MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VERSLO IR EKONOMIKOS INSTITUTAS

ILONA MAMENIŠKĖ

ATSAKINGO ATSKLEIDIMO PRINCIPO ĮGYVENDINIMO VIEŠAJAME SEKTORIUJE MODELIS

Kibernetinio saugumo valdymo magistro baigiamasis darbas

Vadovas
prof. dr. Marius Laurinaitis

VILNIUS, 2024

MYKOLO ROMERIO UNIVERSITETAS
VIEŠOJO VALDYMO IR VERSLO FAKULTETAS
VERSLO IR EKONOMIKOS INSTITUTAS

ILONA MAMENIŠKĖ

ATSAKINGO ATSKLEIDIMO PRINCIPO ĮGYVENDINIMO VIEŠAJAME SEKTORIUJE MODELIS

Kibernetinio saugumo valdymo magistro baigiamasis darbas
Studijų programa 6211LX066

Vadovas
_____ prof. dr. Marius Laurinaitis
2024 05

Recenzentas
_____
2024 05

Atliko
KSVvmis22-1 gr. stud.
_____ I. Mameniškė
2024-05-02

VILNIUS, 2024

TURINYS

LENTELĖS

PAVEIKSLAI

SANTRUMPOS

BDAR – Bendrasis duomenų apsaugos reglamentas

CCB – Belgijos kibernetinio saugumo centras (anglų k. *the Centre for Cyber Security Belgium*)

CERT – Kompiuterių greitojo reagavimo komanda (anglų k. *the Computer Emergency Response Team*)

CRIST – Kompiuterių saugumo incidentų reagavimo komanda (anglų k., *the Computer Security Incident Response Team*)

CVD – Koordinuotas pažeidžiamumo atskleidimas

ENISA – Europos Sąjungos tinklų ir informacijos apsaugos agentūra

ES – Europos sąjunga

IS – informacinės sistemos

IT – informacinės technologijos

KSĮ – Lietuvos Respublikos kibernetinio saugumo įstatymas

KSS – kibernetinio saugumo subjektas

NCSC-NL – Nyderlandų nacionalinis kibernetinio saugumo centras (anglų k. *the National Cyber Security Centre – Netherlands*)

IRT – informacinės ir ryšių technologijos

NIST – Nacionalinis standartų ir technologijos institutas (anglų k. *the National Institute of Standards and Technology*)

NKSC – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos

ĮVADAS

Temos aktualumas. Kibernetinio ir informacijos saugumo užtikrinimo klausimai buvo svarbūs jau gana seniai, tačiau tik pastaraisiais metais imta plačiau apie tai kalbėti ir diskutuoti. Informacinėms technologijoms sparčiai tobulėjant, verslo bei valstybių viešojo administravimo sektoriaus procesai neišvengiamai persikelia į elektroninę erdvę, todėl kibernetinio saugumo užtikrinimas, siekiant apsaugoti duomenis ir informacinius išteklius, vis dažniau tampa vienu iš prioritetinių klausimų, kadangi kibernetinių incidentų skaičius kasmet didėja tiek Lietuvoje, tiek visame pasaulyje[1].

Kibernetinio saugumo temos svarbos padidėjimui didelės įtakos turėjo ir visą pasaulį paveikusi COVID-19 pandemija, kurios metu dėl taikomų suvaržymų įprastinė gyventojų, įmonių ir įstaigų veikla persikėlė į virtualią erdvę. Kaip teigiama Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) 2020 m. Nacionalinėje kibernetinio saugumo būklės ataskaitoje, Lietuvoje 2020 metais kibernetinių incidentų skaičius padidėjo ketvirtadaliu, o incidentų, susijusių su kenkimo programinės įrangos platinimu, – net 49 proc. Viso to priežastys – ne tik gyvenimo dėl COVID-19 pandemijos perkėlimas į elektroninę erdvę, bet taip pat informacinių ir ryšių technologijų plėtra, sparčiai augantis prie interneto prijungtų išmaniųjų įrenginių skaičius bei kibernetinio saugumo higienos trūkumas[2].

Siekiant stiprinti valstybės kibernetinį saugumą ir sudaryti daugiau viešojo ir privataus sektorių bendradarbiavimo galimybių[3], 2021 m. birželio mėn. buvo priimtos ir įsigaliojo Lietuvos Respublikos kibernetinio saugumo įstatymo (toliau – KSĮ) pataisos[4], kurios įteisino atsakingo ryšių ir informacinių sistemų spragų atskleidimo procesą. Tuometinio Lietuvos Respublikos krašto apsaugos ministro Arvydo Anušausko teigimu, nustačius aiškias sąlygas, kada sistemų spragų galima ieškoti teisėtai ir kaip tinkamai apie jas pranešti, ne tik užkertamas kelias būsimiems kibernetiniams incidentams, bet taip pat ir stiprinama bendra šalies kibernetinė branda[5]. Taigi, priėmus minėtas KSĮ pataisas, buvo įtvirtintas atsakingo ryšių ir informacinių sistemų spragų atskleidimo principas ir sudarytos galimybės teisėtai ieškoti informacinių sistemų

[1] 2020 m. Nacionalinė kibernetinio saugumo būklės ataskaita. Lietuvos Respublikos krašto apsaugos ministerija, p. 7.
[2] *Ibid.*, p. 9.
[3] Nacionalinė kibernetinio saugumo strategija, patvirtinta Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 37 p.
[4] 2021 m. birželio 17 d. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 6, 8, 9, 13 straipsnių, V skyriaus pavadinimo, priedo pakeitimo ir Įstatymo papildymo 17 straipsniu ir VI skyriumi įstatymas Nr. XIV-413.
[5] Lietuvos Respublikos krašto apsaugos ministerijos pranešimas spaudai, „LR Seimas įteisino atsakingą kibernetinių spragų atskleidimą“ [interaktyvus, žiūrėta: 2024-04-29]. Prieiga per internetą: https://kam.lt/lr-seimas-iteisino-atsakinga-kibernetiniu-spragu-atskleidima/.

saugumo spragų, o jas suradusiam bei norinčiam ištaisyti asmeniui bendradarbiauti su kibernetinio saugumo subjektais, kurių ryšių ir informacinėse sistemose spraga buvo aptikta.

Temos naujumas ir ištirtumas. Lietuva yra viena pirmųjų Europos Sąjungos (toliau – ES) šalių, reglamentavusių atsakingo ryšių ir informacinių sistemų spragų atskleidimo principą, tačiau vis dar nėra pakankamai išnagrinėtas jo taikymas Lietuvos viešajame sektoriuje, taip pat nėra ištirtas atsakingo atskleidimo principo veiksmingumas užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą, pasigendama specialistų ir mokslininkų įžvalgų bei rekomendacijų šia tema.

Mokslinė problema. Šio darbo mokslinė problema – kaip atsakingo atskleidimo principo įgyvendinimo modelis įgalintų analizuoti atsakingo atskleidimo principo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą?

Tyrimo objektas – atsakingo atskleidimo principo įgyvendinimas viešajame sektoriuje.

Tyrimo tikslas – išanalizuoti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelį bei įvertinti atsakingo atskleidimo principo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą.

Uždaviniai:

1. Išnagrinėti atsakingo atskleidimo principo įgyvendinimo teorinius aspektus.
2. Išanalizuoti Lietuvos viešojo sektoriaus institucijų atsakingo atskleidimo principo įgyvendinimo praktiką.
3. Identifikuoti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje problematiką.
4. Empiriškai ištirti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelį.

Duomenų rinkimo metodai:

1. Sisteminė mokslinės literatūros (anglų k. *content*) analizė: nagrinėjama esama mokslinė literatūra, susijusi su atsakingo atskleidimo principu, kibernetiniu saugumu ir viešojo sektoriaus institucijomis.
2. Juridinių dokumentų turinio (anglų k. *content*) analizė: nagrinėjami teisės aktai, susiję su kibernetiniu saugumu ir atsakingo atskleidimo principo reglamentavimu Lietuvoje bei atsakingo atskleidimo principo įgyvendinimu viešojo sektoriaus institucijose, – įstatymai, nuostatai ir kiti oficialūs dokumentai.
3. Pusiau struktūrizuotas interviu: interviu metu apklausiami už atsakingo atskleidimo principo įgyvendinimą atsakingi viešojo sektoriaus institucijų darbuotojai.

Duomenų analizės metodai:

1. Kokybinė dokumentų turinio (anglų k. *content*) analizė: išnagrinėjami viešojo sektoriaus organizacijų dokumentai, susiję su atsakingo atskleidimo principo įgyvendinimu.

2. Pusiau struktūrizuoto interviu kokybinė turinio (anglų k. *content*) analizė ir interpretavimas: interviu metu gauti duomenys analizuojami ir interpretuojami, siekiant išskirti svarbiausias tendencijas, susijusias su atsakingo atskleidimo principo įgyvendinimu viešajame sektoriuje.

3. Kokybinė gautų duomenų analizė: tyrimo metu gauti duomenys apibendrinami ir įvertinami, siekiant atsakyti į tyrimo klausimus bei pateikti rekomendacijas.

Darbo struktūra. Darbą sudaro penkios dalys: įvadas, teorinė dalis, empirinė dalis, išvados ir rekomendacijos atsakingo spragų atskleidimo principo įgyvendinimo Lietuvos viešojo sektoriau institucijose gerinimui. Įvadinėje darbo dalyje apžvelgiamas temos aktualumas, naujumas bei ištirtumas, mokslinė problema, iškeliamas darbo tikslas ir uždaviniai, pristatomi darbo metodai. Teorinėje darbo dalyje apžvelgiami reikšmingiausi atsakingo atskleidimo principo istorinės raidos aspektai, atsakingo atskleidimo principo samprata, atsakingo atskleidimo principo įgyvendinimo teorinis modelis bei užsienio šalių – Belgijos ir Nyderlandų – atsakingo atskleidimo principo įgyvendinimo praktika. Antrojoje darbo dalyje pateikiama tyrimo metodologija. Trečiasis skyrius – empirinė dalis, kurioje nagrinėjama atsakingo atskleidimo principo raiška viešajame sektoriuje, šio principo įgyvendinimo problematika, Vilniaus miesto savivaldybės atsakingo spragų atskleidimo programa, analizuojamas atsakingo atskleidimo principo įgyvendinimo šioje viešojo sektoriaus institucijoje modelis bei siekiama pagrįsti atsakingo atskleidimo principo įgyvendinimo veiksmingumą užkrintant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą. Darbo pabaigoje pateikiamos tyrimo rezultatus apibendrinančios išvados ir rekomendacijos, pateikiamas šaltinių sąrašas bei priedai.

Praktinis pritaikomumas. Šio darbo empirinio tyrimo rezultatai gali būti naudingi siekiant atskleisti, kaip Lietuvos viešojo sektoriaus institucijos yra pasirengusios taikyti atsakingo atskleidimo principą, jo įgyvendinimo problematiką, veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą bei formuojant strategijas ir politiką, siekiant stiprinti viešojo sektoriaus kibernetinį saugumą.

1. ATSAKINGO ATSKLEIDIMO PRINCIPO TEORINIAI ASPEKTAI

Atsakingo ryšių ir informacinių sistemų spragų atskleidimo praktika yra kibernetinio saugumo sritis, kuria siekiama identifikuoti ir pašalinti spragas, galinčias kelti grėsmę kibernetiniam saugumui, kuris yra svarbus visuomenės bei organizacijų veiklai. Įgyvendinama atsakingo atskleidimo praktika leidžia organizacijoms laiku sužinoti apie galimas problemas ir imtis veiksmų jų ištaisymui. Atsakingo ryšių ir informacinių sistemų spragų atskleidimo praktika taip pat yra grindžiama principu, kad per anksti atskleidus techninę informaciją apie spragą, puolėjai gali ją išnaudoti.

Šioje darbo dalyje bus apžvelgiami reikšmingiausi atsakingo atskleidimo principo istorinės raidos aspektai, atsakingo atskleidimo principo samprata, atsakingo atskleidimo principo įgyvendinimo teorinis modelis bei užsienio šalių – Belgijos ir Nyderlandų – atsakingo atskleidimo principo įgyvendinimo praktika.

1.1. Atsakingo atskleidimo principo istorinė raida

Diskusijos apie sistemų saugumą ar nesaugumą, jų tobulinimą bei pažeidžiamumo atskleidimą šiuolaikinėje epochoje tęsiasi jau dešimtmečius, o galbūt ir daug ilgiau, jei atsižvelgsime į įvairius pasisakymus šiais klausimais[6]. Šioje darbo dalyje bus apžvelgiami reikšmingiausi atsakingo atskleidimo principo istorinės raidos aspektai.

Šaltkalvis Alfredas Čarlzas Hobbsas – diskusijų apie sistemų pažeidžiamumų atskleidimą pradininkas – 1853 m. parašė „Pradinį traktatą apie spynų konstrukciją“, kuriame atskleidžiama ankstyvoji spynų konstrukcija. Šiame veikale jis pripažino, kad vis dažniau diskutuojama apie spynų saugumą ir (arba) nesaugumą, ir pasisakė už informacijos atskleidimą vardan naujovių: „Išradėjas pagamina spyną, kuri, jo manymu, pasižymės tokiomis ir tokiomis savybėmis, ir savo įsitikinimą paskelbia pasauliui. Jei kiti turi kitokią nuomonę dėl šių savybių, jie gali tai pasakyti; ir sąžiningai vedama diskusija turi duoti naudos visuomenei: diskusija skatina smalsumą, o smalsumas skatina išradimus“[7]. Tai reiškė diskusijų dėl saugumo sprendimų nesaugumo atskleidimo siekiant pagerinti saugumą pradžią[8].

Devintajame dešimtmetyje ankstyvieji kompiuterių išnaudojimo atvejai paskatino JAV vyriausybę bausti blogus veikėjus naujoje ir menkai suprantamoje srityje, kad atgrasytų juos nuo

[6] Kennedy, D. „Exploring Coordinated Disclosure“. 451 Research, 2019, p. 5.
[7] Hobbes, A.C. „Rudimentary Treatise on the Construction of Locks“. London, England: Levey, Robson and Franklyn, Vol. 83, p. 3 [interaktyvus, žiūrėta: 2024-01-21]. Prieiga per internetą: https://books.google.com/books?id=PsUzAQAAMAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.
[8] Pam, T. T.; Meer, H. „History of Vulnerability Disclosure“ [interaktyvus, žiūrėta: 2024-01-21]. Prieiga per internetą: https://duo.com/labs/research/history-of-vulnerability-disclosure.

veiklos. Įstatymų leidėjai į piktavališką elgesį nukreipė JAV kovos su įsilaužimais įstatymą – Kompiuterinio sukčiavimo ir piktnaudžiavimo įstatymą (anglų k. *Computer Fraud and Abuse Act, CFAA*). Šis įstatymas priimtas 1986 m. ir iš dalies pakeistas 1994 bei 1996 m. gali būti taikomas visiems, kurie neteisėtai prisijungia prie kompiuterio, ir už tai numatytos baudžiamosios ir civilinės sankcijos. Šis įstatymas yra prieštaringai vertinamas kibernetinės teisės mokslininkų, o daugelis ankstyvųjų teisminių aiškinimų nustatė labai plačią taikymo sritį, kuri apimtų daug potencialiai naudingų saugumo tyrimų.[9]

1988 m. Kornelio universiteto pirmakursis informatikos magistrantas Robertas Morisas sukūrė ir išleido kirminą (žinomą kaip *Morris worm* arba *Internet worm of November 2, 1988)*, kuris užkrėtė kelis tūkstančius kompiuterių ir tapo žinomas kaip pirmasis didelis virusas, sulaukęs visuotinio dėmesio. Jame buvo pasinaudota keliomis žinomomis pažeidžiamomis vietomis ir silpnais slaptažodžiais. R. Morisas buvo pirmasis nuteistasis pagal 1986 m. Kompiuterinio sukčiavimo ir piktnaudžiavimo įstatymą – jis buvo nuteistas trejiems metams lygtinai bei bauda. Šis incidentas yra ankstyvas tam tikros viešos išnaudojimo galimybių atskleidimo formos pavyzdys – bandymai platinti kirminą yra vienas iš būdų atkreipti dėmesį į tai, kad egzistuoja daugybė pažeidžiamumų.[10]

Šiame kontekste svarbu paminėti „Bugtraq“ elektroninių pašto adresų sąrašą, kuris buvo pradėtas kurti 1993 m. reaguojant į esamus to meto interneto saugumo infrastruktūros trūkumus. „Bugtraq“ tikslas buvo skelbti informaciją apie pažeidžiamumus: skirtingai nei CERT patarimai, kurie suteikė ribotą kiekį techninės informacijos apie pažeidžiamumą, „Bugtraq“ atskleidimai dažnai pateikdavo detalią informaciją, taip pat nuorodas į išnaudojimo kodą[11]. Prieš sukuriant „Bugtraq“, pažeidžiamumas buvo perduodamas tarp artimų įsilaužėlių, programinės įrangos inžinierių ir saugos specialistų. Šios „komercinės paslaptys“ buvo naudojamos tiek gerais, tiek piktavališkais tikslais ir retai sulaukdavo pakankamai viešumos, kad atkreiptų plačiosios visuomenės dėmesį.[12].

1999 m. MITRE korporacija, ne pelno siekianti organizacija, teikianti techninę paramą JAV vyriausybei, sukūrė informacinę sistemą, skirtą iš įvairių šaltinių gautai informacijai apie

[9] „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022, p. 42.
[10] Pam, T. T.; Meer, H. „History of Vulnerability Disclosure“ [interaktyvus, žiūrėta: 2024-01-21]. Prieiga per internetą: https://duo.com/labs/research/history-of-vulnerability-disclosure.
[11] Arora A.; Telang R. „Economics of Software Vulnerability Disclosure“. Economics of Information Security, p. 20 [interaktyvus, žiūrėta: 2024-01-21]. Prieiga per internetą: https://www.heinz.cmu.edu/~rtelang/Economics_of_software_vulnerability_disclosure.pdf.
[12] Shepherd, S. „How do we define Responsible Disclosure?“. SANS Institute, 2003, p. 2 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: 932.pdf (egnyte.com).

pažeidžiamumą integruoti ir tvarkyti centralizuotoje duomenų bazėje[13]. Autoriai siekė sudaryti standartizuotą informacijos apie pažeidžiamumą sąrašą, kuriame[14]:

- būtų išvardyti ir atskirti visi žinomi pažeidžiamumai;
- kiekvienai pažeidžiamai vietai būtų priskirtas standartinis ir unikalus pavadinimas (dėl nuoseklumo);
- egzistuotų nepriklausomai nuo skirtingų požiūrių į tai, kas yra pažeidžiamumas;
- informacija būtų viešai prieinama ir ja būtų galima dalytis be platinimo apribojimų.

Sąvoka „atsakingas atskleidimas“ pradėta vartoti 2001 m., kai „Microsoft" Saugumo reagavimo centro vadovas Scottas Culpas spragų atskleidimą palygino su informacijos anarchija[15]. Straipsnyje „Laikas nutraukti informacinę anarchiją“ S. Clupas metė iššūkį visiško atskleidimo (anglų k. *Full Disclosure*) („informacijos anarchijos“) šalininkams: jis teigė, kad visiškas atskleidimas apginkluoja priešą išsamia technine informacija, kuri vėliau naudojama automatinių atakų įrankių kūrimui ir bet kas apsiginklavęs šiais įrankiais gali pradėti atakas prieš pažeidžiamas sistemas. Tuo tarpu visiško atskleidimo šalininkai teigė, kad jie atskleisdami išnaudojimo kodą motyvuoja administratorius pataisyti savo sistemas. [16]

NIST 2020 m. nustatė atsakingo pažeidžiamumo atskleidimo gaires: NIST buvo pavesta sukurti ataskaitų teikimo, koordinavimo, skelbimo ir informacijos apie saugumo spragas gavimo gaires kaip 2020 m. Daiktų interneto (anglų k. *the Internet of Things, IoT*) kibernetinio saugumo tobulinimo akto dalį. Gairėse aptariama[17]:

- sukurti federalinę pažeidžiamumo atskleidimo sistemą, įskaitant Federalinę koordinavimo įstaigą (anglų k. *the Federal Coordination Body, FCB*) ir pažeidžiamumo atskleidimo programos biurus (anglų k. *the Vulnerability Disclosure Program Office, VDPO*);
- informacijos apie galimą saugumo spragą gavimas informacinėje sistemoje, kuri priklauso valstybinei įstaigai arba yra jos valdoma (įskaitant daiktų interneto įrenginį);
- informacijos apie agentūros valdomos ar kontroliuojamos informacinės sistemos (įskaitant daiktų interneto įrenginį) saugumo pažeidžiamumo pašalinimą skleidimas.

[13] Pam, T. T.; Meer, H. „History of Vulnerability Disclosure“ [interaktyvus, žiūrėta: 2024-01-21]. Prieiga per internetą: https://duo.com/labs/research/history-of-vulnerability-disclosure.
[14] Mann, D. E.; Christey, S. M. „Towards a Common Enumeration of Vulnerabilities“ [interaktyvus, žiūrėta: 2024-01-21]. Prieiga per internetą: https://cve.mitre.org/docs/docs-2000/cerias.html.
[15] Kennedy, D. „Exploring Coordinated Disclosure“. 451 Research, 2019, p. 5.
[16] Shepherd, S. „How do we define Responsible Disclosure?“. SANS Institute, 2003, p. 3 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: 932.pdf (egnyte.com).
[17] Vulnerability Disclosure Guidance. NIST, 2023 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: https://csrc.nist.gov/projects/vdg.

Apibendrinant tai, kas buvo išdėstyta, darytina išvada, jog diskusijos apie atsakingą spragų atskleidimą yra aktualios ir tęsiasi ilgą laiką, o istorinė raida atskleidžia šio principo evoliuciją nuo spynų konstrukcijos iki modernių informacinių sistemų saugumo spragų atskleidimo.

1.2. Atsakingo atskleidimo principo samprata

Pažeidžiamumai – tai kompiuterinių sistemų trūkumai arba klaidos, kuriomis galima pasinaudoti siekiant pažeisti paveiktų sistemų tinklo ir informacijos saugumą. Tai yra įėjimo į sistemą taškas arba vartai, per kuriuos galima išnaudoti sistemą, todėl gali kelti didelę grėsmę saugumui[18].

Pažeidžiamumą gali sukelti programinės įrangos defektai, konfigūracijos ar dizaino sprendimai, netikėta sistemų sąveika arba aplinkos pokyčiai. Informacijos apdorojimo sistemose pažeidžiamumų gali atsirasti jau projektavimo etape ar sistemos diegimo metu[19]. Sėkmingas pažeidžiamumo išnaudojimas gali sukelti techninių padarinių, todėl svarbu nustatyti ir ištaisyti pažeidžiamumus, o pažeidžiamumų atskleidimo procesas yra labai svarbus komponentas, kurio negalima nuvertinti. Pažeidžiamumų atskleidimo procesas yra sudėtingas, jame dalyvauja kelios suinteresuotosios šalys, įskaitant tiekėjus, IT saugumo paslaugų teikėjus, nepriklausomus tyrėjus, žiniasklaidą, piktavalius naudotojus, vyriausybes ir galiausiai plačiąją visuomenę.[20]

NIST siūlo šiuos pažeidžiamumo apibrėžimus[21]:

- „informacinės sistemos, sistemos saugumo procedūrų, vidaus kontrolės ar diegimo trūkumai, kuriuos gali išnaudoti arba suaktyvinti grėsmės šaltinis“;
- „sistemos, programos ar tinklo trūkumas, kuris gali būti išnaudojamas arba netinkamai naudojamas“;
- „informacinės sistemos, sistemos saugumo procedūrų, vidaus kontrolės ar diegimo trūkumai, kuriais galėtų pasinaudoti grėsmės šaltinis“.

Pažeidžiamumo nustatymas gali būti įvairių formų: nuo specialiai nukreipto programinės įrangos testavimo iki paprasto sistemos naudojimo, kai saugumu besirūpinantis asmuo pastebi kokią nors netinkamai veikiančią funkciją. Tam, kad spragos atradimas būtų aktualus atsakingo atskleidimo aspektu, jis turi baigtis pranešimu apie pažeidžiamumą.[22]

Šaltiniuose galima aptikti išskiriamus keturis pažeidžiamumo atskleidimo tipus:

[18] „Good Practice Guide on Vulnerability Disclosure“. ENISA, 2015, p. 7.
[19] Householder, A. D. et al. „The CERT® Guide to Coordinated Vulnerability Disclosure“. Carnegie Mellon University, 2017, p. 2.
[20] „Good Practice Guide on Vulnerability Disclosure“. ENISA, 2015, p. 7.
[21] *Pgl.* Householder, A. D. et al. „The CERT® Guide to Coordinated Vulnerability Disclosure“. Carnegie Mellon University, 2017, p. 2.
[22] Householder, A. D. et al. „The CERT® Guide to Coordinated Vulnerability Disclosure“. Carnegie Mellon University, 2017, p. 3.

