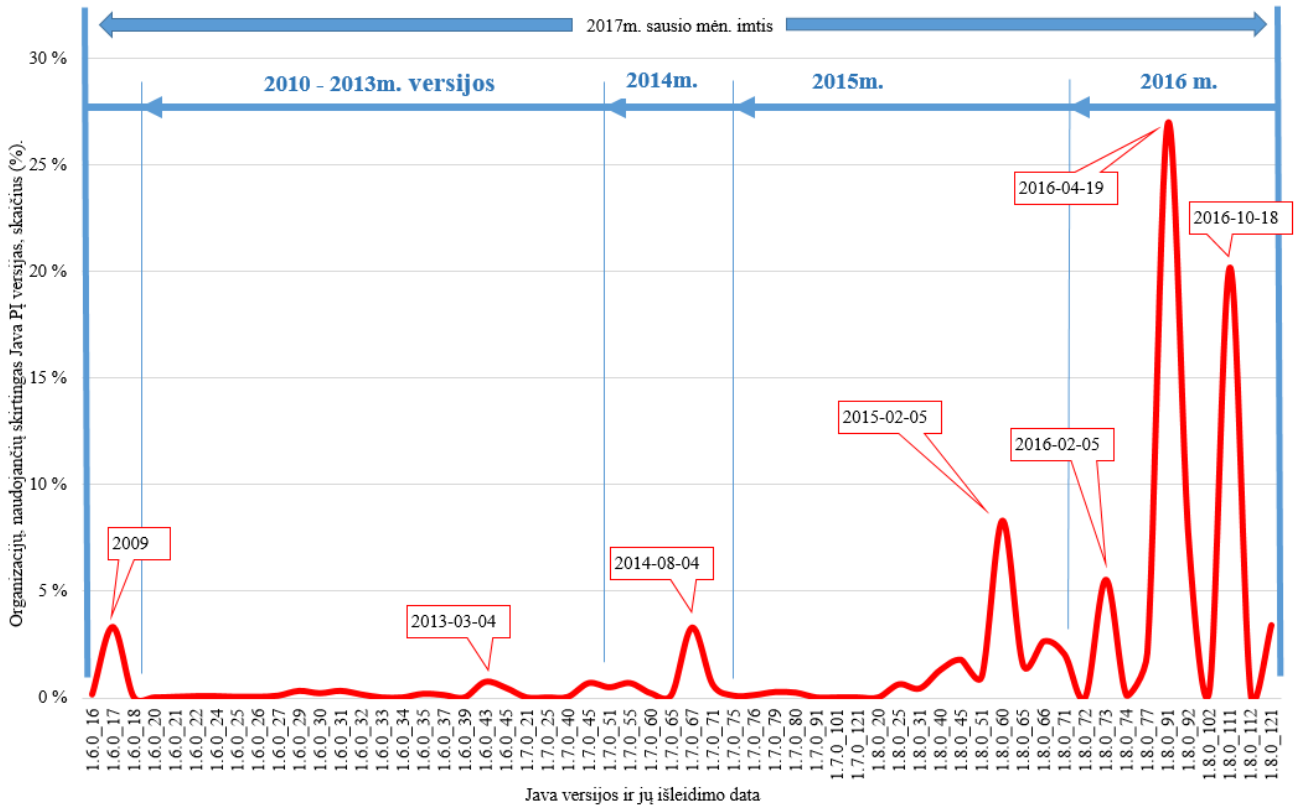
Nustatyta beveik 1000 kompiuterių, kurie, nors ir naudoja gamintojo dar palaikomą operacinę sistemą Microsoft Windows 7, naudoja pasenusias ir todėl nesaugias Internet Explorer naršyklių versijas (IE8, 9 ir 10), nors jas galima lengvai atnaujinti į ženkliai saugesnę. Šios naršyklės gamintojas 2016 metų sausio mėnesį nutraukė senesnių nei Internet Explorer 11 naršyklių palaikymą[7], tačiau akivaizdu, kad Lietuvos organizacijos neatsižvelgė į šį su kompiuterių sistemų saugumu tiesiogiai sietiną pranešimą, neatnaujino programinės įrangos ir taip padidino kibernetinės atakos prieš organizacijas sėkmės tikimybę.

Aptikta apie 7500 kompiuterių, kuriuose įdiegtos ir internetui naršyti naudojamos pasenusios (pažeidžiamos) interneto naršyklės.

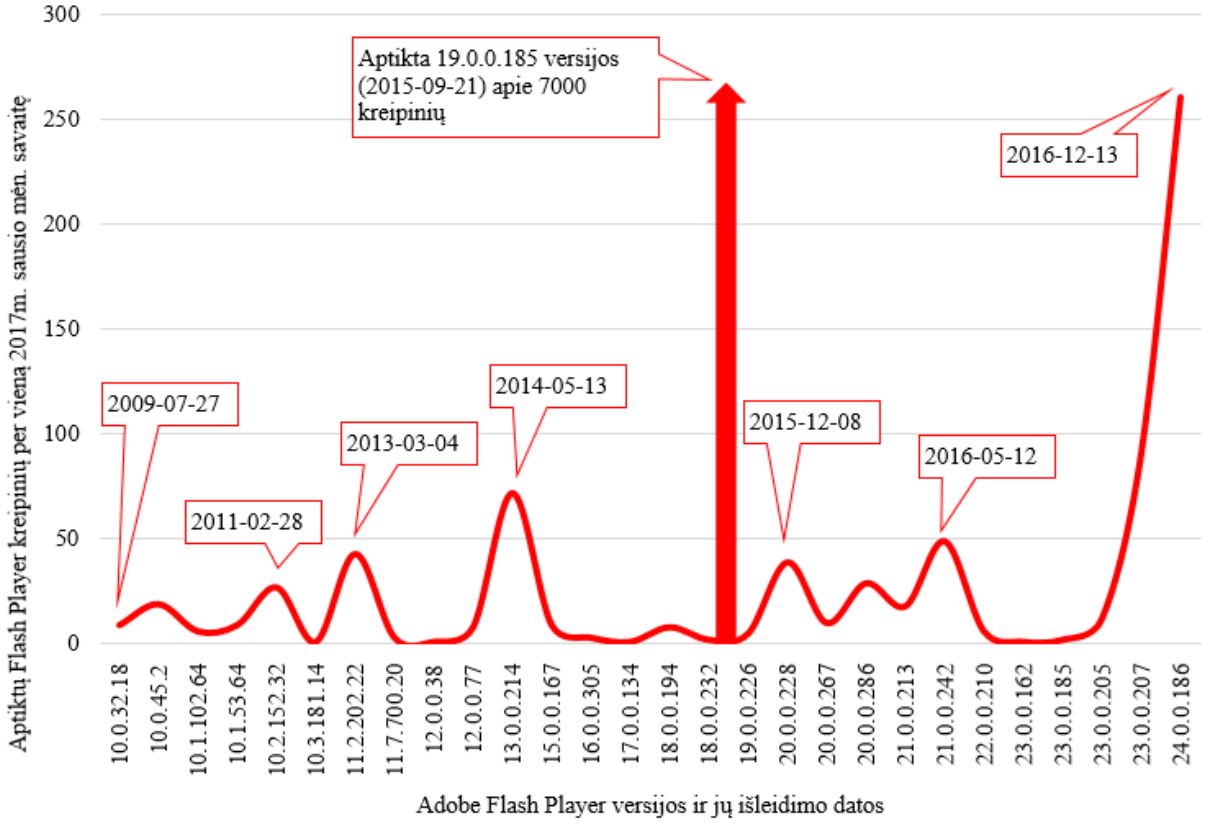
Pastebima, kad ir toliau daug kompiuterių, kuriais naršoma internete, turi įdiegtą seną, kartais net daugiau kaip 5 metus neatnaujintą programinės įrangos versiją. Pvz., 2016 m. pabaigoje buvo tikrinama, kokios Java versijos veikia organizacijų kompiuteriuose, naršančiuose internete. Aptiktos bent 58 skirtingos Java versijos, iš kurių maždaug 30 proc. turi 6 ar daugiau mėn. senumo saugumo spragas. Tai reiškia, kad daug kompiuterių turi saugumo spragų, kurias išnaudojus potencialiai galima įsibrauti į organizacijų kompiuterių tinklus. Keli procentai naršančių internetą kompiuterių apskritai neatnaujino Java programinės įrangos nuo 2009 m. (14 pav.).

Panaši situacija ir su kita populiaria programine įranga – Adobe Flash Player (15 pav.).

[7] *"...Beginning January 12, 2016, only the most current version of Internet Explorer available for a supported operating system will receive technical supports and security updates.* ***Internet Explorer 11 is the last version of Internet Explorer, and will continue to receive security updates, compatibility fixes, and technical support*** *on Windows 7, Windows 8.1, and Windows 10. Internet Explorer 11 offers improved security, increased performance, better backward compatibility, and support for the web standards that power today's websites and services. Microsoft encourages customers to upgrade and stay up-to-date on the latest browser for a faster, more secure browsing experience. [...]* ***After January 12, 2016, Microsoft will no longer provide security updates or technical support for older versions of Internet Explorer****. Security updates patch vulnerabilities that may be exploited by malware, helping to keep users and their data safer. Regular security updates help protect computers from malicious attacks, so upgrading and staying current is important."*
https://www.microsoft.com/en-us/WindowsForBusiness/End-of-IE-support



14 pav. Aptiktų kompiuterių, kuriais naršoma internete pasenusiomis naršyklėmis, skaičius (vnt.).



15 pav. Aptiktos naudojamos pasenusios ir turinčios kritinių saugumo spragų Adobe Flash Player programinės įrangos versijos.

SOCIALINĖ INŽINERIJA

> *2016 metais NKSC automatinės atpažinimo priemonės aptiko tris kartus daugiau socialinės inžinerijos požymių turinčių elektroninių laiškų, lyginant su 2015 metais.*

Socialinė inžinerija yra būdas apgauti kompiuterio naudotoją, priversti jį savanoriškai atlikti veiksmus, kurie padeda įsibrauti ir užvaldyti įmonės ar organizacijos kompiuterių tinklus. Stebima, kad vis dažniau socialinės inžinerijos metodai naudojami siekiant įtikinti naudotoją atskleisti konfidencialią informaciją (slaptažodžius, kredito kortelės numerius ir pan.), užkrėsti kompiuterį kenksmingu kodu. Šiuo metodu yra manipuliuojama naudotojų emocijomis ir psichologija, pastabumo stoka, technologijų neišmanymu. 2016 metais užfiksuota naujų socialinės inžinerijos atvejų, aiškiai nukreiptų į Lietuvos valstybines institucijas.

2016 metų liepos mėnesį valstybinės įstaigos darbuotojo elektroninio pašto dėžutę pasiekė laiškas su prisegtu vykdomuoju failu. Atlikta analizė parodė, kad vykdomasis failas iš operacinės sistemos registrų vagia įvairių paslaugų prisijungimo vardus ir slaptažodžius, iš naršyklių - išsaugotus slaptažodžius. Gauto laiško turinys buvo pritaikytas pagal įstaigos darbo sritį, imituojant dažnai gaunamus pranešimus. Taip pat, 2016 metų lapkričio mėnesį NKSC fiksavo kibernetinę ataką prieš vieną iš stambių Lietuvos organizacijų. Jos metu, naudojant socialinės inžinerijos metodus, buvo vykdomas masinis brukalų (SPAM) siuntimas organizacijos darbuotojams. Laiško turinys imitavo gautą oficialų laišką, o jo viduje buvo patalpintas kenksmingas kodas. Pažymėtina, kad atakos metu piktavaliai keitė atakos vektorius, elektroninio laiško antraštes bei turinį. Tokie veiksmai rodo didelį susidomėjimą konkrečiomis Lietuvos valstybės institucijomis ir jų konfidencialia informacija.

