Vilniaus universitetas
TARPTAUTINIŲ SANTYKIŲ IR POLITIKOS MOKSLŲ INSTITUTAS

Šiuolaikinės Politikos Studijų programa

DOMINYKA BERNOTAITĖ
II kurso studentė

Kibernetinis atsparumas Lietuvoje: Kibernetinio atsparumo ir rizikos valdymo metodų tyrimas

MAGISTRINIS DARBAS

Darbo vadovas: Doc. Dr. Deividas Šlekys

Vilnius, 2024

MAGISTRO DARBO PRIEŠLAPIS

Magistro darbo vadovo išvados dėl darbo gynimo:

.....

.....

.....

....
(data) (v., pavardė) (parašas)

Bakalauro/magistro darbas įteiktas gynimo komisijai:

....
(data) (Gynimo komisijos sekretoriaus/ės parašas)
Bakalauro/magistro darbo recenzentas/ė:

.....
(v., pavardė)

Bakalauro/magistro darbų gynimo komisijos įvertinimas:

.....
Komisijos pirmininkas/ė:

Komisijos nariai:

BIBLIOGRAFINIO APRAŠO LAPAS

Bernotaitė D. ***Kibernetinis atsparumas Lietuvoje: Kibernetinio atsparumo ir rizikos valdymo metodų tyrimas***: magistro darbas / VU Tarptautinių santykių ir politikos mokslų institutas; darbo vadovas Doc. Dr. Deividas Šlekys – Vilnius, 2024, 63p.

Reikšminiai žodžiai: kibernetinis saugumas, atsparumas, rizikų valdymas, grėsmių valdymas, , kibernetinė erdvė, kibernetinė ataka.

Šiame darbe nagrinėjama kibernetinio atsparumo ir rizikos valdymo strategijų praktika Lietuvoje, analizuojant organizacijų požiūrius į išorines kibernetines grėsmes ir jų taikomas kibernetinio saugumo strategijas. Pagrindinis dėmesys skiriamas analizei, kaip (ir ar) organizacijos Lietuvoje pereina nuo tradicinių rizikos valdymo požiūrių, orientuotų į grėsmių prevenciją, prie integruotų atsparumo valdymo metodų, kuriuose pabrėžiama ne tik grėsmių aptikimo ir prevencijos svarba, bet ir gebėjimas atsigauti ir prisitaikyti po kibernetinių incidentų.

Darbo tikslas buvo įvertinti, ar ir kaip organizacijos, taikydamos atsparumo didinimo strategijas, sumažina kibernetinių atakų poveikį ir užtikrina savo veiklos tęstinumą. Pateikiami penki pagrindiniai tyrimo atvejai ir organizacijos: Ignitis grupė, Vilniaus savivaldybė, Vilniaus rajono savivaldybė, Vilniaus Universitetas, ir Kauno technologijos universitetas, kuriuose buvo analizuojami kibernetinių incidentų valdymo procesai ir atsparumo didinimo strategijos. Atvejų ir interviu analizė parodė, kad organizacijos, investuojančios į atsparumo didinimą, turi geresnes galimybes greitai atsigauti po kibernetinių atakų ir išlaikyti ilgalaikį funkcionalumą.

Tyrime remiamasi atsparumo mokslo teorija ir metodais, siekiant išanalizuoti, kaip organizacijos pritaiko keturis pagrindinius atsparumo komponentus – pasirengimą, absorbciją, atsigavimą ir prisitaikymą. Pateikiama praktinė analizė, kaip šios strategijos įgyvendinamos Lietuvos organizacijose, ir kaip jos prisideda prie kibernetinio atsparumo stiprinimo. Išvados atskleidžia, kad, nors prevencija vis dar yra svarbi, organizacijos vis daugiau dėmesio skiria ir atsparumo valdymui, kuris užtikrina ne tik greitą reagavimą į incidentus, bet ir jų poveikio sumažinimą.

Turinys

1. Įvadas

Šiuolaikinėje skaitmeninėje eroje kibernetinė erdvė tapo itin svarbia sritimi, darančia įtaką nacionaliniam saugumui, ekonominiam stabilumui ir visuomenės gerovei. Kompiuteris dabar yra dvidešimt pirmojo amžiaus gyvenimo dalis - įrankis receptams kataloguoti, (pa)leidžiant raketas, skraidant lėktuvams ar eksploatuojant atomines elektrines. Tačiau toks efektyvumas ir išplėstas patogumas taip pat turi ir savo kaštus. Kompiuteriai ir internetas turi daugybę saugumo spragų, kuriomis sumaniai pasinaudojus, gali būti parklupdyta bet kuri nuo jų priklausanti valstybė.[1] Tobulėjant ir populiarėjant technologijoms, didėja ir šios srities grėsmės - nuo kibernetinių atakų prieš ypatingos svarbos infrastruktūrą iki duomenų saugumo pažeidimų ir dezinformacijos kampanijų. Būtent pasaulio išgyvenami iššūkiai ir augančios grėsmes, didėjantis atakų skaičius ne tik pasaulyje, bet ir Lietuvoje, bei didėjanti šių įvykių įtaka viešajam valdymui ir visuomenės gyvenimui tampa ypač aktualus. Būtent šios grėsmes ir jų reiškimasis gali sukelti krizes ar kitus reikšmingus įvykius. Šios krizės paskatina galimybių lango viešosios politikos kaitai atsiradimą, išryškina esamų sistemų veikimo spragas. Viešasis sektorius, kuriam pavesta saugoti nacionalinius interesus, vis dažniau remiasi strateginiais dokumentais ir politika, kad galėtų valdyti ir mažinti šias grėsmes. Tačiau vis dažniau susirūpinimą kelia tai, kad išorinės grėsmės nėra kontroliuojamos ir priklausančios nuo vidinių veikėjų. Tai išryškina rizikų ir grėsmių valdymo modelio ribotumą, ir verčia susimąstyti ar atsparumo grėsmėms didinimas, kuris lemtų perėjimą nuo bandymo išvengti grėsmių, prie bandymo apsiginti ir kuo greičiau atsistatyti grėsmių, nėra labiau logiška ir veiksminga kibernetinio saugumo politikos formavimo strategija.

Prieš gilinantis plačiau į patį atsparumo valdymo ir strategijos modelį, svarbu aptarti ir suprasti grėsmių valdymą ir jo formavimą, kas yra įtraukiama ir suprantama kaip grėsmės bei kokie išskiriami kovos su jomis/prieš jas iššūkiai. Tai padėtų geriau suprasti būtent kaip veikia išorinės kibernetinio saugumo grėsmės ir padėti suprasti, kodėl yra sunku jas kontroliuoti ar jų išvengti.

Kalbant apie kibernetinę erdvę, jos grėsmės ir jų keliamos problemos yra visiškai kitokio ir neregėto pobūdžio, nei įprastos politinių grėsmių erdvėje. Jų nepriskirsi nei prie tradicinių saugumo kategorijų, grindžiamų individualia saugumo atsakomybe, ekonominėmis ar įmonių saugumo problemomis, karinėmis saugumo problemomis, ar šalių vidaus ir tarptautinėmis problemomis. Taip pat kibernetinis saugumas nėra geografinis, todėl teritorinis atsakomybės pasidalijimas neturi prasmės. Kadangi kompiuterinė informacija sklinda po visą pasaulį, vietinės valstybės saugumo

[1] Richard J. Harknett, and James A. Stever, *The new policy world of cybersecurity*, (Public Administration Review 71.3, 2011), 455.

organizacijos, siekdamos išaiškinti kibernetinius nusikaltimus, vis dažniau turi bendradarbiauti su užsienio teisėsaugos institucijomis.[2]

Kibernetinės erdvės keliamos grėsmės yra kitokios savo pobūdžiu, o vienas pagrindinių grėsmingų veikimo būdų pasitelkiant kibernetinę erdvę yra kibernetinis karas (angl. Cyberwar). Autorius Chandra Kamal Borah būtent ir aprašo kibernetinio karo grėsmę ir veiksmus, kuriuos valstybėm reikėtų daryti bandant apsisaugoti. Autorius kalba, kad dėl nešifruojamo interneto žinučių pobūdžio kibernetinis karys gali lengviau gauti informaciją, o tai, kad nėra tarptautinės institucijos, kuri reguliuotų tarptautinę kibernetinę veiklą, yra dar viena kliūtis saugiai kibernetinei erdvei.[3] Kaip autorius teigia - silpnybės skatina naujas iniciatyvas.[4] 1995 m. buvo sudaryta JAV prezidento komisija dėl ypatingos svarbos infrastruktūros (PCCIP), kuri nustatė, kad kibernetinė erdvė yra pažeidžiamiausia infrastruktūra, susijusi su kiekviena ypatingos/kritinės svarbos infrastruktūra - elektros tinklais, logistikos grandine, finansų sistema ir pan. Šis suvokimas sustiprėjo po to, kai JAV susidūrė su keliomis kibernetinėmis krizėmis. Nors ir po atakų JAV dažnai imtasi iniciatyvų saugumui sustiprinti, tačiau susidurta su sunkumais dėl didžiulės privatiems veikėjams priklausančių kritinių infrastruktūrų, kurių tiesiogiai nekontroliuoja vyriausybė, gausos. JAV karinė kibernetinė vadovybė turi galimybę ir įgaliojimus apsaugoti tik karinius tinklus, bet ne visos šalies kibernetinę erdvę, nuo kurios didele dalimi priklauso JAV gyventojai. Šiuo atveju Kinija gerokai lenkia JAV, nes turi galimybių ir priemonių atjungti savo kibernetinę erdvę nuo likusio pasaulio bet kokio rimto kibernetinio karo atveju.[5]

Reaguodami į tokį pažeidžiamumą, autoriai, siūlo sprendimą, kuris eina būtent link grėsmės valdymo, o ne atsparumo valdymo teorijos link - „gynybinę triadą“ kibernetiniam saugumui užtikrinti. Pirmasis gynybinės triados komponentas yra „šerdis“ (Angl. the core). Kibernetinės erdvės „šerdis“ - tai „interneto paslaugų teikėjas“, kuris yra susijęs su kiekvienu svarbiu šalies infrastruktūros komponentu. Antrasis elementas yra elektros tinklas, be kurio būtų nutrauktas kiekvienos ypatingos svarbos infrastruktūros veikimas, o kibernetinė ataka galėtų sukelti ilgalaikį tiekimo nutraukimą. Trečioji gynybinės triados grandis yra pats Gynybos departamentas (DoD). Yra buvę incidentų, kai buvo pažeisti DoD visiškai slaptieji tinklai (angl. Secret Internet Protocol Router Network (SIPRNET) ir Joint Worldwide Intelligence Communications System (JWICS)). Autoriai aptaria „Deep Pocket Inspection System“, skirtą „nulinės dienos kenkėjiškoms“ (angl. Zero-Day Malware) programoms pažeidžiamose juodajame internete filtruoti. Užtikrinus gynybą, autoriai pasisako už

[2] *Ibid*, 455-456.

[3] Chandra Kamal Borah, *Cyber war: the next threat to national security and what to do about it? by Richard A. Clarke and Robert K. Knake*, (Strategic Analysis, 39:4, 2015), 459.

[4] *Ibid*, 459.

[5] *Ibid.*

deklaratyvią kibernetinio karo poziciją siekiant atgrasyti potencialias grėsmes ir įtvirtinti JAV pranašumą kibernetinėje erdvėje.[6]

Tarptautinėje arenoje egzistuoja ir daugiau iš kibernetinės erdvės kylančių grėsmių. Remiantis Lietuvos Nacionaline Kibernetinio Saugumo ataskaita 2023, pastarųjų dvejų metų pasaulinės krizės suteikė sukčiams galimybę kurti apgaulingas schemas, susijusias su aktualiais įvykiais (pavyzdžiui, Rusijos invazija į Ukrainą, žemės drebėjimai Turkijoje ir Sirijoje).[7] Tačiau nepaisant to 2023 m. užregistruotos nusikalstamos veikos elektroninėje erdvėje (3 912 nusikalstamos veikos) neturėjo įtakos registruoto nusikalstamumo augimui ir jų grėsmės lygis gerokai nukrito, palyginti su 2022 m. (5 309 nusikalstamos veikos elektroninėje erdvėje).[8]

Tarp aktualių kibernetinių grėsmių reikėtų atskirai išskirti ir prieš tai minėtus kibernetinius nusikaltimus - sukčiavimą bei socialinės inžinerijos metodus.[9] Įvairių formų elektroniniai nusikaltimai kelia vis didesnę grėsmę ES. Kibernetinės atakos, seksualinis vaikų išnaudojimas ir sukčiavimas internete yra sudėtingi nusikaltimai, pasireiškiantys skirtingais veikimo būdais. ***Vienas iš iššūkiu, su kuriuo yra susiduriama bandant suvaldyti kibernetinės erdvės grėsmes*** - nusikaltėliai ir toliau labai lengvai prisitaiko prie naujų technologijų ir visuomenės pokyčių, kartu nuolat stiprindami bendradarbiavimą ir tobulindami specializaciją. Nusikaltimai elektroninėje erdvėje vis plačiau plintą bei daro didelę žalą asmenims, viešajam ir privačiam sektoriui, organizacijoms, ES ekonomikai ir saugumui. Taip pat pastaraisiais metais kibernetinės erdvės saugumui pasaulyje turėjo Ukrainos-Rusijos karas ir geopolitinė situacija. Daugiausia dėl to, kad buvo įvykdyta daug DDoS (angl. Distributed Denial of Service) atakų, kenkiančių nacionalinėms ir regioninėms viešosioms institucijoms. Šios atakos dažnai buvo politiškai motyvuotos ir koordinuojamos prorusiškų įsilaužėlių grupių, reaguojant į pasisakymus ar veiksmus, kuriais remiama Ukraina. Invazija į Ukrainą taip pat dar kartą parodė kibernetinių nusikaltėlių gebėjimą prisitaikyti prie tarptautinės politinės situacijos ir oportunizmą. Internete sukčiai greitai reagavo į aplinkybes ir pasinaudojo krize kurdami įvairius su ja susijusius scenarijus.[10]

---

[6] *Ibid*, 460.

[7] Krašto Apsaugos Ministerija, *Nacionalinės kibernetinio saugumo būklės ataskaitą 2023m.*, Skelbta 2024m. Gegužės 21d., žiūrėta 2024 Birželio 19d., 55. https://www.nksc.lt/naujienos/pristatyta_2023_m_nacionaline_kibernetinio_saugumo.html

[8] *Ibid*.

[9] *Ibid*, 58.

[10] *Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaita 2024* (angl. Internet Organised Crime Threat Assessment (IOCTA 2024)). Prieiga per internetą https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf

Atsižvelgus į ilgalaikę sukčiavimų elektroninėje erdvėje spartaus augimo tendenciją, galima daryti išvadą, kad 2023 m. Lietuvoje buvo dažnesni socialinės inžinerijos metodai, kurie neturėjo poveikio informacinėms sistemoms ir (ar) jų duomenims. Socialinė inžinerija, tai duomenų išviliojimo atakos, kuriomis siekiama iš aukos išgauti prisijungimo ar kredito kortelių duomenis. Apgaulė gali pasireikšti išgalvotu tekstu ar netikro, suklastoto siuntėjo vardu el. laiškuose ar SMS trumposiose žinutėse. Duomenų viliojimo atakos išlieka populiarios ir jomis naudojasi visų tipų kibernetiniai nusikaltėliai. Pasikeitus ES reguliavimui ir apsunkinus sukčiavimo schemų, pasitelkiančių mokėjimo korteles, galimybes, nusikaltėliai daugiau dėmesio pradėjo skirti kortelių naudotojams, o ne manipuliavimui skaitmeninėmis sistemomis. Duomenų viliojimas yra pagrindinė priemonė, kurią naudoja sukčiai savo internetinio sukčiavimo schemose ir kenkimo atakų atvejais, kai siekia įsilaužti į sistemas, pavogti duomenis arba išvilioti pinigus.[11]

Šio darbo problema: Jei išorinės grėsmės yra neišvengiamos ir jų negalima visiškai kontroliuoti, kodėl organizacijos Lietuvoje vis dar pasikliauja grėsmių valdymo strategijomis, siekdamos išvengti atakų, užuot investavusios į sistemos atsparumo didinimą? Kitaip tariant, problema yra neatitikimas tarp grėsmių valdymo strategijų ir realybės, kai atakos vyksta ir daro žalą. Ar atakų dažnumas gali būti susijęs su valstybės atsparumo trūkumu? Kokie esminiai skirtumai tarp organizacijų, kurios išvengia atakų poveikio, ir tų, kurias jos paveikia? Ar skirtingas požiūris į valdymo strategijas lemia šiuos skirtumus?

Pagrindinis šio tyrimo **tikslas** – ištirti organizacijų, kurios sėkmingai išvengia atakų arba sušvelnina jų poveikį, praktiką ir palyginti jas su organizacijomis, kurios susiduria su didesnėmis neigiamomis pasekmėmis. Tyrimas analizuos, kurios organizacijos renkasi grėsmių valdymo strategijas, kurios – atsparumo stiprinimą, bei kokie veiksniai lemia šiuos pasirinkimus. Bus nagrinėjama, kas skatina tiek privačias, tiek viešas organizacijas keisti požiūrį į kibernetinį saugumą ir ar tai lemia augantis suvokimas, jog organizacijos turi būti atsparesnės.

Nors pripažįstama, kad išorinės kibernetinės grėsmės yra neišvengiamos ir negali būti visiškai kontroliuojamos, organizacijos Lietuvoje ir toliau remiasi tradicinėmis kibernetinio saugumo (rizikos valdymo) strategijomis, orientuotomis į grėsmių prevenciją ir mažinimą, užuot investavusios į visapusiškas atsparumo didinimo strategijas. Šiame tyrime keliamos **dvi hipotezės**. Pirmoji **hipotezė** teigia, kad perėjimas prie kibernetinio atsparumo – pabrėžiant įvairovę, dubliavimą, junglumą ir tarpsektorinį bendradarbiavimą – ne tik geriau parengtų organizacijas atlaikyti kibernetinius incidentus ir atsigauti po jų, bet ir užtikrintų nepertraukiamą veiklą ir prisitaikymą po incidento. Todėl hipotezėje teigiama, kad *organizacijos, taikančios į atsparumą orientuotas strategijas, greičiausiai sumažins kibernetinių atakų neigiamą poveikį ir grėsmę, bei išlaikys ilgalaikį funkcionalumą,*

[11] Krašto Apsaugos Ministerija, *Nacionalinė kibernetinio saugumo būklės ataskaita 2023*, 56.

palyginti su organizacijomis, kurios daugiausia naudoja tik įprastines kibernetinio saugumo priemones.

Antroji **hipotezė** pabrėžia, kad, nors išorinės grėsmės yra neišvengiamos ir negali būti visiškai (su)kontroliuojamos, norint veiksmingai reaguoti į kibernetines grėsmes, reikia teikti pirmenybę atsparumui, o ne vien rizikos/saugumo valdymui. Toks požiūris galėtų padėti sumažinti atakų pasekmes ir užtikrinti tęstinumą, gebėjimą prisitaikyti ir atsigavimą.

Šio tyrimo **uždaviniai** yra susiję su keliomis pagrindinėmis tyrimo kryptimis. Pirmiausia, bus ištirta, kaip organizacijos Lietuvoje renkasi grėsmių valdymo ir atsparumo didinimo strategijas bei kokie veiksniai lemia šiuos pasirinkimus. Tai padės geriau suprasti, kaip organizacijos reaguoja į kibernetines grėsmes ir kokie yra jų prioritetai, siekiant užtikrinti veiklos tęstinumą. Antrasis uždavinys – sukurti tyrimo modelį, skirtą analizuoti organizacijų atsparumą kibernetinėms grėsmėms, naudojant tiek teorinius, tiek praktinius duomenis. Tyrimo modelis bus pagrįstas struktūruotais interviu ir dokumentų analize, siekiant giliau suprasti, kaip organizacijos įgyvendina atsparumo strategijas. Trečiasis uždavinys apima klausimyno parengimą ir interviu atlikimą su įvairių sektorių organizacijų atstovais, kad būtų įvertintas jų požiūris į kibernetinio saugumo strategijas ir atsparumo stiprinimą. Galiausiai, ketvirtasis uždavinys – atlikti dokumentų analizę, įvertinant Lietuvos kibernetinio saugumo teisės aktus ir jų poveikį organizacijų atsparumo didinimui, ypač atsižvelgiant į viešojo ir privataus sektoriaus bendradarbiavimą.

2. Teorinė dalis

Kalbant apie kibernetinį saugumą, viena iš svarbiausių diskusijų temų - geriausias būdas apsaugoti skaitmenines infrastruktūras vis labiau susijusiame pasaulyje. Tradiciškai kibernetinio saugumo strategijose daugiausia dėmesio skiriama rizikos prevencijai, aptikimui ir mažinimui, kad būtų išvengta kibernetinių atakų ir didelės žalos. Taikant šiuos metodus pirmenybė teikiama stiprios gynybos priemonių kūrimui, kad grėsmės būtų sustabdytos prieš joms įvykstant, remiantis prielaida, kad išorinius pavojus galima numatyti ir užkirsti jiems kelią vykdant stebėseną ir prevenciją.

Tačiau tobulėjant technologijoms ir sudėtingėjant kibernetinėms grėsmėms, manoma, kad šio į prevenciją orientuoto modelio nebepakanka. Kritikai atkreipia dėmesį į vis sudėtingesnes atakas, pavyzdžiui, išpirkos reikalaujančias programas, „phishing“ ir DDoS atakas, ir teigia, kad pasikliauti vien tik prevencija yra nerealu. Kibernetinių grėsmių nenuspėjamumas ir nuolatinė raida aiškiai rodo, kad nė viena sistema negali būti visiškai apsaugota nuo įsilaužimo.

Dėl to dėmesys pereina prie atsparumo koncepcijos, kurioje pabrėžiamas gebėjimas atsigauti ir prisitaikyti, kai kibernetinės atakos neišvengiamai įvyksta kaip nekontroliuojama išorinė grėsmė. Užuot sutelkus dėmesį ne tik į gynybą nuo grėsmių, atsparumo strategijose prioritetas teikiamas užtikrinimui, kad sistemos galėtų greitai atsigauti ir toliau veikti net ir po atakos. Tai apima tokių priemonių, kaip dubliavimas, išteklių pritaikomumas ir greito atkūrimo protokolai, įgyvendinimą.

Diskusijos tarp rizikos valdymo ir atsparumo taip pat apima ir tai, kaip turėtų būti skirstomi ištekliai. Tradicinio rizikos valdymo šalininkai pasisako už dideles investicijas į gynybą, kad pirmiausia būtų užkirstas kelias atakoms. Kita vertus, atsparumo šalininkai teigia, kad organizacijos taip pat turėtų investuoti į savo gebėjimą atsigauti ir prisitaikyti po atakos, taip sumažinant ilgalaikę žalą veiklai.

Šioms diskusijoms įsibėgėjant, atsparumas tampa vis svarbesne visapusiškos kibernetinio saugumo strategijos dalimi. Juo pripažįstama, kad nors nė viena sistema negali būti visiškai apsaugota nuo visų grėsmių, organizacijos vis tiek gali užtikrinti savo išsilaikymą ir tolesnį veikimą, sutelkdamos dėmesį į tai, kaip sėkmingai jos gali atsigauti. Toks besikeičiantis požiūris į kibernetinį saugumą reikalauja dinamiškesnio požiūrio, kuris suderina ir prevenciją, ir gebėjimą greitai prisitaikyti ir atsigauti po kibernetinių incidentų.

2.1 Auganti kibernetinė grėsmė tarptautinėje arenoje

Viena labiausiai pasaulyje kylančių ir aptariamų 2021-ais metais kibernetinio saugumo grėsmių buvo duomenis šifruojantis ir išpirkos reikalaujantis kenkimo kodas (angl. ransowmare).[12] Per 2023-us metus jų skaičius tik augo[13], to paties tikimasi ir 2024-iais metais, vis augant nelegaliai paviešintos privačios informacijos skaičiui[14]. Pasak 2022-ų metų grėsmių nacionaliniam saugumui vertinimo, „ransomware" atakų skaičius kasmet tik auga.[15] Šio tipo atakos pasižymi tuo, kad dažniausiai neturi valstybinio viršininko ar „galvos", bet dažnai taikomos prieš tokius veikėjus kaip valstybinės organizacijos, dirbančios su sveikatos duomenimis, ar su valstybinių organizacijų duomenimis dirbančias institucijas. Tai atakos, kuomet grupė individų gauną prieigą prie objekto kompiuterių sistemos, dažnai naudojant kitą atakų rūšį – informacijos rinkimo atakas (angl. phishing), bei taip pat įtraukia ir įsilaužimą į virtualų privatų tinklą (angl. virtual private network arba VPN), kurio pirminė paskirtis būna riboti bei filtruoti darbuotojų prieigą prie vidinės įmonės IT sistemos, kai dirbama ne iš ofisų, saugumo sumetimais. Įsibrovėliams patekus į sistemą, yra paliekama kenkėjiška sistema/programa, kuri užšifruoja kompiuteriuose ir sistemoje esančią informaciją taip neleidžiant jos pasiekti. Pavogus prieigą prie resursų, grupuotės reikalauja išpirkos mainais į duomenų iššifravimą.[16] Kaip teigiama Kibernetinio Saugumo ataskaitoje, 2023 m. sumokėti išpirką buvo prašoma tiek valiuta, tiek konvertuojant ją į kriptovaliutą ir pervedant į nurodytą piniginės adresą. 2023 m. reikalautų išpirkų dydis buvo nuo 186,8 ETH (400 Eur) iki 900 000 USD (832 254 Eur), o didžiausia 2022 m. prašoma išpirkos suma buvo 1000 BTC (22 529 000 Eur). 2023 m. nustatyta, kad elektroniniams duomenims užšifruoti buvo naudojami 11-os šeimų elektroninius duomenis užšifruojantys ir išpirkos reikalaujantys kenkimo programinio kodo virusai[17].

Taip pat tarp populiarių grėsmių išskiriamos ir anksčiau minėtos DDoS atakos, kurios pasireiškia kaip informacinių sistemų sutrikdymo programos, kurių metu yra perkraunami sistemų serveriai, siekiant jų „užlūžimo". Kaip rašoma Nacionalinio Kibernetinio Saugumo strategijoje, 2023 m. pradėti 2 ikiteisminiai tyrimai (arba 1-u mažiau nei 2022 m.) dėl informacinių sistemų trikdymo

---

[12] Krašto Apsaugos Ministerija, *Nacionalinė kibernetinio saugumo būklės ataskaita, 2021.*.

[13] Krašto Apsaugos Ministerija, *Nacionalinė kibernetinio saugumo būklės ataskaita 2023*, 62.

[14] Avast, *Avast 2023 Predictions Highlight Increase Risk for Detrimental Damage Caused By Rnasomware Gangs*, 2022, žiūrėta 2024m. Birželio 16d., https://press.avast.com/avast-2023-predictions-highlight-increased-risk-for-detrimental-damage-caused-by-ransomware-gangs

[15] Lietuvos valstybės saugumo departamentas, *Grėsmių Nacionaliniam saugumui vertinimas 2022,* (2022), 46.

[16] Dan Milmo, „NHS Ransomware attack: what happened and how bad it is*?",* The Guardian, 2022, žiūrėta 2024m. Birželio 16d.,
https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and- how-bad-is-it

[17] Krašto Apsaugos Ministerija, *Nacionalinė kibernetinio saugumo būklės ataskaita 2023*, 62.

DDoS atakomis. Nuo 2020 m. Lietuvos policijos tyrimų, pradėtų dėl DDoS atakų, skaičius išlieka stabilus (2020–2023 m. laikotarpio vidurkis – iki 3-jų atvejų per metus). Vienas iš ikiteisminių tyrimų buvo pradėtas dėl masinių DDoS atakų prieš Lietuvos valstybinių institucijų ir verslo interneto svetainių paveikimo nuo 2023 m. gegužės 6 d. iki 2023 m. birželio 4 d. (ne mažiau kaip 40 svetainių) ir nuo 2023 m. liepos 10 d. iki 2023 m. liepos 13 d. (ne mažiau kaip 21 svetainė). Šioms DDoS atakoms, kuriomis buvo reaguojama į Lietuvos valstybės paramą, skirtą padėti Ukrainai atremti Rusijos karinę agresiją, taip pat į NATO viršūnių susitikimą 2023 m. liepos mėnesį Vilniuje, organizuoti susivienijo ne mažiau kaip 17 Rusijos programišių grupių. Tarp jų buvo ir 2022 m. prieš Lietuvą veikusi Rusijos programišių grupė „Killnet“. Atakuotų Lietuvos svetainių sąrašus ir poveikio joms rezultatus Rusijos programišių grupė „Noname05716“ viešino „Telegram“ kanale.[18]

Tarp įvairių kibernetinių grėsmių mokslininkai taip pat įvardija kibernetinį terorizmą kaip didelį susirūpinimą keliančią problemą. Autorių Denniso Broederso, Fabio Cristiano ir Daano Weggemanso straipsnyje nagrinėjama nacionalinės politikos ir tarptautinės diplomatijos kibernetinio terorizmo srityje raida ir sąveika Jungtinių Tautų Saugumo Tarybos penkių nuolatinių narių grupėje ir JT procesai, susiję su kibernetinėmis normomis. Autoriai atskleidžia, kaip nacionalinėje politikoje kibernetinis terorizmas vis dažniau įvardijamas kaip informacinio saugumo klausimas, taikant prevencines priemones, taikomas mažo poveikio kibernetinei veiklai ir interneto turiniui. Jie taip pat problematizuoja išsamių ir netikslių apibrėžčių priėmimą diplomatine kalba, kuri gali suteikti tarptautinę paramą autoritariniams režimams, kovojantiems su terorizmu, kad persekiotų vidaus opoziciją ir pažeidžiamas grupes. Be to, autoriai daro išvadą, kad norint užtikrinti žmogaus teisių apsaugą visame pasaulyje, būtina derinti normatyvines diskusijas dėl kibernetinio terorizmo ir diskusijas dėl informacinio saugumo.[19]

Straipsnyje pabrėžiami kibernetinio terorizmo apibrėžimo ir ***kovos su juo iššūkiai,*** pažymint, kad daugumoje apibrėžimų atskiriami politiškai motyvuoti smurtiniai veiksmai naudojant internetą ir parengiamoji veikla, pavyzdžiui, verbavimas ir bendravimas. Dėl terorizmo „mažos tikimybės/rizikos, didelio poveikio“ pobūdžio vyriausybės pirmiausia sutelkia dėmesį į kovą su šia parengiamąja veikla. Dėl to atsirado skaitmeninės priežiūros tendencija ir išskirtinių saugumo priemonių taikymas platesnei veiklai internete. Autoriai teigia, kad skaitmeninės priežiūros įgaliojimų išplėtimas kovojant su kibernetiniu terorizmu kelia didelį susirūpinimą dėl pagrindinių teisių, tokių kaip privatumas ir žodžio laisvė. Išskirtinių priemonių normalizavimas liberaliose

[18] *Ibid*, 62.