1. **Neatskleidimas.** Neatskleidimo politika reiškia, kad informacija apie pažeidžiamumą turi būti griežtai saugoma, jog plačioji visuomenė niekada nesužinotų apie jos egzistavimą. Pavyzdžiui, „juodakepurių“ įsilaužėlių (anglų k. *black-hat hacker*) bendruomenė laikosi neatskleidimo politikos: kai pažeidžiamumą aptinka „juoda skrybėlė“, informaciją saugo tas asmuo arba ji protingai paskirstoma „juodųjų skrybėlių“ grupei. Tada šios „juodos kepurės“ naudoja pažeidžiamumą, kad prasiskverbtų į neapsaugotas sistemas bet kokiam slaptam tikslui, kurio jos nori. Galiausiai pažeidžiamumo informacija nuteka ir paskelbiama viešame forume, tačiau iki šio laiko sistemos ir jų administratoriai neturi jokios apsaugos nuo spragos išnaudojimo.[23]

Kai kurie tiekėjai ir saugos įmonės bando propaguoti neatskleidimo politiką. Jie mano, kad informaciją apie pažeidžiamumą galima kontroliuoti ir bus informuoti tik „patikimi“ asmenys – tokiu būdu jie gali „apsaugoti“ pažeidžiamas sistemas, kol bus galima rasti pataisymą. Manoma, jog pagrindinis šio mąstymo trūkumas yra įsitikinimas, kad informaciją galima kontroliuoti, tačiau nėra jokio būdo užtikrinti, jog pasirinktais asmenimis galima pasitikėti ir jie nenaudos privilegijuotos pažeidžiamumo informacijos savo naudai.[24]

2. **Visiškas atskleidimas.** Visiško atskleidimo atveju visa informacija apie spragą yra paskelbiama viešai. Visiško atskleidimo šalininkai nurodo keletą šios rūšies atskleidimo privalumų: pirma, programinės įrangos tiekėjas yra motyvuotas laiku pateikti pataisą arba sprendimą dėl naujo pažeidžiamumo – jei tai nėra padaroma laiku, atsiranda grėsmė tiekėjo reputacijai bei pajamoms. Be to, siekiant išvengti neigiamos žiniasklaidos dėmesio ateityje, programinės įrangos tiekėjas yra motyvuotas kurti mažiau pažeidžiamus produktus. Antra, visiškai atskleidžiant pažeidžiamumo informaciją pažeidžiamų sistemų administratoriai yra aprūpinti informacija, kuri yra reikalinga imantis atitinkamų gynybinių veiksmų.[25]

3. **Ribotas atskleidimas.** Kaip ir neatskleidimo atveju, pagrindinė riboto atskleidimo koncepcija yra ta, kad informacija apie pažeidžiamumą dalijasi kuo mažiau asmenų – pradiniame atskleidimo etape tik nedidelei grupei asmenų suteikiama prieiga prie visos informacijos apie pažeidžiamumą. Šią grupę sudaro atskleidėjas, tiekėjas ir galbūt trečiosios šalies koordinatorius. Pradiniame viešame atskleidime tik aprašomas gaminys su trūkumais ir pateikiama labai mažai informacijos apie pažeidžiamumą. Riboto atskleidimo atveju net galutinai atskleidžiant spragą nėra pateikiama visa techninė informacija, o paskelbimas vykdomas tik tiekėjui ištaisius trūkumą. Techninės informacijos kiekio ribojimo koncepcija grindžiama įsitikinimu, kad vartotojams, programuotojams ir administratoriams nereikia išsamios techninės informacijos,

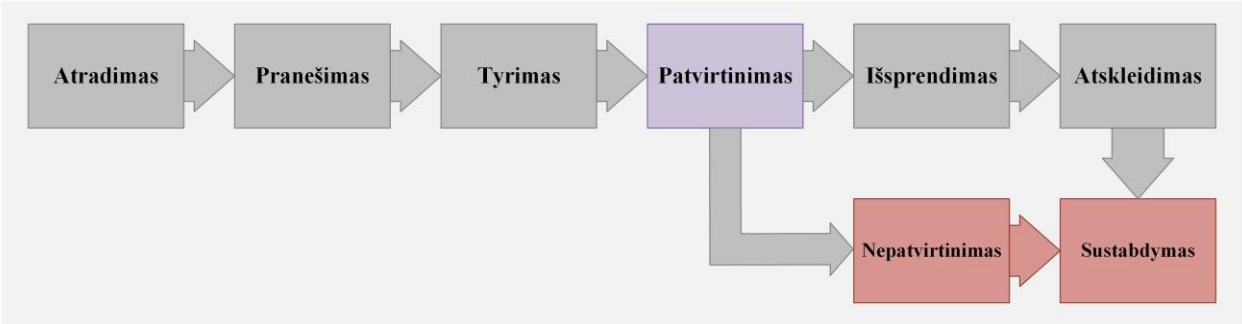
[23] Shepherd, S. „How do we define Responsible Disclosure?“. SANS Institute, 2003, p. 6 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: 932.pdf (egnyte.com).
[24] *Ibid.*
[25] *Ibid.,* p. 7.

kad galėtų pataisyti sistemas. Be to manoma, jog visos techninės informacijos atskleidimas tik padeda „juodųjų skrybėlių“ bendruomenei.[26]

4. **Atsakingas atskleidimas.** Atsakingo atskleidimo pagrindą sudaro įmonių taisyklės ir gairės, leidžiančios asmenims apie aptiktą pažeidžiamumą pranešti tiesiogiai organizacijoms ir nurodančios, kaip tai padaryti. Atsakingo atskleidimo atveju daugumą programinės įrangos spragų paprastai atranda nepiktybiniai vartotojai ar etiški įsilaužėliai (anglų k. *etichal hacker)*.[27]

Pagrindiniai pažeidžiamumo atskleidimo etapai. Nors kiekvienoje organizacijoje (ar nacionalinėje valstybėje) pažeidžiamumo atskleidimo procesas gali skirtis, paprastai jį sudaro šie žingsniai[28]:

1. Pažeidžiamumo aptikimas (pranešėjo, pvz., saugumo tyrėjo, ar darbuotojo);
2. Pranešimas pažeidžiamos sistemos ar programinės įrangos savininkui, gamintojui ar pardavėjui;
3. Savininko, gamintojo ar pardavėjo atliekamas galimo pažeidžiamumo ir jo poveikio tyrimas;
4. Pažeidžiamumo patvirtinimas (arba nepatvirtinimas);
5. Problemos išsprendimas pataisant arba kitaip sumažinant ar pašalinant pažeidžiamumą;
6. Viešas informacijos apie pažeidžiamumą (ir pataisą) atskleidimas.

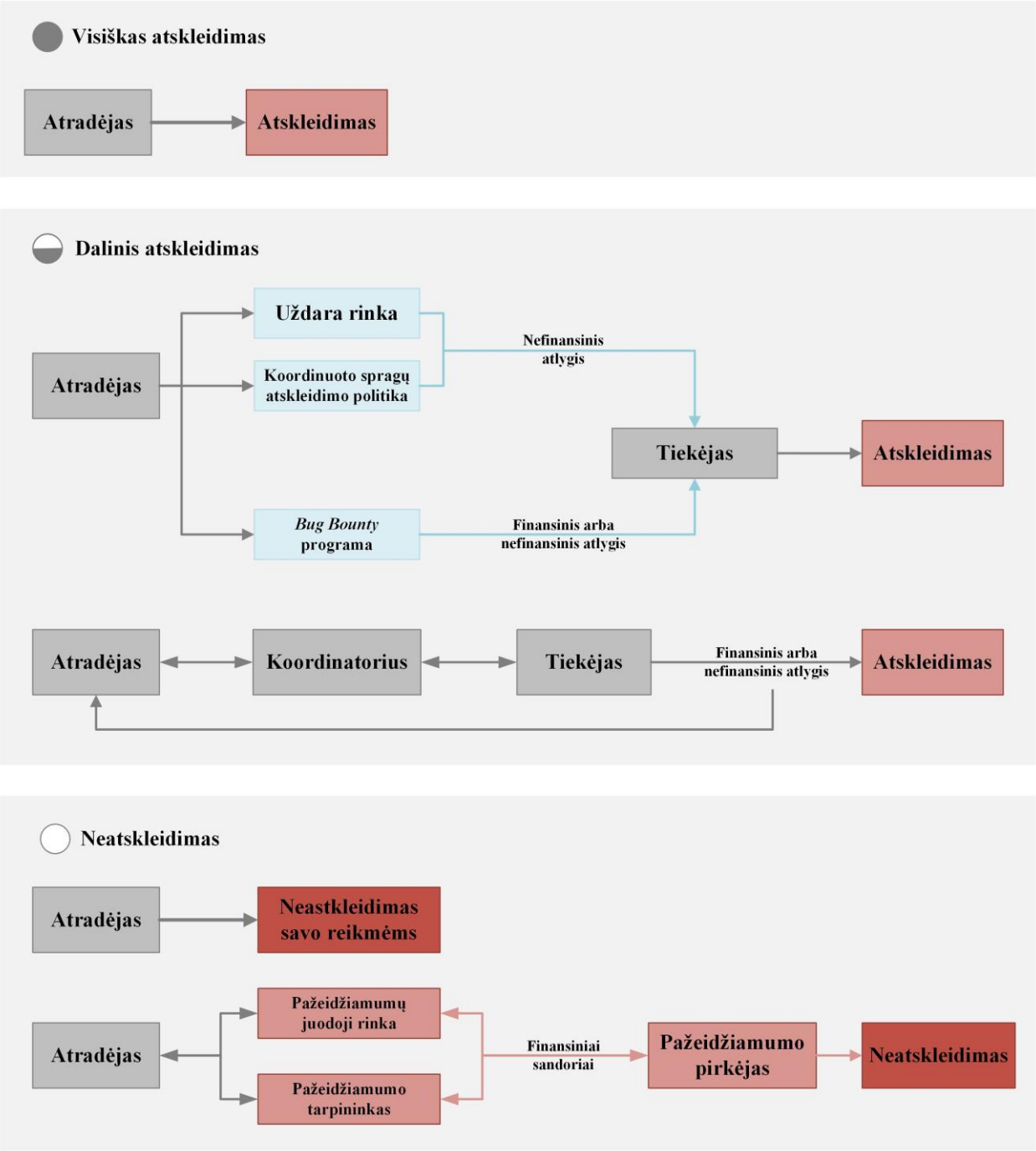


Šaltinis: išversta pagal „GFCE Global Good Practices. Coordinated Vulnerability Disclosure (CVD)“, p. 7

1 pav. **Pagrindiniai pažeidžiamumo atskleidimo etapai**

Žemiau pateikiama aukšto lygio pažeidžiamumo atskleidimo procesų ir srautų apžvalga[29]:

[26] *Ibid.*, p. 8.
[27] Yi Ding, A. et al. „Ethical Hacking for IoT Security: A First Look into Bug Bounty Programs and Responsible Disclosure“. ICTRS 2019 - Proceedings of the 8th International Conference on Telecommunications and Remote Sensing, 2019, p. 4.
[28] „GFCE Global Good Practices. Coordinated Vulnerability Disclosure (CVD)“. Global Forum on Cyber Expertise, 2017, p. 7.
[29] „Economics of vulnerability disclosure“. ENISA, 2018, p. 13.



Šaltinis: išversta pagal „Economics of vulnerability disclosure“, p. 13
2 pav. **Aukšto lygio pažeidžiamumo atskleidimo procesų ir srautų apžvalga**

Atkreiptinas dėmesys į tai, kad anksčiau literatūroje, moksliniuose šaltiniuose bei straipsniuose buvo vartojama sąvoka „atsakingas atskleidimas“, kuri tuo metu buvo įprastas šios praktikos terminas. Vėliau tapo aišku, kad šiuo terminu per daug pabrėžiama pranešančiosios šalies atsakomybė, nors pagrindinis principas yra tas, jog pranešančioji šalis ir potencialiai pažeidžiama organizacija turėtų būti lygiaverčiai dialogo partneriai. Šią nuostatą geriau atspindi šiuo metu plačiai vartojamas terminas „koordinuotas pažeidžiamumo atskleidimas“ (anglų k.

Coordinated Vulnerability Disclosure, CVD).[30] Koordinuotas pažeidžiamumo atskleidimas – tai informacijos rinkimas iš pažeidžiamumą radusių asmenų, atitinkamų suinteresuotųjų šalių dalijimosi ta informacija koordinavimas ir programinės įrangos pažeidžiamumų buvimas bei jų mažinimo atskleidimas įvairioms suinteresuotosioms šalims, įskaitant visuomenę[31].

ISO/IEC 29147 standartas pažeidžiamumo atskleidimą apibrėžia taip[32]:

- „pažeidžiamumo atskleidimas yra procesas, kurio metu tiekėjai ir pažeidžiamumo ieškantys asmenys gali bendradarbiauti ieškodami sprendimų, kurie sumažintų su pažeidžiamumu susijusią riziką“;
- „tai apima tokius veiksmus kaip informacijos apie pažeidžiamumą ir jo pašalinimą teikimas, koordinavimas ir skelbimas“;
- „pažeidžiamumo atskleidimo tikslai yra šie: a) užtikrinti, kad būtų pašalintas nustatytas pažeidžiamumas; b) pažeidžiamumų keliamos rizikos sumažinimas; c) suteikti vartotojams pakankamai informacijos, kad būtų galima įvertinti jų sistemų pažeidžiamumo riziką“.

Pažeidžiamumo atskleidimo procese yra keturios pagrindinės dalyvių grupės[33]:

1. Programinės įrangos, techninės įrangos ir paslaugų naudotojai, kurie gali būti pavieniai asmenys, organizacijos arba vyriausybės;

2. Pardavėjai, kuriuos sudaro programinės įrangos, techninės įrangos ir paslaugų kūrėjai, gamintojai ir tiekėjai. Tai taip pat gali būti vadinamieji „tarpiniai pardavėjai“, kurie sudaro konkretaus produkto ar paslaugos tiekimo grandinę;

3. Ieškotojai, kurie sudaro asmenų, nustatančių ir pranešančių apie pažeidžiamumus, bendruomenę. Ieškotojai kartais dar vadinami atradėjais, pranešėjais arba tyrėjais;

4. Koordinatoriai – tai patikimos organizacijos, kurios tarpininkauja tarp ieškotojų ir pardavėjų, siekdamos užtikrinti, kad pažeidžiamumai būtų atskleisti ir atsakingai sumažinti. Gerai žinomi koordinatoriai yra kompiuterinių incidentų tyrimo ir reagavimo į ekstremalias situacijas grupės (CERT), pvz., JAV CERT koordinavimo centras (CERT/CC), Suomijos CERT (CERT-FI) ir Japonijos CERT (JP-CERT).

Be to, yra nemažai antrinių veikėjų, netiesiogiai dalyvaujančių pažeidžiamumų atskleidimo procese, įskaitant vyriausybes, žiniasklaidą ir priešiškai nusiteikusius veikėjus[34]:

[30] „Coordinated Vulnerability Disclosure: the Guideline“. NCSC, 2018, p. 5.
[31] Householder, A. D. et al. „The CERT® Guide to Coordinated Vulnerability Disclosure“. Carnegie Mellon University, 2017, p. 3.
[32] *Pgl.* Householder, A. D. et al. „The CERT® Guide to Coordinated Vulnerability Disclosure“. Carnegie Mellon University, 2017, p. 3.
[33] „Economics of vulnerability disclosure“. ENISA, 2018, p. 10.
[34] *Ibid.*

1. Vyriausybės vaidina sudėtingą vaidmenį pažeidžiamumo atskleidimo procese. Jos gali būti pažeidžiamumų ieškotojos, pardavėjos ir koordinatorės, taip pat gali įsigyti arba saugoti pažeidžiamumus nacionalinio saugumo tikslais. Vyriausybės taip pat rengia teisės aktus ir reglamentus, kurie gali turėti įtakos pažeidžiamumų atskleidimui.

2. Žiniasklaida praneša apie pažeidžiamumus ir dalyvauja skleidžiant informaciją apie juos.

3. Priešiški veikėjai, pvz., organizuoti nusikaltėliai ar kiti priešininkai, gali pasinaudoti pažeidžiamumais arba įsitraukti į pažeidžiamumų atskleidimo procesą siekdami nedorų tikslų.

Pažymėtina, jog pažeidžiamumo atskleidimas yra tarp dviejų kraštutinumų[35]:

1. Kai tik sužinosite, atskleiskite visiems viską, ką žinote apie pažeidžiamumą;

2. Niekada niekam neatskleiskite nieko, ką žinote apie pažeidžiamumą.

Pažeidžiamumo atskleidimo praktikos tyrimai parodė, kad nė vienas iš aukščiau pateiktų požiūrių nėra socialiai optimalus[36]. Manoma, kad būtent koordinuoto pažeidžiamumo atskleidimo procesas užtikrina pagrįstą šių konkuruojančių interesų pusiausvyrą. Visuomenė ir ypač pažeidžiamų produktų naudotojai nusipelno būti informuoti apie su tais produktais susijusias problemas ir apie tai, kaip pardavėjas sprendžia šias problemas. Tuo pačiu metu tokios informacijos atskleidimas be peržiūros ir švelninimo tik atveria visuomenei galimybę ją išnaudoti. Idealus scenarijus įvyksta tada, kai visos atsakingos šalys procesą koordinuoja ir bendradarbiauja, kad apsaugotų visuomenę. Šis koordinavimas taip pat gali būti paverstas viešųjų ryšių laimėjimu tiekėjui greitai sprendžiant problemą ir taip išvengiant blogo spaudos dėmesio dėl nepasiruošimo.[37]

Šiame kontekste taip pat svarbu paminėti tai, jog, teisės srities mokslininkų nuomone, atsakingo atskleidimo procesas kelia diskusijų dėl pažeidžiamumų atradėjų veiksmų teisėtumo ir teisinės atsakomybės jiems taikymo. Pažymėtina, jog atsakingo informacijos atskleidimo politika, vertinant teisiniu požiūriu, yra pilkoji zona, balansuojanti tarp teisėtumo ir neteisėtumo – kartais ši riba būna gana neryški. Nė vienas tarptautiniu mastu privalomas teisės aktas neįpareigoja valstybių įgyvendinti tam tikras teisės normas, įteisinančias atsakingo atskleidimo politiką, todėl kartais įsilaužimų teisėtumo ar neteisėtumo vertinimas priklauso nuo asmens, kuris turi teisę inicijuoti baudžiamąjį procesą[38].

[35] *Pgl.* Householder, A. D. et al. „The CERT® Guide to Coordinated Vulnerability Disclosure“. Carnegie Mellon University, 2017, p. 6.
[36] *Ibid,*
[37] Householder, A. D. et al. „The CERT® Guide to Coordinated Vulnerability Disclosure“. Carnegie Mellon University, 2017, p. 7.
[38] Ķinis, U., From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach. Computer Law & Security Review, 2018.34(3), 2018, p. 7.

Teisinės diskusijos dėl atsakingo atskleidimo proceso prasidėjo 2005 m., kai interneto apsaugos sistemų darbuotojas Michaelas Lynnas rado „Cisco“ interneto maršrutizatorių pažeidžiamumą, galintį rimtai paveikti interneto infrastruktūrą, ir apie atrastą pažeidžiamumą turėjo kalbėti Nevados „Black Hat“ konferencijoje, tačiau dėl „Cisco“ spaudimo organizatoriai atšaukė M. Lynno pranešimą. Be to, „Cisco“ padavė M. Lynn į teismą: „Cisco“ teigė, kad M. Lynnas pažeidė kelis įstatymus, įskaitant autorių teisių pažeidimą ir komercinių paslapčių atskleidimą. Profesorius J. S. Granickas, kuris šioje byloje buvo gynybos advokatas, pateikė išsamią teisinę analizę, susijusią su atskleidimo proceso teisinėmis pasekmėmis[39].

Vėlesniais metais teisės srities mokslininkai daugiau dėmesio skyrė atsakingo atskleidimo terminui ir turiniui bei jo atitikčiai žmogaus teisėms, pvz., ar visiškas viešas pažeidžiamumo atskleidimas, įskaitant instrukcijas, kaip taisyti pažeidžiamumą, turėtų būti apsaugotas pagal saviraiškos laisvę[40]. Kai kurie autoriai informaciją, kurią nepriklausomas tyrėjas gavo atradęs pažeidžiamumą, vertino kaip autorių teises[41].

Taigi, apibendrinus tai, kas buvo išdėstyta, darytina išvada, kad pažeidžiamumo atskleidimas yra procesas, kurio metu informacija apie pažeidžiamumą – idealiu atveju su patarimais, kaip jį sumažinti ar pataisyti – perduodama gaminio vartotojams ir apskritai plačiajai visuomenei, tačiau kai kuriais atvejais šis procesas kelia diskusijų dėl pažeidžiamumų atradėjų veiksmų teisėtumo ir teisinės atsakomybės jiems taikymo.

Lietuva. 2021 m. birželio mėnesį Lietuvoje buvo priimtos ir įsigaliojo KSĮ pataisos, kurios įtvirtino atsakingo ryšių ir informacinių sistemų spragų atskleidimo principą. Iki KSĮ papildymo 17-uoju straipsniu Lietuvoje atsakingo spragų atskleidimo procesas nebuvo reglamentuotas, tad įstatymais nebuvo apibrėžta informacijos ir ryšių technologijų saugumo spragų atskleidimo praktika.

Atsakingo ryšių ir informacinės sistemos spragų atskleidimo proceso reglamentavimo nebūvimas kėlė sunkumų asmenims, surasdavusiems spragą ir norintiems ją ištaisyti ar apie ją pranešti, nes nebuvo sudarytos sąlygos bendradarbiauti su įstaigomis, kurių sistemose spraga būdavo surasta. Taip pat dėl šios priežasties identifikuotos spragos dažnai likdavo neatskleistos, o jas atradę asmenys rizikuodavo užsitraukti administracinę ar net baudžiamąją atsakomybę. Reglamentuojant atsakingo spragų atskleidimo procesą buvo siekiama apsaugoti kibernetinio

[39] *Ibid.*, p. 2.
[40] *Pgl.* Ķinis, U., From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach. Computer Law & Security Review, 2018.34(3), 2018, p. 2.
[41] *Ibid.*

saugumo subjektus nuo kibernetinio saugumo spragų galimos žalos arba ženkliai ją sumažinti ir taip pat prisidėti prie visapusės kibernetinio saugumo brandos augimo Lietuvoje[42].

Bendrąją prasme, įsilaužimas į sistemą yra procesas, kurio metu pažeidžiamas kibernetinio saugumo subjekto privatumas ir konfidenciali informacija. Įsilaužiant į sistemą yra nustatomos jos silpnosios vietos arba tinklo spragos ir pasiekiama privati kibernetinio saugumo subjekto informacija[43]. Bandymas įsilaužti į sistemą įprastai yra laikomas neteisėta ir kenkėjiška veikla, tačiau, kai ji yra vykdoma turint gerus ketinimus ir nesiekiama padaryti žalos, tokia veikla vadinama etišku įsilaužimu (anglų k. *etichal hacking*), kurį atlieka „baltakepuriai“ įsilaužėliai.

Asmenys, kurie specializuojasi etiško įsilaužimo srityje, vadinami etiškais įsilaužėliais. Šie asmenys yra informacinių technologijų specialistai, programuotojai, kurie bando įsilaužti į sistemą ar tinklą ieškodami klaidų, spragų ir pažeidžiamų, kuriais gali pasinaudoti „juodakepuriai“ įsilaužėliai. Etiškų įsilaužėlių turimi įgūdžiai ir mąstysena prilygsta įsilaužėlių, turinčių piktavališkų ketinimų, tačiau „baltakepuriais“ įsilaužėliais galima pasitikėti, kadangi jie turi geranoriškus ketinimus ir motyvus[44].

Remiantis KSĮ 17 straipsniu, atsakingą spragų atskleidimą galima apibrėžti kaip procesą, kada asmuo, teisės aktų nustatyta tvarka, ieško ryšių ir informacinės sistemos klaidų, spragų ir pažeidžiamų, dėl kurių gali įvykti kibernetinis incidentas, o atradęs apie jas praneša NKSC ir (arba) kibernetinio saugumo subjektui, kurio ryšių ir informacinėje sistemoje spraga buvo aptikta. Pažymėtina, kad atliekant spragų paiešką negali būti trikdomas ar keičiamas ryšių ir informacinės sistemos darbas, funkcionalumas, teikiamos paslaugos bei duomenų prieinamumas ar vientisumas, taip pat neturi būti siekiama be reikalo, daugiau, negu reikia spragai patvirtinti, stebėti, fiksuoti, perimti ar kitaip disponuoti kibernetinio saugumo subjekto valdomais ir (ar) tvarkomais duomenimis, neturi būti bandoma atspėti slaptažodžius, naudojami neteisėtu būdu gauti slaptažodžiai ir negali būti manipuliuojama kibernetinio saugumo subjekto darbuotojais ar kitais asmenimis, turinčiais teisę naudotis viešai neskelbtina informacija, reikšminga spragų paieškai[45]. Taip pat atkreiptinas dėmesys į tai, kad KSĮ numato prievolę informuoti NKSC ir (arba) kibernetinio saugumo subjektą ne tik apie aptiktas spragas, bet ir apie vykdytą spragų paiešką, o įsitikinus, kad spraga yra, nutraukti spragos paieškos veiklą, susijusią su aptikta spraga.

---

[42] Viešoji konsultacija dėl atsakingo kibernetinio saugumo spragų atskleidimo praktikos įteisinimo. 2019 m. rugsėjo mėn., Vilnius, p. 1 [interaktyvus, žiūrėta: 2022-04-19]. Prieiga per internetą: http://kurklt.lt/wp-content/uploads/2019/03/Vie%C5%A1osios-konsultacijos-ataskaita-atsakingas-kibernetinio-saugumo-sprag%C5%B3-atskleidimas-1.pdf.

[43] Ushmani, A. „Ethical Hacking“. International Journal of Information Technology (IJIT), Volume 4 Issue 6, Nov-Dec 2018, p. 1.

[44] *Ibid.*, p. 2

[45] Lietuvos Respublikos kibernetinio saugumo įstatymas (su pakeitimais ir papildymais). TAR, 2014-12-23, Nr. 20553.

Apibendrinus tai, kas buvo išdėstyta, darytina išvada, kad atsakingo atskleidimo principas įgalina asmenį teisėtai ieškoti ryšių ir informacinės sistemos klaidų, spragų ir pažeidžiamų, dėl kurių gali įvykti kibernetinis incidentas, o atradus – apie juos pranešti kibernetinio saugumo subjektui arba NKSC. Taip pat galima teigti, jog atsakingo spragų atskleidimo procesas turėtų sudaryti galimybes glaudesniam viešojo ir privataus sektorių bendradarbiavimui siekiant didinti įstaigų kibernetinį saugumą, kadangi ryšių ir informacinės sistemos saugumo spragas atradęs asmuo apie jas informuoja sistemų valdytojus, kad šie trūkumus pašalintų.

1.3. Atsakingo atskleidimo principo įgyvendinimo teorinis modelis

2021 m. birželio mėn. priimtos ir įsigaliojusios KSĮ pataisos ne tik įtvirtino atsakingo ryšių ir informacinių sistemų spragų atskleidimo principą, bet kartu numatė ir šio principo įgyvendinimo modelį. Remiantis KSĮ ir Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašu[46], išskirtinos šios atsakingo atskleidimo proceso dalys[47]:

1. Kibernetinio saugumo subjekto atsakingo atskleidimo tvarkos parengimas ir paviešinimas;
2. Pranešimų apie spragas priėmimo ir informacijos dalinimosi procesų parengimas;
3. Pranešimų apie spragas priėmimas iš išorinių šaltinių;
4. Pranešimo apie spragą gavimo patvirtinimas;
5. Spragos verifikavimas;
6. Rekomendacijų teikimas sistemos vartotojams ir potencialiai paveiktiems kibernetinio saugumo subjektams;
7. Spragos pašalinimas;
8. Suteikiamas leidimas pranešėjui viešai dalintis informacija apie spragą.

Kibernetinio saugumo subjekto atsakingo atskleidimo tvarkos parengimas ir paviešinimas. Remiantis KSĮ 17 str. 1 d., kurioje įvardinama, kad „spragų paieška ir atskleidimas laikomi teisėtais ir tokius veiksmus atlikusiam asmeniui neužtraukia teisinės atsakomybės tik tais atvejais, kai spragų paieška atliekama laikantis <...> kibernetinio saugumo subjekto nustatytos spragų atskleidimo tvarkos apraše <...> numatytų apribojimų“, kibernetinio saugumo subjektas turėtų parengti ir paviešinti atsakingo spragų atskleidimo tvarką. Šioje tvarkoje turėtų būti numatytos kibernetinio saugumo subjekto spragų atskleidimo sąlygos,

[46] Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2021 m. liepos 9 d. įsakymu Nr. V-484 „Dėl nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašo patvirtinimo“.