Palyginimui, krašto apsaugos sistemą vidutiniškai per mėnesį pasiekia 320.000 laiškų, iš kurių 70.000 yra brukalas (~22 proc.). NKSC naudojamos priemonės taip pat atpažino ir sulaikė apie 10.000 elektroninių laiškų, siunčiamų krašto apsaugos sistemos adresatams, turinčių specialių socialinės inžinerijos požymių. **Iš viso 2016 metais buvo atpažinta ir sulaikyta apie 106 tūkst. tokio pobūdžio laiškų. Tai yra beveik trigubai daugiau, nei praėjusiais metais**. Ženkliai išaugęs socialinės inžinerijos atvejų skaičius bei nuolat tobulėjantys socialinės inžinerijos kibernetiniai instrumentai, leidžia daryti prielaidą, kad ateityje tokio pobūdžio laiškų tik daugės.

Ypatingų socialinės inžinerijos sezoniškumo ar modernumo tendencijų 2016 metais NKSC nepastebėjo.

ELEKTRONINIŲ PASLAUGŲ TRIKDYMAS

DDoS (angl. Distributed Denial of Service) ataka yra vienas iš būdų sutrikdyti sistemų, teikiančių paslaugas internetu, veikimą. Pagrindinis šios atakos tikslas – padaryti paslaugą nepasiekiama naudotojams. Tai naudotojams sukelia nepatogumų, o svetainių valdytojai patiria didelių nuostolių.

2016 metų DDoS atakos – Lietuvos elektroninių ryšių tinklų infrastruktūros atsparumo žvalgyba.

Tokio pobūdžio atakos prieš valstybės institucijų tinklalapius buvo vykdomos 2016 metų balandžio mėnesį. Pirmuoju piktavalių taikiniu buvo pasirinkta LR Seimo interneto svetainė. Galimai ataka prieš Seimo tinklalapį buvo susijusi su tuo metu vykstančiu renginiu – pasauline Krymo totorių konferencija, kurią ketinta transliuoti internetu. Jai pasibaigus, atakos nesibaigė ir buvo tęsiamos, ko pasėkoje sutrikimus patyrė visos eilės svarbių valstybės institucijų tinklalapiai. NKSC turimos stebėsenos sistemos užfiksavo, kad didelio masto DDoS atakos blokavo vieną iš tinklo mazgų, kuris aptarnavo minėtus tinklalapius. Atsižvelgiant į šį ir kitus panašius 2016 metų įvykius, manytina, kad tokie veiksmai galėjo turėti kitą, nei vien tinklalapių sutrikdymo tikslą. **NKSC daro išvadą, kad 2016 metų DDoS atakos – Lietuvos elektroninių ryšių tinklų infrastruktūros atsparumo žvalgyba.**

Rezonansiniai įvykiai, susiję su DDoS atakomis, atskleidė spragas, susijusias su funkcijų bei atsakomybių suvokimu, tarpinstituciniu bendradarbiavimu, informacijos dalijimusi. Stengiantis sumažinti šiuos trūkumus, būtina stiprinti teisinę bazę bei kasmet organizuoti kibernetinio saugumo pratybas.

2015 metais NKSC akcentavo daiktų interneto įrenginių (angl. Internet of Things, IoT) saugumo problemas ir prognozavo didėsiantį kibernetinių atakų, pasitelkiant šiuos įrenginius, mastą. Prognozė pasitvirtino - 2016 metais pasaulyje vyko viena didžiausių DDoS atakų prieš interneto infrastruktūrą, išnaudojant daiktų interneto saugumo spragas. Atakai buvo panaudota apie 150 tūkst. daiktų interneto įrenginių, kurie net kelioms valandoms sutrikdė tokių didžiųjų tinklapių kaip „Amazon“, „Twitter“, „Netflix“ veiklą. Tikėtina, kad 2017 metais tokio pobūdžio atakos bus dar stipresnės, o jų poveikis darys ženklią įtaką pasaulinio interneto darbui.

ŽALINGOS PROGRAMINĖS ĮRANGOS PLITIMAS

Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie Krašto apsaugos ministerijos grėsmių nacionaliniam saugumui 2016 metams vertinimo ataskaitose[8,9] buvo įvardijamos kibernetinio šnipinėjimo grėsmės ir priešiškų jėgų siekiai įsibrauti į kompiuterių tinklus. Lietuvos žvalgybos institucijų dokumentuose konstatuojama, kad ateityje augs kibernetinių atakų skaičius, o kibernetinio šnipinėjimo operacijos kels grėsmę Lietuvos ypatingos svarbos infrastruktūrai.

NKSC 2016 metais stebėjo augančią sudėtingos žalingos programinės įrangos (*angl. malware*) ir būdų, skirtų įsibrauti į organizacijų tinklus ir vykdyti kenksmingą veiklą, plitimo tendenciją. Per 2016 metus NKSC virš 350 kartų aptiko ir neutralizavo tokios programinės įrangos veikimą, tame tarpe užfiksavo kelis atvejus, kuomet buvo naudojama speciali šnipinėjimo programinė įranga (angl. Advanced Persistant Threat, toliau - APT), siejama su užsienio valstybių žvalgybos tarnybomis ir joms dirbančioms APT28 ir APT29[10] grupėmis. NKSC yra žinoma, kad keliose užsienio valstybėse šių APT sukurta programinė įranga buvo panaudota ir fiziniams efektams užkrėstose sistemose ar tinkluose pasiekti.

Pasaulinė praktika rodo, kad sudėtinga žalinga programinė įranga paprastai aptinkama po apytiksliai 250 dienų nuo jos atsiradimo organizacijos tinkluose, ir tai tik tais atvejais, kai dėl kitur atsiradusių specifinių požymių ar patirtos žalos (pvz., buvo parduoti ar panaudoti pagrobti duomenys), sekant nusikaltimo pėdsakais, teisėsaugos įstaigos kreipiasi į organizaciją, kurioje veikia žalinga programinė įranga. Organizacijos, siekiančios savo ištekliais aptikti žalingą programinę įrangą, paprastai ją aptinka greičiau: tai trunka 30-60 dienų. Kompiuterių tinkluose, kurių sauga kartu su valdytoju rūpinasi ir NKSC, šis laikas yra gerokai trumpesnis – nuo kelių valandų iki kelių parų. Svarbu paminėti, kad remiantis NKSC patirtimi, beveik visų organizacijų kompiuterių tinkluose pasitaiko veikiančios žalingos programinės įrangos: visuose tinkluose, kuriuos NKSC pradėjo stebėti ir analizuoti savo techninėmis priemonėmis, buvo aptikta ir neutralizuota žalinga programinė įranga. Organizacijose naudojamos kibernetinio saugumo priemonės paprastai nesugeba aptikti sudėtingos ir moderniais būdais infiltruotos programinės įrangos dėl daugelio priežasčių. Vienos svarbiausių – dėmesio kibernetinei saugai stoka,

[8] http://www.vsd.lt/Page.aspx?pageID=269
[9] http://www.kam.lt/lt/struktura_ir_kontaktai_563/kas_institucijos_567/aotd.html
[10] https://www2.fireeye.com/APT29-HAMMERTOSS-WEB-2015-RPT.html, https://www2.fireeye.com/WEB-2017-RPT-APT28.html

nepakankama atsakingų asmenų kompetencija ir silpni kibernetinių grėsmių nuolatinio vertinimo pajėgumai. Svarbiausi veiksniai, galintys pagerinti kibernetinio saugumo būklę žemesnės kibernetinio saugumo brandos organizacijoms arba mažesnėms organizacijoms, kurioms, natūralu, trūksta lėšų rimtai kibernetinei saugai organizuoti – keistis aktualia informacija apie incidentus ir jų šalinimo būdus su kitomis organizacijomis ir drauge su NKSC būti vieningoje stebimoje kibernetinėje erdvėje.

NKSC pastebi, kad sudėtingos žalingos programinės įrangos, kuri dažnai išnaudojama duomenų rinkimui, paplitimas Lietuvoje geografiškai siejasi su šaliai svarbios ūkio infrastruktūros ir svarbių karinių objektų dislokacija. Tuose regionuose (apylinkėse, miesteliuose) minėta programinė įranga kartais yra paplitusi net plačiau, lyginant su šalia esamomis žymiai tankiau gyvenamomis vietovėmis, rajonų centrais ar miestais (16 pav.).

16 pav. Sudėtingos žalingos programinės įrangos paplitimas Lietuvoje.

ORGANIZACINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ ĮGYVENDINIMAS VALDANT IR TVARKANT VALSTYBĖS INFORMACINIUS IŠTEKLIUS

VII VALDYTOJŲ IR TVARKYTOJŲ APKLAUSA

2016 metų pabaigoje NKSC parengė elektroninį klausimyną ir surengė antrąją savo apklausą, kuri vadinosi „Kibernetinio saugumo organizacinių reikalavimų įgyvendinimas Lietuvos organizacijose“. Apklausa buvo skirta įvertinti organizacinių – viešojo administravimo subjektų – kibernetinio saugumo reikalavimų[11] įgyvendinimo lygį Lietuvoje ir nustatyti problemas, su kuriomis susiduria juos įgyvendinantys valstybės informacinių išteklių valdytojai ir tvarkytojai.

Tik maža dalis valstybės institucijų žino, kiek ir kokių valstybės informacinių išteklių valdo ir (arba) tvarko pavaldūs reguliavimo srityje esantys subjektai

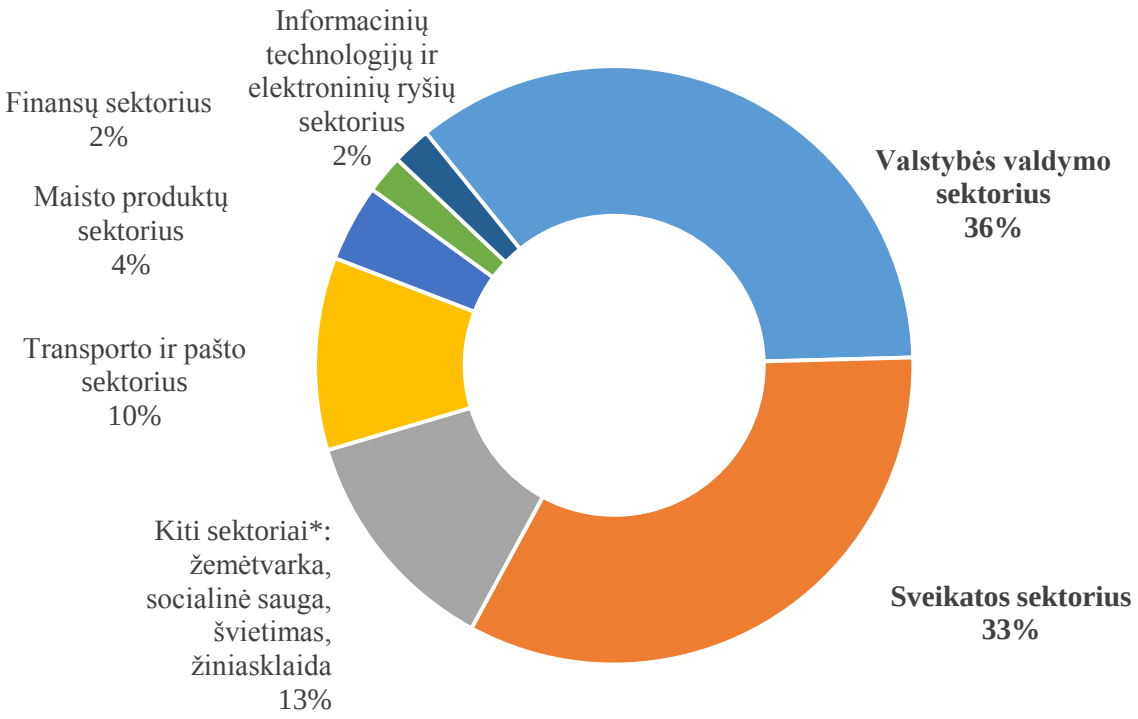
Toliau dokumente šios visos įmonės ir organizacijos vadinamos bendru pavadinimu – Organizacijos.

Vienas iš apklausos tikslų buvo paskatinti viešojo administravimo subjektus, valstybės įmones ir organizacijas, savarankiškai išnagrinėti klausimyno klausimus, įvertinti savo gebėjimus kovoti su kibernetinėmis grėsmėmis ir, remiantis tokio vertinimo išvadomis, priimti sprendimus dėl kibernetinio saugumo būklės įmonėje ar organizacijoje gerinimo, tobulinti nustatytų reikalavimų įgyvendinimą.

