MYKOLO ROMERIO UNIVERSITETAS

EKONOMIKOS IR VERSLO FAKULTETAS

MINDAUGAS MATULIONIS

KOLEKTYVINĖS IR INDIVIDUALIOS KIBERNETINĖS GYNYBOS VIEŠAJAME SEKTORIUJE VERTINIMAS

Magistro baigiamasis darbas

Atliko

KSVvmis18-1 gr. stud.

M.Matulionis

2020 04 01

Vadovas

Prof. dr. D.Štitilis

Vilnius, 2020

TURINYS

ĮVADAS 6

1. VIEŠOJO SEKTORIAUS KIBERNETINIO SAUGUMO TEISINIS REGULIAVIMAS LIETUVOJE, IR GYNYBOS UŽTIKRINIMO GALIMYBĖS

1.1 Kibernetinės gynybos aspektai 9

1.2 Lietuvos ryšių ir informacinių sistemų kibernetinio saugumo užtikrinimo teisinio reguliavimo raida 12

1.3 Lietuvos viešojo sektoriaus ryšių ir informacinių sistemų kibernetinio saugumo užtikrinimo organizavimas bei įgyvendinimas 19

2. VIEŠOJO SEKTORIAUS KOLEKTYVINĖ KIBERNETINĖ GYNYBA 29

2.1 Kolektyvinės kibernetinės gynybos modelis 34

2.2 Kibernetinių atakų ir kolektyvinės gynybos resursų bei kokybės valdymo tyrimo metodika .. 39

2.3 Kibernetinių atakų ir kolektyvinės gynybos atsparumo bei kokybės valdymo analizė 41

2.4 Kibernetinių atakų, kurias patiria Saugusis tinklas analizė 57

2.5 Kibernetinių atakų, kurias patiria viešojo sektoriaus interneto svetainės analizė 51

3. INDIVIDUALI VIEŠOJO SEKTORIAUS KIBERNETINĖ GYNYBA

3.1 Individualios kibernetinės gynybos modelis 57

3.2 Individualios kibernetinės gynybos analizė 58

IŠVADOS 63

LITERATŪRA 65

SANTRAUKA 67

SUMMARY 68

LENTELIŲ SĄRAŠAS

lentelė 1 SVDPT tinklo prieinamumas 41
lentelė 2 SVDPT tinklo detalus prieinamumas 42
lentelė 3 Kitų tinklų prieinamumas (proc.) 43
lentelė 4 SVDPT santykinis gedimų skaičius 100-ui paslaugų 43
lentelė 5 Papildoma informacija. SVDPT paslaugų incidentų ir gedimų kiekis vienetais 44
lentelė 6 Gedimų pašalintų kontroliniu laiku, dalis 44
lentelė 7 Paslaugų, kurioms šalinti gedimai, prieinamumo užtikrinimas* (*- skaičiuojant visus vieno kliento gedimus) 45
lentelė 8 Kontroliniu laiku išspręstų incidentų (visų paslaugų) dalis 46
lentelė 9 Viso užregistruota paslaugų incidentų ir gedimų 46
lentelė 10 Santykinis gedimų bei incidentų skaičius 100-ui paslaugų 47
lentele 11 Kontroliniu laiku sureaguotų incidentų (visų paslaugų) dalis 47
lentelė 12 Bendrų 12 mėnesių sulaikytų DDoS atakų į SVDPT suminis skaičius 50
lentelė 13 DDoS atakos nukreiptos (į TOP 10 klientų) į SVDPT kurių trukmė iki vienos minutės 50
lentelė 14 DDoS atakos nukreiptos (TOP 10 klientų) į SVDPT kurių trukmė nuo1 iki 5 min 51
lentelė 15 WAF sulaikytų atakų bendras skaičius į SVDPT per 12 mėnesių 53
lentelė 16 WAF sulaikytų atakų bendras skaičius į SVDPT per 12 mėnesių TOP 10 53
lentelė 17 WAF saugumo efektyvumas 54

PAVEIKSLĖLIŲ SĄRAŠAS

Pav. 1 Investicijos 2019 11
Pav. 2 Kibernetinio saugumo aplinka Lietuvos viešajame sektoriuje 17
Pav. 3 Organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas Lietuvoje 2016 metais 23
Pav. 4 Organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas Lietuvoje 2017 metais 23
Pav. 5 Kibernetinio saugumo aplinka Lietuvos viešajame sektoriuje 2019 27
Pav. 6 Informacinio saugumo triada 29
Pav. 7 EU Testa-NG tinklo loginė schema 32
Pav. 8 Kibernetinio saugumo aplinka Lietuvos viešajame sektoriuje 33
Pav. 9 Saugiojo tinklo kolektyvinės kibernetinės gynybos modelis 35
Pav. 10 Saugiojo tinklo fizinės saugos ir kontrolės sistema 37
Pav. 10 Lietuvos ir Estijos kolektyvinės kibernetinės apsaugos modelis 36
Pav. 11 DDoS ataka kaip prekė 48
Pav. 12 Srauto stebėjimo sistema 49
Pav. 13 Kenksmingo interneto turinio ir aplikacijų blokavimas (WAF) 51
Pav. 14 Internetinių svetainių pažeidžiamumų TOP 10 54
Pav. 15 Lietuvoje naudojamos kolektyvinės kibernetinės gynybos modelis 57
Pav. 16 NKSC ataskaita 58
Pav. 17 KVTC- CERT klientų informavimo ataskaita 59

SANTRUMPOS IR SĄVOKOS

Vartojamos sąvokos:

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.

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.

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.

Santrumpos:

NKSC – Nacionalinis kibernetinio saugumo centras

SVDPT – Saugus valstybinis duomenų perdavimo tinklas

KSĮ – Kibernetinio saugumo įstatymas

KVTC – Kertinis valstybės telekomunikacijų centras

ĮVADAS

Temos aktualumas ir naujumas. Pastaraisiais metais kibernetinis saugumas yra sparčiai analizuojamas ir moksliniame lygmenyje, kadangi technologijų vystymasis apima vis daugiau sričių, o jų taikymas ir prieinamumas tampa beribis. Kibernetinis saugumas įvardinamas kaip pamatas technologiškai išsivysčiusioje visuomenėje. (Schjolberg ir Ghernaouti-Hele, 2011).

Interneto sklaida visame pasaulyje padarė nemažą proveržį ir naujų nusikalstamų veikų atsiradimui, bei sudarė sąlygas susikurti tarptautinėms nusikalstamoms grupuotėms. „Elektroninės erdvės ribų nebuvimas sukūrė palankias sąlygas vykdyti nusikaltimus būnant bet kuriame pasaulio taške, kur tik yra galimybė prisijungti prie interneto. Vis labiau didėjant nusikaltimams elektroninėje erdvėje interneto pagalba, jų apsaugai turi būti skiriamas didelis dėmesys. Todėl labai svarbu apsisaugoti nuo elektroninių nusikaltimų, vykdomų pasitelkiant internetą. Kibernetinis saugumas yra pamatas valstybės bei jų piliečių apsaugai nuo kibernetinių nusikaltėlių.“ (Darius Štitilis, 2013).

Informacinės technologijos bei jų plėtra turi didelę įtaką visuomenės išsivystymui bei progresui. Nuolatos didėjanti kibernetinių išpuolių gausa privertė šalis imtis veiksmingų prevencinių priemonių, norint efektyvios kibernetinės gynybos bei prevencijos. Kibernetinės atakos gali sukelti globalų elektroninės informacijos apsikeitimo tarp valstybių sutrikdymą. Jeigu yra įsilaužiama į vieną iš Europos Sąjungos viešojo sektoriaus informacinę duomenų bazę, pasekmės gali būti jaučiamos visoje Europos sąjungoje. Kibernetinio saugumo aktualumas tapo pagrindiniu klausimu, saugant valstybių elektroninę erdvę, kritinę infostruktūrą, bei informacinius išteklius. Pasaulis priverstas kurti kibernetinio saugumo strategijas bei programas. Šalims vis daugiau viešųjų paslaugų perkeliant į elektroninę erdvę tam, kad būtų išvengta biurokratizmo ir sudarytos galimybės gyventojams gauti kuo daugiau švietimo, sveikatos, aplinkos apsaugos, kitų viešųjų paslaugų ir jos nebūtų sutrikdytos, gynyba turi būti sukoncentruota į informacijos konfidencialumą, vientisumą ir prieinamumą. Pagrindinis viešojo sektoriaus kibernetinio saugumo strategijų tikslas yra apsaugoti informacinius išteklius, užtikrinti infrastruktūros veiklą esant kritinei situacijai. Analizuojant kibernetinio saugumo sąvoką bei valdymo būdus visų pirma reiktų atsakyti į klausymą: „Kibernetinis saugumas, kas turi būti saugoma ir nuo ko turi būti saugomasi“(James A. Lewis 2006). Šį teiginį galima būtų papildyti kokia apimtimi ir kaip saugome. Kibernetinio saugumo sąvoka yra beribė ir ją yra sunku apibrėžti. „Sąvoka, kas yra kibernetinis saugumas vis dar nėra įtvirtinta“ (Richard A. Kemmerer 2003). Jis ganėtinai plačiai analizavo kibernetinio saugumo sąvoką.

Kad viešojo sektoriaus kibernetinė gynyba yra ne mažiau svarbi už karinę įrodė tai, kad po didelės kibernetinės atakos, nukreiptos prieš Estijos viešojo sektoriaus informacinius išteklius, 2008 metais po kibernetinių atakų Estijoje, NATO įkūrė kibernetinio saugumo centrą Taline, prie kurio buvo pasiūlyta prisijungti dešimčiai valstybių. Po šios kibernetinės atakos atsirado glaudesnis

bendradarbiavimas tarptautiniu lygmeniu bendroje kibernetinio saugumo kovoje. 2010 m. Lietuva buvo tarp tų dešimties valstybių kurios pasirašė kibernetinės gynybos bendradarbiavimo sutartį.

Atsakingos institucijos nuolatos konstatuoja faktus apie kibernetines grėsmes. „Opi kibernetinio saugumo problema yra interneto svetainių pažeidžiamumai. Interneto skenavimų metu iš 118 000 aukščiausiojo „.lt“ domeno interneto svetainių su turinio valdymo sistemomis identifikuota 56 400. Tyrimų duomenimis, 62 proc. iš jų naudoja neatnaujintą turinio valdymo sistemos programinę įrangą, kuri nėra saugi dėl publikuotų pažeidžiamumų. Be to, 37 proc. visų interneto svetainių turi atvirą prieigą prie svetainės valdymo skydo, todėl piktavaliai gali bandyti į jas įsilaužti, automatinėmis priemonėmis generuodami prisijungimo vardus bei slaptažodžius (NKSC, 2019). Lietuvoje didžioji dalis kibernetinių incidentų yra padaroma ne Lietuvos Respublikos teritorijoje. Kovoje su tokiomis grėsmėmis, norint užtikrinti elektroninės erdvės gynybą, yra būtinas tarptautinis bendradarbiavimas ir patirties kibernetinėje kovoje apsikeitimas.

Lietuva, optimizuodama bei modernizuodama viešojo sektoriaus valdymą, siekdama sklandžios integracijos į vis didėjančius Europos šalių narių duomenų mainus tarp šalių, siekia valstybės viešojo sektoriaus valdymo sistemos pertvarkymo, konsoliduodama IT sritį ir taikydama jai kolektyvinę kibernetinę gynybą. Šiuo metu Lietuvoje taikoma kibernetinė gynyba apima tik dalį viešojo sektoriaus institucijų, ir iki šio nebuvo tiriamas viešojo sektoriaus kolektyvinės kibernetines apsaugos efektyvumas bei patikimumas.

Tyrimo problema – Dalinis viešojo sektoriaus kolektyvinės gynybos patikimumas, efektyvumas ir pakankamas kibernetinio saugumo užtikrinimas.

Tyrimo objektas - Viešojo sektoriaus kibernetinio saugumo valdymas.

Tyrimo dalykas - kolektyvinė ir individuali kibernetinė gynyba viešajame sektoriuje kibernetinio saugumo valdymo kontekste.

Tyrimo hipotezė – Vienoje institucijoje sutelktas valstybės IT bei ryšių infrastruktūros turėjimas, resursų valdymas bei kibernetinės gynybos koordinavimas (Lietuvoje dalinai įgyvendina SVDPT) leis sustiprinti valstybės institucijų kibernetinio saugumo lygį, bei suvaldyti nepertraukiamą jų veiklą, centralizuotas valdymas leis užtikrinti konfidencialumą, vientisumą ir prieinamumą.

Tyrimo tikslas:

Išnagrinėti, palyginti ir įvertinti kolektyvinės ir individualios kibernetinės gynybos viešajame sektoriuje modelius, jų efektyvumą ir skirtumus.

Tyrimo uždaviniai:

1. Išnagrinėti kibernetinės gynybos teorinius aspektus;

2. Išanalizuoti Lietuvos viešojo sektoriaus kibernetinio saugumo teisinį reglamentavimą, bei jo įgyvendinimą kibernetinės gynybos kontekste;

3. Išanalizuoti viešojo sektoriaus institucijų kolektyvinės kibernetinės gynybos teorinius aspektus ir įvertinti gynybos efektyvumą;

4. Įvertinti viešojo sektoriaus atsparumo bei valdymo rizikas, naudojant kolektyvinę arba individualią kibernetinę gynybą.

Tyrimo šaltiniai ir metodai: Darbe buvo naudojama kibernetinio saugumo srities išsami užsienio šalių mokslinės literatūros bei informacinių pranešimų analizė. Tiriant kibernetinio saugumo raidą Lietuvoje buvo analizuojami teisės aktai, reglamentuojantys kibernetinio saugumo įgyvendinimą. Darbe buvo naudojamas mokslinės literatūros, teisės aktų, gerųjų praktikų, kibernetinio saugumo ataskaitų ir standartų analizės metodas. Atliekant teisės aktų, gerųjų praktikų, kibernetinio saugumo ataskaitų ir standartų analizę, taikomi aiškinamasis ir lyginamasis metodai. Tyrimo temos ir tikslo atskleidimui buvo naudojamas sisteminis metodas. Tiriamos temos problemos kritiniam nagrinėjimui ir vertinimui naudojamas analitinis metodas. Pasirinktos IT ir ryšių paslaugas viešajam sektoriui teikiančios organizacijos, vidinių kibernetinio saugumo grėsmių valdymo, priemonių ir jų įgyvendinimo praktikai ištirti naudojami empiriniai atvejo analizės, stebėjimo, pokalbio, dokumentų analizės metodai. Rengiant išvadas ir teikiant pasiūlymus apie viešojo sektoriaus atsparumo bei valdymo rizikas naudojamas apibendrinamasis metodas.

1. VIEŠOJO SEKTORIAUS KIBERNETINIO SAUGUMO TEISINIS REGULIAVIMAS LIETUVOJE IR GYNYBOS UŽTIKRINIMO GALIMYBĖS

1.1 Kibernetinės gynybos aspektai

Gilinantis į skirtingą mokslinę literatūrą paaiškėjo, kad kibernetinio saugumo sąvoka nėra vieninga, priešingai nei informacinio saugumo sąvoka. Nagrinėdami kibernetinį saugumą bei jo teisinį reglamentavimą Lietuvoje apžvelgsime ir jo raidą užsienio valstybėse.

Kibernetinio saugumo iššūkiai prasidėjo XX amžiaus pradžioje, technologijų proveržis išplečia nacionalinio ir tarptautinio kibernetinio saugumo problematiką. Pastarąjai atsiradus tiek viešajame, tiek privačiame sektoriuose iškilo kibernetinių grėsmių sąvoka. Apie informacinį karą ir kibernetinį saugumą tyrimuose, nebuvo skiriamas rimtas dėmesys informacinėms technologijoms, susiduriančioms su saugumo problemomis(Johan Eriksson, Giampiero Giacomello 2006).

Užduodant klausimą kas yra kibernetinis saugumas ir kokia yra jo apimtis, galima būtų apibūdinti taip: „nėra standartinės visuotinai pripažintos kibernetinio saugumo apibrėžties. Apskritai kalbant, yra priimtos visos apsaugos priemonės ir kitos priemonės, kuriomis siekiama apginti informacines sistemas ir jų naudotojus nuo neteisėtos prieigos, išpuolių ir žalos, siekiant užtikrinti duomenų konfidencialumą, vientisumą ir prieinamumą. Kibernetinis saugumas apima kibernetinių incidentų prevenciją, reagavimą į juos ir atsigavimą nuo jų. Incidentai gali būti numatomi arba ne, jų diapazonas gali būti nuo atsitiktinio informacijos atskleidimo iki išpuolių prieš verslo subjektus ir ypatingos svarbos infrastruktūros objektus, asmens duomenų vagysčių ir net kišimosi į demokratinius procesus. Jie visi gali daryti kenksmingą poveikį asmenims, organizacijoms ir bendruomenėms(Europos Audito Rūmų grupė 2019).

Siekdamas viešajame sektoriuje kibernetinio saugumo užtikrinimo, 2003 metais JAV Gynybos departamentas Nacionalinėje saugios elektroninės erdvės strategijoje nustatė pagrindinius tikslus bei veiksmus viešojo sektoriaus elektroninei erdvei apsaugoti, nurodė nuolat vertinti kibernetinių sistemų grėsmes ir pažeidžiamumus, sukurti saugius ryšio tinklus, autentifikuoti sistemų vartotojus, gerinti vyriausybės užsakomųjų paslaugų ir viešųjų pirkimų saugumą (The National Strategy to Secure Cyberspace, 2003)

2007 metai tapo kibernetinio saugumo sąvokos įsitvirtinimo metais. Po plataus masto kibernetinės atakos prieš Estijos viešojo sektoriaus institucijas imta daug plačiau naudoti sąvoką kibernetinis saugumas. Po šio įvykio atsirado ne tik kibernetinio saugumo sąvoka bet ir kibernetinio karo sąvoka (James A. Lewis, “Cyber Attacks Explained 2007). Šis įvykis parodė, kad nesant efektyviai kibernetinei gynybai, gali sustoti visi tarptautiniai elektroniniai ryšiai(Joshua Davis 2008).Europos sąjungos teisės aktuose pirmi įrašai apie kibernetinį saugumą atsiranda 2001 metais. Elektroninės informacijos saugatokia formuluotė buvo naudojama ankstesniais metais kibernetiniam saugumui apibrėžti. Pagrindiniai akcentai dokumentuose buvo apie tai, kad telekomunikacinės technologijos bei informacinės sistemos

sudarys ateities visuomenės vystymosi pagrindą. Tuo metu visoje Europoje, ir ne tik, vis didesnės kibernetinės grėsmės kyla tiek verslui, tiek ir valstybių saugumui bei stabilumui. Kadangi Europos sąjungos šalių narių išsivystymo lygis kibernetinėje srityje buvo skirtingas, todėl padarius žalą bent vienai iš jų, būtų padaryta žala ir visai Europos sąjungai. 2006 metais, galima sakyti, atsiranda kolektyvinio kibernetinio teisinio reguliavimo užuomazgos. Jos atkreipė dėmesį i tai, kad Europoje būtina sukurti saugią, vieningą kibernetinę erdvę, pasitelkus visus valdžios partnerius. Dėl skirtingo viešojo ir privataus sektoriaus technologinio išsivystymo, bei skirtumo tarp šalių, duomenys buvo saugomi tiek privačiose, tiek viešojo sektoriaus duomenų saugyklose, o kartais net ir už Europos sąjungos ribų. Tokios informacijos vagystė, pakeitimas ar sunaikinimas gali padaryti nepataisomą žalą ir sukelti didelius piniginius nuostolius verslo sektoriui, bei viešojo administravimo subjektams. Atsižvelgdamos į tai, Europos Sąjungos valstybės atkreipia visą dėmesį, kad tik bendru Europos sąjungos šalių teisiniu reguliavimu galima pasiekti norimą rezultatą kibernetinėje kovoje su vis didėjančiomis kibernetinėmis grėsmėmis. Taip pat atsiranda nauja sąvoka kaip kritinė arba ypatinga infrastruktūra bei informaciniai ištekliai, kurių apsauga yra būtina norint apsaugoti bendrą Europos sąjungos ekonominę erdvę bei saugią plėtrą. Tuo metu visoje Europos sąjungoje tarp valstybių narių atsiranda labai daug duomenų mainų platformų, kurių pagalba šalys apsikeitinėja duomenimis tam, kad būtų efektyviai išnaudojamos technologijos, siekiant sustiprinti bendrą technologinį ir ekonominį lygmenį. Toks duomenų apsikeitimas reiškia, kad valstybių narių duomenys yra pasiskirstę tarp visų narių. Iš to galima daryti išvadą, kad tai buvo bendra, kibernetinio saugumo strategijos pradžia. „Kibernetiniai incidentai šiuolaikinėje visuomenėje yra beribiai. Siekiant užtikrinti kibernetinį saugumą turi būti vieningas bendradarbiavimas tiek nacionaliniu, tiek tarptautiniu lygmeniu. Kadangi gali būti taikomi skirtingi teisės aktai ir skirtingos jurisdikcijos, vienas iš pagrindinių ES uždavinių yra išgryninti visų pagrindinių šalių vaidmenis ir atsakomybes (Darius Štitilis, 2013).

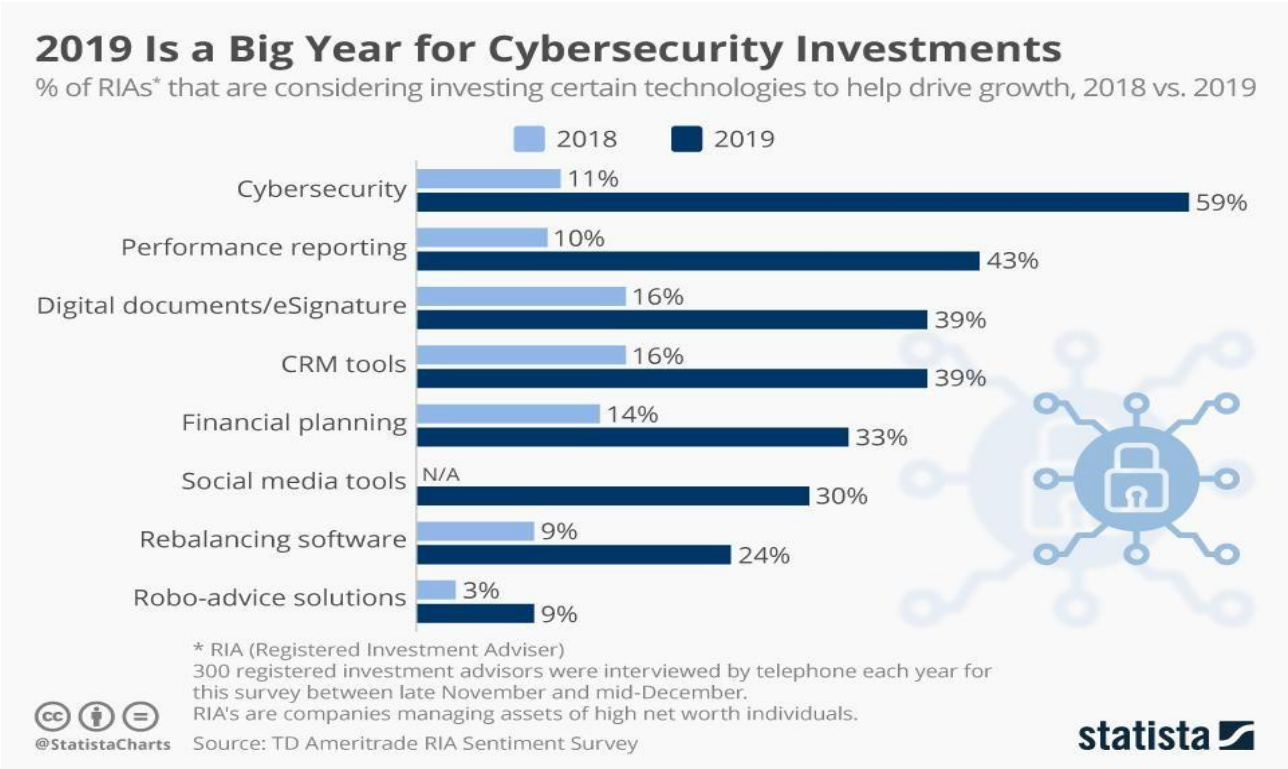
2010 metais apie bendrą kibernetinio saugumo būklę skelbė ir (SpringerBriefs in Cybersecurity). Jie konstatavo, kad organizacijos daugiausia pastangų skyrė suvaldyti išorinėms grėsmėms - įsilaužėliams, sukčiams ir pinigų plovėjams, kurie išnaudodavo silpnąsias organizacijos gynybos vietas ir mažiau dėmesio skyrė vidiniams pažeidžiamumas ir grėsmėms iš vidaus. Buvo naudojamos informacinės sistemos, kurios ne tik sugesdavo, tačiau ir veikdavo nepakankamai gerai, dėl organizacijos negebėjimo investuoti į saugumo įgyvendinimą. Daugybė kompanijų vis dar neturi saugumo politikos, o galiojanti saugumo politika yra dažnai neveiksminga. Organizacijos taip pat nelinkusios pranešti apie saugumo pažeidimus, bijodamos reputacijos praradimo. Todėl apibendrinti to meto kibernetinių atakų padarytą žalą ir mastą yra ganėtinai sudėtinga.

Kibernetinė gynyba yra pozicionuojama kaip aukštesnio lygmens saugumo tikslas, kurį sudaro kompleksinis kibernetinio saugumo sprendimas. „Kibernetinis saugumas reikalingas ne tik ryšių tinklo išoriniame perimetre, bet ir vidiniuose tinkluose. Standartinę tinklo perimetro gynybą sudaro įsibrovimų

užkardos, aptikimo sistemos ir saugi architektūra, o vidinė gynyba apimtų vientisumo patikrinimus, tinklo stebėjimą ir žurnalų analizę“ (SpringerBriefs in Cybersecurity).

Valstybės ekonominio išsivystymo lygis yra tiesiogiai proporcingas kibernetinėms grėsmėms. Didesnį pelną nusikaltėliams garantuoja kibernetinės atakos, nukreiptos prieš turtingas įmones, gyventojus bei viešąjį sektorių, kurie dažniausiai turi lėšų sumokėti už pavogtų duomenų grąžinimą ir neatskleidimą, tačiau būtina paminėti, kad ekonomiškai stiprios šalys yra labiau pajėgios investuoti į kolektyvinę kibernetinę gynybą užtikrinančias technologijas, didinti kibernetinės brandos lygį bei užtikrinti prevenciją. Vis didėjančiam kibernetinių incidentų kiekiui didelę įtaką turi technologinis progresas bei didėjanti interneto infrastruktūra. Pastaraisiais metais investicijos į kibernetinį saugumą šoktelėjo beveik 6 kartus. Tai atspindi investicijų sparta bei investicijos į kibernetinio saugumo sprendimus teikiančią pramonę pav. 1 (FORBES,2020).

.



Šaltinis: FORBES 2020

Pav. 1 Investicijos 2019

Šiandien pasaulio lyderiai baiminasi, kad kibernetinis terorizmas bei kibernetinis karas kelia naują ir, galbūt, rimtą grėsmę nacionaliniam saugumui. Internetas yra galingas išteklius, šiuolaikinė visuomenė yra vis labiau priklausoma nuo jo, o kibernetiniai užpuolikai pademonstravo gebėjimą manipuliuoti ir trikdyti internetą dėl įvairių politinių ir karinių tikslų.

Nacionalinio saugumo planuotojams yra aišku, kaip parengti kibernetinę gynybą tiek taktiniame, tiek strateginiame lygmenyje. Svarbu yra padėti sprendimus priimantiems asmenims su vėlesniu strateginiu lygmeniu pasirinkti efektyviausius strateginio lygmens veiksmus, siekiant apginti savo nacionalinius interesus kibernetinėje erdvėje (Strategic cyber security).

1.2 Lietuvos ryšių ir informacinių sistemų kibernetinio saugumo užtikrinimo teisinio reguliavimo raida

1997 metais Lietuvoje buvo patvirtinti pirmieji informacijos saugumo reikalavimai, kurie vadinosi Bendraisiais duomenų apsaugos reikalavimais. Reikalavimai buvo taikomi visiems duomenų valdytojams, kurie privalėjo vadovaudamiesi Lietuvoje galiojančiais bei tarptautiniais ISO standartais, užtikrinti elektroninės informacijos apsaugą bei patikimumą ir užkirsti kelią neteistam jų naudojimui.

2001 m. į kibernetinį saugumą (informacijos saugą) buvo žiūrima didesne apimtimi. Lietuvoje atsiranda informacijos technologijų sauga bei jos įgyvendinimo planus apibendrinanti valstybinės strategija, kuri numatė raidos kryptis, priemones ir jų įgyvendinimą. 2001 metų strategijoje buvo suformuoti pagrindiniai tikslai apimantys teisinio reglamentavimo plėtrą, atsižvelgiant į tarptautinius standartus, NATO ir Europos Sąjungos rekomendacijas, užtikrinti svarbiausiųjų valstybės informacinių sistemų saugą.