[19] Dennis Broeders, Fabio Cristiano & Daan Weggemans, *Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy*, (Studies in Conflict & Terrorism, 46:12, 2023), 2426.

demokratinėse šalyse gali pakenkti jų, kaip skaitmeninių teisių gynėjų, pozicijai ir tapti precedentu autoritariniams režimams pateisinti represinius veiksmus.[20]

Taip pat kibernetinį terorizmą minį autoriai Hulisi Öğüt, Srinivasan Raghunathan ir Nirup Menon. Šiame straipsnyje nagrinėjami ***kibernetinio saugumo rizikos ir grėsmių valdymo*** iššūkiai tiek iš įmonės (privačių veikėjų), tiek iš politikos perspektyvos. Autoriai nagrinėja koreliuotos rizikos, netobulos galimybės įrodyti nuostolius ir galimybės stebėti savisaugos pastangas poveikį įmonių kibernetinio saugumo strategijoms. Jie nustatė, kad dėl šių veiksnių įmonės į savisaugą ir draudimą investuoja mažiau, nei būtų socialiai optimalu. Tyrime siūloma, kad tinkamos viešosios politikos intervencijos, pavyzdžiui, savisaugos subsidijos ir draudimo įmokų mokesčiai, gali pagerinti kibernetinio saugumo rizikos ir grėsmių valdymą.

Pirma, autoriai aiškina, kad įmonės susiduria su koreliuojančia rizika dėl bendrų technologijų ir tarpusavyje susijusių sistemų, kurios gali sustiprinti pažeidžiamumą. Įvykus pažeidimui, įmonėms dažnai sunku įrodyti draudikams savo nuostolius, ypač kai tai susiję su nematerialiais nuostoliais, tokiais kaip (gera) reputacija.[21] Šią problemą apsunkina tai, kad išorės šalims, pavyzdžiui, draudikams, sunku stebėti įmonių savisaugos bei apsaugos priemones, todėl nepakankamai investuojama į saugumą ir draudimą.[22]

Straipsnyje siūloma, kad viešoji politika gali atlikti svarbų vaidmenį mažinant šiuos iššūkius. Pavyzdžiui, jei draudikai gali stebėti įmonės savisaugos priemones, tuomet savisauga ir draudimas veikia kaip vienas kitą papildantys elementai. Tokiu atveju savisaugos subsidija gali paskatinti įmones optimaliai investuoti ir į apsaugą, ir į draudimą. Ir atvirkščiai, jei savisaugos neįmanoma stebėti, savisauga ir draudimas veikia kaip pakaitalai. Šiuo atveju draudimo įmokų mokestis gali paskatinti įmones investuoti į savisaugą.[23]

Analizėje apžvelgiama esama literatūra apie rizikos valdymą ir draudimą, pabrėžiant pagrindinius Ehrlicho ir Beckerio bei Rothschildo ir Stiglitzo darbus. Šie darbai suteikia pagrindą suprasti savisaugos ir draudimo sąveiką.[24] Autoriai taip pat gilinasi į kibernetinį draudimą, pažymėdami, kad nors jis yra ribotas, tačiau labai svarbus kibernetinei rizikai valdyti. Majuca ir kt.

---

[20] *Ibid*, 2427, 2430, 2432, 2437.

[21] Hulisi Öğüt, Srinivasan Raghunathan, and Nirup Menon, *Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection*, (Risk Analysis: An International Journal 31.3, 2011), 497.

[22] Hulisi Öğüt,, Srinivasan Raghunathan, and Nirup Menont, 498.

[23] *Ibid*, 499.

[24] *Ibid*, 498-499.

bei Gordon, Loeb ir Sohail tyrimuose pabrėžiama, kad kibernetiniam draudimui reikalingi tinkami kainodaros modeliai.[25]

Autoriai daro išvadą, kad dėl koreliuojančios rizikos ir netobulos galimybės įrodyti nuostolius įmonės nepakankamai investuoja į savisaugą ir draudimą. Siekiant paskatinti įmones investuoti socialiai optimaliu lygiu, būtina imtis viešosios politikos intervencijų, pritaikytų prie to, ar savisauga yra stebima, ar ne. Ši analizė galioja nepriklausomai nuo to, ar draudimo rinka yra tobulai konkurencinga, ir pabrėžia, kad vien tik draudimo rinkos reformos nepakanka, norint pasiekti veiksmingą kibernetinio saugumo rizikos ir grėsmių valdymą.[26]

Be kylančių saugumo grėsmių kibernetinėje erdvėje, taip pat yra susiduriama ir su grėsmių ir atakų „atgrasymu“. Tai plačiai aptaria Autorius Joseph Nye. Mokslininkai vis daugiau dėmesio skiria sudėtingai kibernetinio saugumo ir viešosios politikos dinamikai. Pagrindinis šios srities klausimas - ar šalys gali veiksmingai atgrasyti kitus nuo žalos kibernetinėje erdvėje darymo. Buvęs Estijos prezidentas Toomas Ilvesas pabrėžė nuolatinį atgrasymo iššūkį NATO, pabrėždamas veiksmingų strategijų kibernetinėms grėsmėms įveikti poreikį.[27] ***Sparti interneto, kuris dabar jungia beveik pusę pasaulio gyventojų ir reikšmingai prisideda prie pasaulio ekonomikos augimo, plėtra sukūrė naujų tarptautinio (ne)saugumo aspektų. Prie interneto prijungtų įrenginių plitimas ir didėjanti ypatingos svarbos infrastruktūros priklausomybė nuo kibernetinės erdvės pabrėžia didėjantį kibernetinių atakų pažeidžiamumą ir žalos potencialą***. Pavyzdžiui, Jungtinės Valstijos tapo labai priklausomos nuo kibernetinės erdvės įvairioms ypatingos svarbos funkcijoms vykdyti, todėl jos neproporcingai pažeidžiamos tiek nacionalinių valstybių, tiek nevalstybinių veikėjų keliamų kibernetinių grėsmių. Šis paradoksas išryškina sunkumus kuriant veikiančią ir efektyvią ***grėsmių valdymo*** kibernetinio saugumo politiką, kuri galėtų neatsilikti nuo besikeičiančios grėsmių aplinkos. Josephas Nye, nagrinėjo tradicinių atgrasymo teorijų apribojimus kibernetinėje erdvėje, atkreipdami dėmesį į unikalius iššūkius, kylančius dėl priskyrimo ir nekinetinio kibernetinių atakų pobūdžio. Literatūroje taip pat pabrėžiama tarptautinio bendradarbiavimo, viešojo ir privačiojo sektorių partnerystės ir patikimų reguliavimo sistemų svarba siekiant padidinti kibernetinį saugumą.[28] Apskritai, mokslinėje diskusijoje pabrėžiama, kad reikia įvairiapusio požiūrio į kibernetinį saugumą, integruojant technines, politines ir strategines perspektyvas, kad būtų galima spręsti sudėtingas ir dinamiškas kibernetinių grėsmių problemas.

[25] *Ibid*, 500.

[26] *Ibid*, 502-503.

[27] Joseph S. Nye Jr., *Deterrence and dissuasion in cyberspace*, (International security 41.3, 2016), 44.

[28] Nye, 68-71.

Aptariant kibernetines grėsmes ir reglamentus, labai svarbu suprasti mechanizmus ir subjektus, atsakingus už šių reglamentų įgyvendinimą, kuris žymiai prisideda ne tik prie kibernetinio saugumo grėsmių valdymo strategijų, bet lygiai taip pat ir tampa svarbus komponentas vykdant kibernetinio ***atsparumo didinimo/valdymo strategijose***. Per pastaruosius dešimtmečius kibernetinis saugumas užėmė svarbią vietą Europos Sąjungos politinėje darbotvarkėje. Toks dėmesys lėmė Europos Sąjungos kibernetinio saugumo agentūros (ENISA), kuri yra pagrindinis ES kibernetinio saugumo pastangų veikėjas, įsteigimą. Myriam Dunn Cavelty ir Maxo Smeetso straipsnyje nagrinėjama, kaip ENISA iškilo ir stabilizavosi kaip pagrindinė agentūra, nepaisant didelių iššūkių siekiant įgyti episteminį autoritetą. Remdamiesi politinių dokumentų, antrinių šaltinių ir pusiau struktūruotų interviu duomenimis, autoriai analizuoja agentūros pastangas išsikovoti specifinį vaidmenį platesnėje ES kibernetinio saugumo ekosistemoje. Jie atskleidžia ENISA formavimosi sudėtingumą, parodydami, kaip agentūros vaidmenį lėmė vykstanti politinė kova ir poreikis prisitaikyti prie besikeičiančių technologijų ir grėsmių.[29]

Autoriai teigia, kad ENISA vystymosi "kelionė" pabrėžia platesnę saugumo valdymo dinamiką ES, kur reguliavimo metodai dažnai vyrauja prieš tiesioginį valstybės įsikišimą. Jie pabrėžia, kad ENISA kova siekiant įsitvirtinti kaip autoritetinga veikėja simbolizuoja iššūkius, su kuriais susiduria reguliavimo agentūros, siekdamos užsitikrinti episteminį autoritetą. Straipsnyje teigiama, kad nors ENISA trajektorija palaiko reguliavimo valdymo bandymus, jos vaidmuo nuolat kinta ir išlieka didesnės, sudėtingos saugumo valdymo sistemos dalimi. Šis tyrimas padeda suprasti, kaip saugumo valdymas turi išlikti lankstus, kad galėtų prisitaikyti prie hibridinių formų ir politinių kovų, pabrėždamas, kad reikia niuansuoto požiūrio į saugumo valstybių reguliavimo analizę.[30]

2.2 Atsparumas

Aptarus kibernetinio saugumo arba kitaip grėsmių, rizikos valdymo strategijas, reikėtų aptarti ir kibernetinio atsparumo supratimą ir apibrėžimą, kad galima būtų siekti visokeriopo supratimo apie tai, kuo skiriasi šios dvi kibernetinės erdvės politikos strategijos.

Kalbant apie kibernetinę erdvę ir jos saugumą, neatsiejama sąvoka tampa ir kibernetinis atsparumas. Autoriai Kottas ir Linkovas savo darbe apie kibernetinio atsparumo matavimą, pabrėžia, kad kibernetinis atsparumas skiriasi nuo kibernetinio saugumo grėsmių ir rizikos valdymo, kuriuo tradiciškai siekiama užkirsti kelią grėsmėms.[31] *Kol kibernetinio saugumo grėsmių ir rizikos valdymas*

[29] Myriam Dunn Cavelty & Max Smeets, *Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority*, (Journal of European Public Policy, 30:7, 2023), 1331.

[30] Myriam Dunn Cavelty & Max Smeets, 1342.

[31] A. Kott., & Linkov, I. *To Improve Cyber Resilience, Measure It.* (IEEE Computer, 2021, 54(2)), 80-85.

labiau kreipia dėmesį į grėsmės kelio užkirtimą, jų aptikimą ir grėsmės sumažinimą, nuolat bandant jas aptikti, stebėti ir laiku išsikišti, ***vietoj to kibernetinis atsparumas sutelkia dėmesį į sistemos gebėjimą pasipriešinti, atsistatyti ir adaptuotis po įsilaužimo***. Skirtingai nuo tradicinių rizikos valdymų ir vertinimų (saugumo), kuriais matuojama konkrečių komponentų gedimo/pažeidimo tikimybė/rizika esant nustatytoms grėsmėms, kibernetinis atsparumas pripažįsta kibernetinių grėsmių tikimybę/riziką ir sutelkia dėmesį į sistemos atsigavimo trajektoriją po nepageidaujamo įvykio. Šis pokytis pabrėžia, kad svarbu atsparumą vertinti ne tik pagal pirminį atsparumą (atsparumą nuo atakos), bet ir pagal tai, kaip efektyviai ir greitai sistema gali atkurti funkcijas ir prisitaikyti prie naujų grėsmių.[32]

Kott ir Linkovas pabrėžia, kad kibernetinio atsparumo pasiekimas ir vertinimas yra sudėtingas, nurodydami, kad *daugelis atsparumo strategijų paprasčiausiai sutvirtina sistemas, o ne užtikrina adaptyvų atsistatymą*. Jie pažymi, kad pridėjus per daug apsaugos priemonių, gali atsirasti pažeidžiamumų, nes padidėja pačios atakos plotas ir gali kilti grandininių klaidų. Taigi, norint užtikrinti tikrą kibernetinį atsparumą, reikia taikyti matavimo metodus, kuriais būtų vertinami ne statiški sutrikimų tikimybės rodikliai, o laikini atkūrimo ir prisitaikymo modeliai. Autoriai teigia, kad reikia taikyti empirinius, griežtus atsparumo kiekybinio įvertinimo metodus, lyginant juos su medžiagų savybių matavimu fizikoje, kad būtų užtikrinta, jog sistemos gali išlaikyti kritines funkcijas esant kibernetiniams spaudimo veiksniams/sąlygoms. Jų metodas apima užduočių, kurios yra svarbios tikslui, apibrėžimą, įvairių priešiškų veiksnių spaudimo taikymą ir sistemos tvaraus funkcionalumo įvertinimą, siekiant sukurti patikimą kibernetinio atsparumo vertinimo ir gerinimo sistemą.[33]

Remdamiesi ankstesniu Kotto ir Linkovo kibernetinio atsparumo, kaip sistemos gebėjimo atsigauti ir prisitaikyti po kompromiso, tyrimu, Linkovas ir Kottas knygoje „Fundamental Concepts of Cyber Resilience: Introduction and Overview" praplečia šį supratimą, aptardami didėjančią šiuolaikinės visuomenės priklausomybę nuo sudėtingų kibernetinių sistemų, kurios yra pažeidžiamos vis didesnio kibernetinių grėsmių skaičiaus[34]. Kibernetinis atsparumas, kaip jie jį apibrėžia, peržengia tradicinio kibernetinio saugumo ribas, sutelkdamas dėmesį į sistemos **gebėjimą pasirengti, absorbuoti, atsigauti ir prisitaikyti** prie nepalankių kibernetinių įvykių[35]. Nors tradiciniuose rizikos vertinimuose rizika apskaičiuojama remiantis žinomomis grėsmėmis, pažeidžiamumais ir pasekmėmis, jie teigia, kad toks požiūris yra ribotas, kai reikia atsižvelgti į nenuspėjamą kibernetinių

[32] *Ibid.*

[33] *Ibid.*

[34] I. Linkov, & Kott, A. *Fundamental Concepts of Cyber Resilience: Introduction and Overview*. (In Cyber Resilience of Systems and Networks, Springer, 2018), 1-13.

[35] *Ibid.*

grėsmių pobūdį ir grandininį poveikį, kurį šios atakos gali sukelti tarpusavyje susijusioms sistemoms[36]. Dėl to reikia pereiti prie atsparumo, panašaus į biologinį imunitetą, siekiant padidinti sistemų gebėjimą reaguoti ir atsigauti po kibernetinių pažeidimų [37].

Autoriai taip pat paaiškina, kad kibernetinis atsparumas apima kelių sričių - fizinės, informacinės, kognityvinės ir socialinės - ypatybes, pabrėždami, kad kiekvienoje iš jų reikalingi atsparumo mechanizmai[38]. Jie nurodo, kad atsparumas yra kilęs iš įvairių disciplinų, nuo ekologijos iki inžinerijos, kurių kiekviena prisideda prie skirtingų, tačiau persidengiančių principų. Tarp jų - kritinės svarbos charakteristikos, adaptyvus valdymas ir įsiminimas, būtini norint išlaikyti veiklos efektyvumą krizės metu. Jau anksčiau minėta, kad atsparumą apibrėžia keturi komponentai. Kibernetinį atsparumą taip pat apibrėžią ir Nacionalinė mokslo akademija (angl. National Academies of Science), kaip gebėjimą ***planuoti, absorbuoti, atsigauti ir prisitaikyti***; Linkovas ir Kottas pritaria šiai apibrėžčiai, pažymėdami, kad ji plačiai taikoma visose socialinėse ir techninėse sistemose[39]. Ši išsami atsparumo struktūra leidžia įvairiapusiškai jį suprasti, neapsiribojant vien tik grėsmės atgrasymu/užkirtimu (kas būdinga grėsmių valdymui ir rizikos valdymų grįstoms kibernetinio saugumo strategijoms), pripažįstant, **kad tam tikro laipsnio poveikis yra neišvengiamas**, ir sutelkia dėmesį į tai, kaip greitai ir veiksmingai sistema gali atsigauti[40].

Remdamasis Kotto ir Linkovo fundamentalia diskusija apie kibernetinį atsparumą kaip priemonę, padedančią išlaikyti sistemos funkcionalumą po pažeidimo, Hauskenas išplečia šią koncepciją, nagrinėdamas kibernetinį atsparumą ir įvairiuose visuomenės veikėjų ir organizacijų lygmenyse[41]. Hauskenas mano, kad kibernetinis atsparumas apima ne tik sistemas ir kompiuterių tinklus, bet ir veikėjų - - individų, organizacijų ar vyriausybių - elgseną, resursus ir pasirinkimus. Svarbu tai, kad jis atskiria grėsmės nekeliančius veikėjus, kurie stengiasi didinti kibernetinį atsparumą, ir grėsmę keliančius veikėjus, kurių veikla trukdo atsparumui. Be to, jis pateikia hibridinių veikėjų, kurie, priklausomai nuo jų tikslų ir aplinkybių, gali ir palaikyti, ir mažinti atsparumą, sąvoką[42].

Hauskenas pabrėžia, kad kibernetinis atsparumas, priešingai nei grėsmių ir rizikos valdymų grįstas kibernetinis saugumas, turi prisitaikyti prie sudėtingos veikėjų sąveikos ir grėsmių aplinkos nenuspėjamumo. Užuot sutelkęs dėmesį ne tik į sistemų stiprinimą, Hauskenas teigia, kad strategijos

[36] *Ibid.*

[37] *Ibid.*

[38] *Ibid.*

[39] *Ibid.*

[40] *Ibid.*

[41] Kjell Hausken, *Cyber resilience in firms, organizations and societies*m, (*Internet of Things* 11, 2020, 100204), 2.

[42] *Ibid*, 3.

turi apimti atsparumą didinančias priemones ir kompetencijas, pavyzdžiui, išteklių paskirstymą, technologinius atnaujinimus ir prisitaikymo strategijas tarp organizacinių ir individualių dalyvių[43]. Toks požiūris yra būtinas siekiant spręsti šiuolaikinėms infrastruktūroms būdingus pažeidžiamumus, pavyzdžiui, dalykų interneto (angl. Internet of Things, IoT) infrastruktūroms, kuriose kibernetinių ir fizinių trikdžių potencialas sudaro milžinišką atakų plotą. Hauskenas pažymi, kad plačiai paplitusi IoT integracija ir dirbtinio intelekto bei kompiuterinio mokymosi įtraukimas gali palengvinti kasdienes funkcijas, tačiau taip pat kelia didelę etinę, techninę ir saugumo riziką[44].

Hauskenas taip pat nagrinėja kibernetinio draudimo, kaip rizikos perkėlimo mechanizmo, kuris gali paskatinti organizacijas taikyti patikimas kibernetinio saugumo priemones, vaidmenį. Nustatydamos prisijungimo reikalavimus ir siūlydamos reagavimo į incidentus ir duomenų atkūrimo paslaugas, draudimo bendrovės gali padidinti apdraustų organizacijų kibernetinį atsparumą. Hauskenas teigia, kad veiksmingos atsparumo strategijos turi apimti pasirengimo, išteklių paskirstymo ir prisitaikymo kombinaciją, taip pat griežtus standartus ir bendradarbiavimą dalijantis informacija tarp sektorių ir veikėjų[45]. Šis daugiasluoksnis požiūris į atsparumą atspindi platesnes atsparumo apibrėžtis, kurios apima tokias sritis kaip ekologija ir inžinerija ir yra nuosekliai pagrįstos sistemos gebėjimu pasirengti, absorbuoti, atsigauti ir prisitaikyti prie įvykių[46].

Rasa Bortkevičienė, Vitalis Nekrošius, Inga Patkauskaitė-Tiuchtienė, Ramūnas Vilpišauskas atsparumą įvardina kitaip - ne kaip tam tikrų krizinių situacijų ir grėsmių išvengimą, bet kaip atsispyrimą ir atsistatymą nuo jų. Autoriai atsižvelgia į kelis aspektus. Pirmiausia tai, kad viešasis sektorius vis dažniau susiduria su kompleksinėmis problemomis ir rutininių įvykių mastą viršijančiais įvykiais, dėl ko sisteminių grėsmių ateityje tik daugės. Antra - neįmanoma iš anksto suplanuoti visų grėsmių ir joms pasirengti, dėl to svarbų stiprinti institucijų atsparumą, jog vienoje srityje sukelti reikšmingi iššūkiai nesustabdytų kitų sistemos dalių veikimo. Autoriai taip pat pabrėžia, kad nors ir su atsparumo sąvoka dažniausiai yra siejamas institucijų ar sistemų gebėjimas atsigauti po patirtų šokų ir grįžti į pradinę poziciją, socialinėje srityje labiau pastebimas ne poreikis “atšokti atgal”, o “atsispirti nuo” reikšmingų įvykių, prisitaikant prie veikimo naujoje realybėje.[47] Autoriai atsparumą supranta kaip viešojo sektoriaus institucijų gebėjimą suvaldyti reikšmingus įvykius bei prisitaikyti prie pakitusių veikimo sąlygų, pritaikant išmokas pamokas ir tobulinant viešosios politikos

[43] *Ibid*, 4.

[44] *Ibid.* 7.

[45] *Ibid*, 5.

[46] *Ibid*, 6.

[47] Rasa Bortkevičiūtė, Vitalis Nakrošis, Inga Patkauskaitė-Tiuchtienė, and Ramūnas Vilpišauskas. *Nėra to blogo, kas neišeitų į gera? Reikšmingų įvykių įtaka viešosios politikos kaitai Lietuvoje 2004-2020m*. (2024).

uždavinius, priemones, įgyvendinimo sąrangą bei gebėjimus, siekiant apsisaugoti nuo panašių reiškinių ateityje ar sumažinti jų galimą poveikį.[48]

Autoriai taip pat teigia, kad atsparumo sąvoka nėra vienalytė ir yra skiriamos skirtingos jos dimensijos: socialinis (sietinas su visuomenės, institucijų tinklo veikla šoko akivaizdoje ir po jo), fizinis arba techninis (sietinas su esama infrastruktūra, jos gebėjimu vykdyti funkcijas susidūrus su krizėmis ar nelaimėmis) bei informacinis (sietinas su keitimusi informacija ir duomenimis reikšmingo įvykio metu) atsparumas[49]. Nors skirtingos dimensijos pasižymi skirtingais atsparumo kriterijais, galima pastebėti ir horizontalių, visoms atsparumo kategorijoms būdingų charakteristikų, pavyzdžiui: įvairovė (veikėjų, išteklių ir kt.), sudaranti galimybę pasirinkti iš kelių veikimo alternatyvų; sampyna, užtikrinsianti, jog tą pačią funkciją gali atlikti kelios institucijos ar veikėjai; susietumas, leidžiantis sklandžiai keistis informacija ir ištekliais, reikalingais sistemoms veikti. Taip pat, galiausiai, atsparumo stiprinimas sietinas su skirtingų veikėjų, institucijų ir sektorių bendradarbiavimu, suteikiančiu prieigą prie gausesnių fizinių ir informacinių išteklių[50].

Remdamiesi koncepcijomis, kuriose pabrėžiamas strateginis kibernetinio atsparumo vaidmuo ypatingos svarbos infrastruktūroje, Harropas ir Mattesonas nagrinėja, kaip Jungtinė Karalystė ir JAV taiko saugumo priemones, kad apsaugotų nacionalinį saugumą ir būtinąsias paslaugas didėjant kibernetinėms grėsmėms.[51] Kibernetinis atsparumas, kaip jie apibrėžia, yra ne tik gynybinė priemonė, bet ir ***pagrindinė nacionalinio saugumo kryptis***, kuria sprendžiami vis labiau tarpusavyje susijusių infrastruktūrų pažeidžiamumo klausimai. Jų analizėje pabrėžiami iššūkiai, kylantys dėl pažangių, koordinuotų kibernetinių atakų prieš ypatingos svarbos nacionalinę infrastruktūrą (angl. critical national infrastructure, CNI), ir ypatinga rizika, kurią kelia "daiktų internetas" (angl. Internet of Things, IoT), dar labiau išplečiantis „atakos paviršių" dėl tarpusavyje sujungtų įrenginių tinklų.[52]

Harropas ir Mattesonas iliustruoja aktyvius veiksmus, kurių ėmėsi abi šalys, siekdamos nustatyti, atgrasyti ir likviduoti kibernetines grėsmes. Pavyzdžiui, JAV pripažįsta kibernetinę erdvę kaip nacionalinio saugumo sritį, įsteigė Jungtinių Valstijų kibernetinę vadavietę (USCYBERCOM) ir įgyvendina tokias iniciatyvas kaip Visapusiška nacionalinė kibernetinio saugumo iniciatyva (CNCI), kad sustiprintų ypatingos svarbos infrastruktūrą nuo kibernetinių incidentų.[53] Tuo tarpu

[48] *Ibid*, 62-63.

[49] *Ibid*, 63.

[50] *Ibid*, 64.

[51] W. Harrop, & Matteson, A. *Cyber resilience: A review of critical national infrastructure and cybersecurity protection measures applied in the UK and USA*. (Journal of Business Continuity & Emergency Planning, 2014, 7(2)), 150.

[52] *Ibid*, 151.

[53] *Ibid*, 157.

Jungtinė Karalystė sukūrė tvirtas sistemas, tokias kaip Nacionalinės ypatingos svarbos infrastruktūros apsaugos centras (angl. Centre for the Protection of Critical National Infrastructure, CPNI), ir pradėjo įgyvendinti Kibernetinio dalijimosi informacija partnerystę (angl. Cyber Information Sharing Partnership, CISP), kuria siekiama skatinti vyriausybės ir verslo bendradarbiavimą realiu laiku.[54] Šios iniciatyvos atspindi bendrą supratimą, kad kibernetinių atakų grėsmė ypatingos svarbos infrastruktūrai - nuo energetikos tinklų iki transporto tinklų - reikalauja ne tik techninių apsaugos priemonių, bet ir nuolatinio koordinavimo ir dalijimosi informacija tarp sektorių.

Be to, abi šalys nuolat diskutuoja dėl privatumo ir etinės stebėsenos, kuri yra kibernetinio atsparumo dalis, poveikio. Pavyzdžiui, 2012 m. JAV Kibernetinio saugumo įstatyme buvo siūloma plačiai stebėti elektroninius duomenų perdavimus siekiant apsaugoti infrastruktūrą, tačiau galiausiai jis buvo atmestas dėl susirūpinimo privatumo teise.[55] Panašiai ir Jungtinės Karalystės iniciatyvos sukėlė visuomenės susirūpinimą dėl stebėjimo, ypač po informacijos nutekinimo apie PRISM programą.[56] Harropas ir Mattesonas teigia, kad tokios priemonės, nors ir prieštaringos, pabrėžia sudėtingą atsparumo, saugumo ir pilietinių laisvių pusiausvyrą nacionalinėje politikoje.

Apibendrindami Harropas ir Mattesonas pabrėžia kibernetinio atsparumo svarbą nacionalinei infrastruktūros apsaugai, ypač didėjant technologinei priklausomybei. Jų darbe pabrėžiama, kad kintantis kibernetinių grėsmių pobūdis reikalauja ne tik tvirtų saugumo sistemų, bet ir nuolatinio prisitaikymo ir bendradarbiavimo tarp viešojo ir privačiojo sektorių, kad būtų išlaikytas pagrindinių paslaugų atsparumas.

Kalbant apie atsparumo terminą, jo taikymas yra kur kas platesnis nei kibernetinės erdvės srityje; atsparumas apima daugybę sričių - nuo aplinkosaugos sistemų ir civilinės infrastruktūros iki socialinių ir ekonominių struktūrų. Bostick, Connelly, Lambert ir Linkov iliustruoja šią plačią atsparumo taikymo sritį civilinės infrastruktūros srityje, kur atsparumas politikoje ir investicijose prisitaiko prie įvairių ir dažnai nenuspėjamų grėsmių, pavyzdžiui, stichinių nelaimių ir sisteminės rizikos didelio masto infrastruktūros tinkluose.[57] Autoriai teigia, kad pastarojo meto atšiaurūs meteorologiniai reiškiniai, įskaitant 2017 m. uraganų sezoną Atlanto vandenyne, kurio nuostoliai siekė beveik 200 mlrd. dolerių, pabrėžia tradicinių metodų, orientuotų tik į **rizikos ir tikimybės mažinimą**, ribotumą ir reikalauja naujų atsparumu grindžiamų strategijų, kuriose pabrėžiamas atsigavimas ir gebėjimas prisitaikyti.[58]

---

[54] *Ibid*, 153.

