VšĮ „Investuok Lietuvoje“

Atsakingas kibernetinio saugumo spragų atskleidimas

Teminio tyrimo

Atsakingo kibernetinio saugumo spragų atskleidimo poreikis Lietuvoje ir taikymas užsienyje

ATASKAITA

Žygimantas Tamošauskas

Vilnius

2019

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

Šiuo metu Lietuvoje nėra įteisintos atsakingo viešojo ir privataus sektorių informacijos ir ryšių technologijų (IRT) saugumo spragų atskleidimo praktikos. Tai reiškia, kad saugumo spragą suradusiam ir norinčiam ją ištaisyti asmeniui nėra galimybių bendradarbiauti su organizacijoms, kurių IRT saugumo spraga buvo atskleista. Dėl atsakingo saugumo spragų atskleidimo praktikos trūkumo, identifikuotos spragos neretai lieka neatskleistos, o jas suradę kibernetinio saugumo tyrėjai rizikuoja užsitraukti administracinę arba baudžiamąją atsakomybę. IRT saugumo spragų atskleidimo tvarkos atsiradimas ne tik apsaugotų kibernetinio saugumo subjektus nuo kibernetinio saugumo spragų galimos žalos arba ją ženkliai sumažintų, bet ir prisidėtų prie visapusės kibernetinio saugumo brandos augimo Lietuvoje.

Kibernetinio saugumo spragų atskleidimas yra Krašto apsaugos ministerijos prioritetinis darbas. Nacionalinėje kibernetinio saugumo strategijoje, patvirtintoje Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ nustatytas atsakingo kibernetinio saugumo spragų atskleidimo praktikos poreikis. Strategijos 37 punkte nurodoma, kad „siekiant atsakingumo atskleidžiant IRT saugumo spragas, svarbu sudaryti galimybę saugumo spragą suradusiam ir norinčiam ją ištaisyti asmeniui bendradarbiauti su kibernetinio saugumo subjektais, kurių IRT saugumo spraga buvo atskleista. Kibernetinio saugumo subjektai, nustatę ir viešai paskelbę IRT saugumo spragų atskleidimo tvarką, apsisaugotų nuo kibernetinių incidentų galimos žalos arba ją labai sumažintų. IRT saugumo spragų atskleidimo tvarkos nustatymas ir viešas paskelbimas prisidėtų prie valstybės kibernetinio saugumo užtikrinimo ir sudarytų daugiau viešojo ir privataus sektorių bendradarbiavimo galimybių“. Strategijos 38.3 punkte teigiama, kad atsakinga viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktika bus kuriama „inicijuojant atsakingą viešojo ir privataus sektorių IRT spragų atskleidimo praktiką, nustatant šios srities veiklos principus, metodų, techninių gebėjimų ar kitų priemonių taikymo tvarką.“

Tai yra Lietuvos Respublikos Vyriausybės prioritetinis darbas, įtvirtintas Vyriausybės programoje. Vyriausybės programos įgyvendinimo plane minimas šis darbas:

- 5.2.1. Darbas. Kibernetinių incidentų prevencija ir valdymo sistemos tobulinimas

Tai yra Lietuvos Respublikos Seimo prioritetinis darbas – Nacionalinio saugumo strategijoje, patvirtintoje Seimo 2002 m. gegužės 28 d. nutarimu Nr. IX-907 „Dėl nacionalinio saugumo strategijos patvirtinimo" buvo nustatytas šis Lietuvos Respublikos nacionalinio saugumo politikos prioritetas:

- 18.16. kibernetinio saugumo stiprinimas. Siekdama visapusiškai stiprinti nacionalinės kibernetinės erdvės saugumą.

Tyrime naudojami analizės metodai:

1. Esamai situacijai nustatyti ir įvertinti atsakingo atskleidimo praktikos Lietuvoje poreikį bei įteisinimo galimybes, atlikta pirminių ir antrinių informacijos šaltinių (Lietuvos ir

Europos Sąjungos teisės aktų, populiarių ir mokslinių straipsnių) apžvalga, lyginimas tarpusavyje ir bendrinė jų analizė.

