VšĮ Investuok Lietuvoje

Regioninio kibernetinės gynybos centro steigimas

Teminio tyrimo

Regioninio kibernetinės gynybos centro poreikio ir pridėtinės vertės Lietuvai nustatymas bei panašios institucinės sąrangos Lietuvoje įstaigų ir tarptautinių bendradarbiavimo platformų organizacinių modelių įvertinimas

ATASKAITA

Gabrielė Bilevičiūtė ir Justas Kidykas

Vilnius

2020

Kuriame Lietuvos ateitį

2014–2020 metų Europos Sąjungos fondų investicijų veiksmų programa

Teminis tyrimas yra parengtas Vyriausybės kanceliarijos įgyvendinamo projekto „Atviros Vyriausybės iniciatyvos“ metu. Projektas finansuojamas Europos socialinio fondo ir Lietuvos Respublikos valstybės biudžeto lėšomis.

Įvadas / Kontekstas

Kibernetinės atakos ir milžiniškos duomenų vagystės vis dažniau atsiduria žiniasklaidos antraštėse. Pasaulio ekonomikos forumo visuotinių grėsmių ataskaitoje yra skelbiama, kad kibernetinių nusikaltimų padaroma žala pasaulinei ekonomikai 2021 m. gali siekti net 6 trilijonus JAV dolerių. Kibernetinių išpuolių nesustabdo sienos, o programišiai nėra lengvai įbauginami: jų atakų taikiklyje gali atsidurti tiek valstybinės institucijos, tiek verslas, tiek bet kuris iš mūsų besinaudojantis bet kokiomis skaitmeninėmis paslaugomis. Dėl to, kibernetinis saugumas nėra tik vieno subjekto ar vienos šalies klausimas, bet rimta problema reikalaujanti glaudaus bendradarbiavimo tarptautiniu mastu.

2020 m. grėsmių nacionaliniam saugumui vertinime pabrėžiama, kad aktyvėjanti priešiškų valstybių kenkėjiška veikla skaitmeninėje erdvėje kelia kibernetinių incidentų riziką Lietuvoje. Akcentuojamos ne tik operacijos susijusios su technine informacinių sistemų žvalgyba, bet ir didėjančios rizikos susijusios su 5G ryšio technologijų pritaikymu viešajame ir privačiajame sektoriuje bei pažeidžiamumų išnaudojimu tiekimo grandinėse. Nors tokio pobūdžio atakų žala Lietuvoje kol kas sąlyginai maža, pasaulinės kibernetinių atakų tendencijos leidžia manyti, kad ateityje šių atakų rizikų poveikis Lietuvos verslui ir šalies kritinei infrastruktūrai augs toliau.

Svarbūs Lietuvos užsienio partneriai gynybos srityje susiduria su tomis pačiomis kibernetinio saugumo problemomis. Jungtinėse Amerikos Valstijose (toliau – JAV), šalies institucijos nuolatos kovoja su bandymais sutrikdyti jos rinkiminius procesus ir kenčia nuo išpirkų reikalaujančių kenkėjiškų virusų (angl. *ransomware*), o verslas sunkiai susidoroja su įsilaužimais, kurių metu yra pasisavinamos jų komercinės paslaptys. Tuo tarpu, kaimynai rytuose susiduria net su rimtesniais incidentais. 2019 m. spalį užsienio programišiai paralyžiavo Sakartvelo valstybines institucijas ir žiniasklaidos priemones siekiant destabilizuoti visuomenę ir kelti sumaištį, o 2016 m. žiemą dalis Ukrainos liko be elektros, kai kibernetinės atakos metu buvo laikinai sutrikdyta elektros skirstymo tinklų veikla. Augantis kibernetinių incidentų skaičius reikalauja tarptautinių pastangų koordinavimo siekiant pasiruošti naujai realijai.

Atsižvelgiant į tai, yra svarbu plėtoti bendradarbiavimą kibernetinio saugumo srityje su Lietuvos strateginiais partneriais, kaip JAV bei įtraukti Rytų partnerystės nares, Ukrainą ir Sakartvelą, nes šios šalys kibernetinio saugumo srityje yra padidintos rizikos zonoje ir patiria didesnį spaudimą. O šiose šalyse pasikartoję scenarijai gali pasikartoti ir Lietuvoje.

Regioninis kibernetinės gynybos centras (RKGC) yra dvišalė Lietuvos ir JAV iniciatyva siekianti sukurti tarptautinį kompetencijų centrą ir pagrindinę bendradarbiavimo platformą regione, suteikiančią galimybę keistis gerosiomis praktikomis kibernetinio saugumo srityje bei dirbti kartu kovojant su bendromis kibernetinėmis grėsmėmis. Šią dieną yra pasiekti politiniai susitarimai dėl Regioninio kibernetinės gynybos centro steigimo, tačiau nėra išanalizuota koks turėtų būti šio Centro juridinis statusas ir veiklos modelis.