[11] *Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimas Nr. 387 "Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo",* https://www.e-tar.lt/portal/lt/legalAct/30d42bc00b7111e6a238c18f7a3f1736

Dalyvavusių apklausoje Organizacijų buvo prašoma priskirti save sektoriams, kurių sąrašas yra nustatytas Lietuvos Respublikos Vyriausybės nutarime[12]. Didžiąja dalimi Organizacijos atstovavo valstybės valdymo ir sveikatos sektorius (atitinkamai 33 ir 36 proc.,17 pav.).

Daug Lietuvos organizacijų ignoruoja kibernetinio saugumo klausimus.



17 pav. Apklausoje dalyvavusių Organizacijų pasiskirstymas pagal sektorius.
(* Nepatenkantys į Lietuvos Respublikos Vyriausybės 2016 m. liepos 20 d. nutarime Nr. 7 "Dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo" nurodytą ypatingos svarbos sektorių sąrašą)

NKSC atkreipė dėmesį į kelias Organizacijas, kurios išskirtinai parodė aukštą kibernetinio saugumo problematikos supratimą ir norą bendromis pastangomis spręsti Lietuvai svarbius klausimus. Tai - Muitinės departamentas prie Lietuvos Respublikos finansų ministerijos, Valstybės įmonė Registrų centras, Šalčininkų rajono savivaldybės administracija, Nacionalinė mokėjimo agentūra prie Žemės ūkio ministerijos, Valstybinė mokesčių inspekcija prie Lietuvos Respublikos finansų ministerijos ir kt.

[12] *Lietuvos Respublikos Vyriausybės 2016 m. liepos 20 d. nutarime Nr. 7 "Dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo" nurodytas ypatingos svarbos sektorių sąrašas.* https://www.e-tar.lt/portal/lt/legalAct/9915c0b24f2611e6b72ff16034f7f796

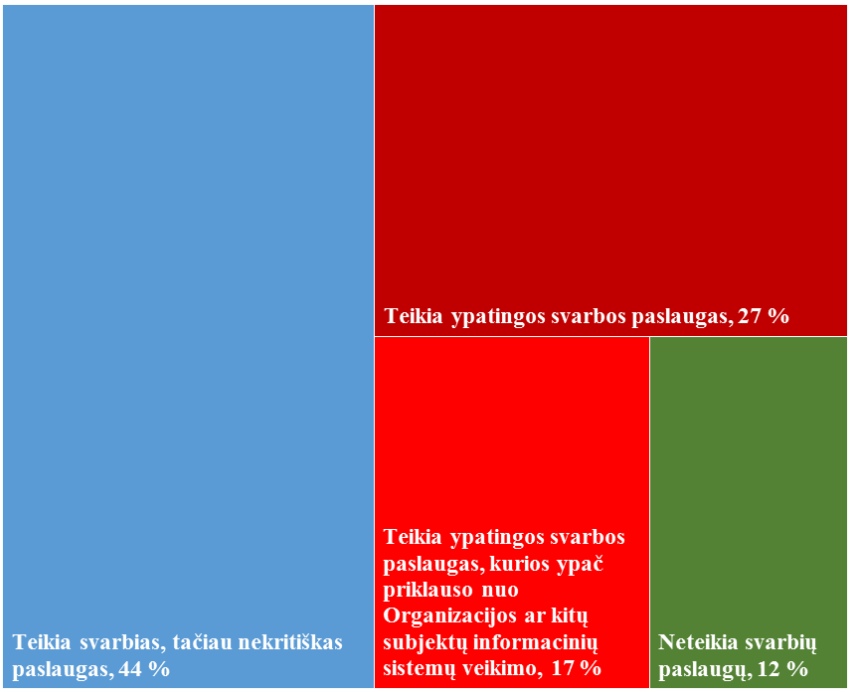
Apklausoje taip pat dalyvavo Lietuvos Nacionalinis transliuotojas - vienas svarbiausių informacijos šaltinių Lietuvos gyventojams – Nacionalinis Lietuvos radijas ir televizija.

Kaip ir praėjusiais metais, pusė apklaustų Organizacijų nesutiko, kad jų pavadinimas būtų viešai skelbiamuose dokumentuose susietas su konkrečiu atsakymu į NKSC apklausos klausimą.

Žemiau pateikiami situacijos vertinimai, įžvalgos, analizės ir išvados yra gautos NKSC sugretinus įvairius duomenis: gautus iš Organizacijų apklausos metu, NKSC techninėmis priemonėmis surinktus kibernetinio saugumo būklės stebėsenos duomenis, iš kitų šaltinių gautą informaciją.

13 proc. dalyvavusių apklausoje Organizacijų teikia elektroninių ryšių ir/ar prieglobos paslaugas kitoms Organizacijoms, ir net 77 proc. teikia paslaugas internetu (informacijos sklaida, viešos el. paslaugos gyventojams ir pan.).

Organizacijos nurodė valdančios ir (arba) tvarkančios iki 30 informacinių sistemų, tinklų ar registrų, vidutiniškai įsteigusios po 5 informacines sistemas(35 proc. apklaustųjų Organizacijų turi po 1, o 17 proc. - nuo 15 iki 30 įsteigtų informacinių sistemų). Beveik pusė Organizacijų deklaravo, kad teikia svarbias, tačiau nekritiškas paslaugas. 44 proc. Organizacijų deklaravo, kad teikia ypatingos svarbos paslaugas. Net 17 proc. respondentų pažymėjo, kad jų Organizacijų teikiamos ypatingos svarbos paslaugos ypač priklauso nuo Organizacijos ar kitų subjektų informacinių sistemų veikimo (18 pav.).



18 pav. Apklausoje dalyvavusių Organizacijų pasiskirstymas pagal deklaruotą teikiamų paslaugų svarbą

Trečdalis Organizacijų, kurios deklaravo turinčios 11 ir daugiau informacinių sistemų, tinklų ar registrų, nurodė, kad arba nežino, kiek iš šių valdomų ir (arba) tvarkomų sistemų yra oficialiai įsteigta, arba nurodė, kad apskritai nė viena nėra įsteigta, kaip to reikalauja teisės aktai.

KIBERNETINIO SAUGUMO POLITIKA

35 proc. Organizacijų nėra paskyrusios kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą.

Trečdalis (!) apklausoje dalyvavusių Organizacijų nurodė, kad nėra susipažinę su 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"[13], **nėra išnagrinėję teisės akto ir suplanavę, kaip įgyvendins organizacinius kibernetinio saugumo reikalavimus.** Atsižvelgiant į tai, kad respondentai teikė duomenis praėjus 4 mėnesiams po Lietuvos Vyriausybės nustatyto organizacinių reikalavimų įgyvendinimo termino, galima daryti išvadą, kad yra ignoruojami Lietuvos Vyriausybės sprendimai. Tik kelios apklaustos Organizacijos nurodė, kad teisės aktą išnagrinėjo ir pasirengė bei patvirtino organizacinių kibernetinio saugumo reikalavimų įgyvendinimo planą. Beveik identiška situacija yra su Organizacijų techninių kibernetinio saugumo reikalavimų įgyvendinimu: dauguma apklaustųjų neturi Lietuvos Vyriausybės nutarimu būtino parengti techninių kibernetinio saugumo reikalavimų įgyvendinimo plano ir, juolab, nepateikė jo NKSC, kaip to reikalaujama minėtame nutarime. 75 proc. Organizacijų teigia nepatvirtinusi teisės aktų, reglamentuojančių kibernetinio saugumo politiką ir jos įgyvendinimą (kibernetinio saugumo dokumentų), o tos, kurios reglamentavo kibernetinio saugumo politiką, tai dažniausiai padarė papildydamos kiekvienos valdomos ir (arba) tvarkomos informacinės sistemos (registro) ar tinklo saugos dokumentų[14] turinį.

Viena Organizacija, kuri deklaravo, kad yra viešojo administravimo subjektas ir valstybės informacinių išteklių valdytojas ir (arba) tvarkytojas, konstatavo, kad minėtas teisės aktas[15] jai nėra taikytinas, ir todėl neturi parengusi jokių kibernetinio saugumo reikalavimų įgyvendinimo planų.

[13] *Op. Cit. 11, 22 psl.*
[14] *Dokumentai, rengiami pagal Bendrųjų elektroninės informacijos saugos reikalavimų aprašą, patvirtintą 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“, https://www.e-tar.lt/portal/lt/legalAct/TAR.FC952AC6A109/ZfVJrXrsJl*
[15] *Op. Cit. 11, 22 psl.*

Ketvirtadalis Organizacijų rengia tik informacinių sistemų saugos dokumentaciją, kai to prireikia įsteigti pastarąsias, tačiau bazinių kibernetinio saugumo politiką nustatančių dokumentų neturi. Kitas ketvirtadalis Organizacijų deklaruoja turintys bazinius saugos politiką nustatančius dokumentus, tačiau jais nesivadovaujama (nereferuojama į juos), kai reikia apibrėžti informacinių sistemų saugą.

50 proc. Organizacijų nemato tikslo reglamentuoti kibernetinio saugumo politikos ir procedūrų, nes, jų manymu, visa tai gali kontroliuoti ir valdyti IT specialistas (administratorius) savo nuožiūra.

Net 35 proc. apklaustųjų Organizacijų nėra paskyrusios kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, kaip to jau 2 metai reikalauja Kibernetinio saugumo įstatymas. Šiek tiek mažiau nei ketvirtis Organizacijų, siekdamos, kad būtų užtikrinta, kad kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą, būtų mokomas kibernetinio saugumo klausimais ir turėtų tinkamą kvalifikaciją, siunčia juos į kursus, tačiau **nevertina, ar kursai yra efektyvūs**. Apie **20 proc. Organizacijų apskritai nesiunčia atsakingų asmenų į kursus** dėl įvairių priežasčių, pvz., dėl nepakankamo finansavimo. **50 proc. Organizacijų dėl įvairių priežasčių nevykdo RIS naudotojų mokymo kibernetinio saugumo klausimais**, 35 proc. Organizacijų rengia kasmetinius darbuotojų mokymus, kuriuose nagrinėjami ir kibernetinio saugumo klausimai, ir **tik kelios Organizacijos teigia turinčios darbuotojų mokymo programas**, o viena iš jų - dar ir mokymų efektyvumo nustatymo mechanizmą.

Priešingai nei reikalauja teisės aktai ir rekomenduoja tarptautiniai standartai bei pasaulyje gerąja laikoma kibernetinio saugumo praktika, net **50 proc. Organizacijų nemato reikalo reglamentuoti kibernetinio saugumo politikos ir procedūrų**, nes, jų manymu, visa tai gali kontroliuoti ir valdyti IT specialistas (administratorius) savo nuožiūra ir savo gebėjimų ribose.

Tik 25 proc. Organizacijų per paskutinius 12 mėn. yra peržiūrėję kibernetinio saugumo dokumentus[16] ir turi tokios peržiūros įrodymą (išleista nauja dokumentų redakcija, išleistas įsakymas peržiūrai ir pan.). Tai reiškia, kad didžioji dauguma Organizacijų neatsižvelgė į Lietuvos Respublikos Vyriausybės nutarimą[17] ir ignoravo jo nuostatas, reikalaujančias pokyčių minėtuose saugos dokumentuose.

[16] *Op. Cit. 14, 26 psl.*
[17] *Op. Cit. 11, 25 psl.*

ORGANIZACINIŲ REIKALAVIMŲ REGLAMENTAVIMAS

30 proc. Organizacijų mano, kad RIS naudotojai nėra susiję su kibernetinio saugumo klausimų sprendimu.