[55] *Ibid*, 160.

[56] *Ibid*, 160.

[57] Thomas P. Bostick, Connelly, E. B., Lambert, J. H., & Linkov, I., *Resilience science, policy and investment for civil infrastructure*, (Reliability Engineering & System Safety 175, 2018), 19.

[58] *Ibid,* 3.

Civilinėje infrastruktūroje atsparumas apima ne tik išgyvenimą krizės metu, bet ir sistemos gebėjimą atsigauti ir vystytis. Autoriai apibrėžia esminį skirtumą tarp tradicinio rizikos/saugumo valdymo, kuris orientuotas į žinomų grėsmių kiekybinį įvertinimą (kiek ir kokių grėsmių yra, taip vertinant jų pavojingumą ir rimtumą) ir mažinimą, ir atsparumo mokslo, kuris pabrėžia sistemos gebėjimą atlaikyti, prisitaikyti ir atsigauti po įvairių ir nenumatytų sutrikimų.[59] Šis skirtumas atitinka naujas politikos kryptis, pavyzdžiui, JAV vykdomąjį įsakymą Nr. 13653, kuriame raginama projektuoti infrastruktūrą taip, kad būtų užtikrintas gebėjimas prisitaikyti ir greitai atsistatyti, pabrėžiant holistinių atsparumo strategijų poreikį šiuolaikinėse infrastruktūros sistemose.[60]

Autorių siūloma atsparumo sistema apima keturis, jau minėtus ir pristatytus ankstesnių autorių, etapus: ***pasirengimą, absorbciją, atsigavimą ir prisitaikymą***. Šis visapusis požiūris leidžia suinteresuotosioms šalims įvertinti infrastruktūros veikimą prieš (su)trikdančius įvykius, jų metu ir po jų ir padeda priimti sprendimus, kuriais suderinami neatidėliotini atstatymo poreikiai ir ilgalaikiai atsparumo tikslai[61]. Bostick ir kt. pabrėžia, kad atsparumas yra tiek fizinė, tiek socialinė ir techninė charakteristika, grindžiama sistemų lankstumu ir žinių, gautų iš ankstesnės patirties, integravimu, kad būtų galima informuoti apie būsimą atsaką, taip sukuriant grįžtamąjį ryšį, padedantį nuolat tobulėti.[62]

Apibendrindami Bostick ir kt. pasisako už didesnį atsparumo mokslo integravimą į nacionalinę ir regioninę infrastruktūros politiką. Neapsiribojant tik rizika ir grėsmėmis grindžiamais modeliais, atsparumo mokslas yra esminis pagrindas investicijoms, kuriomis išlaikomos svarbiausios funkcijos ir didinamas gebėjimas prisitaikyti, užtikrinant, kad sistemos būtų pasirengusios įvairiems ateities neapibrėžtumams.[63] Toks požiūris ne tik didina fizinį atsparumą, bet ir suderina infrastruktūros plėtrą su kintančiais visuomenės poreikiais ir vertybėmis.

2.3 Atsparumas VS grėsmių ir rizikos valdymas

Taigi, susipažinus su kibernetinio saugumo rizikos bei grėsmių valdymo ir atsparumo sąvokomis, galima gilintis į šių dviejų sąvokų skirtumus ir iššūkius, ypač siekiant geriau suprasti, kuri iš jų gali būti tinkamesnė, aktualesnė ir svarbesnė šių dienų besikeičiančioje skaitmeninėje aplinkoje.

Kibernetinių grėsmių valdymo srityje tradiciškai daugiausia dėmesio skiriama grėsmių prevencijai, aptikimui ir mažinimui, siekiant išlaikyti sistemų ir duomenų konfidencialumą, vientisumą ir prieinamumą. Pagrindinis jo tikslas - apsisaugoti nuo konkrečių grėsmių įgyvendinant

[59] *Ibid*, 4.

[60] *Ibid*, 6.

[61] *Ibid*, 12.

[62] *Ibid*, 14.

[63] Bostick, Thomas P., et al, 18.

apsaugos priemones, stebėjimo ir stebėsenos sistemas, kuriomis siekiama nustatyti kenkėjiškus subjektus/veikėjus ir kovoti su jais. Taikant šį metodą daug dėmesio skiriama grėsmių žvalgybai (pavyzdys - Lietuvos kritinės energetikos infrastruktūros ir finansų sektoriaus kibernetinių grėsmių analizė, Grėsmių nacionaliniam saugumui vertinimas), prieigos kontrolei ir tinklo saugumui, kad būtų sukurta apsauga aplink informacines sistemas ir užkertamas kelias įsilaužėliams prasiskverbti į gynybines sistemas[64]. Priešingai, **kibernetinis atsparumas** apima ne tik prevenciją, bet ir gebėjimą atlaikyti sutrikimus ir atsigauti po jų. Atsparumas sutelkiamas į veiklos tęstinumo (nepertraukimo) užtikrinimą net ir atakos metu, taip pat pabrėžiamas gebėjimas prisitaikyti ir atsigauti po įvykusio incidento. Kibernetiniame atsparume pripažįstama, kad ne visų grėsmių galima išvengti, todėl pirmenybė teikiama sistemų, galinčių absorbuoti sutrikdymus, atnaujinti esmines operacijas ir prisitaikyti prie kintančių grėsmių, kūrimui[65]. Šis požiūris atitinka realią situaciją, kad grėsmės veikėjai nuolat kuria naujus metodus žalos darymui, atakoms, todėl visiška prevencija tampa vis didesniu iššūkiu.

Siekiant įsivardinti kibernetiniam atsparumui būdingas charakteristikas, galima remtis anksčiau Rasos Bartkevičienės, Vitalio Nekrošiaus, Ingos Patkauskaitės-Tiuchtienės, Ramūno Vilpišausko pristatytomis bendromis atsparumo charakteristikomis.[66] Nors skirtingos atsparumo dimensijos pasižymi savitais kriterijais, yra universalių savybių, kurios būdingos visoms, įskaitant kibernetinio atsparumo kategorijoms. Tarp tokių savybių galima išskirti įvairovę – tai **įvairūs technologiniai sprendimai**, skirtingi veikėjai ir ištekliai, leidžiantys pasirinkti alternatyvius veikimo būdus kibernetinio incidento atveju. **Sampyna** užtikrina, kad tą pačią kibernetinę funkciją gali atlikti kelios sistemos ar technologijos, taip sumažinant priklausomybę nuo vieno infrastruktūrinio elemento ir didinant atsparumą. **Susietumas** skatina sklandų informacijos ir duomenų mainų procesą tarp skirtingų kibernetinių saugumo struktūrų, kas padeda greitai identifikuoti ir neutralizuoti grėsmes. Galiausiai, kibernetinio atsparumo stiprinimas neatsiejamas nuo **tarpsektorinio** bendradarbiavimo tarp viešojo ir privataus sektoriaus, akademinių institucijų ir tarptautinių partnerių, suteikiančio prieigą prie platesnių technologinių ir informacinių resursų, reikalingų greitam reagavimui ir sistemų atkūrimui po incidentų.

Tipas	Kuo pasireiškia / Tikslas	Sėkmės matavimas
Kibernetinių rizikų ir grėsmių valdymas	Bando Apsisaugoti nuo atakų - **prevencija, aptikimas, mažinimas**. Apsaugos priemonių	Kibernetinio saugumo sėkmė dažnai vertinama pagal tai, kaip

[64] Hausken, K. 7 .

[65] Kott, A., & Linkov, I. *To Improve Cyber Resilience, Measure It.,* 1-13.

[66] Bortkevičiūtė, Rasa, Vitalis Nakrošis, Inga Patkauskaitė-Tiuchtienė, and Ramūnas Vilpišauskas, 64.

	įgyvendinimas, stebėjimas, dėmesys sistemų "žvalgybai", prieigos kontrolė ir dėmesys tinklo saugumui, kad grėsmės aktorius neprasiskverbtų į gynybines sistemas. Kibernetinis grėsmių/ rizikos valdymas grindžiamas aktyviu/realiam laike esančių grėsmių valdymu, naudojant ir analizuojant realaus laiko informaciją ir duomenis, kad būtų galima iš anksto reaguoti į galimą riziką ir kylančią grėsmę. *Kibernetinis grėsmiu/rizikos valdymas*grindžiamas aptikimu ir intervencija.	gerai pavyksta sustabdyti arba sužlugdyti (išvengti) atakas;
Kibernetinis atsparumas	Neneigia, kad atakos įvyks. Teigia, kad reikia žiūrėti kaip greit atsistato sistemos ir kaip galima suamžinti jų poveikį bei žalą. Tvirtumas bei greitas atsistatymas eina kartu. Visa esmė yra **pasirengti, absorbuoti, atsigauti ir prisitaikyti** - sutelktas dėmesys į veiklos tęstinumo užtikrinimą, net ir atakų metu, bei prisitaikymą ir atsigavimą po incidento. atsparumo valdymas yra labiau strateginis ir orientuotas į sistemos patikimumą, dubliavimą (angl. redundancy) ir lankstumą, siekiant valdyti ir sušvelninti atakos padarinius. *Atsparumo* valdyme pirmenybė teikiama pasirengimui ir gebėjimui prisitaikyti	Atsparumas matuojamas pagal tai, kaip greitai ir veiksmingai organizacija gali atsigauti ir atnaujinti įprastą veiklą po incidento
skirtumas	Atsparumas apima ne tik prevenciją, bet ir gebėjimą atlaikyti sutrikimus ir atsigavimą po jų.	

Kibernetinių grėsmių ir rizikos valdymo srityje siekiama užkirsti kelią grėsmėms, o **kibernetinio atsparumo** srityje daroma prielaida, kad pažeidimai yra neišvengiami, todėl pabrėžiamas gebėjimas greitai ir veiksmingai atsigauti. Kibernetinių grėsmių ir rizikos valdymas grindžiamas aktyviu/realiam laike esančių grėsmių valdymu, naudojant ir analizuojant realaus laiko informaciją ir duomenis, kad būtų galima iš anksto reaguoti į galimą riziką ir kylančią grėsmę[67]. Priešingai, atsparumo valdymas yra labiau strateginis ir orientuotas į sistemos patikimumą, dubliavimą (angl. redundancy) ir lankstumą, siekiant valdyti ir sušvelninti atakos padarinius. Šis dėmesio skirtumas lemia ir skirtingus metodus: *kibernetinių grėsmių ir rizikos valdymas* grindžiamas aptikimu ir intervencija, o *atsparumo* valdyme pirmenybė teikiama pasirengimui ir gebėjimui prisitaikyti. Kibernetinių grėsmių ir rizikos valdymo sėkmė dažnai vertinama pagal tai, kaip gerai pavyksta sustabdyti arba sužlugdyti (išvengti) atakas; tačiau atsparumas matuojamas pagal tai, kaip greitai ir veiksmingai organizacija gali atsigauti ir atnaujinti įprastą veiklą po incidento[68].

Kiekviena iš šių strategijų yra susijusios su unikaliais iššūkiais. Kibernetinio ių grėsmių ir rizikos valdymo iššūkis - nuolat kintantis grėsmių pobūdis, todėl reikia nuolat atnaujinti ir budriai šalinti pažeidžiamumus ir stebėti galimą riziką. Kadangi grėsmės veikėjai tampa vis sudėtingesni, kibernetinis saugumas turi tobulėti tokiu pat tempu, reikalaudamas daug išlaidų ir išteklių[69]. Be to, stiprėjant stebėjimui/sekimui, kyla etinių problemų dėl privatumo ir pilietinių laisvių, ypač tada, kai vykdomas plataus masto duomenų rinkimas ir stebėjimas[70]. Suderinti šiuos etinius aspektus išlaikant patikimas saugumo priemones darosi vis sudėtingiau. Kita vertus, kibernetinis atsparumas turi savo ribotumų - jis susiduria su pasirengimo ir sąnaudų iššūkiais, nes prisitaikančioms ir patikimoms sistemoms kurti reikia didelių investicijų. Atsparumas reikalauja organizacinio įsipareigojimo sukurti atsarginius mechanizmus, perteklines sistemas ir reagavimo į krizes protokolus. Laikantis tokio požiūrio reikia reguliariai testuoti ir tobulinti reagavimo į incidentus strategijas, o tai gali apkrauti išteklius[71]. Be to, atsparumas gali susidurti su instituciniu pasipriešinimu, jei organizacijos pirmenybę teikia neatidėliotinam išlaidų taupymui, o ne ilgalaikėms investicijoms į atkūrimą ir gebėjimą prisitaikyti. Kita vertus, kalbant apie atsparumą, galima išvengti fokusavimosi į techninius jo aspektus, bet labiau socialiniai - komunikacija ir bendradarbiavimas. Kibernetinis atsparumas apima

[67] Dennis Broeders, Fabio Cristiano, and Daan Weggemans., *Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy,* (Studies in Conflict & Terrorism 46.12 (2023)), 2426.

[68] Bostick, Connelly, Lambert, and Linkov, 18.

[69] Harrop & Matteson, 19.

[70] Broeders et al., 2426.

[71] Kott, Linkov, *To Improve Cyber Resilience, Measure It*, 80.

ne tik sistemas ir kompiuterių tinklus, bet ir veikėjų - individų, organizacijų ar vyriausybių - elgseną, resursus ir pasirinkimus[72].

Atsižvelgiant į vis sudėtingesnes kibernetines grėsmes, kurios dažnai sukurtos taip, kad būtų galima apeiti prevencines priemones, kibernetinis atsparumas tampa itin svarbus užtikrinant, kad organizacijos galėtų tęsti veiklą net atakos metu ir po jos. Pripažinimas, kad grėsmių nebegalima visiškai išvengti, pabrėžia atsparumo, kaip pamatinės skaitmeninio saugumo strategijų dalies, poreikį. Kibernetinis atsparumas pabrėžia ne tik gebėjimą atlaikyti atakas, bet ir prisitaikyti reaguojant į besikeičiančias grėsmes, todėl jis ypač aktualus dinamiškoje grėsmių aplinkoje, kurioje visiška prevencija yra nepasiekiama[73]. Kaip ir minėta anksčiau - sparti interneto, jungiančio beveik pusę pasaulio gyventojų ir reikšmingai prisideda prie pasaulio ekonomikos augimo, plėtra sukūrė naujų tarptautinio (ne)saugumo aspektų. Prie interneto prijungtų įrenginių skaičiaus augimas ir ypatingos svarbos infrastruktūrų didėjanti priklausomybė nuo kibernetinės erdvės išryškina vis didesnį kibernetinių atakų pažeidžiamumą ir potencialią žalą. Tai akivaizdu remiantis 2022 metų Lietuvos Grėsmių Nacionaliniam Saugumui vertinimu bei 2023 metų Nacionalinės kibernetinio saugumo ataskaita, kuriose pateikiama statistika apie nuolat augantį kibernetinių atakų ir nusikaltimų skaičių. Šie duomenys rodo ne tik grėsmių augimą, bet ir didėjantį jų neišvengiamumo tikimybę, o tai dar kartą patvirtina kibernetinio atsparumo būtinybę.[74]

Apibendrinant galima teigti, kad nors kibernetinių grėsmių ir rizikos valdymas išlieka labai svarbus, kibernetinis atsparumas vis dažniau laikomas būtinu papildymu, suteikiančiu organizacijoms priemonių, padedančių atlaikyti incidentus ir atsigauti po jų. Šiandieninėje aplinkoje atsparumas gali būti praktiškiausias kelias siekiant apsisaugojimo nuo išorės grėsmių, kadangi juo pripažįstama iš išorės kylančių grėsmių ir pažeidimų neišvengiamybė ir daugiausia dėmesio skiriama atkūrimui ir tęstinumui, galiausiai užtikrinant, kad svarbiausios operacijos išliktų veikiančios nepaisant iššūkių.

[72] Hausken K., 7.

[73] Bostick et al., 2426.

[74] Krašto Apsaugos Ministerija, *Nacionalinė kibernetinio saugumo būklės ataskaita 2023*, 62.

2.4 Metodologija

Šiame tyrime, taikant atvejo tyrimo metodą ir struktūruotus ekspertų interviu, nagrinėjama Lietuvos kibernetinio saugumo aplinka ir vertinama, ar šalis pereina nuo rizikos valdymo modelio prie kibernetinio atsparumo modelio, kiek Lietuvoje atsispindi kibernetinio atsparumo konceptas.

Šio darbo aktualumas - dinamiškas kibernetinių grėsmių aplinkos pobūdis reikalauja nuolatinio prisitaikymo, ypač atsižvelgiant į spartų kibernetinių grėsmių augimą ir vis platesnį išmaniųjų technologijų ir daiktų interneto tinklų naudojimą. Technologijoms vis labiau skverbiantis į organizacinį, verslo ir individualų visuomenės lygmenį, atsparumu grindžiamo požiūrio - tokio, kuris pabrėžia gebėjimą ne tik užkirsti kelią grėsmėms, bet ir palaikyti veiklą atakų metu bei greitai atsigauti po jų - poreikis tampa itin svarbus. Atsižvelgiant į tai, Lietuvoje apskritai pirmenybė teikiama rizikos ir grėsmių valdymui, kaip rodo Kibernetinio saugumo įstatymas, Nacionalinio kibernetinio saugumo centro strategijos ir naujausios nacionalinės kibernetinio saugumo grėsmių ataskaitos. Tačiau šis požiūris gali būti ribotas, nes išorės grėsmių neįmanoma visiškai išvengti; nors prevencija išlieka labai svarbi, poveikio mažinimas pasitelkiant atsparumą gali užtikrinti tvaresnę gynybą.

Iki 2019 metų Lietuva sparčiai vijosi kitų pasaulio šalių pavyzdžius kibernetinio saugumo srityje. 2019 metais Lietuva pagal kibernetinio saugumo indeksą užėmė ketvirtą vietą pasaulyje. [75] Tačiau dinamiškas kibernetinės erdvės pobūdis verčia nuolat prisitaikyti prie naujų grėsmių ir apsisaugojimo priemonių, ypač sparčiai tobulėjant kibernetinėms grėsmėms bei plečiantis išmaniųjų technologijų ir IoT tinklui. Technologijoms įgaunant vis didesnę svarbą tiek organizaciniu, tiek verslo lygmeniu, jos taip pat vis labiau įsiskverbia į kasdienį žmonių gyvenimą.

Kadangi kibernetinė erdvė ir grėsmės joje greitai kinta, tradicinės tik grėsmių ir rizikų valdymų paremtos strategijos tampa nepakankamos. Vis dažniau dėmesys sutelkiamas ir į atsparumo valdymą – gebėjimą ne tik išvengti grėsmių, bet ir išlikti funkcionaliems po atakos, sparčiai atsigauti bei prisitaikyti prie naujų sąlygų. [76]

Lietuvos atveju, gilinantis tiek į Kibernetinio saugumo įstatymo nuostatomis, tiek Nacionalinio kibernetinio saugumo centro strategija ir komunikacija bei leidžiamomis „Nacionalinės kibernetinio saugumo grėsmių ataskaitomis“, šiame darbe daroma prielaida, kad pirmenybė vis dar teikiama grėsmių valdymui. Vis dėlto ši strategija yra ribota, nes išorinės grėsmės negali būti visiškai išvengiamos. Nors apsisaugojimas nuo išorės grėsmių yra ribotas, jų poveikį galima sumažinti.

---

[75] Skaitmeninės Etikos Centras, *Įdomu: Lietuva pasaulinio kibernetinio saugumo reitingo 10-tuke*, žiūrėta 2024m. Gruodžio 26d., https://e-etika.lt/idomu-lietuva-pasaulinio-kibernetinio-saugumo-reitingo-10-tuke/

[76] Kott & Linkov, *To Improve Cyber Resilience, Measure It,* 80-85.

Šio tyrimo metodologinė sistema grindžiama Bostick[77] ir Kott & Linkov[78] suformuluotais atsparumo mokslo modeliais, kuriuose atsparumas pristatomas kaip daugiapakopis procesas, reikalaujantis pereiti nuo tradicinio rizikos mažinimo prie adaptyvaus valdymo reaguojant į nenuspėjamus sutrikdymus. Taip pat į metdologinę sistemą įtrauktos ir Rasos Bortkevičienės, Vitalio Nekrošiaus, Ingos Patkauskaitės - Tiuchtienė, Ramūno Vilpišausko pasiūlytos atsparumo charakteristikos[79]. Tyrimo kriterijai, padėsiantys atskirti, ar organizacijos Lietuvoje taiko kibernetinio atsparumo ar kibernetinio saugumo ir rizikos valdymo strategijas, apims kelis svarbius aspektus, susijusius su keturiais atsparumui būdingais kriterijais, sujungiant anksčiau pristatytas atsparumui būdingas charakteristikas bei kriterijus - **pasirengti, absorbuoti, atsigauti ir prisitaikyt.** Minėtos visoms atsparumo kategorijoms būdingos charakteristikos **- įvairovė, sampyna, susietumas.** Kibernetiniam atsparumui tirti bus priskiriami šie kriterijai:

1. **Išteklių paskirstymas (įvairovė bei pasirengimas)** – ar organizacijos investuoja į atsarginių sistemų kūrimą, atkūrimo protokolus ir prisitaikymo strategijas, kurios užtikrina greitą atsigavimą po atakos ir veiklos tęstinumą. Apims išteklių paskirstymo ir kompetencijų vertinimą, siekiant įvertinti investicijų lygį ir technologinius įsipareigojimus, skirtus atsparumui skatinti, ir tai palyginti su rekomenduojama atsparumo praktika[80]. Vertinamas planavimas prieš įvykius ir galimų kibernetinių grėsmių valdymo protokolai.
2. **Tarpusavio ir tarptautinis bendradarbiavimas** (sampyna, absorbavimas)– ar įgyvendinamos iniciatyvos, skatinančios informacijos mainus tarp institucijų ir bendrą atsako priemonių koordinavimą, siekiant veiksmingai atsigauti po kibernetinių incidentų. Kibernetinių incidentų poveikį mažinančių ar atitolinančių mechanizmų vertinimas. Analizuojama, kaip greitai ir veiksmingai po incidento sistemos vėl pradeda veikti įprastai.
3. **Ilgalaikės strategijos (atsistatymas, atsigavimas ir prisitaikymas)** – ar organizacijos politikos dokumentuose skatinama atsparumo elementų integracija kaip esminė kibernetinio saugumo dalis, leidžianti prisitaikyti prie naujų sąlygų po atakos. Taip pat ar egzistuoja peržiūrėjimas sistemų ir protokolų patobulinimų, kad būtų pasirengta būsimiems įvykiams.

Kibernetinių grėsmių ir rizikos valdymui tirti bus priskiriami šie kriterijai:

1. **Technologinių priemonių naudojimas grėsmių identifikavimui ir neutralizavimui** – ar organizacijos didžiausią dėmesį skiria pažeidžiamumų šalinimui, atakų prevencijai ir sustabdymui.

[77] Bostick, Thomas P., et al, 19-23.

[78] Kott & Linkov, *To Improve Cyber Resilience, Measure It*, 80-85.

[79] Bortkevičiūtė, Rasa, Vitalis Nakrošis, Inga Patkauskaitė-Tiuchtienė, and Ramūnas Vilpišauskas, 64.

[80] *Ibid.*

2. **Išankstinės apsaugos strategijos** – ar strategijos orientuojamos į grėsmių prevenciją, užkertant kelią atakoms prieš joms įvykstant.
3. **Operatyvinis reagavimas** – ar prioritetas skiriamas greitam ir tiksliam atsakui į incidentą siekiant neutralizuoti grėsmę ir išvengti didesnės žalos.

Toks kriterijų išskyrimas leis sistemingai įvertinti, kurios organizacijos laikosi atsparumo principų ir investuoja į gebėjimą atsigauti bei prisitaikyti, o kurios remiasi tradicinėmis kibernetinio saugumo priemonėmis, orientuotomis į grėsmių valdymą ir rizikos mažinimą. Be to, bus vertinama, kaip organizacijos subalansuoja šių strategijų diegimą ir kaip jų požiūris koreliuoja su įstatymų bei politikos nuostatų reikalavimais. Šis tyrimas neapsiribos vien technologiniais sprendimais – bus atsižvelgiama ir į organizacines bei socialines priemones, kurios prisideda prie kibernetinio atsparumo stiprinimo. Tai apima darbuotojų mokymus, sąmoningumo didinimo programas ir koordinaciją tarp įvairių sektorių, siekiant užtikrinti holistinį atsaką į kibernetines grėsmes.

Atsižvelgiant į suformuluotas hipotezes ir pateiktą informaciją, pagrindiniai šio tyrimo klausimai yra šie: kokiu mastu organizacijos Lietuvoje teikia pirmenybę atsparumo strategijoms, palyginti su tradiciniais rizikos valdymo metodais, ir kaip tai atsispindi jų kibernetinio saugumo sistemose? Kokios konkrečios atsparumo priemonės, pavyzdžiui, dubliavimo mechanizmai, reagavimo į krizes protokolai ir tarpsektorinis bendradarbiavimas, buvo įdiegtos siekiant užtikrinti atsparumą, ir kokį poveikį jos daro organizacijų gebėjimui atlaikyti ir atsigauti po kibernetinių incidentų? Taip pat svarbu ištirti, kaip atsparumo praktikos skiriasi tarp skirtingų organizacijų tipų – privačių įmonių, viešojo sektoriaus institucijų ir universitetų – bei kokie iššūkiai ir kliūtys kyla organizacijoms pereinant nuo rizikos valdymo prie atsparumo orientuotų strategijų. Tyrimas taip pat nagrinės, kokią įtaką atsparumo praktikų diegimui daro nacionalinė politika, įskaitant Kibernetinio saugumo įstatymo ir Nacionalinės kibernetinio saugumo strategijos nuostatas, ir koks vaidmuo tenka tarp-organizaciniam bei tarpsektoriniam bendradarbiavimui stiprinant kibernetinį atsparumą Lietuvoje, lyginant tai su ES ir kaimyninių šalių, pavyzdžiui, Estijos, praktika.

Šis tyrimas nagrinėja kompleksinius iššūkius, su kuriais Lietuva susiduria pereidama nuo tradicinio rizikos valdymo prie atsparumą grindžiamo požiūrio į kibernetinį saugumą. Pagrindiniai iššūkiai apima viešojo ir privataus sektorių koordinavimo trūkumus, lėtą politikos priėmimo procesą bei struktūrines spragas atsakomybėje ir tarpžinybiniame bendradarbiavime. Šie veiksniai prisideda prie atotrūkio tarp strateginių tikslų ir realių rezultatų, trukdydami organizacijoms užtikrinti veiklos tęstinumą ir gebėjimą greitai atsigauti po kibernetinių išpuolių. Tyrimo tikslas – išsiaiškinti, kodėl kai kurios organizacijos sėkmingai susidoroja su kibernetinėmis grėsmėmis, o kitos patiria didelę žalą. Ieškant atsakymų, siekiama suprasti, kaip atsparumo praktikos, pasiruošimas ir gebėjimas greitai prisitaikyti prie nenuspėjamų išpuolių lemia organizacijų sėkmę. Norint spręsti šiuos iššūkius, būtina stiprinti sektorių koordinavimą, aiškinti atsakomybes ir integruoti visapusiškas atsparumo priemones,

kad būtų sumažintas išorinių grėsmių poveikis ir užtikrintas organizacijų ilgalaikis prisitaikymas prie kintančios grėsmių aplinkos.

Šiame tyrime numatyta taikyti atvejo analizę kartu su struktūruotais ekspertų interviu, siekiant ištirti organizacijų Lietuvoje kibernetinio atsparumo veiksmus ir tendencijas, bei įvertinti, ar organizacijos šalyje pereina nuo tradicinių rizikos/grėsmių valdymo metodų prie atsparumu grindžiamo požiūrio. Atvejų tyrimai bus atrenkami pagal įvairius kriterijus, tokius **ankstesnė kibernetinių atakų patirtis, organizacijos tipas (organizacijos, nepatyrusios atakų, bet tokio paties tipo kaip atakos, kurios buvo pažeistos atakų ar patyrė atakas).** Pagrindiniai atvejai apims tiek nukentėjusias organizacijas, kurioms teko spręsti kibernetinių išpuolių poveikį, tiek tas, kurios aktyviai įgyvendino atsparumo priemones ir išvengė rimtų padarinių.

Socialinė realybė nėra iki galo pažini. Tačiau, atsikleidžiant veikėjų patirtis ir požiūrį į tam tikrą įvykį, reiškinį ar procesą, įmanoma patikimai analizuoti jų socialinės realybės supratimą[81]. Siekiant to, šiame tyrime bus atliekami pusiau struktūruoti ekspertiniai interviu, leidžiantys tiriamus įvykius ir organizacijas suprasti ir tirti iš respondentų perspektyvos. Atsižvelgiant į tai, kad pats tyrimas yra skirtas teorijai testuoti, pasirinktas sisteminantis ekspertinių interviu tipas, sudarantis galimybių surinkti visapusišką ir struktūruotą ekspertinę informaciją[82]. Struktūrizuotų ekspertų interviu tikslas yra gauti įžvalgas iš atsakingų pareigūnų, kibernetinio saugumo specialistų ir valdžios atstovų, tiesiogiai dalyvaujančių strateginio atsako ir kibernetinių strategijų planavimo procesuose. Šių dalyvių atrankos kriterijai apima jų dalyvavimą kibernetinio atsparumo srityje, ir interviu metu jie pateiks tiek asmeninę patirtį, tiek platesnio masto iššūkius, su kuriais susiduriama Lietuvoje siekiant atsparumo.

Struktūrizuoti interviu buvo atliekami su valstybės tarnautojais, kibernetinio saugumo pareigūnais, organizacijų vadovais ir viešojo sektoriaus atstovais, dalyvaujančiais kibernetinio saugumo, atsako, grėsmių planavime ir reagavime į incidentus.