[47] *Pgl.* Tamošiūnas, Ž. R. „Atsakingo atskleidimo sąvokos, procesas, komunikacijos planas, principai ir tvarka“ [interaktyvus, žiūrėta: 2024-04-29]. Prieiga per internetą: http://kurklt.lt/wp-content/uploads/2019/03/Atsakingo-atskleidimo-tvarka.pdf.

nustatytas informacijos apie spragų paieškos rezultatus turinys, informacijos pateikimo kibernetinio saugumo subjektui tvarka, informacijos apie aptiktą spragą viešo atskleidimo būdas.

Pranešimų apie spragas priėmimo ir informacijos dalinimosi procesų parengimas. Kibernetinio saugumo subjektas taip pat turėtų numatyti procesus, kaip bus priimami pranešimai apie spragas bei kaip gauta informacija bus dalinamasi su už kibernetinį saugumą, aptiktų spragų pašalinimą atsakingais subjektais.

Pranešimų apie spragas priėmimas iš išorinių šaltinių. Šiame etape, vadovaujantis aukščiau minėtomis kibernetinio saugumo subjekto parengtomis tvarkomis, iš išorės šaltinių yra gaunami ir priimami pranešimai apie aptiktas spragas. Gavęs pranešimą kibernetinio saugumo subjektas turi pranešėjui patvirtinti, kad pranešimą gavo.

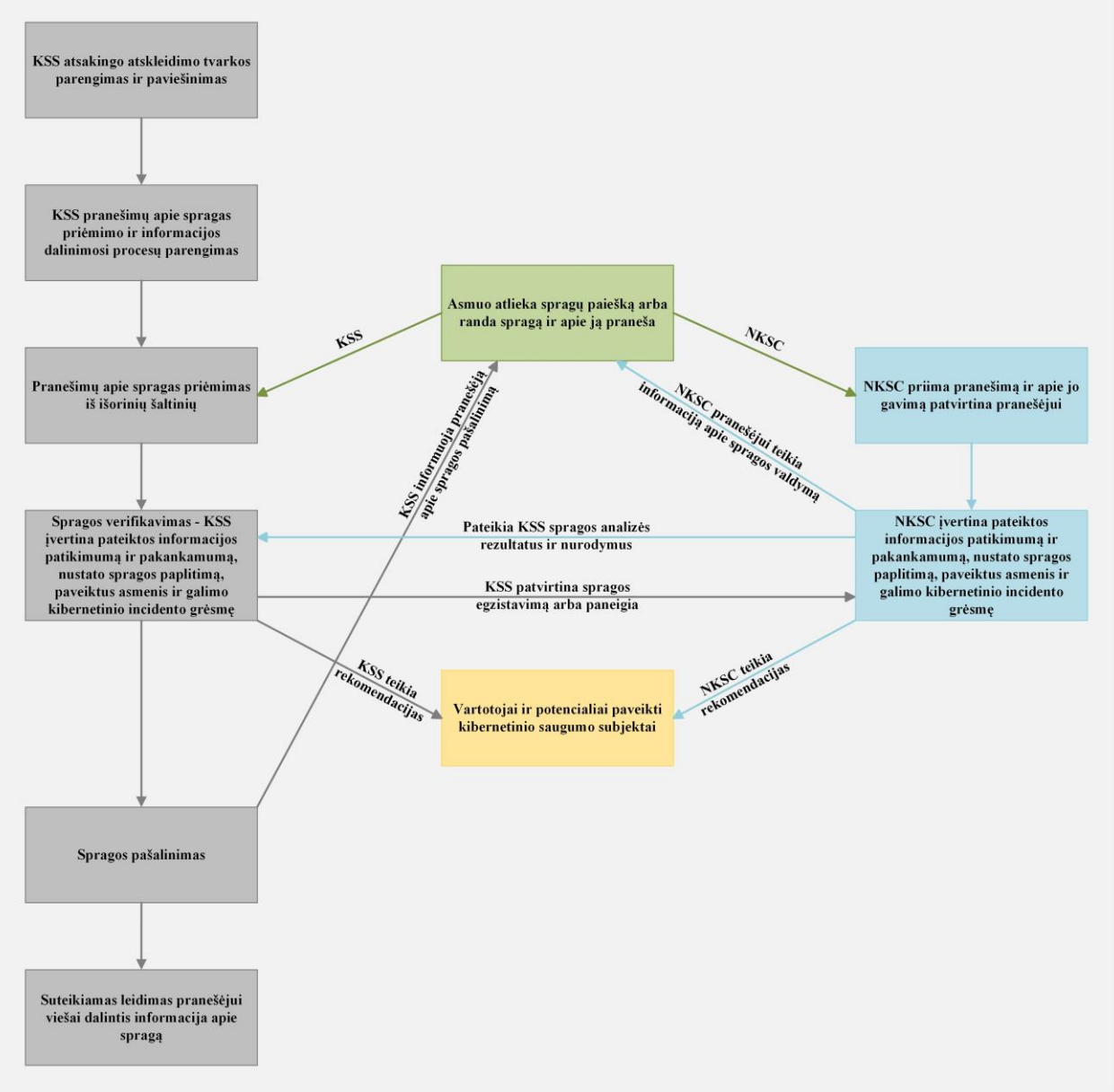
Spragos verifikavimas – kibernetinio saugumo subjektas įvertina pateiktos informacijos patikimumą ir pakankamumą, nustato spragos paplitimą, paveiktus asmenis ir galimo kibernetinio incidento grėsmę, taip pat informuoja pranešėją apie įvertinimo rezultatus.

Rekomendacijų teikimas sistemos vartotojams ir potencialiai paveiktiems kibernetinio saugumo subjektams. Įsitikinęs, kad pranešimas apie kibernetinio saugumo spragą buvo teisingas bei nustatęs spragos paplitimą, paveiktus asmenis ir galimo kibernetinio incidento grėsmę, kibernetinio saugumo subjektas sistemos vartotojams ir potencialiai paveiktiems kibernetinio saugumo subjektams bei kitiems kibernetinio saugumo subjektams, kurie galimai susiduria su panašaus tipo spragomis, teikia rekomendacijas dėl spragos poveikio mažinimo.

Spragos pašalinimas – šiame etape kibernetinio saugumo subjektas per 90 kalendorinių dienų nuo informacijos apie spragą gavimo pašalina atrastą kibernetinio saugumo spragą ir apie tai informuoja pranešėją.

Suteikiamas leidimas pranešėjui viešai dalintis informacija apie spragą. Kibernetinio saugumo subjektas suteikia pranešėjui leidimą viešinti informaciją apie spragą. Pranešėjas informaciją viešina kibernetinio saugumo subjekto atsakingo atskleidimo tvarkoje numatytu būdu.

Grafinis atsakingo atskleidimo principo įgyvendinimo teorinio modelio atvaizdavimas, sudarytas remiantis KSĮ ir Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašu:



Šaltinis: sudaryta remiantis Lietuvos Respublikos kibernetinio saugumo įstatymu ir Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašu

3 pav. **Teorinis atsakingo atskleidimo principo įgyvendinimo modelis**

Kaip vieną iš praktinių atsakingo atskleidimo principo įgyvendinimo pavyzdžių galima pateikti kibernetinio saugumo spragos pašalinimą Lietuvos organizacijų plačiai naudojamoje dokumentų ir procesų valdymo sistemoje „Avilys“. Šioje sistemoje atlikdami testavimą klaidą aptiko UAB „Transcendent Group“ specialistai ir laikydamiesi atsakingo atskleidimo principo apie ją pranešė NKSC[48]. Kaip teigė saugumo spragą atradęs vyresnysis IT saugumo konsultantas, jis testuodamas pastebėjo, kad „dokumentų valdymo sistemoje esantys duomenys yra laisvai pasiekiami net ir oficialių prisijungimų prie „Avilio“ duomenų neturintiems

[48] Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos pranešimas spaudai „Gerieji“ kibernetiniai įsilaužėliai padeda pašalinti pavojingas spragas“ [interaktyvus, žiūrėta: 2024-04-29]. Prieiga per internetą: https://www.nksc.lt/naujienos/gerieji_kibernetiniai_isilauzeliai_padeda_pasalint.html

asmenims. Tačiau didžiausią riziką kėlė ne pati prisijungimo galimybė, o tai, kad nelegaliai prisijungęs asmuo galėjo ne tik susipažinti su ten esančiais dokumentais, bet ir perimti administratoriaus paskyrą bei keisti ar net trinti „Avilyje“ esančius dokumentus. Kitaip sakant, įsilaužėlis turėjo galimybę tapti nematomu organizacijos vadovu, kuris netgi galėjo pakeisti įprastinę organizacijos veiklą.“[49] Laikantis visų atsakingo atskleidimo proceso reikalavimų, informacija apie spragą nedelsiant buvo perduota NKSC, kuris apie ją pranešė dokumentų ir procesų valdymo sistemos „Avilys“ informacinės sistemos kūrėjams, – rasti trūkumai buvo pašalinti, o klientams įdiegti reikiami sistemos atnaujinimai[50].

Apibendrinant tai, kas buvo išdėstyta, galima teigti, jog teisės aktai nustato gana aiškų atsakingo spragų atskleidimo procesą, kuris turėtų būti nesunkiai įgyvendinamas, tačiau tam, kad atsakingo atskleidimo principo įgyvendinimo modelis sėkmingai funkcionuotų, reikalingas visų subjektų, dalyvaujančių atsakingo spragų atskleidimo procese, įsitraukimas ir įdirbis, ypatingai – kibernetinio saugumo subjektų, kurie turi būti tinkamai pasiruošę reaguoti į pranešimus dėl atrastų spragų ir pasirengę jas pašalinti.

1.4. Užsienio šalių atsakingo atskleidimo principo įgyvendinimo praktika

Nepaisant to, kad ES, atsižvelgdama į pasaulinę skaitmeninės transformacijos tendenciją, aktyviai siekia užtikrinti kibernetinį saugumą, ES rinka tarp ES valstybių narių šiuo aspektu yra susiskaidžiusi. Belgija, Prancūzija, Lietuva ir Nyderlandai yra vienintelės keturios ES valstybės narės, turinčios visiškai nusistovėjusią nacionalinę kibernetinio saugumo politiką[51]. Pažymėtina, kad šių keturių šalių politikos iniciatyvos labai skiriasi[52].

Šioje darbo dalyje bus aptariamos Belgijos ir Nyderlandų – užsienio šalių, turinčių kibernetinio saugumo politikas – atsakingo atskleidimo principo įgyvendinimo praktika. Pažymėtina, kad Prancūzija taip pat yra įgyvendinusi koordinuoto pažeidžiamumo atskleidimo politiką, tačiau dėl šaltinių trūkumo šios valstybės praktika nebus nagrinėjama.

Minėtų užsienio šalių praktika bus nagrinėjama vertinant šiuos kriterijus:

1. Atsakingo atskleidimo principo teisinis reglamentavimas;
2. Atsakingo atskleidimo principo politikos taikymo sektorius;
3. Atsakingo atskleidimo principo politikos tikslai;
4. Atsakingo atskleidimo principo modelis.

[49] Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos pranešimas spaudai „Gerieji“ kibernetiniai įsilaužėliai padeda pašalinti pavojingas spragas“ [interaktyvus, žiūrėta: 2022-04-23]. Prieiga per internetą: https://www.nksc.lt/naujienos/gerieji_kibernetiniai_isilauzeliai_padeda_pasalint.html.
[50] *Ibid.*
[51] „Developing national vulnerability programmes“. ENISA, 2023, p. 10.
[52] „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022, p. 6.

Išanalizavimus užsienio valstybių praktiką bus galima įžvelgti atsakingo atskleidimo principo įgyvendinimo panašumus bei skirtumus, palyginti veikimo modelius ir įvertinti, kaip užtikrinama teisėto atskleidimo praktika.

1.4.1. Belgijos atsakingo atskleidimo principo įgyvendinimo praktika

Atsakingo atskleidimo principo teisinis reglamentavimas. Nuo 2018 m. Belgijos kibernetinio saugumo centras (anglų k. *Centre for Cyber Security Belgium, CCB,* toliau – CCB) bendradarbiauja su valstybine prokuratūra, pažeidžiamumo pranešėjų bendruomene, privačiu sektoriumi ir valdžios institucijomis kurdamas nacionalinį požiūrį į Koordinuoto pažeidžiamumo atskleidimo (anglų k. *Coordinated Vulnerability Disclosure, CVD,* toliau – CVD) politiką. Nacionalinė CVD politika yra formali politika, aiškiai įtraukta į Belgijos kibernetinio saugumo strategiją ir į CCB bazines saugumo gaires. 2019 m. CCB, kaip pavyzdį kitoms organizacijoms, patvirtino CVD politiką ir ją paskelbė savo interneto svetainėje. 2020 m. gruodžio mėn. CCB paskelbė nacionalines gaires, skatinančias visas Belgijos organizacijas taikyti CVD politiką arba klaidų atlyginimo – „Bug bounty“ – programą.[53]

„Bug bounty“ programa – tai organizacijos apibrėžtų taisyklių rinkinys, pagal kurį dalyviams, nustačiusiems jos naudojamų technologijų pažeidžiamumą, suteikiamas atlygis. Šis atlygis gali būti pinigų suma, dovanos arba viešas pripažinimas (patekimas tarp geriausių dalyvių, publikacija, konferencija ir t. t.). Tai tam tikra koordinuojamos pažeidžiamumų atskleidimo politikos forma, kai dalyviui atlyginama pagal pateiktos informacijos kiekį, svarbą ar kokybę. Ši politikos forma yra patrauklesnė potencialiems dalyviams ir dažnai užtikrina geresnius rezultatus organizacijoms.[54]

2023 m. vasario mėnesį CCB įgyvendino naują sistemą, kurioje numatyta, kad bet kas gali tirti įmones, kurių informacinė sistema yra Belgijoje, ir pranešti apie bet kokį aptiktą pažeidžiamumą nepasirašęs su atitinkama įmone jokios sutarties. Tačiau tai įmanoma tik laikantis griežtų taisyklių[55]:

- veiksmai, kurių imamasi, turi būti griežtai proporcingi įrodytam pažeidžiamumo faktui. Tai reiškia, kad spraga negali būti išnaudojama daugiau, nei būtina saugumo trūkumui įrodyti. Pavyzdžiui, „neproporcingais“ ir „neteisėtais“ laikomi tokie veiksmai kaip

[53] „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022, p. 14.
[54] FAQ on Coordinated Vulnerability Disclosure Policy (CVDP) and Bug Bounty Programmes [interaktyvus, žiūrėta: 2024-02-04]. Prieiga per internetą: https://ccb.belgium.be/en/faq-coordinated-vulnerability-disclosure-policy-cvdp-and-bug-bounty-programmes.
[55] „Vulnerability reporting in Belgium: A safe harbour for ethical hackers“, 2023 [interaktyvus, žiūrėta: 2024-02-04]. Prieiga per internetą: https://www.headmind.com/en/vulnerability-reporting-belgium-safe-harbour-ethical-hackers/.

sukčiavimo atakos, socialinės inžinerijos atakos, DDoS, grubios jėgos atakos, duomenų kopijavimas keičiant ir (arba) ištrinant duomenis iš sistemos ir pan.;

- veiksmai turi būti atliekami tik gerais ketinimais ir be jokių nesąžiningų ar žalingų ketinimų;
- vos tik aptikus pažeidžiamumą, geriausia – per 72 valandas, apie jį turi būti pranešta oficialia rašytine ataskaita atitinkamai organizacijai ir CCB, veikiančiai kaip nacionalinė CSIRT;
- atliekant tyrimą negalima sąmoningai tvarkyti asmens duomenų, nebent tai yra absoliučiai būtina saugumo problemai įrodyti. Be to, jie turi būti ištrinti iš karto, kai tik pranešama apie pažeidžiamumą;
- turi būti išlaikytas duomenų konfidencialumas. Jokia informacija apie aptiktą pažeidžiamumą neturi būti atskleista be CCB sutikimo, o IT duomenys ar asmens duomenys neturi būti perduoti jokiai trečiajai šaliai.

Atsakingo atskleidimo principo politikos taikymo sektorius. Politika skatina priimti suderintas pažeidžiamumo atskleidimo gaires privatiems ir viešiesiems subjektams ir yra suskirstyta į šiuos skirtingus dokumentus: I vadovas – Geroji praktika; II vadovo dalis – Teisiniai aspektai; politikos pavyzdys; aplankas; ir DUK. CCB yra atsakingas už nacionalinės CVD politikos įgyvendinimą ir pateikia politikos šabloną. Pagal nacionalinę CVD politiką CVD koordinatoriaus vaidmuo pagal nutylėjimą priskiriamas CCB (kartu su jo CERT komanda). Jei pažeidžiamumas dar nėra žinomas ir gali turėti tiesioginį ar netiesioginį poveikį kitur, už jo nustatymą atsakinga organizacija turi informuoti CCB ir kitas galimai susijusias organizacijas, net jei ji nenori, kad pažeidžiamumas būtų paskelbtas viešai.[56]

Atsakingo atskleidimo principo politikos tikslai. Belgijos CVD – tai už IT sistemas atsakingos organizacijos iš anksto nustatytų taisyklių rinkinys, leidžiantis dalyviams (arba etiškiems įsilaužėliams), turintiems gerų ketinimų, nustatyti galimus sistemų pažeidžiamumus arba apie juos pateikti visą reikiamą informaciją. Šios taisyklės, paprastai skelbiamos interneto svetainėje, leidžia apibrėžti atsakingos organizacijos ir politikos dalyvių bendradarbiavimo teisinę bazę. Šios taisyklės turėtų užtikrinti, *inter alia*, informacijos, kuria keičiamasi, konfidencialumą ir sukurti atsakingą ir suderintą bet kokio aptiktų pažeidžiamumų atskleidimo sistemą.[57]

[56] „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022, p. 15.
[57] „Coordinated Vulnerability Disclousure Policies „CVDP“. Center of Cyber Security Belgium, 2020, p. 3 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: https://ccb.belgium.be/sites/default/files/Brochure_CVDP_UK_A5_DP2%20%28002%29.pdf.

Išskiriami šie CVD politikos tikslai[58]:

1. Naudingo, sąžiningo, veiksmingo, teisėto ir biudžetą tausojančio bendradarbiavimo teisinės bazės sukūrimas;
2. IT sistemų saugumo gerinimas ir tyrimų skatinimas;
3. Naudotojų pasitikėjimo IT technologijomis užtikrinimas;
4. Konfidencialumo garantija;
5. Užtikrinti, kad būtų geriau laikomasi teisinių įsipareigojimų IT saugumo srityje.

Naudingo, sąžiningo, veiksmingo, teisėto ir biudžetą tausojančio bendradarbiavimo teisinės bazės sukūrimas. Kai organizacija savo IT sistemų saugumui patikrinti naudoja tam tikrą išorinį paslaugų teikėją, ji sudaro saugumo audito sutartį, į kurią gali būti įtraukti „pentestai“ (arba „įsiskverbimo testai“), imituojantys piktavališkų ketinimų turinčių asmenų ataką, kad parodytų esamus pažeidžiamumus. Tokiu atveju šalių tarpusavio teisinės pareigos iš esmės yra aprašytos konkrečioje sutartyje arba bendrosiose sąlygose. Tačiau taip būna ne visada, kai organizacija nori bendradarbiauti su nenurodytais asmenimis (dalyviais ar etiškais įsilaužėliais), kurie gali nustatyti jos IT sistemų pažeidžiamumą, – tokiu atveju tarp šalių nėra aiškios sutartinės sistemos ir prieš kiekvieną bendradarbiavimą organizacija turi apibrėžti savo lūkesčius ir dalyvių teisinius įsipareigojimus. Šiuo atžvilgiu suderinta pažeidžiamumo atskleidimo politika yra tam tikros rūšies prisijungimo sutartis, kurioje išdėstytos visos atsakingos organizacijos sutartinės nuostatos, o dalyvis, laisva valia nusprendęs dalyvauti programoje, sutinka su ja.[59]

CVD politikos priėmimas paaiškina dalyvių teisinę padėtį – jie gali įrodyti, kad turi išankstinį leidimą pasiekti atitinkamas IT sistemas ir todėl neteisėtai nesikiša į tas sistemas, jei tenkinamos politikoje nustatytos sąlygos. Šis bendradarbiavimas gali suteikti atsakingai organizacijai teisingą ir teisėtą informaciją apie jos sistemų pažeidžiamumą ir leisti jai laiku imtis tinkamų veiksmų. Tokiu būdu galima veiksmingai užkirsti kelią galimai rizikai ir žalai, kurią gali sukelti pažeidžiamumai.[60]

IT sistemų saugumo gerinimas ir tyrimų skatinimas. Tokios politikos įvedimas suteikia atsakingai organizacijai galimybę gauti informacijos apie savo IT sistemų saugumą iš įvairių šaltinių. Atsižvelgiant į dabartinį šių sistemų sudėtingumą ir techniškai pažangų pobūdį, labai

[58] „Guide to coordinated vulnerability disclosure policies. Part 1: good practices“. Center of Cyber Security Belgium, 2020, p. 7 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: https://www.cybersecuritycoalition.be/content/uploads/CCB-Guide-Policies-CVDP.pdf.
[59] „Coordinated Vulnerability Disclousure Policies „CVDP“. Center of Cyber Security Belgium, 2020, p. 7 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: https://ccb.belgium.be/sites/default/files/Brochure_CVDP_UK_A5_DP2%20%28002%29.pdf.
[60] *Ibid.,* p. 8.

naudinga įtraukti daug potencialių ekspertų, o ne pasitelkti kelis išorės paslaugų teikėjus, kurie negali būti visų organizacijos naudojamų technologijų ekspertais.[61]

Be kitų techninių ir organizacinių priemonių, tokio bendradarbiavimo sukūrimas gali būti tinkama priemonė užkirsti kelią incidentams, kurie keltų pavojų tinklo ir informacinių sistemų saugumui. Toks bendradarbiavimas turi neabejotiną pranašumą – pažeidžiamumas nustatomas ir pašalinamas prieš įvykstant saugumo incidentui. Didesnis saugumas gali būti pasiektas pašalinus pažeidžiamumą, sumažinus su tam tikrais pažeidžiamumu susijusią riziką ir nuolat vertinant šią riziką atsakingos organizacijos IT sistemoms.[62]

CVD politikos įdiegimas akivaizdžiai parodo, kad organizacija turi saugumo priemones, kurias galima išbandyti, ir vidinę (arba išorinę) komandą, kuri gali sekti dalyvių pateiktą informaciją. Be saugumo didinimo, tokio tipo politika taip pat gali pagerinti žinias apie kibernetinį saugumą ir paskatinti šios srities tyrimus. Tyrėjų darbas leidžia nustatyti naujus pažeidžiamumus, jų atsiradimo aplinkybes, išvengimo ir pašalinimo būdus.[63]

Naudotojų pasitikėjimo IT technologijomis užtikrinimas. Įgyvendinant CVD politiką visuomenei ir naudotojams parodoma, kad atsakinga organizacija teikia didelę reikšmę savo IT technologijų saugumui – šis metodas reiškia, kad organizacija įsipareigoja apdoroti dalyvių pateiktą informaciją ir stengtis ištaisyti nustatytas silpnąsias vietas arba bent jau informuoti naudotojus apie riziką. Toks įsipareigojimas taip pat gali būti vertinga rinkodaros priemonė.[64]

Konfidencialumo garantija. Informacijos apie IT sistemos pažeidžiamumą konfidencialumas turi būti užtikrintas kiek įmanoma labiau – Belgijos požiūriu, visiškas pažeidžiamumo atskleidimas kelia didelę riziką IT saugumui, kadangi trečiosios šalys, turinčios blogų ketinimų, gali sukurti ir platinti konkrečias priemones, skirtas pažeidžiamumui išnaudoti. Dėl šios priežasties nepageidautina skelbti saugumo problemos viešai, kol jos neišsprendė atsakinga organizacija, kuriai turėtų būti suteikta pakankamai laiko tai padaryti. Visiškas atskleidimas taip pat gali atidėti efektyvų pažeidžiamumo sprendimo taikymą, nes atsakinga organizacija yra priversta reaguoti krizinėje situacijoje.[65]

Saugumo problemų atskleidimas taip pat gali pakenkti atsakingos organizacijos reputacijai ir pakirsti vartotojų pasitikėjimą atitinkamomis technologijomis. Be to, IT duomenų, pvz., programinės įrangos ar instrukcijų, leidžiančių įsiskverbti į IT sistemų saugumą, skleidimas arba viešinimas gali būti laikomas baudžiamuoju nusikaltimu[66] arba informaciją paskelbusiam

[61] *Ibid.*, p. 9.
[62] *Ibid.*
[63] *Ibid.*
[64] *Ibid.*, p. 10.
[65] *Ibid.*
[66] *Pgl.* „Guide to coordinated vulnerability disclosure policies. Part 1: good practices“. Center of Cyber Security Belgium, 2020, p. 11 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: https://www.cybersecuritycoalition.be/content/uploads/CCB-Guide-Policies-CVDP.pdf.

asmeniui gali būti taikoma civilinė atsakomybė[67]. Taigi, informacija apie pažeidžiamumą turi būti viešai skelbiama itin atsargiai ir tai derinant su atsakinga organizacija.[68]

Atsakinga organizacija turi reaguoti per protingą terminą: įdiegti sprendimą arba bent informuoti dėl pažeidžiamumo paveiktus IT sistemų vartotojus. Taip pat tam, kad būtų vykdomi pažangūs IT saugumo tyrimai, gali būti labai naudinga paskelbti informaciją apie aptiktus pažeidžiamumus po to, kai bus pašalintos pagrindinės saugumo rizikos, todėl CVD politikos interesas yra sukurti teisinę sistemą, kuri sustiprintų konfidencialumą ir sudarytų geriausią įmanomą pagrindą galimam viešam atskleidimui.[69]

Užtikrinti, kad būtų geriau laikomasi teisinių įsipareigojimų IT saugumo srityje. Įgyvendindama suderintą informacijos atskleidimo politiką, organizacija parodo savo įsipareigojimą laikytis teisinių įsipareigojimų užtikrinti savo tinklo ir IT sistemų saugumą.[70]

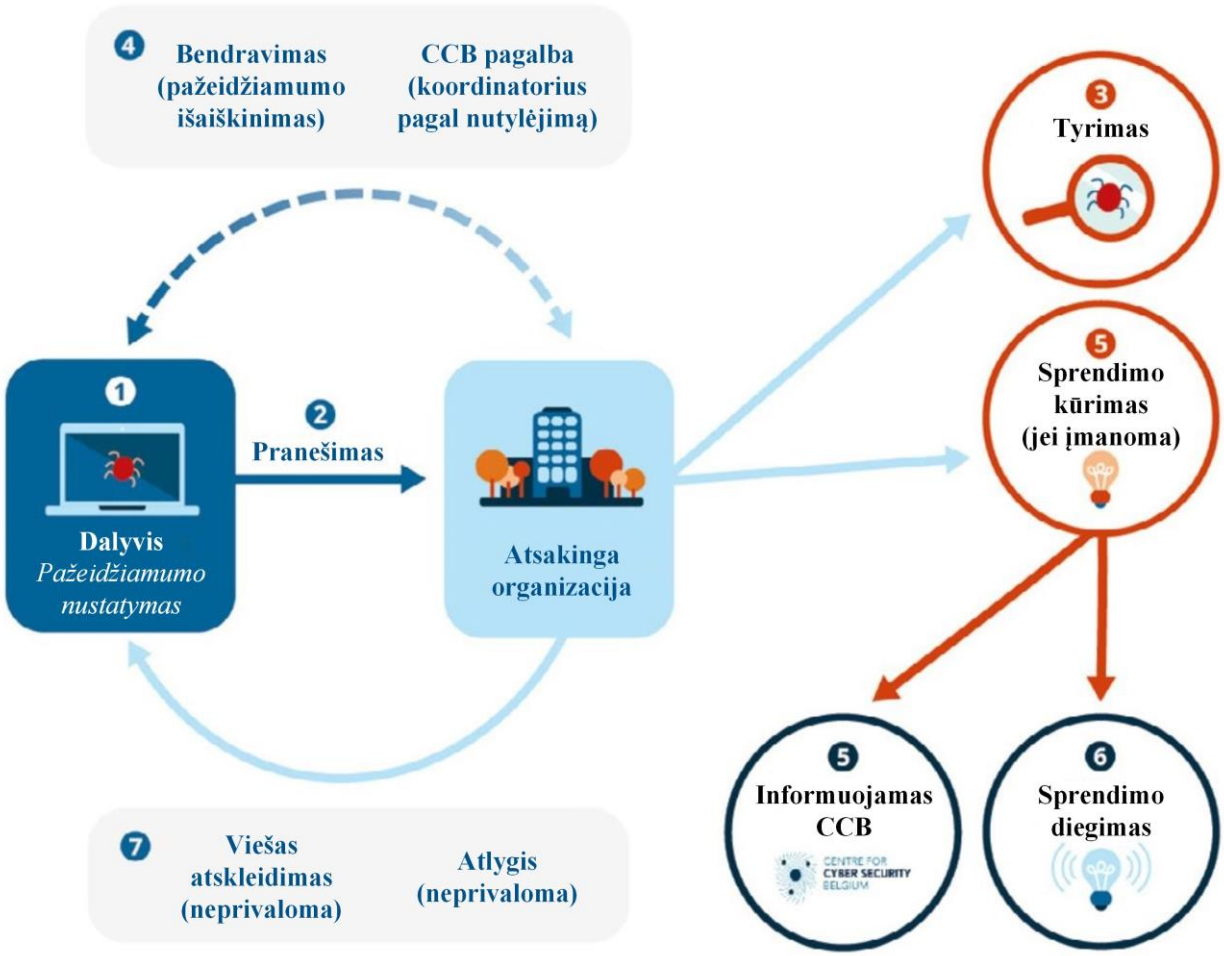
Belgijos privatumo apsaugos komisija (dabar – Duomenų apsaugos institucija) savo rekomendacijoje dėl saugumo priemonių siekiant užkirsti kelią duomenų pažeidimams primena, kad svarbu prireikus dokumentuoti, stebėti ir tobulinti IT saugumo priemones. Buvusios Belgijos privatumo apsaugos komisijos išleistose asmens duomenų informacijos saugumo gairėse taip pat nurodoma, kad duomenų valdytojas turėtų reguliariai organizuoti tinkamą asmens duomenų informacijos saugumo auditą ir imtis valdymo priemonių, kad užtikrintų duomenų konfidencialumą ir vientisumą[71].