Tai yra Lietuvos Respublikos Vyriausybės prioritetinis darbas, įtrauktas Vyriausybės programoje. Vyriausybės programos įgyvendinimo planas:

V PRIORITETAS. Saugi valstybė.

5.2. Kryptis. Kibernetinio ir energetinio saugumo stiprinimas

5.2.1. Darbas. Kibernetinių incidentų prevencija ir valdymo sistemos tobulinimas

Tyrime naudojami analizės metodai:

1. Esamai situacijai įvertinti ir nustatyti Regioninio kibernetinės gynybos centro poreikį ir pridėtinę vertę Lietuvai, atlikta pirminių ir antrinių informacijos šaltinių apžvalga, lyginamoji ir bendrinė jų analizė.
2. Atliktas žvalgomasis tyrimas, kurio metu, atrenkant nagrinėtinus atvejus, analizuojama geroji Lietuvos ir užsienio šalių praktika.

Lietuvos apžvalga

Parengta Lietuvos esamos situacijos analizė atskleidė, kad Regioninis kibernetinės gynybos centras steigimas ir jo vykdomos veiklos prisidėtų prie Lietuvos tarptautinio bendradarbiavimo kibernetinio saugumo srityje stiprinimo, kuris yra būtinas dėl šių priežasčių:

- Kibernetinės grėsmės tampa vis įvairesnėmis bei sudėtingesnėmis, ir vis dažniau nusitaiko į valstybines institucijas, jų demokratinius procesus bei jų vientisumo užtikrinimą. Todėl šalims yra svarbu keistis informacija, stiprinti tarpusavio sąveiką ir dalintis gerosiomis praktikomis šioje srityje.
- Lietuvos kibernetinių grėsmių analizės pajėgumų trūkumas.
- Kibernetiniai incidentai nepaiso valstybių sienų. Vienas apkrėstas kompiuteris greitai gali apkrėsti kitus įrenginius, kituose subjektuose, kitoje šalyje ar net kitame žemyne. Dėl to, yra būtina sukurti patikimas komunikacijos platformas leidžiančias valstybėms keistis informacija ir duomenimis didelio masto ar poveikio incidentų atvejais.
- Dėl tarptautinės teisės aktų, apibrėžiančių kibernetinių operacijų veiksmus, trūkumo, glaudesnis bendradarbiavimas prisideda prie atsakingo valstybių elgesio kibernetinėje erdvėje bei normų ir kultūros kūrimo.
- Tarpvalstybinis bendradarbiavimas mokslinėje srityje leidžia greičiau pasirengti ateities scenarijams bei kurti naujas kibernetinio saugumo priemones.

Nacionalinėje kibernetinio saugumo strategijoje Lietuva yra įsivardinusi būtent tarptautinio bendradarbiavimo stiprinimą, kaip vieną iš pagrindinių kibernetinio saugumo politikos tikslų. Atsižvelgdama į tarpvalstybinį, sienų nepaisantį kibernetinių grėsmių ir rizikų pobūdį, Lietuva siekia stiprinti šalies kibernetinius pajėgumus aktyviai

bendradarbiaujant tiek dvišaliu, tiek daugiašaliu formatais. Iš dalies šį tikslą Lietuva įgyvendina sukūrusi bendras Europos Sąjungos kibernetines greitojo reagavimo pajėgas nuolatinio struktūrizuoto bendradarbiavimo (PESCO) formatu. Tačiau šiais žingsniais strategijos tikslų ir politinių siekių pildymas nesibaigia. Vienas iš iškeltų uždavinių yra dvišalio Lietuvos ir Jungtinių Amerikos Valstijų politinio ir techninio lygmens bendradarbiavimo vystymas kibernetinės gynybos ir saugumo srityje. Taigi, šį tikslą Lietuva galėtų įgyvendinti per RKGC vystydama praktines bendradarbiavimo galimybes su JAV ir Rytų partnerystės šalimis.

Atliktos esamos situacijos analizės metu buvo įvertinta steigiamo RKGC nauda Lietuvai:

- Nuolatinis JAV kibernetinių pajėgų buvimas Lietuvoje;
- Apibrėžta dalijimosi informacija tvarka;
- Politinių pozicijų derinimas dvišalėje patariamojoje taryboje;
- Sukurta mokymų infrastruktūra ir tematinės programos;
- Kibernetinių pajėgų sąveikos (angl. *interoperability*) stiprinimas;
- Sustiprinti kibernetinių grėsmių analizės pajėgumai;
- Atliktos tarptautinės mokslinės galimybių studijos;
- Patobulintos incidentų atpažinimo ir stebėjimo technologijos;
- Atsakingo valstybių elgesio kibernetinėje erdvėje puoselėjimas;
- Lietuvos, kaip regiono kibernetinio saugumo lyderės, pozicijos stiprinimas.