Atlikti šeši interviu su penkių institucijų atstovais, iš kurių trys yra organizacijų, patyrusių kibernetines atakas, ir trys iš institucijų, nepatyrusių kibernetinių atakų. Tokia sudėtis leidžia lyginti įžvalgas organizacijų, kurios tiesiogiai patyrė kibernetinio saugumo incidentus, ir organizacijų, kurios laikosi apsisaugojimo pozicijų, įžvalgas. Anot autorės, į problemą orientuotas interviu yra vertingas siekiant išsiaiškinti, kaip ekspertų asmeninės perspektyvos daro įtaką jų profesiniams veiksmams ir strategijoms[83]. Naudodamas pusiau struktūruoto interviu gaires, planuoju sukurti dialogo aplinką,

[81] Stefanie Döringer, *The problem-centred expert interview'. Combining qualitative interviewing approaches for investigating implicit expert knowledge*, (International journal of social research methodology 24.3, 2021), 265-278.

[82] Bortkevičiūtė, Rasa, Vitalis Nakrošis, Inga Patkauskaitė-Tiuchtienė, and Ramūnas Vilpišauskas, 70.

[83] Döringer, Stefanie, 269.

kurioje ekspertai galėtų pasidalyti savo aiškiomis žiniomis apie kibernetinės strategijos formavimo praktiką, kartu atskleisdami pagrindines prielaidas, numanomas strategijas ir gebėjimą prisitaikyti reaguojant į kibernetines grėsmes.

Šis metodas ypač tinka tyrimui, nes leidžia niuansuotai suprasti, kaip ir ar skirtingos institucijos Lietuvoje pereina nuo rizikos valdymu grindžiamo požiūrio prie atsparumu grindžiamo požiūrio. Pateikiant tikslinius klausimus ir pasikartojančias diskusijas, siekiu atskleisti, kaip organizacijos strategijos, ištekliai ir bendradarbiavimas prisideda prie kibernetinio atsparumo didinimo ar mažinimo. Tai leis visapusiškai pažvelgti į tai, kaip kibernetinis atsparumas konceptualizuojamas ir praktikuojamas įvairiose institucinėse aplinkose, ir potencialiai pasiūlyti pagrįstą teoriją apie strateginius organizacijų pasirinkimus didėjant kibernetinėms grėsmėms[84].

Interviu atlikti sudarytas standartinis temų sąrašas, kylantis iš tyrimo teorinio pagrindo. Temų sąrašas apima įvadinius klausimus, susijusius su reikšmingu įvykiu ar jo prevencija susijusius (jeigu įvykis įvyko - su įvykusiu įvykiu; Jeigu neįvyko - su prevencija) ir kaitos procesą atskleidžiančius, bei baigiamuosius klausimus. Interviu ir atvejų analizė lygins atsparumu grindžiamas strategijas su rizikos bei grėsmių valdymu, siekiant išanalizuoti kelias sritis. Bus nagrinėjami atkūrimo/sistemų atstatymo protokolai/strategijos ir prisitaikymo mechanizmai, lyginant juos su pažeidžiamumo šalinimu ir grėsmių mažinimu. Atsparumui būdingi įgyvendinimo iššūkiai, tokie kaip investicijos į dubliavimo (angl. back-up) sistemas, atkūrimo mechanizmus ir krizės valdymo protokolus, bus palyginami su tradicinių saugumo priemonių kaštų struktūra. Taip pat bus įtraukti etiniai klausimai, susiję su atsparumo ir kibernetinio saugumo praktikomis, įskaitant privatumo apsaugą bei galimas problemas dėl duomenų rinkimo ir stebėjimo. Atsparumo strategijos turi subalansuoti šiuos etinius aspektus, kartu išlaikant veiksmingas saugumo priemones.

2.5 Atvejai - organizacijos

Lietuvos požiūrį į kibernetinį atsparumą per pastaruosius penkerius metus lėmė keli kritiniai kibernetiniai incidentai, paveikę šalies ir organizacijų bei savivaldybių infrastruktūras. Šiame tyrime analizuojamos penkios organizacijos, tiesiogiai ar netiesiogiai susijusios su ar priklausančios taip pačiai industrijai, kad būtų galima susidaryti išsamesnį vaizdą apie tarp organizacijų Lietuvoje pasirinktas kibernetines strategijas bei kokios priežastis lemia tai, kad vienos organizacijos tapo pažeidžiamos atakų, o kitos ne.

2017 m. Vilniaus rajono savivaldybė susidūrė su didele kibernetine ataka, dėl kurios sutriko socialinių išmokų, įskaitant vaiko pinigus, mokėjimas. Šis incidentas išryškino savivaldybės kibernetinės gynybos pažeidžiamumą, todėl laikinai buvo sustabdytos svarbiausios paslaugos.

[84] *Ibid,* 271.

Nacionalinis kibernetinio saugumo centras (NKSC) intensyviai dirbo siekdamas atkurti paveiktas sistemas ir pirmenybę teikti pašalpų mokėjimo atnaujinimui. Pasak administracijos direktoriaus Vladislavo Kondratovičiaus, dauguma išmokų buvo greitai atkurtos ir pervestos daugiau kaip 20 000 gavėjų, o jų suma viršijo 2 mln. eurų.[85] Šis atvejis pabrėžia veiksmingų kibernetinio saugumo priemonių įgyvendinimo viešajame administravime sudėtingumą ir iššūkius. Dėl būtinybės glaudžiai bendradarbiauti viešajam ir privačiam sektoriams ir laipsniško kibernetinio saugumo politikos priėmimo sistemos dažnai lieka veikiamos sudėtingų grėsmių. Panašios problemos buvo pastebėtos ir 2017 m. „NotPetya“ atakos metu, kuri paveikė daugelį sektorių visame pasaulyje.

Vilniaus miesto savivaldybė taip pat įgyvendina reikšmingas kibernetinio saugumo priemones, siekdama stiprinti atsparumą prieš galimas kibernetines grėsmes. Skirtingai nuo Vilniaus rajono savivaldybės, kuri 2017 m. susidūrė su dideliais iššūkiais dėl kibernetinės atakos, sutrikdžiusios socialinių išmokų teikimą, Vilniaus miesto savivaldybė 2024 m. įgyvendina aktyvias prevencines ir atsparumo stiprinimo priemones, kad išvengtų tokių incidentų.

Viena iš pagrindinių Vilniaus miesto savivaldybės iniciatyvų yra bendradarbiavimas su NORD Cyber Security – šiam projektui skirta 2,9 mln. eurų, siekiant padidinti kibernetinės erdvės atsparumą ir užtikrinti saugumą nuo potencialių išpuolių[86]. Vilniaus miesto savivaldybė 2024 m. surengė viešą konkursą, skatinantį kibernetinio saugumo entuziastus ir ekspertus aktyviai prisidėti prie saugumo spragų identifikavimo, siūlydama atlygį iki 3 tūkst. eurų už kiekvieną rastą spragą savivaldybės sistemose[87].

Šios ir prevencinės priemonės rodo Vilniaus miesto savivaldybės atsakingą požiūrį į kibernetinio saugumo strategiją, pabrėžiant tiek rizikos valdymą, tiek atsparumo stiprinimą. Atsižvelgiant į tai, jog Vilniaus miestas nesusidūrė su reikšmingomis kibernetinėmis atakomis, ši savivaldybė tampa svarbiu pavyzdžiu, kaip nuoseklios investicijos į saugumą ir tarpsektorinis bendradarbiavimas gali prisidėti prie tvarios kibernetinės gynybos.

2023 m. gruodžio 8 d. Kauno technologijos universitetas (KTU) patyrė didelę kibernetinę ataką, kuri tapo reikšmingu saugumo incidentu ne tik universitetui, bet ir platesnei Lietuvos

---

[85] Made In Vilnius, *After the cyber attack, the Vilnius district municipality is already transferring the child's money*, Made In Vilnius, 2023m. Gruodžio 20, žiūrėta 2024 m. Birželio 21d,, https://madeinvilnius.lt/en/news/district/after-the-cyber-attack%2C-the-Vilnius-district-municipality-is-already-transferring-the-child%27s-money/

[86] ELTA, „NRD Cyber Security ir Vilniaus savivaldybė už 2,9 mln. eurų stiprins kibernetinės erdvės atsparumą*“,* LRT, žiūrėta 2023m. Lapkričio 12d., https://www.lrt.lt/naujienos/verslas/4/2102993/nrd-cyber-security-ir-vilniaus-savivaldybe-uz-2-9-mln-euru-stiprins-kibernetines-erdves-atsparuma

[87] Vilniaus Miesto Savivaldybe, „Išskirtinis dėmesys Vilniaus kibernetiniam saugumui: entuziastai kviečiami dalyvauti konkurse ir ieškoti spragų“, žiūrėta 2023m, Lapkričio 12d, https://vilnius.lt/lt/2024/10/11/isskirtinis-demesys-vilniaus-kibernetiniam-saugumui-entuziastai-kvieciami-dalyvauti-konkurse-ir-ieskoti-spragu/

kibernetinio saugumo bendruomenei[88]. Per šią ataką įsilaužėliai gavo prieigą prie KTU informacinių sistemų ir nutekino įvairius asmens duomenis, kurie vėliau pasirodė tamsiajame internete.[89] Nutekinti duomenys apėmė svarbią ir jautrią informaciją apie universitetą bei jo bendruomenės narius, o tai sukėlė susirūpinimą dėl duomenų apsaugos ir kibernetinių grėsmių valdymo Lietuvos švietimo įstaigose.

Po šio įvykio KTU skubiai ėmėsi veiksmų, siekdamas sumažinti atakos padarinius. Universitetas pradėjo sistemų atstatymą ir atnaujinimą, siekiant sustiprinti savo informacinių sistemų apsaugą ir sumažinti galimybes panašioms grėsmėms ateityje. Viešai buvo pranešta, kad dalis sistemų jau buvo atkurta, tačiau galutinis atsigavimas užtruko dėl būtinybės iš naujo įdiegti saugumo protokolus bei patikrinti sistemos komponentus.[90]

KTU incidentas atskleidė iššūkius, su kuriais susiduria švietimo institucijos kibernetinio saugumo srityje, ir parodė, kad grėsmių valdymas, grindžiamas vien tradicinėmis apsaugos priemonėmis, gali būti nepakankamas. Tokios organizacijos kaip KTU turi ne tik gerinti rizikos valdymo strategijas, bet ir stiprinti atsparumo strategijas, siekiant greičiau atsigauti po kibernetinių atakų bei užtikrinti, kad tokie incidentai nepadarytų esminės žalos jų veiklai.

Taip pat darbe tiriama Vilniaus universiteto (VU) kibernetinio saugumo strategijos bei pastangos. Skirtingai nei KTU, VU pastaruoju metu nesusidūrė su reikšmingais kibernetiniais incidentais, tačiau universitetas aktyviai stiprina ir kreipia daug dėmesio savo kibernetinę apsaugą. To pavyzdys įdiegdamas dviejų veiksnių autentifikavimo (2FA/MFA) sistemą[91]. Šis žingsnis yra svarbus rizikos valdymo srityje, nes 2FA technologija suteikia aukštesnį vartotojų tapatybės patvirtinimo lygį, taip efektyviai sumažinant galimų įsilaužimų riziką ir padedant užtikrinti sistemų saugumą.

VU taip pat dalyvauja kibernetinio saugumo ir kibernetinės žvalgybos ekspertų rengimo projekte kartu su kitais Europos universitetais, pabrėžiančiu kibernetinio saugumo svarbą aukštojo

---

[88] KTU, „Dėl asmens duomenų nutekėjimo per gruodžio 8 d. įvykdytą kibernetinę ataką prieš KTU*“,* žiūrėta 2023m., Lapkričio 11d., https://ktu.edu/news/del-asmens-duomenu-nutekejimo-per-gruodzio-8-d-ivykdyta-kibernetine-ataka-pries-ktu

[89] LRT, BNS, „Per kibernetinę ataką nutekinti KTU duomenys pardavinėjami tamsiajame internete“, LRT, žiūrėta 2024m. Lapkričio 11d,, https://www.lrt.lt/naujienos/mokslas-ir-it/11/2153835/per-kibernetine-ataka-nutekinti-ktu-duomenys-pardavinejami-tamsiajame-internete

[90] KTU, *Dėl asmens duomenų nutekėjimo per gruodžio 8 d. įvykdytą kibernetinę ataką prieš KTU*, žiūrėta 2024m. Lapkričio 11d.

[91] Vilniaus Universitetas, „INSTRUKCIJA tekstu - „Microsoft Authenticator“ diegimas ir konfigūravimas”, žiūrėta 2024m. Lapkričio 11d., https://santaka.vu.lt/pages/viewpage.action?pageId=181829791

mokslo srityje[92]. Ši iniciatyva apima mokslinę ir praktinę parengtį kibernetiniams incidentams, stiprinant ne tik universiteto, bet ir platesnės akademinės bendruomenės apsaugos gebėjimus.

Tyrime bus lyginama VU ir KTU kibernetinio saugumo praktika, analizuojant, kaip vienas universitetas reagavo į kibernetinę ataką ir kokius veiksmus atliko po jos, o kitas – kaip aktyviai stiprina prevencines priemones be būtinybės reaguoti į rimtą incidentą. Šis lyginimas leis suprasti, **kokie konkretūs veiksniai gali būti esminiai siekiant užtikrinti kibernetinį atsparumą Lietuvos universitetuose, ir ar egzistuoja aiškus skirtumas tarp strategijų, orientuotų į prevenciją, ir strategijų, orientuotų į atkūrimą bei prisitaikymą po incidentų.**

Šiame tyrime taip pat nagrinėjama viena didžiausių Lietuvos energetikos grupių „Ignitis“, kuri pastaraisiais metais susidūrė su reikšmingomis kibernetinėmis grėsmėmis. „Ignitis“ patyrė du reikšmingus kibernetinius incidentus: pirmąjį 2022 m., o antrąjį, palyginti nedidelį, 2024 m. 2024 m. ataka, priskiriama prokremliškai grupuotei, pažeidė „Ignitis“ sistemas, tačiau buvo greitai suvaldyta, o tai rodo bendrovės taikomas atsparumo užtikrinimo priemones. Pasak generalinio direktoriaus Dariaus Maikštėno, užpuolikai gavo tik laikiną prieigą prie trečiosios šalies suteiktos išorinės debesijos sistemos, nukopijavo kai kuriuos duomenis ir trumpam sutrikdė jų įkrovimo stotelių veiklą. Pažymėtina tai, kad šis sutrikimas buvo labai trumpas; „Ignitis“ sakėsi esą įsidegę daugybę apsaugos priemonių. Sutrikimai truko nuo kelių minučių iki poros valandų, kaip teigė D. Maikštėnas[93]. Toks reagavimas rodo, kad „Ignitis“ daug dėmesio skiria greitam sistemų atkūrimui, siekiant kuo labiau sumažinti poveikį operacijoms, o tai rodo tvirtą įsipareigojimą užtikrinti atsparumą

Priešingai, pirmasis 2022 m. įvykdytas išpuolis prieš „Ignitį“, kuriam vadovavo su Rusija susijusi grupuotė „Killnet“, pasirodė esąs didžiulis iššūkis, išryškinęs atsparumo spragas. Šis kibernetinis incidentas, apibūdinamas kaip rimčiausias išpuolis prieš „Ignitis“ per daugiau nei dešimtmetį, pakirto bendrovės gynybinius pajėgumus masine paskirstyto atsisakymo aptarnauti (DDoS) ataka.[94] Nepaisant „Ignitis“ kibernetinio saugumo priemonių, atakos mastas ir intensyvumas sukėlė didelių veiklos sutrikdymų. Šis įvykis išryškino organizacijos pažeidžiamumą, kadangi dėl

[92] Vilniaus Universitetas, „VU ir dar trys Europos universitetai rengs kibernetinio saugumo ir kibernetinės žvalgybos ekspertus“, žiūrėta 2024m. Lapkričio 11d., https://naujienos.vu.lt/vu-ir-dar-trys-europos-universitetai-rengs-kibernetinio-saugumo-ir-kibernetines-zvalgybos-ekspertus/

[93] Rasa Lukaitytė-Vnarauskienė, „Maikštėnas – apie jau išsiaiškintą kibernetinę ataką: veikė prokremlinė grupuotė“, Delfi, žiūrėta 2024m. Lapkričio 11d. https://www.delfi.lt/verslas/energetika/maikstenas-apie-jau-issiaiskinta-kibernetine-ataka-veike-prokremline-grupuote-95875633

[94] Karolina Konopko, „Į Ignitis grupę“ nusitaikė „Killnet“ programišiai: didžiausią ataką per dešimtmetį pavyko suvaldyti“, 15min, žiūrėta 2024m. Lapkričio 11d., https://www.15min.lt/naujiena/aktualu/lietuva/killnet-atakuoja-ignitis-grupe-tai-didziausia-ataka-per-desimtmeti-56-1900188

atakos intensyvumo „Ignitis“ sunkiai galėjo išlaikyti paslaugų tęstinumą be didelių nutraukimų.[95] 2022 m. incidentas pabrėžė pažangesnių atsparumo strategijų poreikį, kad ateityje būtų galima veiksmingai atremti tokias didelio poveikio grėsmes.

Atlikdama tyrimą, analizuosiu pagrindinius šaltinius, tokius kaip kibernetinio saugumo įstatymas ir jo pakeitimai, bei organizacijų bendradarbiavimą su NKSC ir viešojo sektoriaus institucijomis. Atsakymų tikslas – suprasti, kaip organizacijos vertina įstatymo pokyčius ir kokia jų praktika bendradarbiaujant su NKSC, kad būtų galima analizuoti, kaip šie pokyčiai veikia kibernetinio saugumo atsparumą ir prisitaikymą prie teisės aktų reikalavimų. Analizuosiu ir kibernetinio saugumo teisės aktų poveikį atsparumui, ypač skirtumą tarp viešojo ir privataus sektoriaus pranešimų apie kibernetinius incidentus. Šis skirtumas atskleidžia bendradarbiavimo ir komunikacijos spragas, galinčias neigiamai paveikti nacionalinį atsparumą. Be to, nagrinėsiu neseniai atliktus Kibernetinio saugumo įstatymo pakeitimus, kurie stiprina nacionalinę kibernetinio saugumo sistemą ir skatina sektorių bendradarbiavimą. Bus siekiama išsiaiškinti, kaip šie pokyčiai veikia atsparumo priemones ir organizacijų prisitaikymą. Įžvalgos apie NKSC ir įstatymą padės suprasti, kaip pokyčiai veikia kibernetinio saugumo praktiką Lietuvoje ir kokie žingsniai gali padidinti atsparumą bei skatinti geresnį bendradarbiavimą tarp viešojo ir privataus sektorių.

[95] *Ibid.*

3. Atsparumas nacionalinėje kibernetinio saugumo struktūroje - Kibernetinio saugumo įstatymas ir jo pakeitimai

Lietuvos Respublikos kibernetinio saugumo įstatymas buvo priimtas 2014 m. gruodžio 11 d. ir įsigaliojo 2015 m. sausio 1 d. Nuo to laiko įstatymas buvo keičiamas, siekiant atsižvelgti į besikeičiančią kibernetinio saugumo situaciją ir Europos Sąjungos teisės aktų reikalavimus. Pavyzdžiui, 2024 m. spalio 18 d. įsigaliojo atnaujinta įstatymo redakcija, perkelta Europos Parlamento ir Tarybos direktyva (TIS 2), siekiant suvienodinti kibernetinio saugumo lygį visoje Europos Sąjungoje.[96]

2014 m. gruodžio 11 d. priimtu Lietuvos Respublikos kibernetinio saugumo įstatymu siekiama apibrėžti nacionalinius kibernetinio saugumo reikalavimus ir atsakomybę viešiesiems ir privatiems subjektams, sutelkiant dėmesį į ypatingos svarbos informacinės infrastruktūros apsaugą ir saugios kibernetinės aplinkos užtikrinimą Lietuvoje.

Šis įstatymas pirmiausia atspindi rizikos valdymo požiūrį, daugiausia dėmesio skiriant kibernetinio saugumo incidentų prevencijos, aptikimo ir reagavimo į juos priemonėms. Jo elementai, tokie kaip saugumo protokolų nustatymas, atitikties užtikrinimas visuose sektoriuose ir reikalavimas pranešti apie incidentus, atitinka rizikos valdymo principus: jais siekiama sumažinti žinomas grėsmes ir pažeidžiamumą užtikrinant apsaugos priemones ir kontrolę.

Tačiau šiame įstatyme taip pat pastebimi atsparumo valdymo aspektai. Pavyzdžiui, įstatyme taip pat pabrėžiama, kad kibernetinis saugumas - tai visumą teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti (2 strp. 5d). Būtent aptikti ir analizuoti, reaguoti į incidentus, veiklai, įvykus incidentams, atkurti, galima priskirti prie anksčiau minėtų kibernetiniam atsparumui priskiriamų savybių - pasirengti, absorbuoti, atsigauti ir prisitaikyt. Jame taip pat pabrėžiamas ypatingos svarbos paslaugų nepertraukiamumas, visų pirma reikalaujant, kad viešieji ir privatūs ypatingos svarbos informacinių technologijų operatoriai turėtų procedūras, kaip išlaikyti pagrindines paslaugas incidentų metu ir po jų. Būtent šiose dalyse atsispindi, kad įstatymu netiesiogiai skatinamas atsparumas, nes jame reikalaujama pasirengti trikdžiams bei atsispindi pagrindiniai kibernetiniam atsparumui būdingi elementai. Tokiu būdu Lietuvos įstatymas remia pirminius žingsnius atsparumo link, stiprindamas sistemos tęstinumą ir prisitaikymą, tačiau

[96] Lietuvos Respublikos Krašto Apsaugos Ministerija, *Įsigalioja atnaujintas Kibernetinio saugumo įstatymas: pagrindiniai pokyčiai ir įgyvendinimo etapai*, 2024-10-18, Žiūrėta 2024m. Gruodžio 13d., https://kam.lt/isigalioja-atnaujintas-kibernetinio-saugumo-istatymas-pagrindiniai-pokyciai-ir-igyvendinimo-etapai/?utm_source=chatgpt.com> ,

jame iš esmės pabrėžiamas prevencinis rizika grindžiamas požiūris, o ne holistinė atsparumo sistema, kuri apima atstatymą ir adaptaciją kaip pagrindinius komponentus.

Lietuvos kibernetinio saugumo įstatyme, pirmiausia nustatoma nacionalinės kibernetinio saugumo sistemos organizavimo, valdymo ir kontrolės sistema. Nors įstatyme aptariami pagrindiniai kibernetinio saugumo principai ir pateikiamos incidentų prevencijos, aptikimo ir reagavimo į juos gairės, jame daug dėmesio skiriama kibernetinės rizikos valdymui, o ne išsamioms kibernetinio atsparumo strategijoms. Įstatyme akcentuojamos rizikos vengimo ir mažinimo priemonės, pavyzdžiui, nustatomi techniniai ir organizaciniai reikalavimai ypatingos svarbos informacinei infrastruktūrai ir viešiesiems tinklams (5 straipsnio 3 dalis, 13, 14 straipsniai). Tai iš esmės yra rizikos valdymo praktika, orientuota į pažeidžiamumo mažinimą ir incidentų prevenciją. Prievolės pranešti apie kibernetinio saugumo incidentus (13, 14, 15 str.) ir incidentų valdymo planų rengimas sustiprina tradicinėms rizikos valdymo sistemoms būdingą reaktyvų požiūrį į grėsmių valdymą.

Įstatymo nuostatos liečia atkūrimo ir tęstinumo priemones, už kurias ypač atsakingas Nacionalinis kibernetinio saugumo centras (NKSC). Pavyzdžiui, centrui pavesta sukurti nacionalinius ir konkrečių sektorių incidentų valdymo planus ir stebėti, kaip jų laikomasi (6, 10 str.). Tačiau tai daugiau operatyvinės ir procedūrinės, o ne strateginės atsparumo didinimo iniciatyvos. Į atsparumą orientuotos priemonės, pavyzdžiui, tos, kuriomis pabrėžiamas prisitaikymo pajėgumas, sistemų dubliavimas, ilgalaikis atsigavimas ir prisitaikymas, nėra aiškiai nurodytos.

Įstatyme nustatyti tarpžinybinio bendradarbiavimo ir keitimosi informacija mechanizmai (17, 18 straipsniai), kurie yra atsparumo stiprinimo pagrindas. Viešojo ir privačiojo sektorių partnerystės įtraukimas ir NKSC vaidmuo skatinant bendrus projektus (10 str. 9 d.) yra teigiami pokyčio link labiau integruotos kibernetinio saugumo ekosistemos rodikliai. Vis dėlto šios pastangos nėra pakankamai išplėtotos ir jose daugiau dėmesio skiriama skubiam reagavimui į incidentus, o ne gebėjimo prisitaikyti ir atsparumo skatinimui.

Naujausi pakeitimai ir patikslinimai:

Įstatymo atnaujinimai, ypač nacionalinių kibernetinio saugumo incidentų valdymo planų integravimas (5 straipsnio 4 dalis, 6 straipsnio 2 dalis), rodo pažangą siekiant atsparumo, nes pabrėžiamas pasirengimas ir sisteminis valdymas. Tačiau šiuose atnaujinimuose vis dar teikiama pirmenybė reikalavimų laikymuisi ir reagavimui, o ne atsparumo praktikos naujovėms.

Įstatyme aiškiai neaptariamas išteklių pasiskirstymas, tarpusavio ryšiai, tarpsektorinis bendradarbiavimas ar išteklių įvairovė ir kompetencijų vertinimas, siekiant įvertinti investicijų lygį ir technologinius įsipareigojimus - pagrindiniai atsparumo elementai pagal šiuolaikines atsparumo mokslo sistemas[97]. - pagrindiniai atsparumo elementai pagal šiuolaikines atsparumo mokslo

[97] Kott & Linkov, *To Improve Cyber Resilience, Measure It*, 80-85.

sistemas[98]. Nors tam tikri aspektai, pavyzdžiui, NKSC vaidmuo valdant ilgalaikius planus ir vykdant modeliavimą (10 straipsnio 7 dalis), yra užuomina apie atsparumą, jie nėra visiškai operacionalizuoti teisiniame tekste.[99]

Nors į Lietuvos kibernetinio saugumo įstatymą įtraukta visapusiška rizikos valdymo sistema, jo dvasia iš esmės tebėra įtvirtinta prevencijos ir poveikio mažinimo srityje. Pastangos didinti atsparumą, ypač pasitelkiant koordinavimą ir planavimą, yra akivaizdžios, tačiau nepakankamai išplėtotos. Reikia tolesnių teisinių korekcijų, kad būtų aiškiai skatinamas sisteminis atsparumas - pabrėžiant pasirengimą, atkūrimą ir gebėjimą prisitaikyti - siekiant užtikrinti tvirtesnę apsaugą nuo kintančių kibernetinių grėsmių.

Šių metų Spalio 18d. įsigaliojo atnaujinta Kibernetinio saugumo įstatymo versija, sustiprinanti kibernetinio saugumo valdysenos modelį Lietuvoje. Įstatymas numatė investicijų į kibernetinį saugumą didinimą ir kibernetinio saugumo ekosistemos sutvirtinimą, siekiant užtikrinti būtent tai, kad Lietuva taptų atsparesnė kibernetinėse grėsmėse. Naujuoju įstatymu į nacionalinę teisę yra perkeliama Europos Sąjungos priimta Tinklų ir informacinių sistemų direktyva (TIS 2), kuri numato, kad didėjant kibernetinėms grėsmėms organizacijos turi būti pasiruošusios užtikrinti savo tinklų ir sistemų saugumą, nes incidentai gali turėti rimtų pasekmių jų veiklai ir visuomenei. Kibernetinio saugumo įstatymas bus taikomas skirtinguose sektoriuose veikiančioms įmonėms, viešojo sektoriaus institucijoms ir fiziniams asmenims, o pokyčiai palies ir kiekvieną Lietuvos gyventoją. Ruošiant naująjį įstatymą, Krašto apsaugos ministerija ne tik siekė įgyvendinti TIS 2 direktyvą, bet ir atliepti privataus verslo atstovų, asociacijų, akademikų saugumo poreikį ir lūkesčius naujam teisiniam reguliavimui. Interviu su Krašto Apsaugos KSITPG atstove Inga Sūnelaitiene, buvo užsiminta, kad "Ruošiant naująjį įstatymą, Krašto apsaugos ministerija ne tik siekė įgyvendinti TIS 2 direktyvą, bet ir atliepti privataus verslo atstovų, asociacijų, akademikų saugumo poreikį ir lūkesčius naujam teisiniam reguliavimui".[100]

Pagal atnaujintą Kibernetinio saugumo įstatymą, organizacijos turėtų imtis kelių svarbių veiksmų. Pirmiausia, būtina įsivertinti, ar jų veikla patenka į įstatymo reguliavimo sritį, ypač jei organizacija veikia sektoriuose, kurie yra esminiai ES socialinei ir ekonominei gerovei. Didesnį dėmesį turi atkreipti vidutinės ir didelės įmonės, o mažos bei labai mažos įmonės bus reguliuojamos

[98] Bostick, Thomas P., et al, 19-23.