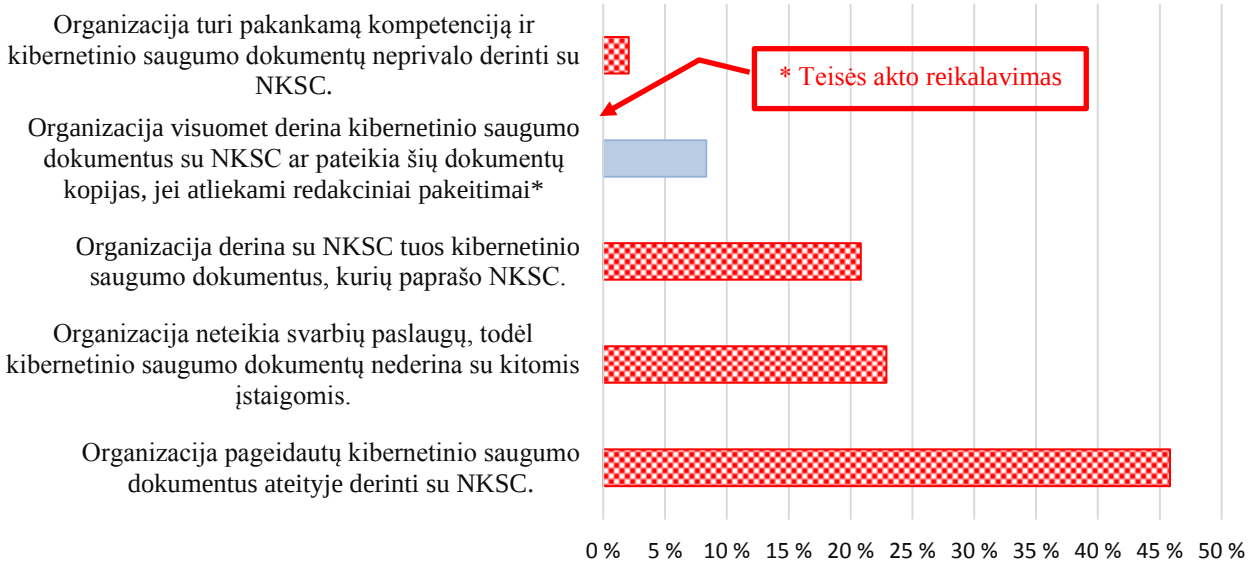
Lietuvos Respublikos Vyriausybė 2016 m. balandžio 20 d. nutarimu Nr. 387 "Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo" nustatė virš 70 organizacinių kibernetinio saugumo reikalavimų, kurie gali būti suskirstyti į kelias sritis: saugos politika, atsakingų asmenų veikla, incidentų valdymas, rizikos valdymas ir pažeidžiamumų analizė, prevencinės priemonės. Analizuojant apklausos rezultatus, kaip ir 2015 metais, pastebimas Organizacijų abejingumas kibernetinei saugai. Vyrauja ypač ydingas požiūris, kad jokių papildomų organizacinių priemonių, kurios leistų kompleksiškai ir nuosekliai spręsti kibernetinio saugumo klausimus, Organizacijai nereikia: pakanka kibernetinę saugą palikti IT padalinio, o tiksliau – konkretaus IT specialisto (pvz., administratoriaus) asmeniniu reikalu. Net 30 proc. apklaustųjų Organizacijų mano, kad nereikia įvardinti RIS naudotojų pareigų ir funkcijų, susijusių su kibernetiniu saugumu, nes, paprasčiausiai, jų manymu, RIS naudotojai nėra susiję su kibernetinio saugumo klausimų sprendimu. Tokio požiūrio rezultatas – atitinkamų teisės aktų reikalavimų ignoravimas ir itin prasta kibernetinio saugumo Organizacijoje būklė.

Viena iš kelių svarbiausių kibernetinio saugumo prevencinių priemonių, minima Lietuvos Respublikos Vyriausybės nutarime ir nuolat akcentuojama pasaulinėje kibernetinio saugumo praktikoje[18], yra savalaikis programinės įrangos atnaujinimas, kurio metu yra ištaisomos ne tik jos veikimo klaidos, bet ir kritiniai programinio kodo moduliai, turintys didelės įtakos atsparumui kibernetinėms atakoms. Tam, kad programinės įrangos atnaujinimo procesas būtų efektyvus, būtina šį procesą Organizacijoje pirma sukurti ir aprašyti, deleguoti funkcijas atsakingiems asmenims ir vykdyti procedūras nustatyta apimtimi bei nustatytu laiku (pvz., Microsoft, Adobe ir Oracle programinių produktų naujinius sudiegti ne vėliau, kaip per 48 val. nuo jų išleidimo). Deja, daugiau kaip **70 proc. atvejų Organizacijose programinės įrangos atnaujinimus, klaidų taisymus vertina ir diegia IT sistemų administratoriai savo asmenine nuožiūra ir apimtimi, neturėdami tokių procedūrų aprašymo ar kokių nors taisyklių.**

[18] *Naudojimasis tik identifikuota ir leistina technine įranga, naudojimasis tik leistina programine įranga, teisingas ir saugus techninės ir programinės įrangos konfigūravimas, savalaikis programinės įrangos atnaujinimas – pažeidžiamumų šalinimas, išteklių pasiekimo privilegijuotų teisų (administratoriaus paskyrų) griežta kontrolė*, https://www.cisecurity.org/critical-controls.cfm, https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

Daugiau, kaip pusė Organizacijų per paskutinius 12 mėn. nevykdė jokių valdomų ir (arba) tvarkomų RIS atitikties kibernetinio saugumo reikalavimams vertinimų, 35 proc. vykdė atitikties kitiems ar mažesnės apimties (nei Lietuvos Respublikos Vyriausybės nustatyta) vertinimus ir apie 7 proc. Organizacijų atitiktį kibernetinio saugumo reikalavimams vertino tokia pat ar didesne kaip nustatyta apimtimi. Praktiškai visos apklaustos Organizacijos, išskyrus kelias išimtis, neturi įgytos kibernetinių incidentų valdymo patirties vertinimo procesą aprašančio dokumento, kas reiškia, kad kibernetiniai incidentai nėra tinkamai tiriami, analizuojamos jų priežastys ir nenaudojamos priemonės incidentų užkardymui.

2016 metais priėmus anksčiau minėtą kibernetinio saugumo reikalavimus nustatantį teisės aktą, be kita ko, įtvirtino viešojo administravimo subjektams pareigą derinti kibernetinio saugumo dokumentus su NKSC. Nors informacinių sistemų ir registrų registre yra užregistruota virš 300 informacinių sistemų ir registrų, tik keli kibernetinio saugumo dokumentų komplektai tebuvo atsiųsti derinimui su NKSC, ir tik vienas komplektas šiuo metu yra pilnai suderintas. Organizacijų apklausos metu buvo stengiamasi išsiaiškinti teisės akto reikalavimų nevykdymo priežastis, todėl Organizacijų buvo klausiama, kaip pastarosios derina saugos dokumentus su kitomis organizacijomis. 19 pav. pateikiami Organizacijų atsakymai, iš kurių akivaizdu, kad Organizacijos pasirinkdamos vieną iš penkių pateiktų galimų atsakymų pademonstravo teisės akto reikalavimų nežinojimą (nepaisant to, kad didelė dalis respondentų deklaravo, kad yra susipažinę su kibernetinio saugumo organizaciniais reikalavimais), o kai kurie – ir žemą supratimo apie tarpinstitucinio darbo vertę lygį.



19 pav. Apklausos respondentų atsakymai, susiję su teisės akte nurodyta prievole be išlygų derinti kibernetinio saugumo dokumentus su NKSC.

KIBERNETINIŲ INCIDENTŲ VALDYMO REGLAMENTAVIMAS

50 proc. Organizacijų neturi RIS įprastinės veiklos atkūrimo tvarką reglamentuojančio dokumento, kuriame atsispindėtų ir kibernetinių incidentų padarinių likvidavimas.

2016 metų sausio 25 d. Lietuvos Respublikos Vyriausybė priėmė nutarimą Nr. 87 „Dėl nacionalinio kibernetinių incidentų valdymo plano“, kuriuo buvo nustatyti viešojo administravimo subjektų, tvarkančių valstybės informacinius išteklius, veiksmai, atliekami siekiant suvaldyti kibernetinius incidentus, galinčius sutrikdyti ar sutrikdančius valstybės informacinių išteklių, ypatingos svarbos informacinės infrastruktūros ir (ar) kitų elektroninių ryšių tinklų ir paslaugų ir (ar) informacinių sistemų darbą ir taip sukelti grėsmę nacionaliniam saugumui, žmonių sveikatai ar gyvybei, visuomenės gerovei ar valstybės funkcijų atlikimui, taip pat tarpinstitucinę kibernetinių incidentų valdymo sąveiką, kibernetinių incidentų klasifikavimo tvarką ir tarpinstitucinį bendradarbiavimą tiriant kibernetinius incidentus. Šiuo teisės aktu nustatyta, kad **kibernetinių incidentų prevenciją ryšių ir informacinėse sistemose vykdo jų tvarkytojai**. Kitame teisės akte - Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarime Nr. 387 "Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo", apibrėžiami kibernetinio saugumo reikalavimai, susiję su organizaciniais kibernetinių incidentų valdymo klausimais. Šiame teisės akte yra nurodyti per dešimt tokių reikalavimų, tačiau NKSC vykdytos apklausos respondentai dažniausiai nurodė, kad tokie reikalavimai dėl vienokių ar kitokių priežasčių nėra vykdomi.

Net **pusė apklaustų Organizacijų deklaravo, kad neturi RIS įprastinės veiklos atkūrimo tvarką reglamentuojančio dokumento, kuriame atsispindėtų ir kibernetinių incidentų padarinių likvidavimas**. Didžioji dauguma Organizacijų taip pat neturi pasirengę RIS incidentų susijusių su atkirtimo nuo paslaugos (angl., (Distributed) Denial of Service, DoS, DDoS) stabdymo (gynybos) plano ar kitokio, kovos su vykstančia DoS ataka procedūras nustatančio dokumento. Kelios Organizacijos mini, kad problemą sprendžia rangovas ar Organizacijai pakanka veiklos tęstinumo planų, o kita dalis Organizacijų, net ir tos, kurios nurodo turinčios po kelias informacines sistemas ir teigia, kad teikia paslaugas internetu (informacijos sklaida, viešos el. paslaugos gyventojams ir pan.), neturi kovos su vykstančiomis DoS atakomis reglamentuojančių dokumentų, nes **yra įsitikinę, kad Organizacijos valdomos ir (arba) tvarkomos RIS neturi atkirtimo nuo paslaugos (DoS) rizikos**. Tai – mažiausiai keistas požiūris, kadangi 2016 metais

vyko ženkliai daugiau rezonansinių DoS kibernetinių atakų prieš Lietuvos informacines infrastruktūras, nei 2015 metais.