Apie Lietuvoje informacinių technologijų panaudojimą valstybės institucijų priimamų sprendimų veiksmingumui skatinti, diegti informacinių technologijų ir telekomunikacijų priemones viešojo administravimo institucijų darbe, užtikrinti jų saugumą, 2002 metais buvo patvirtinta „Valstybės ilgalaikės raidos strategija“, tačiau dėmesys šiai sferai buvo itin mažas. Kitame strateginės reikšmės dokumente – „Nacionalinio saugumo strategijoje“ buvo skirtas tik vienas, prie vidaus saugumo stiprinimo priemonių numatytas sakinys „ kuris teigė ,kad teisinis reglamentavimas turi būti tobulinamas vadovaujantis tarptautiniais standartais, stiprinamas valstybės informacinių išteklių kibernetinis saugumas bei privalo būti įgyvendinta saugumo priemonių kontrolė“(Nacionalinio saugumo strategija, 2002).

Iki 2005 metų jautėsi dėmesio stoka kibernetiniam saugumui „Didėjant Lietuvoje elektroninių paslaugų ir informacinių technologijų naudojimui, valstybės institucijos, elektroninių ryšių tinklų, elektroninių paslaugų teikėjai ir vartotojai per mažai dėmesio skiria tinklų ir informacijos saugumui.“(LRV Nacionalinio saugumo būklės ir plėtros 2005 metų ataskaita).

Technologijų priemonių nepakankamumas bei žema informacijos valdymo branda neleido efektyviai valdyti valstybės informacinių išteklių.

Elektroninių ryšių tinklų progreso nebuvimas, bei valdymo trūkumai ir saugumo neužtikrinimas neleido valstybei efektyviai valdyti informacinių išteklių. Lietuvoje Elektroninės informacijos saugos (kibernetinio saugumo) teisinis reglamentavimas prasidėjo 2006 metais nuo Lietuvos Respublikos Vyriausybės nutarimo Nr. 406, kuris apsibrėžė informacijos saugos strategiją valstybės institucijų informacinėse sistemose bei įgyvendinimo priemonių planą. Pagrindiniai strategijos tikslai buvo sureguliuoti viešąjį sektorių, elektroninės informacijos saugą, elektroninių ryšių saugą, kelti informacijos saugos brandą.

Analizuojant to meto teisinį reglamentavimą, galima teigti, kad tai buvo daroma paskubomis tam, kad įstojus į Europos sąjungą būtų galima įgyvendinti duomenų mainų programą tarp ES. 2004 metais buvo patvirtintos „Elektroninio keitimosi duomenimis su Europos Sąjungos ir valstybių narių administracijomis taisyklės“. Lietuvoje keitimasis duomenimis su ES IDA (nuo 2018 metų „ISA2“ (angl. Interoperability Solutions for Public Administrations, Businesses and Citizens)) programos tinklais vykdomas tik per SVDPT. Buvo patvirtintos „Saugaus valstybinio duomenų perdavimo tinklo nuostatai ir paslaugų teikimo taisyklės“. VĮ „Infostruktūra“ pavesta vykdyti šio tinklo operatoriaus funkcijas.

Apibūdinti to meto Lietuvos kibernetinę brandą galima būtų taip: „ Lietuvoje nėra pamatinių teisės normų, reglamentuojančių kibernetinio saugumo klausimus. Tam tikros kibernetinio saugumo teisinio reglamentavimo iniciatyvos žlugo: buvo parengtas Lietuvos Respublikos elektroninių ryšių įstatymo projektas, tačiau šis projektas nebuvo priimtas. Tam tikros teisės normos dėl kibernetinio saugumo numatytos tik valstybės informacinių išteklių įstatyme, tačiau jos reglamentuoja tik valstybės informacinių išteklių saugą bei saugos įgaliotinio institutą, be to, yra fragmentiškos“ (Darius Štitilis 2013).

Jeigu apie kibernetinio saugumo sąvoką plačiau imta kalbėti nuo 2007 metų, tai apie kibernetinio incidento sąvoką tik nuo 2014 metų ir iki šiol dar nėra vieningos nuomonės. „Jungtinių Amerikos valstijų teisėje pabrėžiama, kad kibernetiniu incidentu laikomi ne tik įvykiai, bet ir planuoti veiksmai, sukeliantys realius arba potencialius pavojus informacinėms sistemoms ar jose esančiai informacijai“(National Information Assurance Glossary 2010). Analizuojant Europos pavyzdį 2014 metų Čekijos parlamento priimtame kibernetinio saugumo akte, kibernetiniu incidentu laikomas įvykis, kurio metu pažeidžiamos informacinės sistemos, apsaugos programos arba telekomunikacinis tinklas(Act on Cyber Security, Parliament of Chech Republic 2014). Lietuvoje kibernetinis incidentas apibūdinamas taip: įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą prie informacinių sistemų ar elektroninių ryšių tinklų, gali perimti informacinių sistemų procesų valdymą. Tai galima būtų apibūdinti kaip vientisumui , prieinamumui bei konfidencialumui padarytą žalą. Išanalizavus visus tris pavyzdžius matyti, kad vyrauja labai didelė įvairovė, ir prie vieningos nuomonės dar ilgai nebūtų prieita.

2011 metais Lietuva padarė didelį proveržį, nelaukdama kol Europos Komisija paskelbs konsultacijas apimančias ES kibernetinio saugumo strategiją. Nederindama su ES bendrąja kibernetinio saugumo strategija, Lietuva padarė proveržį vyriausybei patvirtinus nutarimą Nr. 796, kuris numatė elektroninės informacijos saugos plėtrą 2011–2019 metams. Taip skubos tvarka ir buvo priimta plėtros programa 2011–2019 metams. Rengiant naują programą pagrindinis dėmesys buvo skirtas dideliam technologiniam progresui, kuris atlieka vis didesnį vaidmenį valstybės ir visuomenės gyvenime. Informacinėmis ir ryšių technologijomis perduodama elektroninė informacija bei jos sauga turi didelę įtaką visuomenės gyvenime, atsiradusios tarpvalstybinės elektroninės informacijos tvarkymo ir apsikeitimo galimybės paskatino nacionalinį bei tarptautinį kibernetinio saugumo bendradarbiavimo atsiradimą ir paskatino efektyvinti bei modernizuoti šalių turimas infrastruktūras ir efektyvinti valstybės valdymą. Šalims vis labiau skaitmenizuojant informaciją bei ją perkeliant į elektroninę formą, atsiranda ne tik tarpinstituciniai mainai bet ir tarpvalstybiniai duomenys tampa globalūs. Šalys vis sparčiau automatizuoja bei skaitmenizuoja įvairius šalies veiklos, valdymo ir ūkio procesus, bei perkelia juos į elektroninę erdvę. Dėl tokios globalizacijos viešųjų paslaugų informacija tapo patraukliu pavienių asmenų, tarptautinių nusikalstamų grupuočių, nedraugiškų valstybių ir kitų piktavalių taikiniu.

2011 metais, vyriausybei patvirtinus elektroninės informacijos saugos 2011–2019 metų programą, buvo nustatyti ir pagrindiniai tikslai bei uždaviniai. Siekiant sėkmingo programos įgyvendinimo turi būti užtikrintas prieinamumas, vientisumas bei konfidencialumas. Tai yra būtina norint užtikrinti elektroninių ryšių tinklų, ypatingos svarbos informacinės infrastruktūros bei kritinės infrastruktūros kibernetinį saugumą. Programos tikslas yra labiau orientuotas į viešojo sektoriaus kibernetinį saugumą, ir tik nedidele dalimi paliestas privatus sektorius. Siekiant užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais butų pasiekta institucijos valdančios arba tvarkančios valstybės informacinius išteklius būtų įgyvendinę 98 procentus organizacinių it techninių kibernetinio saugumo reikalavimų, kad incidentų įalinimo laikas netuktų ilgiau nei puse valandos. Buvo užsibertas ir sunkiai įgyvendinamas bei pamatuojamas tikslas kad net 60 procentų gyventojų i saugiai jaustas elektroninėje erdvėje.

Kad būtų galima pasiekti užsibrėžtą kibernetinio saugumo brandą, siekiant apsaugoti valstybės informacinius išteklius bei ryšio tinklus, plėtros programoje buvo nustatyti įgyvendinimo tikslai:

A) Sukurti efektyvią elektroninės informacijos saugos valdymo sistemą;
B) Parengti trūkstamus teisės aktus, suteikti įgaliojimus bei įpareigoti institucijas kurios įgyvendina kibernetinio saugumo kontrolę ir koordinavimą;
C) Skatinti Lietuvos viešojo sektoriaus bendradarbiavimą su verslo organizacijomis kibernetinio saugumo srityje, kadangi jo nebuvimas neskatina efektyvios elektroninės kibernetinio saugumo srities plėtros;
D) Organizuoti kibernetinio atsparumo bei spragų pažeidžiamumo aptikimo centralizavimą.

Tai padėtų efektyviai valdyti žmogiškuosius resursus bei vienoje vietoje konsoliduoti jų kompetenciją;

E) Mažinti kibernetinių incidentų skaičių bei didinti kibernetinį atsparumą;

Pagrindinių 2011–2019 metų siekiamų plėtros programos tikslų įgyvendinimui būtina atlikti sekančius uždavinius: Parengti trūkstamus teisės aktus, reglamentuojančius elektroninės informacijos saugą viešajame sektoriuje; vystyti saugią valstybės informacinę infrastruktūrą bei elektroninių ryšių tinklus; rengti elektroninės informacijos saugos (kibernetinio saugumo) projektus bei skatinti jų įgyvendinimą; vystyti bei užtikrinti patikimą tapatybės nustatymą, siekti mažinti rizikas bei valdyti grėsmes; didinti kibernetinio saugumo tarptautinį bendradarbiavimą, siekti narystės tarptautinėse kibernetinio saugumo organizacijose; užtikrinti ryšio ir kitų informacinės bei kritinės infrastruktūros paslaugų saugumą; kelti specialistų kompetencijas bei skatinti bendradarbiavimą, plėsti prevencinę veiklą; plėtoti bei koordinuoti kibernetinio saugumo kontrolę ir koordinavimą;

2015 m. sausio 1 d. Lietuvoje įsigaliojo Kibernetinio saugumo įstatymas, kuris buvo paskelbtas 2014 m. gruodžio 11 d. Šis įstatymas įgyvendina pagrindinius kibernetinio saugumo teisinio reguliavimo tikslus, nustato kaip bus organizuojamas kibernetinio saugumo užtikrinimas, koks bus valdymas bei kontrolė. Įstatymui įsigaliojus buvo paskirtos institucijos atsakingos už politikos formavimą bei įgyvendinimą, apibrėžtos jų kompetencijos, funkcijos, teisės ir pareigos. Nustatytos pareigos bei atsakomybė valstybės informacinių išteklių valdytojams, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų bei prieglobos paslaugų teikėjams, kurie privalo užtikrinti organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimą“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014). Kibernetinio saugumo įstatymas taikomas *„valstybės institucijoms, formuojančioms ir įgyvendinančioms kibernetinio saugumo politiką, viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų teikėjams ir elektroninės informacijos prieglobos paslaugų teikėjams, informacinių technologijų srityje veiklą vykdantiems verslo subjektams, mokslo ir studijų institucijoms“* (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Kibernetinio saugumo įstatymas įgyvendina didžiąją Kibernetinio saugumo 2011–2019 metų plėtros programos tikslų dalį. Pagrindinis įstatymo uždavinys yra orientuotas į viešąjį sektorių ir nukreiptas apsaugoti valstybės informacinius išteklius. Kibernetinio saugumo įstatymas paremtas bendraisiais teisiniais principais, kibernetinės erdvės nediskriminavimo bei elektroninių ryšių veiklos reguliavimo principu, kur teisės aktų nuostatos turi būti taikomos tiek elektroninėje, tiek fizinėje erdvėje. Taip pat paremtas kibernetinio saugumo proporcingumo principu, kur užtikrinant kibernetinį saugumą negalima taikyti griežtesnių priemonių nei būtina. Kibernetinio saugumo įstatyme atsiranda visam

viešajam sektoriui bei kritinei infostruktūrai taikomi privalomi organizaciniai ir techniniai reikalavimai skirti kibernetiniam saugumui užtikrinti. Nustatyta, kad reikalavimai neturi apriboti institucijų bei organizacijų veiklos. Nepamirštas buvo ir viešojo intereso viršenybės principas, kuris apibrėžia, kad kibernetinio saugumo užtikrinimo priemonės nepažeis viešojo intereso, atskirų vartotojų teisių bei garantuos jo apsaugą kibernetinėje erdvėje.

Vadovaudamasi kibernetinio saugumo įstatymu, Lietuvos Respublikos Vyriausybė nustato strateginius tikslus ir priemones, reikalingas kibernetinio saugumo įgyvendinimui. Įstatymas numato, kad kibernetinio saugumo sritį kuruoja Lietuvos Respublikos Krašto apsaugos ministerija. Jai pavesta formuoti kibernetinio saugumo politiką bei paskirti kuruojančią instituciją, kuri užtikrins jos įgyvendinimą. Įstatymas numato, kad institucijos atsakingos už kibernetinio saugumo įgyvendinimą pagrindinį vaidmenį atliks Nacionalinis kibernetinio saugumo centras, kuris kontroliuos bei prižiurės organizacinių ir techninių reikalavimų įgyvendinimą, Valstybinė duomenų apsaugos inspekcija, kuri prižiūrės savo kontroliuojamą sritį, Policijos departamentas kuris tirs nusikaltinus elektroninėje erdvėje, bei kitos institucijos tokios, kaip Lietuvos Respublikos vidaus reikalų ministerija, Lietuvos Respublikos ryšių reguliavimo tarnyba (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymo nuostatomis, Kibernetinio saugumo informacinį tinklą valdo Nacionalinis kibernetinio saugumo centras. Kibernetinio saugumo informacinis tinklas yra patikima informacijos mainų platforma, kuri surenka ir apdoroja informaciją apie kibernetinius incidentus. Susistemintą informaciją su rekomendacijomis jie pateikia naudotojams siekdami stiprinti bendrą informacinio tinklo narių kibernetinį saugumą. Tik atitikę šio tinklo nuostatuose nurodytus reikalavimus vartotojai gali naudotis informaciniu tinklu ir gauti aktualią informaciją apie kibernetinius incidentus, taip pat kitų subjektų kontaktinę informaciją kurie yra atsakingi už kibernetinio saugumo organizavimą ir kibernetinių incidentų valdymą. Nacionalinis kibernetinio saugumo centras, Ryšių reguliavimo tarnyba, Policijos departamentas ir kitos policijos įstaigos bendradarbiauja tiriant kibernetinius incidentus, keičiasi su kibernetinių incidentų tyrimais susijusia informacija, kuri reikalinga tyrimams atlikti. Valstybinė duomenų apsaugos inspekcija bendradarbiauja su Nacionalinio kibernetinio saugumo centru ir Ryšių reguliavimo tarnyba tiriant kibernetinius incidentus, susijusius su asmens duomenų saugumo pažeidimais, keičiasi informacija, reikalinga teisės aktų nustatytoms funkcijoms, susijusioms su kibernetinių incidentų, pažeidžiančių asmens duomenų saugumą, tyrimu, atlikti“ (Lietuvos Respublikos kibernetinio saugumo įstatymas, 2014).

Kibernetinio saugumo įstatymas aiškiai suskirstė Lietuvos institucijų, vykdančių kibernetinio saugumo užtikrinimą veiklos sritis ir funkcijos pagal savo kompetencijas:

1. Lietuvos Respublikos Vyriausybė;
2. Lietuvos Respublikos krašto apsaugos ministerija;

3. Vidaus reikalų ministerija;
4. Nacionalinis kibernetinio saugumo centras;
5. Ryšių reguliavimo tarnyba;
6. Valstybinė duomenų apsaugos inspekcija;
7. Policijos departamentas.

Apibendrinant galima būtų teigti, kad iki 2015 metų pabaigos Lietuvoje teisinis reguliavimas kėlė didelį pavojų efektyviam kibernetinio saugumo užtikinimui. „Išnagrinėję kibernetinio saugumo ir el. informacijos saugos politiką formuojančių ir įgyvendinančių įstaigų tarpusavio ryšius ir vykdomas funkcijas, nustatėme, kad 2015 m. pradėjo veikti kibernetinio saugumo valdymo sistema, tačiau ji nesudaro visų su el. informacijos sauga susijusių sričių darnaus valdymo sąlygų. Kibernetinio saugumo įstatyme apibrėžtos kibernetinio saugumo politiką formuojančios ir įgyvendinančios institucijos, jų įgaliojimai, tačiau iš tiesų kol kas neišvengiama dalinio įstaigų veiklos dubliavimo. Nėra paskirtos vienos institucijos, atsakingos už kibernetinio saugumo politikos formavimą bei įgyvendinimą. Neperžiūrėtos institucijų vykdomos funkcijos pagal kuruojamas sritis. “(Valstybinio audito ataskaita, 2015 m). Iš valstybės kontrolės ataskaitos matyti silpna viešojo sektoriaus kibernetinio saugumo branda pav. 2.



Šaltinis: 2015 metų valstybės kontrolės audito ataskaita

Pav. 2 Kibernetinio saugumo aplinka Lietuvos viešajame sektoriuje

2018 metais Lietuvoje pirmą kartą rimčiau susirūpinta ne tik kibernetinio saugumo teisiniu reglamentavimu bet ir jo įgyvendinimu. Nuo 2018 metų Krašto apsaugos ministerijai pavesta formuoti, kontroliuoti ir koordinuoti valstybės informacinių išteklių kibernetinio saugumo įgyvendinimą, kibernetinio saugumo bei elektroninės informacijos saugos politiką. Krašto apsaugos ministerija pradeda stiprinti valstybės kibernetinio saugumo pajėgumus, vykdys bet kurios saugumo srities užtikrinimą.

Nuo 2018 metų liepos 4 dienos įsigaliojus naujam Lietuvos Respublikos kibernetinio saugumo įstatymui bei Administracinių nusižengimų kodekso pakeitimams, atsirado sąlygos efektyviau valdyti vykstančius incidentus, taip pat numatyti atsakomybę už realius pažeidimus, kurie kelia grėsmes kibernetiniam saugumui. Po šio įstatymo įsigaliojimo pradedamas rengti Nacionalinės kibernetinio saugumo strategijos projektas, kuriame didelis dėmesys būtų skirtas kovai su pastaraisiais metais Lietuvoje vis didėjančiais kibernetiniais išpuoliais prieš viešąjį sektorių, kritinę infostruktūrą bei nacionaliniam saugumui svarbius objektus.

2019 metų liepos 3 d. Vyriausybės patvirtintame Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniame veiklos plane (2019-2021 m.), išskiriamos konkrečios priemonės ir asignavimai kibernetinio saugumo srityje, taip pat paskirtos atsakingos Lietuvos institucijos ir įstaigos.

Pagrindinės veiklos plano priemonės bei tikslai susiję su informacinės visuomenės plėtra, nusikalstamų veikų elektroninėje erdvėje mažinimu, energetikos sektoriaus kibernetinio saugumo užtikrinimo stiprinimu, naujų inovacijų diegimu finansinių technologijų sektoriuje, mokslinės veiklos finansavimu ir kitose technologijų srityse. Tarp daugelio numatomų įgyvendinti priemonių, ketinama vystyti kibernetinės gynybos pajėgumus, numatoma kurti Regioninio kibernetinio saugumo centrą Kaune. Bendradarbiaujant su mokslo įstaigomis kurti modernias ankstyvojo kibernetinių grėsmių aptikimo ir automatinio užkardymo sistemas, taip pat didelis dėmesys būtų skirtas kibernetinės gynybos priemonių įsigijimui tam, kad būtų galima aprūpinti Ryšių ir informacinių sistemų batalioną, kuris neseniai buvo įkurtas Lietuvos kariuomenėje. Įgyvendinant strategijos veiklos planą, pagal savo kompetenciją dalyvaus Krašto apsaugos, Vidaus reikalų, Policijos departamentas, Ekonomikos ir inovacijų ministerija, Vyriausybės kanceliarija, Švietimo, Mokslo ir Sporto ministerija, Užsienio reikalų ir Teisingumo ministerijos, Nacionalinis kibernetinio saugumo centras, kitos Lietuvos valstybės ir savivaldybių institucijos, įstaigos ir organizacijos.

Atsižvelgiant į tarptautinių standartų ir metodikų pateikiamus kibernetinio saugumo apibrėžimus ir valdymo praktiką, kibernetinis saugumas šiame darbe bus analizuojamas plačiau, kartu su kitomis saugos sritimis, pagal Tarptautinės standartizacijos organizacijos standartus (ISO/IEC 27032:2012), bei gerąsias Tarptautines kibernetinio saugumo praktikas. Kibernetinis saugumas tiesiogiai susijęs su elektroninės informacijos, taikomųjų programų, tinklų, interneto ir ypatingos svarbos informacinės infrastruktūros saugos sritimis.

Galima teigti, kad Lietuva padarė milžinišką proveržį teisiniame reguliavime, susijusiame su kibernetiniu saugumu, tačiau teisinis reguliavimas dar negarantuoja faktinio kibernetinio saugumo užtikrinimo. Kitame skyriuje bandysime išanalizuoti faktinį teisės aktų veikimą, siekiant užtikrinti kibernetinę gynybą bei efektyvų kibernetinių pajėgumų valdymą.

1.3 Lietuvos viešojo sektoriaus ryšių ir informacinių sistemų kibernetinio saugumo užtikrinimo organizavimas bei įgyvendinimas

Esant didelei technologinei globalizacijai neužtenka tik Lietuvoje užtikrinti kibernetinį saugumą, tačiau būtina bendradarbiauti ir tarptautiniu mastu. Esant didelio masto kibernetinėms grėsmėms yra labai svarbu koordinuoti tarpusavio veiksmus kibernetinio saugumo srityje. Europos Komisija pasisako už glaudų bendradarbiavimą su tarptautiniais partneriais, užtikrinant bendrą Europos sąjungos kibernetinę gynybą. 2017 metais, tam kad būtų pasiektas efektyvus gynybos būdas kovoje su kibernetiniais išpuoliais, Europos sąjungos institucijos sustiprino tarpusavio bendradarbiavimą. 2017 metais buvo įsteigta nuolatinė CERT-EU (Kompiuterinių incidentų tyrimo tarnyba), kuri glaudžiai bendradarbiauja su atitinkamomis NATO tarnybomis bei vienija Europos sąjungos institucijas, atsakingas už kibernetinį saugumą.

Šiame skyriuje apžvelgsime kaip įgyvendinami kibernetinio saugumo uždaviniai, kuriems tikslai buvo suformuoti Lietuvos Respublikos Vyriausybės 2011 m. birželio 29 d. nutarimu Nr. 796 „Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo“, bei 2019 metų liepos 3 d. Vyriausybės patvirtinta Nacionalinės kibernetinio saugumo strategija, o įgyvendinamas buvo užtikrinamas senuoju 2014 m. gruodžio 11 dienos bei naujuoju 2018 metų liepos 4 dienos įsigaliojusiu Lietuvos Respublikos kibernetinio saugumo įstatymu bei Administracinių nusižengimų kodekso pakeitimais.

2016 metais, praėjus metams po pirmo kibernetinio saugumo įstatymo įsigaliojimo buvo susirūpinta jo įgyvendinimu ir pirmą kartą buvo paminėta kolektyvinės kibernetinės gynybos svarba. „Lietuvoje šiandien turime situaciją, kai rūpinimasis kolektyvine kibernetine gynyba kol kas lieka tik kalbomis. Yra daug institucijų, valdančių svarbius ir labai svarbius valstybei duomenis, tačiau jų kibernetinė apsauga neatitinka šių dienų reikalavimų. Dar daugiau, ne visos šios institucijos naudojasi saugiu duomenų perdavimo tinklu, yra pasirinkusios tiekėjus savo nuožiūra, tai reiškia, kad vienos kitoms svarbius duomenis siunčia viešu interneto ryšiu, tad sutrikdyti jų perdavimą arba suorganizuoti kibernetinę ataką yra labai lengva. Tokią situaciją reikia taisyti. Gal efektyviausia būtų sujungti šias institucijas į vieną saugų ir uždarą tinklą, kuris maksimaliai apsaugotų nuo kibernetinių pavojų, leistų be trikdžių dirbti net ir patyrus išpuolį" (situaciją aiškina NSGK pirmininkas A. Paulauskas). Kibernetinio saugumo centras stebi kas vyksta valstybinių institucijų tinkluose, tačiau Kibernetinio saugumo įstatymas įrankių veikti jiems 2016 metais dar nenumatė. Įstatymiškai yra taip, kad sistema kolektyvinei gynybai užtikrinti lyg ir sukurta, tačiau įgaliojimų veikti ir resursų tam nėra. Laikas žengti antrąjį žingsnį po įstatymo priėmimo - įgyvendinti kolektyvinę kibernetinę gynybą. Tam yra būtina, kad visos svarbius duomenis valdančios institucijos atsidurtų saugiame ir uždarame tinkle, kuris net rimtos atakos atveju veiktų ir užtikrintų tarpinstitucinį duomenų perdavimą ir leistų valstybei atlikti savo

funkciją - aptarnauti Lietuvos gyventojus. Kibernetinių atakų neišvengsime, tačiau sumažinti jų pasekmes įmanoma".

2016 metais įvyko ženklių ir, galima sakyti, ilgai lauktų pokyčių Lietuvos kibernetinio saugumo reglamentavime. Nuo 2015 metų, kai buvo pradėtas teisinės bazės kibernetinio saugumo srityje tobulinimas, ir buvo priimti pirmieji Kibernetinio saugumo įstatymo normas reglamentuojantys bei realizuojantys teisės aktai tokie kaip Lietuvos Kibernetinio saugumo įstatymas, įvyko nemažai pasikeitimų. 2016 metų sausio 25 d. Lietuvos Respublikos Vyriausybė priima nutarimą Nr. 87 „Dėl nacionalinio kibernetinių incidentų valdymo plano“. Šiuo planu buvo nustatyti valstybės informacinių išteklių ir kritinės informacinės infrastruktūros valdytojų bei tvarkytojų veiksmai bei atsakomybė, siekiant suvaldyti nuolatos didėjančius reikšmingus kibernetinius incidentus. Šitie veiksmai buvo nukreipti siekiant vienyti bei konsoliduoti institucijų ir organizacijų pastangas kibernetinėje kovoje. Šiame teisės akte buvo reglamentuotas kibernetinių incidentų klasifikavimas, jų nustatymas bei vertinimo tvarka, nustatyta reagavimo į kibernetinius incidentus tvarka, kibernetinio incidento tyrimo analizės būtinumas bei tarpinstitucinis bendradarbiavimas tiriant kibernetinius incidentus ir stiprinant bendrą valstybės kibernetinio saugumo brandą.

2017 metais Kibernetinio saugumo ir telekomunikacijų tarnyba prie Krašto apsaugos ministerijos pirmą kartą atliko Lietuvos nacionalinio kibernetinio saugumo būklės ataskaitą. Ją išanalizavus, galima teigti, kad kibernetinio saugumo būklė Lietuvoje nėra gera, o tik patenkinama. Ataskaitoje išanalizuotas viešojo sektoriaus pasirengimas parodė kad:

1) Lietuvos viešasis sektorius vadovaujasi Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa, kuri yra pasenusi, nebeatspindi vis didėjančių aktualių kibernetinių grėsmių. Lietuvoje stebimas atotrūkis tarp elektroninės informacijos apsaugos ir kibernetinio saugumo teisinio reglamentavimo, kas trukdo efektyviai ir kompleksiškai spręsti kibernetinio saugumo problemas.
2) Vėluojama identifikuoti šalies kritinę infrastruktūrą ir ypatingos svarbos informacinę infrastruktūrą. Valstybės informacinių išteklių valdytojai ir (arba) tvarkytojai nėra pajėgūs laiku ir numatyta apimtimi įgyvendinti Lietuvos Respublikos Vyriausybės patvirtintų kibernetinio saugumo organizacinių ir techninių reikalavimų.
3) IT sprendimų bei talpinimo paslaugų teikėjai neskiria pakankamo dėmesio kibernetiniam saugumui, neapibrėžiama atsakomybė ir saugos spragų šalinimas, nepakankamai kontroliuojama atliktų darbų kokybė bei neatliekamas kibernetinių pažeidžiamumų vertinimas, ko pasėkoje yra sukuriamas pažeidžiamas produktas.
4) Viešojo sektoriaus organizacijos nesidalina aktualia kibernetinio saugumo informacija arba neturi galimybės dalintis pastebėtomis kibernetinėmis atakomis ar naujais išpuolių būdais, jos mano kad viską išspręs savarankiškai.