Sėkmingos praktinės daugiašalio bendradarbiavimo platformos sukūrimas prisidėtų prie Lietuvos kibernetinio saugumo būklės stiprinimo ir atsparumo didinimo, kibernetinės gynybos specialistų tobulėjimo ir gebėjimo laiku atpažinti ir užkirsti kelią mūsų regione vykstantiems kibernetiniams incidentams.

Lietuvos ir užsienio šalių geroji praktika

Gerųjų praktikų analizės pirmoje dalyje buvo apžvelgtos šios panašios įstaigos bei institucijos (pagal savo veiklos pobūdį arba savo institucinę sąrangą) Lietuvoje ir tarptautinės dalinimosi informacija organizacijos: *NATO kompetencijų centrų charakteristika, NATO Bendros kibernetinės gynybos kompetencijos centras, NATO Energetinio saugumo kompetencijos centras, Europos kovos su mišriomis grėsmėmis kompetencijos centras, Vyriausybės strateginės analizės centras – STRATA, Branduolinio saugumo kompetencijos centras* ir gautos šios išvados:

- Pirmiausia buvo nustatyta, kad nėra vieno universalaus modelio ir juridinio statuso, kuris tiktų visoms įstaigoms.
- Kaip rodo analizuotas NATO Energetinio saugumo kompetencijos centro pavyzdys ir tai, kad iš pradžių Centras buvo įsteigtas ne kaip tarptautinė organizacija, bet kaip biudžetinė įstaiga prie Užsienio reikalų ministerijos, RKGC juridinis statusas ateityje taip pat galėtų keistis.

- Visi analizėje apžvelgti centrai, kurie yra įsteigti kaip tarptautinės organizacijos, savo struktūroje turi valdančiosios (patariamosios) tarybos organą. Jų veikloje dalyvauja ne tik šalys narės, bet ir įvairų statusą turinčios šalys partnerės (be balsavimo teisės), ES bei NATO atstovai. Tai parodo, kad siekiant užtikrinti šalių įsitraukimą į Centro veiklą yra būtina kiek įmanoma labiau įtraukti partnerius ir išklausyti bei atsižvelgti į jų nuomonę.
- Nagrinėtų įstaigų atveju centrų vadovais yra paskirti šalių, kurioje yra steigiamas centras, tautybės asmuo, dėl to ir RKGC vadovą skirti yra rekomenduojama Lietuvos tautybės.
- Branduolinio saugumo kompetencijos centro atvejis parodė, kad siekiant įsteigti naują specializuotos paskirties „organą" nėra būtinybės kurti atskirą juridinį statusą turinčią įstaigą. Naują darinį galima sukurti ir esamos institucijos ar organizacijos viduje, t.y. struktūrinį padalinį.

Antroje geryjų praktikų analizės dalyje buvo apžvelgtos šios pagrindinės tarpvalstybinės informacijos apie kibernetines grėsmes iniciatyvos ir platformos: *Forum of Incident Response and Security Teams (FIRST), Task Force – CSIRT, APCERT, AfricaCERT, OIC – CERT* ir padarytos šios išvados:

- Reagavimo į incidentus komandų ir kitų kibernetinio saugumo subjektų tarptautinis bendradarbiavimas iki šios dienos dar nėra išnaudojęs savo potencialo.
- Nepaisant didėjančio bendradarbiavimo platformų skaičiaus, pats tarpininkavimas dažniausiai pasireiškia tik organizuojamais sporadiškais susitikimais ir konferencijomis, ruošiamais naujienlaiškiais ar saugumo atmintinėmis, ir pan.
- Tarptautinės CERT centrų bendruomenės daugiau užima *think-tank* organizacijų funkcijas, kuriose yra aktyviai dalijamasi patirtimi ir įžvalgomis, pateikiamos geryjų praktikų gairės CERT centrų veiklai bei formuojama kibernetinio saugumo ir incidentų valdymo ekspertų bendruomenė.
- Apžvelgtos organizacijos pasižymi tuo, kad jos suteikia galimybę skirtingų valstybių ir institucijų atstovams vienoje vietoje aptarti jiems svarbius kibernetinio saugumo klausimus ir pasidalinti savo patirtimi vykdant CERT centrų veiklą bei valdant kibernetinius incidentus.
- RKGC organizacinio modelio steigimo procese svarbu yra atsižvelgti į tarptautinių CERT bendradarbiavimo platformų sėkmės istorijas: kaip nustatyti standartinės veiklos procedūras (angl. *standart operating procedures, SOPs*), kokias būdais stiprinti partnerių tarpusavio pasitikėjimą, ir, paprasčiausiai, kaip peržengti galimus politinius, kultūrinius bei socialinius barjerus siekiant užtikrinti sėkmingą komandinį darbą.