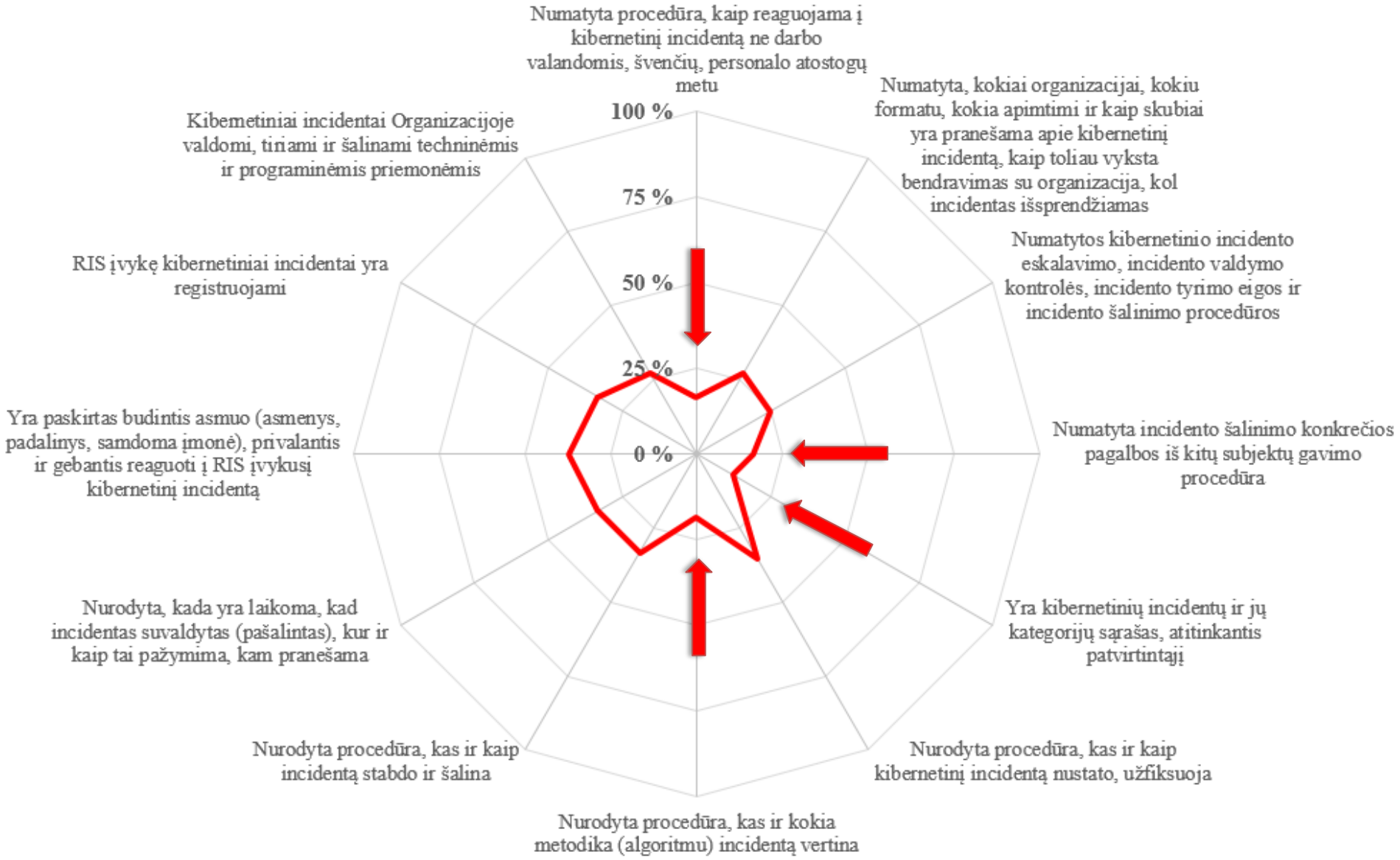
NKSC vykdytoje apklausoje nemažas dėmesys buvo skiriamas kibernetinių incidentų valdymo klausimams, tad surinkta informacija pasitarnavo gilesnei organizacinių kibernetinio saugumo reikalavimų, susijusių su kibernetinių incidentų valdymo organizavimu, analizei. 20 pav. pateikiama tokios analizės grafinė išraiška.

Pirma, Organizacijos tinkamai nevertina rizikų ir nesprendžia, kaip valdys kibernetinį incidentą (pvz., teikiamų elektroninių paslaugų trikdymą DDoS metu) nesant specialistams vietoje. **Svarbu pažymėti, kad tik apie 6 proc.Organizacijų apskritai yra reglamentavę kibernetinių incidentų valdymą**. Silpniausiai reglamentuotas kibernetinių incidentų valdymas švenčių, ne darbo metu ir atsakingų asmenų atostogų laikotarpiu.

Antroji silpniausiai reglamentuota sritis – reagavimo į incidentus algoritmas. Organizacijos paprastai nereglamentavo, kokiais kriterijais vadovaujantis ir vykdant kokią procedūrą yra vertinamas kibernetinis incidentas, t.y. neaišku, kaip Organizacijos nustato kibernetinio incidento mastą, svarbą, potencialiai galimą patirti žalą. Tai reiškia, kad NKSC ar kitos kibernetinį saugumą užtikrinančios įstaigos Lietuvoje gauna tikrovės neatitinkančią informaciją apie pas viešojo administravimo subjektus – valstybės informacinių išteklių valdytojus ar tvarkytojus – vykstančius kibernetinius incidentus.

Trečioji silpniausiai reglamentuota sritis – pagalbos iš kitų subjektų gavimas, kai reikia suvaldyti kibernetinį incidentą, kurio suvaldymui trūksta Organizacijos vidinių išteklių arba kibernetinis incidentas vyksta plačiu mastu, incidentą valdo pvz., NKSC, o Organizacija nėra prioritetinė kitų Organizacijų atžvilgiu.

Ketvirtoji silpniausiai reglamentuota sritis – kibernetinių incidentų klasifikavimas. Nors teisės aktu yra apibrėžti kibernetiniai incidentai, o pastarieji – suskirstyti į konkrečias kategorijas, tik labai maža dalis apklausos respondentų, kurie turi įsivardinę kibernetinių incidentų aibę, nurodė, kad ši yra suderinama su numatytąja nemažesne apimtimi, nei apibrėžia teisės aktas.



20 pav. Kibernetinių incidentų valdymo reglamentavimas Organizacijose.
Kreivė nurodo, kiek Organizacijų (%) yra reglamentavusios konkretų kibernetinių incidentų valdymo aspektą.

ORGANIZACINIUS KIBERNETINIO SAUGUMO REIKALAVIMUS APIBRĖŽIANČIO TEISĖS AKTO ANALIZĖ

Viešojo administravimo subjektai, ypač – mažesnės Organizacijos, yra nepasirengusios taikyti viso komplekso kibernetinio saugumo reikalavimų.

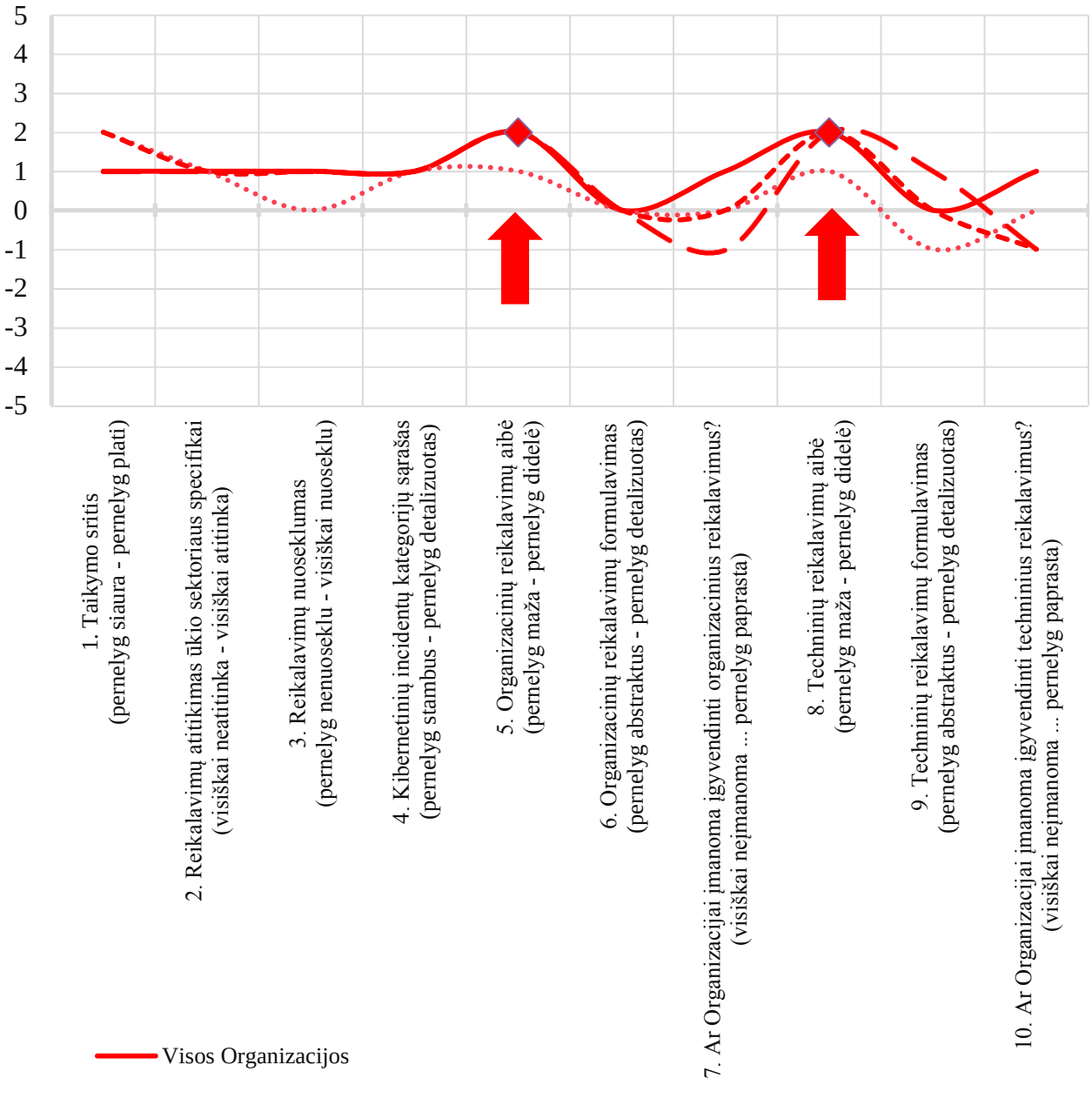
Lietuvos Respublikos Vyriausybei 2016 m. balandžio 20 d. priėmus nutarimą Nr. 387 "Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo", daugumai Organizacijų iškilo klausimai apie šio teisės akto taikymo apimtis, nuostatų įgyvendinimo kiekybinį ir kokybinį aspektą, dažnai pasigirsdavo kritikos teisės aktu patvirtinto aprašo struktūrai, nuoseklumui ir apimčiai. Į NKSC yra kreipusios Organizacijos dėl vieno ar kito apraše minimo kibernetinio saugumo reikalavimo išaiškinimo ar taikomumo konkrečiu atveju.

Siekiant nustatyti minėtu teisės aktu patvirtintų kibernetinio saugumo reikalavimų atitikimą Lietuvos viešojo administravimo subjektų – valstybės informacinių išteklių valdytojų ir tvarkytojų – pajėgumams įgyvendinti reikalavimus, apibendrinti daugumai kylančias problemas ir teikti siūlymus kibernetinio saugumo politiką nustatantiems subjektams dėl teisės akto tobulinimo, NKSC į vykdytą apklausą įtraukė specialią klausimyno dalį, susijusią su teisės akto analize. Organizacijų buvo prašoma pateikti savo pastabas ir pasiūlymus teisės akto tobulinimui, bei įvertinti teisės aktą įverčiais nuo -5 (blogiausia) iki +5 (geriausia) pagal dešimtį kibernetinio saugumo reikalavimų aibę ir taikomumą apibrėžiančius požymius. Reikšmė „0“ buvo vertinama kaip nuomonės duotu klausimu neturėjimas. Didelis kreivės pokytis nuo "0" ašies (išsk. reikšmes prie 2 ir 3 klausimo) būtų reiškęs netobulą teisės aktą, pernelyg sudėtingus kibernetinio saugumo reikalavimus ar pernelyg didelę naštą viešojo administravimo subjektams, valdantiems ar tvarkantiems valstybės informacinius išteklius. 21 pav. pateikiama šios analizės grafinė išraiška, kurioje atsispindi trijų Organizacijų grupių vertinimai. Kreivės rodo, kaip vieną ar kitą teisės aktu patvirtintų kibernetinio saugumo reikalavimų aibės aspektą vertina:

a) visos apklausoje dalyvavusios Organizacijos,
b) Organizacijos, pagal kurių pateiktus paslaugų svarbą žyminčius atsakymus vertinamos, kaip teikiančios ypatingos svarbos paslaugas (paslaugų svarbos rodiklis >70%),

c) Organizacijos, pagal kurių pateiktą organizacinių kibernetinio saugumo reikalavimų įgyvendinimo suminį skaičių vertinamos, kaip įgyvendinusios didžiąją daugumą reikalavimų (kiekybinis rodiklis >70%),

d) Organizacijos, kurių įgyvendinti organizaciniai kibernetinio saugumo reikalavimai yra pažymėti kaip išspręsti išsamiausiai (subjektyvus kokybinis rodiklis >70%).



21 pav. Apklausos respondentų atsakymai, susiję su teisės akte nurodytų kibernetinio saugumo reikalavimų aibės taikomumu.