Pažymėtina, kad Belgijoje šiuo metu daugelis įmonių jau taiko suderintą pažeidžiamumo atskleidimo politiką, pvz.: „Roximus“, „Telenet“, „Voo“, „Base“, SNCB, „Brussels Airlines“, Antverpeno uostas, VRT, „Kinepolis“, KUL, „Randstad“, „Itsme“, „New pharma“, „Cybersecurity coalition“, „Tomorrowland“, „Torfs“ ir „Dpg Media“. Taip pat Belgijoje yra įsikūrusi svarbi atlygio už klaidas platforma („Intigriti“), kuri koordinuoja kai kurias politikos kryptis.[72]

Atsakingo atskleidimo principo modelis. Žemiau pateikiamas atsakingo atskleidimo modelių – be koordinatoriaus ir su juo – grafinis atvaizdavimas:

[67] *Ibid.*
[68] „Guide to coordinated vulnerability disclosure policies. Part 1: good practices“. Center of Cyber Security Belgium, 2020, p. 11 [interaktyvus, žiūrėta: 2024-01-22]. Prieiga per internetą: https://www.cybersecuritycoalition.be/content/uploads/CCB-Guide-Policies-CVDP.pdf.
[69] *Ibid.*, p. 12.
[70] *Ibid.*
[71] *Pgl.* „Guide to coordinated vulnerability disclosure policies. Part 1: good practices“. Center of Cyber Security Belgium, 2020, p. 13.
[72] „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022, p. 15.

Koordinuoto pažeidžiamumo atskleidimo politika be koordinatoriaus

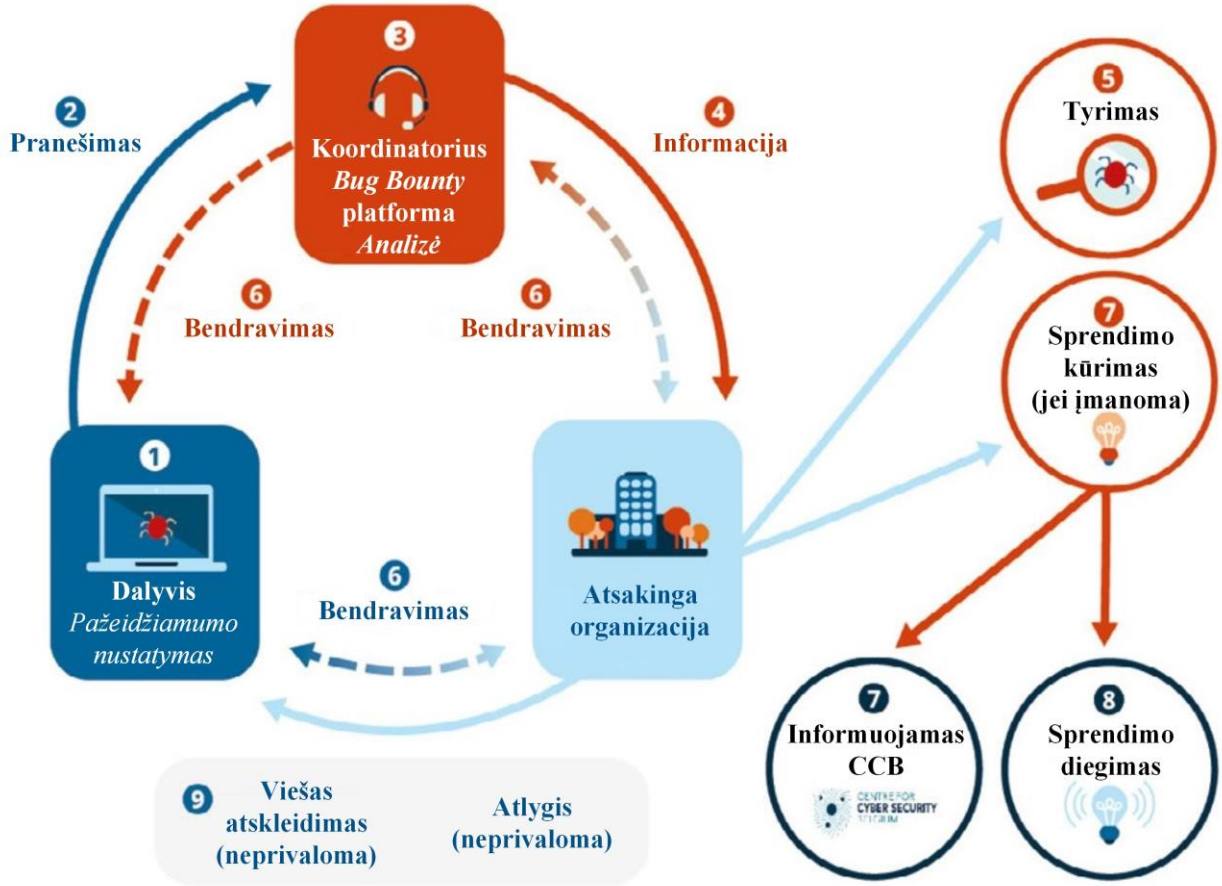


Šaltinis: išversta pagal „Coordinated Vulnerability Disclousure Policies „CVDP“, p. 14

4 pav. **Koordinuoto pažeidžiamumo atskleidimo politika be koordinatoriaus**

1. Dalyvis nustato pažeidžiamumą pagal CVD politiką.
2. Dalyvis informuoja atsakingą organizaciją vadovaudamasis CVD politika.
3. Atsakinga organizacija analizuoja pažeidžiamumą.
4. Siekiant išsiaiškinti pažeidžiamumą, tęsiama komunikacija tarp dalyvio ir atsakingos organizacijos. Jei šiame procese trūksta komunikacijos, galima kreiptis pagalbos į CCB, kuris yra koordinatorius pagal nutylėjimą.
5. Jei įmanoma, sukuriamas sprendimas. Jei pažeidžiamumas gali paveikti ir kitas organizacijas, atsakinga organizacija informuoja CCB.
6. Atsakinga organizacija diegia sprendimą savo naudotojams arba klientams.
7. Gali būti aptariamas viešas atskleidimas bei gali būti skiriamas atlygis, vadovaujantis Koordinuoto pažeidžiamumo atskleidimo politika.

Koordinuoto pažeidžiamumo atskleidimo politika su koordinatoriumi



Šaltinis: išversta pagal „Coordinated Vulnerability Disclousure Policies „CVDP“, p. 15

5 pav. **Koordinuoto pažeidžiamumo atskleidimo politika su koordinatoriumi**

1. Dalyvis nustato pažeidžiamumą pagal CVD politiką.
2. Dalyvis informuoja atsakingą organizaciją per koordinatorių, pvz., per „Bug Bounty„ platformą, vadovaudamasis CVD politika.
3. Koordinatorius analizuoja pažeidžiamumą.
4. Po patvirtinimo koordinatorius informuoja atsakingą organizaciją.
5. Atsakinga organizacija analizuoja pažeidžiamumą.
6. Siekiant išsiaiškinti pažeidžiamumą, tęsiama komunikacija tarp dalyvio ir atsakingos organizacijos, jei pageidaujama – per koordinatorių.
7. Jei įmanoma, sukuriamas sprendimas. Jei pažeidžiamumas gali paveikti ir kitas organizacijas, atsakinga organizacija informuoja CCB.
8. Atsakinga organizacija diegia sprendimą savo naudotojams arba klientams.
9. Gali būti aptariamas viešas atskleidimas bei gali būti skiriamas atlygis, vadovaujantis Koordinuoto pažeidžiamumo atskleidimo politika.

Apibendrinant tai, kas buvo išdėstyta, darytina išvada, jog Belgija, siekdama didinti kibernetinio saugumo lygį, aktyviai įgyvendina CVD politiką. Ši politika grindžiama glaudžiu bendradarbiavimu tarp valstybės institucijų, verslo sektoriaus ir visuomenės. Belgija stengiasi skatinti atsakingus informacijos mainus apie potencialius saugumo pažeidimus ir kibernetinius incidentus taip didindama galimybę greitai į juos reaguoti. Tokias išvadas suponuoja tai, jog Belgijoje CVD politika yra formali politika, aiškiai įtraukta į Belgijos kibernetinio saugumo strategiją ir į CCB bazines saugumo gaires. Ši politika skatina priimti suderintas pažeidžiamumo atskleidimo gaires privatiems ir viešiesiems subjektams. Išskirtini penki CVD politikos tikslai, susiję su naudingo, sąžiningo, veiksmingo, teisėto ir biudžetą tausojančio bendradarbiavimo teisinės bazės sukūrimu, IT sistemų saugumo gerinimu ir tyrimų skatinimu, naudotojų pasitikėjimo IT technologijomis užtikrinimu, konfidencialumo garantija bei siekiu užtikrinti, kad būtų geriau laikomasi teisinių įsipareigojimų IT saugumo srityje.

1.4.2. Nyderlandų atsakingo atskleidimo principo įgyvendinimo praktika

Atsakingo atskleidimo principo teisinis reglamentavimas. Nyderlandai CVD politiką taiko nuo 2013 m. Pažymėtina, jog Nyderlandai vadovavo ES pastangoms kuriant CVD politiką ir daug prisidėjo prie kitų valstybių narių pastangų spręsti savo iššūkius ir rūpesčius. Laikoma, kad tai yra formali politika, nors Nyderlandų teisėje ir nėra nuorodos į CVD, – arčiausiai oficialios politikos yra laisvai išverstas, „Valstybinio prokuroro politinis laiškas dėl CVD“. Gana įdomu tai, jog Nyderlanduose istorinės teisminės bylos nustatė ribas, kuriose, taip vadinamas, saugumo tyrinėtojas ieškodamas spragų gali veikti.[73]

Pažymėtina, kad CVD politikos Nyderlanduose nustatymo procesą inicijavo privatus sektorius, ypač bankai ir interneto paslaugų teikėjai. Šios įmonės parodė pavyzdį ir pradėjo kurti CVD politiką. Tai leido sukurti ekosistemą šalyje, kurioje visuomenė suvokia CVD proceso naudingumą.[74]

Vadovaujantis Nyderlandų CVD, galima pranešti apie pažeidžiamumus, kurie kelia pavojų sistemos saugumui, pvz., pažeidžiamumas, leidžiantis apeiti prisijungimo formas arba suteikia neteisėtą prieigą prie duomenų bazių, kuriose yra asmeninė informacija[75]. Politikoje taip pat pažymima, kad ne kiekvienas sistemos defektas yra pažeidžiamumas ir nurodoma, kad apie šiuos pažeidžiamumus nereikia pranešti[76]:

- defektai, kurie neturi įtakos duomenų prieinamumui, vientisumui ar konfidencialumui;

[73] „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022, p. 29.
[74] *Ibid.*, p. 73.
[75] „Have you discovered a vulnerability in a government system or in a system with a vital function?“ [interaktyvus, žiūrėta: 2024-04-29]. Prieiga per internetą: https://english.ncsc.nl/contact/reporting-a-vulnerability-cvd.
[76] *Ibid.*

- „WordPress xmlrpc.php“ funkcijos prieinamumas, kai piktnaudžiavimas ja apsiriboja vadinamuoju „paslaugų atsisakymo“ ataka;
- galimybė naudoti kelių svetainių scenarijų statinėje svetainėje arba svetainėje, kuri neapdoroja jokių jautrių vartotojo duomenų;
- informacijos apie versiją prieinamumas, pvz., per failą *info.php*. Viena iš galimų šio scenarijaus išimčių yra tada, kai versijos informacija atskleidžia, kad sistema naudoja programinę įrangą, kurioje yra žinomų pažeidžiamumų;
- HTTP saugos antraščių, naudojamų tokiuose mechanizmuose kaip *Cross-Origin Resource Sharing* (CORS), nebuvimas, nebent šis saugos antraštės trūkumas akivaizdžiai sukelia saugos problemą.

Atsakingo atskleidimo principo politikos taikymo sektorius. Nyderlanduose CVD pasirodė esąs labai svarbus viešosioms ir privačiosioms įstaigoms. Jos yra labai priklausomos nuo netrikdomo informacinių sistemų veikimo kasdienėje veikloje. Pranešimai apie jų sistemų pažeidžiamumus pastaraisiais metais padėjo pagerinti sistemų saugumą ir tęstinumą, viena vertus, pašalinant pažeidžiamumus, kita vertus, prisidedant prie bendro Nyderlandų įmonių informuotumo apie IT saugumą.[77]

Pastaraisiais metais tapo aišku, kad pranešimus teikiančios šalys yra pasirengusios dirbti pagal organizacijų parengtos CVD politikos sąlygas. Taip pat atsakingo informacijos atskleidimo praktika parodė, kad gerų ketinimų turinčios pranešančiosios šalys ir pažeidžiamos organizacijos sugebėjo bendradarbiauti ir taip žengti kitą žingsnį didinant tinklų ir informacinių sistemų saugumą.[78]

Pažymėtina, kad nuo 2013 m. Nyderlandų nacionalinis kibernetinio saugumo centras (anglų k. *the National Cyber Security Centre – Netherlands, NCSC-NL,* toliau – NCSC-NL) gavo ir apdorojo šimtus pranešimų. Daugelis šalies organizacijų aktyviai taiko CVD ir yra patenkintos rezultatais. Nors yra pranešimų apie pažeidžiamumą dėl nedidelių ar teorinių problemų, yra keletas svarbių ataskaitų, kurių kitu atveju nebūtų galima rasti ir, jei jais būtų buvę piktnaudžiaujama, tai galėjo turėti didelį neigiamą poveikį infrastruktūros arba klientų duomenų saugumui.[79]

Nyderlanduose yra keletas gerosios praktikos pavyzdžių, susijusių su informuotumo didinimo kampanijomis. „Hack right“ – tai informavimo programa, skirta ypač jauniems pirmiesiems pažeidėjams (iki 23 metų) ir padedanti suprasti savo teises ir pareigas. Programa buvo sukurta 2019 m., kai buvo pastebėta, kad dažniausiai į teismą patenka jaunieji mokslininkai. NCSC-NL paskelbė CVD politikos gaires, kurios buvo naudingos organizacijoms,

[77] „Coordinated Vulnerability Disclosure: the Guideline“. NCSC, 2018, p. 5.
[78] *Ibid.*
[79] „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022, p. 29.

įgyvendinančioms CVD. Be to, Nyderlandų mokslininkai sukūrė platformą, skirtą pranešti apie pažeidžiamumą, remiamą savanorių, taip pat buvo sukurtas ir elgesio kodeksas.[80]

Atsakingo atskleidimo principo politikos tikslai. CVD tikslas – prisidėti prie IT sistemų saugumo didinimo dalijantis žiniomis apie pažeidžiamumą. CVD metu žiniomis dalijamasi su viena ar keliomis potencialiai pažeidžiamomis organizacijomis, kad bendradarbiaujant su pranešančiąja šalimi būtų rastas bendras rastų pažeidžiamumų sprendimas. Svarbu, kad nukentėjusios organizacijos turėtų pakankamai laiko ištaisyti pažeidžiamumą arba apsaugoti sistemas, siekiant kuo labiau apriboti nuostolius ar žalą arba užkirsti jiems kelią. Šio proceso kertinis akmuo yra žinių apie pažeidžiamumą atskleidimas ištaisius pažeidžiamumą.[81]

Pažymėtina, kad CVD labai svarbu, kad visos šalys laikytųsi susitarimų, kaip pranešti apie pažeidžiamumą ir kaip jį pašalinti. Šiame procese padeda tai, jei organizacija iš anksto paskelbia išankstines sąlygas, pvz., kokios sistemos patenka į taikymo sritį ir kokius tyrimus galima atlikti.[82]

Atsakingo atskleidimo principo modelis. Manoma, kad Nyderlandai sukūrė vieną veiksmingiausių CVD procesų ES. Jų teigimu, svarbiausias sėkmės veiksnys Nyderlandams buvo metodas „iš apačios į viršų“, kurio buvo laikomasi nustatant dabartinį CVD procesą. Procesas prasidėjo nuo to, kad pagrindiniai šalies bankai ir interneto paslaugų teikėjai pajuto būtinybę prisitaikyti prie etiškų įsilaužėlių ieškant pažeidžiamumų. Šalis pastebėjo, kad jei įmonės, įstaigos ar organizacijos nėra ištikimos asmenims, pranešantiems apie pažeidžiamumą, sunku juos priversti diegti/priimti CVD sistemą. Taigi, užuot reikalavus, kad įmonės nustatytų CVD politiką (požiūris iš viršaus į apačią), daug naudingiau yra skatinti ekosistemą, kurioje tyrėjai ir (arba) įsilaužėliai žinotų, kad yra teisiškai apsaugoti ir kad visuomenė juos pripažįsta.[83]

Nyderlandų NCSC-NL atsakingo atskleidimo gairėse pateikia tokią apibrėžtį: „Atsakingas atskleidimas IRT srityje – tai atsakingas pažeidžiamų vietų atskleidimas kartu konsultuojantis pranešėjui ir organizacijai, remiantis organizacijų nustatyta atsakingo atskleidimo politika.[84]“ Apibrėžime yra du svarbūs elementai, apibūdinantys NCSC-NL nuostatą: visų pirma, koordinuoto pažeidžiamumo atskleidimo procese pirmiausia dalyvauja dvi šalys – pranešėjas ir organizacija. Antra, NCSC-NL daro prielaidą, kad koordinuoto pažeidžiamumo atskleidimo politiką (iš anksto) nustato organizacija.[85]

[80] *Ibid.,* p. 52.
[81] „Coordinated Vulnerability Disclosure: the Guideline“. NCSC, 2018, p. 7.
[82] *Ibid.*
[83] „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022, p. 59.
[84] *Pgl.* „Coordinated Vulnerability Disclosure Model Policy and Procedure“. CIO Platform Nederland, 2016, p. 10.
[85] *Ibid.*

Galima išskirti šiuos tris Nyderlandų koordinuoto pažeidžiamumo atskleidimo proceso pagrindinius elementus[86]:

1. Organizacija;
2. Pranešimo etapas;
3. Nacionalinis kibernetinio saugumo centras (NCSC-NL).

Organizacija. Siekdama efektyviai bendradarbiauti su įvairiomis šalimis, kad pašalintų pažeidžiamumą, organizacija gali nuspręsti parengti ir paskelbti CVD politiką. Sukūrusi savo CVD politiką, organizacija gali parodyti, kaip ji elgiasi su pranešimais apie pažeidžiamumą. Tokiu būdu organizacija taip pat gali suformuoti būdą, kuriuo ji nori gauti pranešimus. Tokį procesą galima organizuoti taip[87]:

- organizacija nustato ir skelbia CVD politiką. Šioje politikoje organizacija numato aiškias taisykles dėl tyrimų, kuriuos gali atlikti pranešimus teikiančios šalys, pvz., kokie metodai yra leidžiami ir kurios sistemos patenka į taikymo sritį arba už jos ribų;
- organizacija palengvina ir supaprastina pranešimų teikimo procesą. Viena iš galimybių – standartizuoto pranešimų teikimo metodo naudojimas, pvz., konkretaus el. pašto adreso nurodymas arba internetinės formos pateikimas. Be to, organizacija gali nuspręsti, ar priimti anoniminius pranešimus;
- organizacija nustato tvarką, kad galėtų tinkamai reaguoti į pranešimus. Patartina nustatyti procesą, kuriuo remiantis būtų galima tinkamai ištaisyti visus rastus pažeidžiamumus;
- praktinė patirtis rodo, kad po pirminio CVD politikos paskelbimo yra didesnis susidomėjimas pranešti apie pažeidžiamumą organizacijai, todėl organizacija turėtų į tai atsižvelgti planuodama pajėgumus[88];
- kai organizacija gauna pažeidžiamumo pranešimą, ji užtikrina, kad pranešimas kuo greičiau pasiektų tą skyrių, kuris turi daugiausiai kompetencijos jį įvertinti ir išnagrinėti;
- organizacija pranešančiajai šaliai išsiunčia pranešimo gavimo patvirtinimą;
- vėliau organizacija pradeda konsultacijas su pranešimą pateikusia šalimi, kad nustatytų laikotarpį, per kurį bus paskelbtas bet koks viešas skelbimas. Šis laikotarpis labai priklauso nuo pažeidžiamumo pobūdžio ir sistemos tipo. Paprastai programinės įrangos pažeidžiamumui nustatyti taikomas maždaug 60 dienų laikotarpis. Sunkiau ištaisomų techninės įrangos pažeidžiamumų atveju galima taikyti 6 mėnesių laikotarpį. Taip pat gali būti pageidaujama abipusiu susitarimu pratęsti arba sutrumpinti šį laikotarpį,

[86] „Coordinated Vulnerability Disclosure: the Guideline“. NCSC, 2018, p. 13.
[87] *Ibid.*
[88] *Pgl.* „Coordinated Vulnerability Disclosure: the Guideline“. NCSC, 2018, p. 13.

atsižvelgiant į tai, kiek IT sistemų priklauso nuo sistemos, kurioje buvo aptiktas pažeidžiamumas, arba ar pažeidžiamumą lengviau ar sunkiau pašalinti;

- pažeidžiamumą gali būti sunku pašalinti arba visai neįmanoma to padaryti, arba jį pašalinti gali prireikti didelių išlaidų. Tokiais atvejais organizacija gali sutikti pažeidžiamumą laikyti priimta rizika ir jos nepašalinti;
- organizacija informuos atskaitingą šalį apie proceso eigą;
- taip pat organizacija gali pasiūlyti, kad pranešusioji šalis būtų viešai pripažinta paskelbusi pažeidžiamumą. Taip pat galima pasirinkti bendrą viešą atskleidimą;
- pageidautina atlyginti pranešusiajai šaliai už pranešimą apie sistemų pažeidžiamumą, jei šalis laikėsi CVD politikos taisyklių. Atlygio dydis gali priklausyti nuo pranešimo kokybės. Apdovanojimas pranešančiajai šaliai gali sukurti geresnius santykius tarp tos šalies ir organizacijos, taip pat padidinti žmonių norą teikti naujas ataskaitas pagal CVD politiką;
- pasikonsultavusi su pranešusiąja šalimi, organizacija gali susitarti informuoti platesnę IT bendruomenę apie pažeidžiamumą, jei tikėtina, kad pažeidžiamumas yra ir kitose vietose;
- savo CVD politikoje organizacija gali įsipareigoti laikytis principo, kad ji nepateiks skundo policijai, jei pranešančioji šalis laikysis politikoje nustatytų taisyklių.