2. Atliktas žvalgomasis tyrimas, kurio metu, atrenkant nagrinėtinus atvejus, analizuojama geroji užsienio šalių ir tarptautinių kompanijų praktika. Šalys ir kompanijos: Nyderlandai, Jungtinės Amerikos Valstijos, Latvija ir kompanija „HackerOne.“

Lietuvos apžvalga

Lietuvos esamos situacijos analizė atskleidė, kad nepaisant numatomo kibernetinio saugumo specialistų trūkumo, Lietuvos Respublikos teisės aktuose nėra formalaus atsakingo kibernetinio saugumo spragų atskleidimo apibrėžimo. Šalyje atsakingo atskleidimo praktikos naudojimas nėra paplitęs, o spragas aptikę ir norintys apie jas pranešti asmenys nėra tikri, ar jų atrasta spraga bus pašalinta, bei susiduria su neužtikrintumu dėl savo teisinės padėties:

- Didėjant specialistų trūkumui, būtinas platesnis visuomenes įtraukimas į kibernetinio saugumo spragų aptikimo procesus. Atsakingo kibernetinio saugumo spragų atskleidimo praktikos atsiradimas Lietuvoje galėtų tapti kertiniu žingsniu link platesnio viešojo ir privataus sektorių bendradarbiavimo spragų valdymo srityje.
- Lietuvių kalba atliekant paieškas, susijusias su atsakingo atskleidimo praktika, internetinių paieškos variklio pagalba, matomi tik pavieniai rezultatai, o Lietuvoje savo veiklą vykdančios ir atsakingo atskleidimo tvarką taikančios organizacijos dažniausiai tokią tvarką viešina ne lietuvių kalba.
- Dėl reglamentavimo ir rekomendacijų trūkumo, atsakingo kibernetinio saugumo spragų atskleidimo tvarką Lietuvoje viešina tik septynios privataus ir viešojo sektorių organizacijos.
- Pranešti apie aptiktas kibernetinio saugumo spragas visuomenę skatina ir Lietuvos Nacionalinis kibernetinio saugumo centras, kuris savo internetiniame portale viešina pranešimo apie spragą formą, tačiau nepublikuoja atsakingo atskleidimo tvarkos, detaliai paaiškinančios institucijos įsipareigojimus ir apie spragą pranešusio asmens teises ir pareigas.
- Kibernetinį saugumą Lietuvoje reglamentuoja platus spektras nacionalinių ir tarptautinių teisės aktų, tačiau atlikus jų detalią apžvalgą, buvo nustatyta, kad atsakingo spragų atskleidimo praktikai ypatingai aktualūs septyni teisės aktai, iš kurių trys nacionaliniai ir keturi tarptautiniai:
    1. Kibernetinio saugumo įstatymas
    2. Vyriausybės nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo
    3. Baudžiamasis kodeksas
    4. Bendras Komunikatas Europos Parlamentui ir Tarybai „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“

5. Bendras komunikatas Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“
6. ES direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR
7. Bendrasis duomenų apsaugos reglamentas

Identifikuotos galimybės įteisinti atsakingo atskleidimo praktiką:

- Papildžius šiuo metu galiojantį Kibernetinio saugumo įstatymą sąvokomis, apibrėžiančiomis atsakingą atskleidimą ir kibernetinio saugumo spragą, būtų padėtas pagrindas atsakingo atskleidimo praktikos Lietuvoje įteisinimui.
- Papildžius Kibernetinio saugumo įstatymo 16 straipsnį formuluotėmis, suteikiančiomis asmenims galimybę pranešti apie kibernetinio saugumo spragas ne tik jų, bet ir trečiųjų šalių valdomose ryšių ir informacinėse sistemose, bei parengus technologiškai neutralų šio pranešimo proceso aprašymą poįstatyminiuose Kibernetinio saugumo įstatymo aktuose, Lietuvoje būtų pasiektas atsakingo atskleidimo praktikos įteisinimas.

- Nors Lietuvos Respublikos baudžiamasis kodeksas numato bausmes už veiksmus, tiesiogiai susijusius su atsakingo atskleidimo praktika, svarbu atkreipti dėmesį į šio kodekso XXX skyriuje nusikalstamą veiklą sąlygojančią „neteisėtumo“ sąvoką. Su atsakingo atskleidimo procesais susiję veiksmai, kurie šiuo metu galėtų užtraukti baudžiamąją atsakomybę būtų laikomi teisėtais jeigu: nustatoma, kad spragą aptikęs asmuo laikėsi Kibernetinio saugumo įstatyme ir jo poįstatyminiuose aktuose nustatytos tvarkos ir sąlygų arba sistemos valdytojas, kurio sistemoje buvo aptikta spraga, viešina tai sistemai taikomą atsakingo atskleidimo tvarką.