5) Organizacijų kibernetinio saugumo branda nėra aukšta, jos nesupranta, kad kibernetiniai nusikaltėliai, tikslingai planuodami kibernetines atakas ir koordinuodami savo veiksmus, gali padaryti nepataisomą žalą institucijai.
6) Organizacijos ir toliau naudoja pasenusias ir gamintojo nebepalaikomas operacines sistemas bei programinę įrangą. Neinvestuoja į personalo ugdymą bei kompetencijų kėlimą kibernetinio saugomo srityje.

Pabrėžtina tai, kad visuose to meto dokumentuose ši tarnyba vadinama Lietuvos Nacionaliniu kibernetinio saugumo centru (NKSC), nors juridinį statusą ji įgavo tik 2018 metais. Analizuojant Lietuvos Respublikos kibernetinio saugumo įstatymą (2014 m. gruodžio 11 d. Nr. XII-1428.) galima daryti išvadą, kad nuo 2015 metų iki 2018 metų Nacionalinis kibernetinio saugumo centras neturėjo teisinio pagrindo, pagal kompetenciją įgyvendinti kibernetinio saugumo politikos, ir vykdyti valstybės informacinių išteklių, ypatingos svarbos informacinių infrastruktūrų kibernetinių incidentų valdymo padalinio veiklos. Registrų centro duomenimis tik 2018 sausio 2 dieną buvo pakeistas Vyriausybinių ryšių centro prie Krašto apsaugos ministerijos pavadinimas į Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos. Atkreiptinas dėmesys ir į tai, kad Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatai buvo patvirtinti Lietuvos Respublikos krašto apsaugos ministro tik 2017 metų rugpjūčio 31 dieną.

Įvertinus žemiau įvardytus darbus kurie buvo pavesti Lietuvos Respublikos kibernetinio saugumo įstatymu Nacionaliniam kibernetinio saugumo centrui:

1) pagal savo įgaliojimus rengti ir teikti pasiūlymus dėl viešojo sektoriaus organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimo užtikrinimo;

2) atlikti atitikties vertinimą organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

3) rengti specialiuosius kibernetinių incidentų valdymo planus, taikomus ypatingos svarbos informacinėms infrastruktūroms;

4) Konsultuoti valstybės informacinių išteklių valdytojus, bei teikti jiems rekomendacijas kibernetinio saugumo klausimais;

5) analizuoti nacionalinę kibernetinio saugumo situaciją ir rengti ataskaitas apie kibernetinio saugumo būklę;

6) Kartą metuose rengti ir teikti nacionalinio kibernetinio saugumo būklės ataskaitas krašto apsaugos ministrui;

7) rengti ypatingos svarbos informacinių infrastruktūrų kibernetinės gynybos planus;

8) valdyti kibernetinio saugumo informacinį tinklą;

9) vykdyti informacijos sklaidą kibernetinio saugumo klausimais;

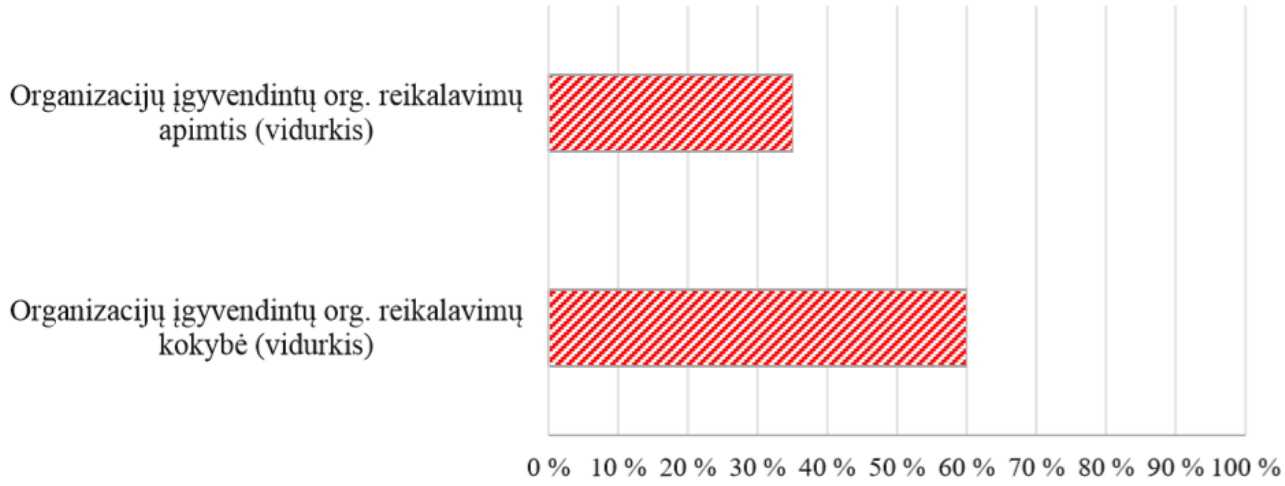
10) laikantis krašto apsaugos ministro nustatytos tvarkos, reaguoti į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose;

11) atlikti kitas Lietuvos Respublikos teisės aktuose nustatytas funkcijas kibernetinio saugumo užtikrinimo srityje.

Galima teigti, kad toks pavėluotas Nacionalinio kibernetinio saugumo centro įteisinimas turėjo didelę įtaką kibernetinio saugumo užtikrinimui bei raidai Lietuvoje. Be to, išanalizavus uždavinius, galima matyti, kad Nacionalinis kibernetinio saugumo centras nevykdo faktinės kibernetinės gynybos, o tik formuoja politiką, prevenciją bei vertina atitiktį organizaciniams bei techniniams kibernetinio saugumo reikalavimams.

Labai svarbią įtaką kibernetinio saugumo stiprinimui turi ir vyriausybės 2016 metų nutarimo organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų viešajam sektoriui, įgyvendinimas. Siekiant įgyvendinti šio nutarimo 2.2 punktą, kuris numato, kad ne vėliau kaip per 4 mėnesius būtina pateikti Nacionaliniam kibernetinio saugumo centrui saugumo reikalavimų įgyvendinimo priemonių planą institucijoms jį pateikti buvo praktiškai neįmanoma, nes centras juridinį statusą įgauna tik 2018 metų sausio mėnesį.

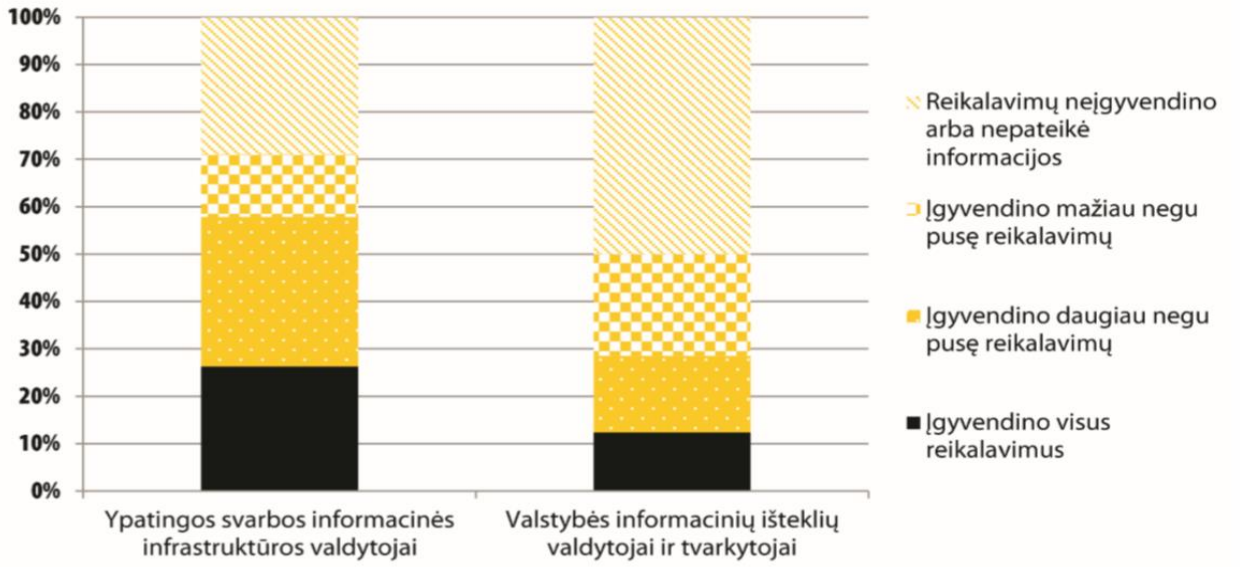
Apie organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimo būklę 2016 - 2017 metais Kibernetinio saugumo ir telekomunikacijų tarnyba prie Krašto apsaugos ministerijos pateikė išvadas nacionalinio kibernetinio saugumo būklės ataskaitose, 2016 metų Pav. 3 buvo konstatuota kad: „organizacijų 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., iš 2017 metų Pav. 4 ataskaitos matyti, kad esminio proveržio neįvyko. Tai parodo žemą kibernetinio saugumo brandą, 2016 - 2017 metų nacionalinio kibernetinio saugumo būklės ataskaitos.



Kibernetinio saugumo organizacinių reikalavimų įgyvendinimo Lietuvoje.

Šaltinis: 2016 metų nacionalinio kibernetinio saugumo būklės ataskaita

Pav. 3 Organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas Lietuvoje 2016 metais.



YSII ir VII valdytojų ir tvarkytojų organizacinių reikalavimų įgyvendinimas

Šaltinis: 2017 metų nacionalinio kibernetinio saugumo būklės ataskaita

Pav. 4 Organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas Lietuvoje 2017 metais.

Šioje srityje situacija turėtų gerėti kai Europos Sąjungos kibernetinio saugumo agentūra (ENISA), Europos kibernetinio saugumo kompetencijos centras pradės labiau plėsti savo bendradarbiavimą su Lietuvos institucijomis užtikrinančiomis kibernetinį saugumą. ENISA padeda ES šalims geriau pasirengti užketant kelią informacijos saugumo problemoms, jas nustatyti ir į jas reaguoti.

Iki 2018 metų viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų saugumu Lietuvoje daugiausiai rūpinosi Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT, kuris buvo įsteigtas Lietuvos Respublikos ryšių reguliavimo tarnyboje 2006 metais. Šis RRT padalinys atlieka elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimus, rengia rekomendacijas apie grėsmes. 2017 m. gruodžio 19 d. Seimas priėmė Kibernetinio saugumo įstatymo pataisas, kuriomis konsoliduota informacinių išteklių saugumo sritis, o RRT atliekamos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio funkcijos nuo 2018 m. sausio 1 d. perduotos naujai įsteigtam Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos. Atitinkamai buvo pakeistas ir Elektroninių ryšių įstatymas. Priimtų įstatymų pataisų pagrindu įgyvendinti pokyčiai padės užtikrinti bendrą ir koordinuotą informacinių išteklių saugumo politikos įgyvendinimą, aiškų ir nuoseklų informacinių išteklių saugumo reglamentavimą. Iki minėtų pasikeitimų įsigaliojimo informacinių išteklių saugumą užtikrino Kibernetinio saugumo ir telekomunikacijų tarnyba prie Krašto apsaugos ministerijos.

Galima teigti, kad 2018 metais pasiektas lūžio taškas, kada pradėta įgyvendinti ne tik teorinė, teisiškai reglamentuota kibernetinė gynyba, bet ir praktinis jos taikymas. Pilnai reglamentuota ir įteisinta Nacionalinio saugumo centro prie Krašto apsaugos ministerijos (NKSC) veikla. Ji tampa institucija, kuri yra atsakinga už vieningą kibernetinių incidentų valdymą, atlieka viešojo sektoriaus stebėseną ir kontroliuoja kibernetinio saugumo reikalavimų įgyvendinimą, vykdo ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir informacinių išteklių patikrą. Lietuvoje atsirado vieno langelio principu paremtas koordinuotas kibernetinio saugumo bei pajėgumų valdymas, kurį užtikrina tinklų ir informacijos saugumo departamento Saugumo incidentų tyrimo skyrius CERT-LT. Jis buvo suformuotas apjungiant Krašto apsaugos CERT ir Ryšių reguliavimo tarnybos CERT į vieną pagrindinį CERT-LT. Sukuriamas Kibernetinio saugumo informacinis tinklas, kurio paskirtis ir naudojimasis juo yra griežtai reglamentuotas:

1. Kibernetinio saugumo informacinio tinklo paskirtis – rinkti ir sisteminti informaciją apie galimus ir įvykusius kibernetinius incidentus, teikti rekomendacijas techniniams sprendimams ir kitomis priemonėms įgyvendinti.

2. Kibernetinio saugumo informaciniu tinklu gali naudotis tik tie kibernetinio saugumo subjektai, kurie atitinka Kibernetinio saugumo informacinio tinklo nuostatuose nurodytus reikalavimus.

3. Šiame tinkle skelbiama apie asmenis atsakingus už kibernetinio saugumo įgyvendinimą, incidentų valdymą,

Tačiau tai nėra elektroninių ryšių tinklas tiesiogine prasme, tai tiesiog elektroninis duomenų mainų portalas bei komunikavimo pramonė su Nacionaliniu kibernetinio saugumo centru. Pradedamos rengti kasmetinės kibernetinio saugumo pratybos, kurios skiria daug dėmesio organizacinių ir techninių

kibernetinio saugumo reikalavimų įgyvendinimo praktiniam taikymui. Pratybose dalyvauja valstybės informacinių išteklių valdytojai ir tvarkytojai, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjai, taip pat kibernetinius incidentus valdančios ir tiriančios institucijos

Nuo 2018 metų, įsigaliojus naujoms Administracinių nusižengimų kodekso pataisoms, Nacionalinis kibernetinio saugumo centras įgauna dar daugiau įgaliojimų, kuriais jiems suteikiama teisė duoti nurodymus ir skirti įspėjimus bei nuobaudas. Iki šiol nei Krašto apsaugos ministerija nei jai pavaldžios institucijos tokių įgaliojimų neturėjo. Jeigu tokias baudas pradėtų skirti Nacionalinis kibernetinio saugumo centras, galimai, lauktų ne vienas teisminis procesas.

2017 m. gegužės 31 d. Lietuvos Respublikos vyriausybės nutarimu Nr. 406 VĮ „Infostruktūra“ prie Lietuvos respublikos susisiekimo ministerijos valdanti „SAUGŲ VALSTYBĖS DUOMENŲ PERDAVIMO TINKLĄ“ (SVDPT) buvo perduota valdyti Lietuvos Respublikos Krašto apsaugos ministerijai. Krašto apsaugos ministerija nusprendė imtis veiksmų ir valstybės įmonė „Infostruktūra“ buvo pertvarkyta į biudžetinę įstaigą „Kertinis valstybės telekomunikacijų centras“, kuri savo veiklą pradėjo nuo 2019metų liepos 1 dienos. „Kertinis valstybės telekomunikacijų centras“ užtikrina jam priskirtos naujos ir gyvybiškai svarbios valstybės funkcijos vykdymą – rūpinasi naujojo Saugiojo valstybinio duomenų perdavimo tinklo (Saugusis tinklas) steigimu, kuris buvo sukurtas senojo Saugaus valstybinio duomenų perdavimo tinklo pagrindu. Saugusis tinklas yra nepriklausomas nuo viešųjų ryšių tinklų ir gali veikti krizės ar karo sąlygomis. Toks tinklas apjungia tik svarbiausias Lietuvos institucijas, kurios turi pavestas funkcijas ekstremalių situacijų, stichinių nelaimių, mobilizacijos, karo ir kitų kritinių atvejų metu. Vyriausybės patvirtintame saugiojo tinklo naudotojų sąraše įrašyta 451 institucija, tarp kurių – valdžios institucijos ir joms pavaldžios įstaigos, ligoninės, savivaldybių administracijos ir kitos. 2019 m. gegužės 2 d. Lietuvos Respublikos Vyriausybė patvirtino saugiojo tinklo naudotojų sąrašą, kuris nustatė, kad visi esantys tame sąraše privalo naudotis saugiuoju tinklu. Tuo patvirtinama, kad Lietuva pradėjo viešojo sektoriaus kolektyvinės kibernetinės gynybos įgyvendinimą. 2019 m. liepos 2 d. Nr. V-583 Lietuvos Respublikos Krašto apsaugos ministro įsakymu Saugiajam tinklui pradėti taikyti griežti specialieji organizaciniai ir techniniai reikalavimai bei paslaugos, kurias teikia Saugusis tinklas. Pagrandinės paslaugos, kurios yra teikiamos Saugiuoju tinklu sąraše esančioms institucijoms neatlygintinai:

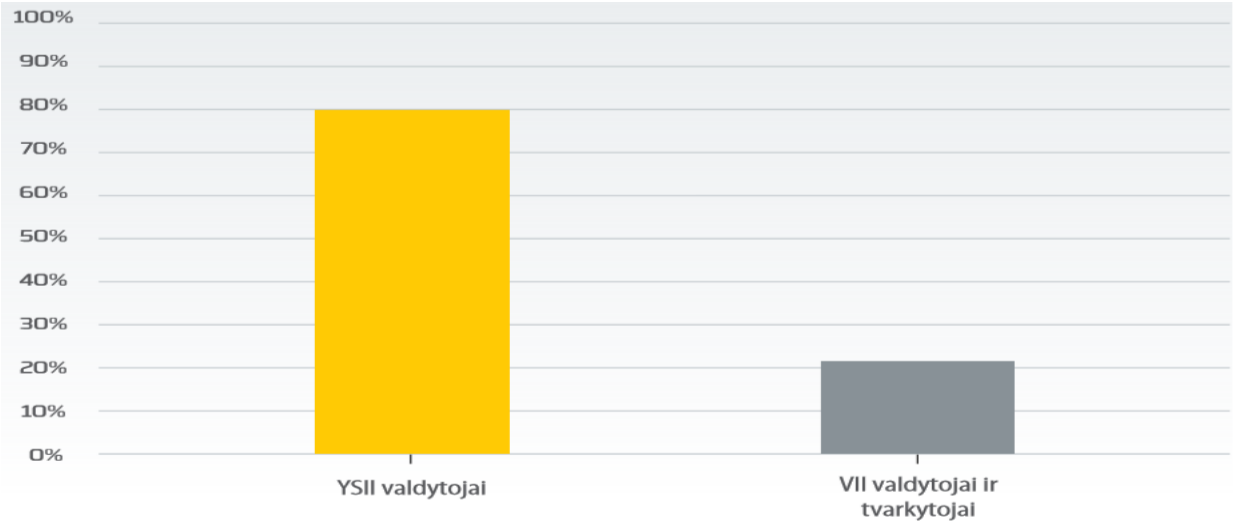
1. Elektroninių ryšių paslaugos;
2. Kolektyvinė apsauga kibernetinio saugumo priemonėmis;
3. Sąveika su Europos Sąjungos ir jos valstybių narių institucijomis.

Pažymėtina tai, kad paslaugos Saugiojo tinklo naudotojams teikiamos neatlygintinai. Tai padeda efektyviai valdyti valstybės resursus, siekiant išlaikyti maksimalų kibernetinį saugumą tinkle bei

apsaugoti informacinius išteklius. Saugiojo tinklo naudotojai prisijungti prie tinklo gali tik atitikę griežtus kibernetinio saugumo reikalavimus, kurie yra numatyti kibernetinio saugumo įstatyme bei prisijungimo prie tinklo taisyklėse.

Dar vieną kibernetinio saugumo sprendimą konsoliduojant išteklius, centralizuotai teikti IT paslaugas bei steigiant valstybinius duomenų centrus, numatyta įgyvendinti vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu 2011 m. gruodžio 15 d. Nr. XI-1807. Šis įstatymas numato prievolę viešojo sektoriaus institucijoms. Viena iš pagrindinių naujovių ta, kad viešosios institucijos, įrašytos į Saugiojo tinklo naudotojų sąrašą, privalo visų jų valdomų serverių ir (arba) kitą registrų ir valstybės bei kitų informacinių sistemų įrangą ir duomenis laikyti valstybiniuose duomenų centruose. Toks sprendimas padeda užtikrinti, kad valstybės duomenys būtų saugomi uždarame tinkle. Tokiu būdu yra efektyviai bei centralizuotai valdomi duomenų centrų resursai bei užtikrinamas jų kibernetinis saugumas.

Iš aukščiau paminėtos informacijos būtų galima teigti, kad Lietuva padarė didelį žingsnį į priekį, stiprinant kibernetinį saugumą. Tačiau šiuo metu realybė yra kitokia. Pagrindiniai darbai padaryti, sukurta kolektyvinė apsauga, sukurtas saugusis tinklas, įkuriant valstybinius duomenų centrus vienoje vietoje būtų sutelkti ir valstybės informaciniai ištekliai. Tačiau 2019 metų Nacionalinio kibernetinio centro ataskaita atskleidžia kiek kitokį vaizdą Lietuvos kibernetinio saugumo padangėje. Nacionalinis kibernetinio saugumo centras, vykdydamas kibernetinio saugumo reikalavimų įgyvendinimo stebėseną nustatė, kad YSII valdytojų reikalavimų įgyvendinimas išaugo – 80 proc. YSII valdytojai 2019 m. buvo įgyvendinę kibernetinio saugumo reikalavimus (5 pav.). Deja VII valdytojams ir tvarkytojams ir toliau kyla keblumų su reikalavimų įgyvendinimu. Ši analizė dar kartą parodo viešojo sektoriaus senas problemas, tai yra labai žemą kibernetinės brandos lygį. Dokumentų apimtis yra ganėtinai didelė ir sudėtinga, ne kiekvienas net patyręs kibernetinio saugumo specialistas gali su jais susitvarkyti. Kita problema - per dažnas teisės aktų keitimas apsunkina jų parengimą pagal naujus reikalavimus. Šioje vietoje iniciatyvos turėtų imtis Nacionalinio Kibernetinio saugumo centras ir paruošti metodinę medžiagą dokumentų rengimui. Tokiu atveju dokumentų rengimu institucijose galėtų užsiimti ir žemesnę kvalifikaciją turintys specialistai. Dar viena ne mažiau svarbi problema organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinime yra ta, kad dokumentai yra labai gerai parengti ir suderinti su Nacionaliniu kibernetiniu centru, tačiau jie yra tik „popieriniai“, niekas netestuoja jų veiksmingumo. To priežastis yra labai paprasta. Išanalizavus skirtingų institucijų organizacinių ir techninių kibernetinio saugumo reikalavimų dokumentaciją, galima daryti išvadą, kad šitie reikalavimai yra labai didelės apimties ir dažnai nėra suderinami su jau veikiančiais vidiniais institucijos informacijos saugą įgyvendinančiais procesais. Be to daugelis institucijų neturi ne tik žmogiškųjų bet ir finansinių resursų. Stebint tokią situaciją galima teigti, kad Lietuvai dar prireiks nemažai laiko pereiti prie aukštesnio viešojo kibernetinio saugumo lygio.



Šaltinis: Nacionalinio kibernetinio saugumo būklės ataskaita 2019

Pav. 5 Kibernetinio saugumo aplinka Lietuvos viešajame sektoriuje 2019

Pagrindinis klausimas ir dilema vis dar aktuali kabant apie kibernetinį saugumą yra ta, kad nėra aišku ką ginti, kokia apimtimi, kokį gynybos būdą taikyti individualų ar kolektyvinį, kiek tam skirti lėšų. Analizuojant šių dienų kibernetines grėsmes ir jų padarinius, galima teigti, kad kaip ir krašto gynybai skiriami 2% nuo BVP taip ir kibernetinei gamybai būtų galima skirti tam tikrus procentus nuo BVP. Tačiau finansavimas turėtų būti subalansuotas vertinant rizikas. Absoliutus kibernetinis saugumas neegzistuoja, viskas priklauso nuo finansavimo, skiriamo kibernetiniams nusikaltimams vykdyti, ir kaip apsiginti kai nusikaltimai vykdomi valstybiniu lygmeniu.

Iš pasirinkimo, ką valstybė turėtų ginti ir kiek tam skirti lėšų galima būtų paminėti keletą punktų:

1. Valstybės informacinius išteklius.
2. Kritinę infostruktūrą.
3. Valstybines institucijas.
4. Nacionaliniam saugumui svarbias įmones.

Šį apsisprendimą padaryti būtina, kadangi pagal dabartinį teisinį reguliavimą visi, kas nepatenka į Saugiojo tinklo sąrašą palikti gintis patys: darželiai, mokyklos, bibliotekos, vaikų globos namai ir kita.

Analizuojant kitų šalių pasirinkimus vieningos nuomones taip pat nėra. Lietuvos modelis labiausiai turi panašumų su Vokietija, kurios pirmas pasirinkimas - Ypatingos svarbos informacinės infrastruktūros objektų apsauga. (Luiijf, H. A. M et al., 2013).

2. VIEŠOJO SEKTORIAUS KOLEKTYVINĖ KIBERNETINĖ GYNYBA

Literatūroje, informacinės saugos teorijoje, dažnai sutinkamas informacijos užtikrinimo modelis, dar vadinamas saugumo trikampiu ar informacinio saugumo triada. JAV Nacionalinis standartų institutas apibrėžia informacinį saugumą kaip „*informacijos ir informacinių sistemų apsaugą nuo neautorizuotos prieigos, naudojimo, atskleidimo, sutrikdymo, modifikavimo ar sunaikinimo, siekiant užtikrinti konfidencialumą, vientisumą ir prieinamumą*“ (NIST) Pav. 6.



Šaltinis: IT Governance USA Blog

Pav. 6 Informacinio saugumo triada

Šioje temoje mes nagrinėsime praktinį viešojo sektoriaus konfidencialumo, vientisumo ir prieinamumo įgyvendinimą, kolektyvinės valstybės kibernetinės gynybos ypatumus bei efektyvumą. Viešai prieinamos informacijos šia tema beveik nėra, kadangi dauguma šalių tai laiko paslaptyje ir informacija nėra viešinama. Detalių mokslinių tyrimų bei straipsnių apie praktinio taikymo efektyvumą taip pat nėra. Svarbiausia yra atskirti sąvokas, kibernetinė gynyba ir kibernetinis saugumas. Kibernetinio saugumo, prevencijos bei stebėsenos temomis galima rasti daug straipsnių bei mokslinių tyrimų. Nagrinėdami šią temą mes naudosimės duomenimis gautais iš vienos iš Lietuvos valstybės kolektyvinės gynybos modelio dalies kuri yra įdiegta Saugiajame valstybės duomenų perdavimo tinkle (Saugusis tinklas (iki 2019-07-07 Saugus valstybinis duomenų perdavimo tinklas)) bei atliksime jų analizę.

Pagrindiniai bendri kolektyvinės valstybės kibernetinės gynybos uždaviniai:

A. Pirmasis uždavinys – kurti sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą. Šis uždavinys būtų įgyvendinamas tobulinant kibernetinio saugumo rizikos nustatymo, vertinimo ir prognozavimo būdus, formuojant kibernetinio saugumo atpažinties paveikslą ir rizikos žemėlapį, kuris atskleistų atskiriems sektoriams būdingas rizikas, kuriant regioninį kibernetinio saugumo centrą ir valstybės valdomą elektroninių ryšių tinklą su kompleksinėmis kibernetinio saugumo priemonėmis, jungiantį valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti paskirtas vykdyti valstybės ir savivaldybių institucijas, įstaigas ir įmones,

atliekant kibernetinio saugumo būsenos tyrimus, pažangos matavimus ar brandos vertinimus, užtikrinant visuomenės informavimą apie kibernetinio saugumo būklę, vykdant kitas kibernetinį saugumą ir prevencinę veiklą stiprinančias priemones ir veiksmus.

B. Antrasis uždavinys – didinti kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą, mažinant administracinę naštą kibernetinio saugumo subjektams. Šis uždavinys būtų įgyvendinamas tobulinant kibernetinio saugumo teisinį reguliavimą, parengiant standartizuotus, bet diferencijuojamus kibernetinio saugumo reikalavimus, atliekant gerosios praktikos, standartų, taikomų užtikrinant kibernetinį saugumą, analizę, skatinant kibernetinio saugumo subjektus jais vadovautis, nustatant nacionalinį integruotą krizių valdymo mechanizmą, užtikrinant visų lygmenų struktūrų sklandų bendradarbiavimą, atnaujinant kibernetinio saugumo rizikos vertinimo sistemą, įvertinant metodines galimybes vykdyti kibernetiniam saugumui reikalingų lėšų stebėseną ir kontrolę, nustatant jų skyrimo ir naudojimo pirmumą, vykdant kitas kibernetinio saugumo politikos formavimo ir įgyvendinimo plėtojimo priemones.