Pranešimo etapas. Pranešimą teikianti šalis yra sėkmingo CVD proceso raktas. Vienaip ar kitaip ši šalis sugebėjo nustatyti pažeidžiamumą ir nori prisidėti prie IT sistemų saugumo užtikrindama, kad ši spraga būtų pašalinta organizacijos ir paskelbta viešai. Tai darydamos pranešančios šalys pripažįsta, kad gali įnešti svarų indėlį į visuomenę, koordinuotai atskleisdamos pažeidžiamumą. Kad CVD procesas būtų sėkmingas, pranešimą teikiančiai šaliai svarbūs šie elementai[89]:

- pranešančioji šalis yra atsakinga už savo veiksmus ir tirdama pažeidžiamumą bei pranešdama apie jį turi laikytis proporcingumo ir subsidiarumo principų. Kitaip tariant, pranešančioji šalis neturėtų daryti daugiau, nei būtina pažeidžiamumui įrodyti, ir visada pirmiausia turėtų pranešti apie pažeidžiamumą sistemos / informacijos savininkui;
- pranešanti šalis turi kuo greičiau pranešti apie problemą, kad piktybinės šalys neaptiktų pažeidžiamumo ir juo nepasinaudotų;
- pranešančioji šalis turi pateikti pranešimą organizacijai konfidencialiai, kad kiti negalėtų gauti šios informacijos;

[89] *Ibid.,* p. 14.

- pranešančioji šalis negali reikalauti atlygio už pranešimo ar tolesnės informacijos teikimą. Iniciatyva skirti atlygį pranešimo atveju tenka gaunančiajai organizacijai, kuri savo paskelbtoje politikoje gali nurodyti išankstines sąlygas;
- pranešančioji šalis ir organizacija sudaro aiškius susitarimus dėl pažeidžiamumo atskleidimo. Jei dalyvauja daugiau nei viena organizacija, pagrindinis principas yra tas, kad pažeidžiamumas gali būti paskelbtas tik tada, kai visos organizacijos sutinka su šiuo faktu. Šiuos susitarimus patartina sudaryti ankstyvoje stadijoje;
- pranešimą teikianti šalis ir dalyvaujanti organizacija gali sudaryti susitarimus dėl platesnės IT bendruomenės informavimo, pvz., ši situacija gali būti taikoma pažeidžiamumui, kuris, kaip žinoma, yra daugiau nei vienoje vietoje.

NCSC-NL gali dalyvauti šiame procese, kad palaikytų tikslines centrinės valdžios ir ypatingos svarbos infrastruktūros grupes arba informuotų kelias šalis iškilus pažeidžiamumui, kuris paveikia daugelį sistemų.

Nacionalinis kibernetinio saugumo centras (NCSC-NL). Pažymėtina, jog CVD procesas visų pirma yra organizacijų ir atskaitingų šalių reikalas, tačiau nepaisant to, NCSC-NL skatina naudoti CVD procesą. Konsultuodamasis su pranešančia šalimi ir organizacija, NCSC-NL taip pat gali būti įtrauktas į dalijimąsi informacija apie pažeidžiamumą su savo apygarda, kad būtų apribota tolesnė saugumo rizika, kylanti dėl pažeidžiamumo. Jei pranešimas apie pažeidžiamumą vyksta ne taip, kaip tikisi pranešančioji šalis, arba jei ji nenorėtų tiesiogiai apie pažeidžiamumą pranešti organizacijai, ji gali susisiekti su NCSC-NL. Tokiu atveju NCSC-NL prireikus gali veikti kaip tarpininkas.[90]

IT sistemos savininkas visada yra atsakingas už sistemos saugumą. NCSC-NL negali priversti sistemos savininko ištaisyti pažeidžiamumą, taip pat negali garantuoti, kad savininkas nesiims teisinių veiksmų prieš pranešančią šalį, todėl pranešančioji šalis, ieškodama pažeidžiamumo ir pranešdama apie jį turi atsižvelgti į pirmiau minėtus elementus. Pranešimą teikianti šalis gali tikėtis, kad NCSC-NL padarys viską, ką gali, kad pažeidžiamumas būtų ištaisytas, ir pranešimą nagrinės konfidencialiai. NCSC-NL nesidalina jokiais asmens duomenimis, nebent yra teisiškai įpareigotas tai daryti. Jei įmanoma, NCSC-NL naudoja gautą informaciją apie pažeidžiamumą konsultuodamasis su organizacijomis ir pranešimus pateikusiomis šalimis, kad galėtų toliau dalytis žiniomis su IT bendruomene. [91]

NCSC-NL veiksmai koordinuoto spragų atskleidimo procese[92]:

[90] *Ibid.*
[91] *Ibid.*
[92] *Ibid.*

- atsižvelgdamas į atitinkamą organizaciją ir nustatyto pažeidžiamumo pobūdį, NCSC-NL deda pastangas, kad atkreiptų atitinkamos organizacijos dėmesį į pažeidžiamumą, tačiau atitinkamos IT sistemos savininkas lieka atsakingas už sistemą;
- kai įmanoma ir būtina, NCSC-NL pateikia atitinkamai organizacijai patarimų, kaip ištaisyti pažeidžiamumą;
- NCSC-NL pranešimus nagrinėja konfidencialiai ir nesidalina pranešimus teikiančių šalių ar gaunančios organizacijos asmens duomenimis be sutikimo, nebent tai išplaukia iš įstatymais numatytų įsipareigojimų;
- jei įmanoma, NCSC-NL informuoja pranešančią šalį apie ryšių su organizacija eigą ir pažeidžiamumo pašalinimą;
- tais atvejais, kai pranešimas pateikiamas NCSC-NL, NCSC-NL stengiasi suartinti pranešimą pateikusią šalį ir organizaciją;
- jei pranešančioji šalis aptiko programinės įrangos produkto pažeidžiamumą arba pažeidžiamumą, kuris turi įtakos daugeliui skirtingų sistemų, pranešančioji šalis gali paprašyti NCSC-NL koordinuoti pažeidžiamumo ištaisymą ir atskleidimą.

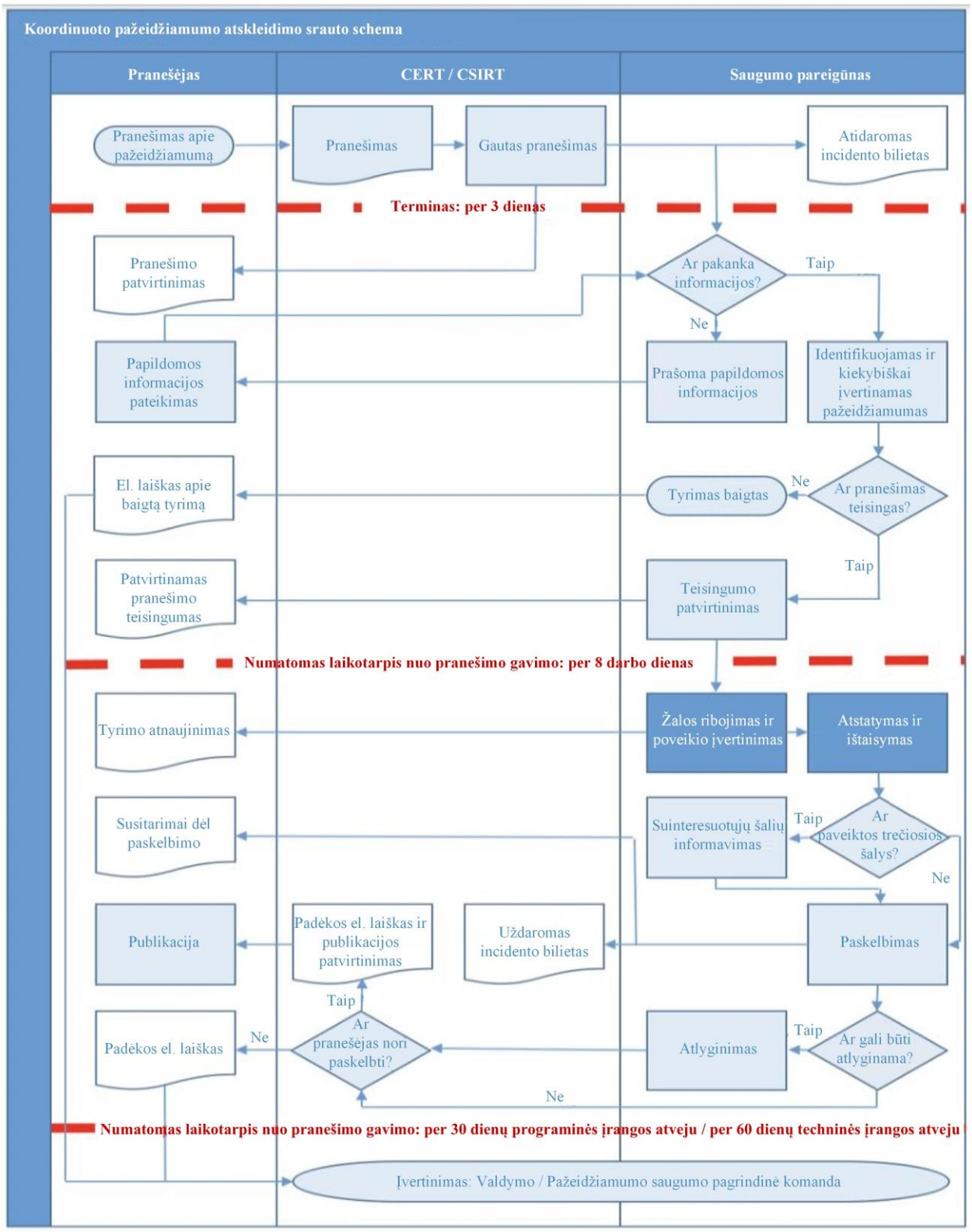
Kartu su pranešančia šalimi, partneriais ir (arba) programinės įrangos kūrėjais ir kitomis saugumo komandomis NCSC-NL padeda kontroliuojamai analizuoti, ištaisyti pažeidžiamumą, koordinuoti ir atskleisti pažeidžiamumą. Visas šis procesas vyksta glaudžiai konsultuojantis su pranešančia šalimi, kuri rado pažeidžiamumą.[93]

CVD politika bando rasti pusiausvyrą tarp svarbos kuo greičiau imtis priemonių dėl pažeidžiamumų atskleidimo ir svarbos, kad kūrėjai ir tiekėjai turėtų pakankamai laiko pažeidžiamumui ištaisyti. Šiam procesui NCSC-NL taiko standartinį 60 dienų terminą nuo pranešimo pateikimo iki viešo paskelbimo, tačiau gali būti aplinkybių, kurioms esant gali būti nuspręsta šį laikotarpį pratęsti arba sutrumpinti.[94]

NCSC-NL informacija apie pažeidžiamumą su trečiosiomis šalimis dalinasi tik pasikonsultavusi su pranešančia šalimi. Šiame kontekste labai svarbu paminėti, jog NCSC-NL bendradarbiauja ir dalinasi informacija apie pažeidžiamumą su suinteresuotosiomis šalimis, kad pažeidžiamumas būtų atskleistas koordinuotai. Tai darydama NCSC-NL užtikrina, kad tinkamos šalys galėtų dirbti ištaisydamos pažeidžiamumą, padeda apriboti nuostolius ar žalą bei padeda atkreipti dėmesį į rastą pažeidžiamumą.[95]

Atsakingo atskleidimo principo modelis. Žemiau pateikiama srauto diagrama, koordinuoto pažeidžiamumų atskleidimo procesas[96]:

[93] *Ibid.,* p. 15.
[94] *Ibid.*
[95] *Ibid.*
[96] „Coordinated Vulnerability Disclosure Model Policy and Procedure“. CIO Platform Nederland, 2016, p. 24.



Šaltinis: išversta pagal „Coordinated Vulnerability Disclosure Model Policy and Procedure“, p. 24

6 pav. **Koordinuoto pažeidžiamumo atskleidimo srauto schema**

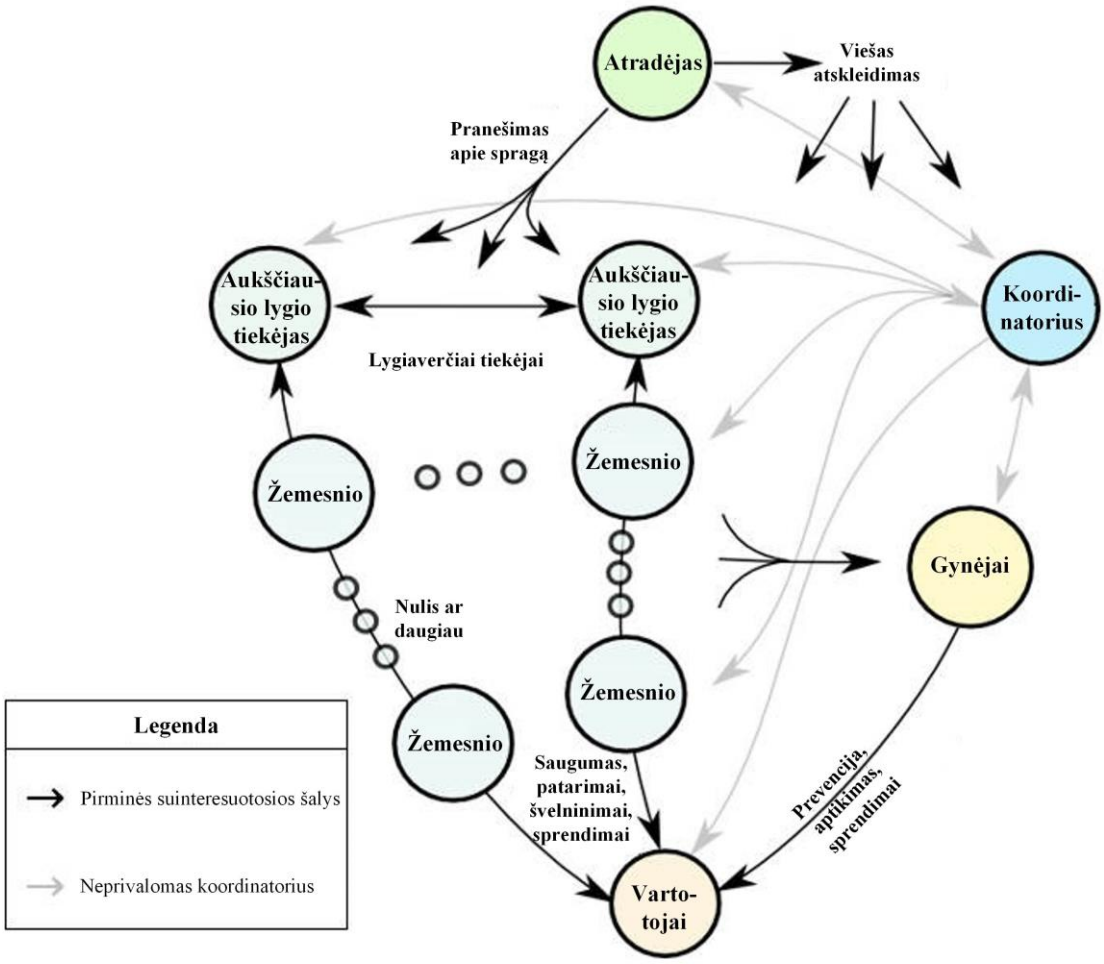
Kelių šalių suderintas pažeidžiamumo atskleidimas. Taip pat yra išskiriamas kelių šalių suderinto pažeidžiamumo atskleidimo (anglų k. *Multi-Party Coordinated Vulnerability Disclosure*) modelis – šiuo atveju CVD procese dalyvauja kelios šalys. Paprastai yra kelios

informaciją priimančiosios organizacijos – tai gali būti susiję su pažeidžiamumu keliuose produktuose arba su tuo pačiu produktu, kuris naudojamas keliose organizacijose. Kelių šalių informacijos atskleidimo procesas susijęs ne tik su informacijos atskleidimo koordinavimu, bet ir su bendradarbiavimu su įvairiomis šalimis ir tarp jų.[97]

Daugiašalio atskleidimo procese dažnai reikia, kad kas nors koordinuotų ir saugotų procesą. NCSC-NL gali imtis šio koordinatoriaus vaidmens, kad padėtų palaikyti procesą, kai pažeidžiamumas yra svarbus. Daugiašalio CVD proceso pavyzdys – 2015 m. Nyderlanduose vykdytas mokslinių tyrimų projektas, kurio metu buvo nustatyta, kad numatytieji belaidžių maršrutizatorių slaptažodžiai buvo nuspėjami. Radboudo universiteto tyrėjai kreipėsi į NCSC-NL prašydami paremti šį procesą – NCSC-NL pasinaudojo savo tinklu ir informavo įvairius Nyderlandų interneto paslaugų teikėjus, o šie su savo tiekėjais aptarė veiksmus, kad būtų galima naudotis atnaujinimais ir atlikti pakeitimus tiekimo grandinėje. Taigi, buvus keletui interneto tiekėjų, kurių kiekvienas turėjo skirtingus tiekėjus, į procesą buvo įtraukta daug šalių, dėl to visiems reikėjo sudaryti aiškius susitarimus ir kartu išlaikyti konfidencialumą.[98]

Pažymėtina, kad kelių šalių atskleidimas gali tapti daug sudėtingesnis nei įprastas pažeidžiamumo atskleidimo procesas – žemiau schemoje pavaizduoti skirtingi vaidmenys ir santykiai, iš kurių matyti, jog tai gali būti sudėtingas procesas[99]:

[97] „Multi-party disclosure - how does it work?“. Nacional Cyber Security Centre, 2021 [interaktyvus, žiūrėta: 2024-03-27]. Prieiga per internetą: https://english.ncsc.nl/latest/weblog/weblog/2021/multi-party-disclosure.
[98] *Ibid.*
[99] *Ibid.*



Šaltinis: išversta pagal „Multi-party disclosure - how does it work?“
7 pav. **Kelių šalių suderinto pažeidžiamumo atskleidimo schema**

Pažymėtina, jog skirtingos daugiašalio atskleidimo procese dalyvaujančios organizacijos turi skirtingus interesus ir kultūrą. Šiam procesui įtakos turi, pvz., atvirojo kodo bendruomenės, premijų už klaidas programos, sudėtingėjančios tiekimo grandinės arba skirtingi tiekėjų ir kitų organizacijų saugumo komandų vaidmenys. Kiekvienas iš šių veiksnių atlieka tam tikrą vaidmenį, o kiekviena organizacija yra suinteresuota pažeidžiamumų atskleidimu bei poveikio mažinimu, ir kiekviena – savaip.[100]

Apibendrinant tai, kas buvo išdėstyta, darytina išvada, jog Nyderlandai CVD politiką taiko jau seniai ir turi sukaupę nemažai patirties šioje srityje. Laikoma, kad CVD politika yra formali politika, nors Nyderlandų teisėje ir nėra nuorodos į CVD. CVD yra labai svarbus viešosioms ir privačiosioms įstaigoms, kadangi jos yra labai priklausomos nuo netrikdomo informacinių sistemų veikimo kasdienėje veikloje. Pranešimai apie jų sistemų pažeidžiamumus padeda pagerinti sistemų saugumą ir tęstinumą, o pašalinant pažeidžiamumus taip pat prisidedama prie bendro Nyderlandų įmonių informuotumo apie IT saugumą. CVD tikslas – prisidėti prie IT

[100] *Ibid.*

sistemų saugumo didinimo dalijantis žiniomis apie pažeidžiamumą: CVD metu žiniomis dalijamasi su viena ar keliomis potencialiai pažeidžiamomis organizacijomis, kad bendradarbiaujant su pranešančiąja šalimi būtų rastas bendras rastų pažeidžiamumų sprendimas.

2. ATSAKINGO ATSKLEIDIMO PRINCIPO ĮGYVENDINIMO VIEŠAJAME SEKTORIUJE MODELIO TYRIMO METODOLOGIJA

Šiame tyrime pasirinkta nagrinėti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelį, siekiant įvertinti jo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą. Nepaisant to, kad Lietuva yra viena iš pirmųjų ES šalių, įgyvendinusių atsakingo atskleidimo principą, vis dar stokojama išsamių jo taikymo viešajame sektoriuje tyrimų bei mokslininkų rekomendacijų šiuo klausimu. Šiuo tyrimu siekiama užpildyti minėtą spragą ir prisidėti prie efektyvesnio kibernetinio saugumo užtikrinimo Lietuvoje, kuris yra labai aktualus šiuolaikinėje visuomenėje. Autorius, nagrinėdamas atsakingo atskleidimo principo įgyvendinimą viešajame sektoriuje, siekia išryškinti esamus trūkumus, o tyrimo rezultatai gali būti naudingi formuojant strategijas ir politiką, siekiant stiprinti viešojo sektoriaus kibernetinį saugumą.

Tyrimo metodika. Siekiant išnagrinėti atsakingo atskleidimo principo įgyvendinimą viešajame sektoriuje ir jo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą, pasirinktas kokybinio tyrimo metodas.

Tyrimo objektas – atsakingo atskleidimo principo įgyvendinimas viešajame sektoriuje.

Tyrimo tikslas – išanalizuoti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelį ir remiantis gautais duomenimis įvertinti atsakingo atskleidimo principo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą.

Tyrimo uždaviniai:

1. Parinkti Lietuvos viešojo sektoriaus institucijas.
2. Įvertinti Lietuvos viešojo sektoriaus institucijų pasiruošimą atsakingo atskleidimo principo įgyvendinimui.
3. Ištirti, kaip pasirinktos institucijos įgyvendina atsakingo atskleidimo principą.
4. Nustatyti atsakingo atskleidimo principo įgyvendinimo poveikį institucijų kibernetinio saugumo užtikrinimui.

Tyrimo metodai. Tyrimui atlikti naudojami šie metodai:

1. **Juridinių dokumentų turinio (anglų k. *content*) analizė:** nagrinėjami teisės aktai, susiję su kibernetiniu saugumu ir atsakingo atskleidimo principo reglamentavimu Lietuvoje bei atsakingo atskleidimo principo įgyvendinimu viešojo sektoriaus institucijose, – įstatymai, nuostatai ir kiti oficialūs dokumentai.

2. **Pusiau struktūrizuotas interviu:** interviu metu apklausiami už atsakingo atskleidimo principo įgyvendinimą atsakingi viešojo sektoriaus institucijų darbuotojai. Šis metodas leidžia gauti įžvalgų iš praktinės pusės.

3. **Pusiau struktūrizuoto interviu kokybinė turinio (anglų k. *content*) analizė ir interpretavimas:** interviu metu gauti duomenys analizuojami ir interpretuojami, siekiant išskirti svarbiausias tendencijas, susijusias su atsakingo atskleidimo principo įgyvendinimu viešajame sektoriuje.

4. **Kokybinė gautų duomenų analizė:** tyrimo metu gauti duomenys apibendrinami ir įvertinami, siekiant atsakyti į tyrimo klausimus bei pasiūlyti rekomendacijas.

Tyrimo imtis. Kokybinės strategijos tyrimo imties sudarymui taikyta netikimybinė tikslinė atranka tikslingai renkantis 15 didžiausių valstybės valdomų įmonių[101], kurios, remiantis Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu[102], yra svarbios Lietuvos Respublikos nacionaliniam saugumui užtikrinti, bei Vilniaus miesto savivaldybę, kuri jau kelerius metus įgyvendina atsakingo atskleidimo programą.

Tyrimo ribotumas. Nė viena iš 15 tirtų valstybės valdomų įmonių nėra parengusi ir paskelbusi atsakingo spragų atskleidimo tvarkos, todėl darbe analizuojamas tik Vilniaus miesto savivaldybės atsakingo spragų atskleidimo principo įgyvendinimo modelis.

Tyrimo eiga:

1-as etapas. Šiame etape atliekamas tyrimas, ar 15 didžiausių valstybės valdomų įmonių, kurios, remiantis Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu, yra svarbios Lietuvos Respublikos nacionaliniam saugumui užtikrinti, yra parengusios ir savo interneto svetainėse paskelbusios atsakingo spragų atskleidimo tvarkas.

2-as etapas. Šiame etape atliekamas pusiau struktūrizuotas interviu su Vilniaus miesto savivaldybės atstove apie atsakingo atskleidimo programos įgyvendinimą Vilniaus miesto savivaldybėje. Tyrimu siekiama išanalizuoti atsakingo atskleidimo principo įgyvendinimo Vilniaus miesto savivaldybėje modelį.

3-ias etapas. Šiame etape aptariami gauti rezultatai, siekiant įvertinti atsakingo atskleidimo principo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą.

[101] Remiantis Valdymo koordinavimo centro duomenimis [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://governance.lt/apie-imones/vvi-sarasas/.

[102] Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas (su pakeitimais ir papildymais). Valstybės žinios, 2002-10-30, Nr. 103-4604.

1 lentelė. **Tyrimo instrumentarijus**

Tyrimo kriterijai	Tyrimo indikatoriai	Tyrimo metodai
Atsakingo atskleidimo principo raiška viešajame sektoriuje.	1. Atsakingo atskleidimo principo teisinis reglamentavimas. 2. Atsakingo atskleidimo principo įgyvendinimo priemonės.	Juridinių dokumentų turinio analizė.
Atsakingo atskleidimo principo įgyvendinimo viešojo sektoriaus institucijose modelio analizė.	1. Viešojo sektoriaus institucijų pasiruošimo atsakingo atskleidimo principo įgyvendinimui nustatymas. 2. Atsakingo atskleidimo principo įgyvendinimo viešojo sektoriaus institucijose problematikos atskleidimas. 3. Bendrų atsakingo atskleidimo principo įgyvendinimo viešojo sektoriaus institucijose tendencijų nustatymas.	1. Juridinių dokumentų turinio analizė. 2. Pusiau struktūrizuoto interviu kokybinė turinio analizė ir interpretavimas. 3. Kokybinė gautų duomenų analizė.
Atsakingo atskleidimo principo įgyvendinimo veiksmingumo viešojo sektoriaus institucijų kibernetinio saugumo užtikrinimui pagrindimas.	1. Gaunamų pranešimų apie kibernetinio saugumo spragas skaičiaus nustatymas. 2. Kibernetinių atakų skaičiaus pradėjus įgyvendinti atsakingo atskleidimo principą pokyčio analizė. 3. Santykio tarp gaunamų pranešimų apie kibernetinio saugumo spragas ir kibernetinių atakų skaičiaus pokyčio nustatymas.	1. Juridinių dokumentų turinio analizė. 2. Pusiau struktūrizuoto interviu kokybinė turinio analizė ir interpretavimas. 3. Kokybinė gautų duomenų analizė.

3. ATSAKINGO ATSKLEIDIMO PRINCIPO ĮGYVENDINIMO VIEŠAJAME SEKTORIUJE MODELIO TYRIMO ANALIZĖ

Nepaisant to, kad teisės aktai nustato, iš pirmo žvilgsnio, gana aiškų atsakingo spragų atskleidimo procesą, visgi, autoriaus nuomone, pasigendama platesnės informacijos, rekomendacijų, mokymų dėl praktinio jo įgyvendinimo.

Teisės aktais įtvirtinant atsakingo atskleidimo principą, buvo siekiama apsaugoti kibernetinio saugumo subjektus nuo kibernetinio saugumo spragų galimos žalos arba ženkliai ją sumažinti ir taip pat prisidėti prie visapusės kibernetinio saugumo brandos augimo Lietuvoje, tačiau šis tikslas nebus pasiektas, jei teisės aktų nuostatos nebus įgyvendinamos praktiškai, t. y., jei šio principo įmonės ir organizacijos neįgyvendins ar tai darys nepakankamai savo organizacijos viduje.