[99] Lietuvos Respublikos Seimas*, Lietuvos Respublikos Kibernetinio Saugumo įstatymas, 2014m. Gruodžio 11d.,* žiūrėta 2024m. Gruodžio 13d., https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/f6958c2085dd11e495dc9901227533ee

[100] Lietuvos Respublikos Krašto apsaugos ministerija, „Lietuva stiprina dar vieną gynybos liniją: kaip pasiruošti netrukus įsigaliosiančiam Kibernetinio saugumo įstatymui?", 2024-09-19, žiūrėta 2024m. Gruodžio 13d., https://kam.lt/lietuva-stiprina-dar-viena-gynybos-linija-kaip-pasiruosti-netrukus-isigaliosianciam-kibernetinio-saugumo-istatymui/

tik išimtiniais atvejais, jei jų veiklos sutrikimai galėtų reikšmingai paveikti visuomenės saugumą ar sveikatą.[101]

Kitas žingsnis – pradėti ruoštis atitikti kibernetinio saugumo reikalavimus dar prieš įsigaliojant priežiūrai, kuri bus pradėta tik po 12 mėnesių nuo organizacijos įtraukimo į Kibernetinio saugumo subjektų registrą. Ankstyvas pasiruošimas ne tik sumažins išlaidas, bet ir suteiks galimybę samdyti aukštos kvalifikacijos specialistus bei diegti efektyvesnes priemones.[102]

Organizacijos taip pat turėtų suburti komandą, atsakingą už informacijos saugos valdymo sistemos diegimą. Ši komanda turėtų apimti informacijos saugumo pareigūną (CISO), kibernetinių incidentų specialistą, teisininką ar atitikties pareigūną, mokymų koordinatorių ir kitus specialistus. Vadovas privalės paskirti atsakingą asmenį už kibernetinio saugumo reikalavimų įgyvendinimą.[103]

Galiausiai, svarbu ugdyti kibernetinio saugumo kultūrą organizacijoje. Visi darbuotojai, įskaitant vadovus, turės dalyvauti kibernetinio saugumo mokymuose, kurie yra privalomi bent kartą per dvejus metus. Be to, organizacijos turės užtikrinti tiekimo grandinės saugumą, nustatydamos saugumo reikalavimus tiekėjams ir rangovams. Šie žingsniai padės užtikrinti, kad organizacija atitiktų Kibernetinio saugumo įstatymo reikalavimus ir būtų pasiruošusi veiksmingai reaguoti į kibernetinius iššūkius.[104]

3.1 Organizacinė praktika: Atsparumas praktikoje bei jo iššūkiai

Kalbant apie kibernetinio atsparumo konceptą Lietuvoje, svarbu ne tik išsiaiškinti, kaip kibernetinis atsparumas atsispindi įstatymuose, pirminiuose šaltiniuose ir teisėkūros praktikoje, bet ir suprasti, kiek jis yra taikomas Lietuvos organizacijų veikloje bei organizacinėje praktikoje. Siekiant šio supratimo, buvo pagal anksčiau aptartus atvejus pasirinktos ir apklaustos Lietuvos organizacijos bei jose dirbantys kibernetinio saugumo ekspertai.

Interviu su kibernetinio saugumo ekspertais atskleidė įdomių įžvalgų apie kibernetinio atsparumo konceptą ir teoriją Lietuvoje bei tarp Lietuvos organizacijų. Viena iš beveik visuose interviu paminėtų bendrų temų buvo pripažinimas, kad abi kibernetinio saugumo dalys – prevencija ir atsparumas – yra svarbios. Vis dėlto buvo pastebėta, kad prevencija vis dar dominuoja tarp Lietuvos organizacijų, o tai išryškina vieną iš pagrindinių iššūkių ir silpnųjų vietų kibernetinio saugumo srityje.

---

[101] Lietuvos Respublikos Krašto Apsaugos Ministerija, *Įsigalioja atnaujintas Kibernetinio saugumo įstatymas: pagrindiniai pokyčiai ir įgyvendinimo etapai*, Žiūrėta 2024m. Gruodžio 13d.

[102] *Ibid,* Žiūrėta 2024m. Gruodžio 13d.

[103] *Ibid*, Žiūrėta 2024m. Gruodžio 13d.

[104] *Ibid,* Žiūrėta 2024m. Gruodžio 13d.

Šarūnas Končius, Kauno technologijos universiteto duomenų registro kibernetinio saugumo vadovas, kalbėdamas apie kibernetinio atsparumo principus, akcentavo svarbą paskirstyti organizacijos išteklius į tris pagrindines dalis: prevenciją, detekciją ir reagavimą. Tai, kaip jis apibūdino, gerai atspindi atsparumo kriterijų, tokių kaip pasirengimas, absorbcija, atsigavimas ir prisitaikymas, struktūrą. Kaip ir šiame darbe išskirti atsparumo aspektai, taip ir respondentas teigė, kad organizacijos turi rasti tinkamą balansą tarp šių trijų funkcijų, kad užtikrintų tvarų ir greitą atsaką į kibernetinius incidentus. Pasak jo, organizacijos neturėtų manyti, kad apsaugoti save nuo visų galimų grėsmių yra įmanoma, todėl turėtų būti pasirengusios greitai reaguoti ir atkurti veiklą, kai įsilaužimas vis tiek įvyksta. Tai puikiai atitinka šio darbo požiūrį į atsparumo išteklių paskirstymą, ypač į tai, kaip organizacijos investuoja į atsargines sistemas, atkūrimo protokolus ir prisitaikymo strategijas, kad užtikrintų veiklos tęstinumą po atakos.[105]

Interviu metu Š. Končius aptarė, kaip jų organizacijoje suprantamas ir įgyvendinamas kibernetinis atsparumas. Jis pabrėžė, kad KTU požiūris į kibernetinį atsparumą yra subalansuotas tarp rizikos valdymo, prevencijos ir reagavimo. Pasak jo, organizacija turėtų savo resursus paskirstyti į tris dalis**: siekti, kad neįvyktų įsilaužimas, pastebėti įsilaužimą ir būti pasiruošusi reaguoti**. Organizacija vadovaujasi ISO 27001 standartu, kuris skiria išteklius kibernetiniam saugumui į tris pagrindines sritis: užkirsti kelią įsilaužimams, aptikti juos ir efektyviai reaguoti į jau įvykusius pažeidimus. Jis pabrėžė, kad organizacijos neturėtų remtis tik prevencija, bet taip pat turi būti pasirengusios pastebėti ir reaguoti į įsilaužimus: „negali apsisaugoti, tas įsilaužimas vis tiek įvyks, todėl reikia pagalvoti, kaip pastebėti ir reaguoti“[106]. Toks požiūris rodo, kad organizacija turi ne tik siekti išvengti atakų, bet ir būti pasirengusi jas efektyviai valdyti ir minimalizuoti žalą. Tai ypač svarbu dirbant su moderniomis sistemomis, paremtomis „Zero Trust“ principu, kuris, pasak respondento, „leidžia užtikrinti saugumą net tada, kai ataka įvyksta“[107]. Organizacijos neturėtų remtis tik prevencija, bet taip pat turi būti pasirengusios pastebėti ir reaguoti į įsilaužimus. Būtent minėtas “Zero Trust“ modelis, kuris veikia pagal prielaidą, kad įsilaužimas yra neišvengiamas, todėl kiekvienas prisijungimas turi būti laikomas nepatikimu. Šis požiūris puikiai atitinka mano analizuojamus kibernetinio atsparumo komponentus – **pasirengimas, absorbcija, atsigavimas ir prisitaikymas**. KTU duomenų registro strategija, kai pasirengimas atakoms, sistemų tobulinimas, atsarginių sistemų kūrimas ir prisitaikymas nuolatiniam pokyčiui, aiškiai iliustruoja visapusišką kibernetinio atsparumo modelį.[108]

[105] Šarūnas Končius (KTU Domreg), virtualus interviu, 2024m. Gruodžio 12d.

[106] *Ibid.*

[107] *Ibid.*

[108] *Ibid.*

Taip pat, kaip pabrėžė Š.Končius, svarbu įvertinti ilgalaikes strategijas, kurios užtikrina organizacijos atsparumą ir gebėjimą prisitaikyti. Tai labai susiję su atsparumo aspektu, kad organizacijos nuolatos turi peržiūrėti savo sistemas ir atnaujinti protokolus, kad būtų pasiruošusios ateities iššūkiams. Šis požiūris atitinka šio darbo ilgalaikės strategijos kriterijus, kur organizacijos politikos dokumentuose turi būti skatinama integruoti atsparumo elementus kaip esminę kibernetinio saugumo dalį, taip pat peržiūrėti sistemas ir protokolus, kad būtų pasiruošusios būsimiems įvykiams. Šie aspektai – prevencija, detekcija, reagavimas ir ilgalaikės strategijos – puikiai atspindi esminius kriterijus, kuriuos naudojant kibernetinio atsparumo tyrimams galima analizuoti organizacijos pasirengimą ir jos gebėjimą susidoroti su kibernetiniais incidentais.[109]

Igničio grupės vyriausiasis informacijos saugumo pareigūnas (angl. Chief Information Security Officer), Donatas Vitkus, pabrėžė, kad sunku išskirti, ką reikėtų labiau prioterizuoti, kadangi, jų strategija orientuota į abu - ir į prevenciją, grėsmių aptikimą, užkardymą, ir į atsparumą, t.y. veiklos tęstinumą, užkardymą, atstatymą, ataką į ataką. Prioriteto kažkuriam vienam nėra. Tačiau jis taip pat pažymėjo, kad šimtu procentu saugių sistemų nėra - “Incidentas vis tiek įvyks. Klausimas yra tame, kaip greit sureaguosi, kaip sukoordinuosi darbus viduje, kaip iškomunikuosi, kaip atsistatysi iš po incidento”[110]. Donatas Vitkus pabrėžė, kad „Ignitis“ organizacijoje strateginis požiūris į kibernetinį saugumą visada apėmė visą ciklą – nuo prevencijos ir aptikimo iki korekcinių veiksmų ir sistemų atsistatymo. „Visa strategija visada primenu nuo A iki Z: nuo aptikimo, prevencijos iki atsistatymo,“ – sakė Vitkus. Tokia holistinė strategija yra būtina užtikrinti ilgalaikį organizacijos atsparumą, nes ji apima visus svarbius kibernetinio saugumo aspektus – tiek prevenciją, tiek atsistatymą po incidentų.[111]

Tačiau lygiai taip pat buvo pripažinta, kad tarp daugelio Lietuvos organizacijų, ypač tarp įmonių vadovų, vis dar yra paplitęs požiūris, jog prioritetas yra prevencijai ir bet kokiam bandymui išvengti atakų. Tarp įmonių vadovų dar vis yra paplitęs supratimas, kad jeigu “jeigu aš jau investavau daug į kibernetinį saugumą, nusamdžiau geriausius ekspertus, supirkau brangiausią įrangą, kad incidento neatsitiks ir esu apsisaugojęs. Ir čia jokių atstatymo planų nereikia”[112]. Tai sukuria tam tikrą silpną vietą, kuomet išorės grėsmių neišvengsi ir nesukontroliuosi.

Vilniaus rajono savivaldybė taip pat akcentuoja svarbą tiek kibernetinių grėsmių ir rizikų valdymui, tiek atsparumo užtikrinimui. Stanislav Sokolovski, Vilniaus rajono savivaldybės informacinių technologijų skyriaus vyr. patarėjas, laikinai einantis vadovo pareigas, pabrėžė, kad savivaldybė investuoja į nepertraukiamą darbą ir atsparumą, skirdama daug dėmesio tiek

[109] *Ibid.*

[110] Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

[111] *Ibid.*

[112] *Ibid.*

programinei, tiek techninei įrangai (hardware ir software). Svarbiausias tikslas yra užtikrinti, kad būtų išvengta įsilaužimų, tačiau taip pat nemažiau svarbus yra ir veiksmų planas, paruoštas siekiant sumažinti galimą žalą įvykus kibernetinei atakai. Tai rodo, kad savivaldybė ne tik pasikliauja prevencija, bet ir aktyviai rengia strategijas, kurios užtikrintų organizacijos atsparumą ir gebėjimą greitai atsigauti po incidentų.[113]

Vilniaus universiteto (VU) kibernetinio saugumo strategija puikiai atspindi tendenciją, kur organizacijos derina tiek prevenciją, tiek atsparumą. Interviu metu, Viktoras Bulavas, duomenų privatumo ir informacijos saugumo centro vadovas pabrėžė, kad nuo 2016 metų, kai NATO priėmė sprendimą įteisinti kibernetinės gynybos pajėgas kaip oficialią kariuomenės rūšį[114], organizacija pradėjo derinti abu požiūrius – tiek prevenciją, tiek atsparumą. Tai rodo, kad organizacija ne tik investuoja į kibernetinių atakų prevenciją, bet taip pat stiprina gebėjimą greitai atkurti sistemas ir prisitaikyti prie naujų grėsmių. V. Bulavas nurodė, kad po svarbių kibernetinių incidentų, tokių kaip 2021 m. VGTU ir 2023 m. KTU atakos, organizacija vis daugiau dėmesio skiria greitojo atsistatymo procesams ir infrastruktūrai. Tai atspindi atsparumo požiūrį, kurio svarba auga, kai kibernetiniai incidentai tampa vis dažnesni.[115]

Anksčiau organizacija daugiausia reaguodavo pagal kiekvieno darbuotojo gebėjimus, tačiau po šių incidentų pripažinta bendros gynybos poreikis, o strategija "kiekvienas už save" pasikeitė į bendrą apsaugą. Tai rodo, kad organizacija perėjo prie holistinio požiūrio, kuris apima tiek prevenciją, tiek greitą atsistatymą ir prisitaikymą. V. Bulavas taip pat pabrėžė, kad universiteto IT paslaugų centras aktyviai ieško spragų ir atlieka tinklo stebėjimą, kad užtikrintų saugumą. Tai taip pat rodo, kad organizacija stengiasi užkirsti kelią grėsmėms ir tuo pačiu užtikrinti, kad net ir įvykus incidentui, infrastruktūra būtų greitai atkuriama. Taip pat svarbūs minkštieji, kultūriniai aspektai, kurie apima darbuotojų švietimą ir jų aktyvų įsitraukimą į organizacijos saugumo procesus, kurie yra būtini siekiant užtikrinti ilgalaikį atsparumą.[116]

Vilniaus universiteto atstovas Viktoras Bulavas, atsakydamas į klausimą apie pereinamąjį procesą nuo rizikos ir grėsmių valdymo požiūrio prie atsparumo grindžiamo požiūrio, pabrėžė, ***kad tradiciniame rizikos valdyme daugiausia dėmesio skiriama grėsmių identifikavimui ir jų šalinimui, tačiau atsparumo požiūris reikalauja visiškai kitokios mąstysenos. „Daugeliui organizacijų sunku prognozuoti, kokios grėsmės ir incidentai gali įvykti, todėl neaišku, kurioms sritims teikti***

[113] Stanislav Sokolovskis (Vilniaus Rajono Savivaldybė), interviu, interviu telefonu, 2024m. Gruodžio 10d.

[114] European Council, *EU-NATO joint declaration*, žiūrėta 2024m. 12 19d., https://www.consilium.europa.eu/en/press/press-releases/2016/07/08/eu-nato-joint-declaration/

[115] Viktoras Bulavas (Vilniaus Universitetas), virtualus interviu, 2024m. Gruodžio 10d.

[116] *Ibid.*

prioritetą“, – sakė V. Bulavas, pabrėždamas, kad šis požiūris akcentuoja ne tik prevenciją, bet ir greitą atsistatymą bei prisitaikymą.[117]

Jonas Pidkovas, Vilniaus savivaldybės IT ir Inovacijų komandos vadovas, aptarė organizacijos požiūrį į kibernetinį atsparumą, pabrėždamas, kad šiuo metu organizacijos tikslas yra sukurti holistinį požiūrį, kuris apima tiek prevenciją, tiek greitą atsistatymą po incidentų. Jo teigimu, „vienas lauke ne karys“, todėl svarbu, kad komanda, dirbdama su kibernetiniu saugumu, būtų integruota ir bendradarbiautų. Organizacija ne tik vertina savo kibernetinio atsparumo lygį, bet ir reguliariai vykdo praktinius testus, tokius kaip duomenų atstatymo pratybos ir grėsmių, tokių kaip **„**ransomware**“**, analizė. J. Pidkovas pabrėžė, kad jų komanda ne tik prižiūri esamas sistemas, bet ir aktyviai ieško technologinių sprendimų, kurie galėtų užtikrinti greitą atstatymą po incidentų, taip pat atsižvelgiant į kaštų efektyvumą. „Netgi nagrinėjame technologinius sprendimus, kurie pigesni būtų, architektūriškai, kur eit, kad atsitatyt greitai“, – sakė jis, taip pabrėždamas, kad sprendimų priėmimas yra pagrįstas tiek saugumo, tiek efektyvumo aspektais.[118] Vilniaus savivaldybės pasiruošima kibernetinio atsparumo klausimais parodo ir administracijos vadovo Adomo Bužinsko supratimas ir požiūris į tai. Adomas pabrežė, kad buvo įkurta ir atskiras atsparumo skyrius, pabrėžiant, kad išorinių grėsmių neišvengsi, jos įvyks – „Tai gaunasi, kad vis tiek sistema….aš kaip vadovas administracijos negaliu pasakyti, kad viskas ok, kol mūsų subsidijos nėra pasiruošusios. Tai apie tai yra tas atsparumo skyrius, kad mūsų bendrą standartą pritaikyti kitur ir kai būna tos didesnės atakos, ir jie daro srautą, kad tas srautas nueitų į nepasiruošusias organizacijas, tai vat…bet iš tos pusės mes niekad nesakom, kad esam fully pasiruošę, bet čia yra neklausimas “ar gali įsibrauti?”, o “per kiek laiko?”. kol kiti yra silpniau pasiruošę, mes esam stiprūs.”[119]

Kalbant apie vertinimo rodiklius, Vilniaus savivaldybė nustatė konkrečius kibernetinio atsparumo tikslus ir naudoja KPIs, kad stebėtų, kiek veiksmingai jie įgyvendina savo strategiją. „Turimė pasidarę, kaip pasakyt, kartais pakliūna tokie dalykai, kur greit negali ištaisyt jų, kad ištaisyt reikia laiko“, – nurodė J. Pikdovas, pabrėždamas, kad organizacija siekia kuo greičiau reaguoti į kibernetines grėsmes ir nuolat tobulinti savo atsistatymo procesus. Be to, jis paminėjo, kad organizacija reguliariai tikrina, kaip darbuotojai reaguoja į potencialias grėsmes, pvz., „phishingo“ bandymus, kad galėtų įvertinti jų atsparumą ir veiksmingumą. „Tai šitą, tada kiek kas paspaudė ir suvedė savo duomenis“, – sakė jis, atskleidžiant, kad tokie rodikliai yra naudojami ne tik kaip įrankiai vertinant atsparumą, bet ir kaip būdas įvertinti organizacijos pasirengimą reaguoti į grėsmes realiuoju laiku.[120]

---

[117] *Ibid.*

[118] Jonas Pidkovas (Vilniaus Savivaldybė), interviu, Vilnius, 2024m. Gruodžio 4d.

[119] Adomas Bužinskas (Vilniaus Savivaldybė), interviu, Vilnius, 2024 metų, Gruodžio 11d.

[120] *Ibid.*

Vilniaus savivaldybės požiūris į kibernetinį atsparumą atspindi augantį organizacijų siekį ne tik užkirsti kelią grėsmėms, bet ir užtikrinti greitą atsistatymą bei adaptaciją, kad organizacija galėtų išlikti funkcionali net ir susidūrusi su kibernetiniais incidentais. Prie Vilniaus savivaldybės kibernetinio atsparumo praktikos galima pridėti ir jų supratimą apie investicijas kibernetiniam atsparumui. Adomas Bužinskas dalinasi, kad jis, kaip vadovas, supranta gerų specialistų kompetencijos svarbą šioje srityje, kurie sudėlioja investicijas. Pabrėžiama, kad būtent ši sritis reikalauja daug investicijų: „mes iš vadybinės pusės, jeigu taip grynai, tai mano tikslas yra susamdyt gerus žmones savo srityse ir tas sritis padengti. Tai tas sritis nebuvo padengta, mes sukūrėm tą padalinį, aš iš esmės neateinu ir nenurodau jiems kaip ką daryt, jie ateina pas mane su sprendimais, biudžeto poreikiu ir panašiai, tai jau tą mes managin‘am. Bet faktas, kad įkūrę tą skyrių, ką aš jau minėjau administracijai, kad tu pasidarysi auditą tam tikrų sričių, IT saugumo ir pamatysi, kur esam, tavo biudžeto poreikis smarkiai išaugs. Tai vat planuojant 2025ų metų poreikį jau yra daug cyber security dalių, kurias mes uždengiam ir jos eina milijonais, reik suprasti. šitoj dalyje yra prioritetas, ta prasme čia tiesiog aš tai vertinu net ne kaip prioritetą, bet kaip higieną, kaip užsirakinam duris vakare pastato, taip ir sistema turi mano būti be skilių visa.“ A. Bužinsko nuomone, kibernetinio saugumo priemonės tampa ne tik prioritetu, bet ir būtinybe, kurios integracija užtikrina organizacijos atsparumą bei ilgaamžiškumą. Tai rodo, kad siekiant užtikrinti tinkamą kibernetinį atsparumą, organizacijoms reikia nuolatos investuoti į tiek žmogiškuosius išteklius, tiek technologijas, o kibernetinio saugumo praktikos turi tapti įprasta dalimi organizacijos kasdienybės.[121]

Apibendrinant šį skyrių, galima teigti, kad Lietuvoje kibernetinio atsparumo praktikoje išryškėja svarbus balansavimas tarp prevencijos ir reagavimo, kur prevencija dažnai dominuoja, tačiau organizacijos vis daugiau dėmesio skiria atsparumo užtikrinimui ir greitam atsigavimui po incidentų. Pavyzdžiui, Kauno technologijos universiteto ir Vilniaus rajono savivaldybės atstovai pabrėžė svarbą ne tik užkirsti kelią kibernetinėms atakoms, bet ir turėti strategijas, leidžiančias greitai reaguoti ir atkurti sistemas, kai ataka įvyksta. Tai atitinka keturis pagrindinius atsparumo komponentus, kurie buvo nagrinėti metodologijoje – pasirengimą, absorbciją, atsigavimą ir prisitaikymą. Taip pat buvo pastebėta, kad daugelis organizacijų vis dar susiduria su iššūkiu, kai pasitikima tik prevenciniais įrankiais, o ne investuojama į ilgalaikes atsparumo strategijas ir reagavimo mechanizmus. A. Bužinsko, V. Bulavo, Š. Končiaus, D. Vitkaus ir J. Pidkovo pasisakymai atskleidžia, kad atsparumas nėra vienkartinis procesas, bet nuolatinis, dinamiškas procesas, reikalaujantis visapusiškos strategijos, įskaitant tiek prevenciją, tiek greitą reakciją ir adaptaciją, kad būtų užtikrintas organizacijos gebėjimas atlaikyti kibernetines grėsmes ir išlikti funkcionalia net ir po incidentų. Viktoras Bulavas, atstovaujantis Vilniaus universitetui, pabrėžė, kad organizacija po

[121] *Ibid.*

svarbių kibernetinių incidentų sustiprino savo greito atsistatymo procesus ir infrastruktūrą, taip pat perėjo prie holistinio požiūrio, kuris apima ir bendrą gynybą, ir greitą prisitaikymą. Šis požiūris puikiai papildė anksčiau minėtus komponentus ir pabrėžė ilgalaikės kibernetinio atsparumo strategijos svarbą, ypač kai organizacijos susiduria su vis dažnėjančiomis grėsmėmis.

3.2 Atsparumo iššūkiai ir gerosios praktikos organizacijose

Atsparumo iššūkiai Lietuvoje ir gerosios praktikos organizacijose yra susijusios su nuolatiniais kibernetinio atsparumo vertinimais, testavimais ir prisitaikymu prie naujų grėsmių. Analizė atskleidė, kaip skirtingos organizacijos suvokia ir taiko atsparumo principus bei metodikas, susijusias su pasirengimu, absorbcija, atsigavimu ir prisitaikymu, kad užtikrintų ilgalaikį atsparumą ir gebėjimą sėkmingai reaguoti į kibernetinius incidentus.

Vilniaus universitetas (VU) kibernetinio atsparumo vertinimui naudoja kelias metodikas ir nuolat atliekamus vertinimus. Viktoras Bulavas pabrėžė, kad organizacija reguliariai atlieka rizikos vertinimus kartu su papildomu valdymo procesų brandos vertinimu. „Pirmiausia (2016 m.) pradėjome nuo informacinių sistemų valdymo procesų pagal ISO 2700x vertinimą, naudojome ISO 33020 modelį“, – teigė jis, pridurdamas, kad vėliau, reaguodami į BDAR (Bendrasis duomenų apsaugos reglamentas), įvertino ir ISO 29151, kuris apima privatumo ir asmens duomenų apsaugos procesus. Šiemet taip pat buvo atliktas SOC (Security Operations Center) procesų brandos vertinimas pagal SOC-CMM metodiką[122]. Tai gerai atspindi pasirengimo ir absorbcijos aspektus – nuolatinis vertinimas padeda organizacijai pasiruošti galimiems incidentams ir greitai prisitaikyti prie besikeičiančių grėsmių. VU ypatingą dėmesį skiria laikui, per kurį atstatomos paslaugos po incidentų. Bulavas taip pat paminėjo, kad „periodiškai išsibandome svarbiausias sistemas ir jų atkuriamumą po incidentų, ypač po didesnių infrastruktūrinių pakeitimų, vykdome veiklos tęstinumo atkūrimo išbandymus“, taip užtikrinant, kad po incidento paslaugos būtų atstatytos per priimtiną laiką. Tai rodo, kad organizacija derina įvairius vertinimo metodus ir nuolat tikrina savo pasirengimą užtikrinti atsparumą ir veiklos tęstinumą, atsižvelgiant į informacijai keliamus reikalavimus ir svarbą. VU metodika orientuojasi į atsparumo laiko tikslus, priklausančius nuo informacijos svarbos, ir atspindi atsigavimo bei prisitaikymo aspektus, nes tai reikalauja nuolatinio prisitaikymo prie organizacijos ir jos sistemos poreikių.[123]

Viktoras Bulavas papasakojo plačiau ir apie tai, kaip KTU ataka paveikė jų bendras sistemas ir infrastruktūrą. 2023 metų gruodžio 8 d. įvykęs kibernetinis incidentas Kauno technologijos

[122] SOC-CMM, „SOC-CMM About“, žiūrėta 2024m. Gruodžio 19d., https://www.soc-cmm.com/about/

[123] Viktoras Bulavas (Vilniaus Universitetas), virtualus interviu, 2024m. Gruodžio 10d.

universitete (KTU) turėjo tiesioginį poveikį ir Vilniaus universiteto (VU) sistemoms, nes abu universitetai yra susiję per bendrą LITNET infrastruktūrą. Siekiant užkirsti kelią incidento plėtrai, buvo priimtas sprendimas laikinai atjungti tam tikrus tinklus, tačiau tai lėmė dalies vidutinės svarbos paslaugų prastovą, o pilnai paslaugos buvo atnaujintos tik po keturių dienų. „Nors buvome pasitvirtinę, kad tų paslaugų priimtino neveikimo laikas yra 5 dienos, tapo aišku, kad toks neveikimo laikotarpis, nustatytas beveik prieš 10 metų, nebeatitinka naudotojų lūkesčių, todėl ėmėmės papildomų priemonių sutrumpinti atstatymo laiką“, – pasakojo V. Bulavas. Tai rodo, kad po incidentų organizacija nuolat atnaujina savo atsparumo strategijas ir technologinius sprendimus. V. Bulavas nurodė, kad ši situacija paskatino universitetą atlikti papildomus veiksmus, įskaitant greitesnį reagavimo procesą, tinklo segmentavimą ir papildomų automatizuotų atsarginių kopijų atkūrimo procedūrų įdiegimą.[124]

Tuo tarpu Donatas Vitkus, kalbėdamas apie „Ignitis“ organizaciją, akcentavo tiek technologinius, tiek procedūrinius aspektus, kurie sudaro organizacijos atsparumo praktiką. „Mes reguliariai atliekame testavimus, kad įvertintume, kaip efektyviai mūsų sistemos atsako į kibernetinius incidentus“, – teigė Vitkus. Tai rodo, kad praktiniai testavimai yra būtini norint užtikrinti ne tik greitą atsistatymą, bet ir tikslų reagavimą į galimas grėsmes. D. Vitkus pabrėžė, kad kibernetinio atsparumo plane turi būti aiškiai apibrėžti incidentų valdymo procesai – nuo grėsmių aptikimo iki pranešimo ir atsako. Kaip interviu pažymėjo D. Vitkus, organizacijoms kibernetinio atsparumo pagrindu tampa poveikio veiklai vertinimai (angl. Business Impact Analysis), kuriuose analizuojami tokie aktualūs rodikliai kaip kritiniai procesai, kritiniai resursai, juos palaikantys procesai ir palaikantys resursai. Taip pat pabrėžiamos reikšmės, susijusios su atstatymo laiku (Recovery Time Objective, RTO) ir atkūrimo taško tikslu (Recovery Point Objective, RPO): „Reikėtų turėti pirmiausia tai poveikio veiklai vertinimus (angl. Business impact analysis), analizes su aktualiais rodikliais - tai yra kritiniai procesai, kritiniai resursai, palaikantys procesai, palaikantys resursai. Tada indikuotos <RPO ir RTO> reikšmės - atstatymo laikas ir “Recovery Point Objective”. Iš to turi sekti veiklos tęstinumo planas, kur numatyti alternatyvūs veikimo būdai, poveikio mažinimo būdai, komunikacija, krizių komunikacija ir lygiagrečiai statymo planas (angl. disaster recovery). Tai yra detalios instrukcijos, kaip atstatyti, kur guli “backup’ai”, kokios instrukcijos, kokie prisijungimo duomenis. Tai nu, aš matyčiau, ką turėtų turėt. Aš manyčiau, kad mes visus tuos dalykus turim, bet dar kai kai kuriuos planus reikėtų atnaujinti.” – teigė D. Vitkus. Šių rodiklių pagrindu formuojami veiklos tęstinumo planai, kuriuose numatomi alternatyvūs veikimo scenarijai, poveikio mažinimo priemonės, komunikacijos ir krizių komunikacijos strategijos. Lygiagrečiai svarbus ir atkūrimo planas (angl. Disaster Recovery), kuriame pateikiamos detalios instrukcijos, kaip atkurti veiklą, kur

[124] *Ibid.*

saugomos atsarginės duomenų kopijos, kokios naudojamos instrukcijos ir prisijungimo duomenys. Taip pat, kaip buvo pabrėžiama, nors organizaciją turi šiuos elementus, pastebima, kad vienas iš iššūkių, su kuriuo organizaciją susiduria, tai yra tai, kad kai kurie planai reikalauja atnaujinimo, siekiant užtikrinti jų aktualumą ir efektyvumą.[125] Tai gerai atspindi absorbcijos ir atsigavimo principus, nes praktiniai testavimai leidžia organizacijai pasiruošti ne tik techniniams iššūkiams, bet ir krizių komunikacijai, kuri taip pat turi svarbų vaidmenį užtikrinant greitą organizacijos atsistatymą.