C. Trečiasis uždavinys – skatinti nacionalinių pratybų vykdymą ir dalyvavimą tarptautinėse pratybose. Šis uždavinys būtų įgyvendinamas periodiškai rengiant kompleksines nacionalines kibernetinio saugumo pratybas, dalyvaujant Europos Sąjungos, NATO ir kitų šalių organizuojamose pratybose, integruojant nacionalinių ir tarptautinių pratybų patirtį atliekant situacijų valdymo, incidentų vertinimo, informacijos komunikavimo ar kitus veiksmus.

D. Ketvirtasis uždavinys – plėtoti valstybės kibernetinės gynybos pajėgumus. Šis uždavinys būtų įgyvendinamas užtikrinant efektyvią Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, plėtojant kibernetinės gynybos pajėgumus ir teikiant pagalbą kitoms valstybės ir savivaldybių institucijoms ir įstaigoms.

Pirmą kartą Lietuvoje apie kibernetinę gynybą buvo pradėta kalbėti tik 2018 metais „Kibernetinės atakos nepaiso valstybių sienų, tačiau šalys iki šiol neturėjo sprendimo, kaip galėtų apjungti pajėgas kovai su grėsmėmis šioje dimensijoje. Lietuva pirmoji pasiūlė konkretų praktinį sprendimą, kaip sustiprinti kolektyvinę kibernetinę gynybą, ir kovoti su grėsmėmis naujoje dimensijoje“(sako krašto apsaugos ministras Raimundas Karoblis 2018).

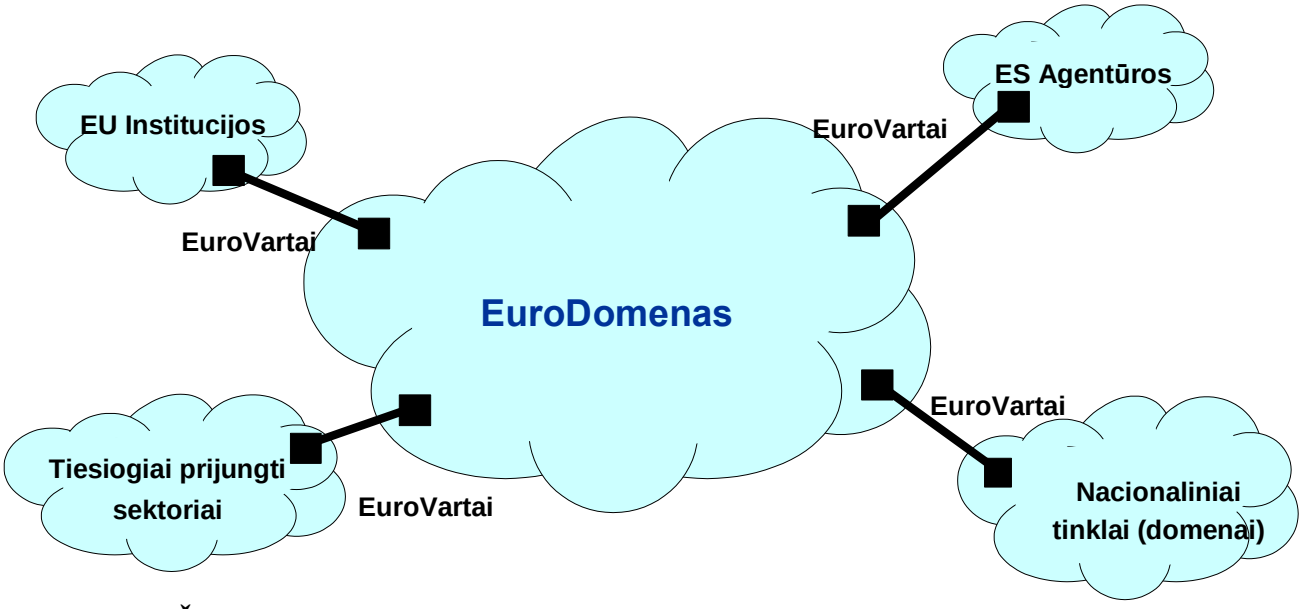
Siekdama pakelti kibernetinio saugumo būklės lygį Lietuvoje, Krašto apsaugos ministerija 2018 m. antroje pusėje parengė Valstybės informacinių išteklių valdymo įstatymo pakeitimą ir pasiūlė nustatyti pareigą valstybės ir savivaldybių institucijoms ir įstaigoms, vykdančioms valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti, naudoti Saugųjį tinklą. Saugusis tinklas būtų atskirtas nuo viešųjų ryšių tinklų ir galėtų veikti krizės ar karo sąlygomis. Minėtą įstatymą Lietuvos Respublikos Seimas priėmė 2018 m. gruodžio 20 d. Šio įstatymo įgyvendinimas sudarys galimybę ne tik užtikrinti greitesnį ir efektyvesnį reagavimą į kibernetinius incidentus, bet būtų taupomi kibernetiniam saugumui skiriami ištekliai, būtų centralizuojamas kibernetinės saugos užtikrinimas ir sudarytos sąlygos efektyviau taikyti kolektyvinės gynybos priemones.

Lietuvoje kaip ir visoje Europos sąjungoje galioja bendras teisinis reguliavimas, kuris numato bendrus kibernetinio saugumo aspektus bei reikalavimus kibernetinei gynybai (EP 2017 09 13). Tačiau niekur nėra kalbama apie bendrą gynybos modelį, o tiesiog yra priimami nacionaliniai teisės aktai, kurie reglamentuoja kokius kibernetinio saugumo reikalavimus turi užtikrinti kritine infostruktūra pripažintos ar ypatingos svarbos informacinius išteklius valdančios institucijos. Bendru kolektyvinės kibernetinės gynybos modelio pavyzdžiu galima būtų laikyti apsikeitimo tarp Europos šalių narių kai kurių registrų informaciją. Tačiau tai apima tik labai mažą informacijos kiekį. Visose Europos Sąjungos šalyse yra įsteigti ir veikia viešojo administravimo institucijų telematiniai tinklai skirti viešajam administravimui. Šie tinklai skirti elektroninės valdžios funkcionavimui užtikrinti. Tinklai sujungti su Europos Sąjungos IDABC programos sukurtu Europos Sąjungos administracijų telematiniu tinklu TESTA.

Europos Sąjungos šalyse paplitusi geroji praktika interneto paslaugas viešojo administravimo institucijoms teikti centralizuotai, o ne kiekvienai atskirai.

Ne mažiau kaip 15 Europos Sąjungos šalių viešojo administravimo institucijų interneto paslaugas gauna centralizuotai per nacionalinius viešojo administravimo institucijų telematinius tinklus. Šių tinklų pagrindiniai uždaviniai, kurie yra taikomi kibernetiniam saugumui užtikrinti, tai prieinamumas, vientisumas ir konfidencialumas. Tokius tinklus turi tokios šalys kaip: Airija, Estija, Čekija, Jungtinė karalystė, Kipras, Kroatija, Lenkija, Malta, Norvegija, Olandija, Portugalija, Slovakija, Slovėnija, Suomija, Vengrija. Šaltinis: (ePractice - Joinup)

Lietuvoje nuo 2004 metų pradėjo veikti Saugus valstybinis duomenų perdavimo tinklas sujungtas su Europos administracijų duomenų perdavimo tinklu TESTA Pav.7 (angl. Trans-European Telematics Networks for Administrations) ir Lietuvos valdžios institucijos pradėjo keistis duomenimis su ES institucijomis. TESTA tinklo veikla buvo paremta kolektyvinės kibernetinės gynybos pagrindu. Siekiant naudotis TESTA tinklu Saugus valstybinis duomenų perdavimo tinklas privalėjo atitikti griežčiausius kibernetinio saugumo reikalavimus.



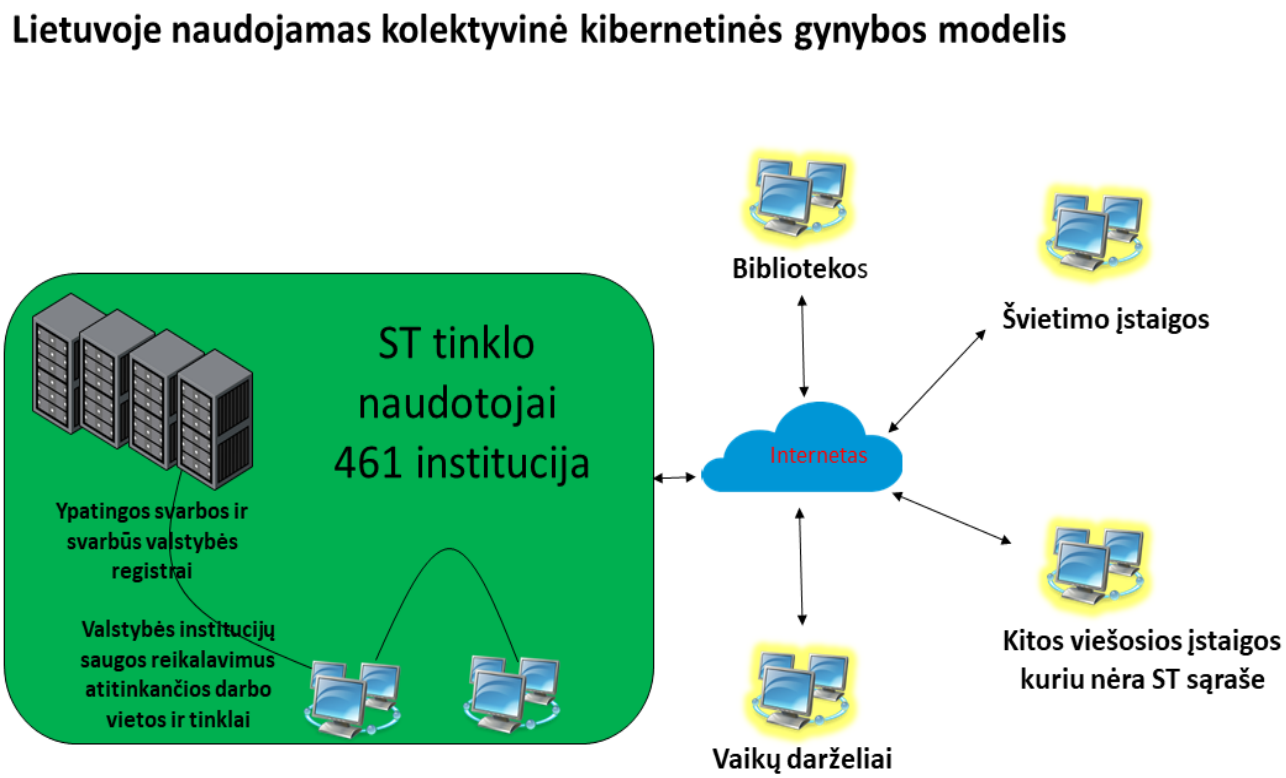
Šaltinis: Kertinis valstybės telekomunikacijų centras

Pav.7 EU Testa-NG tinklo loginė schema

Šiuo metu Lietuvoje kolektyvinė kibernetinė gynyba kol kas lieka įgyvendinta tik dalinai, kadangi kolektyvinę apsaugą gali naudotis tik svarbiausios Lietuvos institucijos, kurios turi pavestas funkcijas ekstremalių situacijų, stichinių nelaimių, mobilizacijos, karo ir kitų kritinių atvejų metu. Vyriausybės patvirtintame saugiojo tinklo naudotojų sąraše įrašyta 451 institucija, kuri privalo juo naudotis. Šis sąrašas yra nuolat atnaujinamas. Daugybė institucijų valdo svarbius ir labai svarbius valstybei duomenis, tačiau jų kibernetinė apsauga neatitinka šių dienų reikalavimų. Taigi, šiuo metu ne visos šios institucijos naudojasi Saugiuoju tinklu, joms yra skirtas pereinamasis laikotarpis iki 2022 metų liepos pirmos dienos. Šiuo metu jos yra pasirinkę tiekėjus savo nuožiūra, tai reiškia, kad vienos kitoms svarbius duomenis siunčia viešu interneto ryšiu, sutrikdyti tokių institucijų duomenų perdavimą arba suorganizuoti kibernetinę ataką yra labai lengva. Teisės aktuose nėra numatyta galimybė institucijoms, nesančioms institucijoms tinklo naudotojų sąraše naudotis Saugiuoju tinklu. Duomenys, neatsižvelgiant į jų svarbą, tarp valstybės įstaigų ir institucijų perduodami per skirtingus tinklus, naudojantis skirtingų operatorių paslaugomis. Tokia situacija iki 2022 metų sudarys nemažai problemų kibernetinio saugumo valdyme bei užtikrinime. Efektyviausia būtų kuo skubiau sujungti šias institucijas į vieną saugų ir uždarą tinklą, kuris maksimaliai apsaugotų nuo kibernetinių pavojų, leistų be trikdžių dirbti net ir patyrus išpuolius, atremti vis didėjantį kibernetinio saugumo incidentų skaičių, bei siekti efektyviai užkirsti kelią kibernetinėms atakoms. Saugusis tinklas - tai viena iš kolektyvinės valstybės kibernetinės gynybos sudėtinių dalių. Ją galima būtų įvardyti taip - pagrindinė viešojo sektoriaus kibernetinį saugumą užtikrinanti sistema kuri skirta:

1. Efektyviai valdyti viešajam sektoriui skiriamus resursus kibernetiniam saugumu užtikrinti Lietuvoje.
2. Efektyviai suvaldyti kibernetines atakas.
3. Institucijoms saugiai ir efektyviai keistis informacija su Europos sąjungos institucijomis ir valstybių narių administracijomis.
4. Stiprinti svarbiausių valstybės informacinių sistemų saugą.
5. Institucijoms saugiai keistis informacija tarpusavyje ir tarp institucijų struktūrinių padalinių.
6. Saugiam duomenų perdavimui tarp žinybinių ryšio tinklų.
7. Esant kritinei situacijai viešųjų ryšių tinkluose užtikrinti viešojo sektorius veiklą.
8. Spręsti įvairias kompiuterinio saugumo problemas, kylančias Saugiajame tinkle bei Lietuvos valstybės viešojo administravimo institucijų informacinėse sistemose.

Analizuojant Lietuvoje naudojamo kolektyvinės kibernetinės gynybos modelio vizualizaciją galima teigti, kad Lietuva naudoja hibridinę kolektyvinę sistemą. Centralizuotai gina tik apie 500 viešojo sektorius institucijų. Kitos viešojo sektoriaus institucijos kibernetiniu saugumu paliktos pasirūpinti pačios Pav. 8, nors jos ir naudojasi valstybės informaciniais ištekliais.



Šaltinis: Kertinis valstybės telekomunikacijų centras

Pav. 8 Kibernetinio saugumo aplinka Lietuvos viešajame sektoriuje

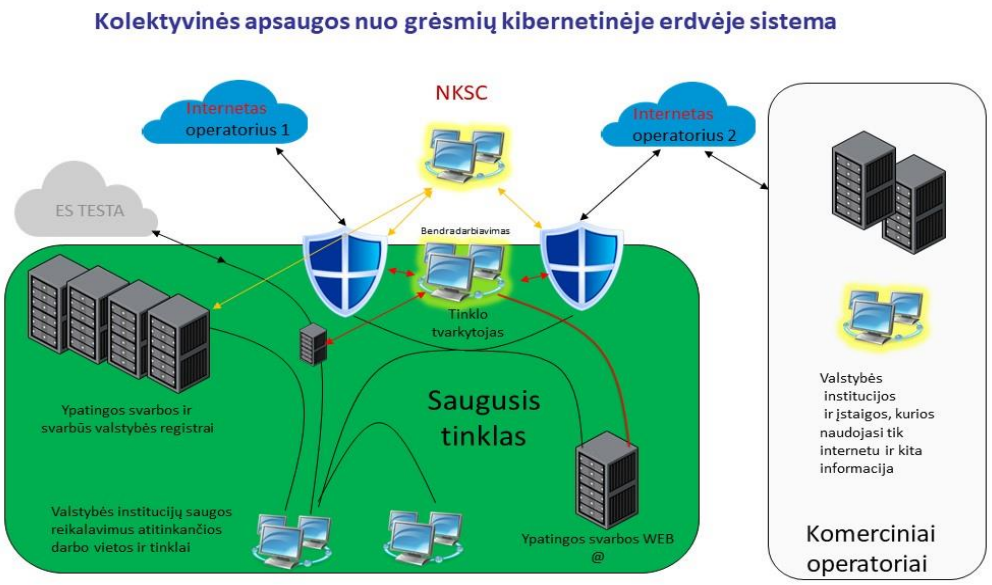
2.1 Kolektyvinės kibernetinės gynybos modelis

Šiame skyriuje detalizuosime kolektyvinės kibernetinės gynybos modelį, kuris yra įdiegtas Saugojo valstybinio duomenų perdavimo tinkle, detalizuosime jo architektūrą bei jo sudedamąsias dalis jų valdymą bei saugumo užtikrinimą ir stebėseną. Tai padės mums susidaryti bendrą vaizdą iš ko susideda kibernetinės kolektyvinės gynybos modelis.

Pagrindinės modelio sudedamosios dalys bei reikalavimai:

1. Uždaras elektroninių ryšių tinklas.
2. Privalo turėti mažiausiai du sujungimus su viešaisiais elektroninių ryšių tinklais (INTERNETU).
3. Visos saugomos institucijos privalo būti saugiojo tinklo viduje.
4. Institucijos negali turėti elektroninių ryšių su kitai tiekėjais.
5. Jos privalo būti įgyvendinę organizacinius ir techninius kibernetinio saugumo reikalavimus.
6. Institucijos informaciniai ištekliai privalo būti tinklo viduje.
7. Institucijų svetainės privalo būti tinklo viduje.
8. Valstybiniai duomenų centrai privalo būti tinklo viduje.
9. Kompleksinė apsauga nuo DDos atakų.
10. Kenksmingo interneto turinio ir aplikacijų blokavimas(WAF).
11. Gambling ir nelegalių interneto svetainių blokavimas DNS valdymo priemonėmis.
12. Įvykių stebėsenos sistema.
13. Uždaras ryšys su Europos sąjungos registrais.
14. ST- CERT
15. Institucijų elektroninis paštas privalo būti tinklo viduje.
16. IP telefonija privalo būti tinklo viduje.
17. Tinklas turi būti valdomas specialiaisiais saugumo reikalavimais.

Kaip matyti iš modelio sudedamųjų dalių, tokio modelio įgyvendinimas reikalauja nemažai pastangų, resursų bei žmogiškųjų išteklių. Be to, visi tinklo naudotojai privalo pasiekti gana aukštą kibernetinio saugumo brandą. Iš struktūrinės schemos Pav. 9 matyti, kad dauguma saugumo priemonių bei tinklų privalo būti dubliuoti, o tai gerokai didina veiklos kaštus, tačiau tokie sprendimai ženkliai didina tinklo patikimumą.



Šaltinis: Kertinis valstybės telekomunikacijų centras

Pav. 9 Saugojo tinklo kolektyvinės kibernetinės gynybos modelis

Išanalizavus tokio modelio struktūrą bei veikimo principus, galima teigti, kad šis modelis vadybos prasme turi nemažai teigiamų rezultatų:

1. Leidžia sutaupyti didelę dalį žmogiškųjų resursų (IT darbuotojų).
2. Leidžia sutelkti bei išlaikyti aukštą kibernetinio saugumo specialistų lygį.
3. Gali centralizuotai vykdyti įrangos pirkimus, o tai mažina kaštus.
4. Leidžia efektyviai užkirsti kibernetines atakas.
5. Visi saugiojo tinklo naudotojai net ir praradę ryšį su viešaisiais tinklais galės ir toliau atlikti savo funkcijas.

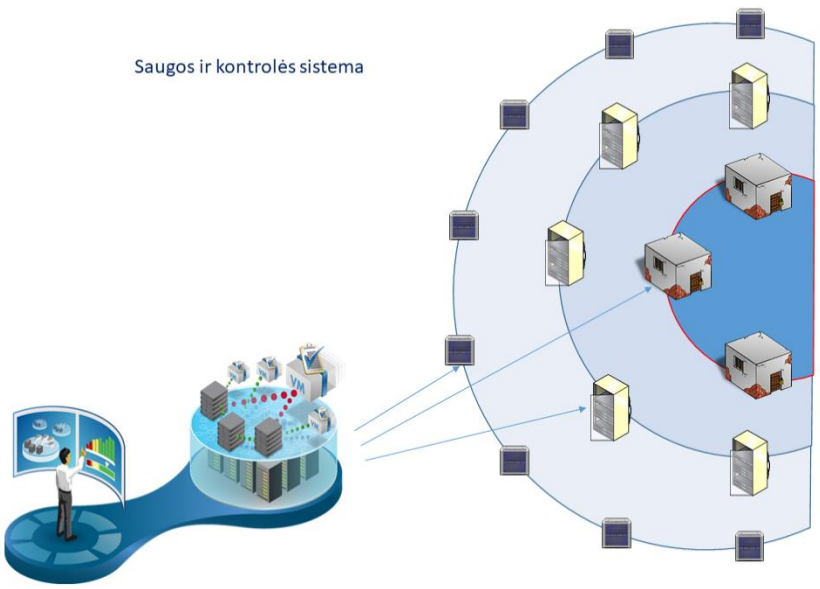
Toliau detalizuosime kokiomis priemonėmis Saugiajame tinkle mažinamos kibernetinių grėsmių rizikos:

1. Saugiojo tinklo naudotojams ir jų struktūriniams padaliniams - Duomenų perdavimas, teikiamas saugaus valstybinio duomenų perdavimo tinklo Saugiojo tinklo dalyje, uždaroje nuo bendrojo naudojimo tinklų (interneto). Prieš paslaugos teikimą atliekama paslaugų gavėjo vietiniame tinkle esančios kompiuterinės ir tinklo įrangos pažeidžiamumo patikra, programinės įrangos skenavimas bei pateikiama ataskaita ir rekomendacijos dėl identifikuotų pažeidimų šalinimo. Siekiant užtikrinti prie Saugiojo tinklo prijungiamų institucijų tinklų saugumą, bei bendrą Saugiojo tinklo saugumą, vieną kartą per metus atliekama pakartotinė pažeidžiamumo patikra.

2. Paslaugos teikimui reikalinga galinė įranga, kuri parenkama atsižvelgiant į paslaugų gavėjo greitaveikos ir funkcionalumo poreikius. Kiekvienam paslaugų gavėjui sukuriamas šifruotas duomenų perdavimo kanalas. Perduodamos informacijos teikėjai ir gavėjai yra apjungiami į vieną Saugiojo tinklo vartotojų grupę.
3. Kolektyvinė apsauga kibernetinio saugumo priemonėmis yra paslauga, privaloma institucijoms, norinčioms naudotis Saugiojo tinklo paslaugomis, ir nustatytos spartos prieigos prie viešųjų ryšių tinklų paslaugomis. Paslaugos teikimui naudojamos įdiegtos centralizuotos kibernetinės saugumo sistemos, kurios kompleksiškai saugo paslaugų gavėjo vietinio tinklo infrastruktūrą ir turimas informacinių technologijų sistemas nuo kibernetinių grėsmių. Kolektyvinė apsauga kibernetinio saugumo priemonėmis užtikrina bendrą Saugiojo tinklo saugumą.
4. Sąveika su Europos Sąjungos ir jos valstybių narių institucijų valdomais informaciniais ištekliais - TESTA NG duomenų perdavimo paslauga užtikrina Saugiojo tinklo paslaugų gavėjų šifruotą ir saugų prisijungimą prie Europos Sąjungos ISA programos projektų ir informacinių sistemų. Lietuvos institucijos per TESTA tinklą gali prisijungti prie daugelio Europos viešojo administravimo institucijų sąveikumo sprendimų ISA programos projektų. TESTA NG duomenų perdavimo paslauga teikiama Saugiojo tinklo dalyje, atskiroje nuo bendrojo naudojimo tinklų (interneto). Paslaugos teikimui reikalinga galinė įranga, šifruotas duomenų perdavimo kanalas į informacinės sistemos duomenų perdavimui saugumui keliamus reikalavimus atitinkančią Saugiojo tinklo dalį. Perduodamos informacijos teikėjai ir gavėjai yra apjungiami į vieną Saugiojo tinklo vartotojų grupę, kuri tvarkoma vartotojų grupės savininko (tuo pačiu dažniausiai ir perduodamos informacijos tvarkytojo) nustatyta tvarka.
5. Nustatytos spartos prieiga prie viešųjų ryšių tinklų. Ši paslauga teikiama Saugiojo tinklo dalyje, kuri yra sujungta su bendrojo naudojimo tinklais (Internetu) ir atskirta nuo uždarų Saugiojo tinklo dalių. Šia paslauga gali naudotis institucijos, savo veiklai naudojančios saugius regioninius (Lietuvos Respublikos aprėpties) duomenų perdavimo tinklus ir kurioms reikalinga prieiga prie viešųjų resursų. Paslaugos teikimui institucijos padaliniuose turi būti įdiegiama institucijos ryšio paslaugų poreikius ir pralaidumo reikalavimus atitinkanti įranga su ugniasienės funkcijomis.
6. Valstybės valdomų elektroninių ryšių tinklų, kurie naudojami vykdant valstybines mobilizacines užduotis, dalių sujungimas - Ryšio linijų teikimas Lietuvos viešojo saugumo ir pagalbos tarnybų skaitmeninio mobiliojo radijo ryšio bazinėms stotims. Esant poreikiui ši paslauga gali būti teikiama kitoms institucijoms.

7. Saugiojo tinklo paslaugų saugumą ir prevenciją užtikrina akredituota KVTC-CERT tinklų ir informacijos saugumo incidentų tyrimų grupė (angl. Computer Emergency Response Team), kurios paskirtis – spręsti įvairias kompiuterinio saugumo problemas, kylančias Saugiajame tinkle ir Lietuvos valstybės viešojo administravimo institucijų informacinėse sistemose. KVTC-CERT informuoja ir konsultuoja klientus apie įvairiausią programinį ir techninį sistemų pažeidžiamumą bei analizuoja informacijos saugumo užtikrinimo tendencijas.
8. Saugiojo tinklo valdyme yra įdiegtos procesų valdymo priemonės, užtikrinančios rezultatyvų įstaigos vadybos sistemos veikimą bei nuolatinį veiklos kokybės gerinimą. Tinklo saugą užtikrina daugiaplanė įstaigos saugos strategija, numatanti ir palaikanti prevencijos, tiesioginio suvaržymo, aptikimo, reagavimo, veiklos atkūrimo priemones ir procesus. Tai įrodo įstaigoje įdiegta kokybės vadybos sistema, sertifikuota atitikties sertifikatu, patvirtinančiu, kad įstaigos kokybės vadybos sistema atitinka LST EN ISO 9001:2015 standarto reikalavimus. Įstaigai įteiktas ir integruotos informacijos saugumo vadybos sistemos atitikties sertifikatas, patvirtinantis, kad informacijos saugumo vadybos sistema atitinka LST ISO/IEC 27001:2017 standarto reikalavimus.
9.

Fizinis tinklo įrangos saugumas yra neatsiejama kibernetinio saugumo dalis. Saugiojo tinklo fizinės saugos ir kontrolės sistemos Pav. 9 tikslas yra užtikrinti Saugiojo tinklo įrangos ir kitų komponentų fizinę saugą, kontrolę, stebėjimą ir valdymą, užtikrinant Saugiojo tinklo vientisumą, prieinamumą ir konfidencialumą.