Šioje darbo dalyje bus nagrinėjama atsakingo atskleidimo principo raiška viešajame sektoriuje, Vilniaus miesto savivaldybės atsakingo spragų atskleidimo programa, analizuojamas atsakingo atskleidimo principo įgyvendinimo šioje viešojo sektoriaus institucijoje modelis bei siekiama pagrįsti atsakingo atskleidimo principo įgyvendinimo veiksmingumą užkrintant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą.

3.1. Atsakingo atskleidimo principo raiška viešajame sektoriuje

Autorius, siekdamas išsiaiškinti, ar viešojo sektoriaus institucijos įgyvendina atsakingo spragų atskleidimo procesą savo organizacijoje ir yra paskelbusios atsakingo spragų atskleidimo tvarkas, apžvelgė 15 didžiausių valstybės valdomų įmonių, kurios, remiantis Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu, yra svarbios Lietuvos Respublikos nacionaliniam saugumui užtikrinti ir kurių kibernetinio saugumo užtikrinimas yra itin svarbus valstybės atžvilgiu. Informacijos apie atsakingą spragų atskleidimą buvo ieškoma šių valstybės valdomų įmonių interneto svetainėse:

1. AB „Ignitis grupė“[103] (energetikos sektorius);
2. UAB „EPSO-G“ įmonių grupė[104] (energetikos sektorius);
3. AB „KN Energies“[105] (energetikos sektorius);
4. VĮ Ignalinos atominė elektrinė[106] (energetikos sektorius);
5. AB „Lietuvos geležinkeliai“ įmonių grupė[107] (susisiekimo sektorius);

[103] AB „Ignitis grupė“ [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://www.ignitisgrupe.lt/.
[104] UAB „EPSO-G“ įmonių grupė [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://www.epsog.lt/.
[105] AB „KN Energies“ [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://www.kn.lt/.
[106] VĮ Ignalinos atominė elektrinė [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://www.iae.lt/.
[107] AB „Lietuvos geležinkeliai“ įmonių grupė [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://ltg.lt/.

6. AB Lietuvos pašto įmonių grupė[108] (susisiekimo sektorius);
7. AB Lietuvos radijo ir televizijos centras[109] (susisiekimo sektorius);
8. AB „Kelių priežiūra“[110] (susisiekimo sektorius);
9. AB „Oro navigacija“[111] (susisiekimo sektorius);
10. AB Klaipėdos valstybinio jūrų uosto direkcija[112] (susisiekimo sektorius);
11. AB Lietuvos oro uostai[113] (susisiekimo sektorius);
12. AB Vidaus vandens kelių direkcija[114] (susisiekimo sektorius);
13. AB „Via Lietuva”[115] (susisiekimo sektorius);
14. VĮ Valstybinių miškų urėdija[116] (miškininkystės sektorius);
15. VĮ Registrų centras[117] (sektorius – kita).

Pamėginus ieškoti informacijos, susijusios su kibernetinių spragų atskleidimo procesu, minėtų įmonių interneto svetainėse jos rasti nepavyko, tad darytina išvada, jog įmonės atsakingo spragų atskleidimo tvarkų nėra parengusios ir paskelbusios. Žinoma, tokiu atveju kibernetinio saugumo spragą šių įmonių sistemose radęs asmuo apie ją turėtų pranešti NKSC, tačiau tai, kad įmonės nėra paskelbusios jokios informacijos, iš dalies rodo, jog kibernetinio saugumo užtikrinimas nėra šių institucijų prioritetinis klausimas.

Šiame kontekste pažymėtina, jog per 2022 m. NKSC sulaukė 51 pranešimo iš kibernetinio saugumo specialistų apie galimas spragas valstybinių institucijų interneto svetainėse – buvo gauta vertingos informacijos apie svarbių sistemų saugumo spragas, tarp kurių viešajame sektoriuje populiari dokumentų valdymo sistema „Avilys“ bei viešojo sektoriaus valdomos informacinės sistemos. Tuo tarpu 2021 m., laikydamasis atsakingo atskleidimo principų, NKSC gavo 81 pranešimą apie įvairias kibernetinio saugumo spragas.[118]

Autoriaus nuomone, atsakingo spragų atskleidimo principo įgyvendinimui praktikoje sunkumų gali kelti šie veiksniai:

1. Žinių stoka;
2. Atsainus įstaigų vadovų požiūris į kibernetinio saugumo užtikrinimo svarbą;
3. Informacinių technologijų specialistų trūkumas arba nepakankama jų kompetencija;

[108] AB Lietuvos pašto įmonių grupė [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://www.post.lt/.
[109] AB Lietuvos radijo ir televizijos centras [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://www.telecentras.lt/.
[110] AB „Kelių priežiūra“ [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://keliuprieziura.lt/.
[111] AB „Oro navigacija“ [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://www.ans.lt/.
[112] AB Klaipėdos valstybinio jūrų uosto direkcija [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://portofklaipeda.lt/.
[113] AB Lietuvos oro uostai [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://ltou.lt/.
[114] AB Vidaus vandens kelių direkcija [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://vvkd.lt/.
[115] AB „Via Lietuva” [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://vialietuva.lt/.
[116] VĮ Valstybinių miškų urėdija [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://vmu.lt/.
[117] VĮ Registrų centras [interaktyvus, žiūrėta: 2024-02-18]. Prieiga per internetą: https://www.registrucentras.lt/.
[118] 2022 m. Nacionalinė kibernetinio saugumo būklės ataskaita. Lietuvos Respublikos krašto apsaugos ministerija, p. 13.

4. Atsakomybės, papildomo darbo krūvio vengimas.

Žinių stoka. Kaip jau buvo minėta, autoriaus nuomone, pasigendama platesnės informacijos ir išsamesnių paaiškinimų, kaip atsakingo spragų atskleidimo procesas turėtų būti įgyvendinamas – nuo teisinio reglamentavimo organizacijos viduje iki bendradarbiavimo su pranešėjais, NKSC ir kitais kibernetinio saugumo subjektais organizavimo, kad kibernetinio saugumo subjektams būtų aišku, ko iš jų yra tikimasi ir suprastų bei žinotų, kaip reikalavimus tinkamai įgyvendinti.

Vertinant plačiąją prasme, autoriaus nuomone, valstybė turėtų daugiau dėmesio skirti visuomenės švietimui apie kibernetinį saugumą ir jo svarbą užtikrinant, kad visos susijusios suinteresuotosios šalys, o taip pat ir piliečiai, įskaitant mokyklinio amžiaus vaikus, bei verslo atstovai gautų tvarius mokymus. Kaip tokio atvejo pavyzdį galima pateikti Samoa valstybę, kuri suprasdama, kad kibernetinis saugumas yra bendra visų interneto vartotojų bendra atsakomybė ir siekdama ugdyti bei stiprinti skaitmeninius piliečių gebėjimus, Nacionalinėje kibernetinio saugumo strategijoje[119] yra numačiusi mokymo programų tam tikrų sričių specialistams (pvz., teisėsaugos pareigūnams, finansininkams, prokurorams, paslaugų tiekėjams, teisėjams, komunikacijos specialistams, IT inžinieriams) rengimą bei kitų suinteresuotųjų šalių mokymą.

Atsainus įstaigų vadovų požiūris į kibernetinio saugumo užtikrinimo svarbą. Stingant kibernetinio saugumo užtikrinimo svarbos akcentavimo, taip pat išaiškinimų, mokymų, kaip tinkamai įgyvendinti numatytus teisės aktų reikalavimus, neretai pastebimas atsainus įstaigų vadovų požiūris į kibernetinį saugumą. Manytina, kad tam įtakos turi ir tai, jog kokybiškas įmonės kibernetinio saugumo užtikrinimas reikalauja nemažai lėšų, todėl šiai sričiai, kol nenukenčiama, nėra skiriama pakankamai dėmesio ir investicijų.

Būtina atkreipti dėmesį į tai, kad atsainus įstaigų, ypatingai – svarbių šalies nacionaliniam saugumui užtikrinti, vadovų požiūris į kibernetinio saugumo užtikrinimo svarbą gali turėti ilgalaikių neigiamų padarinių, įskaitant teikiamų paslaugų teikimo sutrikdymą, duomenų nutekėjimą, finansinius nuostolius ir reputacijos žalą. Taigi, dėl šių priežasčių yra labai svarbu, kad organizacijos vadovai suprastų kibernetinio saugumo svarbą ir įsipareigotų skirti pakankamai dėmesio bei resursų šiai sričiai.

Informacinių technologijų specialistų trūkumas arba nepakankama jų kompetencija. Tai, kad informacinių technologijų specialistų trūksta, nėra paslaptis. Kompetentingų informacinių technologijų specialistų trūkumas ypatingai juntamas viešojo sektoriaus institucijose, kur šios srities darbuotojus sunku pritraukti ir išlaikyti dėl sąlyginai mažo, lyginant su privačiu sektoriumi, darbo užmokesčio dydžio. Remiantis skaitmeninių technologijų

[119] Samoa National Cybersecurity Strategy 2016-2021. Ministry of Communication and Information Technology, p. 10.

sektoriaus asociacijos „Infobalt“ duomenimis[120], Lietuvoje trūksta daugiau nei 13 tūkst. specialistų. Taigi, mažai tikėtina, kad institucijos kibernetinis saugumas gali būti tinkamai užtikrinamas neturint pakankamai kompetentingų šios srities specialistų.

Autoriaus nuomone, kompetentingų informacinių technologijų specialistų pritraukimas į viešojo sektoriaus institucijas ir išsaugojimas jose turėtų būti skatinamas valstybės lygiu. Kaip pavyzdį, kaip to būtų galima siekti, galima pateikti Suomiją, kurios Nacionalinėje kibernetinio saugumo strategijoje[121] pabrėžiama svarba nacionalinėms įmonėms rasti būdų, kaip didėjant tarptautinei konkurencijai išlaikyti geriausius savo informacinių technologijų specialistus.

Autoriaus nuomone, trūkstant informacinių technologijų specialistų, esami darbuotojai linkę vengti prisiimti atsakomybę ir atsirandantį papildomą darbo krūvį, taip pat to daryti nemotyvuoja ir gaunamas mažas darbo užmokestis.

Apibendrinus tai, kas buvo išdėstyta, darytina išvada, kad, nors atsakingo spragų atskleidimo principo teisinis reglamentavimas yra pakankamas, jo praktinis įgyvendinimas yra problematiškas ir pačios viešojo sektoriaus institucijos vis dar nėra linkusios jį savarankiškai taikyti savo viduje.

3.2. Vilniaus miesto savivaldybės atsakingo atskleidimo programa

Bene viena pirmųjų viešojo sektoriaus institucijų, pradėjusių įgyvendinti atsakingo spragų atskleidimo procesą, buvo Vilniaus miesto savivaldybė, kuri paskelbė atsakingo atskleidimo programą „Surask spragas, jei gali“ (anglų k. *„Hack me if you can“*). Kaip skelbiama, Vilniaus miesto savivaldybė, „rūpindamasi savo ir kitų saugumu, 2020-ųjų vasario mėn. pradėjo taikyti atsakingo atskleidimo politiką.“[122]

Savivaldybė savo interneto svetainėje kviečia „pilietiškus vilniečius ir visus, kurie nori prisidėti prie Vilniaus miesto kibernetinio saugumo didinimo ir pasižada laikytis nustatytų taisyklių, dalyvauti Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programoje.“[123] Taip pat teigiama, kad minėta programa „įgalina asmenį, nepažeidžiant galiojančių teisės aktų, neatlygintinai identifikuoti kibernetinio saugumo spragas, apie jas pranešti Vilniaus miesto savivaldybės administracijai, o jas pašalinus apie tai pasidalinti informacija su kitais.“[124]

---

[120] IRT specialistų pasiūlos ir paklausos tyrimas „IRT specialistai Lietuvoje: situacija darbo rinkoje ir darbdavių poreikiai“. „Infobalt“, „Investuok Lietuvoje“, p. 20.
[121] Finland‘s Cyber Security Strategy 2019. The Security Committee p. 8.
[122] „Atsakingo atskleidimo politika Vilniaus m. savivaldybėje“ [interaktyvus, žiūrėta: 2024-04-13]. Prieiga per internetą: https://www.nrdcs.lt/klientu-istorijos/atsakingo-atskleidimo-politika-vilniaus-m-savivaldybeje/.
[123] „Hack me if you can“ [interaktyvus, žiūrėta: 2024-04-13]. Prieiga per internetą: https://vilnius.lt/lt/vilnius-2in/kibernetinis-saugumas.
[124] *Ibid.*

Pažymėtina, kad Vilniaus miesto savivaldybės vykdoma atsakingo atskleidimo programa „Surask spragas, jei gali“ turi nustatytas aiškias ribas – spragų dalyvaujant programoje galima ieškoti tik šiose Vilniaus miesto savivaldybės administracijos valdomose informacinėse sistemose:

1) active.vilnius.lt
2) aktai.vilnius.lt
3) api-tvarkau.vilnius.lt
4) api.vilnius.lt
5) atviras.vilnius.lt
6) avilys.vilnius.lt
7) dalyvauk.vilnius.lt
8) darboviete.vilnius.lt
9) ebalsavimas.vilnius.lt
10) ivs.vilnius.lt
11) konkursai.vilnius.lt
12) login.vilnius.lt
13) paslaugos.vilnius.lt
14) patalpunuoma.vilnius.lt
15) sup.vilnius.lt
16) svietimas.vilnius.lt
17) tvarkaumiesta.lt
18) vilnius.lt

Taip pat apibrėžta, kad kibernetinio saugumo spraga yra programinės įrangos ir (ar) techninės įrangos ir (ar) internetinės paslaugos pažeidžiamumas, kuris gali būti išnaudotas kibernetinės atakos metu ir kelia grėsmę informacijos saugumui[125].

Vilniaus miesto savivaldybės vykdomojo atsakingo atskleidimo programoje gali dalyvauti ne jaunesnis kaip 18 metų fizinis asmuo, pasirašęs konfidencialumo pasižadėjimą, arba nepilnametis nuo 14 iki 18 metų, pateikęs tėvų (rūpintojų) rašytinį sutikimą bei pasirašęs konfidencialumo pasižadėjimą, ir neatlygintinai identifikuojantis spragas[126].

Kaip numatyta Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programoje, atsakingo atskleidimo programos įgyvendinimą sudaro šie 4 etapai:

[125] Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programa, patvirtinta Vilniaus miesto savivaldybės administracijos direktoriaus 2020 m. vasario 10 d. įsakymu Nr. 30-317/20 „Dėl Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programos tvirtinimo“ [interaktyvus, žiūrėta: 2024-04-13]. Prieiga per internetą: https://aktai.vilnius.lt/document/30336083.
[126] *Ibid.*

1. Programos dalyvio registracija;
2. Pranešimas apie identifikuotą spragą;
3. Spragos šalinimas;
4. Informacijos, susijusios su spragos identifikavimu, viešinimas.

Vilniaus miesto savivaldybė taip pat griežtai apibrėžusi, kas spragų identifikavimo metu yra draudžiama:[127]

- viršyti programos ribas – trikdyti ir keisti kompiuterinio tinklo, duomenų banko ar informacinės sistemos darbą;
- vykdyti DDoS ir kitokias atakas, kurios gali pakenkti ar kitaip daryti įtaką Vilniaus miesto savivaldybės administracijos valdomoms informacinėms sistemoms, paslaugų ar duomenų patikimumui bei vientisumui;
- naudoti socialinės inžinerijos atakas;
- bandyti fiziškai paveikti infrastruktūrą arba bandyti naudoti fizinio poveikio priemones (bandyti patekti į patalpas, gadinti techninę įrangą);
- atlikti veiksmus, kurie leistų programos dalyviui ar trečiosioms šalims pasiekti, išsaugoti, sunaikinti ar kitais būdais paveikti Vilniaus miesto savivaldybės administracijos valdomus duomenis;
- naudotis aptiktomis spragomis siekiant finansinės naudos ar pažeisti Lietuvos Respublikos teisės aktų reikalavimus;
- daryti poveikį elektroniniams duomenims, juos perimti ir naudoti kitais tikslais;
- skelbti viešai ar kitaip dalintis informacija apie aptiktas spragas, apie tai nepranešus Vilniaus miesto savivaldybės administracijai ir nesuderinus informacijos viešinimo sąlygų.

Taip pat numatyta, kad aptikus spragą būtina nutraukti su jos identifikavimu susijusią veiklą ir pranešti apie spragą Vilniaus miesto savivaldybės administracijai tiesiogiai užpildant elektroninę pranešimo formą. Viešai skelbti informaciją, susijusią su spragos identifikavimu programos dalyvis gali tik gavęs patvirtinimą apie spragos pašalinimą ir suderinęs viešinimo sąlygas su Vilniaus miesto savivaldybės administracija.[128] Be to, pabrėžiama, kad:

- informacijos viešinimas turi būti etiškas ir nenaudojamas siekiant tiesioginės finansinės naudos iš Vilniaus miesto savivaldybės administracijos;
- paviešinta informacija neturi sukelti žalos Vilniaus miesto savivaldybės administracijai ar tretiesiems asmenims;

[127] „Hack me if you can“ [interaktyvus, žiūrėta: 2024-04-13]. Prieiga per internetą: https://vilnius.lt/lt/vilnius-2in/kibernetinis-saugumas.
[128] *Ibid.*

- iš skelbiamos informacijos privalo būti pašalinti asmens duomenys;
- skelbiamas tekstas neturi kurstyti nesantaikos ir patyčių.

Apibendrinant tai, kas buvo išdėstyta, darytina išvada, kad įstaigos, kurios rūpinasi savo kibernetinio saugumo užtikrinimu, reikalingus atsakingo spragų atskleidimo procesus sėkmingai vykdo savo iniciatyva. Atkreiptinas dėmesys į tai, kad Vilniaus miesto savivaldybė atsakingo atskleidimo programą pradėjo vykdyti 2020 metais, kai atsakingo spragų atskleidimo principas dar nebuvo įtvirtintas įstatymu, tačiau Vilniaus miesto savivaldybei tai nebuvo kliūtis pradėti taikyti atsakingo atskleidimo politiką.

3.3. Atsakingo atskleidimo principo įgyvendinimo viešojo sektoriaus institucijose modelio analizė

Kaip buvo minėta anksčiau, siekiant išsiaiškinti, ar viešojo sektoriaus institucijos įgyvendina atsakingo spragų atskleidimo procesą savo organizacijoje ir yra paskelbusios atsakingo spragų atskleidimo tvarkas, buvo apžvelgta 15 didžiausių valstybės valdomų įmonių, kurios, remiantis Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu, yra svarbios Lietuvos Respublikos nacionaliniam saugumui užtikrinti ir kurių kibernetinio saugumo užtikrinimas yra itin svarbus valstybės atžvilgiu, tačiau informacijos, susijusios su kibernetinių spragų atskleidimo procesu, minėtų įmonių interneto svetainėse rasti nepavyko.

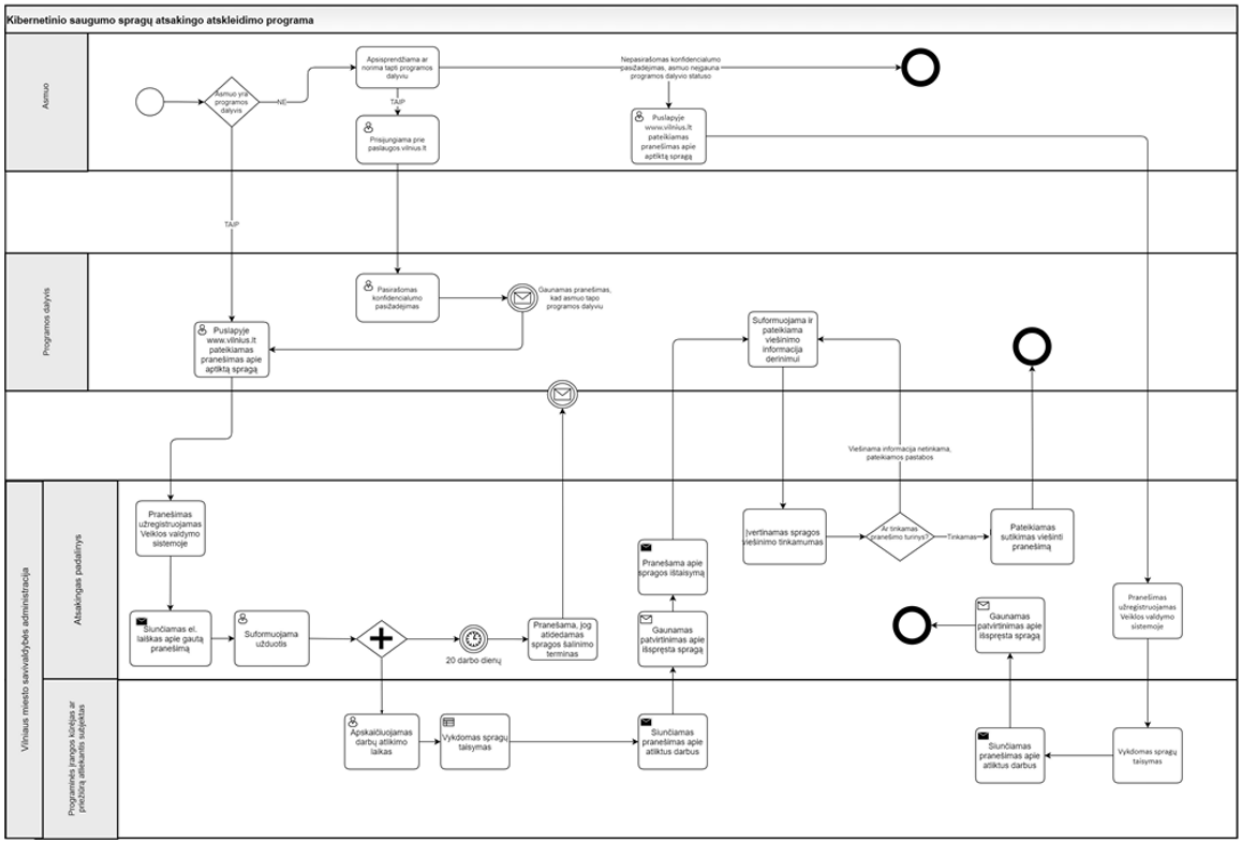
Taigi, dėl tyrimo duomenų ribotumo šioje darbo dalyje analizuojamas Vilniaus miesto savivaldybės atsakingo atskleidimo principo įgyvendinimo modelis.

Programos paskirtis ir tikslas

Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programoje[129] reglamentuojama, jog Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programos paskirtis – sukurti procesą, suteikiantį galimybę asmeniui nepažeidžiant galiojančių teisės aktų identifikuoti kibernetinio saugumo spragas, apie jas pranešti, efektyviai valdyti tokius pranešimus, šalinti rastus pažeidžiamumus, apibrėžti savivaldybės administracijos ir apie kibernetinio saugumo spragą pranešusio asmens teises ir pareigas, nustatyti informacijos, susijusios su kibernetinio saugumo spragų identifikavimu, viešinimo sąlygas.

[129] Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programa, patvirtinta Vilniaus miesto savivaldybės administracijos direktoriaus 2020 m. vasario 10 d. įsakymu Nr. 30-317/20 „Dėl Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programos tvirtinimo“ [interaktyvus, žiūrėta: 2024-04-14]. Prieiga per internetą: https://aktai.vilnius.lt/document/30336083.

Programos tikslas – kontroliuoti ir apsaugoti savivaldybės administracijos informacinių technologijų infrastruktūrą įtraukiant kuo daugiau pilietinės visuomenės narių, galinčių prisidėti prie šių sistemų neatlygintino vertinimo ir tobulinimo. Programoje taip pat nurodoma, jog programos įgyvendinimą sudaro procesas, kurio metu kibernetinio saugumo spragos atskleidimas koordinuojamas su asmeniu, pranešusiu apie kibernetinio saugumo spragą, Vilniaus miesto savivaldybės administracija ir subjektu, kurio sistemose buvo aptikta kibernetinio saugumo spraga.[130]



Šaltinis: Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programa

8 pav. **Kibernetinio saugumo spragos atsakingo atskleidimo proceso schema**

Dalyvavimas programoje

Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programoje[131] numatyta, jog programos įgyvendinime dalyvauja savivaldybės atsakingas padalinys ir programos dalyviai, siekiantys identifikuoti spragas dalyvaujant programoje. Asmuo, pretenduojantis dalyvauti programoje, negali būti savivaldybės administracijos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį ar darbuotojų artimieji giminaičiai, kaip apibrėžta Lietuvos Respublikos civilinio kodekso 3.135 straipsnyje.

[130] *Ibid.*
[131] *Ibid.*

Kaip jau buvo užsiminta anksčiau, spragų gali būti ieškoma tik internetinėje svetainėje *vilnius.lt* nurodytose savivaldybės administracijos valdomose informacinėse sistemose, o programos įgyvendinimas susideda iš šių keturių etapų[132]:

1. Programos dalyvio registracija;
2. Pranešimas apie identifikuotą spragą;
3. Spragos šalinimas;
4. Informacijos, susijusios su spragos identifikavimu, viešinimas.

Programos dalyvio registracija apima asmens identifikavimą, registracijos formos užpildymą ir konfidencialumo pasižadėjimo pasirašymą[133]:

- asmuo, siekiantis dalyvauti programoje, internetinėje svetainėje *paslaugos.vilnius.lt* pasirenka „Registracija dalyvauti kibernetinio saugumo spragų atsakingo atskleidimo programoje“ ir prisijungia naudodamasis asmens tapatybę identifikuojančiomis priemonėmis, elektroninių valdžios vartų paslauga;
- atsivėrusiame lange asmeniui pasiūloma pasirašyti konfidencialumo pasižadėjimą siekiant užtikrinti teisiškai apibrėžtą ir kontroliuojamą atsakingo atskleidimo procesą;
- asmuo konfidencialumo pasižadėjimą užpildo tiesiogiai internetinėje svetainėje *paslaugos.vilnius.lt* arba jį atsisiunčia, atsispausdina, pasirašo ir nuskenavęs atsiunčia el. paštu *security@vilnius.lt*;
- pasirašęs konfidencialumo pasižadėjimą svetainėje ir gavęs dalyvio registracijos numerį arba gavęs elektorinį patvirtinimą apie gautą skenuotą jo versiją ir suteiktą dalyvio registracijos numerį asmuo įgauna programos dalyvio statusą bei pradeda dalyvauti programoje.