Teisės akto analizė parodė, kad visos Organizacijų grupės teisės aktą vertino labai panašiai, todėl teigtina, kad tiek vadybine prasme brandžioms, tiek silpnesnėms Organizacijoms teisės aktu patvirtinti kibernetinio saugumo reikalavimai yra suprantami. NKSC pateikia apibendrintus respondentų atsakymus:

1. Kibernetinio saugumo reikalavimų aibė yra paini: skirtingai, nei tai padaryta gerosios praktikos metodikose ir standartuose, organizaciniai reikalavimai nesugrupuoti į esmines tikėtiną rezultatą reiškiančias grupes, o techninių reikalavimų aibė yra pernelyg didelė, taikoma tiek žemos kategorijos informacinių sistemų, tiek I kategorijos informacinių sistemų saugai.
2. Organizaciniai kibernetinio saugumo reikalavimai yra nevisiškai nuoseklūs, besikaitaliojantys: dalis jų susiję su Organizacijos kibernetinio saugumo politika, dalis – orientuota į konkrečios informacinės sistemos saugą aprašančius dokumentus.
3. Kibernetinio saugumo reikalavimai nėra tiesiogiai taikytini įvairiuose ūkio sektoriuose veikiančioms Organizacijoms, ir valstybės valdymo bei sveikatos sektoriams dėl pernelyg didelės reikalavimų apimties.
4. Kibernetinio saugumo reikalavimų įgyvendinimui labai kenkia atskiras kibernetinio saugumo ir elektroninės informacijos apsaugos nagrinėjimas bei šias stipriai susijusias sritis reglamentuojantys nesusinchronizuoti ir painiavą įnešantys teisės aktai.
5. Viešojo administravimo subjektai, ypač – mažesnės Organizacijos, yra nepasirengusios taikyti viso komplekso kibernetinio saugumo reikalavimų. Efektyviau būtų taikyti gerąja pasaulyje pripažinta praktiką ir nustatyti laipsnišką reikalavimų taikymą, pradedant nuo esminių: be elementarių kibernetinio saugumo vadybos klausimų, įgyvendinti pagrindinius keturis-penkis kibernetinio saugumo reikalavimus[19], duodančius esminį teigiamą efektą kibernetinio saugumo būklei Organizacijoje.

[19] *Naudojimasis tik identifikuota ir leistina technine įranga, naudojimasis tik leistina programine įranga, teisingas ir saugus techninės ir programinės įrangos konfigūravimas, savalaikis programinės įrangos atnaujinimas – pažeidžiamumų šalinimas, išteklių pasiekimo privilegijuotų teisų (administratoriaus paskyrų) griežta kontrolė*, https://www.cisecurity.org/critical-controls.cfm, https://www.asd.gov.au/infosec/top-mitigations/top-4-strategies-explained.htm

VII VALDYTOJŲ IR TVARKYTOJŲ LŪKESČIAI

Pagrindinė Lietuvos prastos kibernetinio saugumo būklės priežastis – kibernetinio saugumo svarbos nuvertinimas Organizacijose.

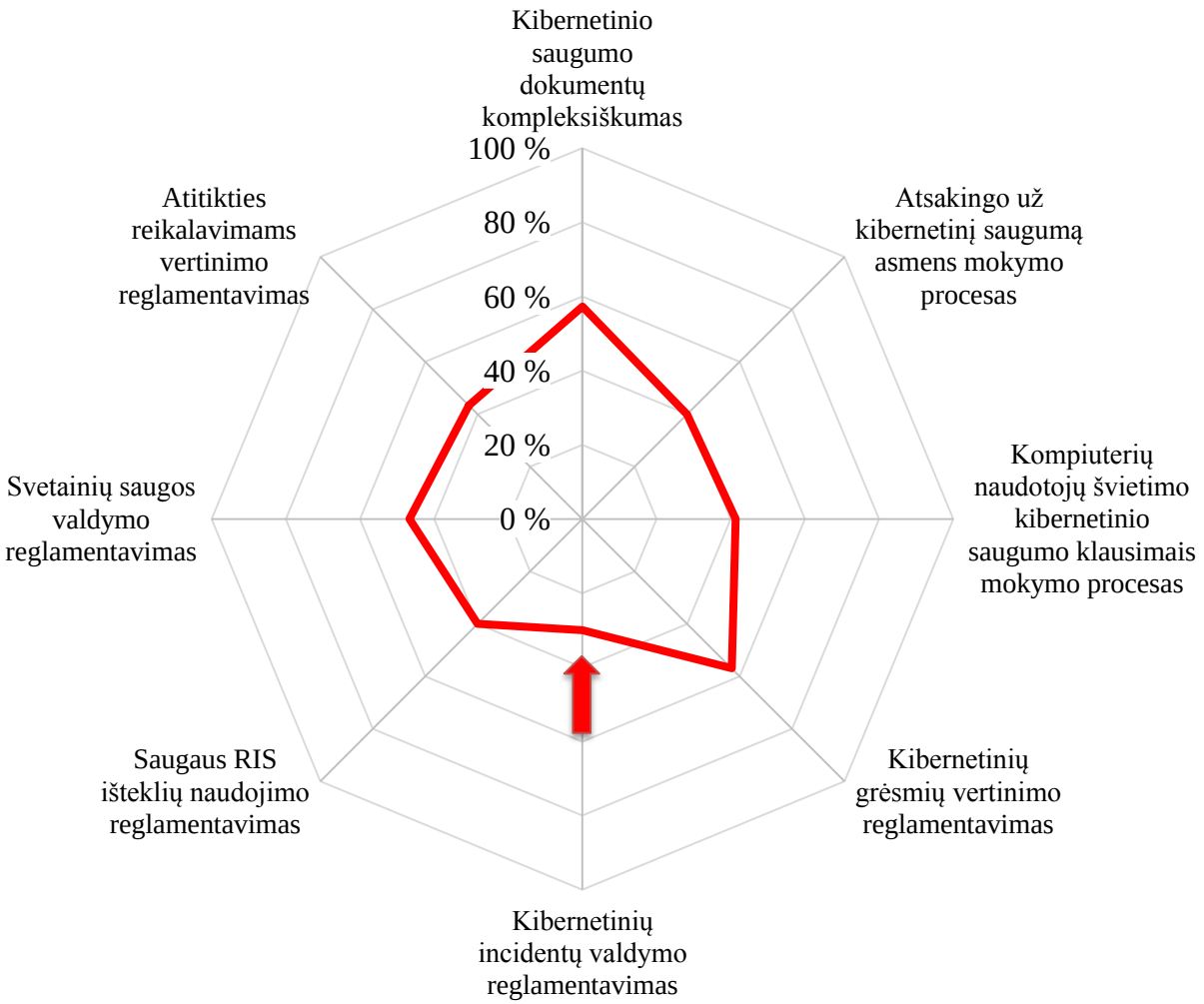
Valstybės informacinių išteklių valdytojai ir tvarkytojai mano, kad kibernetinio saugumo reikalavimai turėtų būti įgyvendinami tik palaipsniui, o kibernetinio saugumo ir elektroninės informacijos apsaugos reikalavimai turėtų būti sujungti į vieną dokumentą. Visi reikalavimai turėtų sudaryti vieningą sistemą, turėti vieningą terminologiją bei būti prižiūrimi ir valdomi vienos organizacijos.

Pagrindinės probleminės Lietuvos kibernetinio saugumo būklės priežastys, kaip ir nuo praėjusių metų besikartojančios įsisenėjusios problemos, yra:

1. Kibernetinio saugumo svarbos nuvertinimas Organizacijose;
2. Nesuteiktas papildomas finansavimas kibernetinės saugos klausimams spręsti;
3. Ypač mažesnėse Organizacijose trūksta etatų: dauguma Organizacijų nurodo, kad net vienam specialistui, nuolat dirbančiam kibernetinio saugumo klausimais, neįmanoma aprėpti ir išspręsti visas kibernetinio saugumo reikalavimų įgyvendinimo Organizacijoje problemas;
4. Trūksta metodinės paramos: kibernetinio saugumo žinios brangios, o finansavimas kvalifikacijai kelti yra per menkas. Todėl reikėtų valstybinio požiūrio ir sprendimo valstybės masteliu dėl švietimo kibernetinio saugumo klausimais.

ORGANIZACINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ ĮGYVENDINIMO LIETUVOJE LYGIS

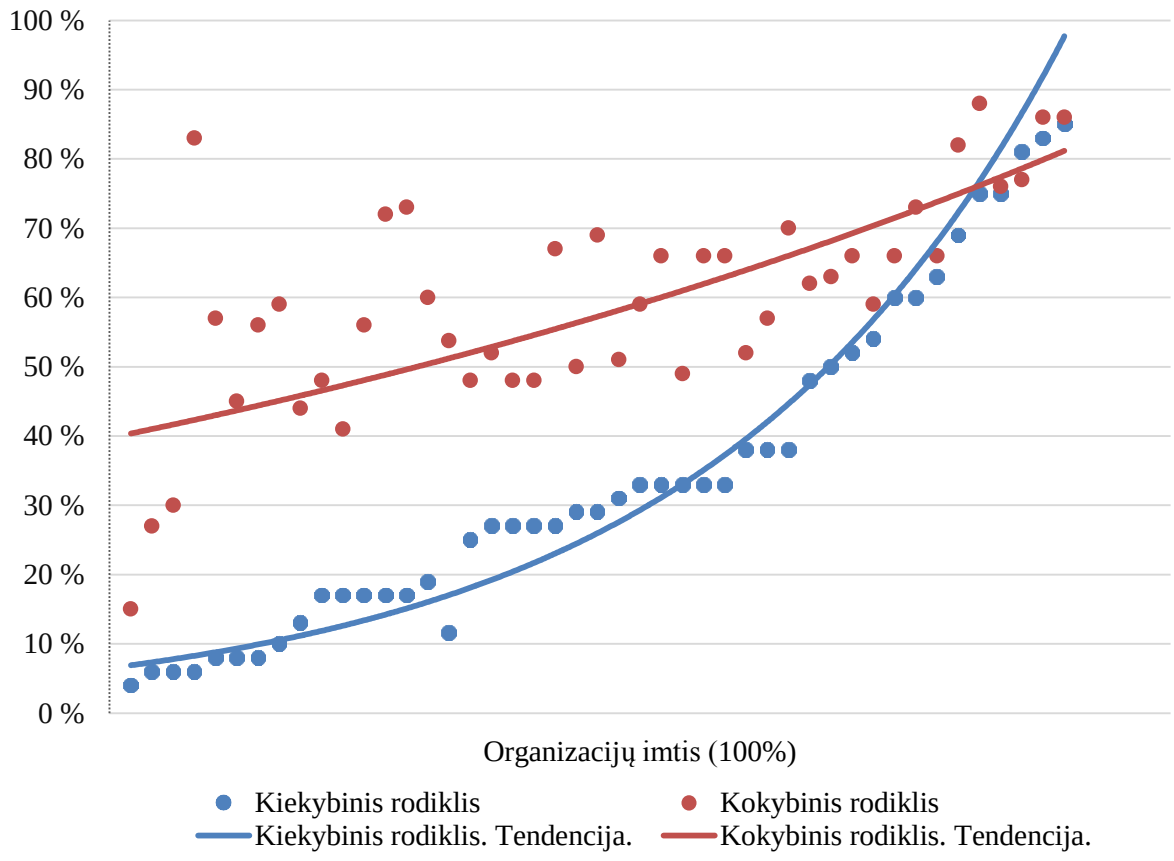
NKSC išanalizavo apklausos duomenis ir nustatė, kad Organizacijos mažiausiai dėmesio skyrė reglamentuojant kibernetinių incidentų valdymą, nenustatė taisyklių, kaip reaguojama į kibernetinius incidentus ir kaip likviduojami kibernetinių incidentų padariniai. 22 pav. pateikiamas grafikas atspindi kibernetinio saugumo organizacinių reikalavimų įgyvendinimą atskirose teminėse reikalavimų grupėse. Grafiko vertė nurodo kaip Organizacijos išsamiai ir visapusiškai reglamentavo vieną ar kitą kibernetinio saugumo aspektą.