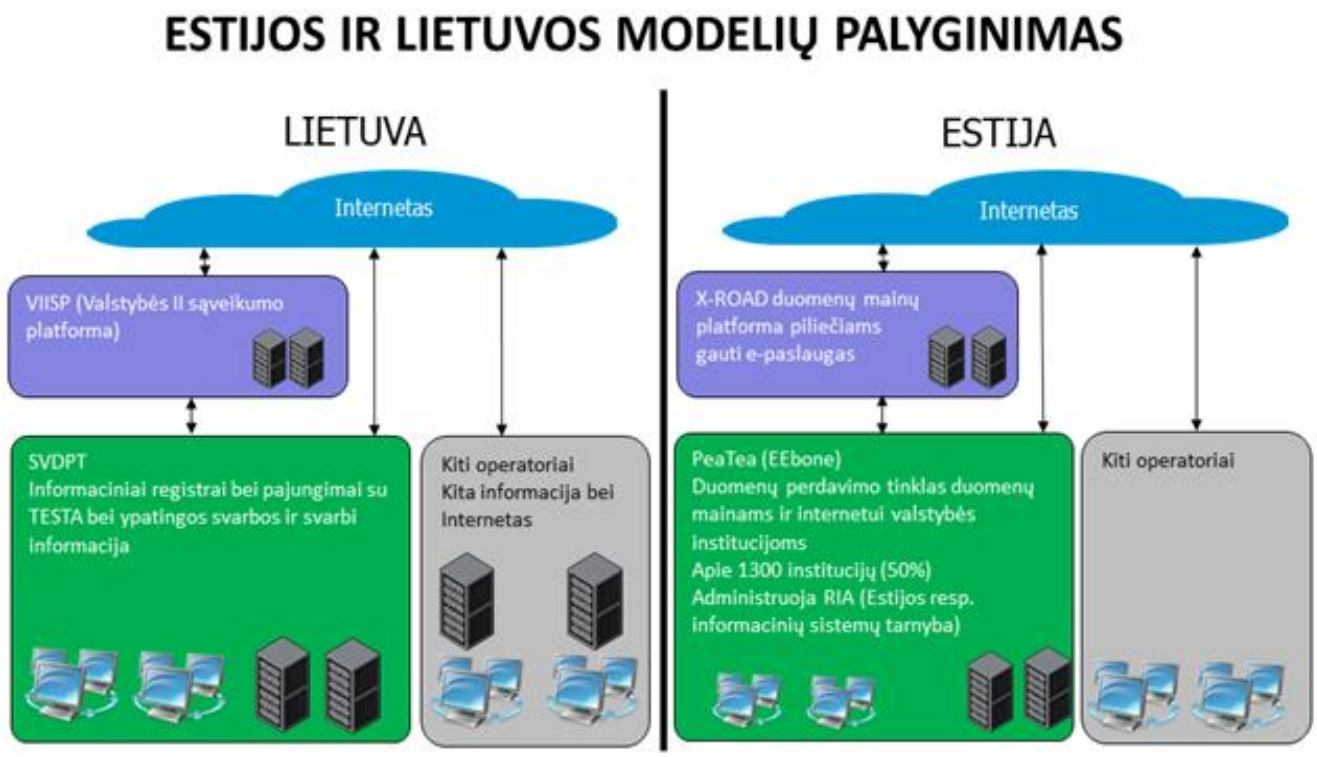
Šaltinis: Kertinis valstybės telekomunikacijų centras

Pav. 10 Saugiojo tinklo fizinės saugos ir kontrolės sistema

Šio tyrimo metu bus naudojama tinklo, kuris buvo sukurtas vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 2 straipsnio 13 dalimi. Saugus valstybinis duomenų perdavimo tinklas (toliau – SVDPT nuo 2019-07-01 Saugusis tinklas) – elektroninių ryšių tinklas, atskirtas ir apsaugotas nuo viešųjų elektroninių ryšių tinklų (interneto) bei neteikiamas viešai, skirtas visoms Lietuvos Respublikos valstybės ir savivaldybių institucijoms, įstaigoms ir įmonėms bei kitiems juridiniams asmenims, kuriuo jie gali saugiai teikti duomenis, bendradarbiauti su Europos Sąjungos institucijomis, užtikrinant duomenų mainų dalyvių tapatybės nustatymą, perduodamų duomenų konfidencialumą, vientisumą ir prieinamumą.

SVDPT buvo sukurtas įgyvendinant Europos Parlamento ir Tarybos sprendimų Nr. 1719/1999/EB ir Nr. 1720/1999/EB bei Nr. 2004/387/EB nuostatas, kurios, be kita ko, nurodo „funkcionalių, tarpusavyje suderintų“ valstybių narių tinklų, skirtų nacionalinio ir regioninio lygmens saugiam ir efektyviam duomenų keitimuisi.

SVDPT analogas yra PeeTea (EEbone) Pav. 11 Tinklas, kuris valdomas Estijos Respublikos informacinių sistemų tarnybos. Jame pajungta apie 50% valstybės institucijų (apie 1300), taip pat ir privačios bendrovės, vykdančios valstybės deleguotas funkcijas. Per šį tinklą centralizuotai įstaigoms teikiamas ir internetas. Be pagrindinio tinklo ši organizacija administruoja valstybinių institucijų vietinius tinklus, konsultuoja operatorius. Šis tinklas sukurtas 1993 m. pasienio apsaugos, muitinės valdybos bei policijos valdybos ASONet (Administration Services Only Network) pagrindu.



Šaltinis: Kertinis valstybės telekomunikacijų centras

Pav. 11 Lietuvos ir Estijos kolektyvinės kibernetinės apsaugos modelis

Visi instituciniai, tarpinstituciniai prisijungimai, kuriems reikalinga prieiga prie Europos sąjungos institucijų, prie ypatingos svarbos ir/arba svarbių valstybės informacinių išteklių, turi būti vykdomi per vienalytį apsaugotą tinklą – SVDPT. Prisijungimai prie šių valstybės informacinių sistemų negalimi per viešuosius tinklus. Tokiais atvejais prieiga prie viešųjų tinklų (interneto) turi būti centralizuota per kibernetinės saugos platformą.

Esant kritinei situacijai institucijos, prisijungusios prie viešųjų tinklų ne per kibernetinės saugos platformą, būtų atskirtos nuo Europos sąjungos TESTA tinklo, kuris užtikrina duomenų apsikeitimą tarp Lietuvos institucijų ir Europos Sąjungos administracijų valstybės institucijų ir įstaigų bei valstybės informacinių išteklių. Atkreiptinas dėmesys, kad toks SVDPT modelis yra įgyvendintas daugelyje ES šalių narių, tokių kaip:

- Vokietija
- Jungtinė Karalystė
- Olandija
- Estija ir kt.

2.2 Kibernetinių atakų ir kolektyvinės gynybos resursų bei kokybės valdymo tyrimo metodika

Kaip parodė aukščiau pateikta gerųjų praktikų teisės aktų analizė, saugumo priemonės vidinėms kibernetinio saugumo grėsmėms suvaldyti yra panašios, tad galima suformuoti jų standartinį kompleksą.

Tai, kaip konkrečios kibernetinio saugumo priemonės būtų įdiegtos organizacijoje ir ar iš tikrųjų būtų veiksmingos, o pasirinktas saugumo priemonių praktinis taikymas būtų efektyvus ir ar būtų veiksmingai kontroliuojamas įdiegtų saugumo priemonių įgyvendinimas ir galiausiai koks būtų organizacijos parinktų saugumo priemonių resursų pakankamumas.

Kolektyvinės kibernetinės gynybos sistemos efektyvumą vertinsime analizuodami konfidencialumo, vientisumo ir prieinamumo užtikrinimą. Efektyvumo nustatymui bus vertinami pagrindinių rodiklių tikslai. Pagrindiniai rodikliai: prieinamumas, incidentų ir gedimų kiekis, gedimų ir incidentų pašalintų kontroliniu laiku, atsparumas kibernetinėms atakom, pažeidžiamumų užkardymas.

Tyrimo problema – organizacijos pasirinktų vidinių kibernetinio saugumo grėsmių, konfidencialumo, prieinamumo, nepaneigiamumo užtikrinimas, valdymo priemonių efektyvumas.

Tyrimo tikslas – Efektyvus viešojo sektoriaus kibernetinio saugumo valdymas. Kolektyvinės kibernetinės apsaugos modelio efektyvumas.

Tyrimo uždaviniai:

1. Išanalizuoti kolektyvinio kibernetinio saugumo priemonių taikymą tinklo prieinamumo kontekste.

2. Identifikuoti vidinių kolektyvinio kibernetinio saugumo grėsmių valdymo priemonių taikymo trūkumus ir pateikti siūlymus priemonių tobulinimui.

Tyrimo metodika ir jos pasirinkimo pagrindimas

Atvejo analizė kaip pagrindinis tyrimo metodas pasirinktas siekiant nuosekliai išnagrinėti konkrečios organizacijos kelią nuo jos elgesio formuluojant kolektyvines kibernetinio saugumo priemones, iki įvykusio vidinio saugumo incidento suvaldymo. Atvejo analizei duomenys ir informacija buvo renkami taikant kokybinius tyrimo metodus – organizacijos vidinių procesų analizės, lyginimo su gerosiomis praktikomis metodus, empirinius stebėjimo, dokumentų analizės metodus. Atvejo analizei atlikti pasirinkti kokybiniai informacijos rinkimo ir apdorojimo metodai. Ši strategija skirta tyrimo uždaviniams pasiekti, nes leis visapusiškai išanalizuoti vidinį kolektyvinio kibernetinio saugumo efektyvumą, kibernetinių grėsmių suvaldymą, padės plačiau pažvelgti į vidinių kibernetinio saugumo grėsmių valdymo priemonių diegimo ir įgyvendinimo problematiką.

Dokumentų analizės metodas buvo naudojamas analizuojant vidinio incidento tyrimo informaciją. Analizė atlikta išsamiai analizuojant incidento tyrimo rezultatus, proceso valdymo sistemų audito duomenų palyginimus.

Tyrimo eigą, taikant atvejo analizės metodą, galima sąlyginai išskirti į etapus:

-Tyrimo vieneto (organizacijos) pasirinkimas ir pagrindimas;

-Atvejo nustatymas (pasirinktos organizacijos vidinių kibernetinio saugumo grėsmių valdymo priemonių įgyvendinimo atvejis);

-Atvejo ribų nustatymas (analizuojamas atvejis nuo vidinių kibernetinio saugumo grėsmių valdymo priemonių pasirinkimo iki reagavimo į įvykusį saugumo incidentą, analizuotos vidinių kibernetinio saugumo grėsmių organizacinės valdymo priemonės);

-Duomenų rinkimas(duomenų apie įvykusių incidentą ir jo tyrimą rinkimas);

-Atvejo analizės rezultatų apibendrinimas, rekomendacijų pateikimas.

Tyrimo vienetas ir jo pasirinkimo pagrindimas

Tyrimui atlikti pasirinkta elektroninį ryšį bei kibernetinį saugumą užtikrinanti organizacija, teikianti viešajam sektoriui ryšio bei kibernetinio saugumo paslaugas. Tiriamos organizacijos darbuotojai dirba vienoje patalpoje, organizacija neturi nutolusių padalinių. Organizacijos struktūrą sudaro 4 tiesioginės veiklos padaliniai: tinklo technologijų padalinys, saugumo padalinys, bendrųjų reikalų padalinys ir klientų aptarnavimo padalinys.

Šios organizacijos pasirinkimą lėmė tai, jog tokio tipo organizacija yra vienintelė Lietuvoje užtikrinanti kolektyvinį viešojo sektoriaus kibernetinį saugumą, tačiau susiduria su iššūkiais, kuriuos privataus sektoriaus organizacijos gali spręsti lanksčiau ir operatyviau. Griežti finansavimo apribojimai

pagal veiklas, griežti etatų ir organizacijos struktūros reguliavimai, sunku pritraukti aukštos kvalifikacijos kibernetinio saugumo specialistus, nekonkurencinga darbo užmokesčio sistema.

Tikimasi, kad tyrimo metu gauti rezultatai būtų naudingi nustatant kolektyvinės kibernetinės apsaugos viešojo sektoriaus efektyvumą bei patikimumą. Tyrimo rezultatai taip pat gali būti naudingi kolektyvinio kibernetinio saugumo taikymo praplėtimui visam viešajam sektoriui. Metodinėse rekomendacijose turėtų būti atsižvelgta į papildomus iššūkius, su kuriais susiduria viešojo sektoriaus organizacijos, kurios netaiko kolektyvinės kibernetinė apsaugos.

2.3 Kibernetinių atakų ir kolektyvinės gynybos atsparumo bei kokybės valdymo analizė

Šioje dalyje analizuojama Saugaus valstybinio duomenų perdavimo tinklo saugomų valstybės informacinių išteklių bei tinklų atsparumas kibernetinėms atakoms, tinklo pajėgumų valdymas, duomenų konfidencialumo, prieinamumo, nepaneigiamumo užtikrinimas. Analizei atlikti naudojama Saugiojo valstybinio duomenų perdavimo tinklo stebėjimo sistemos duomenų bazės informacija už 2019 metus, pažeidžiamumų vertinimo analizės, tyrimo metu naudojami kokybiniai ir kiekybiniai metodai. Analizės rezultatai turi parodyti pagrindinių, Saugiojo tinklo, kuris atlieka kolektyvine kibernetinę viešojo sektoriaus ganybą, uždavinių įgyvendinimą.

2019 METŲ PAGRINDINIŲ RODIKLIŲ VYKDYMAS

Šio skaičiavimo tikslas - nustatyti ar yra užtikrinamas Saugiojo tinklo naudotojų apie 500 viešojo sektoriaus institucijų kolektyvinės kibernetinės gynybos pagrindiniais tikslais tinklo prieinamumas. 1 lentelėje nustatyta, kad visus 2019 metus tikslas yra visiškai įgyvendintas ir net viršytas. Iš gautų duomenų galima teigti, kad vidiniai procesai bei įdiegti standartai (LST ISO/IEC 20000, LST ISO/IEC 27001) leidžia pasiekti norimą rezultatą.

1 lentelė SVDPT tinklo prieinamumas

Sudaryta autoriaus pagal SVDPT duomenis

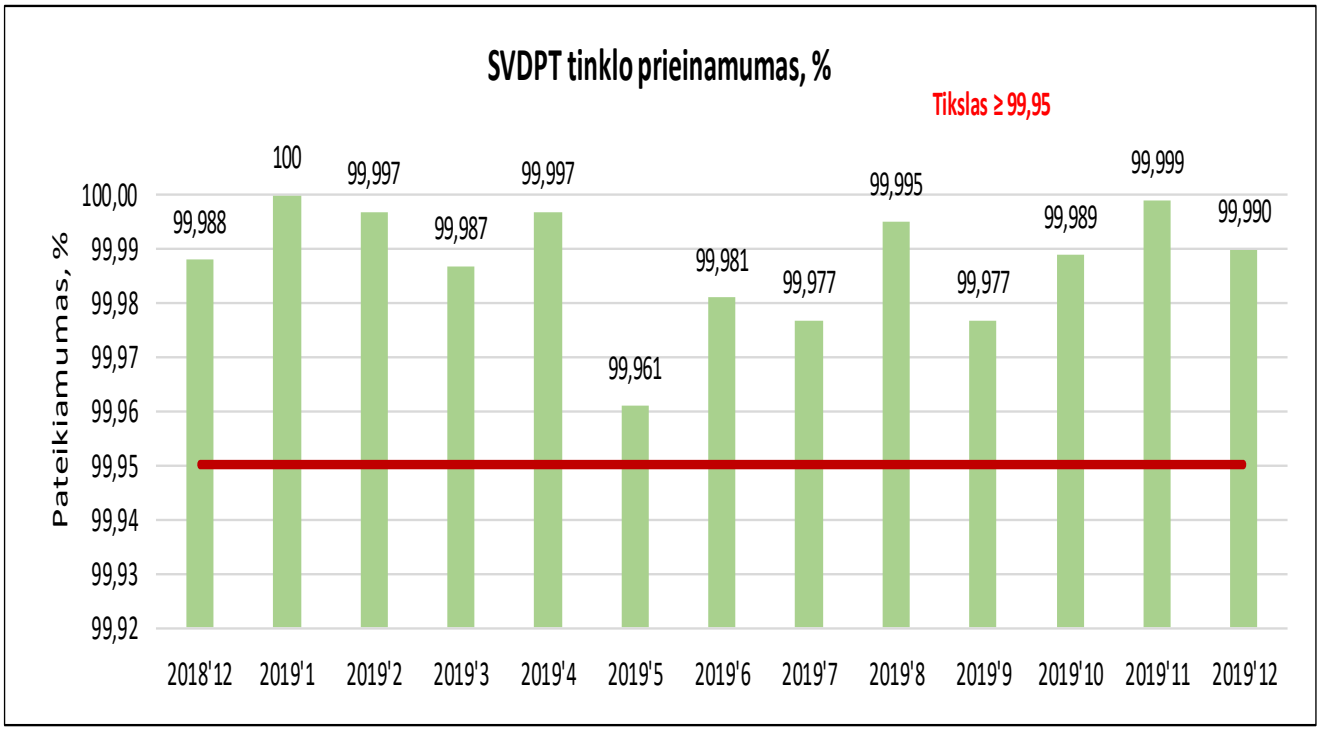
Ataskaitinis laikotarpis	Tikslas	2019'IQ	2019'IIQ	2019'IIIQ	2019'IVQ	2019
SVDPT tinklo prieinamumas, %	**99,95**	**99,995**	**99,980**	**99,983**	**99,993**	**99,988**
Kontroliniu laiku pašalintų gedimų, dalis, %	**92**	**90,58**	**86,27**	**87,25**	**79,33**	**85,48**

Santykinis SVDPT paslaugų gedimų skaičius 100 paslaugų* vid. per mėnesį (* - vartotojų kiekis pagal tinklo stebėjimo sistemą)	**3,5**	**2,34**	**2,52**	**3,21**	**3,40**	**2,86**

Vertinant 2 lentelės duomenis galima nustatyti laikotarpį, kurį išanalizavus pasirenkant pagal konkretų periodą bei įvykius ir priėmus tinkamus sprendimus būtų galima dar labiau gerinti tinklo prieinamumą.

2 lentelė SVDPT tinklo detalus prieinamumas

Sudaryta autoriaus pagal SVDPT duomenis



Pateikiame palyginimui kitų tinklų (3 lentelė) prieinamumo informaciją, kuria remiantis galima teigti, kad institucijoje naudojamas tinklo motelis yra efektyviai valdomas, o kolektyvinės kibernetinės apsaugos sprendimas yra efektyvus.

3 lentelė Kitų tinklų prieinamumas (proc.):

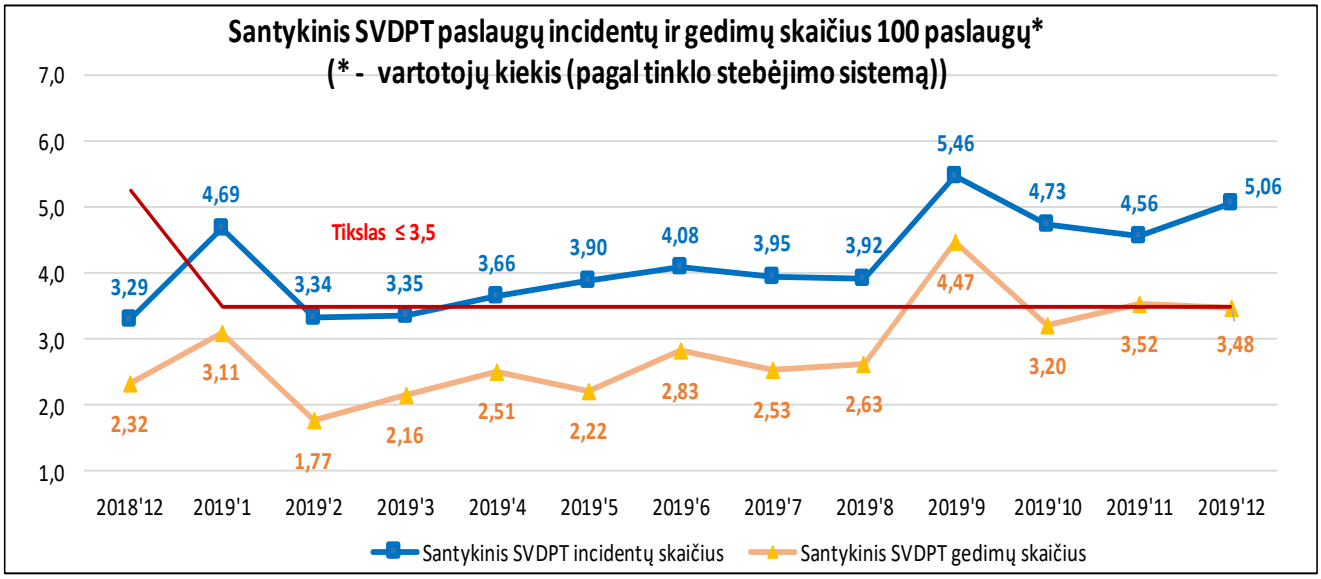
Sudaryta autoriaus pagal SVDPT duomenis

Tinklas	2019'4	2019'5	2019'6	2019'7	2019'8	2019'9	2019'10	2019'11	2019'12
ns.ripe.net (Europa)	99,996	100	100	99,989	99,873	99,981	99,91	99,989	99,996
ns1.relcom.ru (Rusija)	99,992	99,994	100	99,980	85	99,965	99,992	99,992	99,996
b.root-servers.net (Šiaures Amerika)	99,976	99,849	99,988	99,991	99,973	99,912	99,987	99,973	100
DNS_Google	100	100	100	99,997	100	99,992	100	100	100

Sekantys skaičiavimai parodo, ar tinklo valdymui įdiegti procesai tokie kaip ISO 20000 ir ISO27001 leidžia efektyviai suvalduti resursus. 4 lentelė parodo ar priimti techniniai sprendimai yra efektyvūs ar dar galima juos tobulinti. Lentelės rezultatatai parodo kad tikslas vykdomas tačiau nėra tolygus.

4 lentelė SVDPT santykinis gedimų skaičius 100-ui paslaugų

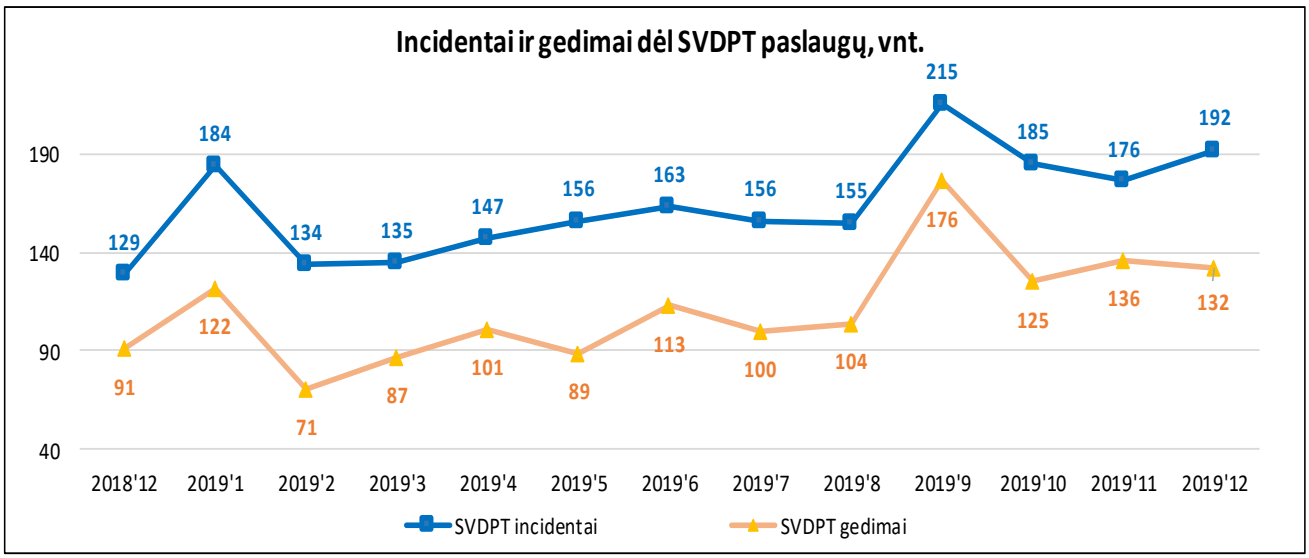
Sudaryta autoriaus pagal SVDPT duomenis



Sekantys skaičiavimai parodo viso tinklo įrenginių gedimų kiekį Saugiajame tinkle per tam tikrą laikotarpį lentelėje 5.

5 lentelė Papildoma informacija. SVDPT paslaugų incidentų ir gedimų kiekis vienetais

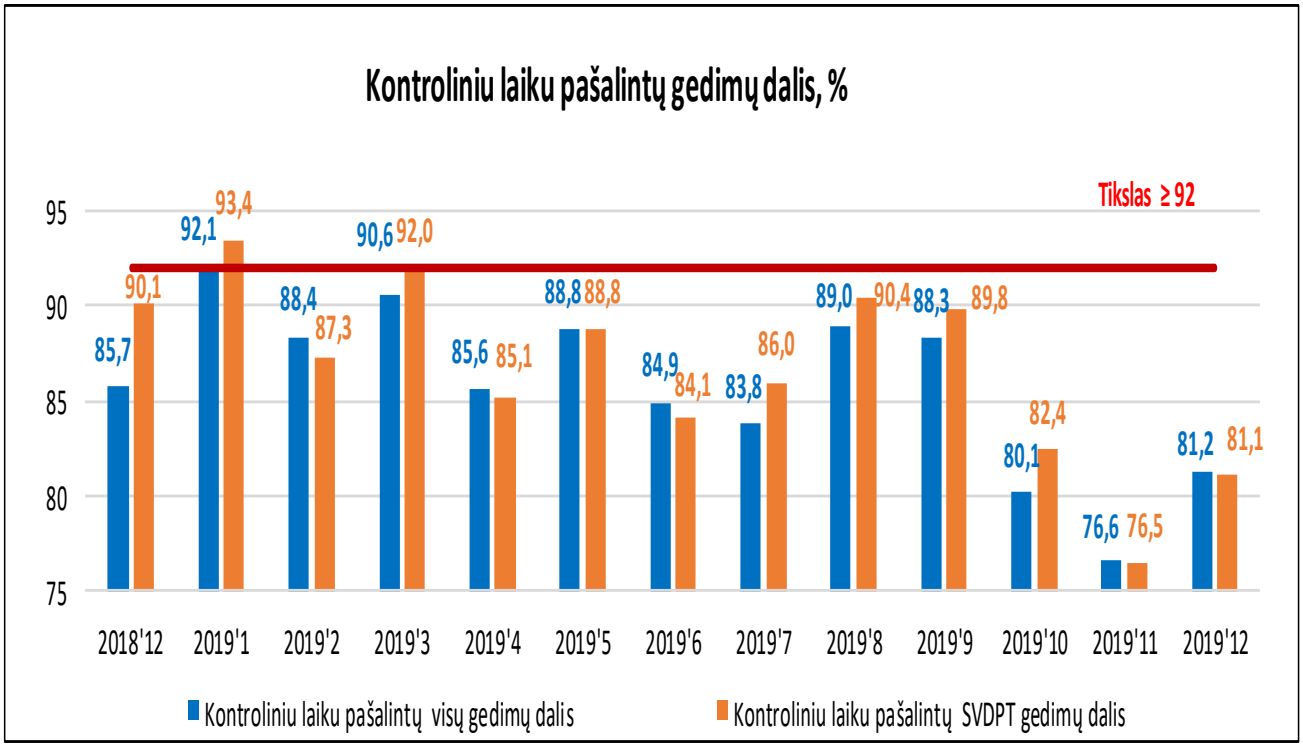
Sudaryta autoriaus pagal SVDPT duomenis



Ne mažiau svarbus efektyvus valdymo procesų įgyvendinimas. Vienas iš tinklo užtikrinimo rodiklių yra gedimų pašalinimas per numatytą laiką 6 lentelė. Neįgyvendinus numatyto rodiklių tikslo tampa sunku įgyvendinti techninius įsipareigojimus

6 lentelė Gedimų pašalintų kontroliniu laiku, dalis

Sudaryta autoriaus pagal SVDPT duomenis



Iš lentelėje pateiktų rezultatų nustatyta, kad tikslas yra nevykdomas. Gavus šiuos rezultatus, buvo atliktas tyrimas ar šio tikslo nevykdymas turi įtakos saugiojo tinklo, konfidencialumo, prieinamumo, nepaneigiamumo užtikrinimui bei kas lėmė tokių rezultatų atsiradimą.

Pastabos:

1. Kadangi Saugus tinklas veiklą pradėjo 2019 liepos 1 dieną, jame neturi likti prijungtų institucijų, nesančių Saugiojo tinklo sąraše. Sistema tiesiog fiksavo atjungtus klientus, todėl šis grafikas neatitinka visiškai tikros padėties.
2. Išanalizavus ar tai turėjo įtakos tinklo prieinamumui nustatyta kad ne, tai atsispindi ir lentelėje 3.

Viso buvo 26 vnt. virškontrolinių gedimų, iš kurių 11 vnt. šalino trečiosios šalys (gedimus šalina rangovai pagal sutartis). Trečiosios šalys šalino 22 vnt. gedimų.