Kalbėdamas apie veiklos tęstinumą ir atstatymą, D. Vitkus pabrėžė, kad organizacijos gebėjimas sėkmingai valdyti incidentus priklauso nuo dviejų pagrindinių faktorių: aiškaus plano ir nuolatinio testavimo. „Pratybų ir testavimų svarba Lietuvoje yra neįkainojama, nes jie padeda sustiprinti organizacijų atsparumą ir pasirengimą krizėms“, – sakė Vitkus. Tai atspindi kibernetinio atsparumo komponentus – atsigavimą ir prisitaikymą, nes tik testavimai leidžia organizacijai būti pasiruošusiai realiems iššūkiams, kurie dažnai apima didelį stresą ir išorinius spaudimus. Šioje vietoje yra svarbus ne tik techninis pasirengimas, bet ir gebėjimas reaguoti žingsnis po žingsnio, kaip pabrėžė D.Vitkus dalyvavęs pratybose, tiek Lietuvoje, tiek NATO organizuotose. Tai padeda išlaikyti ramybę ir tinkamai reaguoti.[126]

Kalbant apie organizacijų sėkmingumą, „Ignitis“ grupė yra viena iš organizacijų, turėjusių nesmagią patirtį su kibernetinėmis atakomis, kai prieš keletą metų prieš juos buvo vykdyta anksčiau minėta ir pristatyta DDoS ataka. Tačiau pastaruoju metu grupė išvengė bet kokių rimtesnių pažeidimų, nors atakų taip pat buvo. Kaip vieną iš skirtumų, Donatas Vitkus pabrėžė, kad buvo imtasi papildomų priemonių. „Tai priemonės, kurių imamės – aišku, yra planai ir planų testavimai, kai DDoS visada buvo įvardintas kaip galima grėsmė. Visgi DDoS testavimas yra sudėtingas, nes tai tik testavimas – ne reali ataka. <...> Šiuo atveju suvaldymas turėjo būti mūsų interneto tiekėjo pusėje, nes atakos dydis buvo toks, kad organizacija pati to nebevaldo,“ – teigė. D. Vitkus. Taip pat, nors ir tarp organizacijų labiau paplitę yra reguliarūs info saugos mokymai, mokymai naujai priimtiems darbuotojas, “phishing’o” testam mokymai pagal skirtingas pareigybes, iš tiesų tokios situacijos yra labiau prevencijos didinimui. Bet vis dėlto, jeigu kalbant apie tai, kas praktikoje didintų atsparumą, tai minėtų veiklos tęstinumo planų testavimai, atstatymo planų testavimai. Anot D. Vitkaus - “Panašiai kaip ir su evakuacijom. Evakuacijas, tarp kitko, irgi darom kartą per ketvirtį. Visas ofisas išsievakuojam su gaisro signalu. Tai tu jau žinai, ką daryti. Tai darome testavimus veiklos tęstinumo ir atstatymo planams”.[127]

Pasak Donato Vitkaus, po ankstesnių incidentų „Ignitis“ pradėjo diegti nuolatinę 24/7 stebėseną, kuri padėjo greitai atpažinti galimus pažeidimus. Vis dėlto, kaip pavyzdį jis pateikė ir kitus

[125] Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

[126] *Ibid.*

[127] *Ibid.*

incidentus, tokius kaip slaptažodžių nutekėjimas ar reputaciniai pavojai, kuriuos lėmė išorinės aplinkybės ir trečiųjų šalių sistemų saugumo spragos. Vitkus pažymėjo: „Tiek „Ignitis ON“, tiek „I Solar“ sistemų mes nevaldome tiesiogiai – tai trečiųjų šalių įrankiai, kurie, deja, neturi dviejų faktorių autentifikavimo. Tai yra išorinių sistemų apribojimas, kurio techninėmis priemonėmis negalime išspręsti.“ Šie pavyzdžiai išryškina dvi pagrindines problemas – technologinių spragų kontrolę ir trečiųjų šalių atsakomybę už sistemų saugumą. „Ignitis“ patirtis rodo, kad net ir pažangios priemonės, tokios kaip stebėsena ar planavimas, negali šimtu procentų užtikrinti kibernetinio atsparumo, kai tam tikri komponentai yra už organizacijos tiesioginės kontrolės ribų.[128]

Jonas Pidkovas, Vilniaus savivaldybės IT ir Inovacijų skyriaus vadovas, taip pat išskyrė svarbą nuolat vertinti grėsmes ir greitai prisitaikyti prie jų. „Mes žiūrime į tai, kas atsitiktų, jei atsitiktų ekstremalūs įvykiai, kaip karas ar kitos situacijos“, – sakė J. Pidkovas. Savivaldybė aktyviai stebi ir numato potencialias grėsmes, dalyvaudama įvairiose komunikacijos platformose ir analizuodama informaciją iš neoficialių šaltinių, tokių kaip „Telegram“ ar „Twitter“, bei dark web. Šis „predikcijos“ metodas padeda organizacijai išlikti pasirengusiai greitai reaguoti į kylančius pavojus. Tokie prevencijos metodai atspindi pasirengimo ir absorbcijos principus, nes tai rodo organizacijos gebėjimą ne tik apsaugoti nuo grėsmių, bet ir įvertinti rizikas, kurios galėtų iškilti dėl nenumatytų situacijų.[129]

Be to, Jonas Pidkovas paminėjo, kad Vilniaus savivaldybė siekia sukurti holistinį požiūrį į kibernetinį atsparumą, apimantį tiek prevenciją, tiek greitą reagavimą ir atsistatymą po incidentų. „Hack me if you can“ programa, kurios tikslas buvo išbandyti sistemas, rodo, kad organizacija neapsiriboja tik teorinėmis priemonėmis, bet aktyviai siekia tobulinti savo atsparumą nuolatiniame praktiniame testavime. „Tai parodo, kad mes aktyviai siekiame tobulinti savo kibernetinio atsparumo strategiją“, – teigė J. Pidkovas. Tokie testai padėjo organizacijai atskleisti savo pažeidžiamumus ir pagerinti savo atsparumą, o rezultatai buvo įtraukti į tolesnį strateginių veiksmų planavimą. Tai parodo, kad Vilniaus savivaldybė neapsiriboja tik teorinėmis priemonėmis, bet aktyviai siekia tobulinti savo kibernetinio atsparumo strategiją per nuolatinius praktinius testus. Ši strategija puikiai atspindi visus keturis atsparumo principus: pasirengimą, absorbciją, atsigavimą ir prisitaikymą, nes organizacija ne tik kuria atsparumo planus, bet ir juos nuolat tikrina realiomis sąlygomis.[130]

J. Pikdovas taip pat pabrėžė, kad organizacija laikosi atsarginio plano principo, užtikrindama, kad turėtų du skirtingus planus ir įrankius, kad būtų pasiruošusi greitai atsistatyti po bet kokio incidento. „Jo, kai turi du planus, įrankius. Kas liečia technologinius dalykus, mes turime ir alternatyvius įrankius, ir atsarginius planus, kurie leidžia greitai pereiti prie kito veikimo metodo, jei

[128] *Ibid.*

[129] Jonas Pidkovas (Vilniaus Savivaldybė), interviu, Vilnius, 2024m. Gruodžio 4d.

[130] *Ibid.*

pirmas nepavyksta. Tai suteikia mums lankstumo ir užtikrina, kad net ir netikėtos situacijos nepaliks mūsų be atsako. Būtent šis dviejų planų ir įrankių principas leidžia mums užtikrinti, kad net esant kritiniams įvykiams, mes galėsime greitai atsigauti ir tęsti darbą“, – sakė J. Pidkovas. Toks požiūris atspindi organizacijos pasirengimą ne tik reaguoti į grėsmes, bet ir užtikrinti spartų atsigavimą, nepriklausomai nuo situacijos sunkumo. Taip pat J. Pidkovas išskyrė, kad įstatymų laikymuisi dažnai prioritetas tampa dokumentacijos, tačiau norint greito reagavimo, ko dažnai reikalauja kibernetinė erdvė ir jos grėsmes, tai nėra paranku. Dėl to ne visuomet pasiteisina ilgalaikiai planai ar dokumentacija. Kaip pavyzdį jis pateikė naujos sistemos diegimą, kuomet reikia greito “persimetimo” iš vienos sistemos į kitą. Jis pabrėžė, kad “jeigu turėtume griežtą strategiją, negalėtume greit dabar į šitą persimesti”. Taigi, tam tikrais momentais planai ir strategijos gali trukdyti greitai reaguoti į kibernetinės erdvės dinamiškumą ir net gautis tam tikras iššūkis.[131]

Be prevencijos ir atsistatymo priemonių, Vilniaus savivaldybė taip pat akcentuoja bendruomenės įsitraukimą ir bendradarbiavimą su kitomis organizacijomis, siekiant pasidalinti gerąja praktika ir įvertinti naujas grėsmes. „Turim tą bendruomenę, į ją įeina kas nori, pasakojame apie realius atvejus...“, – sakė J. Pidkovas[132]. Tai rodo, kad bendruomenės įtraukimas į kibernetinio atsparumo procesą padeda ne tik gerinti atsparumą organizacijos viduje, bet ir skleisti gerąsias praktikas visame sektoriuje. Bendruomenės svarba tapo akivaizdi ir Vilniaus universitete, kur Viktoras Bulavas akcentavo, kad žinių dalijimasis ir bendruomenės įtraukimas padeda stiprinti viso sektoriaus atsparumą. „Kai pradėjome bendruomenėje skųstis dėl tų visų programų, kur praneša ir gauna per galvą, tada pradėjome mąstyti, kaip ta bendruomene, kuri irgi nori prisidėti, įtraukti, kad būtų tas atsparumas“, – sakė V. Bulavas[133]. Tai rodo, kad kibernetinio atsparumo gerinimas reikalauja ne tik techninių sprendimų, bet ir organizacinės kultūros kūrimo.

Pasak Vilniaus universiteto atstovo Viktoro Bulavo, pereinant nuo tradicinio rizikos valdymo požiūrio į atsparumo grindžiamą požiūrį, reikia visiškai kitokios mąstysenos: „Daugeliui organizacijų sunku prognozuoti, kokios grėsmės ir incidentai gali įvykti, todėl neaišku, kurioms sritims teikti prioritetą“. Jis pabrėžė, kad atsparumo požiūris akcentuoja ne tik prevenciją, bet ir greitą atsistatymą bei prisitaikymą. Šis požiūris tapo dar svarbesnis prasidėjus karui Ukrainoje, kai VU peržiūrėjo pagrindinius atakų vektorius ir pasidalino šia informacija su kitų aukštųjų mokyklų darbuotojais: „Atlikome eilę patikrinimų ir susijusių pakeitimų, kurie turėtų padėti sumažinti žalą įvykus panašioms atakoms“. V. Bulavas pabrėžė, kad organizacija turi „gyvą“ (nuolat atnaujinamą ir peržiūrimą) svarbiausių kibernetinio saugumo priemonių įgyvendinimo planą, kuris apima tiek infrastruktūrinius pokyčius, tiek socialinio bendruomenės atsparumo pratybas. Pavyzdžiui, VU dalyvauja Nacionalinio

[131] *Ibid.*

[132] Ibid.

[133] Viktoras Bulavas (Vilniaus Universitetas), virtualus interviu, 2024m. Gruodžio 10d.

kibernetinio saugumo centro organizuojamose pratybose, tokiose kaip „Kibernetinis skydas“, kuriose per kelis metus dalyvavo daugiau nei šimtas Lietuvos organizacijų. Universiteto dalyvavimas šiose pratybose buvo dvipusis: tyrėjai dalyvavo modeliuojant ir įgyvendinant pratybų poligonus, o kita dalis bendruomenės patyrė pačias pratybas. Tai rodo, kad VU ne tik rūpinasi techniniais kibernetinio saugumo aspektais, bet ir aktyviai skatina bendruomenės įsitraukimą į atsparumo didinimo procesus.[134]

Apie atsparumo iššūkius užsiminė ir Vilniaus rajono savivaldybės IT skyriaus vyr. patarėjas Stanislav Sokolovski, aptardamas 2024 m. gruodžio 5 d. įvykdytą kibernetinę ataką prieš savivaldybę. Vilniaus rajono savivaldybės IT skyriaus vadovo Stanislav Sokolovski pateiktas pavyzdys apie kibernetinę ataką parodo, kaip organizacija susidūrė su realiais iššūkiais reaguojant į incidentą ir kaip po to buvo atlikti reikšmingi organizaciniai pokyčiai: “Kai įvyko ataka ir darbuotojai pradėjo kreiptis pagalbos, nelabai atrodė, kad organizacija tiksliai žinojo, ką reikia daryti. Galbūt jie žinojo, ką reikia atlikti teoriškai, bet praktikoje – nelabai. Organizacija turi bazę ir instrukcijas, tačiau realiai daugiausia pagalbos suteikė „Telia“. Po atakos buvo skirtos baudos už tai, ko nepadarėme, bet niekas nesigilino į tikrąją situaciją. Be to, kai paprašai pagalbos, ne visada aiškiai pasako, ką ir kaip reikia daryti. Krašto apsaugos sistema suteikia daugiau realios pagalbos, ypač organizuojant phishingo testus. „KVTC“ taip pat kažkiek padeda, bet trūksta kvalifikuotų žmonių. Jei reikia pagalbos iš tinklo specialistų, tai užtrunka labai ilgai, o patyrę specialistai brangiai kainuoja. Jei paimsime, pavyzdžiui, mažesnę savivaldybę, kaip Akmenės, sunku įsivaizduoti, kaip jie viską tvarkys. Reikalavimų daug, instrukcijos sudėtingos, o resursų ir žinių – mažai. Vilniuje vis tiek turime daugiau išteklių ir supratimo, bet net ir čia žmonių trūkumas labai jaučiamas. Jei giliniesi į licencijas, tai nelieka laiko tvarkyti kitų svarbių užduočių.” Jo teigimu, savivaldybė nebuvo tinkamai pasirengusi tokiam incidentui – trūko specialistų, iš esmės dirbo tik du su puse žmogaus, atsakingų už 700 žmonių sistemą. Po šios atakos buvo priimti papildomi specialistai, suformuotas naujas skyrius ir glaudžiai bendradarbiauta su KVTC (Kertinis valstybės komunikacijų centras). Visa duomenų bazė ir serveriai buvo perkelti į duomenų centrą, o saugumui užtikrinti įsigyta naujos kartos antivirusinė programa. Tai rodo, kad organizacijos, norėdamos pasiekti ilgalaikį atsparumą, turi ne tik investuoti į prevenciją ir aptikimą, bet ir nuolat stiprinti savo atsistatymo bei prisitaikymo gebėjimus, kad galėtų greitai reaguoti į bet kokias nenumatytas grėsmes.[135]

Skyrius buvo sustiprintas, siekiant išvengti atsakomybių sukoncentravimo vieno žmogaus rankose, kadangi vienam atsakingam darbuotojui buvo per sunku susidoroti su tokio masto iššūkiais. Ataka buvo įvykdyta labai profesionaliai, naudojant sudėtingas programines priemones, todėl tai

[134] *Ibid.*

[135] Stanislav Sokolovskis (Vilniaus Rajono Savivaldybė), interviu, interviu telefonu, 2024m. Gruodžio 10d.

buvo rimtas ir sudėtingas incidentas. Stanislav Sokolovski teigė, kad jei būtų buvę daugiau žmogiškųjų išteklių, reakcija galėjo būti greitesnė – pavyzdžiui, serveriai galėjo būti laiku atjungti nuo tinklo. Šiuo metu įgyvendintos priemonės užtikrina, kad įvykus panašiai atakai, būtų prarasta tik keletas dienų ar mėnesių duomenų, o ne metai, kaip buvo šios atakos metu. Vis dėlto, S. Sokolovski pripažino, kad įsilaužėliai taip pat tobulėja: „vieni kuria programinę įrangą su spragomis, kiti jas aktyviai ieško.“[136]

Palygindami šiuos atsparumo aspektus su mano metodologijoje naudojamais keturiais atsparumo principais – pasirengimu, absorbcija, atsigavimu ir prisitaikymu – matome, kad dauguma organizacijų Lietuvoje orientuojasi į visapusišką atsparumo kūrimą. Pasirengimas yra susijęs su grėsmių vertinimu ir rizikos analizėmis, kaip pabrėžta VU ir Ignityje, kai organizacijos reguliariai tikrina savo sistemas ir plėtoja atsparumo planus. Absorbcija ir atsigavimas atsispindi nuolatinėse pratybose ir planų testavime, kaip matome „Ignitis“ ir Vilniaus savivaldybėje, kur organizacijos ne tik kuria planus, bet ir juos tikrina praktikoje. Prisitaikymas yra akivaizdus tiek Vilniaus universiteto, tiek Vilniaus savivaldybės požiūriuose, nes organizacijos aktyviai stebi naujas grėsmes ir prisitaiko prie besikeičiančios kibernetinės aplinkos. Tai rodo, kad Lietuvos organizacijos supranta kibernetinio atsparumo svarbą kaip visapusišką ir nuolatinį procesą, kuris apima ne tik technologijas, bet ir organizacines praktikas bei kultūrą.

3.3 Atsiliepimas apie įstatymą ir analizė: poveikis ir praktinis įgyvendinimas

Vienas iš Kibernetinio saugumo įstatyme numatytų aspektų yra organizacijų atsakomybė už bendradarbiavimą ir priežiūrą kibernetinio saugumo srityje Lietuvoje. Vienas iš šio darbo siekių – išsiaiškinti, kiek šis bendradarbiavimas realiai vyksta ir kaip organizacijos bendradarbiauja su institucijomis, tokiomis kaip Nacionalinis Kibernetinio Saugumo Centras (NKSC) ar Krašto apsaugos ministerija, ypač atakų atvejais.

Anot Donato Vitkaus, „Ignitis“ grupė glaudžiai bendradarbiauja su šiomis institucijomis: „Pirmiausia, bendradarbiaujame su Nacionaliniu kibernetinio saugumo centru, Krašto apsaugos ministerija – tai pagrindinės šalys, su kuriomis mes dirbame. Visa kita yra daugiau ekspertinio lygmens bendradarbiavimas.“ D. Vitkus taip pat pažymėjo, kad grupė bendradarbiauja su Lietuvos kariuomene, tačiau šis bendradarbiavimas nėra tiesiogiai įpareigotas įstatymų, o vyksta ekspertiniame lygmenyje. Tai rodo, kad bendradarbiavimas su valstybės institucijomis, nors ir svarbus, nėra pakankamai reglamentuotas, o tai gali kurti spragas, kurias reikia užpildyti aiškesniais įstatyminiais reikalavimais.[137]

---

[136] *Ibid.*

[137] Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

D. Vitkus išskyrė, kad bendradarbiavimas daugiausia vyksta prevencijos srityje, įskaitant keitimąsi gerąja praktika ir dalyvavimą kibernetinio saugumo pratybose. Atakos atveju „Ignitis“ pasitelkia Lietuvos kariuomenės ryšių batalioną ar Krašto apsaugos ministerijos greitojo reagavimo komandą, o NKSC informuojama pagal įstatymą. Ši praktika rodo, kad, nors bendradarbiavimas yra stiprus ir glaudus, realių atsparumo stiprinimo priemonių trūksta. Vitkus pažymėjo, kad įstatymas daugiausia nustato prevencinius reikalavimus ir priemones, o atsparumo mechanizmams trūksta detalumo.[138]

Dabartinėje sistemoje organizacijoms privalu turėti veiklos tęstinumo planus, tačiau šių planų turinys ir kokybės kriterijai paliekami jų pačių interpretacijai. Vitkus teigia, kad „tai jokios įtakos didelėms organizacijoms, tokioms kaip „Ignitis grupė“, neduoda, tačiau mažoms įmonėms galėtų būti pagalba.“ Tai rodo, kad dabartinis įstatymas neturi aiškių gairių, kaip formuoti ir įgyvendinti veiklos tęstinumo planus, o tai gali lemti nevienodą pasiruošimą tarp sektorių. Mažesnės organizacijos, turinčios mažesnius išteklius, patiria sunkumų pritaikydamos atsparumo strategijas ir įgyvendindamos įstatymų reikalavimus, todėl reikalingos aiškesnės gairės, kaip sukurti ir vykdyti šiuos planus.[139] Ta pačia tema užsiminė ir Šarūnas Končius (KTU Domreg’as). Jis aptarė kelis iššūkius, su kuriais susiduria mažos ir vidutinės organizacijos įgyvendindamos kibernetinio atsparumo strategijas. Vienas iš pagrindinių iššūkių yra klaidingas požiūris, kad mažos organizacijos nėra dideli taikiniai kibernetiniams nusikaltėliams. „Mažos organizacijos dažnai mano, kad niekas pas jas neateis, nes jos yra per mažos, tačiau nusikaltėliai dažnai renkasi lengviau pažeidžiamus taikinius“. Pasak jo, tai klaidinga nuostata, nes kibernetiniai nusikaltėliai, siekdami lengvai pasiekti pelną, dažnai taiko automatizuotas atakas prieš mažas organizacijas. Taip pat, jis paminėjo, kad Naujojo kibernetinio saugumo įstatymo direktyva pradeda labiau orientuotis į mažas ir vidutines įmones: „Dabar šis įstatymas labiau orientuotas į mažas ir vidutines įmones, kad jos pradėtų rimčiau žiūrėti į savo saugumą“. Ši direktyva skatina organizacijas užtikrinti, kad net mažos įmonės būtų pasirengusios reaguoti į kibernetinius incidentus.[140]

Paklaustas apie įstatymo tobulinimo galimybes, D. Vitkus išskyrė, kad būtų naudinga įtraukti detalesnes gaires dėl veiklos tęstinumo planų turinio. Tai padėtų organizacijoms lengviau integruoti atsparumo strategijas į savo veiklą. Taip pat, jis pažymėjo, kad dabartiniame reguliavime trūksta gairių, kaip pasirinkti ar įgyvendinti šiuos planus, dėl ko jie dažnai tampa formalūs ir nėra žiūrima į juos po incidentų. Tokie patobulinimai leistų ne tik fokusuotis į prevenciją, bet ir skatintų

[138] *Ibid.*

[139] *Ibid.*

[140] Šarūnas Končius (KTU Domreg), virtualus interviu, 2024m. Gruodžio 12d.

prisitaikymą bei greitą atsistatymą po incidentų, ypač svarbų mažoms ir vidutinėms organizacijoms.[141]

Apibendrinant, dabartinė reguliavimo sistema orientuojasi į prevenciją ir bendradarbiavimą, tačiau atsparumo stiprinimo mechanizmai yra nepakankamai detalizuoti. Tai ypač aktualu mažesnėms organizacijoms, kurioms trūksta resursų savarankiškai parengti veiksmingus planus. Gairių dėl atsparumo priemonių detalizavimas galėtų sustiprinti bendrą Lietuvos kibernetinio saugumo strategiją, prisidedant prie efektyvesnio kibernetinių grėsmių valdymo ir adaptacijos mechanizmų kūrimo.

Kalbant apie grėsmių valdymo praktikas ir strategijas, Donatas Vitkus paaiškino, kad jų organizacija šias analizės vykdo pati, tačiau naudoja įvairius šaltinius, kaip, pavyzdžiui, Nacionalinį kibernetinio saugumo centrą (NKSC) ir ENISA „threat analysis“. Pasak D. Vitkaus, nors NKSC ataskaitos nėra visada aktualios, nes jos apibendrina jau pateiktus duomenis, vis tiek naudingos siekiant suprasti, kokios grėsmės yra įvykusios praeityje ir kokie incidentai galėjo paveikti organizaciją. ENISA, savo ruožtu, teikia prognozes apie galimas grėsmes ateinančiais metais, tačiau šios prognozės dažniausiai yra bendro pobūdžio ir daugiau orientuotos į platesnę grėsmių aplinką.[142]

Donatas Vitkus paaiškino, kad nauji kibernetinio saugumo įstatymo pakeitimai, įskaitant ypatingos svarbos infrastruktūros sąrašo pakeitimą, nepaveikė jų organizacijos kasdienių praktikų, nes jie jau buvo įtraukti į kritinės infrastruktūros sąrašą. Naujasis įstatymas pakeitė sąvokas ir dabar apibrėžia „svarbius subjektus“ ir „esminius subjektus“, tačiau jų situacija iš esmės nesikeičia, nes jie jau priklauso kritinės infrastruktūros grupei.[143]

Kalbėdamas apie Lietuvos kibernetinio saugumo politikos stiprybes ir silpnybes, D. Vitkus pabrėžė, kad stiprybė yra vienodas „baseline'as“ visoms organizacijoms, kuris užtikrina pagrindinius saugumo standartus. Tai teigiamai veikia organizacijų politiką, nes leidžia sukurti bendrus standartus ir principus, kurių turi laikytis visos organizacijos. Tačiau jis taip pat paminėjo, kad mažoms organizacijoms reikia daugiau metodinės pagalbos, kad jos galėtų tinkamai įgyvendinti kibernetinio saugumo reikalavimus. Mažesnės įmonės dažnai susiduria su išteklių ir specialistų trūkumu, kas apsunkina jų galimybes užtikrinti reikiamą kibernetinį atsparumą. Nors didelės organizacijos jau investavo į kibernetinio saugumo vystymą ir turi aukštesnę brandą, mažesnėms įmonėms būtina suteikti daugiau pagalbos, kad jos galėtų pasiekti reikiamą saugumo lygį.[144]

D. Vitkus pabrėžė, kad bendradarbiavimas su Nacionaliniu kibernetinio saugumo centru (NKSC) per incidentus, nors ir reikalauja informacijos teikimo, netrukdo spręsti problemos. Jis teigė,

[141] Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

[142] *Ibid.*

[143] *Ibid.*

[144] *Ibid.*

kad raportuojant apie situaciją, būtina pateikti tam tikrą informaciją, kaip kas atsitiko, kada ir kodėl, kas padeda struktūrizuoti atsakymus ir užtikrina, kad nebūtų pamiršta svarbių detalių, kurios galėtų būti praleistos esant stresui. D. Vitkus pabrėžė, kad NKSC nereikalauja jokios papildomos informacijos, kuri būtų nereikalinga, ir kad organizacijos jau turėtų rinkti šiuos duomenis savo viduje, todėl toks informacijos pateikimas gali tik palengvinti incidentų valdymą.[145]

D. Vitkus pritarė teorijai, kad kai kurios organizacijos vengia dalintis informacija apie įvykusias kibernetines atakas su viešuoju sektoriumi dėl bausmių, kurios gali būti taikomos už šias atakas. Jis mano, kad toks požiūris yra klaidingas ir, su laiku, jis turi keistis, nes organizacijų brandos lygis auga. D. Vitkus pabrėžė, kad, žvelgiant iš platesnės bendruomenės perspektyvos, organizacijos, kurios patiria kibernetines atakas, vis dar dažnai neigiamai vertina tokius incidentus ir stengiasi juos slėpti, manydamos, kad tai yra didelis nesėkmės ženklas. Tačiau, jo nuomone, svarbu komunikuoti, kad nėra nieko, kas būtų visiškai atsparus kibernetinėms atakoms. Jis paminėjo, kad jų organizacija jau pasisakė už viešą kibernetinių atakų komunikavimą, jei jos būtų reikšmingos, ir jie neslėptų tokių įvykių. D. Vitkus mano, kad bendruomenė turi pereiti nuo požiūrio, jog atakos yra kažkas, ką reikia paslėpti, link požiūrio, kad tai yra natūralus procesas ir reikalinga dalytis patirtimi, kad visos organizacijos galėtų išmokti ir tobulėti. Tai reikalauja tam tikros brandos, kuri, kaip jis tikisi, su laiku atsiras.[146]

Kalbėdamas apie kibernetinio saugumo įstatymo pokyčius, Šarūnas Končius (KTU Domregas) teigė, kad pirmasis įstatymas buvo orientuotas į didesnes organizacijas, tačiau dabar, su antrosios versijos direktyva, jis tapo labiau įtraukiantis ir mažas įmones: „Pirmasis įstatymas buvo skirtas didelėms organizacijoms, bet dabar, su antros versijos direktyva, jis tampa įtraukiantis ir mažas įmones, kad jos rimčiau žiūrėtų į saugumą“. Pasak jo, šie pokyčiai gerai atspindi tarptautinius standartus ir padeda organizacijoms, tiek didelėms, tiek mažoms, užtikrinti savo kibernetinį atsparumą. Jis teigė - „Esminiai pokyčiai apima aiškesnį atsakomybės pasiskirstymą – jeigu organizacija nesilaiko saugumo reikalavimų, atsakomybė tenka vadovams, o ne tik IT vadovams“. Tai rodo, kad įstatymas pradeda labiau skatinti atsakomybę už kibernetinį saugumą visose organizacijos grandyse, o ne tik technologiniuose departamentuose.[147]

Vilniaus rajono savivaldybė susidūrė su rimtais iššūkiais po neseniai įvykusios kibernetinės atakos. Stanislav Sokolovski pabrėžė, kad, nors savivaldybė turėjo bazinius instrukcijas, praktiškai buvo neaišku, ką tiksliai reikia daryti. Dažniausiai pagalbą suteikė „Telia“, tačiau po atakos buvo paskirtos baudos už atliktų veiksmų trūkumą, nors realūs iššūkiai nebuvo tinkamai įvertinti. Tai rodo,

[145] *Ibid.*

[146] *Ibid.*

[147] Šarūnas Končius (KTU Domreg), virtualus interviu, 2024m. Gruodžio 12d.

kad, nors laikomasi teisinių reikalavimų, realus pagalbos teikimas ne visada atitinka praktinius poreikius.[148]

S. Skolovski taip pat pažymėjo, kad nors Krašto apsaugos sistema teikia pagalbą, įskaitant phishingo testus, ir Nacionalinis kibernetinio saugumo centras (NKSC) taip pat teikia pagalbą, tačiau trūksta kvalifikuotų specialistų, o jų paslaugos yra brangios. Tai išryškina skirtumus tarp teisinio ir praktinio kibernetinio atsparumo. Mažesnės savivaldybės, kaip Akmenė, susiduria su dar didesniais sunkumais, nes joms trūksta tiek resursų, tiek žinių, kad tinkamai įgyvendintų teisės aktus ir atitiktų kibernetinio saugumo reikalavimus.[149]

Vilniaus savivaldybės IT ir inovacijų vadovas ir administracijos vadovas, Jonas Pidkovas ir Adomas Bužinskas, taip pat pabrėžė, kad kibernetinio saugumo įstatymai kelia tiek iššūkių, tiek galimybių. A. Bužinskas teigė, kad nors įstatymai naudingi, jie dažnai kelia formalius reikalavimus, o ne praktinius sprendimus, kurie atitiktų realius iššūkius.[150] J. Pidkovas pritarė, kad įstatymai, reikalaujantys laikytis tam tikrų taisyklių dėl įrangos tiekimo ir sistemų atnaujinimo, kartais nesutampa su praktinėmis sąlygomis, ypač pereinant prie pažangesnių technologinių sprendimų. Jis taip pat pridūrė, ***kad kibernetinio atsparumo ir prevencijos klausimai Lietuvoje vis dar yra neatskiriami,*** ir dažnai investicijos į atsistatymą, atsigavimą po incidentų, nėra pakankamai įvertinamos. „Į vieną suplakama, nes ir standartuose ir dokumentacijoje, visur dažnai į vieną suplakama“, – nurodė J. Pidkovas. Jis pabrežė, kad tai būdinga ir įstatymui.[151] Tai rodo, kad Lietuvoje vis dar trūksta aiškios diferencijacijos tarp prevencijos ir atsistatymo strategijų, tačiau Vilniaus savivaldybė jau imasi žingsnių, kad atskirtų šias sritis ir įgyvendintų struktūrizuotus veiksmus tiek prevencijos, tiek atstatymo srityse.