Pažymėtina, jog konfidencialumo pasižadėjimas galioja vienerius metus nuo jo tiesioginio pasirašymo svetainėje arba nuo elektroninio patvirtinimo apie gautą skenuotą jo versiją išsiuntimo. Asmuo, norintis tęsti dalyvavimą programoje, privalo iš naujo pasirašyti konfidencialumo pasižadėjimą, o asmuo, jo nepasirašęs, tačiau aptikęs spragą ir apie ją pranešęs, yra kviečiamas dalyvauti programoje ir pasirašyti konfidencialumo pasižadėjimą:

- asmeniui užpildžius konfidencialumo pasižadėjimą ir gavus dalyvio registracijos numerį jis tampa programos dalyviu su visomis iš to kylančiomis teisėmis ir pareigomis;
- asmeniui nesutikus pasirašyti konfidencialumo pasižadėjimo spraga šalinama programos numatyta tvarka, tačiau bendradarbiavimo santykiai tarp jo ir savivaldybės administracijos neatsiranda ir informacijos, susijusios su spragos identifikavimu, viešinimas, platinimas ar dalijimasis su trečiosiomis šalimis be atsakingo padalinio

[132] *Ibid.*
[133] *Ibid.*

sutikimo yra draudžiamas, o atsakingam padaliniui įvertinus tokį veiksmą kaip keliantį žalą savivaldybės administracijos valdomiems procesams, tvarkomų duomenų integralumui, konfidencialumui ar vientisumui paliekama teisė kreiptis į atitinkamas institucijas dėl neteisėtos asmens veikos pagal galiojančius Lietuvos Respublikos teisės aktus.

Pranešimas apie spragą ir jo nagrinėjimas

Kaip numatyta Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programoje[134], programos dalyvis aptikęs spragą apie ją informuoja atsakingą padalinį internetinėje svetainėje *vilnius.lt* tiesiogiai užpildydamas elektroninę formą „Pranešimas apie aptiktą saugumo spragą“ ir detaliai nurodydamas aplinkybes bei identifikuotos spragos detales.

Pranešime apie aptiktą spragą turi būti nurodyta[135]:

- programos dalyvio registracijos numeris, suteiktas asmeniui užsiregistravus dalyvauti programoje, programos dalyvio vardas ir pavardė, jeigu pranešėjas nėra programos dalyvis, taip pat ir kontaktiniai duomenys;
- išsamus spragos aprašymas, įskaitant išnaudojimo galimybes ir poveikį;
- žingsniai, reikalingi spragos išnaudojimo galimybei atkurti;
- bet kokia kita papildoma informacija, galinti padėti įvertinti ir pašalinti spragą.

Savivaldybei gavus pranešimą apie spragą automatiškai generuojamas patvirtinimas programos dalyviui apie pateiktą pranešimą, o atsakingo padalinio veiklos valdymo sistemoje automatiškai sukuriama nauja užduotis, į kurią perkeliama visa programos dalyvio pateikta informacija. Atsakingo padalinio darbuotojas, atsakingas už pranešimų apie aptiktą spragą administravimą, įvertina, ar spraga identifikuota laikantis programos ribų ir nuostatų, pažeidžiamumo svarbą bei suformavęs pažeidžiamumo sprendimo užduotį ją perduoda programinės įrangos kūrėjui ar priežiūrą atliekančiam subjektui.[136]

Numatyta, jog spraga turi būti pašalinta per 20 darbo dienų, tačiau atsiradus objektyvioms priežastims šis terminas gali būti atidėtas, tačiau tuomet atsakingas padalinys informuoja programos dalyvį nurodydamas termino atidėjimo priežastis ir viešinimo atidėjimo terminą iki bus pašalinta spraga arba suderinamas informacijos, kuri nesukeltų žalos savivaldybės

[134] *Ibid.*
[135] *Ibid.*
[136] *Ibid.*

administracijai ar tretiesiems asmenims, viešinimas. Atsakingas savivaldybės padalinys su programos dalyviu bendrauja programos dalyvio nurodytais kontaktais.[137]

Atsakingas savivaldybės padalinys gavęs pranešimą ir įsitikinęs, kad programinės įrangos kūrėjas ar priežiūrą atliekantis subjektas spragą pašalino, siunčia pranešimą programos dalyviui, o programos dalyvis gavęs pranešimą iš atsakingo padalinio apie spragos pašalinimą gali paviešinti informaciją, susijusią su spragos identifikavimu, prieš tai ją suderinęs su atsakingu padaliniu. Pažymėtina, jog informacijos viešinimas turi būti etiškas ir jam taikomi konfidencialumo pasižadėjime numatyti reikalavimai [138]:

- programos dalyvis neturi siekti tiesioginės ar netiesioginės finansinės naudos iš savivaldybės administracijos;
- paviešinta informacija neturi sukelti turtinės ir (ar) neturtinės žalos bei kitų neigiamų pasekmių savivaldybės administracijai, jos darbuotojams ar tretiesiems asmenims;
- iš skelbiamos informacijos privalo būti pašalinti asmens duomenys, konfidenciali informacija, kiti duomenys ar informacija, galinti sukelti turtinę ir (ar) neturtinę žalą bei kitas neigiamas pasekmes Savivaldybės administracijai, jos darbuotojams ar tretiesiems asmenims;
- skelbiamas tekstas neturi kurstyti nesantaikos ir patyčių.

Kaip numatyta Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programoje, galiausiai programos dalyviui už indėlį stiprinant Vilniaus miesto kibernetinį saugumą bus įteikta savivaldybės administracijos padėka.[139]

Apibendrinant tai, kas buvo išdėstyta, darytina išvada, jog Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo modelis yra nuodugniai apgalvotas, išsamus, aiškiai apibrėžtas bei sklandžiai įgyvendinamas.

3.4. Vilniaus miesto savivaldybės patirtis įgyvendinat atsakingo spragų atskleidimo programą

Pusiau struktūrizuoto interviu metu Vilniaus miesto savivaldybės atstovei, kuruojančiai atsakingo spragų atskleidimo programą, buvo užduoti klausimai apie savivaldybės patirtį įgyvendinant šią programą. Toliau pateikiami klausimai ir savivaldybės atstovės atsakymai į juos.

1. Kas paskatino sukurti / pradėti taikyti atsakingo atskleidimo programą? Kokie buvo lūkesčiai kuriant šią programą?

[137] *Ibid.*
[138] *Ibid.*
[139] *Ibid.*

„Vilniaus miesto savivaldybės administracijoje rimtai vertiname saugumo klausimus ir nuolat ieškome priemonių, kaip dar labiau sustiprinti IS vartotojų duomenų ir informacijos saugumą.

Kaip žinote, vis daugiau viešųjų paslaugų teikiamos internetu, diegiamos informacinės sistemos, gyventojų ir klientų duomenys, dokumentai tvarkomi skaitmeninėje erdvėje. Todėl auga poreikis užtikrinti šių sistemų ir gyventojų duomenų saugumą. Dėl minėtų priežasčių nuolat ieškome papildomų sprendimų, kaip proaktyviai valdyti IT sistemas ir užkirsti kelią galimiems incidentams.

Taip pat esame atvira organizacija ir remiame piliečių įtraukimo iniciatyvas. Dėl minėtų priežasčių inicijavome etiškų saugumo tyrėjų bendruomenės įtraukimą į Vilniaus miesto sistemų saugumo didinimo veiklas.

Nuo 2020 m. Vilniaus miesto savivaldybės administracijoje taikėme atsakingo spragų atskleidimo programą „Hack me if you can“. Tačiau praėjus keliems metams suinteresuotumas dalyvauti programoje sumažėjo ir pradėjome ieškoti naujų priemonių, kaip motyvuoti etiškus saugumo tyrėjus dalyvauti tokio pobūdžio iniciatyvose ir neprarasti susidomėjimo. Tad atlikę išsamią analizę ir įsivertinę iniciatyvos pritaikymą Vilniaus miesto savivaldybės administracijoje, 2023 m. inicijavome „Bug Bounty“ konkursą.

Užsienio šalyse panašios į „Bug Bounty“ praktikos nėra naujiena. Atsakingiems programavimo aistruoliams atradus pačių organizacijų nepastebėtas saugumo spragas siūlomi piniginiai prizai. Tuo tarpu Lietuvoje, o ypatingai viešajame sektoriuje, esame viena pirmųjų organizacijų, kurios ėmėsi šios iniciatyvos įgyvendinimo.”

2. Gal būtų galimybė sužinoti, kokie šios programos įgyvendinimo ir palaikymo kaštai?

„Konkursą inicijavome, atlikome analizę ir įgyvendinome vidinės savivaldybės komandos žmogiškaisiais resursais. Papildomos lėšos, kurios buvo reikalingos konkurso dalyvių prizams buvo numatytos savivaldybės biudžete.“

3. Kiek žinoma, atsakingo atskleidimo programos įgyvendinimą sudaro 4 etapai: 1) programos dalyvio registracija; 2) pranešimas apie identifikuotą spragą; 3) spragos šalinimas; 4) informacijos, susijusios su spragos identifikavimu, viešinimas. Siekiant detaliau išsigryninti Jūsų organizacijoje taikomą atsakingo atskleidimo modelį ir tai, kaip jis veikia, gal galėtumėte plačiau papasakoti, kaip vyksta visas šis procesas, kaip praktikoje įgyvendinami šie etapai?

„Turime dvi programas, viena iš jų įgyvendinama neatlygintinai, kita programa įgyvendinama konkurso pagrindu. Abiejų programų etapai šiek tiek skiriasi ir jų apibūdinimą galite rasti čia:

- Detali „Hack me if you can“ tvarka: https://aktai.vilnius.lt/document/30336083
- Detali „Bug Bounty“ tvarka: https://aktai.vilnius.lt/document/30389487“

4. Ar šiame procese bendradarbiaujama su Nacionaliniu kibernetinio saugumo centru (NKSC)?

„Konkrečiai dėl šių iniciatyvų ne, su NKSC bendradarbiaujame kitais saugumo klausimais (organizuojant saugumo pratybas, reaguojant į didesnio pobūdžio atakas ir kt.)“

5. Kiek dalyvių užsiregistruoja kiekvienais metais? Gal žinomas užsiregistravusių dalyvių amžius ar amžiaus vidurkis?

2. lentelė. **Užsiregistravusių dalyvių skaičius Vilniaus miesto savivaldybės vykdomose programose 2020-2023 metais**

Metai	„Hack me if you can“ dalyviai	„Bug bounty“ dalyviai
2020	17	-
2021	1	-
2022	5	-
2023	16	36
Viso:	**39**	**36**

„Tik atkreipiu dėmesį, kad tai tik užsiregistravę dalyviai. T. y., dalis tik užsiregistravo ir neieškojo arba neaptiko spragų ir nepateikė nė vieno pranešimo. Dėl duomenų apsaugos ir BDAR reguliavimo amžiaus nenorėtume detalizuoti.“

6. Kiek pasitvirtinusių pranešimų gaunama kiekvienais metais ir kiek nepasitvirtinusių?

„2023 m. „Bug Bounty“ konkurse iš viso gauti 35 pranešimai (kai kurie pranešimai susiję – apie tą pačią saugumo spragą, tačiau gauti iš skirtingų pranešėjų). Remiantis konkurso nuostatais, kai apie tą pačią saugumo spragą praneša du arba daugiau dalyvių, prizas skiriamas pirmajam apie spragą pranešusiam dalyviui. Iš pateiktų 35 pranešimų prizai buvo skiriami dalyviams dėl 19 pranešimų.“

7. Kiek Vilniaus miesto savivaldybė kiekvienais metais patiria kibernetinių atakų (nuo to laiko, kai pradėjo įgyvendinti atsakingo atskleidimo programą)?

„Lietuvoje vis dažniau susiduriame su kibernetinėmis atakomis, kai įsilaužėliai, pasinaudodami sistemų spragomis, nutekina svarbius klientų duomenis. Kibernetinių atakų skaičiai auga kasmet, visose organizacijose, ir jų nesietume su programomis (plačiau žr. 8 punkte, kodėl). Tai galite identifikuoti pagal pranešimus žiniasklaidoje.

Tuo tarpu savivaldybėje, kaip komanda esame įsidiegę nemažai monitoringo priemonių, kurių dėka galime iš anksto identifikuoti atakas, nedelsiant į jas reaguoti ir išvengti įsilaužimų. Taip pat, nuolat vykdome sistemų atnaujinimus, bendradarbiaujame su NKSC ir kitomis

organizacijomis – komunikuojame atsiradus naujoms atakoms ar jų metu, tokiu būdu didindami vieni kitų budrumą.“

8. Kokias problemas / iššūkius įgyvendinant atsakingo atskleidimo programą galėtumėte įvardinti?

„Atsakingo atskleidimo programos nukreiptos į individualius, atsakingus ir draugiškus etiškus „hakerius“. Programoje apibrėžti griežti reikalavimai, kokių veiksmų negali atlikti dalyviai, numatėme daug apribojimų, (pvz., draudžiama vykdyti DDoS atakas, bandyti pakenkti sistemų darbui ar įsilaužti į sistemas ir pan.) Programos dalyviai pasirašo konfidencialumo pasižadėjimus ir įsipareigoja jų laikytis, atsiranda atsakomybė. Būtent tuo šios programos ir skiriasi nuo 7 punkte minimų atakų, kurios atsiranda iš nedraugiškų šalių (su piktavališkais ketinimais įsilaužti ir pakenkti).“

9. Ar atsakingo kibernetinio saugumo spragų atskleidimo principo įgyvendinimas praktikoje yra veiksmingas užtikrinant Vilniaus miesto savivaldybės kibernetinį saugumą? Kodėl?

„Šiose programose matome didžiulę vertę, kadangi suinteresuoti draugiški asmenys gali dalyvauti konkurse ir prisidėti prie saugumo didinimo Vilniaus miesto savivaldybės administracijos informacinėse sistemose – tapti Vilniaus dalimi.“ Taip pat:

- „užtikrinamas Vilniaus miesto savivaldybės administracijos klientų duomenų, informacijos ir kitų IT išteklių saugumas, galime gauti vertingų įžvalgų, pastebėjimų;
- stiprinamas iniciatyvų rėmimas ir įtraukiami etiški įsilaužėliai į kibernetinio saugumo iniciatyvas Vilniaus miesto savivaldybės administracijoje;
- pateikti pranešimai padeda identifikuoti rizikos nekeliančias spragas, kurios ilgainiui gali išaugti, jas pašalinti;
- Galime proaktyviai valdyti sistemas.“

Apibendrinus tai, kas buvo išdėstyta, darytina išvada, jog Vilniaus miesto savivaldybė labai atsakingai žiūri į savo organizacijos kibernetinio saugumo užtikrinimą bei siekia kaip įmanoma labiau apsaugoti savo valdomų informacinių sistemų vartotojų duomenis, o prie šių tikslų siekimo ženkliai prisideda vykdomos atsakingo spragų atskleidimo programos.

3.5. Atsakingo atskleidimo principo įgyvendinimo veiksmingumo viešojo sektoriaus institucijų kibernetinio saugumo užtikrinimui pagrindimas

NATO oficialiai įvardina kibernetinę erdvę kaip penktąją karinių konfliktų erdvę, kartu su sausuma, oru, jūromis ir kosmine erdve.[140] Kibernetinės atakos tapo nauju, moderniu pavojingu

[140] „NATO Recognizes Cyber as Fifth War Domain“ [interaktyvus, žiūrėta: 2024-04-14]. Prieiga per internetą: https://www.sentar.com/nato-recognizes-cyber-as-fifth-war-domain/.

ginklu, galinčiu paralyžiuoti ne tik atskirų įstaigų, gamybos, prekybos, transporto, ryšių, elektros energijos, vandens tiekimo įmonių veiklą, bet ir valstybių infrastruktūrą.[141] Šiandien, vertinant geopolitinę situaciją Europoje ir visame pasaulyje, kibernetinė sauga yra vienas iš svarbiausių aspektų užtikrinant šalių stabilumą ir saugumą.

Šioje darbo dalyje, siekiant pagrįsti atsakingo atskleidimo principo įgyvendinimo veiksmingumą viešojo sektoriaus institucijų kibernetinio saugumo užtikrinimui, atliekama tyrimo metu gautų duomenų kokybinė analizė bei apžvelgiami teisės aktai, reglamentuojantys atsakingo atskleidimo svarbą ir poreikį.

Atsakingo atskleidimo principo įgyvendinimo praktiniai aspektai

Autoriaus nuomone, institucijos, kurios yra svarbios valstybės nacionaliniam saugumui užtikrinti, ypatingai – atsakingos už energetikos ir susisiekimo sektorius, turėtų jausti didelę atsakomybę dėl kibernetinio saugumo užtikrinimo, kadangi tiek elektros, tiek susisiekimo infrastruktūros yra kritinės svarbos sritys.

Išskirtinos kelios priežastys, kodėl šios minėtos viešojo sektoriaus institucijos turėtų įgyvendinti atsakingo atskleidimo principą:

1. **Kritinė infrastruktūros svarba.** Elektros tiekimas ir transporto tinklai yra kritinės infrastruktūros dalys, kurių veikimas yra esminis visuomenės gerovei, ekonomikos veikimui ir saugumui. Atsakingas atskleidimas apie pažeidžiamumus ar grėsmes šiose srityse padėtų sumažinti galimą poveikį visuomenei ir ekonomikai.

2. **Didelė priklausomybė nuo technologijų ir informacinių sistemų.** Energetikos ir susisiekimo sektoriuose naudojami įvairūs technologiniai sprendimai bei sistemos, o tai padidina kibernetinės saugos grėsmes ir svarbą dalintis informacija apie galimus saugumo pažeidimus.

3. **Piliečių pasitikėjimo svarba.** Piliečiai, o tuo pačiu ir energetinių išteklių vartotojai, turi jausti pasitikėjimą, kad vienos iš svarbiausių jų šalies institucijų efektyviai reaguoja į kibernetines grėsmes ir atlieka reikiamus veiksmus, jog užtikrintų jų saugumą. Bendradarbiavimas, aktyvi, atvira komunikacija ir informacijos dalinimasis apie kibernetinius įvykius bei grėsmes skatina šį pasitikėjimą.

Taigi, institucijos, atsakingos už nacionalinį saugumą, ypatingai – energetikos ir susisiekimo sektoriuose, siekdamos užtikrinti skaidrumą, saugumą ir veiksmingą reagavimą į kibernetines grėsmes, turi būti aktyvios atsakingo atskleidimo principo įgyvendinime, kadangi tai padėtų sumažinti rizikas ir užtikrinti tvarų šių sektorių veikimą. Tačiau, kaip jau buvo minėta,

[141] „Vilniaus universitetas ir Lietuvos kariuomenė bendradarbiaus kibernetinio saugumo srityje“ [interaktyvus, žiūrėta: 2024-04-14]. Prieiga per internetą: https://kariuomene.lt/kas-mes-esame/naujienos/vilniaus-universitetas-ir-lietuvos-kariuomene-bendradarbiaus-kibernetinio-saugumo-srityje/19277.

nė viena iš 15 tirtų didžiausių valstybės valdomų įmonių, svarbių Lietuvos Respublikos nacionaliniam saugumui užtikrinti ir kurių kibernetinio saugumo užtikrinimas yra itin svarbus valstybės atžvilgiu, atsakingo spragų atskleidimo tvarkų nėra parengusios ir paskelbusios. Tai aiškiai parodo, kad šios viešojo sektoriaus institucijos skiria nepakankamai dėmesio savo kibernetinio saugumo užtikrinimui.

Visgi atsakingo atskleidimo principo įgyvendinimo veiksmingumą viešojo sektoriaus institucijų kibernetinio saugumo užtikrinimui iš praktinės pusės pagrindžia Vilniaus miesto savivaldybės įgyvendinamos programos. Kaip minėta interviu metu, Vilniaus miesto savivaldybė įgyvendinamose programose mato didžiulę vertę.

Remiantis Vilniaus miesto savivaldybės atstovės atsakymais, taikant atsakingo atskleidimo principą ir įgyvendinant atsakingo spragų atskleidimo programas, iš suinteresuotų draugiškų asmenų gaunami pranešimai apie sistemų spragas, kurių dėka:

- užtikrinamas klientų duomenų, informacijos ir kitų informacinių technologijų išteklių saugumas, galima gauti vertingų įžvalgų ir pastebėjimų;
- stiprinamas iniciatyvų rėmimas ir etiški įsilaužėliai įtraukiami į kibernetinio saugumo iniciatyvas organizacijoje;
- pateikti pranešimai padeda identifikuoti rizikos nekeliančias spragas, kurios ilgainiui gali išaugti – sudaroma galimybė atlikti prevencinius veiksmus;
- sudaroma galimybė proaktyviai valdyti sistemas.

Taip pat, siekiant išsiaiškinti, ar atsakingo principo įgyvendinimas organizacijoje reikalauja didelių finansinių ir žmogiškųjų resursų, interviu metu buvo pasiteirauta apie programos įgyvendinimo ir palaikymo kaštus. Vilniaus miesto savivaldybės administracijos atstovė pateikė atsakymą, jog abi programos – tiek „Hack me if you can“, tiek „Bug Bounty“ – įgyvendintos pasitelkus vidinius resursus: „konkursą inicijavome, atlikome analizę ir įgyvendinome vidinės savivaldybės komandos žmogiškaisiais resursais. Papildomos lėšos, kurios buvo reikalingos konkurso dalyvių prizams buvo numatytos savivaldybės biudžete.“ Taigi, galima teigti, jog organizacijos, kurios „rimtai vertina saugumo klausimus ir nuolat ieško priemonių, kaip dar labiau sustiprinti informacinių sistemų vartotojų duomenų ir informacijos saugumą,“ nesunkiai randa būtų, kaip tai padaryti.

Apibendrinant esminius aspektus, darytina išvada, jog atsakingo spragų atskleidimo principo įgyvendinimas yra veiksmingas viešojo sektoriaus institucijų kibernetinio saugumo užtikrinimui dėl kelių svarbių priežasčių:

1. **Greitas incidentų aptikimas ir reagavimas.** Aiškus atsakingo spragų atskleidimo procesas leidžia institucijoms greičiau aptikti potencialias grėsmes ir spragas savo sistemose. Tai leidžia greičiau imtis reikiamų priemonių incidentams numalšinti arba prieš juos apsisaugoti.

2. **Saugumo patobulinimai.** Atskleidus spragas institucijos gali greičiau imtis veiksmų jas pašalinti arba sumažinti jų poveikį – tai leidžia nuolat tobulinti kibernetinį saugumą, padidinant sistemos atsparumą potencialioms atakoms.

3. **Pasitikėjimo didinimas.** Viešojo sektoriaus institucijų atvirumas ir gebėjimas atskleisti spragas bei veiksmingai į jas reaguoti didina visuomenės pasitikėjimą – tai yra svarbu siekiant užtikrinti visuomenės paramą ir bendradarbiavimą kibernetinio saugumo srityje.

4. **Bendradarbiavimo skatinimas.** Atsakingas spragų atskleidimas skatina bendradarbiavimą tarp viešojo sektoriaus institucijų, privačiojo sektoriaus ir kitų suinteresuotų šalių. Dalinimasis bendra informacijos apie spragas ir grėsmes leidžia greičiau ir veiksmingiau reaguoti į kibernetinius iššūkius.

5. **Teisėtumo išlaikymas.** Atsakingas spragų atskleidimas padeda institucijoms išlaikyti teisėtumą ir atitiktį reguliavimo reikalavimams – tai svarbu ne tik iš moralinės perspektyvos, bet ir siekiant išvengti galimų teisinių padarinių.

Remiantis šiais argumentais darytina išvada, jog atsakingo spragų atskleidimo principo įgyvendinimas yra reikšmingas ir veiksmingas užtikrinant viešojo sektoriaus institucijų kibernetinį saugumą, kadangi jis leidžia greičiau aptikti bei reaguoti į kibernetinius incidentus, tobulinti saugumo priemones ir didinti visuomenės pasitikėjimą šiomis institucijomis.

Teisės aktų nuostatos

Viešojo ir privataus sektorių bendradarbiavimo svarbą, siekiant stiprinti valstybės kibernetinį saugumą, pagrindžia tai, jog Lietuvos Respublikos Nacionalinėje kibernetinio saugumo strategijoje (toliau – Strategija) yra numatyta stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą[142].

Kaip teigiama Strategijos 34 str., „šiuolaikinėse valstybėse, kuriose gerai išvystyta plačiajuosčio ryšio infrastruktūra, viešojo sektoriaus atstovai nebegali toliau vieni kovoti su pavojingais ar didelės reikšmės kibernetiniais incidentais, o ypatingos svarbos informacinės infrastruktūros valdytojai – neretai privataus sektoriaus atstovai – patys ne visada gali suvaldyti kibernetinius incidentus, dažnai peržengiančius jų organizacijos ribas. Taigi viešojo ir privataus sektorių bendradarbiavimas tampa būtina sąlyga visapusiškam kibernetiniam saugumui užtikrinti. Viešojo ir privataus sektorių efektyvaus bendradarbiavimo esminė sąlyga – visavertė partnerystė: abipusis pasitikėjimas ir nauda, todėl viešojo ir privataus sektorių bendradarbiavimas turėtų būti į tai orientuotas.“[143]

[142] Nacionalinė kibernetinė saugumo strategija, patvirtinta 2018 m. rugpjūčio 13 d. įsakymu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (suvestinė redakcija nuo 2024-01-01), 33 str.
[143] *Ibid.,* 34 str.

Strategijoje taip pat nurodoma, jog „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.“[144]

Taigi, siekiant stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą, Strategijoje numatytas uždavinys „kurti atsakingą viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktiką.[145]“ O šis uždavinys turėtų būti įgyvendinamas inicijuojant atsakingą viešojo ir privataus sektorių IRT spragų atskleidimo praktiką, nustatant šios srities veiklos principus, metodų, techninių gebėjimų ar kitų priemonių taikymo tvarką.[146]

Siekiant pagrįsti atsakingo atskleidimo principo įgyvendinimo veiksmingumą viešojo sektoriaus institucijų kibernetinio saugumo užtikrinimui iš teorinės pusės, remiantis teisės aktų nuostatomis bei praktika, taip pat išskirtinos šios priežastys, kodėl atsakingo atskleidimo principo įgyvendinimas yra veiksmingas:

1. **Skaidrumas.** Atsakingo atskleidimo principas skatina institucijas atvirai informuoti visuomenę apie kibernetinius įvykius ir grėsmes – tai suteikia galimybę žiniasklaidai, verslo bendruomenei ir piliečiams tinkamai reaguoti ir imtis prevencinių arba gynybinių priemonių.

2. **Atsakomybė.** Atsakingas atskleidimas prisideda prie institucijų atsakomybės už kibernetinio saugumo užtikrinimą. Viešai paskelbta informacija apie įvykius, atakas arba incidentus suteikia galimybę vertinti institucijų veiksmus ir reakcijas bei reikalauti atsakomybės už nepakankamą arba neveiksmingą kibernetinio saugumo politiką.