Užsienio geroji praktika

- Remiantis geroja praktika užsienio valstybėse, išskiriami, Nyderlandų, Jungtinių Amerikos Valstijų, Latvijos ir kibernetines saugumo paslaugas teikiančių tarptautinių kompanijų atvejai:
  - Nyderlandai: 2013 m. Nyderlandų saugumo ir teisingumo ministerija savo šalies parlamentui pateikė Atsakingo atskleidimo praktikos kūrimo strategiją. Dokumente buvo pateiktos atsakingo kibernetinio saugumo (toliau – KS) spragų atskleidimo praktikos kūrimo gairės ir aprašyti kertiniai atsakingo atskleidimo tvarkos elementai. Strategija buvo paruošta ministerijai konsultuojantis su pranešėjais apie KS incidentus bei viešojo ir privataus sektorių organizacijomis. Nyderlandų Nacionalinis Kibernetinio saugumo centras 2018 m. spalio mėn. paviešino Koordinuoto spragų atskleidimo gaires. Centro vadovybės teigimu, atnaujintose gairėse atsispindi nuo 2013 m. strategijos paviešinimo įsisavintos pamokos. Nyderlandų prokuratūra viešina, jos veiklos kryptis atskleidžiantį, kreipimąsi į visuomenę, kuriame teigiama, kad, teisinių veiksmų prieš asmenį, pranešusį apie KS spragą, imamasi tik įvertinus su atsakingo atskleidimo praktika susijusias aplinkybes.

- Jungtinės Amerikos Valstijos: „Įsilaužimas į Pentagoną“ buvo pirmoji Jungtinių Valstijų gynybos departamento organizuojama tokio tipo iniciatyva skirta suteikti „etiniams hakeriams“ (kibernetinio saugumo spragų ieškantiems asmenims) galimybę prisidėti prie visuomenei prieinamų Pentagono sistemų saugumo užtikrinimo. Iniciatyvos rėmuose teisėtai pamėginti įveikti Pentagono kompiuterinių sistemų apsaugą galėjo specialią biografijos patikrą perėję JAV piliečiai. 24 dienas trukusios pilotinės iniciatyvos metu, buvo identifikuotos 138 KS spragos. Pentagono skaitmeninės gynybos tarybos atstovai šį rezultatą įvertino kaip „viršijantį visus lūkesčius,“ todėl buvo nuspręstą tokio pobūdžio KS spragų paieškas Gynybos departamente taikyti plačiau. Po sėkmingos „įsilaužimo į Pentagoną“ baigties, JAV gynybos departamentas paviešino oficialią spragų atskleidimo tvarką. Nuo 2016 m. lapkričio mėn., kai departamentas paviešino minėtąją tvarką, nustatančią atsakingo atskleidimo taisykles, daugiau nei 600 KS tyrėjų atsakingai pranešė apie beveik 3000 KS spragų, iš kurių net 100 buvo pripažintos „kritinės reikšmės.“ Jungtinėse Valstijose šiuo metu yra keturi įstatymo projektai susiję su atsakingo KS spragų atskleidimo praktikos įteisinimu. Vienas iš jų, SAUGIŲ technologijų aktas (dokumento Nr. H.R.7327,) jau sulaukė Kongreso bei prezidento patvirtinimo ir tapo galiojančiu. 2017 m. liepos mėnesį JAV teisingumo departamento baudžiamasis padalinys paruošė ir paviešino Spragų atskleidimo programos internetinėms sistemoms gaires (angl. A Framework for a Vulnerability Disclosure Program for Online Systems.) Šiame dokumente buvo nustatyti ir detaliai aprašyti keturi žingsniai, kuriais JAV kibernetinio saugumo subjektai gali vadovautis kurdami savo atsakingo KS spragų atskleidimo programas.

- Latvija: 2016 m. Kovo mėn. Latvijos Krašto apsaugos ministerija sudarė darbo grupę, kurios tikslas buvo įteisinti atsakingo spragų atskleidimo procesą (toliau – ASAP). Darbo grupei buvo keliami du tikslai. Pirmas tikslas: įtraukti atsakingo spragų atskleidimo proceso apibrėžimą į Informacinių sistemų saugumo įstatymą. Antras tikslas: Pakeisti Baudžiamąjį kodeksą suteikiant teisines garantijas asmenims, vykdantiems veiklą pagal nustatytas atsakingo spragų atskleidimo proceso normas. Siekiant Informacinių sistemų saugumo įstatyme apibrėžti atsakingo spragų atskleidimo procesą, buvo atliekamos konsultacijos su Latvijos IT ir ryšių sistemų saugumo ekspertais. Šių konsultacijų metu, buvo identifikuotos penkios ASAP sudedamosios dalys.

- Kibernetines saugumo paslaugas teikiančios tarptautinės kompanijos, tokios kaip „HackerOne,“ „Synack “ ir „Bugcrowd“ grindžia savo verslo modelį „etinių hakerių“ veikla. „HackerOne“ yra privati kompanija vienijanti daugiau nei 200 000 „etinių hakerių“ ir yra viena didžiausių tokio tipo organizacijų pasaulyje. Šios kompanijos pagrindinis tikslas – tarpininkauti tarp viešojo ir privataus sektorių kibernetinio saugumo subjektų ir „etinių hakerių“. Tokių kompanijų atstovai padeda kibernetinio saugumo subjektams parengti organizacijos tikslus atspindinčias spragų atskleidimo tvarkas, registruoja norinčius ieškoti spragų asmenis ir koordinuoja aptiktų spragų atskleidimą ir pašalinimą.