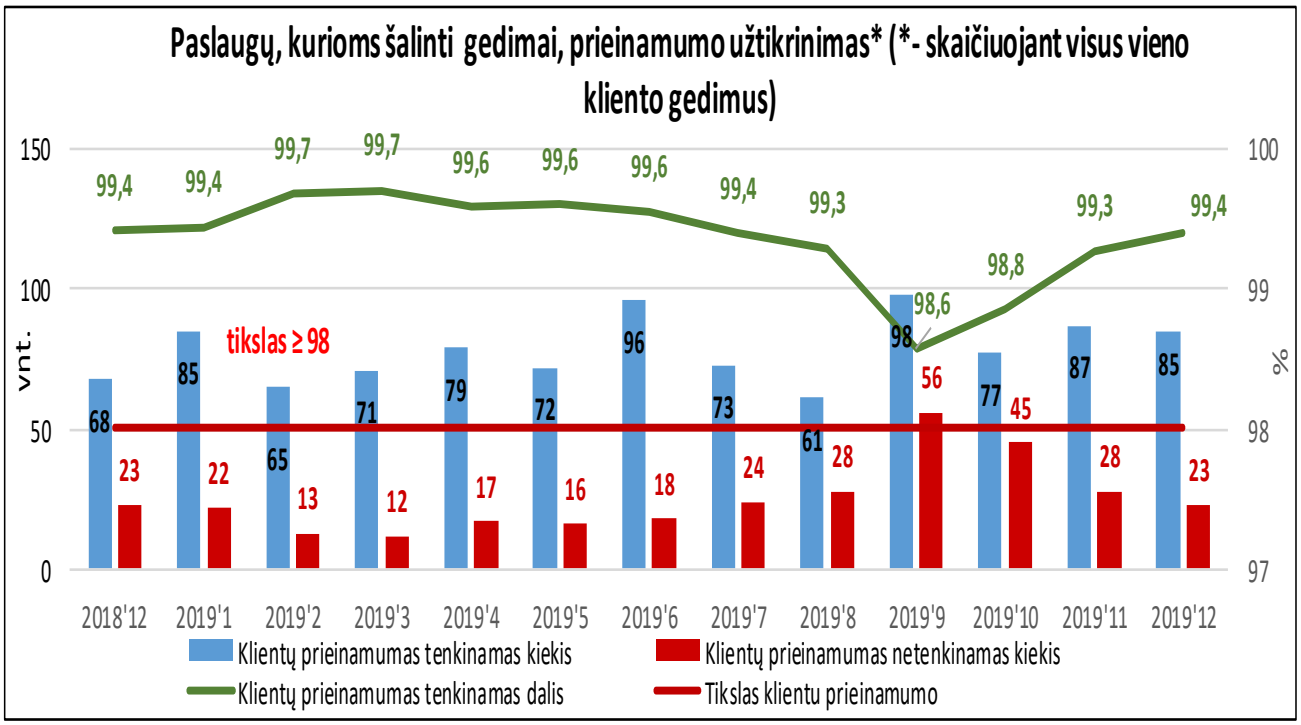
Nuo 2018 metų lapkričio mėn. pradžios Saugiojo tinklo naudotojų, incidentai ir užklausos valdomi naujoje naudotojų ir paslaugų valdymo sistemoje, kurioje reikalavimai paslaugų teikimui – reakcijos į gedimus laikas ir maksimalus paslaugos teikimo atkūrimo laikotarpis – atitinka LR KAM patvirtintas taisykles.

PLANINIAI PROCESŲ VERTINIMO RODIKLIAI

Lentelė 7 - 8 vertina įdiegtus valdymo procesus.

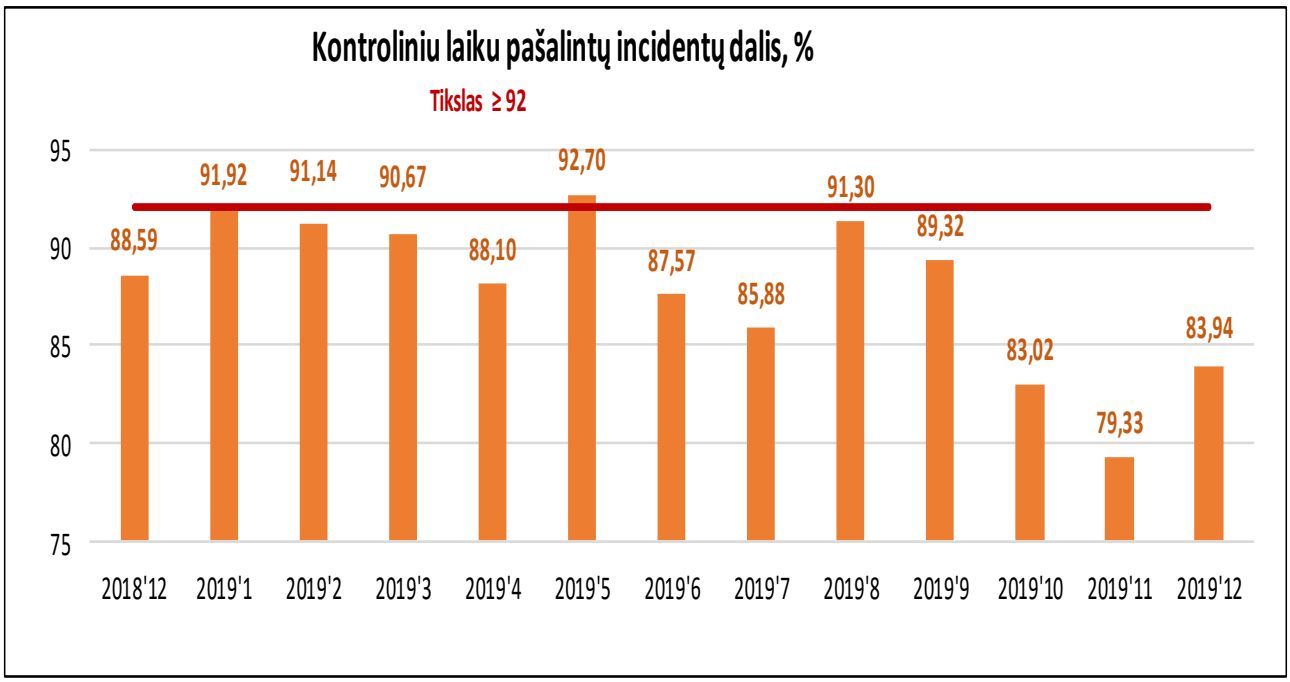
7 lentelė Paslaugų, kurioms šalinti gedimai, prieinamumo užtikrinimas* (*- skaičiuojant visus vieno kliento gedimus)

Sudaryta autoriaus pagal SVDPT duomenis



8 lentelė Kontroliniu laiku išspręstų incidentų (visų paslaugų) dalis:

Sudaryta autoriaus pagal SVDPT duomenis



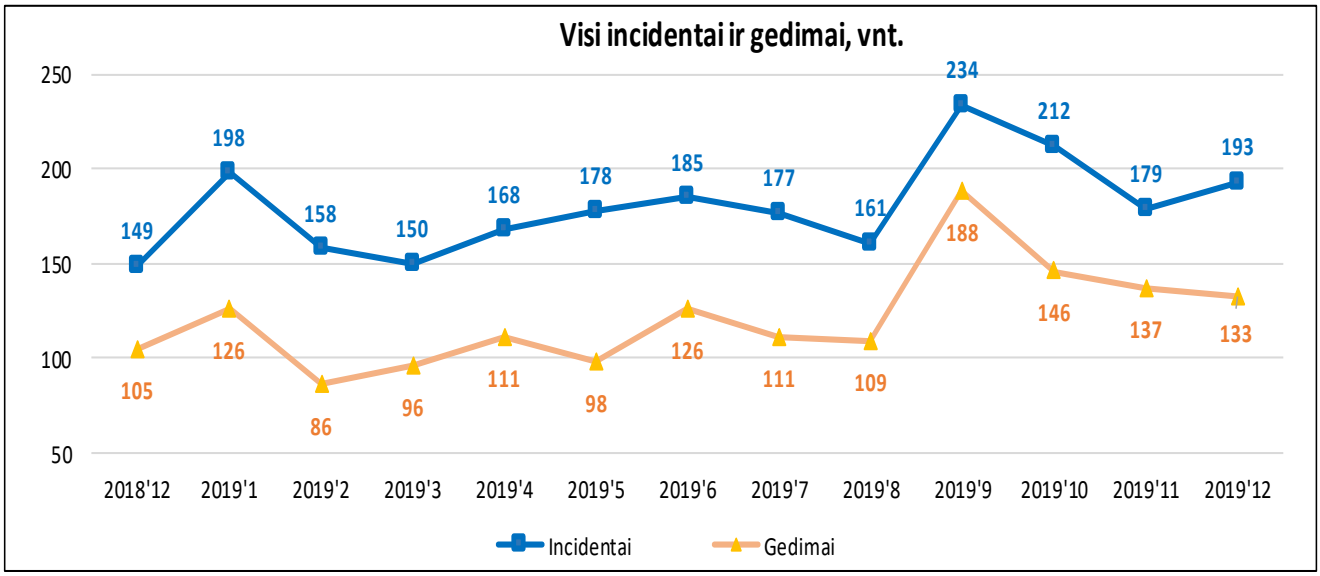
Tikslas nevykdomas, išvados atitinka kaip ir 6 lentelės.

Sekantys skaičiavimai parodo viešajam sektoriui teikiamų ryšio bei prieglobos paslaugų incidentų bei gedimų skaičių,

SVDPT ir DC suminis incidentų ir gedimų skaičius 9 -10 lentelės.

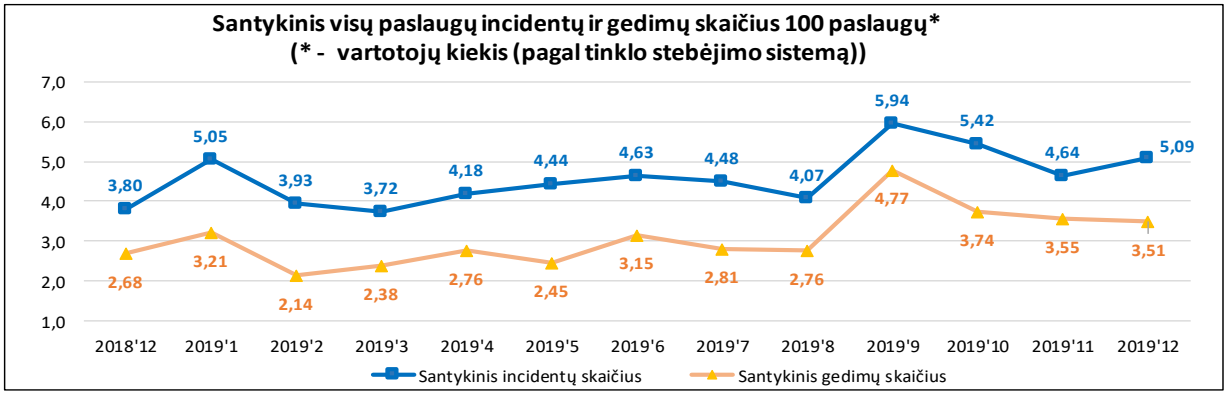
9 lentelė Viso užregistruota paslaugų incidentų ir gedimų:

Sudaryta autoriaus pagal SVDPT duomenis



10 lentelė Santykinis gedimų bei incidentų skaičius 100-ui paslaugų yra:

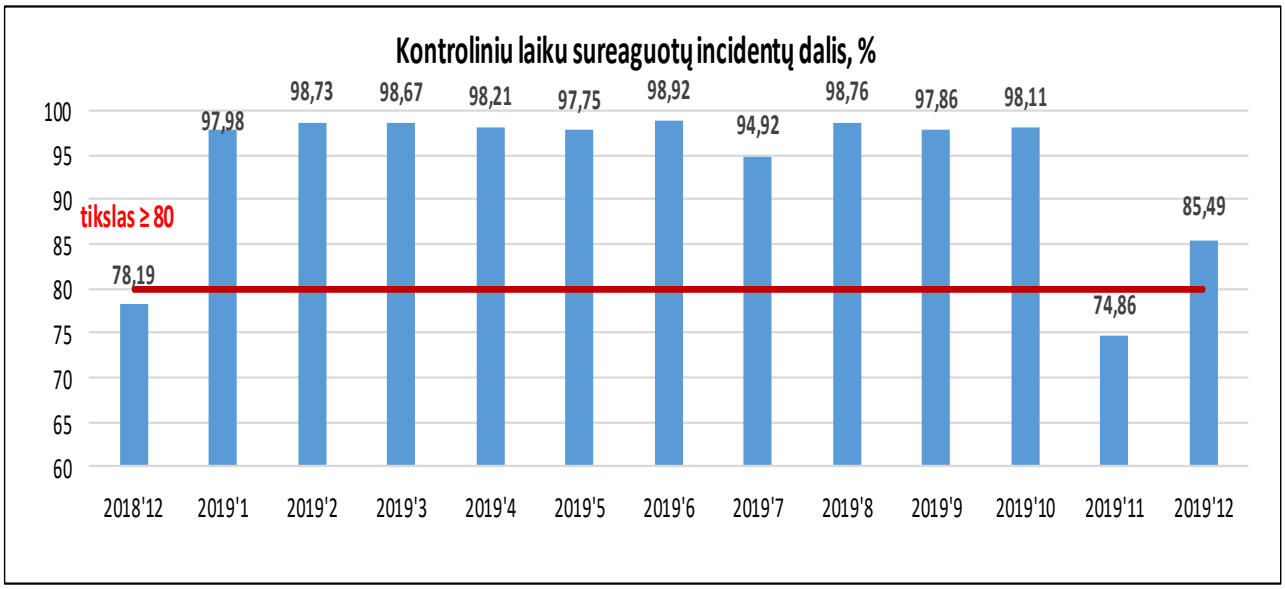
Sudaryta autoriaus pagal SVDPT duomenis:



Sekantys skaičiavimai parodo efektyvų veiklos organizavimą bei kibernetinio saugumo valdymą 11 lentelė.

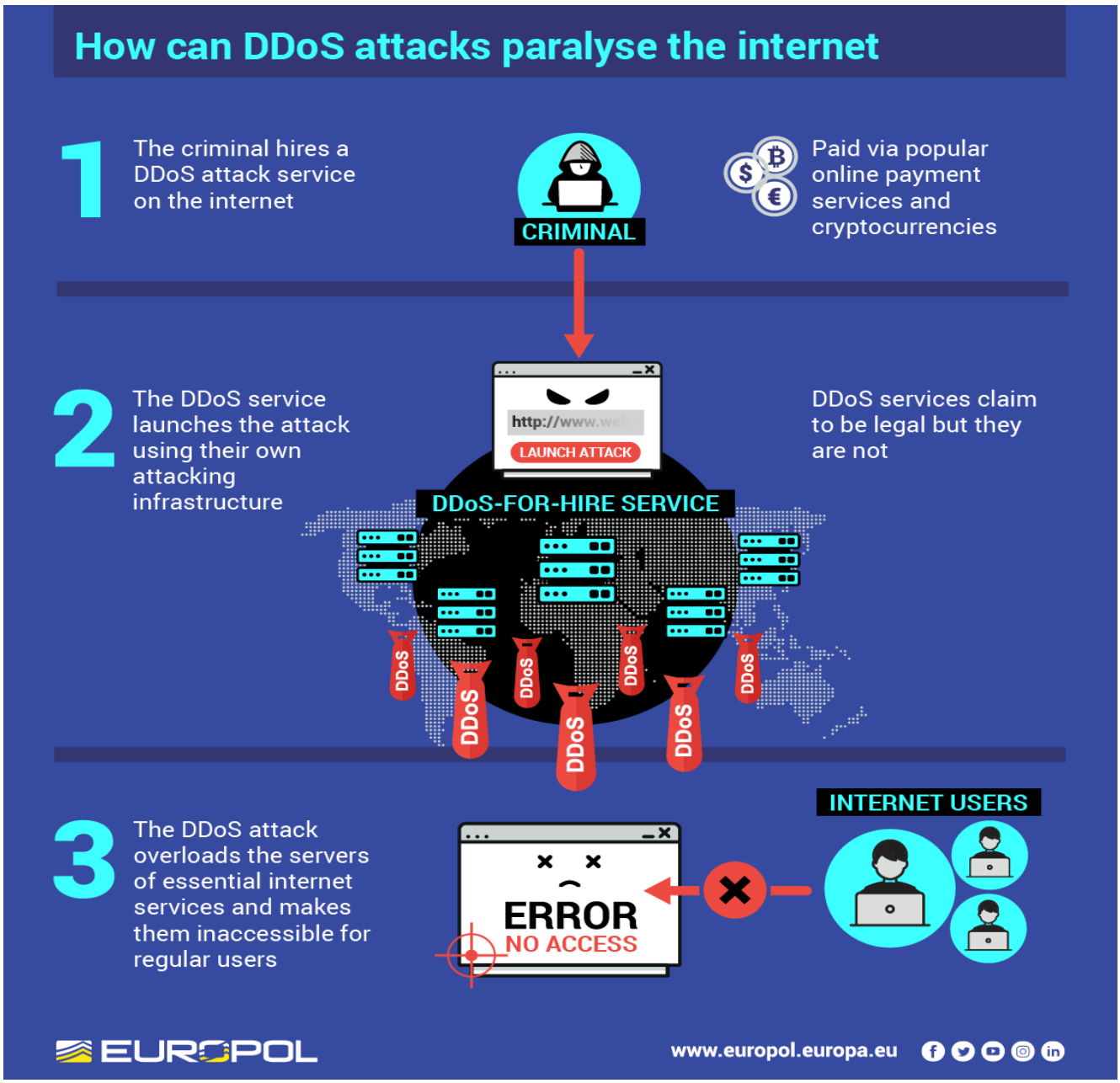
11 lentele Kontroliniu laiku sureaguotų incidentų (visų paslaugų) dalis

Sudaryta autoriaus pagal SVDPT duomenis



2.4 Kibernetinių atakų, kurias patiria Saugusis tinklas analizė

Nepertraukiamas elektroninio ryšio tinklo darbas yra daugiausiai resursų reikalaujantis uždavinys. Per praėjusius metus DDoS (angl. Distributed denial of service) augimas siejamas su tuo, kad jas įvykdyti nereikia specialių kompiuterinių žinių, tai tiesiog yra perkama paslauga, kurios kaina dažnai siekia keliolika eurų. 2018 metais Europolas sustabdė vienos tokias paslaugas teikiančios svetainės darbą, kuria nusikaltėliai naudojosi vos už 15 JAV dolerio kainavusiomis svetainės paslaugomis, surengdami vadinamųjų paskirstyto atsisakymo aptarnauti (DDoS) atakų, kurios nukreipia į aukų serverius didžiulius duomenų srautus ir atjungia jų elektronines sistemas Pav. 11



Šaltinis: Europol

Pav. 11 DDoS ataka kaip prekė

Šioje tyrimo dalyje analizuojamos (DDoS), kibernetinės atakos, kurios yra nukreiptos į Saugųjį tinklą bei jo vartotojus, institucijas kurios yra numatytos Saugiojo tinklo sąraše. Pagrindinis tokių atakų tikslas yra sutrikdyti tiek viso Saugiojo tinklo tiek pavienių institucijų darbą. Pagrindinis tikslas- tinklo prieinamumas.

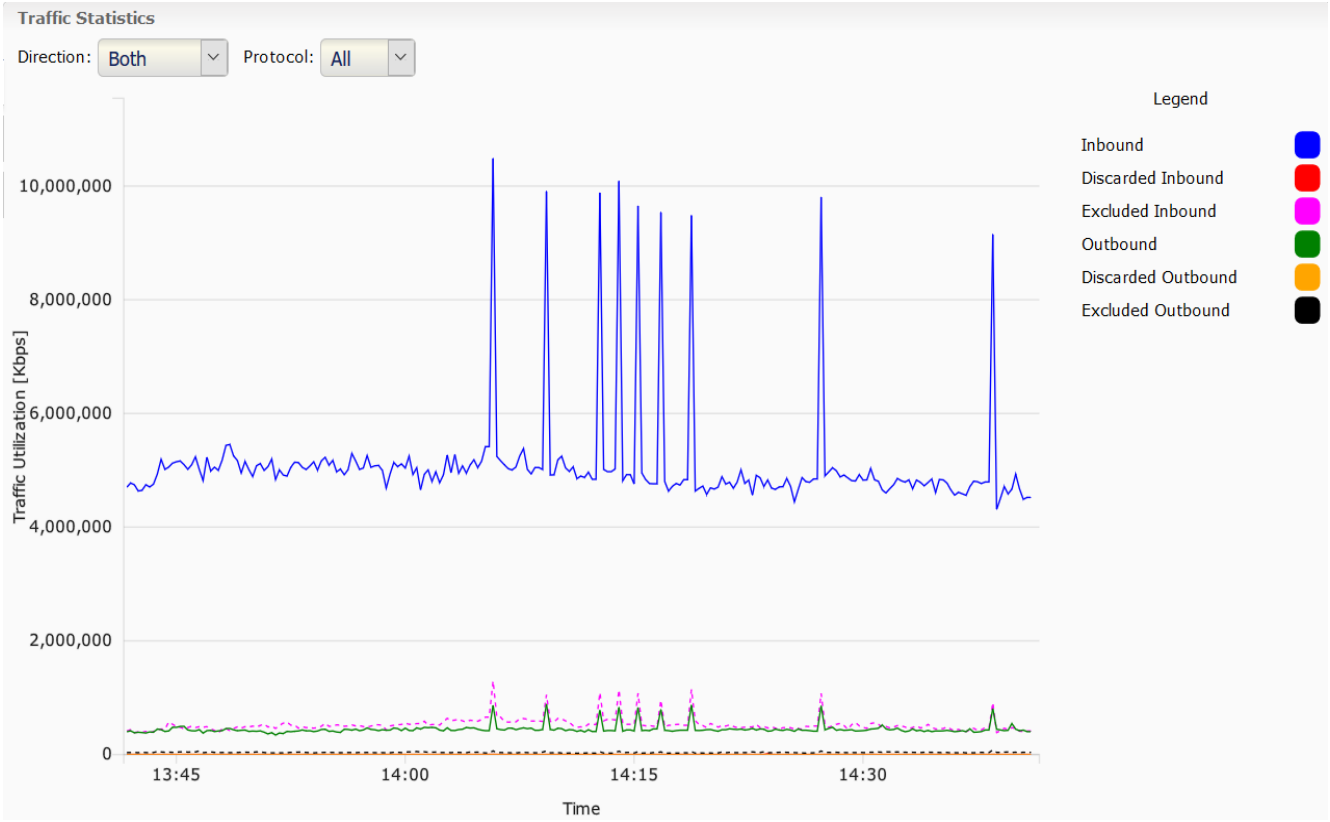
Pagrindiniai DDoS atakų pobūdžai:

1. Labai didelio srauto generavimas.
2. Netinkamo ryšio protokolų siuntimas.
3. Didelis ryšio sujungimų generavimas

Kaip srauto atakos nukreiptos į SVDPT išsiskiria bendrame sraute galima pamatyti Pav.12

Šaltinis: SVDPT

Pav. 12 Srauto stebėjimo sistema



Analizuojant pavaizduotą grafiką galima nustatyti:

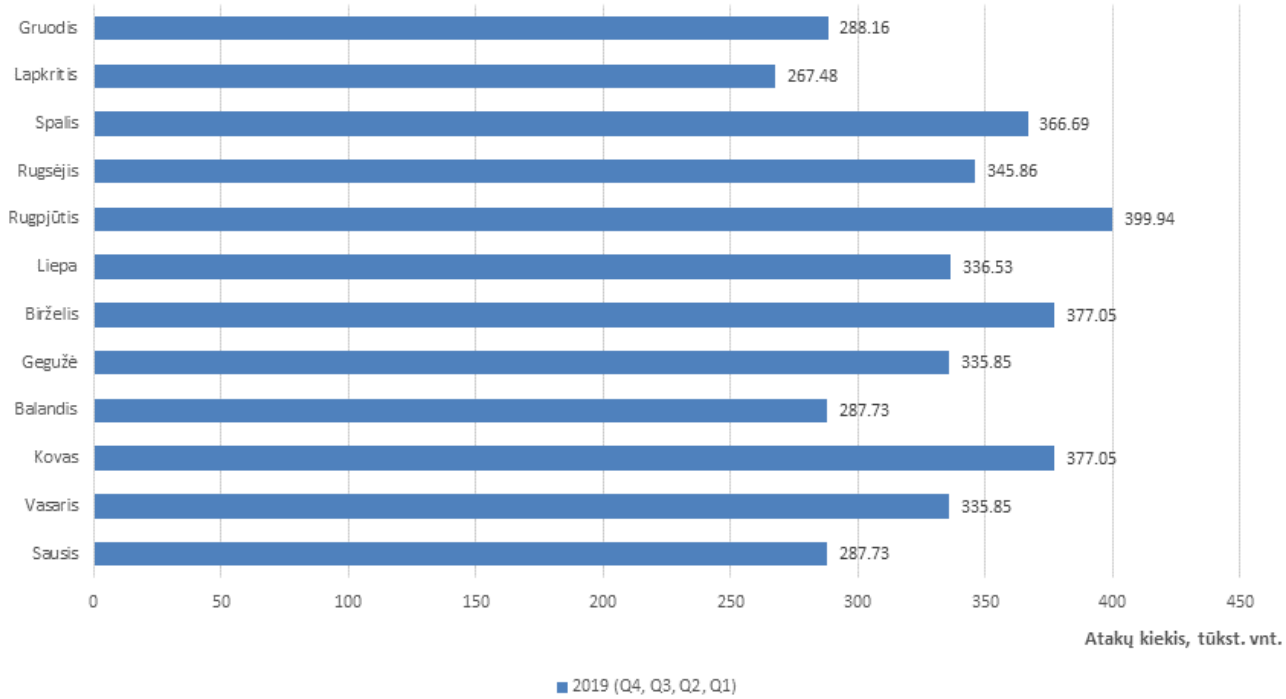
1. Kokio dydžio yra ataka.
2. Atakos pradžia ir pabaiga.
3. Koks srautas buvo praleistas.

Grafike gerai matyti kolektyvinės kibernetinės apsaugos nuo DDoS atakų atsparumo galimybės, kaip veikia gynyba, per kiek laiko yra užkardoma ataka.

Šiame grafike, kuris atvaizduotas lentelėje 12, pavaizduotas suminis (DDoS) atakų skaičius, nukreiptas į Saugųjį tinklą bei jo vartotojus, institucijas kurios yra numatytos Saugiojo tinklo sąraše. Grafikas buvo sudarytas naudojantis SVDPT veiklos įrašų žurnaluose esančia informacija. Lentelėse 13-14 pateikiama TOP 10 klientų į kuriuos nukreiptos atakos išskaitytos pagal trukmę.

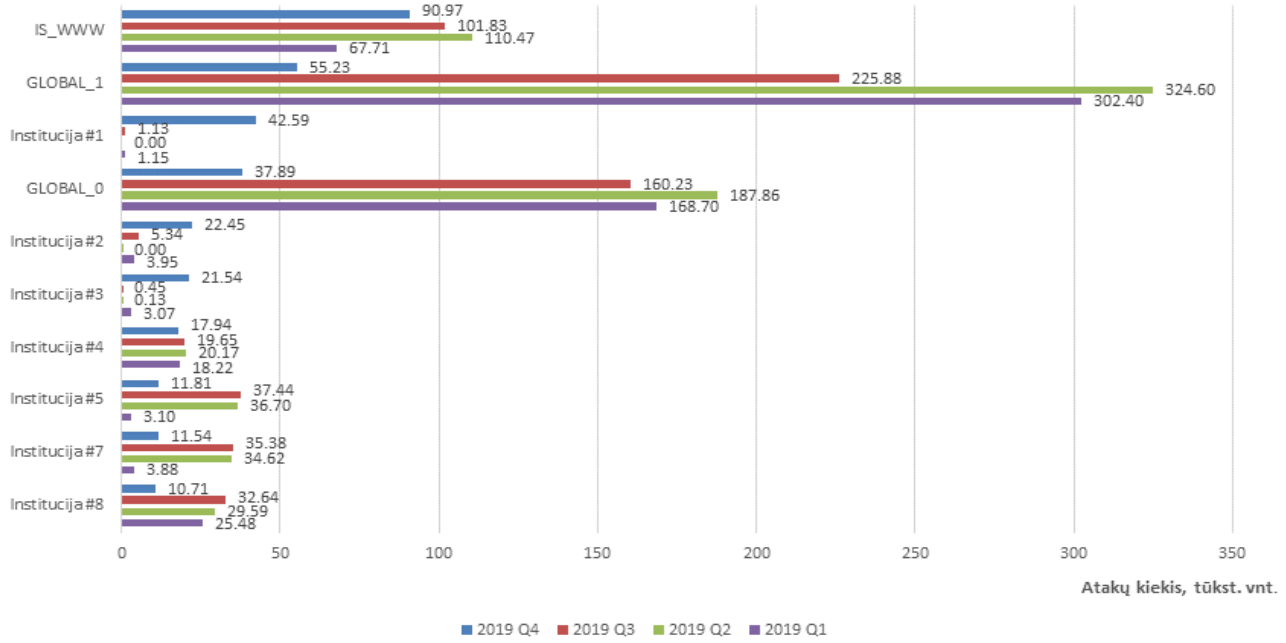
lentelė 12 Bendrų 12 mėnesių sulaikytų DDos atakų į SVDPT suminis skaičius.