22 pav. Įgyvendintų kibernetinio saugumo organizacinių reikalavimų reglamentavimo išsamumas skirtingose reikalavimų grupėse.

NKSC 2016 metų apklausoje pamėgino suskaičiuoti kiekvienos apklausoje dalyvavusios Organizacijos kibernetinio saugumo reikalavimų įgyvendinimo lygį, kurio vidurkis reikštų šių reikalavimų įgyvendinimo lygį Lietuvoje. Pagal Organizacijų pateiktus atsakymus į tam tikrą klausimų aibę buvo skaičiuojamas suminis skaičius, vertinamas, kaip subjektyvusis kiekybinis rodiklis, o pagal atsakymų į šios aibės klausimus kaitą, buvo skaičiuojamas subjektyvusis deklaruotų įgyvendintų reikalavimų kokybinis rodiklis. Pateikus šiuos skaičius Organizacijai, buvo prašoma įvertinti, ar rezultatai atitinka Organizacijos nuomonę apie kibernetinio saugumo reikalavimų įgyvendinimo lygį. Skaičiavimai daugumoje atvejų sutapo su Organizacijų vertinimu. Žemiau 23 pav. pateiktas grafikas demonstruoja, kad Organizacijos, įgyvendinusios daugiau kibernetinio saugumo organizacinių reikalavimų, juos įgyvendino ir išsamiau.

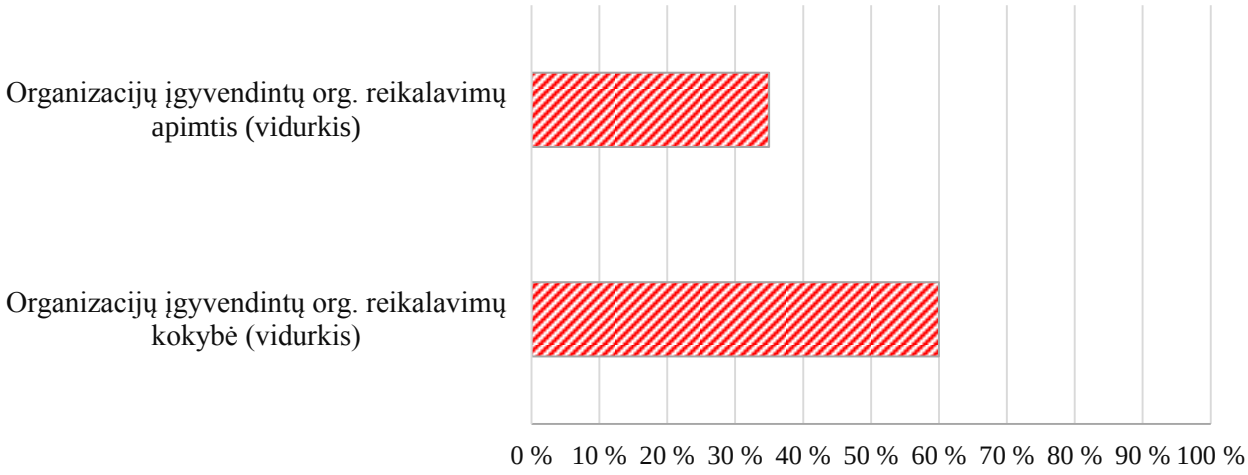
Organizacijos, įgyvendinusios daugiau kibernetinio saugumo reikalavimų, juos įgyvendino ir išsamiau.



23 pav. Įgyvendintų kibernetinio saugumo organizacinių reikalavimų kiekio ir kokybės santykis.

Organizacinių kibernetinio saugumo reikalavimų įgyvendinimo lygis Lietuvoje - nepatenkinamas.

Suskaičiavus apklausoje dalyvavusių Organizacijų įgyvendintus kibernetinio saugumo reikalavimus ir išvedus vidurkius, galima daryti išvadą, kad tik apie 50 proc. Lietuvos viešojo administravimo subjektų, valdančių ar tvarkančių valstybės informacinius išteklius, yra įgyvendinę dalį Lietuvos Respublikos Vyriausybės nutarimu patvirtintų kibernetinio saugumo organizacinių reikalavimų arba tą dalį jau atitiko dar iki išleidžiant teisės aktą. Šios Organizacijos įgyvendino vidutiniškai apie 35 proc. reikalavimų, kurių įgyvendinimo kokybė (išsamumas) vidutiniškai yra apie 60 proc. (24 pav.)



24 pav. Kibernetinio saugumo organizacinių reikalavimų įgyvendinimo Lietuvoje.

NKSC nuomone, Organizacinių kibernetinio saugumo reikalavimų įgyvendinimo lygis Lietuvoje - nepatenkinamas.

KIBERNETINIO SAUGUMO BŪKLĖS GERINIMAS

TEISINIS REGLAMENTAVIMAS

2016 metais nebuvo identifikuota Lietuvos ypatingos svarbos informacinė infrastruktūra.

2016 metais įvyko ženklių pokyčių Lietuvos kibernetinio saugumo reglamentavime. Tęsiant 2015 metais pradėtą teisinės bazės kibernetinio saugumo srityje tobulinimą, kai buvo priimti pirmieji Kibernetinio saugumo įstatymo normas realizuojantys teisės aktai[20], 2016 metų sausio 25 d. Lietuvos Respublikos Vyriausybė priėmė nutarimą Nr. 87 „Dėl nacionalinio kibernetinių incidentų valdymo plano“[21]. Šiuo planu buvo nustatyti valstybės informacinių išteklių ir kritinės informacinės infrastruktūros valdytojų bei tvarkytojų veiksmai, siekiant suvaldyti reikšmingus kibernetinius incidentus, kai yra būtina tai daryti apjungiant organizacijų pastangas. Šiame teisės akte reglamentuota kibernetinių incidentų klasifikavimo, jų nustatymo ir vertinimo tvarka, apibrėžiamas reagavimo į kibernetinius incidentus algoritmas, kibernetinio incidento analizė bei tarpinstitucinis bendradarbiavimas tiriant kibernetinius incidentus.

Ypatingos svarbos informacinės infrastruktūras (YSII) identifikuojamos ir jų sąrašas sudaromas vadovaujantis 2016 metais liepos 20 d. priimtu Lietuvos Respublikos Vyriausybės nutarimu Nr. 742 „Dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo“[22]. Remiantis šiuo nutarimu, atsakingos institucijos YSII valdytojų sąrašą teikia Vidaus reikalų ministerijai, kuri teikia Vyriausybei tvirtinti apibendrintą YSII sąrašą. Nespėjus 2016 metais patvirtinti YSII ir jų valdytojų sąrašo, tikimės, kad tai bus atlikta 2017 metų pradžioje, o iki tol NKSC spręsdama valstybei svarbios informacinės infrastruktūros kibernetinio saugumo

---

[20] *Lietuvos Respublikos Vyriausybės 2015 m. balandžio 23 d. nutarimas Nr. 422 „Dėl kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo“* https://www.e-tar.lt/portal/lt/legalAct/4e3539f0ee4611e4927fda1d051299fb ,
Lietuvos Respublikos krašto apsaugos ministro 2015 gegužės 26 d. įsakymas Nr. V-535 „Dėl kibernetinio saugumo tarybos personalinės sudėties patvirtinimo“
https://www.e-tar.lt/portal/lt/legalAct/cf990800046c11e588da8908dfa91cac ,
Lietuvos Respublikos krašto apsaugos ministro 2015 gegužės 5 d. įsakymas Nr. V-461 „Dėl techninių kibernetinio saugumo priemonių diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje tvarkos aprašo patvirtinimo“
https://www.e-tar.lt/portal/lt/legalAct/7faa0300f3c611e4927fda1d051299fb

[21] *Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimas Nr. 87 „Dėl nacionalinio kibernetinių incidentų valdymo plano“* https://www.e-tar.lt/portal/lt/legalAct/2a916390c5b211e583a295d9366c7ab3

[22] *Lietuvos Respublikos Vyriausybės 2016 m. liepos 20 d. nutarimas Nr. 742 „Dėl ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos patvirtinimo“*
https://www.e-tar.lt/portal/lt/legalAct/9915c0b24f2611e6b72ff16034f7f796

klausimus ir toliau vadovausis krašto apsaugos ministerijos nustatytais prioritetais[23]. 2016 metų balandžio 20 d. Lietuvos Respublikos Vyriausybės nutarimu Nr. 387 „Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“[24] buvo nustatyti organizaciniai ir techniniai kibernetinio saugumo reikalavimai VII ir YSII valdytojams bei tvarkytojams. Šis nutarimas įtvirtino VII valdytojų ir tvarkytojų pareigą įgyvendinti apraše nustatytus organizacinius ir techninius kibernetinio saugumo reikalavimus per nustatytą laikotarpį, pateikti techninių kibernetinio saugumo reikalavimų įgyvendinimo priemonių planus NKSC. 2016 metais NKSC šiuos planus gavo iš 8 organizacijų, o nustatytu terminu planą pateikė tik viena organizacija. Skaičiuojama, kad iš viso valstybės informacinius išteklius valdančios ir tvarkančios organizacijos turi per 300 įvairių informacinių sistemų, tinklų ir registrų, kurių kibernetinio saugumo dokumentai turi būti suderinti su NKSC. Deja, tik keli dokumentacijos komplektai pasiekė NKSC. Kai kurios organizacijos minėto nutarimo nuostatų įgyvendinimo problemas sieja su išteklių trūkumu, tačiau NKSC kaip pagrindinę problemą įvardintų organizacijų žemą brandą, nesureguliuotus veiklos procesus ir saugos (įsk. kibernetinę saugą) kultūros trūkumą.

[23] *Op. Cit. 2, 4 psl.*

[24] *Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimas Nr. 387 „Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“* https://www.e-tar.lt/portal/lt/legalAct/30d42bc00b7111e6a238c18f7a3f1736

PRATYBOS

2016 metais NKSC stebėjo vis tobulėjančius bandymus įsibrauti į Lietuvos valstybės institucijų tinklus, sutrikdyti elektroninių paslaugų veikimą. Tiek rezonansiniai įvykiai Lietuvoje, tiek didėjanti įmonių ir organizacijų veiklos sėkmės priklausomybė nuo naudojamų informacinių technologijų, iššaukė poreikį labiau gilintis į naująsias grėsmes bei tobulinti būdus, kaip su jomis kovoti. Kibernetinio saugumo pratybos – bene efektyviausias būdas gerinti kibernetinio saugumo būklę Lietuvoje.

Didelė naudotojų dalis iki šiol nesugeba įvertinti galimų savo veiksmų pasekmių ir nėra informuoti apie socialinės inžinerijos būdus.

2016 metais, krašto apsaugos ministerijos Kibernetinio saugumo ir informacinių technologijų departamentas kartu su NKSC, Lietuvoje organizavo nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2016“. Jose dalyvavo per 100 atstovų iš daugiau nei 40 Lietuvos valstybės bei kitų institucijų. Pratyboms reikalingą virtualią informacinę infrastruktūrą suteikė Vilniaus universitetas bei Kauno technologijos universitetas. Pratybų pagrindiniai tikslai – patikrinti nacionalinio kibernetinių incidentų valdymo plano procedūras, ugdyti gebėjimą operatyviai keistis informacija tarp institucijų, taikyti procedūras ir technologinius sprendimus kovai su kibernetinėmis grėsmėmis, apsaugai nuo kibernetinių atakų. „Kibernetinis skydas 2016“ pratybose dalyvavo komandos, veikiančios skirtingose Vilniaus, Kauno ir Klaipėdos mokymo vietose. Kiekviena komanda mokėsi aptikti kibernetines atakas, suvaldyti jų valdomuose tinkluose kylančius kibernetinius incidentus.

Kibernetinių incidentų aptikimas ir valdymas pratybų metu buvo vykdomas vadovaujantis 2016 metais vyriausybės patvirtintais dokumentais – Nacionaliniu kibernetinių incidentų valdymo planu[25] ir organizaciniais ir techniniais kibernetinio saugumo reikalavimais, taikomais ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams[26].