3. **Skatinamas bendradarbiavimas.** Atsakingas atskleidimas skatina bendradarbiavimą tarp viešojo sektoriaus institucijų, privačiojo sektoriaus ir net tarptautinių organizacijų. Bendra informacijos apie grėsmes dalinimasis leidžia greičiau identifikuoti ir reaguoti į kibernetinius iššūkius, nes daugelis šalių gali dalintis savo patirtimi ir geriausia praktika.

4. **Visuomenės pasitikėjimas.** Atvirumas ir skaidrumas dėl kibernetinių saugumo grėsmių ir įvykių padidina visuomenės pasitikėjimą valdžios institucijomis. Piliečiai jaučiasi saugesni, žinodami, kad jų valstybės institucijos aktyviai stengiasi apsaugoti juos nuo kibernetinių atakų ir yra pasiruošusios atvirai dalintis informacija.

5. **Europos Sąjungos teisės aktų įgyvendinimas, bendro kibernetinio saugumo lygio užtikrinimas.** Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram

[144] *Ibid.,* 37 str.
[145] *Ibid.,* 38.3 p.
[146] *Ibid.*

kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti[147] įgyvendinimas. Atsakingo atskleidimo principas yra vienas iš būdų, padedančių įgyvendinti šią direktyvą ir užtikrinti aukštą kibernetinio saugumo lygį Europos Sąjungoje.

Minėtoje Europos Parlamento ir Tarybos direktyvos dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti nurodoma, jog „koordinuotas pažeidžiamumų atskleidimas yra struktūrinis procesas, per kurį potencialiai pažeidžiamų IRT produktų ar IRT paslaugų gamintojui arba teikėjui pranešama apie pažeidžiamumus taip, kad jam būtų sudarytos sąlygos pažeidžiamumą nustatyti ir ištaisyti prieš atskleidžiant išsamią informaciją apie pažeidžiamumus trečiosioms šalims arba visuomenei. Koordinuotas pažeidžiamumų atskleidimas taip pat turėtų apimti pranešimą teikiančio fizinio ar juridinio asmens ir potencialiai pažeidžiamų IRT produktų ar IRT paslaugų gamintojo arba teikėjo koordinavimą ištaisymo laiko ir paskelbimo apie pažeidžiamumus klausimais[148]“.

Taigi, remiantis teisės aktų nuostatomis, darytina išvada, jog atsakingo atskleidimo principo įgyvendinimas turi didelę reikšmę: žvelgiant plačiąja prasme – Nacionalinės kibernetinio saugumo strategijos įgyvendinimas, atsakingo saugumo spragų atskleidimo praktikos ir tinkamų organizacinių bei techninių priemonių taikymas padeda stiprinti ne tik viešojo sektoriaus institucijų kibernetinį saugumą, bet prisideda ir prie nacionalinio bei visos ES kibernetinio saugumo užtikrinimo.

[147] Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 2022 m. gruodžio 14 d. dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva).
[148] *Ibid.*, 58 str.

IŠVADOS

1. Atsakingo atskleidimo principas įgalina asmenį teisėtai ieškoti ryšių ir informacinės sistemos klaidų, spragų ir pažeidžiamų, dėl kurių gali įvykti kibernetinis incidentas, o atradus pažeidžiamumų, apie juos pranešti kibernetinio saugumo subjektui ar NKSC.

2. Atsakingo spragų atskleidimo procesas turėtų sudaryti galimybes glaudesniam viešojo ir privataus sektorių bendradarbiavimui siekiant didinti įstaigų kibernetinį saugumą, kadangi ryšių ir informacinės sistemos saugumo spragas atradęs asmuo apie jas informuoja sistemų valdytojus, kad šie trūkumus pašalintų.

3. Teisės aktai nustato gana aiškų atsakingo spragų atskleidimo procesą, kuris turėtų būti nesunkiai įgyvendinamas, tačiau tam, kad atsakingo atskleidimo principo įgyvendinimo modelis sėkmingai funkcionuotų, reikalingas visų subjektų, dalyvaujančių atsakingo spragų atskleidimo procese, įsitraukimas ir įdirbis, ypatingai – kibernetinio saugumo subjektų, kurie turi būti tinkamai pasiruošę reaguoti į pranešimus dėl atrastų spragų ir pasirengę jas pašalinti.

4. Įstaigos, kurios rūpinasi savo kibernetinio saugumo užtikrinimu, reikalingus atsakingo spragų atskleidimo procesus sėkmingai vykdo savo iniciatyva. Kaip tokio atvejo pavyzdį galima įvardinti Vilniaus miesto savivaldybę, kuri atsakingo atskleidimo programą pradėjo vykdyti 2020 metais, kai atsakingo spragų atskleidimo principas dar nebuvo įtvirtintas įstatymu, tačiau Vilniaus miesto savivaldybei tai nebuvo kliūtis pradėti taikyti atsakingo atskleidimo politiką.

5. Nors atsakingo spragų atskleidimo principo teisinis reglamentavimas yra pakankamas, jo praktinis įgyvendinimas yra problematiškas ir pačios viešojo sektoriaus institucijos vis dar nėra linkusios jį savarankiškai taikyti savo viduje.

6. Atsakingo spragų atskleidimo principo įgyvendinimas yra reikšmingas ir veiksmingas užtikrinant viešojo sektoriaus institucijų kibernetinį saugumą, kadangi jis leidžia greičiau aptikti bei reaguoti į kibernetinius incidentus, tobulinti saugumo priemones ir didinti visuomenės pasitikėjimą šiomis institucijomis.

7. Atsakingo atskleidimo principo įgyvendinimas turi didelę reikšmę: žvelgiant plačiąja prasme – Nacionalinės kibernetinio saugumo strategijos įgyvendinimas, atsakingo saugumo spragų atskleidimo praktikos ir tinkamų organizacinių bei techninių priemonių taikymas padeda stiprinti ne tik viešojo sektoriaus institucijų kibernetinį saugumą, bet prisideda ir prie nacionalinio bei visos ES kibernetinio saugumo užtikrinimo.

REKOMENDACIJOS

Siekiant, kad atsakingo spragų atskleidimo principo įgyvendinimas viešojo sektoriaus institucijose vyktų sklandžiau, tikslinga:

1. Daugiau dėmesio skirti visuomenės švietimui apie kibernetinį saugumą ir jo svarbą užtikrinant, kad visos susijusios suinteresuotosios šalys, o taip pat ir piliečiai, įskaitant mokyklinio amžiaus vaikus, bei verslo atstovai gautų tvarius mokymus.

2. Teikti rekomendacijas, išaiškinimus, konsultacijas, kaip praktiškai įgyvendinti atsakingo spragų atskleidimo procesą organizacijų viduje.

3. Daugiau dėmesio skirti kompetentingų informacinių technologijų specialistų pritraukimui į viešojo sektoriaus institucijas bei išsaugojimui jose.

ŠALTINIAI

1. „Atsakingo atskleidimo politika Vilniaus m. savivaldybėje“. Prieiga per internetą: https://www.nrdcs.lt/klientu-istorijos/atsakingo-atskleidimo-politika-vilniaus-m-savivaldybeje/.

2. „Coordinated Vulnerability Disclosure Model Policy and Procedure“. CIO Platform Nederland, 2016.

3. „Coordinated Vulnerability Disclosure: the Guideline“. NCSC, 2018.

4. „Coordinated Vulnerability Disclousure Policies „CVDP“. Center of Cyber Security Belgium, 2020. Prieiga per internetą: https://ccb.belgium.be/sites/default/files/Brochure_CVDP_UK_A5_DP2%20%28002%29.pdf.

5. „Coordinated Vulnerability Disclousure Policies in the EU“. ENISA, 2022.

6. „Developing national vulnerability programmes“. ENISA, 2023.

7. „Economics of vulnerability disclosure“. ENISA, 2018.

8. „GFCE Global Good Practices. Coordinated Vulnerability Disclosure (CVD)“. Global Forum on Cyber Expertise, 2017.

9. „Good Practice Guide on Vulnerability Disclosure“. ENISA, 2015.

10. „Guide to coordinated vulnerability disclosure policies. Part 1: good practices“. Center of Cyber Security Belgium, 2020. Prieiga per internetą: https://www.cybersecuritycoalition.be/content/uploads/CCB-Guide-Policies-CVDP.pdf.

11. „Hack me if you can“. Prieiga per internetą: https://vilnius.lt/lt/vilnius-2in/kibernetinis-saugumas.

12. „Have you discovered a vulnerability in a government system or in a system with a vital function?“. Prieiga per internetą: https://english.ncsc.nl/contact/reporting-a-vulnerability-cvd.

13. „Vilniaus universitetas ir Lietuvos kariuomenė bendradarbiaus kibernetinio saugumo srityje“. Prieiga per internetą: https://kariuomene.lt/kas-mes-esame/naujienos/vilniaus-universitetas-ir-lietuvos-kariuomene-bendradarbiaus-kibernetinio-saugumo-srityje/19277.

14. „Vulnerability reporting in Belgium: A safe harbour for ethical hackers“, 2023. Prieiga per internetą: https://www.headmind.com/en/vulnerability-reporting-belgium-safe-harbour-ethical-hackers/.

15. 2020 m. Nacionalinė kibernetinio saugumo būklės ataskaita. Lietuvos Respublikos krašto apsaugos ministerija.

16. 2021 m. birželio 17 d. Lietuvos Respublikos kibernetinio saugumo įstatymo Nr. XII-1428 1, 2, 6, 8, 9, 13 straipsnių, V skyriaus pavadinimo, priedo pakeitimo ir Įstatymo papildymo 17 straipsniu ir VI skyriumi įstatymas Nr. XIV-413.

17. 2022 m. Nacionalinė kibernetinio saugumo būklės ataskaita. Lietuvos Respublikos krašto apsaugos ministerija.

18. AB „Ignitis grupė“. Prieiga per internetą: https://www.ignitisgrupe.lt/.

19. AB „Kelių priežiūra“. Prieiga per internetą: https://keliuprieziura.lt/.

20. AB „KN Energies“. Prieiga per internetą: https://www.kn.lt/.

21. AB „Lietuvos geležinkeliai“ įmonių grupė. Prieiga per internetą: https://ltg.lt/.

22. AB „Oro navigacija“. Prieiga per internetą: https://www.ans.lt/.

23. AB „Via Lietuva”. Prieiga per internetą: https://vialietuva.lt/.

24. AB Klaipėdos valstybinio jūrų uosto direkcija. Prieiga per internetą: https://portofklaipeda.lt/.

25. AB Lietuvos oro uostai. Prieiga per internetą: https://ltou.lt/.

26. AB Lietuvos pašto įmonių grupė. Prieiga per internetą: https://www.post.lt/.

27. AB Lietuvos radijo ir televizijos centras. Prieiga per internetą: https://www.telecentras.lt/.

28. AB Vidaus vandens kelių direkcija. Prieiga per internetą: https://vvkd.lt/.

29. Arora A.; Telang R. „Economics of Software Vulnerability Disclosure“. Economics of Information Security. Prieiga per internetą: https://www.heinz.cmu.edu/~rtelang/Economics_of_software_vulnerability_disclosure.pdf.

30. FAQ on Coordinated Vulnerability Disclosure Policy (CVDP) and Bug Bounty Programmes. Prieiga per internetą: https://ccb.belgium.be/en/faq-coordinated-vulnerability-disclosure-policy-cvdp-and-bug-bounty-programmes.

31. Finland‘s Cyber Security Strategy 2019. The Security Committee.

32. Hobbes, A.C. „Rudimentary Treatise on the Construction of Locks“. London, England: Levey, Robson and Franklyn, Vol. 83. Prieiga per internetą: https://books.google.com/books?id=PsUzAQAAMAAJ&printsec=frontcover&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false.

33. Householder, A. D. et al. „The CERT® Guide to Coordinated Vulnerability Disclosure“. Carnegie Mellon University, 2017.

34. Yi Ding, A. et al. „Ethical Hacking for IoT Security: A First Look into Bug Bounty Programs and Responsible Disclosure“. ICTRS 2019 - Proceedings of the 8th International Conference on Telecommunications and Remote Sensing, 2019.

35. IRT specialistų pasiūlos ir paklausos tyrimas „IRT specialistai Lietuvoje: situacija darbo rinkoje ir darbdavių poreikiai“. „Infobalt“, „Investuok Lietuvoje“.

36. Kennedy, D. „Exploring Coordinated Disclosure“. 451 Research, 2019.

37. Ķinis, U., From Responsible Disclosure Policy (RDP) towards State Regulated Responsible Vulnerability Disclosure Procedure (hereinafter – RVDP): The Latvian approach. Computer Law & Security Review, 2018.34(3), 2018.

38. Lietuvos Respublikos kibernetinio saugumo įstatymas (su pakeitimais ir papildymais). TAR, 2014-12-23, Nr. 20553.

39. Lietuvos Respublikos krašto apsaugos ministerijos pranešimas spaudai, „LR Seimas įteisino atsakingą kibernetinių spragų atskleidimą“. Prieiga per internetą: https://kam.lt/lr-seimas-iteisino-atsakinga-kibernetiniu-spragu-atskleidima/.

40. Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymas (su pakeitimais ir papildymais). Valstybės žinios, 2002-10-30, Nr. 103-4604.

41. Mann, D. E.; Christey, S. M. „Towards a Common Enumeration of Vulnerabilities“. Prieiga per internetą: https://cve.mitre.org/docs/docs-2000/cerias.html.

42. Nacionalinė kibernetinė saugumo strategija, patvirtinta 2018 m. rugpjūčio 13 d. įsakymu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

43. Nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašas, patvirtintas Lietuvos Respublikos krašto apsaugos ministro 2021 m. liepos 9 d. įsakymu Nr. V-484 „Dėl nacionalinės ryšių ir informacinių sistemų spragų atskleidimo tvarkos aprašo patvirtinimo“.

44. Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos pranešimas spaudai „Gerieji“ kibernetiniai įsilaužėliai padeda pašalinti pavojingas spragas“. Prieiga per internetą: https://www.nksc.lt/naujienos/gerieji_kibernetiniai_isilauzeliai_padeda_pasalint.html

45. Pam, T. T.; Meer, H. „History of Vulnerability Disclosure“. Prieiga per internetą: https://duo.com/labs/research/history-of-vulnerability-disclosure.

46. Valdymo koordinavimo centro duomenys. Prieiga per internetą: https://governance.lt/apie-imones/vvi-sarasas/.

47. Samoa National Cybersecurity Strategy 2016-2021. Ministry of Communication and Information Technology.

48. Shepherd, S. „How do we define Responsible Disclosure?“. SANS Institute, 2003. Prieiga per internetą: 932.pdf (egnyte.com).

49. UAB „EPSO-G“ įmonių grupė. Prieiga per internetą: https://www.epsog.lt/.

50. Ushmani, A. „Ethical Hacking“. International Journal of Information Technology (IJIT), Volume 4 Issue 6, Nov-Dec 2018.

51. VĮ Ignalinos atominė elektrinė. Prieiga per internetą: https://www.iae.lt/.

52. VĮ Registrų centras. Prieiga per internetą: https://www.registrucentras.lt/.

53. VĮ Valstybinių miškų urėdija. Prieiga per internetą: https://vmu.lt/.

54. Viešoji konsultacija dėl atsakingo kibernetinio saugumo spragų atskleidimo praktikos įteisinimo. 2019 m. rugsėjo mėn., Vilnius. Prieiga per internetą: http://kurklt.lt/wp-content/uploads/2019/03/Vie%C5%A1osios-konsultacijos-ataskaita-atsakingas-kibernetinio-saugumo-sprag%C5%B3-atskleidimas-1.pdf.

55. Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programa, patvirtinta Vilniaus miesto savivaldybės administracijos direktoriaus 2020 m. vasario 10 d. įsakymu Nr. 30-317/20 „Dėl Vilniaus miesto savivaldybės administracijos kibernetinio saugumo spragų atsakingo atskleidimo programos tvirtinimo“. Prieiga per internetą: https://aktai.vilnius.lt/document/30336083.

56. Vulnerability Disclosure Guidance. NIST, 2023. Prieiga per internetą: https://csrc.nist.gov/projects/vdg.

57. „Multi-party disclosure - how does it work?“. Nacional Cyber Security Centre, 2021. Prieiga per internetą: https://english.ncsc.nl/latest/weblog/weblog/2021/multi-party-disclosure.

58. „NATO Recognizes Cyber as Fifth War Domain“. Prieiga per internetą: https://www.sentar.com/nato-recognizes-cyber-as-fifth-war-domain/.

59. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 2022 m. gruodžio 14 d. dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva).

Mameniškė I. (2024). *Atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelis* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

ANOTACIJA

Magistro baigiamajame darbe išanalizuotas atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelis bei įvertintas atsakingo atskleidimo principo veiksmingumas užtikrinant viešojo sektoriaus institucijų kibernetinį saugumą. Pirmame skyriuje apžvelgiami reikšmingiausi atsakingo atskleidimo principo istorinės raidos aspektai, atsakingo atskleidimo principo samprata, atsakingo atskleidimo principo įgyvendinimo teorinis modelis bei užsienio šalių – Belgijos ir Nyderlandų – atsakingo atskleidimo principo įgyvendinimo praktika. Antrame skyriuje pateikiama tyrimo metodologija – siekiant išnagrinėti atsakingo atskleidimo principo įgyvendinimą viešajame sektoriuje ir jo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą, pasirinktas kokybinio tyrimo metodas. Trečiame skyriuje nagrinėjama atsakingo atskleidimo principo raiška viešajame sektoriuje, šio principo įgyvendinimo problematika, Vilniaus miesto savivaldybės atsakingo spragų atskleidimo programa, analizuojamas atsakingo atskleidimo principo įgyvendinimo šioje viešojo sektoriaus institucijoje modelis bei siekiama pagrįsti atsakingo atskleidimo principo įgyvendinimo veiksmingumą užkrintant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą. Darbo pabaigoje pateikiamos tyrimo rezultatus apibendrinančios išvados ir rekomendacijos.

Pagrindiniai žodžiai: atsakingo atskleidimo principas, atsakingas spragų atskleidimas, viešojo sektoriaus institucijos, kibernetinio saugumo užtikrinimas.

Mameniškė I. (2024). *The Model for the Implementation of the Principle of Responsible Disclosure in the Public Sector* (master thesis). Vilnius: Mykolas Romeris University

ANNOTATION

The Master thesis analyses the model of implementation of the principle of responsible disclosure in the public sector and assesses the effectiveness of the principle of responsible disclosure in ensuring the cyber security of public sector institutions. The first chapter provides an overview of the most significant aspects of the historical development of the Responsible Disclosure Principle, the concept of the Responsible Disclosure Principle, the theoretical model of the implementation of the Responsible Disclosure Principle and the practice of the implementation of the Responsible Disclosure Principle in the foreign countries of Belgium and The Netherlands. The second chapter presents the research methodology - in order to analyze the implementation of the principle of responsible disclosure in the public sector and its effectiveness in ensuring the cyber security of Lithuanian public sector institutions, a qualitative research method was chosen. The third chapter examines the expression of the principle of responsible disclosure in the public sector, the problems of its implementation, the responsible disclosure program of Vilnius City Municipality, analyses the model of the implementation of the principle of responsible disclosure in this public sector institution, and seeks to substantiate the effectiveness of the implementation of the principle of responsible disclosure in securing the cyber security of Lithuanian public sector institutions. The paper concludes with conclusions and recommendations summarizing the results of the study.

Key words: responsible disclosure principle, responsible vulnerabilities disclosure, public sector institutions, cybersecurity.

Mameniškė I. (2024). *Atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelis* (magistro baigiamasis darbas). Vilnius: Mykolo Romerio universitetas

SANTRAUKA

Magistro baigiamajame darbe nagrinėjamas atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelis, siekiant įvertinti jo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą. Nepaisant to, kad Lietuva yra viena iš pirmųjų ES šalių, įgyvendinusių atsakingo atskleidimo principą, vis dar stokojama išsamių jo taikymo viešajame sektoriuje tyrimų bei mokslininkų rekomendacijų šiuo klausimu. Šiuo tyrimu siekiama užpildyti minėtą spragą ir prisidėti prie efektyvesnio kibernetinio saugumo užtikrinimo Lietuvoje, kuris yra labai aktualus šiuolaikinėje visuomenėje. Autorius, nagrinėdamas atsakingo atskleidimo principo įgyvendinimą viešajame sektoriuje, siekia išryškinti esamus trūkumus, o tyrimo rezultatai gali būti naudingi formuojant strategijas ir politiką, siekiant stiprinti viešojo sektoriaus kibernetinį saugumą. Darbo uždaviniai: išnagrinėti atsakingo atskleidimo principo įgyvendinimo teorinius aspektus, išanalizuoti Lietuvos viešojo sektoriaus institucijų atsakingo atskleidimo principo įgyvendinimo praktiką, identifikuoti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje problematiką, empiriškai ištirti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelį. Darbo metodai: mokslinės literatūros analizė, juridinių dokumentų turinio analizė, pusiau struktūrizuotas interviu.

Darbe siekiama įvertinti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelio veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą. Atliktas kokybinis tyrimas leidžia daryti išvadą, jog atsakingo spragų atskleidimo principo įgyvendinimas yra reikšmingas ir veiksmingas užtikrinant viešojo sektoriaus institucijų kibernetinį saugumą, kadangi jis leidžia greičiau aptikti bei reaguoti į kibernetinius incidentus, tobulinti saugumo priemones ir didinti visuomenės pasitikėjimą šiomis institucijomis. Atsakingo atskleidimo principo įgyvendinimas taip pat turi didelę reikšmę žvelgiant plačiąja prasme – Nacionalinės kibernetinio saugumo strategijos įgyvendinimas, atsakingo saugumo spragų atskleidimo praktikos ir tinkamų organizacinių bei techninių priemonių taikymas padeda stiprinti ne tik viešojo sektoriaus institucijų kibernetinį saugumą, bet prisideda ir prie nacionalinio bei visos ES kibernetinio saugumo užtikrinimo.

Magistro baigiamojo darbo pabaigoje pateikiamos tyrimo rezultatus apibendrinančios išvados ir rekomendacijos dėl sklandesnio atsakingo spragų atskleidimo principo įgyvendinimo viešojo sektoriaus institucijose.

Mameniškė I. (2024). *The Model for the Implementation of the Principle of Responsible Disclosure in the Public Sector* (master thesis). Vilnius: Mykolas Romeris University

SUMMARY

The Master thesis analyses the model of implementation of the principle of responsible disclosure in the public sector in order to assess its effectiveness in ensuring cyber security of Lithuanian public sector institutions. Despite the fact that Lithuania was one of the first EU countries to implement the principle of responsible disclosure, there is still a lack of comprehensive research on its application in the public sector, as well as a lack of scholarly guidance on this issue. This study aims to fill this gap and to contribute to more effective cyber security in Lithuania, which is of great relevance in modern society. The author, by examining the implementation of the principle of responsible disclosure in the public sector, seeks to highlight the existing gaps, and the results of the study may be useful in the formulation of strategies and policies to strengthen public sector cyber security. The objectives of the thesis are: to analyze the theoretical aspects of the implementation of the principle of responsible disclosure, to analyze the practice of the implementation of the principle of responsible disclosure in Lithuanian public sector institutions, to identify the problems of the implementation of the principle of responsible disclosure in the public sector, to empirically investigate the model of the implementation of the principle of responsible disclosure in the public sector. Methods: analysis of scientific literature, content analysis of legal documents, semi-structured interviews.

The aim of the paper is to assess the effectiveness of the model of responsible disclosure in the public sector in ensuring cyber security of Lithuanian public sector institutions. The qualitative study concludes that the implementation of the Responsible Disclosure Principle is significant and effective in ensuring the cybersecurity of public sector institutions, as it allows for quicker detection of and response to cyber incidents, improvement of security measures, and increased public trust in these institutions. The implementation of the principle of responsible disclosure is also of great importance in a broader sense: the implementation of the National Cyber Security Strategy, the practice of responsible disclosure of security gaps and the application of appropriate organizational and technical measures contribute not only to strengthening the cybersecurity of public sector bodies, but also to national and EU-wide cybersecurity.

At the end of the Master's thesis, conclusions summarizing the results of the research and recommendations for a smoother implementation of the principle of responsible gap disclosure in public sector institutions are presented.

PRIEDAI

1 priedas

Interviu klausimai

Sveiki,

esu Mykolo Romerio universiteto Kibernetinio saugumo valdymo magistrantūros studijų studentė. Šiuo metu rašau magistro baigiamąjį darbą tema „Atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelis“, kurio tikslas – išanalizuoti atsakingo atskleidimo principo įgyvendinimo viešajame sektoriuje modelį bei įvertinti atsakingo atskleidimo principo veiksmingumą užtikrinant Lietuvos viešojo sektoriaus institucijų kibernetinį saugumą.

Kiek domėjausi Lietuvos viešojo sektoriaus institucijų praktika, Vilniaus miesto savivaldybė yra stipriausiai pažengusi atsakingo atskleidimo principo įgyvendinimo srityje. Tad noriu pasiteirauti, ar galėtumėte pagelbėti ir suteikti platesnę informaciją, reikalingą magistro baigiamojo darbo rašymui, apie Vilniaus miesto savivaldybės patirtį įgyvendinant atsakingo atskleidimo programą?

Klausimai:

1. Kas paskatino sukurti / pradėti taikyti atsakingo atskleidimo programą? Kokie buvo lūkesčiai kuriant šią programą?
2. Gal būtų galimybė sužinoti, kokie šios programos įgyvendinimo ir palaikymo kaštai?
3. Kiek žinoma, atsakingo atskleidimo programos įgyvendinimą sudaro 4 etapai: 1) programos dalyvio registracija; 2) pranešimas apie identifikuotą spragą; 3) spragos šalinimas; 4) informacijos, susijusios su spragos identifikavimu, viešinimas. Siekiant detaliau išsigryninti Jūsų organizacijoje taikomą atsakingo atskleidimo modelį ir tai, kaip jis veikia, gal galėtumėte plačiau papasakoti, kaip vyksta visas šis procesas, kaip praktikoje įgyvendinami šie etapai?
4. Ar šiame procese bendradarbiaujama su NKSC?
5. Kiek dalyvių užsiregistruoja kiekvienais metais? Gal žinomas užsiregistravusių dalyvių amžius ar amžiaus vidurkis?
6. Kiek pasitvirtinusių pranešimų gaunama kiekvienais metais ir kiek nepasitvirtinusių?
7. Kiek Vilniaus miesto savivaldybė kiekvienais metais patiria kibernetinių atakų (nuo to laiko, kai pradėjo įgyvendinti atsakingo atskleidimo programą)?
8. Kokias problemas / iššūkius įgyvendinant atsakingo atskleidimo programą galėtumėte įvardinti?

9. Ar atsakingo kibernetinio saugumo spragų atskleidimo principo įgyvendinimas praktikoje yra veiksmingas užtikrinant Vilniaus miesto savivaldybės kibernetinį saugumą? Kodėl?