Sudaryta autoriaus pagal SVDPT duomenis

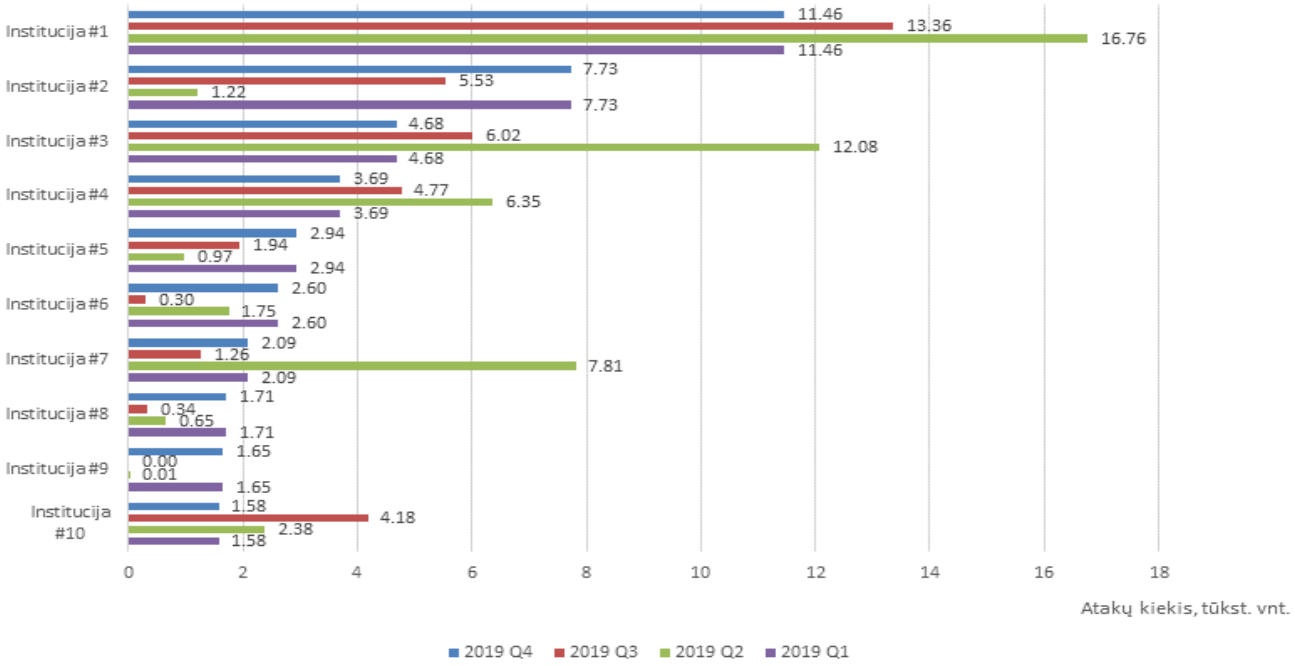


lentelė 13 DDos atakos nukreiptos (į TOP 10 klientų) į SVDPT kurių trukmė iki vienos minutės

Sudaryta autoriaus pagal SVDPT duomenis



lentelė 14 DDos atakos nukreiptos (TOP 10 klientų) į SVDPT kurių trukmė nuo1 iki 5 min.

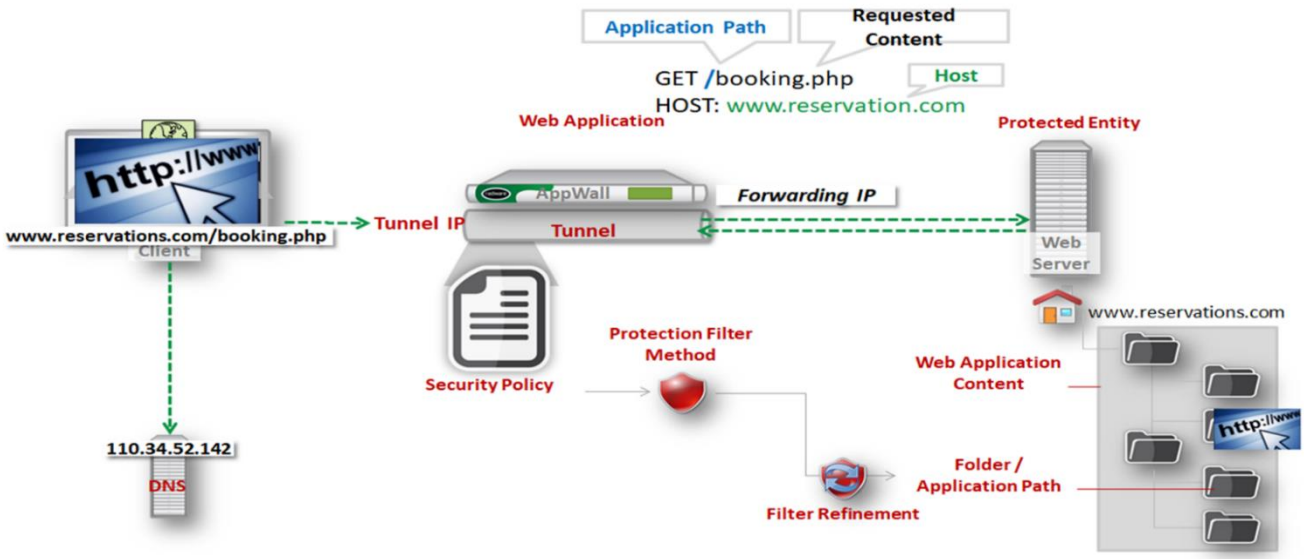


2.5 Kibernetinių atakų, kurias patiria viešojo sektoriaus interneto svetainės analizė

Šioje dalyje analizuojamos kibernetinės atakos, nukreiptos į SVDPT saugomus viešojo sektoriaus portalus, tačiau prieš analizuojant atakas detaliau išnagrinėsime apsaugos organizavimo principą, bei atakas. Vadovaudamiesi 13 pav. nurodyta schema išdėstysime kaip tai veikia ir iš kokių komponentų ji susideda:

Šaltinis: SVDPT

Pav. 13 Kenksmingo interneto turinio ir aplikacijų blokavimas(WAF)



Portalų atakų apsaugos komponentai susideda iš:

- Brute force saugos taisyklių filtro modulio;
- Duomenų bazių saugos taisyklių filtro modulio;
- Bylų išsiuntimo saugos taisyklių filtro modulio;
- Visuotinių nustatymų saugos taisyklių filtro modulio;
- HTTP saugos taisyklių filtro modulio;
- Įvykių žurnalo saugos taisyklių filtro modulio;
- Nustatymų saugos taisyklių filtro modulio;
- Maršrutų blokavimo (path-blocking) saugos taisyklių filtro modulio;
- Saugaus atsakymo (safe reply) saugos taisyklių filtro modulio;
- Sesijų saugos taisyklių filtro modulio;
- Pažeidžiamumų saugos taisyklių filtro modulio;
- WEB paslaugų saugos taisyklių filtro modulio;
- XML saugos taisyklių filtro modulio.

Kaip veikia portalų apsauga:

Klientas inicijuoja užklausą tinklalapyje, šiame pavyzdyje 4 paveikslėlyje – *www.reservations.com/booking.php*

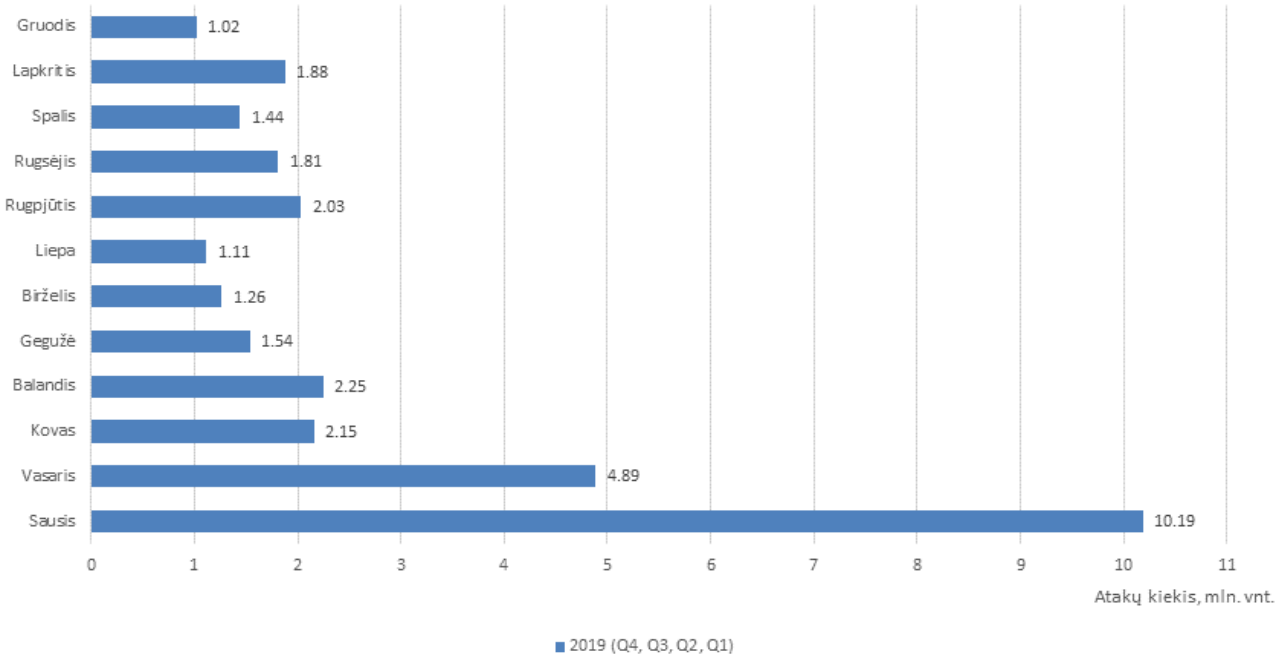
- Naršyklė nustato *hostname (www.reservations.com)* naudojant Tunelio IP.
- Naršyklė siunčia užklausą į "AppWall" tunelį, kuris klausosi konkretaus IP ir port'o.
- "AppWall" tunelis yra susietas su "Protected Entity", kuris yra žiniatinklio serveris.
- "AppWall" nagrinėja tunelį, kuriame gauta užklausa, nurodytą *host* vardą ir *Application Path.*
- Naudojant šiuos parametrus yra išnagrinėjama užklausa naudojant skirtingus saugos filtrus, kurie apsaugo nuo įvarių rūšių išpuolių.
- Kartais saugumo filtras reikalauja patobulinimo, kad atitiktų konkrečius konkretaus puslapio reikalavimus.
- Jei "AppWall" nustato, kad užklausa yra gera, jis ją perduoda atitinkamam žiniatinklio serveriui, naudodamas *forwarding IP*.
- Web serveris ieško prašomo turinio atitinkamame *Application Path* ir siunčia jį atgal į "AppWall".
- "AppWall" tikrina atsaką dėl galimų išpuolių pagal nustatyta saugumo politiką. Jei atsakymas yra *attack – free*, "AppWall" klientui siunčia serverio atsakymą su prašomu turiniu.

Tęsdami SVDPT kolektyvinės kibernetinės įrangos, kuri atsakinga už kenksmingo interneto turinio ir aplikacijų blokavimą (WAF), nustatysime jos efektyvumą bei veiksmingumą, kuris yra taikomas kolektyvinėje kibernetinėje gynyboje. Tyrimo metu buvo analizuojama 180 portalų, kuriems

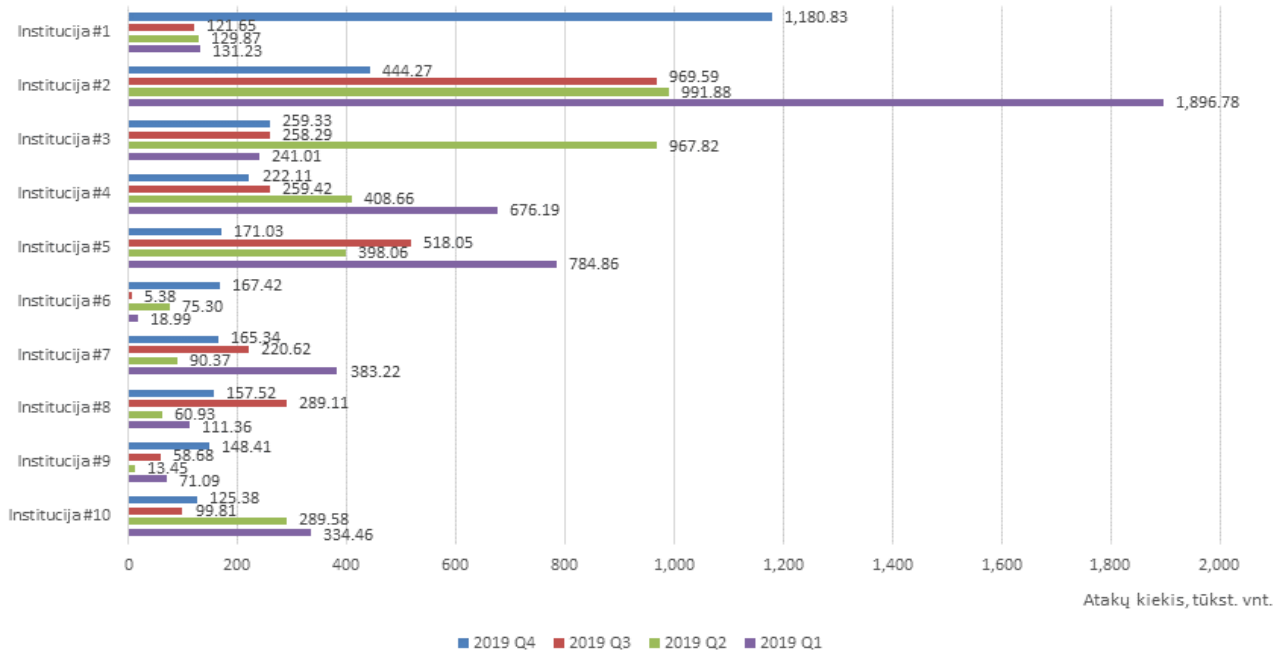
buvo taikoma apsauga. Išanalizavus gautą informaciją ir ją apdorojus, pateikiame15 lentelėje bendrą atakų kiekį, kurį per metus patyrė 180 portalų, ir nebuvo sutrikdyta jų veikla. Iš gautos informacijos matyti, kad valstybinio sektoriaus portalai patiria labai didelius kiekius kibernetinių atakų. Gavus tokius didelius kibernetinių atakų skaičius 16 lentelėje detalizavome ir atvaizdavome kiek atakų patiria vienas portalas (1IP). Portalo tikslaus pavadinimo dėl konfidencialumo skelbti negalime. Iš gautų rezultatų matyti, kad per tris mėnesius vienas portalas gali patirti nuo vieno iki penkių milijonų atakų.

lentelė 15 WAF sulaikytų atakų bendras skaičius į SVDPT per 12 mėnesių**.**

Sudaryta autoriaus pagal SVDPT duomenis



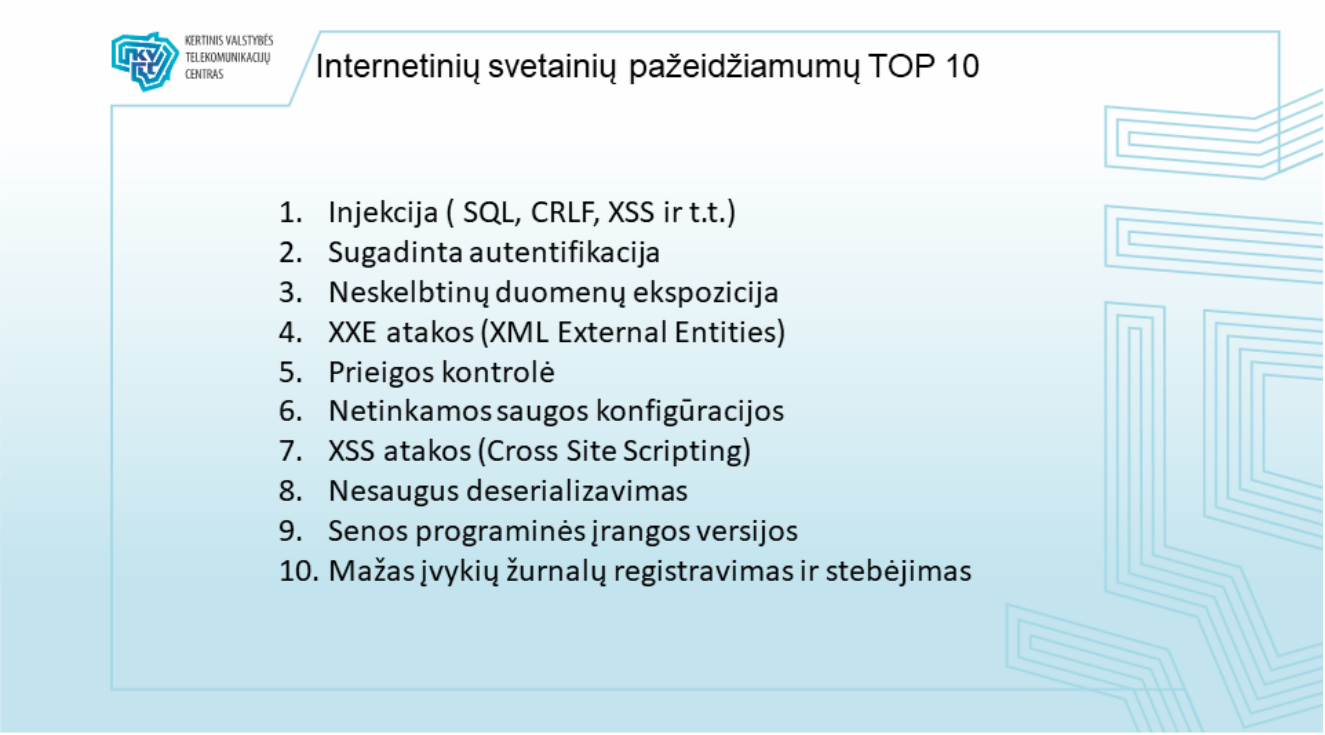
lentelė 16 WAF sulaikytų atakų bendras skaičius į SVDPT per 12 mėnesių TOP 10



Išanalizavus kolektyvinę portalų schemą, galime drąsiai teigti, kad tai tikrai veiksminga apsauga, turinti dideles saugumo galimybes. Naudojant tokią sistemą nesunkiai galima apsisaugoti nuo atakų prieš neapsaugotas bei pažeidžiamas turinio valdymo sistemas, bei kitas portaluose esančias spragas. Išanalizavę SVDPT naudojamą sistemą bei ataskaitas, pristatome 10 populiariausių 2019 metų internetinių puslapių pažeidžiamumų Pav14.

Šaltinis: KVTC - CERT

Pav. 14 Internetinių svetainių pažeidžiamumų TOP 10



Norint nustatyti kolektyvinės kibernetinės apsaugos, skirtos svetainių apaugai efektyvumą, buvo išanalizuota dvidešimties svetainių pažedžiamumų vertinimai ir juose esančios spragos. 17 lentelėje matyti kokią dalį tinklapiuose esančių spragų apsaugo naudojama sistema

Lentelė 17 WAF saugumo efektyvumas

Sudaryta autoriaus pagal KVTC-CERT duomenis

Tinklalapiai:	**Pažeidžiamumų skaičius:**	**Pažeidžiamumai:**	**WAF apsauga (%)**
Tinklalapis1	40	Cross Site Scripting	95%
		HTML form without CSRF protection	
		HTTP parameter pollution	
		Slow HTTP Denial of Service Attack	
		User credentials are sent in clear text	
		Vulnerable Javascript library	

Tinklalapis2	230	HTML form without CSRF protection Slow HTTP Denial of Service Attack	100%
Tinklalapis3	36	HTML form without CSRF protection Slow HTTP Denial of Service Attack Vulnerable Javascript library	97%
Tinklalapis4	10	Wordpress Directory Traversal HTML form without CSRF protection Slow HTTP Denial of Service Attack Vulnerable Javascript library	100%
Tinklalapis5	6	HTML form without CSRF protection Slow HTTP Denial of Service Attack	100%
Tinklalapis6	81	Cross Site Scripting HTML form without CSRF protection Slow HTTP Denial of Service Attack User credentials are sent in clear text	98%
Tinklalapis7	23	Server directory traversal Application error message HTML form without CSRF protection Slow HTTP Denial of Service Attack User credentials are sent in clear text	91%
Tinklalapis8	273	Blind SQL Injection Cross site scripting HTML form without CSRF protection PHPinfo page User controllable charset Vulnerable Javascript library	99%
Tinklalapis9	658	Error message on page HTML form without CSRF protection Insecure crossdomain.xml file PHP hangs on parsing particular strings as floating point number Slow HTTP Denial of Service Attack Vulnerable Javascript library	99%
Tinklalapis10	592	Cross site scripting Session fixation Directory listing HTML form without CSRF protection Liferay version older than 7.0 Liferay XMLRPC Blind SSRF URL redirection Vulnerable Javascript library	98%
Tinklalapis11	114	Application error message Credit card number disclosed Development configuration file HTML form without CSRF protection	92%

		Vulnerable Javascript library	
Tinklalapis12	50	Cross site scripting WordPress 4.9.x Arbitrary File Deletion Vulnerability WordPress 4.9.x Cross-Site Request Forgery WordPress 4.9.x Denial of Service Vulnerability WordPress 4.9.x Multiple Vulnerabilities WordPress Directory Traversal HTML form without CSRF protection HTML injection	92%
Tinklalapis13	348	HTML form without CSRF protection	100%
Tinklalapis14	7	Cross site scripting HTML form without CSRF protection Multiple vulnerabilities fixed in PHP versions 5.5.12 and 5.4.28 Vulnerable Javascript library	71%
Tinklalapis15	138	CRLF injection/HTTP response splitting HTML form without CSRF protection Nginx Redirect Header Injection Vulnerable Javascript library	63%
Tinklalapis16	2202	Blind SQL Injection Cross site scripting Credit card number disclosed Host header attack HTML form without CSRF protection	99%
Tinklalapis17	2	HTML form without CSRF protection	100%
Tinklalapis18	203	WordPress 4.9.x Arbitrary File Deletion Vulnerability WordPress 4.9.x Cross-Site Request Forgery WordPress 4.9.x Denial of Service Vulnerability WordPress 4.9.x Multiple Vulnerabilities WordPress Directory Traversal WordPress Plugin Contact Form 7 Privilege Escalation WordPress Plugin Easy Updates Manager Privilege Escalation WordPress Plugin Limit Login Attempts Cross-Site Scripting Application error message Folder backup HTML form without CSRF protection Slow HTTP Denial of Service Attack TLS 1.0 enabled Vulnerable Javascript library WordPress username enumeration	89%
Tinklalapis19	649	HTML form without CSRF protection Vulnerable Javascript library	99%
Tinklalapis20	169	Cross site scripting HTML form without CSRF protection Vulnerable Javascript library	99%

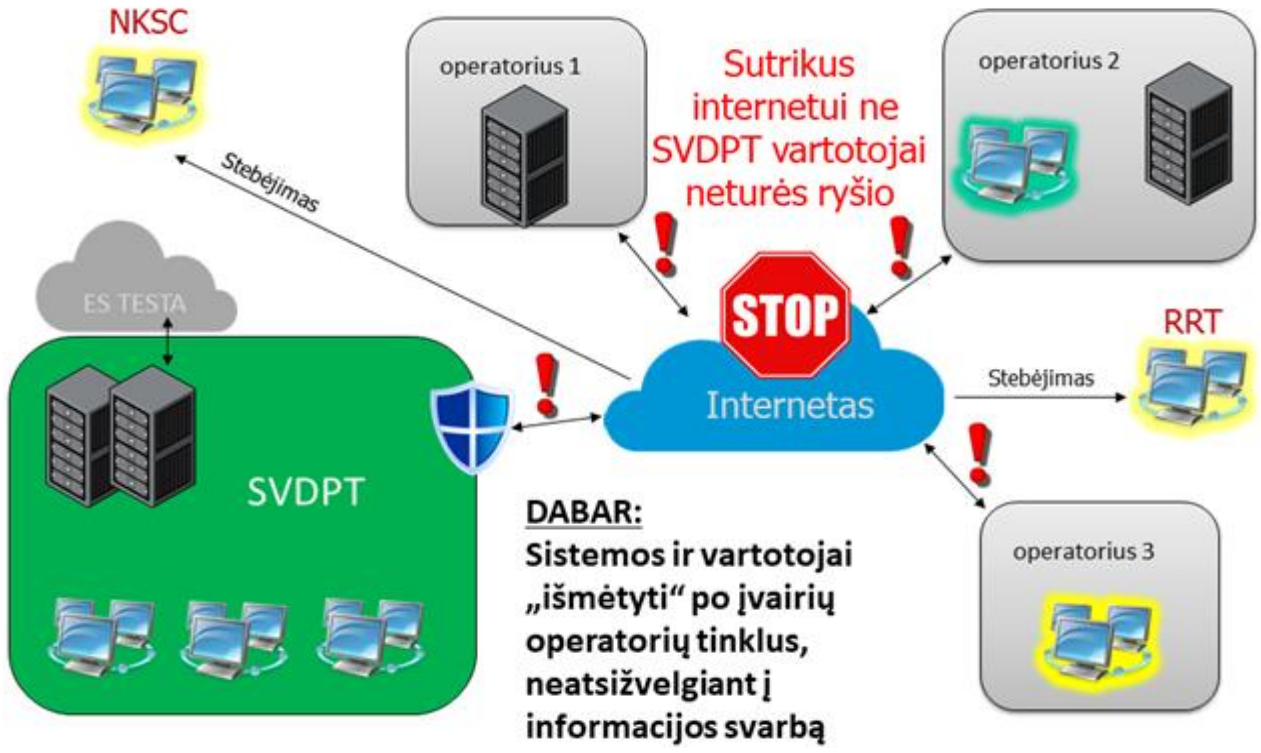
3. INDIVIDUALI VIEŠOJO SEKTORIAUS KIBERNETINĖ GYNYBA

3.1 Individualios kibernetinės gynybos modelis

Šiai dienai sunku surasti valstybę, kurioje būtų taikoma tik individuali kibernetinė gynyba, taikoma viešajam sektoriui. Priėmus tokį sprendimą, visų pirma, būtų susiduriama su labai dideliais kaštais bei kompetencijų stoka. Suvaldyti tokio modelio praktiškai neįmanoma. Lietuvoje taikoma hibridinė kolektyvinė gynyba. Jos pagrindinis tikslas centralizuotai apsaugoti tik svarbius valstybei resursus bei institucijas, kurios yra įrašytos į Lietuvos Respublikos Vyriausybės nutarimu patvirtinto Saugiojo tinklo naudotojų sąrašą. Kitos į sąrašą neįtrauktos institucijos, tokios kaip švietimo įstaigos, bibliotekos bei kitos viešąsias paslaugas teikiančios įstaigos, kibernetiniu saugumu turi rūpintis pačios, nors jos nuolatos jungiasi prie informacinių išteklų. Iš Pav. 15. matyti, kad jos visos jungiasi prie informacinių išteklių iš skirtingų ryšio tiekėjų. Esant kritinei situacijai interneto ryšio tinkluose jos negalės naudotis resursais. Tik Saugiojo tinklo viduje esančios įtaigos nepatirs jokių sutrikimų naudojantis valstybės registrais bei kitomis duomenų bazėmis (turto registras, gyventojų registras, e-sveikatos paslaugos ir kt.).