Viešosios konsultacijos poreikis

Šis tyrimas atskleidė viešosios konsultacijos poreikį. Kadangi problema yra kompleksinė, galima taikyti kelis metodus siekiant sužinoti suinteresuotų šalių nuomones ir organizuoti konsultacijų ciklą. Viešosios konsultacijos tikslas – išgirsti tikslinių auditorijų nuomonę dėl atsakingo kibernetinio saugumo spragų atskleidimo įteisinimo Lietuvoje, bei gauti suinteresuotų šalių komentarus, pasiūlymus ir įžvalgas dėl šiuo metu ruošiamo atsakingo kibernetinio saugumo spragų atskleidimo principus, ribas ir tvarką apibrėžiančio dokumento, skirto atsakingo atskleidimo praktikos įteisinimo pagrindimui.

Taip pat, tikslinga vykdyti interviu ciklą bei apskritojo stalo diskusiją su privataus verslo ir akademinės bendruomenės kibernetinio saugumo ekspertais ir tyrėjais, teisėsaugos atstovais, teisininkais, valstybinių institucijų kibernetinio saugumo specialistais ir užsienio šalių institucijų, taikančių atsakingo atskleidimo praktiką, atstovais. Taip būtų siekiama identifikuoti Lietuvos poreikiams labiausiai tinkantį atsakingo atskleidimo praktikos veikimo ir taikymo modelį, išgirsti naujų pasiūlymų dėl asmenų, pranešančių apie kibernetines saugumo spragas, teisinės padėties, bei nustatyti privataus ir viešojo sektorių bendradarbiavimo galimybes kibernetinio saugumo spragų atskleidimo srityje.

Taip pat, svarbu išsiaiškinti atsakingo atskleidimo praktikos poreikį Lietuvoje. Šį tikslą pasiekti būtų tikslinga atliekant privataus sektoriaus subjektų apklausą, kurioje dalyvautų atstovai iš įvairaus dydžio organizacijų, kurių veiklos sritys apima IT sprendimų kūrimą, finansus, elektroninę prekybą, žiniasklaidą, transportą, teisines paslaugas ir kitas su IT arba ryšių technologijų naudojimu susijusias sritis. Apklausos metu jos dalyvių būtų klausiama, kaip jie vertina atsakingo atskleidimo reglamentavimo poreikį, kokią pridėtinę atsakingo atskleidimo vertę jie mato saugant organizacijos informacinį turtą, bei kokių veiksmų imtųsi jų atstovaujamos organizacijos, gavusios parnešimą apie kibernetinio saugumo spragą.

Suinteresuotos šalys:

1) Lietuvos universitetų atstovai iš šių universitetų:
   - Mykolo Romerio universitetas
   - Vilniaus universitetas
   - Kauno Technologijos universitetas
   - Vilniaus Gedimino technikos universitetas
2) Lietuvos teisėsaugos atstovai iš šių institucijų:
   - Lietuvos Respublikos Generalinė prokuratūra
   - Lietuvos kriminalinės policijos biuro Sunkaus ir organizuoto nusikalstamumo 5-oji valdyba
3) Valstybinių institucijų kibernetinio saugumo ir teisės departamentų atstovai:
   - KAM Kibernetinio saugumo ir informacinių technologijų politikos grupė
   - KAM Teisės departamentas
   - VĮ „INFOSTRUKTŪRA"
   - Nacionalinio kibernetinio saugumo centro prie KAM Kibernetinės gynybos departamentas
4) Privataus sektoriaus kibernetinio saugumo specialistai iš šių organizacijų:

- UAB „Visma Lietuva"
- UAB „NRD CS"
- UAB „Solutionlab Production"
- UAB „NCC Group" ir kt. pagal poreikį.

4) Kibernetinio saugumo asocijacijų atstovai:

- Asociacija „ISACA Lietuva"
- Asociacija „INFOBALT"

5) Užsienio šalių (Latvijos, Nyderlandų) institucijų, taikančių atsakingo atskleidimo praktiką, atstovai:

- Latvijos Reagavimo į IT saugumo incidentus institucija – CERT.LV (angl. Information Technology Security Incident Response Institution of the Republic of Latvia)
- Nyderlandų nacionalinis kibernetinio saugumo centras – NCSC.NL (angl. National Cyber Security Centre)
- Nyderlandų Karalystės ambasada Vilniuje