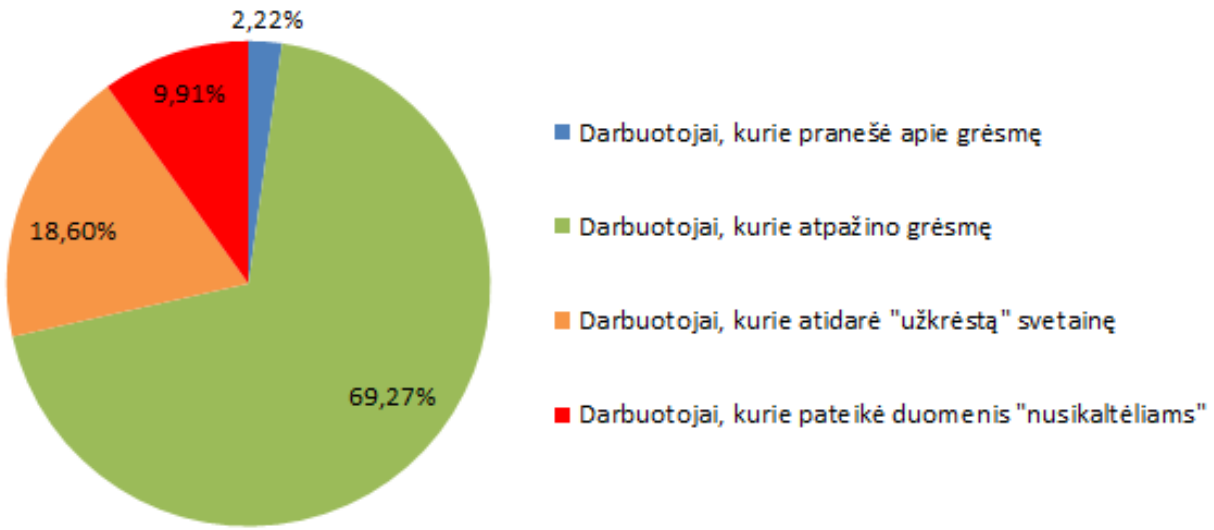
[25] *Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimas Nr. 87 „Dėl nacionalinio kibernetinių incidentų valdymo plano“* https://www.e-tar.lt/portal/lt/legalAct/2a916390c5b211e583a295d9366c7ab3

[26] *Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimas Nr. 387 „Dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“* https://www.e-tar.lt/portal/lt/legalAct/30d42bc00b7111e6a238c18f7a3f1736

Pratybos „Kibernetinis skydas 2016“ parodė, kad iš esmės LRV priimti kibernetinį saugumą reglamentuojantys teisės aktai leidžia identifikuoti ir valdyti kibernetinius incidentus. Taip pat identifikuoti trūkumai, susiję su gebėjimu vadovautis priimtais teisės aktais, skirtingu jų interpretavimu bei kibernetinių incidentų vertinimo ataskaitų teikimu. Tai dar kartą įrodo, kad tokio pobūdžio pratybos yra ypatingai svarbios siekiant tobulinti kibernetinės gynybos pajėgumus Lietuvos institucijose.

Atsižvelgiant į smarkiai augančią socialinės inžinerijos metodais pagrįstų kibernetinių atakų tendenciją, 2016 metų pabaigoje NKSC organizavo pratybas, kuomet kompiuteriais dirbančių darbuotojų pašto dėžutes pasiekė išgalvoti elektroniniai laiškai, siūlantys apsilankyti neegzistuojančios įmonės tinklalapyje. Šiomis pratybomis buvo siekiama įvertinti organizacijos darbuotojų įgūdžius pastebėti apgaulingus elektroninius laiškus ir reakciją į incidentą, o išanalizavus pratybų rezultatus – patikslinti organizacijos kompiuterių naudotojų švietimo kibernetinio saugumo klausimais programą. Nors didžioji dalis darbuotojų atpažino grėsmę, beveik trečdalis jų pasidavė socialine inžinerija pagrįstai kibernetinei atakai: apsilankė „užkrėstoje“ svetainėje ir (arba) pateikė duomenis „nusikaltėliams“.

Kompiuterių naudotojų gebėjimai atpažinti žalingus laiškus atvaizduoti diagramoje (25 pav.).



25 pav. Pratybų statistika.

NKSC vertinimu, didelė naudotojų dalis nesugeba įvertinti galimų savo veiksmų pasekmių ir nėra pasirengę atsisakyti jiems nemokamai siūlomų „dovanų“. Dėl to būtina nuolat šviesti darbuotojus, gerinti jų kibernetinio saugumo žinias, laiku perspėti apie kibernetinėje erdvėje tykančius pavojus ir grėsmių tendencijas.

2016 metų spalio 13-14 dienomis Lietuva dalyvavo tarptautinėse pratybose „Cyber Europe 2016“. Tai didelio masto kibernetinio saugumo pratybos, kurias organizavo Europos tinklų ir informacijos saugumo agentūra ENISA. Jose dalyvavo daugiau kaip 300 organizacijų iš 28 Europos Sąjungos šalių, Šveicarijos ir Norvegijos. Nuo balandžio mėnesio buvo vykdomos organizacinės ir techninės pratybų užduotys. Specialistai iš įvairių Europos Sąjungos šalių organizacijų turėjo suvaldyti incidentus pagal iš anksto sukurtą scenarijų.Šiomis pratybomis buvo siekiama stiprinti bendradarbiavimą tarp Europos Sąjungos šalių, tobulinti gebėjimus kibernetinio saugumo srityje. Pratybų metu Lietuvos kibernetinio saugumo specialistai pasirodė tinkamai pasirengę spręsti ir valdyti kibernetinius incidentus[27]

2016 metų balandžio 19-22 dienomis, Lietuvos kibernetinio saugumo specialistai dalyvavo kasmetinėse NATO Kibernetinio saugumo kompetencijos centro (NATO Cooperative Cyber Defence Centre of Excellence, CCD COE) organizuojamose pratybose „Locked Shields 2016. Pratybų dalyviai treniravosi aptikti ir suvaldyti sudėtingas kibernetines atakas, stiprino tarpusavio bendradarbiavimo ir informacijos mainų gebėjimus. Jiems talkinantys teisės ir viešųjų ryšių specialistai mokėsi sudėtingose situacijose teikti rekomendacijas ir komentuoti situaciją „žiniasklaidos priemonėms“. Iš viso pratybose dalyvavo 20 komandų iš 19 skirtingų šalių.

[27] *https://www.cert.lt/naujienos/europoje_vyko_didelio_masto_kibernetin.html*, *https://www.enisa.europa.eu/news/enisa-news/cyber-europe-2016/*

IŠVADOS IR PROGNOZĖS

KIBERNETINIO SAUGUMO BŪKLĖS VERTINIMAS

Organizacijos neskiria pakankamai dėmesio šiandieninių kibernetinio saugumo iššūkių sprendimui.

Nepaisant kai kurių pozityvių tendencijų, rodančių kibernetinio saugumo lygio Lietuvoje augimą, **NKSC kibernetinio saugumo lygį Lietuvoje vertina kaip nepatenkinamą**. Tokio vertinimo pagrindas – spartesnė kibernetinių grėsmių augimo regione dinamika, lyginant ją su Lietuvos kibernetinio saugumo techninių ir, visų pirma, organizacinių priemonių įgyvendinimo dinamika.

Pagrindiniai rodikliai, kurie nulėmė Lietuvos kibernetinio saugumo 2016 metų būklės vertinimą, yra šie:

1. Lietuva vadovaujasi Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa[28], kuri nebeatspindi šiandien aktualių kibernetinių grėsmių. Lietuvoje stebimas atotrūkis tarp elektroninės informacijos apsaugos ir kibernetinio saugumo teisinio reglamentavimo, kas trukdo efektyviai ir kompleksiškai spręsti kibernetinio saugumo klausimus.
2. Vėluojama identifikuojant šaliai ypatingos svarbos paslaugas teikiančias organizacijas (ypatingos svarbos objektus) ir jų kritines informacines sistemas (ypatingos svarbos informacinę infrastruktūrą). Valstybės informacinių išteklių valdytojai ir (arba) tvarkytojai nėra pajėgūs laiku ir numatyta apimtimi įgyvendinti Lietuvos Respublikos Vyriausybės patvirtintus kibernetinio saugumo organizacinius ir techninius reikalavimus.
3. IT sprendimų pirkėjai, integravimo ar programavimo bei talpinimo paslaugų teikėjai neskiria deramo dėmesio kibernetiniam saugumui, neapibrėžia visų šalių atsakomybių dėl saugos, nepakankamai kontroliuoja atliktų darbų kokybę, ko pasėkoje yra sukuriamas kibernetinėms atakoms neatsparus produktas.

[28] *Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimas Nr. 796 "Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo".* https://www.e-tar.lt/portal/lt/legalAct/TAR.1ABB945646B7

4. Organizacijos, įsk. privatų sektorių, ir toliau vengia dalintis aktualia kibernetinio saugumo informacija (pvz., pastebėtomis kibernetinėmis grėsmėmis ar naujais išpuolių būdais), mano, kad daugumą klausimų yra pajėgios išspręsti savarankiškai, kartais – tik vieno IT specialisto (sistemų administratoriaus) pagalba. Tik itin mažas organizacijų skaičius turi nusistatę realiai veikiančias reagavimo į kibernetinius incidentus tvarkas ir yra pajėgios tinkamai reaguoti.
5. Dauguma organizacijų nesupranta, kad kibernetiniai veikėjai, tikslingai planuodami ir organizuodami savo veiksmus, gali paralyžiuoti visos organizacijos veiklą. Orientuojamasi į pasekmių likvidavimą ir veiklos atstatymą, tačiau visiškai nesistengiama stiprinti incidentų aptikimo ir prevencijos pajėgumų.
6. Organizacijos ir toliau naudoja pasenusią ir gamintojo nebepalaikomas operacines sistemas ir taikomąją programinę įrangą, su reikšmingomis saugumo spragomis, ignoruoja tiek Lietuvos teisės aktuose įtvirtintus reikalavimus, tiek pasaulyje pripažintą gerąją kibernetinio saugumo praktiką.

PROGNOZĖS 2017 METAMS

NKSC prognozuoja tikslines kibernetines atakas prieš energetikos ir transporto sektorius.

2016 m. Lietuvoje buvo stebimos kibernetinių incidentų augimo tendencijos, kibernetiniai nusikaltėliai naudojo vis agresyvesnius kibernetinių atakų metodus. Pastebima planinga veikla kibernetinėje erdvėje, nukreipta į kritines saugumo spragas turinčių įrenginių ir tinklų paiešką, galinti sutrikdyti svarbias elektronines paslaugas ar pramoninius procesus. **NKSC prognozuoja, kad 2017 metais pasaulis ir, galimai Lietuva, susidurs su vis didesnio masto kibernetinėmis atakomis, kurios įtakos pasaulinio interneto darbą.** Kibernetiniai veikėjai, bandydami naujus kibernetinių atakų metodus ir ieškodami naujų veiklos sričių, gali sukelti problemas tradiciškai saugiomis laikytose informacinėse sistemose. Dalis kibernetinių atakų gali būti naudojamos kaip informacinio karo priemonė, siekiant diskredituoti Lietuvos ir NATO institucijas bei jų veiksmus. Tikėtina, kad **išliks populiarios duomenų užšifravimo ir paskesnio išpirkos reikalavimo kibernetinės atakos.**

Didėjanti dėl kibernetinių atakų patiriama žala vers privataus kapitalo įmones įvertinti savo pajėgumus atremti kibernetines grėsmes, papildomai investuoti į saugą įsigyjant ją gerinančias priemones bei vis labiau dalintis aktualia informacija su partneriais ar tame pačiame ūkio sektoriuje veikiančiomis įmonėmis.

Atsižvelgdama į tendencijas regione ir kitose šalyse vykdytus kibernetinius išpuolius, NKSC mano, kad egzistuoja didelė tikslinių kibernetinių atakų prieš energetikos ir transporto sektoriaus įmonių tinklus tikimybė. Tai pat aktyvės kibernetinės atakos, kurios bus rengiamos pasinaudojant daiktų interneto įrenginių bei namų ūkių kompiuterių saugumo spragomis.