Apžvelgus užsienio ir Lietuvos geraąsias praktikas galima teigti, kad Lietuvoje steigiamas RKGC išsiskirs tuo, kad jo pagrindu bus sukurtas ne tik naujas, tarpusavio pasitikėjimu paremtas, informacijos apsikeitimo mechanizmas, bet ir tuo, kad turės vietoje dirbančią tarptautinę kibernetinių grėsmių analizės komandą. Sėkmingai ir tinkamai atlikus paruošiamuosius darbus, RKGC ženkliai prisidės prie Lietuvos kibernetinių

pajėgumų stiprinimo bei bendradarbiavimo su strateginiais partneriais glaudinimo, ir suteiks mums naujų įrankių leidžiančių geriau pasiruošti ateities grėsmėms.

Svarbu pažymėti, kad tiek pirmoje, tiek antroje dalyje atlikta gerųjų praktikų analizė remiasi tik viešai prieinama informacija, kurios nėra pakankama norint objektyviai atsakyti į papildomai iškilusius klausimus dėl dalijimosi informacija apimties ir vidinių organizacinių veiklos principų.

Viešosios konsultacijos poreikis

Šis tyrimas atskleidė viešosios konsultacijos poreikį. Kadangi problema yra specifinė ir reikalaujanti tikslinės auditorijos nuomonės, galima organizuoti viešąją konsultaciją. Viešosios konsultacijos ciklo tikslas – išgirsti tikslinių auditorijų nuomonę siekiant nustatyti, koks juridinis statusas ir organizacinis modelis būtų tinkamiausias steigiamam RKGC.

Šios konsultacijos uždaviniai:
1) Įvertinti, kokie yra skirtingų juridinių statusų privalumai ir trūkumai.
2) Nustatyti, koks juridinis statusas būtų tinkamiausias RKGC.
3) Įvertinti, kokie yra skirtingų įstaigų / centrų veiklos modelių privalumai ir trūkumai.
4) Nustatyti, koks organizacinis modelis būtų efektyviausias RKGC veikloms užtikrinti.
5) Pasiruošti susitarimo memorandumų pasirašymui su RKGC partneriais.

Šiuos tikslus pasiekti būtų tikslinga vykdant pusiau struktūruotų interviu ciklą su teisininkais ir atstovais iš skirtingą juridinį statusą turinčių įstaigų bei panašaus tipo Lietuvoje ir užsienyje veikiančių centrų. Apie vykdomą interviu ciklą paskelbta „e. pilietis“ internetinėje platformoje siekiant padidinti visuomenes dalyvavimo viešajame valdyme veiksmingumą, plėsti informacijos apie Vyriausybės vykdomą veiklą ir visuomenės įtraukimo į sprendimų priėmimą priemones prieinamumą.

Suinteresuotosios šalys:

<u>Teisininkai iš šių įstaigų:</u>
- Krašto apsaugos ministerijos Teisės departamento, Tarptautinių ryšių ir operacijų grupės, Kibernetinio saugumo ir informacinių technologijų politikos grupės. Atstovai iš Krašto apsaugos ministerijos Personalo analizės ir planavimo skyriaus.
- Vyriausybės strateginės analizės centras.
- Valstybės valdymo koordinavimo centras.
- Nepriklausoma teisininkė.

<u>Atstovai iš šių skirtingą juridinį statusą turinčių įstaigų bei panašaus tipo Lietuvoje ir užsienyje veikiančių centrų:</u>
- NATO Energetinio saugumo kompetencijos centras.
- Suomijos Europos atsparumo hibridinėms grėsmėms kompetencijos centras.
- Vyriausybės strateginės analizės centras.

- Branduolinio saugumo kompetencijos centras.
- Valstybės valdymo koordinavimo centras.

Priedai

Regioninis kibernetinės gynybos centras: Tarptautinis bendradarbiavimas kibernetinio saugumo srityje. http://kurklt.lt/wp-content/uploads/2020/04/RKGC-esamoji.pdf

Regioninio kibernetinės gynybos centro steigimas: Lietuvos ir užsienio gerųjų praktikų analizė. http://kurklt.lt/wp-content/uploads/2020/05/RKGC-antroji-gair%C4%97.pdf