Šaltinis: SVDPT

Pav. 15 Lietuvoje naudojamos kolektyvinės kibernetinės gynybos modelis



Pradėjus analizuoti individualų kibernetinio saugumo modelį, paaiškėjo pagrindiniai trūkumai ir problemos, atlikta analizė parodė:

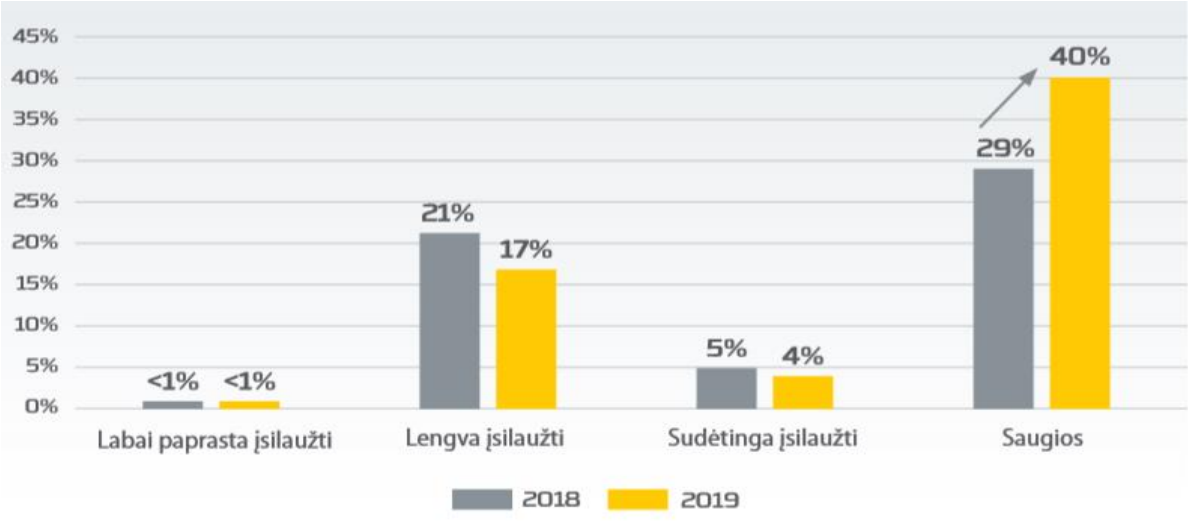
1. Institucijos kuria, modernizuoja bei naudoja savo atskirus duomenų perdavimo tinklus, kurių išlaikymui ir plėtrai kasmet skiriamos didelės valstybės biudžeto lėšos;
2. Daugelio Viešojo administravimo institucijų gebėjimai aptarnauti, prižiūrėti ir vystyti žinybinius ryšių tinklus yra nepakankami;
3. Neracionaliai naudojami žmogiškieji, finansiniai, IRT ištekliai;

3.2 Individualios viešojo sektorius kibernetinės gynybos analizė

Iš 2019 metų nacionalinio kibernetinio saugumo būklės ataskaitos apie viešojo sektoriaus interneto svetainių pažeidžiamumus matome, kad peržiūrėjus ir detalizavus viešojo sektoriaus interneto svetainių kibernetinio saugumo būklės vertinimą bei palyginus su ankstesniu laikotarpiu, viešojo sektoriaus interneto svetainių kibernetinio saugumo būklė gerėja, tačiau vis dar yra apie 17 proc. svetainių į kurias galima lengvai įsilaužti 16 pav.). NKSC, siekdamas pašalinti pažeidžiamumus, potencialiai pažeidžiamų svetainių valdytojus tiesiogiai informuoja ir koordinuoja aukšto prioriteto pažeidžiamumų pašalinimą. Remiantis patikrinimų informacija, NKSC teikia interneto svetainių valdytojams rekomendacijas apie dažniausius interneto svetainių bei informacinių sistemų trūkumus. Šioms svetainėms nebuvo taikoma Saugiojo tinklo kolektyvinė kibernetinė apsauga. Jos svetainių saugumu rūpinosi individualiai.

Šaltinis: NKSC

Pav 16 NKSC ataskaita



Viešojo sektoriaus interneto svetainių kibernetinis saugumas 2018-2019 m. pagal pažeidžiamumų, tenkančiam vienam domenui, vertinimą.

NKSC atkreipia dėmesį, kad subjektai ne visada įsigyja interneto svetainių palaikymo paslaugas, arba į sutartinius įsipareigojimus neįtraukia nuostatų, įpareigojančių pašalinti dėl broko atsiradusias spragas. Interneto svetainės dažnai nėra įteisinamos kaip informacinės sistemos, nėra paskiriami saugos įgaliotiniai, administratoriai neskiria pakankamai dėmesio kibernetinio saugumo klausimams.

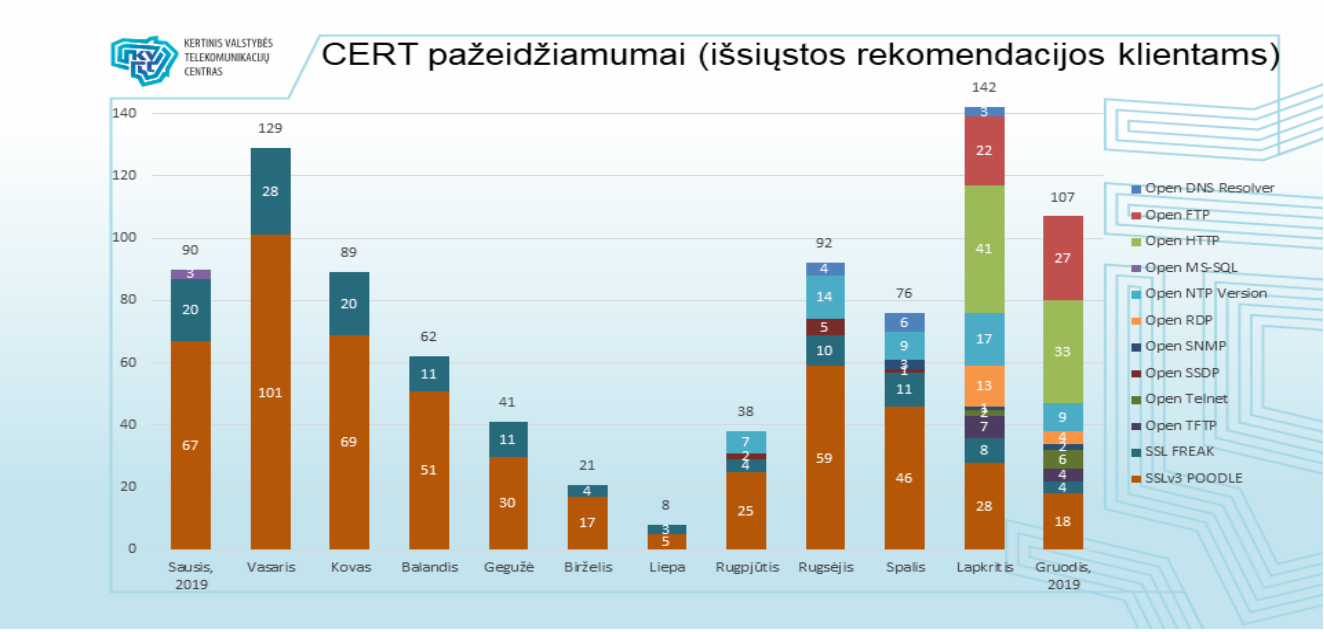
Viešajame sektoriuje efektyvi individuali kibernetinė gynyba, yra sunkiai įgyvendinama, be to, viešajame sektoriuje įgyvendinamos nepakankamos šios srities organizacinės ir techninės priemonės. Viešosios įstaigos savo veikloje nepakankamai dėmesio skiria kibernetiniam saugumui užtikrinti, ne dėl to kad negali, o dėl to, kad neturi kompetencijų. Įstaigų praktinė patirtis ir gebėjimai valdyti kibernetinį saugumą ir el. informacijos saugą, parinkti efektyvias reikalavimų įgyvendinimo kontrolės priemones yra labai riboti.

Esama situacija Lietuvoje parodo, kad tik vienas Saugusis tinklas yra reglamentuotas ir jungiantis 450 institucijų, tuo tarpu kiti valstybės duomenų perdavimo tinklai nėra reglamentuoti, yra skirtinguose operatoriuose. Tai neužtikrina kibernetinio saugumo, bei autonominio visos valstybės informacinių sistemų veikimo, atsijungus nuo viešųjų tinklų.

Po 2019 metų liepos 1 dienos nuo Saugiojo tinklo buvo atjungiami sąraše nesantys vartotojai (švietimo įstaigos) ir jiems nebuvo taikoma kolektyvinė kibernetinė apsauga. Iš pateiktos ataskaitos Pav.12 matyti įstaigose padidėjęs kibernetinių pažeidžiamumų kiekis. Šis paveikslėlis labai aiškiai parodo viešojo sektoriaus gebėjimus gintis individualiai. Galima daryti išvadą kad Lietuvos viešasis sektorius dar nepasiekė tokios kibernetinio saugumo brandos kad galėtų gintis individualiai.

Šaltinis: SVDPT

Pav 17 KVTC- CERT klientų informavimo ataskaita



IŠVADOS

Kibernetinė gynyba yra aukštesnio lygmens kibernetinio saugumo tikslas, kurį galima apibūdinti kaip labiau viešajam sektoriui taikytiną sritį. Ji yra nacionalinio saugumo sudėtinė dalis, taikytina ne tik Lietuvos bet ir visos Europos sąjungos kibernetinei gynybai, kuriai yra taikytinas ir bendras teisinis reguliavimas. Dėl skirtingos kibernetinio saugumo brandos šalyse narėse, bei nesant efektyviai kibernetinei gynybai, gali sustoti tarptautiniai elektroniniai duomenų mainai ne tik šalyse kurios patiria kibernetines atakas, bet ir sutrikti viešosios paslaugos visoje Europos sąjungoje. Siekiant apsaugoti bendrą Europos sąjungos ypatingą infrastruktūrą, informacinius išteklius, ekonominę erdvę bei saugią plėtrą, reikalinga vieninga kibernetinė gynyba, galinti užtikrinti efektyvų pasipriešinimą kibernetinėms atakoms, bei nepertraukiamą viso Europos sąjungos viešojo sektoriaus darbą.

Kibernetinis saugumas kelia vis didesnes grėsmes valstybės institucijų nepertraukiamam darbui bei informacijos saugumui. Tikrasis teisinis reguliavimas, reglamentuojantis kibernetinį saugumą, Lietuvoje prasidėjo nuo 2018 metų. Iki šio laikotarpio Lietuvoje buvo labiau deklaruojamas teisinis reguliavimas. Galima teigti, kad 2018 metai yra atskaitos taškas Lietuvai kovojant su kibernetinėmis grėsmėmis. Lietuvos viešojo administravimo subjektų, valdančių ar tvarkančių valstybės informacinius išteklius, pasirengimas kovai su kibernetinėmis grėsmėmis vis dar yra vidutinis, kadangi tik dalis institucijų yra įgyvendinę Lietuvos Respublikos Vyriausybės nutarimu patvirtintus kibernetinio saugumo organizacinius bei techninius reikalavimus. 2019 metais Lietuvos Respublikos Vyriausybė priima sprendimą daliai viešojo sektoriaus taikyti kolektyvinę kibernetinę gynybą ir patvirtina institucijų sąrašą, kurios bus saugomos vieninga kibernetinės gynybos sistema, taip sušvelnindama kibernetinių grėsmių rizikas viešojo sektoriaus institucijoms kurios vėluoja įgyvendinti kibernetinio saugumo organizacinius bei techninius reikalavimus.

2019 metų liepos 1 dieną pradėjo veikti vieninga kolektyvinio kibernetinio saugumo sistema (Saugusis tinklas), kuri leidžia centralizuotai atremti kibernetines atakas bei užtikrinti viešojo sektoriaus institucijų, esančių Saugiojo tinklo sąraše, nepertraukiamą veiklą. Tačiau pilnas šios sistemos veikimas bei apimtis bus įgyvendinta tik nuo 2022 metų liepos 1 dienos, kada visos institucijos esančios sąraše bus prijungtos prie saugiojo tinklo ir atitiks kibernetinio saugumo organizacinius bei techninius reikalavimus. Tad, galima teigti, kad Lietuvoje kibernetinio saugumo branda yra vidutinė.

Atlikus tyrimą apie kolektyvinę ir individualią kibernetinę gynybą, galima teigti, kad efektyviausia priemonė yra Kolektyvinė kibernetinė apsauga, kadangi įgyvendina užduotus tikslus bei keliamus reikalavimus. Iš to seka išvada, kad visi valstybinio sektoriaus instituciniai, tarpinstituciniai prisijungimai, kur reikalinga prieiga prie Europos Sąjungos institucijų, prie ypatingos svarbos ir/arba svarbių valstybės informacinių išteklių turi būti vykdomi per vienalytį apsaugotą tinklą. Prisijungimai prie šių valstybės informacinių sistemų negalimi per viešuosius tinklus. Tokiais atvėjais prieiga prie viešųjų tinklų (interneto) turi būti centralizuota per saugią kibernetinės saugos platformą. Įvertinant vis

didėjantį kibernetinio saugumo incidentų skaičių, bei siekiant užkirsti kelią kibernetiniams antpuoliams, kolektyvine kibernetinio saugumo platforma bei uždaru tinklu turėtų naudotis ne tik vyriausybės sąraše (Saugiojo tinklo naudotoju sąrašas) patvirtintos įstaigos, bet visos valstybės institucijos, kurios teikia viešąsias paslaugas bei naudojasi informaciniais ištekliais.

Valstybės Kolektyvinis kibernetinės gynybos maksimalus efektyvumas, patikimumas, bei ekonominė nauda būtų tik sudarius galimybę visoms valstybės institucijoms naudotis Saugiuoju tinklu, bei kibernetinės saugos platforma. Tokiu būdu būtų užtikrintas vienodas kibernetinio saugumo lygis bei mažinamos rizikos visame viešajame sektoriuje. Tuomet visos institucijos, o ne tik Saugiojo tinklo naudotoju sąraše esančios, įgyvendintų kibernetinio saugumo organizacinius bei techninius reikalavimus. Būtų tikslinga per vieną prieigą (tinklą) teikti visas elektroninių ryšių paslaugas. Efektyviai būtų taupomos lėšos, panaudojant vieningą sprendimą visiems elektroniniams ryšiams. Visais atžvilgiais šios paslaugos teikimas būtų susijęs išimtinai su valstybės funkcijos įgyvendinimu – siekiu užtikrinti saugių, valstybiškai svarbių duomenų perdavimą, o nustatytas centralizuotas finansavimo mechanizmas bei finansavimo skiriama suma būtų panaudota išskirtinai veiklos sąnaudoms padengti, Saugiojo tinklo infrastruktūrai bei kibernetiniam saugumui gerinti.

Įdiegus tokį pilną o ne dalinį modelį būtų sukurtas operatyvus valdymas, visos paslaugos būtų teikiamos vieno operatoriaus, sprendimai būtų priimami greičiau ir operatyviau. Krizių valdymas būtų vieno operatoriaus rankose, todėl esant krizinei situacijai interneto tinkluose galima lengvai užtikrinti, kad valstybės institucijoms būtų prieinamos informacinės sistemos, visi instituciniai, tarpinstituciniai prisijungimai, kur reikalinga prieiga prie Europos Sąjungos institucijų, prie ypatingos svarbos ir/arba svarbių valstybės informacinių išteklių.

Pagrindinis individualios gynybos modelio trūkumas yra tas, kad esant DDoS ar kitai kibernetinei atakai, kuri sutrikdytų prieinamumą, institucijos neturės jokios galimybės prisijungti prie valstybės informacinių išteklių. Tai dalinai arba visiškai gali sustabdyti institucijų veiklą, kadangi tik būdamos uždarame bendrame tinkle jos galės pasiekti informacinius išteklius esant kibernetinėms atakoms.

2019 metų NKSC ataskaita apie svetainių pažeidžiamumą tik patvirtina, kad individualiai viešasis sektorius neturi kompetencijų užtikrinti savo turimų resursų kibernetinį saugumą. Efektyvi individuali gynyba galima tik tuo atveju kada visos institucijos pasiekia vienodą kibernetinio saugumo brandą ir joms nėra būtinas pastovus prisijungimas prie valstybės informacinių išteklių, jos gali veikti autonomiškai.

LITERATŪRA

1. Lietuvos Respublikos kibernetinio saugumo įstatymas. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee
2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.415499
3. Schjolberg ir Ghernaouti-Hele 2011. A Global Treaty on Cybersecurity and Cybercrime. Geneva. Prieiga per internetą: http://www.cybercrimelaw.net/documents/A_Global_Treaty_on_Cybersecurity_and_Cybercrime,_Second_edition_2011.pdf
4. Darius Štitilis 2011 Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. Prieiga per internetą: https://www.mruni.eu/upload/iblock/39e/013_Stitilis.pdf
5. James A. Lewis 2006. Prieiga per internetą: https://www.csis.org/articles-chapters-and-research-james-lewis
6. Richard A. Kemmerer 2003. Prieiga per internetą: https://www.researchgate.net/publication/4016771_Cybersecurity
7. Lietuvos Krašto apsaugos ministerija ir NATO 2010. Prieiga per internetą: https://kam.lt/lt/tarptautinis_bendradarbiavimas/nato/nato_transformacija/kibernetine_gynyba_ir_energetinis_saugumas.html
8. NKSC 2019. Prieiga per internetą: https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf
9. Johan Eriksson, Giampiero Giacomello 2006. Prieiga per internetą: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A404030&dswid=-2920
10. The National Strategy to Secure Cyberspace 2003. Prieiga per internetą: http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf
11. James A. Lewis, "Cyber Attacks Explained 2007. Prieiga per internetą: https://www.csis.org/analysis/cyber-attacks-explained
12. Joshua Davis 2008 "Hackers Take Down the Most Wired Country in Europe". Prieiga per internetą: https://www.wired.com/2007/08/ff-estonia/
13. Nacionalinio saugumo strategija 2002. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.167925?jfwid=q86m1vqoi
14. LRV Nacionalinio saugumo būklės ir plėtros 2005 metų ataskaita. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.273121?jfwid=1bc6m4z8of
15. Lietuvos Respublikos Vyriausybės nutarimo Nr. 601 2006. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.278475?jfwid=fhhu5mq95

16. Secure Trans European Services for Telematics between Administrations. Prieiga per internetą: https://ec.europa.eu/eurostat/cros/category/acronyms/stesta_en
17. Valstybės įmonės „INFOSTRUKTŪRA“ veiklą reglamentuojantys nuostatai. Prieiga per internetą: http://www.infostruktura.lt/lt/kodel-mes/svdpt/teisine-baze.html
18. National Information Assurance Glossary 2010. Prieiga per internetą: https://www.hsdl.org/?abstract&did=7447
19. Act on Cyber Security, Parliament of Chech Republic 2014. Prieiga per internetą: https://www.govcert.cz/download/kii-vis/preklady/Act_181_2014_EN_v1.0_final.pdf
20. Dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo NUTARIMAS Nr. 796. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.403385
21. Bendrieji duomenų apsaugos reikalavimai, 1997. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.198000
22. Valstybės ilgalaikės raidos strategija 2002. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.193888
23. Dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo Nr. 1625 2001. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.157225?jfwid=sujol5u3x
24. ES kibernetinio saugumo strategija 2013. Prieiga per internetą: https://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+P7-TA-2013-0376+0+DOC+PDF+V0//LT
25. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo 2019. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/faeb5eb4a6c811e9aab6d8dd69c6da66?jfwid=dg8d31595
26. Europos Vadovų Taryba, dėl koordinuoto atsako į didelio masto kibernetinio saugumo incidentus ir krizes 2017. Prieiga per internetą: http://publications.europa.eu/resource/cellar/e7f7a728-9cff-11e7-b92d-01aa75ed71a1.0014.03/DOC_1
27. NSGK pirmininkas A.Paulauskas ragina pasirūpinti kibernetine gynyba. Prieiga per internetą: https://www.respublika.lt/lt/naujienos/lietuva/lietuvos_politika/nsgk_pirmininkas_apaulauskas_ragina_pasirupinti_kibernetine_gynyba/,print.1
28. Dėl nacionalinio kibernetinių incidentų valdymo plano patvirtinimo 2016. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/19f75bc0c5b211e5a141fecd4d43d786?positionInSearchResults=12&searchModelUUID=c1c03ded-6442-4abd-aaa0-247ffa659420

29. NACIONALINIO KIBERNETINIO SAUGUMO BŪKLĖS 2016 METŲ ATASKAITA. Prieiga per internetą: https://www.nksc.lt/doc/nksc_metine_ataskaita_uz_2016.pdf
30. Nutarimas dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo 2016. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/037332710b7111e687e0fbad81d55a7c?jfwid=q8i88m9wh
31. Dėl krašto apsaugos ministro 2013 m. gruodžio 31 d. įsakymo Nr. V-1200 „Dėl Vyriausybinių ryšių centro prie Krašto apsaugos ministerijos nuostatų ir struktūros patvirtinimo“ pakeitimo. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/7bd254a28e2711e7a5e2b345b086d377
32. 2017 metų nacionalinio kibernetinio saugumo būklės ataskaita. Prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2017_[lt].pdf
33. RRT CERT- LT Prieiga per internetą: https://www.rrt.lt/2017-metais-cert-lt-apdorojo-54-414-kibernetiniu-incidentu/
34. Lietuvos Respublikos vyriausybės nutarimas Nr. 406. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/a9b731935ab011e99684a7f33a9827ac?jfwid=tsp3uwv3v
35. Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašas. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAP/dbe591c06cd511e99684a7f33a9827ac?jfwid=t60yn02c1
36. Saugiojo valstybinio duomenų perdavimo tinklo veiklą užtikrinančių dokumentų patvirtinimas. Prieiga per internetą: https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/ead7e7629d8511e9aab6d8dd69c6da66?jfwid=-m92g8jly9
37. State of the Art Report (1) Urban Critical Infrastructure Systems. Prieiga per internetą: https://resin-cities.eu/fileadmin/user_upload/D1-1_UCIsystems_Fraunhofer_2015-11-30.pdf
38. BENDRAS KOMUNIKATAS EUROPOS PARLAMENTUI IR TARYBAI. Prieiga per internetą: https://ec.europa.eu/transparency/regdoc/rep/10101/2017/LT/JOIN-2017-450-F1-LT-MAIN-PART-1.PDF
39. ENISA Threat Landscape Report 2018. Prieiga per internetą: https://securelist.com/ddos-report-q3-2019/94958/
40. ePractice - Joinup. Prieiga per internetą: https://joinup.ec.europa.eu/collection/egovernment/epractice?utm_campaign=epractice&utm_medium=epractice&utm_source=epractice
41. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti Prieiga per internetą: https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=CELEX:32016L1148

42. NATO Cooperative Cyber Defence Centre of Excellence National Cyber Security Framework Manual 2012 m. Prieiga per internetą: https://www.ccdcoe.org/publications/books/NationalCyberSecurityFrameworkManual.pdf
43. Tarptautinės standartizacijos organizacijos standartas ISO/ICE 27032:2012. Prieiga per internetą: https://www.iso.org/standard/44375.html
44. ISA²- Interoperability solutions for public administrations. Prieiga per internetą: https://ec.europa.eu/isa2/solutions/testa_en
45. NIST Prieiga per internetą: https://www.nist.gov/cyberframework
46. LST EN ISO 9001:2015, LST ISO/IEC 27001:2017 Prieiga per internetą: http://www.lsd.lt/index.php?2088203254
47. Europos Sąjungos kibernetinio saugumo agentūra Prieiga per internetą: https://europa.eu/european-union/about-eu/agencies/enisa_lt
48. Securelist. Prieiga per internetą: https://securelist.com/the-cost-of-launching-a-ddos-ttack/77784/
49. EUROPOL Prieiga per internetą: https://www.europol.europa.eu/publications-documents/how-can-ddos-attacks-paralyse-internet
50. VK Prieiga per internetą: https://www.vkontrole.lt/pranesimas_spaudai.aspx?id=23172
51. Štitilis, D. (2013). Kibernetinio saugumo teisinis reguliavimas: kibernetinio saugumo strategijos. *Socialinės technologijos*. 3(1), p. 189–207. Prieiga per internetą: *http://www.mruni.eu/lt/mokslo_darbai/st/paskutinis_numeris/dwn.php?id=351638.*
52. Štitilis, D., Laurinaitis, M. (2009). Tapatybės vagystė elektroninėje erdvėje. *Informacijos mokslai*. P. 240-247. Prieiga per internetą*:* *http://www.zurnalai.vu.lt/informacijosmokslai/article/download/3231/2348.*
53. Štitilis, D., Klišauskas, V. (2012). Elektroninės informacijos saugos reglamentavimas Lietuvoje ir Rusijoje: lyginamieji aspektai. *Socialinės technologijos*. 2(2), p. 441–455. Prieiga per internetą: *www.mruni.eu/en/mokslo_darbai/st/archyvas/dwn.php?id=340100.*
54. Štitilis, D., Paškauskas, Ž. (2007). Valstybės elektroninės informacijos saugos strategija – vienas iš pagrindinių elektroninės informacijos saugos reguliavimo instrumentų: lyginamoji analizė. *Socialinės technologijos.* 2(92); p. 37–45. Prieiga per internetą: *https://www.mruni.eu/en/mokslo_darbai/jurisprudencija/archyvas/dwn.php?id=267948*
55. Europos Audito Rūmų grupė (2019). Prieiga per internetą https://www.eca.europa.eu/lt/Pages/ecadefault.aspx
56. SpringerBriefs in Cybersecurity https://www.springer.com/series/10634
57. FORBES 2020 Prieiga per internetą: https://www.forbes.com/sites/louiscolumbus/2019/06/16/top-10-cybersecurity-companies-to-watch-in-2019/#c8adeef6022c

SANTRAUKA

Nuolatos didėjanti kibernetinių išpuolių gausa privertė šalis imtis veiksmingų prevencinių priemonių norint efektyvios kibernetinės gynybos bei prevencijos. Kibernetinio saugumo aktualumas tapo pagrindiniu klausimu, siekiant apsaugoti nacionalinę šalių kibernetinę erdvę bei informacinius išteklius. Pasaulis priverstas kurti kibernetinio saugumo strategijas bei programas. Šių kibernetinio saugumo strategijų tikslas yra apsaugoti informacinius išteklius, užtikrinti infrastruktūros veiklą esant kritinei situacijai. Didelis dėmesys skiriamas kibernetinio atsparumo didinimui, informacijos ir ryšių technologijų apsaugai, kritinių infrastruktūrų saugumo užtikrinimui.

Pirmame skyriuje, siekiant geriau išanalizuoti teorinius Lietuvos kibernetinio saugumo valdymo aspektus bei raidą, remiantis moksliniais straipsniais, kibernetinį saugumą reglamentuojančiais teisės aktais bei analizuojant kitų šalių praktiką, buvo nagrinėjama Lietuvos institucijų, atsakingų už kibernetinį saugumą veikla, bei kibernetinio saugumo strategijos, programos ir kibernetinio saugumo įstatymo įgyvendinimas.

Antrame skyriuje buvo analizuota kolektyvinės valstybės kibernetinės gynybos ypatumai, veiklos principai, valdymo būdai. Išanalizuotas Lietuvoje jau įdiegtos kolektyvinės kibernetinės gynybos modelio taikymas, valdymo efektyvumas, pagrindinių uždavinių įgyvendinimas. Pateikiama detali kibernetinių atakų analizė, kurią Lietuvoje patiria viešąjį sektorių ginantis Saugusis valstybės duomenų perdavimo tinklas.

Išanalizavus dabartinę situaciją Lietuvoje, paskutiniame skyriuje buvo atliktas kolektyvinės ir individualios gynybos palyginimas, identifikuotos pagrindinės problemos. Apžvelgta Lietuvos kibernetinio saugumo branda bei perspektyvos.

SUMMARY

Constantly increasing abundance of cyber-attacks forced countries to take effective preventive measures in order to achieve efficient cyber defense and prevention. Cyber security relevance became the fundamental question for protecting the national country cyber space and information resources. The world is forced to create cyber security strategies and programs. The goal of cyber security strategies is to protect information resource, ensure the operation of infrastructure in case of a critical situation. Much consideration is given to increasing cyber resilience, protection of information and communication technologies and the assurance of critical infrastructure security.

In the first chapter, in order to better analyze theoretical aspects and development of Lithuanian cyber security management based on scientific articles, cyber security legislation and analysis of other countries' practices, the following was examined: activities of Lithuanian institutions responsible for cyber security and implementation of cyber security strategies, programs and the law on cyber security.

In the second chapter, the following was analyzed: peculiarities of the cyber defense of collective state, principles of activity and management techniques. The application of the collective cyber defense model implemented in Lithuania, management efficiency and implementation of the main tasks was analyzed. A detailed analysis of cyber attacks, which in Lithuania Secure State Data Transmission Network undergoes, is presented.

After analyzing the current situation in Lithuania, in the last chapter a comparison of collective and individual defense was made, the main problems were identified. The maturity and perspectives of Lithuanian cyber security are reviewed.

Forma patvirtinta Mykolo
Romerio universiteto
Senato 2012 m. lapkričio 20 d.
nutarimu Nr.1SN-10

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2020 04 15
Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas), ekonomikos ir verslo fakulteto, kibernetinio saugumo valdymo programos studentas Mindaugas Matulionis, patvirtinu, kad šis magistro baigiamasis darbas

„KOLEKTYVINĖS IR INDIVIDUALIOS KIBERNETINĖS GYNYBOS VIEŠAJAME SEKTORIUJE VERTINIMAS “:

1. Yra atliktas savarankiškai ir sąžiningai;
2. Nebuvo pristatytas ir gintas kitoje mokslo įstaigoje Lietuvoje ar užsienyje;
3. Yra parašytas remiantis akademinio rašymo principais ir susipažinus su rašto darbų metodiniais nurodymais.

Man žinoma, kad už sąžiningos konkurencijos principo pažeidimą – plagijavimą studentas gali būti šalinamas iš Universiteto kaip už akademinės etikos pažeidimą.

Mindaugas Matulionis