Adomas Bužinskas taip pat pabrėžė, kad savivaldybė ne tik reaguoja į teisės aktus, bet ir siekia aukštesnių saugumo standartų. Nors vadovai atlieka papildomus veiksmus, kad užtikrintų didesnį saugumą, jie taip pat nuolat susiduria su biurokratiniais ir praktiniais iššūkiais. „Mes daug ką darom patys, tą keitimą pats turi inicijuot, jeigu susiduri su problema“, – sakė A. Bužinskas. Tai rodo, kad organizacijos turi būti pasirengusios pritaikyti teisės aktus ir integruoti juos į savo strategijas, kad jie atitiktų praktinius poreikius.[152]

Trečiosios šalys (third-party administrators) taip pat kelia iššūkius kibernetiniam atsparumui. Vilniaus savivaldybės atstovas Jonas Pidkovas ir KTU Domreg atstovas Š. Končius, taip pat Ignitis atstovas Donatas Vitkus, visi pabrėžė, kad trečiosios šalys, turinčios prieigą prie organizacijos

[148] Stanislav Sokolovskis (Vilniaus Rajono Savivaldybė), interviu, interviu telefonu, 2024m. Gruodžio 10d.

[149] *Ibid.*

[150] Adomas Bužinskas (Vilniaus Savivaldybė), interviu, Vilnius, 2024 metų, Gruodžio 11d.

[151] Jonas Pidkovas (Vilniaus Savivaldybė), interviu, Vilnius, 2024m. Gruodžio 4d.

[152] Adomas Bužinskas (Vilniaus Savivaldybė), interviu, Vilnius, 2024 metų, Gruodžio 11d.

sistemų, gali turėti tiesioginį poveikį saugumui. J. Pidkovas paminėjo, kad organizacija įdiegė griežtas prieigos kontrolės priemones, kad užtikrintų tiekimo grandinės saugumą.[153] D. Vitkus taip pat pažymėjo, kad organizacijos pradėjo stebėti išorinius resursus, pavyzdžiui, vykdo „web'o" stebėseną, kad nustatytų galimas grėsmes iš trečiųjų šalių, kurios gali turėti įtakos organizacijos saugumui.[154]

Visi interviu dalyviai sutiko, kad trečiosios šalys tampa esminiu saugumo iššūkiu. Tai pabrėžia, kaip svarbu investuoti į tiekimo grandinės stebėjimą ir užtikrinti, kad tiekėjai laikytųsi aukštų saugumo standartų. Taip pat būtina nuolat bendrauti su tiekėjais ir stebėti jų saugumo priemones, kad būtų išvengta galimų saugumo spragų ir apsaugota organizacijos infrastruktūra.

3.4 Pagrindiniai pokyčių indikatoriai: vadovavimas ir vadovai

Vadovų lyderystė ir požiūris į kibernetinį atsparumą yra esminiai veiksniai, lemiantys organizacijos gebėjimą efektyviai reaguoti į kibernetinius incidentus. Stanislav Sokolovski (Vilniaus savivaldybė) pabrėžė, kad vadovai turi suprasti situacijos rimtumą ir būti pasirengę investuoti į saugumą ne tik po incidento, bet ir iš anksto. Svarbu atlikti praktinius testus, tokius kaip phishingo testai, kad vadovai galėtų įvertinti grėsmių rimtumą: „Iš anksto perspėkite apie patikrinimą, o po to parodykite vadovui, kiek procentų darbuotojų neatpažino paprastų grėsmių." Tai rodo, kad praktiniai pavyzdžiai padeda vadovams įvertinti kibernetinio saugumo svarbą ir priimti reikiamus sprendimus.[155]

Deja, dauguma vadovų rimtai žiūri į šiuos klausimus tik po įvykusios atakos. Stanislovas klausia: „Ar verta laukti, kol atsitiks incidentas, kad pradėtume veikti?" Tai rodo, kad proaktyvus požiūris ir vadovų švietimas yra būtini, kad būtų išvengta situacijų, kai saugumo investicijos atliekamos tik po krizės. Jis taip pat atkreipė dėmesį, kad dažnai vadovai perkelia visą atsakomybę už kibernetinį saugumą į IT komandą, tačiau IT specialistai turi ir kitų svarbių užduočių - „IT specialistai turėtų turėti galimybę mokytis ir tobulėti, nes kibernetinis saugumas sparčiai keičiasi." Tai pabrėžia, kad tik su tinkama vadovų lyderyste organizacijos atsparumas gali būti stiprinamas ir pritaikytas nuolat kintančioms grėsmėms.[156]

Donatas Vitkus taip pat pabrėžė, kad **vadovų požiūris** yra esminis veiksnys, lemiantis jau minėtų svarbių atsparumo strategijų įgyvendinimą. Kai kurie vadovai mano, kad investavimas į kibernetinio saugumo sistemas ir ekspertus užtikrina visišką apsaugą nuo incidentų, ignoruojant

[153] Jonas Pidkovas (Vilniaus Savivaldybė), interviu, Vilnius, 2024m. Gruodžio 4d.

[154] Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

[155] Stanislav Sokolovskis (Vilniaus Rajono Savivaldybė), interviu, interviu telefonu, 2024m. Gruodžio 10d.

[156] *Ibid.*

atstatymo planų svarbą. Vadovai turi suprasti, kad incidentai įvyksta anksčiau ar vėliau, ir pasirengti ne tik atitikti reikalavimus, bet ir parengti organizaciją valdyti incidentus. Tai apima išteklių svarbą ir prioritetų nustatymą, kad būtų užtikrintas sklandus atstatymas. D. Vitkus pažymėjo, kad tik realūs incidentai padeda vadovams suprasti organizacijos silpnybes, todėl būtina nuolat testuoti atsparumo strategijas.[157] Panašų požiūrį išsakė S. Sokolovski, kuris teigė, kad vadovai turi rimtai priimti IT rekomendacijas, kad būtų pasiekta sėkmė: „Jei vadovas atsakingai žiūrės į situaciją, bus pasiekta 50% sėkmės.“[158]

Pereinant nuo rizikos valdymo požiūrio prie atsparumo grindžiamo požiūrio, svarbu tinkamai paskirstyti atsakomybes. S. Skolovski pabrėžė, kad IT ir saugumo skyriai turi būti atskirti, nes jų užduotys skiriasi. Tai padeda geriau valdyti saugumo problemas ir užtikrinti, kad komanda galėtų susitelkti į savo sritį. Nors komanda negalėjo dalyvauti seminaruose dėl darbo krūvio, dabar vykdoma spamo ir phishingo testavimai, kurie atskleidė žmogaus klaidų grėsmę: „Iš 200 žmonių apie 40% vis tiek užpildė netikras formas.“ Šiuo metu įdiegtos papildomos saugumo priemonės, tokios kaip aktyvi direktorija, kad sumažintų nesankcionuotą prieigą. Tai rodo, kad pereinant į atsparumą grindžiamą požiūrį, būtina stiprinti ne tik technines priemones, bet ir nuolatinį darbuotojų švietimą.[159]

Vilniaus savivaldybės IT ir Inovacijų komanda ir jos vadovo Jono Pidkovo patirtis rodo, kaip svarbu, kad organizacijoje kibernetinis saugumas nebūtų laikomas tik IT skyriaus atsakomybe. Tai ypač aktualu, kai dėl kasdienių užduočių IT komanda dažnai nesugeba skirti pakankamai dėmesio kibernetiniam atsparumui. Jonas Pidkovas paaiškino, kad jų komanda, skirtingai nei tradicinės organizacijos, neapsiriboja tik teoriniais principais, bet praktiškai taiko kibernetinio saugumo priemones: „Mes kuom skiriames nuo kitų truputėlį, kad mes ne pagal teoriją dirbam, mūsų komanda visa yra inovacijų ir technologijų grupė, yra visi adminai, tinklistas, darbo vietų priežiūros specialistas ir jie kaip komanda kažkiek valandų būtent skyrė kibersaugai“. Tai rodo, kad Vilniaus savivaldybė supranta IT komandos galimybes ir suformavo atskirą kibernetinio saugumo komandą, kuri skiria laiko ir išteklių šiam svarbiam darbui. Komanda neapsiriboja tik vidiniais procesais, bet taip pat pradeda plėsti savo veiklą, konsoliduodama kitų viešojo sektoriaus institucijų, pavyzdžiui, poliklinikų, kibernetinio saugumo vertinimus. Tai rodo, kad kibernetinis saugumas tampa organizacijos prioritetu, ne tik IT komandos atsakomybe, leidžiant efektyviau spręsti atsparumo klausimus ir išplėsti jų taikymą platesniame sektoriuje.[160]

Norint pakeisti vadovų požiūrį ir paskatinti juos pripažinti kibernetinio atsparumo svarbą, J. Pidkovas pabrėžė praktinių vertinimų ir pratybų svarbą, nes jos atskleidžia organizacijos

[157] Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

[158] Stanislav Sokolovskis (Vilniaus Rajono Savivaldybė), interviu, interviu telefonu, 2024m. Gruodžio 10d.

[159] Ibid.

[160] Jonas Pidkovas (Vilniaus Savivaldybė), interviu, Vilnius, 2024m. Gruodžio 4d.

pažeidžiamumą. „Tai pasitelkėm komandą, vienas iš komandos narių turėjo užduotį sutrikdyti operacijas, ir gavosi taip, kad pamatėm, kokie mes neatsparūs kaip įmonė“, – pasakojo J. Pidkovas. Šis atvejis rodo, kad organizacijai reikia tiesiogiai parodyti savo silpnybes, kad būtų paskatintas pokytis. Remdamasis šiuo įvykiu, jis paminėjo, kad nors organizacija buvo pažeidžiama, jie nesibaimino pateikti šias išvadas vadovybei, ir tai paskatino pradėti tobulinti kibernetinio saugumo praktiką. „Ir palaipsniui pradėjom žiūrėti būtent tą savo higieną, tas pradinės rekomendacijas kaip įgyvendinti“, – pridūrė jis.[161]

Be to, J. Pidkovas pažymėjo, kad, apibrėžus kibernetinio atsparumo veiksmų planą ir žingsnius, buvo galima pradėti bendradarbiauti su išorinėmis organizacijomis, kurios dalinasi gerąja patirtimi ir nustato standartus. „Stojom į organizaciją, kuri dalinasi patirtimi ir skaitosi kaip standartą apsirašius kibernetinio saugumo paslaugas savo viduje“, – sakė jis. Tai rodo, kad struktūrizuotos iniciatyvos ir bendradarbiavimas su išorės organizacijomis yra būtini norint sustiprinti kibernetinio atsparumo priemones ir priversti vadovybę matyti šio proceso svarbą.[162]

Vilniaus savivaldybė taip pat atskiria kibernetinio saugumo funkcijas nuo IT komandos, siekdama užtikrinti, kad atitikties klausimai būtų tvarkomi nepriklausomai. „Turime dalinį atitikties, atskirai prie, kuris nepriklauso nuo mūsų, arčiau prie administracijos direktoriaus“, – paaiškino J. Pidkovas. Tai rodo, kad organizacija ne tik įgyvendina prevenciją, bet ir užtikrina atitiktį teisės aktams, įdiegdama papildomą struktūrą, kurioje dirba CISO specialistas, atsakingas už teisės aktų laikymąsi ir organizacijos kibernetinės saugos stebėjimą. Toks integruotas požiūris, apimantis tiek prevenciją, tiek gebėjimą prisitaikyti ir atsigauti, yra esminis kibernetinio atsparumo planavimui ir praktikai.[163]

Vilniaus savivaldybės patirtis rodo, kad vadovų požiūris ir kibernetinio atsparumo prioritetizavimas turi tiesioginį poveikį organizacijos gebėjimui įgyvendinti efektyvias kibernetinio saugumo strategijas. J. Pidkovas pabrėžė, kad norint sukurti efektyvų kibernetinio atsparumo modelį, pirmiausia reikia turėti gerą IT vadovą, kuris galėtų nustatyti prioritetus ir strategijas. „Vadovo atsakomybė nepamesti proto ir skirti pakankamus resursus“, – sakė J. Pidkovas. Tai rodo, kad kibernetinio atsparumo užtikrinimas priklauso nuo vadovų gebėjimo apibrėžti prioritetus ir sukurti sąlygas, kuriomis specialistai galėtų veikti efektyviai.[164]

Vilniaus savivaldybė pasitelkė inovatyvų požiūrį, įsteigdama atskirą kibernetinio atsparumo skyrių, kad šis galėtų užtikrinti atitiktį teisės aktams ir suteikti daugiau dėmesio kibernetinio saugumo

[161] Jonas Pidkovas (Vilniaus Savivaldybė), interviu, Vilnius, 2024m. Gruodžio 4d.

[162] *Ibid.*

[163] *Ibid.*

[164] *Ibid.*

klausimams. Tai leidžia IT komandai susitelkti į kasdienes užduotis ir užtikrinti, kad kibernetinis atsparumas nebūtų apleistas dėl operatyvinių problemų.

Adomas Bužinskas, Vilniaus savivaldybės administracijos vadovas, taip pat pabrėžė, kad kibernetinio saugumo prioritetas kyla iš vadovų sprendimų ir gebėjimo vertinti rizikas. „Mes taip pat galvojame apie tai, kas gali atsitikti, jeigu to nebus, ir tai kyla iš vadovo atsakomybės“, – nurodė A. Bužinskas. Tai rodo, kad kibernetinis atsparumas ne tik reikalauja finansinių investicijų, bet ir nuolatinio vadovų įsitraukimo, kad būtų užtikrinta ilgalaikė organizacijos apsauga. Vilniaus savivaldybė pripažįsta kibernetinės rizikos svarbą ir investuoja į ilgalaikius sprendimus, kad atsparumo lygis būtų nuolat didinamas.[165]

A. Bužinskas taip pat pabrėžė, kad organizacija suvokia, jog negalima tikėtis greito ir lengvo sprendimo, todėl svarbu turėti išsamų kibernetinio saugumo ir atsparumo planą, kurį nuolat tikrintų ir atnaujintų. „Kiekvienas iššūkis yra kompromisas“, – sakė jis, kalbėdamas apie tai, kad vadovams reikia užtikrinti tinkamą biudžeto paskirstymą, kad būtų galima investuoti į ilgalaikes saugumo priemones. Tai rodo, kad Vilniaus savivaldybė suvokia kibernetinio atsparumo svarbą ir pripažįsta, kad tam reikalinga nuolatinė priežiūra, testavimas ir bendradarbiavimas su išorinėmis organizacijomis.[166]

Šarūnas Končius taip pat pabrėžė vadovų vaidmens svarbą kibernetinio atsparumo įgyvendinime, ypač mažose ir vidutinėse įmonėse. „Vadovas turi galėti priimti sprendimus greitai ir efektyviai, nes jeigu nepriimsi laiko sprendimų, gali atsirasti didelės problemos“ - teigė Š. Končius. Pasak jo, organizacijos turi investuoti į žmones ir sukurti kompetentingą komandą, kuri galėtų veikti kibernetinių incidentų atveju: „Organizacijos turi sukurti tinkamas komunikacijos ir veiksmų procedūras, kad greitai reaguotų į grėsmes“. Vadovų gebėjimas priimti greitus sprendimus yra esminis, norint užtikrinti organizacijos atsparumą ir pasirengimą kibernetinėms grėsmėms.[167]

Š. Končius taip pat pažymėjo, kad mažos organizacijos dažnai nesugeba užtikrinti tinkamų resursų ir pasitelkia išorinius paslaugų teikėjus, kad užtikrintų savo kibernetinį atsparumą. „Jeigu organizacija neturi resursų, ji gali pasinaudoti išorinių paslaugų teikėjų pagalba, kad pasiektų reikiamą saugumo lygį“. Tai rodo, kad kibernetinis atsparumas nėra tik vidinės organizacijos atsakomybė – jis turi būti integruotas į visą organizacijos tiekimo grandinę ir bendradarbiavimą su išoriniais partneriais.[168]

[165] Adomas Bužinskas (Vilniaus Savivaldybė), interviu, Vilnius, 2024 metų, Gruodžio 11d.

[166] *Ibid.*

[167] Šarūnas Končius (KTU Domreg), virtualus interviu, 2024m. Gruodžio 12d.

[168] *Ibid.*

3.5 Teorijos papildymas

Atlikdama ekspertinius interviu, taip pat radau vietų, kur galima papildyti teoriją. Kai kurie respondentai išskyrė keletą kritikos vietų, kurios atskleidžia naujus aspektus kibernetinio atsparumo ir rizikos valdymo srityje. Pavyzdžiui, Donatas Vitkus minėjo, kad kalbant apie kibernetinį rizikos valdymą ir kibernetinį atsparumą, reikėtų išskirti ir trečiąjį komponentą – stebėseną. Jis pabrėžė, kad be dviejų pagrindinių komponentų – atsparumo ir rizikos valdymo – stebėsena taip pat vaidina labai svarbų vaidmenį. Vitkus teigė: „Paprastai stebime, kurie išoriniai resursai yra pasiekiami internete. Pakankamai neseniai pradėjome atlikti ir „web'o" stebėseną – stebime, ką apie tave kalba forumuose, kokie slaptažodžiai nutekinti, arba kur atsiranda „Igničio" vardas."[169] Tai leidžia nustatyti, kur trečiosios šalys gali būti patyrusios ataką ir kur jau mūsų organizacijos duomenys gali būti platinami. Ši išplėstinė stebėsenos praktika yra būtina, norint turėti išsamesnį požiūrį į kibernetinį atsparumą ir nustatyti potencialias grėsmes prieš incidentą.

Vilniaus universiteto Duomenų ir Informacinės saugos vadovas Viktoras Bulavas taip pat pabrėžė, kad kibernetinio atsparumo modeliuose reikėtų atsižvelgti į platesnį požiūrį, kuris pranoktų tik kairės ir dešinės dimensijas. Jis teigė, kad šiuolaikinėje politikoje nebėra paprastos kairės-dešinės skirstymo, atsiranda trečioji dimensija, pavyzdžiui, populizmas. „Kibernetinio atsparumo modeliai turėtų apimti trečiąją ir net ketvirtąją ašis, tai galėtų apimti bendruomenių suvokimo skatinimą ir technologinio atsparumo stiprinimą."[170] Šis požiūris praplečia teoriją, įtraukiant naujus kibernetinio atsparumo aspektus, kurie gali pagerinti organizacijų pasirengimą ir adaptaciją. Ypatingai svarbus yra dirbtinio intelekto taikymas, kuris gali būti naudojamas kibernetinio saugumo srityje. Dirbtinis intelektas leidžia pereiti nuo tradicinių rizikos valdymo metodų prie automatizuotų sistemų, kurios sugeba atpažinti ir reaguoti į naujus kibernetinius grėsmes.

Donatas Vitkus pabrėžė, kad nors kibernetinė erdvė nuolat keičiasi, pagrindiniai saugumo ir atsparumo principai išlieka nepakitę. Pasak jo, žvelgiant į kibernetinio saugumo situaciją prieš trisdešimt metų, galima pastebėti, kad dauguma temų ir problemų buvo panašios, todėl radikalių pokyčių kibernetinio atsparumo srityje tikėtis nereikia. Metodai, kurie buvo naudojami anksčiau, iš esmės nesikeičia, tačiau reikia atsižvelgti į turinio, ypač susijusio su dirbtinio intelekto taikymu įvairiems kibernetiniams išpuoliams, pokyčius. D. Vitkus nurodė, kad dirbtinis intelektas gali būti pritaikytas tiek socialinės inžinerijos metodams, tiek „deepfake" skambučiams, o kenkėjiškas kodas jau gali būti sukuriamas bet kieno, naudojant tokius įrankius kaip „ChatGPT" ar kitus GPT modelius. Tuo pačiu jis pabrėžė, kad esminė problema išlieka žmonių švietimas, nes jie vis dar yra silpnoji

[169] Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

[170] Viktoras Bulavas (Vilniaus Universitetas), virtualus interviu, 2024m. Gruodžio 10d.

grandis. Nors jis nemato didelių revoliucinių pokyčių per artimiausius penkerius metus, jis akcentavo, kad reikia nuolat palaikyti atsparumo ir rizikų vertinimo praktiką, įvertinant naujas grėsmes ir ieškant būdų, kaip su jomis kovoti.[171]

Dirbtinio intelekto kontekste kyla svarbi skirtis tarp mašininio mokymo ir kalbinio modelio taikymo. Mašininio mokymo metu apmokamos AI sistemos, kad jos reaguotų ir aptiktų incidentus, tačiau vystantis technologijoms kalbiniai modeliai pradeda atlikti svarbų vaidmenį. Šie modeliai gali būti apmokomi analizuoti ir tirti kibernetinius incidentus realiuoju laiku, suteikdami papildomų apsaugos sluoksnių, analizuojant ir prognozuojant kibernetines grėsmes pagal kalbos modelius. Tai yra nauja ir vis labiau vystoma sritis kibernetinio saugumo tyrimuose, kuri gali tapti esminiu įrankiu siekiant sustiprinti organizacijų atsparumą.

Plačiau žvelgiant į kibernetinio atsparumo kontekstą Lietuvoje, šis teorijos papildymas pabrėžia būtinybę įtraukti pažangias stebėsenos praktikas ir dirbtinio intelekto sprendimus. Kadangi organizacijos vis dažniau tampa sudėtingų kibernetinių grėsmių taikiniais, svarbu suprasti, kad tiek kibernetinis atsparumas, tiek rizikos valdymas turi tobulėti, kad apimtų šias dinamiškas ir vis sudėtingėjančias technologijas. Tyrimo metu naudojama atsparumo mokslo sistema bus taikoma vertinant, kaip organizacijos įvairiuose sektoriuose, įskaitant viešąjį, privatųjį sektorius ir akademines institucijas, valdo savo kibernetinį atsparumą.

Interviu su Šarūnu Končiumi iš Kauno technologijos universiteto duomenų registro buvo naudinga ne tik analizėje apie kibernetinį atsparumą, bet ir atskleidė kai kuriuos teorijos apribojimus, kuriuos galima apibrėžti atsižvelgiant į realią organizacijų praktiką ir požiūrius. Pirmiausia, Š. Končius pabrėžė, kad kibernetinio atsparumo idėja nėra visiškai nauja ir yra tiesiogiai susijusi su jau seniai egzistuojančiais tarptautiniais standartais. Jis paminėjo ISO 27001 standartą, kuris, pasak jo, buvo pirmas, kuris išskyrė atsparumo komponentus kaip atskiras sritis – prevenciją, įsilaužimų atpažinimą ir reagavimą į incidentus. „Pati idėja šita nėra labai nauja, nes jeigu pažiūrėti, kur ji atsispindi, tai aš sakyčiau, pats ISO 27001 standartas“ - teigė Š. Končius.[172] Tai rodo, kad teorija, kuria remiasi mano tyrimas, nėra visiškai novatoriška ir remiasi jau sukurtomis ir pripažintomis struktūromis. Tai galėtų būti laikoma viena iš teorijos ribų – tai, kad ji remiasi plačiai taikytomis ir dažnai naudojamomis normomis, kurios nėra visiškai naujos.

Be to, Š. Končius pabrėžė, kad dauguma organizacijų, įskaitant KTU, daugiausia dėmesio skiria praktikai ir kasdieniam darbui su saugumo priemonėmis, o ne tik teoriniams modeliams. Jis teigė: „Mes dalyvaujame pratybose, kur patikriname, kaip veikia mūsų sistema ir kaip mūsų žmonės reaguoja į kibernetinius incidentus“.[173] Tai rodo, kad organizacijos, kaip KTU, labiau linkusios

[171] Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

[172] Šarūnas Končius (KTU Domreg), virtualus interviu, 2024m. Gruodžio 12d.

[173] *Ibid.*

naudoti praktinius metodus ir atlikti nuolatinį testavimą, o ne tik vadovautis teoriniais modeliais. Tai gali būti teorijos ribojimas, nes praktinis požiūris dažnai nesuderinamas su griežtomis teorinėmis struktūromis, ypač kai kalbama apie kibernetinio atsparumo komponentus, kuriuos teorija bando įvesti į vieningą struktūrą.

Šarūnas Končius taip pat paminėjo, kad kibernetinio atsparumo teorija turi būti lanksti ir adaptuota pagal besikeičiančias aplinkybes: „Tai yra natūralus bendradarbiavimas. Ir tu būsi priverstas kilstelėti savo brandos lygmenį iki priimtino“ - sakė Š. Končius.[174] Šis teiginys atskleidžia, kad kibernetinio atsparumo valdymo teorija, kurią aš naudoju savo darbe, turi būti nuolat tobulinama ir pritaikoma prie konkrečių organizacijos poreikių ir situacijos. Tai rodo, kad teorija nėra absoliuti ir turi būti lanksčiai pritaikyta, atsižvelgiant į organizacijos dydį, išteklius ir grėsmes, su kuriomis ji susiduria.

Be to, iš interviu galima pastebėti, kad kibernetinio atsparumo teoretikai ir praktikai dažnai turi skirtingus požiūrius. Š. Končius teigė, kad „Tai buvo padaryta gana paprastai, nes negali po šitais reikalavimais pakišti“.[175] Tai pabrėžia, kad kibernetinis atsparumas praktikoje nėra toks paprastas, kaip teoriškai apibrėžta. Nors teorija siūlo išsamų atsparumo komponentų aprašymą, reali praktika dažnai reikalauja paprastesnių ir greitai įgyvendinamų sprendimų, kurie gali nesutapti su sudėtingais teoriniais modeliais.

Galiausiai, kibernetinio saugumo įstatymo pokyčiai, kuriuos paminėjo Š. Končius, atskleidžia, kad teisės aktai taip pat yra dinamiški ir kad jie turi būti nuolat atnaujinami, kad atitiktų besikeičiančias organizacijų poreikius: „Naujoji direktyva ir įstatymas pradeda labiau orientuotis į mažas ir vidutines įmones, kad jos pradėtų rimčiau žiūrėti į savo saugumą“ - sakė Š. Končius.[176] Tai rodo, kad teisės aktai ir kibernetinio saugumo standartai nėra statiški, bet turi būti nuolat atnaujinami, kad atitiktų naujas grėsmes ir praktikas. Tai yra svarbus teorijos apribojimas, nes rodo, kad kibernetinis atsparumas ir susijusios teorijos turi būti nuolat tobulinamos ir pritaikytos realioms sąlygoms, kad būtų veiksmingos ir atitiktų nuolat besikeičiančią technologijų ir grėsmių aplinką.

[174] *Ibid.*

[175] *Ibid.*

[176] *Ibid.*

4. Išvados

Šiame darbe buvo analizuojama kibernetinio atsparumo ir kibernetinio rizikos valdymo praktika Lietuvoje, nagrinėjant, kaip organizacijos reaguoja į išorines kibernetines grėsmes bei gilinantis į jų kibernetinio saugumo praktikas bei strategijas. Tyrimo metu buvo suformuluotos dvi hipotezės. Pirmoji hipotezė teigė, kad organizacijos, kurios pereina prie kibernetinio atsparumo metodų, įskaitant išseklių paskirstymą/įvairovę, duomenų ir sistemų dubliavimą ir tarpsektorinį bendradarbiavimą, ilagalikes strategijas ir pasirengimą atakoms, geba geriau atlaikyti kibernetinius incidentus ir užtikrina ilgalaikį funkcionavimą bei prisitaikymą po atakų, palyginti su organizacijomis, kurios orientuojasi tik į grėsmių prevenciją ir mažinimą. Antroji hipotezė teigia, kad Lietuvos organizacijos vis dar daugiausia pasikliauja tradiciniais rizikos valdymo metodais, o ne investuoja į atsparumo didinimą, todėl jų gebėjimas reaguoti į kibernetinius išpuolius ir atsigauti po jų yra ribotas.

Pirmoji hipotezė pasitvirtino, kadangi tyrimas parodė, kad organizacijos, taikančios į atsparumą orientuotas strategijas, greičiausiai turės mažesnį kibernetinių atakų istoriją ar bus geriau su jom susitvarkiusios ir išlaikys ilgalaikį veiklos tęstinumą. Pavyzdžiui, Vilniaus rajono savivaldybės atvejo analizė parodė, kad po kibernetinės atakos, kuri vyko 2024 m. gruodžio 5 d., savivaldybė ėmėsi reikšmingų organizacinių pokyčių, įskaitant papildomų specialistų priėmimą ir naujo atsparumo skyriaus sukūrimą. Tai pavirtina ir parodo, kad organizacijos, kurios geba greitai prisitaikyti ir investuoti į atsparumo didinimą, sugeba veiksmingai atlaikyti atakas ir atsigauti po jų.

Antroji hipotezė, kad Lietuvoje vis dar dominuoja grėsmių valdymo metodai, pasitvirtino tik iš dalies. Nors dauguma organizacijų Lietuvoje ir toliau naudoja tradicines grėsmių prevencijos priemones, daugelis jau pradėjo pereiti prie atsparumo didinimo strategijų, ypač kalbant apie didesnes organizacijas, suprasdamos, kad išorinės grėsmės negali būti visiškai kontroliuojamos.

Tyrimas taip pat atskleidė, kad didžiausi iššūkiai išlieka susiję su žmogiškųjų išteklių trūkumu, nepakankamu vadovų įsitraukimu ir išlaidų valdymu. Tačiau tuo pačiu metu organizacijos, kurios sugeba sėkmingai valdyti ir tvarkytis su šiomis kliutimis, geriau tvarkosi ir implementuoja įvairias atsparumo strategijas bei sėkmingiau vertina save kibernetinio atsparumo srityje. **Atlikti interviu ir dokumentų analizė parodė** poreikį investuoti ne tik į prevencijos priemones, bet ir į ilgalaikį atsparumo didinimą. Kaip parodė interviu, būtina stiprinti vadovų lyderystės gebėjimus ir supratimą apie atsparumą, kad būtų užtikrintos greito reagavimo į incidentus galimybės bei minimalizuotas nuostolis. Be to, kaip pabrėžė keli respondentai – bendruomeniškumas ir bendruomenė, dalinimasis komptencijom ir praktikom taip pat gali būti išskirta kaip atsparumo aspektas. Rekomenduojama skatinti tarpsektorinį bendradarbiavimą ir keitimąsi gerąja praktika tarp organizacijų, kad būtų pasiekti geresni rezultatai kibernetinio saugumo srityje

Pagrindinės išvados rodo, kad nors Lietuvoje yra kuriama nacionalinė kibernetinio saugumo struktūra, vis dar išlieka praktinio įgyvendinimo organizacijose spragų. Šiame tyrime nustatyta, kad daugelis organizacijų, ypač mažosios ir vidutinės organizacijos, ir toliau labai pasikliauja tradicinėmis rizikos valdymo strategijomis, kuriose daugiausia dėmesio skiriama prevencijai, o ne pasirengimui neišvengiamiems kibernetiniams incidentams ir greitam atsigavimui bei veiklos tęstinumui užtikrinti.

Tyrimas rodo, kad Lietuvos kibernetinio atsparumo strategijos, nors popieriuje ir yra parengtos tvirtai, ne visada atsispindi praktikoje. Ypač daug iššūkių kelia tai, kad vis dar pasikliaujama galiojančių reguliavimo nuostatų laikymusi, o ne aktyviu ir integruotu požiūriu į atsparumą. Tyrimas taip pat rodo, kad, palyginti su geriausia tarptautine praktika, Lietuva atsilieka tokiose srityse kaip naujų technologijų, pavyzdžiui, dirbtinio intelekto, integravimas grėsmėms aptikti ir atkurti, taip pat tarpsektorinio viešojo ir privataus sektorių subjektų bendradarbiavimo skatinimas.

Analizėje taip pat pabrėžiamas nacionalinės teisinės ir reguliavimo sistemos, ypač Lietuvos kibernetinio saugumo įstatymo, vaidmuo, kuris, nors ir yra labai svarbus kuriant nacionalinės kibernetinio saugumo politikos pagrindus, turi būti toliau tobulinamas, kad būtų įtrauktos išsamesnės ir praktiškai pritaikomos gairės organizacijoms. Tarp rekomendacijų - gerinti švietimą kibernetinio atpsarumo srityje, peržiūrėti reguliavimo sistemą, kad būtų skatinamos investicijos į atsparumo priemones, ir skatinti glaudesnį sektorių bendradarbiavimą, siekiant pagerinti bendrą šalies saugumo būklę. Be to, tyrime Lietuvos organizacijoms rekomenduojama į kibernetinio saugumo sistemas integruoti adaptyvias strategijas, kad būtų galima geriau pasirengti būsimoms grėsmėms ir užtikrinti veiklos tęstinumą atakos atveju.

Šis tyrimas prisideda prie platesnio diskurso apie kibernetinį atsparumą, pateikdamas įžvalgas apie konkrečius Lietuvos iššūkius ir sprendimus. Išvadose pabrėžiama, kad svarbu neapsiriboti vien tik prevenciniu kibernetinio saugumo požiūriu, o atsparumą suvokti kaip esminį nacionalinio ir organizacinio saugumo komponentą. Šiame tyrime raginama laikytis labiau integruoto, į ateitį orientuoto požiūrio į kibernetinį saugumą, kuris suderintų prevencijos poreikį su gebėjimu atsigauti ir prisitaikyti prie vis sudėtingesnių kibernetinių grėsmių.

Tyrimo išvados taip pat atskleidžia dar vieną svarbų aspektą – kad vis dar išlieka tam tikri neatitikimai tarp supratimo ir suvokimo „rizikos valdymo“ bei „atsparumo valdymo“ terminų ir sudedamųjų dalių. Pavyzdžiui, “Ignitis” apie savivaldybės “Hack me if you can” programą labiau laikė „rizikos valdymu“, nes ji orientuojasi į pažeidžiamumų identifikavimą ir grėsmių sustabdymą, tačiau pati savivaldybė užsiminė, kad nors ir iš pradžių idėja buvo siekti surasti sistemų spragas ir jas “užlopyti”, dabar ją apibrėžia kaip atsparumo valdymą, kadangi, kaip vėliau buvo pastebėta, šiuo metu programa orientuojasi į sistemos gebėjimą atlaikyti atakas. Šis skirtumas rodo, kad nors

organizacijos gali naudoti skirtingus terminus, jų praktikos ir strategijos dažnai persipina, ir svarbu atkreipti dėmesį į šį aspektą, siekiant išvengti painiavos tarp skirtingų valdymo požiūrių.

Galiausiai, šio darbo išvados patvirtina, kad kibernetinis atsparumas ir rizikos valdymas turi būti vertinami ir taikomi kartu. Organizacijų praktika Lietuvoje parodo, kad organizacijos geba derinti šiuos du požiūrius ir išnaudoja tiek prevencijos, tiek atsparumo stiprinimo metodus, yra geriau pasirengusios atsispirti kibernetinėms grėsmėms ir užtikrinti savo veiklos tęstinumą.

Ateities tyrimams būtų naudinga gilintis į kibernetinio atsparumo ir rizikos valdymo integraciją bei tolesnį jų praktinį pritaikymą organizacijose. Galima tirti, kaip skirtingos pramonės šakos ir organizacijos, turinčios įvairius išteklius ir technologijas, pritaiko atsparumo valdymą, siekdamos efektyviau reaguoti į kibernetines grėsmes. Taip pat vertinga būtų tirti, kaip dirbtinio intelekto sprendimai gali būti integruojami į kibernetinio atsparumo modelius, ypač stebėjimo ir grėsmių prognozavimo srityje. Be to, rekomenduojama išplėsti tyrimus į mažas ir vidutines įmones, kurios dažnai susiduria su iššūkiais, susijusiais su ribotais ištekliais, ir ištirti, kaip jos gali prisitaikyti prie greitai besikeičiančių grėsmių bei išteklių (žmogiškųjų ar finansinių) trūkumu. Analizuojant praktines organizacijų patirtis, būtų įdomu įvertinti, kaip šios įmonės gali naudoti naujausias technologijas ir bendradarbiauti su kitomis institucijomis, siekdamos stiprinti savo atsparumą ir užtikrinti kibernetinį saugumą.

Literatūros sąrašas

1. Akbanov, Maxat, Vassilios G. Vassilakis, and Michael D. Logothetis. „WannaCry ransomware: Analysis of infection, persistence, recovery prevention and propagation mechanisms.“ *Journal of Telecommunications and Information Technology* 1 (2019).
2. Avast. „Avast 2023 Predictions Highlight Increase Risk for Detrimental Damage Caused By Ransomware Gangs.“ (2022). Žiūrėta 2024m. Birželio 16d. https://press.avast.com/avast-2023-predictions-highlight-increased-risk-for-detrimental-damage-caused-by-ransomware-gangs.
3. Baezner, Marie, and Patrice Robin. „Stuxnet.“ No. 4. ETH Zurich, 2017.
4. Beerman, Jack, et al. „A review of colonial pipeline ransomware attack.“ In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*. IEEE, 2023.
5. Borah, Chandra Kamal. „Cyber war: the next threat to national security and what to do about it? by Richard A. Clarke and Robert K. Knake.“ *Strategic Analysis* 39.4 (2015).
6. Boyne, George A., et al. „Problems of rational planning in public organizations: An empirical assessment of the conventional wisdom.“ *Administration & Society* 36.3 (2004).
7. Broeders, Dennis, Fabio Cristiano, and Daan Weggemans. „Too Close for Comfort: Cyber Terrorism and Information Security across National Policies and International Diplomacy.“ *Studies in Conflict & Terrorism* 46.12 (2023).
8. Chandra Kamal Borah. „Cyber war: the next threat to national security and what to do about it? by Richard A. Clarke and Robert K. Knake,“ *Strategic Analysis*, 39:4, 2015.
9. Daswani, Neil, et al. „The Equifax Breach.“ *Big Breaches: Cybersecurity Lessons for Everyone*, 2021.
10. Dearden, Lizzie. „Ukraine cyber attack: Chaos as national bank, state power provider and airport hit by hackers.“ *The Independent*, 2017m. Birželio 27. Žiūrėta 2024 Birželio 21. https://www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-computers-wannacry-ransomware-a7810471.html.
11. Europol. *2023 m. Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaita* (Internet Organised Crime Threat Assessment (IOCTA) 2023). Prieiga per internetą https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-assessment-iocta-2023.
12. Harknett, Richard J., and James A. Stever. „The new policy world of cybersecurity.“ *Public Administration Review* 71.3 (2011).

13. Krašto Apsaugos Ministerija. *Nacionalinė kibernetinio saugumo būklės ataskaita 2023m.*, Skelbta 2024m. Gegužės 21d., žiūrėta 2024 Birželio 19d. https://www.nksc.lt/naujienos/pristatyta_2023_m_nacionaline_kibernetinio_saugumo.html.
14. Krašto Apsaugos Ministerija. *Nacionalinė kibernetinio saugumo būklės ataskaita* (2023).
15. Krašto Apsaugos Ministerija. *Nacionalinė kibernetinio saugumo būklės ataskaita*, 2021.
16. Lietuvos valstybės saugumo departamentas. *Grėsmių Nacionaliniam saugumui vertinimas 2022*. 2022.
17. Made In Vilnius. „After the cyber attack, the Vilnius district municipality is already transferring the child's money.“ 2023m. Gruodžio 20. Žiūrėta 2024 Birželio 21. https://madeinvilnius.lt/en/news/district/after-the-cyber-attack%2C-the-Vilnius-district-municipality-is-already-transferring-the-child%27s-money/.
18. Milmo, Dan. „NHS Ransomware attack: what happened and how bad it is?“ *The Guardian*, 2022. Žiūrėta 2024m. Birželio 16d. https://www.theguardian.com/technology/2022/aug/11/nhs-ransomware-attack-what-happened-and-how-bad-is-it.
19. Nye Jr, Joseph S. „Deterrence and dissuasion in cyberspace.“ *International Security* 41.3 (2016).
20. Öğüt, Hulisi, Srinivasan Raghunathan, and Nirup Menon. „Cyber security risk management: Public policy implications of correlated risk, imperfect ability to prove loss, and observability of self-protection.“ *Risk Analysis: An International Journal* 31.3 (2011).
21. Tran, Chi. „The SolarWinds attack and its lessons.“ *E-International Relations*, 2021. Žiūrėta 2024 m. Birželio 21d. https://www.e-ir.info/2021/06/17/the-solarwinds-attack-and-its-lessons.
22. Williams, Bruce A. „Beyond Incrementalism, Organizational Theory and Public Policy.“ *Policy Studies Journal* 7.4 (1979.
23. Europol. *Organizuoto nusikalstamumo internete grėsmių vertinimo ataskaita 2024* (angl. Internet Organised Crime Threat Assessment (IOCTA 2024)). Prieiga per internetą https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf.
24. Lietuvos valstybės saugumo departamentas. *Grėsmių Nacionaliniam saugumui vertinimas 2022*, (2022).
25. Dunn Cavelty, Myriam & Smeets, Max. „Regulatory cybersecurity governance in the making: the formation of ENISA and its struggle for epistemic authority.“ *Journal of European Public Policy*, 30:7, 2023.

26. Kott, A., & Linkov, I. „To Improve Cyber Resilience, Measure It.“ *IEEE Computer*, 54(2), 2021.
27. Linkov, I., & Kott, A. „Fundamental Concepts of Cyber Resilience: Introduction and Overview.“ *In Cyber Resilience of Systems and Networks*, Springer, 2018, 1-13.
28. Hausken, Kjell. „Cyber resilience in firms, organizations and societies.“ *Internet of Things* 11 (2020): 100204.
29. Bortkevičiūtė, Rasa, Vitalis Nakrošis, Inga Patkauskaitė-Tiuchtienė, and Ramūnas Vilpišauskas. *Nėra to blogo, kas neišeitų į gera? Reikšmingų įvykių įtaka viešosios politikos kaitai Lietuvoje 2004-2020m.* 2024.
30. Harrop, W., & Matteson, A. „Cyber resilience: A review of critical national infrastructure and cybersecurity protection measures applied in the UK and USA.“ *Journal of Business Continuity & Emergency Planning* 7(2), 2014.
31. Bostick, T. P., Connelly, E. B., Lambert, J. H., & Linkov, I. „Resilience science, policy and investment for civil infrastructure.“ *Reliability Engineering & System Safety* 175, 2018, 19.
32. Skaitmeninės Etikos Centras. „Įdomu: Lietuva pasaulinio kibernetinio saugumo reitingo 10-tuke,“ žiūrėta 2024m. Gruodžio 26d., https://e-etika.lt/idomu-lietuva-pasaulinio-kibernetinio-saugumo-reitingo-10-tuke/.
33. Döringer, Stefanie. „The problem-centred expert interview: Combining qualitative interviewing approaches for investigating implicit expert knowledge.“ *International journal of social research methodology* 24.3 (2021).
34. ELTA. „NRD Cyber Security ir Vilniaus savivaldybė už 2,9 mln. eurų stiprins kibernetinės erdvės atsparumą,“ *LRT*, žiūrėta 2023m. Lapkričio 12d., https://www.lrt.lt/naujienos/verslas/4/2102993/nrd-cyber-security-ir-vilniaus-savivaldybe-uz-2-9-mln-euru-stiprins-kibernetines-erdves-atsparuma.
35. Vilniaus Miesto Savivaldybė. „Išskirtinis dėmesys Vilniaus kibernetiniam saugumui: entuziastai kviečiami dalyvauti konkurse ir ieškoti spragų,“ žiūrėta 2023m. Lapkričio 12d, https://vilnius.lt/lt/2024/10/11/isskirtinis-demesys-vilniaus-kibernetiniam-saugumui-entuziastai-kvieciami-dalyvauti-konkurse-ir-ieskoti-spragu/.
36. KTU. „Dėl asmens duomenų nutekėjimo per gruodžio 8 d. įvykdytą kibernetinę ataką prieš KTU,“ žiūrėta 2023m. Lapkričio 11d., https://ktu.edu/news/del-asmens-duomenu-nutekejimo-per-gruodzio-8-d-ivykdyta-kibernetine-ataka-pries-ktu.
37. LRT, BNS. „Per kibernetinę ataką nutekinti KTU duomenys pardavinėjami tamsiajame internete,“ *LRT*, žiūrėta 2024m. Lapkričio.

Summary

Cyber Resilience in Lithuania: An Analysis of Cyber Resilience and Risk Management Approaches

This thesis addresses the growing importance of cyber resilience and risk management strategies in Lithuania in response to increasingly complex and evolving cyber threats. While traditional risk management strategies have primarily focused on prevention, this research emphasizes the critical need for organizations—both public and private—to develop strategies that prioritize recovery, adaptation, and overall resilience to cyber threats. Specifically, the study investigates Lithuania's national frameworks for cyber resilience and examines how selected organizations are integrating resilience strategies to handle or avoid cyber incidents.

The research argues that as cyber threats become more sophisticated, a paradigm shift is necessary, where risk management and cyber resilience strategies work together to mitigate the impact of cyberattacks, ensuring organizational continuity and swift recovery. The study's objectives are: 1) to assess the state of cyber resilience in Lithuania; 2) to analyze the integration of resilience strategies in Lithuanian organizations, especially those that have experienced cyber attacks or have avoided them; and 3) to explore the role of Lithuania's legal and regulatory framework in supporting cyber resilience. The research methodology is primarily qualitative, utilizing interviews to gather insights from practitioners and experts in the field.

The goal of this study is to provide a comprehensive understanding of Lithuania's approach to cyber resilience and demonstrate the challenges faced by organizations in integrating effective resilience measures. Key findings show that while Lithuania has made substantial progress in creating a national cybersecurity framework, significant gaps still exist in its practical application within organizations. The study reveals that many organizations, especially small and medium-sized enterprises (SMEs), continue to rely heavily on traditional risk management strategies that focus on prevention rather than preparing for and recovering from inevitable cyber incidents.

The research supports the idea that organizations that adopt resilience-focused strategies—such as data redundancy, system backups, and cross-sector collaboration—are better equipped to withstand cyber incidents and maintain operational continuity. A notable example is the Vilnius District Municipality, which, after a cyberattack in December 2024, took significant organizational steps to enhance resilience, including hiring additional cybersecurity staff and establishing a new resilience department. This case demonstrates that organizations that can adapt quickly and invest in resilience are more capable of effectively managing and recovering from cyber incidents.

While the second hypothesis—that Lithuanian organizations still predominantly rely on traditional risk management methods—holds partially true, the study also shows that larger organizations have begun to recognize the limitations of a purely preventive approach. Some organizations, like Kaunas University of Technology, are shifting towards resilience-focused strategies, acknowledging that external cyber threats cannot be fully controlled. However, many smaller organizations continue to focus primarily on risk management, underestimating the need for resilience strategies.

The research highlights several key challenges, including a shortage of skilled human resources, insufficient managerial involvement, and financial constraints. Organizations that successfully overcome these barriers tend to implement more comprehensive resilience strategies, strengthening their overall cybersecurity posture. The study emphasizes the importance of improving leadership's understanding of cyber resilience, as this is critical for ensuring rapid incident response and minimizing losses. Additionally, the research advocates for fostering greater intersectoral collaboration and the sharing of best practices to enhance overall national cybersecurity.

The study also reveals that while Lithuania's cyber resilience strategies are solid on paper, they are not always reflected in practice. Many organizations continue to rely on regulatory compliance rather than adopting an active, integrated resilience strategy. Compared to international best practices, Lithuania lags in areas such as integrating emerging technologies—like artificial intelligence—for threat detection and recovery, as well as in fostering collaboration between the public and private sectors.

The role of the national legal and regulatory framework, particularly the Lithuanian Cybersecurity Law, is also highlighted. While it lays the groundwork for national cybersecurity policy, it requires further development to provide more actionable guidelines for organizations. The study recommends strengthening cybersecurity education, revising the regulatory framework to encourage investments in resilience, and promoting closer collaboration across sectors. It also advises that organizations integrate adaptive strategies into their cybersecurity frameworks to better prepare for future threats and ensure business continuity during cyberattacks.

This research contributes to the broader discussion on cyber resilience, offering insights into the specific challenges and solutions faced by Lithuania. It compares Lithuania's practices with global standards, emphasizing the need for a shift from solely preventive measures to a more comprehensive approach that includes resilience. The study calls for a more integrated, forward-looking approach to cybersecurity, balancing the need for prevention with the capability to recover and adapt to the rapidly evolving cyber threat landscape.

Priedas nr. 1 Interviu respondentai

Organizacijos pavadinimas	Respondentas	Pozicija
Vilniaus Universitetas	Viktoras Bulavas	Informacinių sistemų departamento direktorius
Vilniaus Rajono Savivaldybė	Stanislav Sokolovskis (Vyr. patarėjas, l. e. vedėjo pareigas)	IT skyriaus vadovas; Vyriausiasis informacijos saugumo pareigūnas (CISO)
Kauno Technologijos Universitetas	Šarūnas Končius (CISO);	Informacinių sistemų departamento direktorius
Vilniaus Savivaldybė	Jonas Pidkovas Adomas Bužinskas	Inovacijų ir technologijų grupės vadovas
Ignitis	Donatas Vitkus (CISO)	Vyriausiasis informacijos saugumo pareigūnas (CISO); Kibernetinio saugumo operacijų vadovas
Nacionalinis Kibernetinio Saugumo Centras		NKSC direktorius; Incidentų reagavimo skyriaus vadovas

Priedas nr. 2 Interviu klausimai

Remiantis hipoteze ir metodika, pateikiamas interviu klausimų sąrašas, pritaikytas įvertinti, kokiu mastu (ir ar) Lietuvos organizacijos pereina nuo tradicinio rizikos valdymo prie atsparumu grindžiamo kibernetinio saugumo modelio. Šie klausimai suformuluoti taip, kad atskleistų kibernetinio saugumo praktiką, iššūkius ir strateginius sprendimus, daugiausia dėmesio skiriant rizikos valdymo ir atsparumo strategijų palyginimui.

Pagrindiniai klausimai

1. Ar galėtumėte apibūdinti savo organizacijos pagrindinį požiūrį į kibernetinio saugumo rizikos valdymą?
    a. Ar galėtumėte teigti, kad jūsų strategijoje daugiausia dėmesio skiriama atakų prevencijai, ar taip pat greitam sistemų atsistatymui ir prisitaikymui?
2. Kaip šiuo metu jūsų organizacija vertina savo kibernetinio saugumo atsparumo lygį?
    a. Kokie rodikliai ar metrikos naudojami atsparumui vertinti ir kaip dažnai šie vertinimai atnaujinami?
3. Kokių konkrečių priemonių ėmėsi jūsų organizacija, kad pasiruoštų galimiems kibernetiniams incidentams?
    a. Ar yra įdiegtos atsarginės sistemos arba atkūrimo protokolai? Kaip apie šias priemones komunikuojama organizacijoje?
4. Kokie, jūsų nuomone, yra pagrindiniai iššūkiai pereinant nuo rizikos valdymo požiūrio prie atsparumu grindžiamo požiūrio?
    a. Su kokiomis konkrečiomis kliūtimis susidūrėte įgyvendindami kibernetinio saugumo (ar atsparumo) strategijas, jei tokių yra?
5. Ar galite pateikti neseniai įvykusio kibernetinio incidento pavyzdį, jei toks buvo, ir apibūdinti savo organizacijos atsaką?
    a. Kokia buvo išmokta patirtis ir kaip ši patirtis paveikė jūsų organizacijos kibernetinio saugumo planavimą?
6. Kokį vaidmenį jūsų organizacijos kibernetinio saugumo strategijoje atlieka atsparumas bei bendradarbiavimas su išorės organizacijomis (viešosiomis ar privačiomis)?
    a. Kaip šis bendradarbiavimas paveikė jūsų organizacijos atsparumą?
7. Ar jūsų organizacija įtraukia atsparumo didinimo planavimą į platesnę strateginę sistemą? Jei taip, kaip?

a. Ar yra specialių komandų ar resursų, skirtų užtikrinti atsparumą atakoms, ir kuo šis požiūris skiriasi nuo tradicinio rizikos valdymo?
b. Kaip jūsų organizacija sprendžia balansą tarp duomenų saugumo ir darbuotojų ar klientų privatumo? Kokią įtaką šiai pusiausvyrai turi teisės aktų laikymosi reikalavimai?

8. Kokios mokymo ar informuotumo didinimo programos padeda įgyvendinti jūsų organizacijos kibernetinio saugumo atsparumo strategiją?
    a. Ar šiomis programomis siekiama labiau skatinti rizikos mažinimą, ar jomis taip pat siekiama pagerinti atsparumą - reagavimą ir prisitaikymą po incidento?

Lyginamieji klausimai apie atsparumą ir rizikos valdymą

9. Kalbant apie jūsų organizacijos kibernetinio saugumo strategiją, ar pasakytumėte, kad ji labiau orientuota į atsparumą (tęstinumą/sistemų nepertraukiamumą ir gebėjimą prisitaikyti), ar į tradicinį rizikos valdymą (atakų prevenciją ir žalos mažinimą)?
    a. Kokie pagrindiniai veiksniai lemia tokį orientavimąsi?
10. Kokią konkrečią atsparumo praktiką, pavyzdžiui, atsarginių kopijų sistemas, reagavimo protokolus ar tarpžinybinį bendradarbiavimą, įgyvendino jūsų organizacija, kad užtikrintų veiklos tęstinumą atakos metu?
    a. Kaip manote, kiek veiksminga ši praktika, remiantis ankstesniais incidentais?
11. Kokios praktikos, jūsų nuomone, padeda užtikrinti organizacijų, kurios sėkmingai susidoroja su kibernetiniais incidentais ir patiria minimalius trikdžius, atsparumą?
    a. Ar manote, kad tai yra praktika, kurią jūsų organizacija galėtų pritaikyti, o gal yra priežasčių, dėl kurių ji netaikytina?
12. Priešingai, kodėl, jūsų nuomone, kai kurios organizacijos patiria didelį poveikį kibernetinių išpuolių metu, o kitoms pavyksta išvengti didelių trikdžių?
    a. Ar, remiantis jūsų patirtimi, tai visų pirma susiję su išteklių, planavimo ar reagavimo strategijų skirtumais?

    Kaip jūsų organizacija pasiruošusi reaguoti į galimus naujų technologijų kibernetinius iššūkius per ateinančius penkerius metus?

Su valdymu ir politika susiję klausimai

13. Kaip Nacionalinis kibernetinio saugumo centras (NKSC) daro įtaką jūsų organizacijos kibernetinio saugumo politikai ar atsparumo strategijoms?
    a. Ar NKSC gairės paskatino kokius nors konkrečius pokyčius, susijusius su kibernetinio saugumo incidentų valdymu?
14. Kaip vertinate naujausius Lietuvos kibernetinio saugumo įstatymo pakeitimus ir kaip jie veikia jūsų požiūrį į atsparumą?

    a. Ar manote, kad šie pakeitimai remia atsparumu grindžiamą požiūrį, ar jie ir toliau labiau orientuoti į tradicinį rizikos valdymą?

15. Ar jūsų organizacija privalo pranešti NKSC apie kibernetinius incidentus? Jei taip, kaip tai veikia jūsų kibernetinio saugumo planavimą ir reagavimą?
    a. Jei pranešti neprivaloma, ar manote, kad savanoriškas pranešimų teikimas galėtų būti naudingas, ar yra trūkumų?
16. Kokios, jūsų požiūriu, yra pagrindinės Lietuvos bendros kibernetinės politikos sistemos stiprybės ir silpnybės, susijusios su atsparumo palaikymu?
    a. Kokius patobulinimus siūlytumėte, kad būtų padidintas nacionalinis atsparumas, ypač viešojo ir privačiojo sektorių bendradarbiavimo srityje?

Baigiamieji klausimai

17. Apmąstydami savo patirtį, ką patartumėte kitoms Lietuvos organizacijoms, norinčioms padidinti savo kibernetinio saugumo atsparumą?
    a. Ar manote, kad atsparumo strategijos užtikrina geresnius rezultatus nei tradiciniai į riziką orientuoti metodai?
18. Kokie, jūsų nuomone, yra esminiai veiksniai, padedantys įgyvendinti veiksmingą atsparumo strategiją Lietuvos kontekste?
    a. Ar šie veiksniai yra pasiekiami pagal dabartinę politikos sistemą, ar jiems reikia papildomos reguliavimo ar išteklių paramos?

Šiais klausimais siekiama atskleisti įžvalgas apie tai, kaip organizacijos pereina prie atsparumo, nustatyti sėkmingas atsparumo strategijas lemiančius veiksnius ir suprasti nacionalinės kibernetinio saugumo politikos įtaką vietos praktikai.

Priedas nr. 3. Interviu transkribcijos

Donatas Vitkus (Ignitis), Interviu, Vilnius, 2024m. Lapkričio 19d.

Dominyka: Taip, tai jau įrašinėju. Man tai pirmasis mano klausimas ir būtų būtent kalbant, jei lyginčiau Igničio grupės kaip organizacijos kibernetinio saugumo strategiją, ar labiau pasakytumėte, kad ta strategija orientuota į atsparumą, tai tą tęstinumą, sistemų nepertraukiamumą, gebėjimą labai greitai prisitaikyti prie atakos ir po jos atsigauti, ar vis dėl to labiau dominuoja požiūris į tradicinį grėsmių / rizikos valdymą, būtent atakų prevenciją ir tą žalos mažinimą, kad apskritai jos nebūtų?

Donatas: Sunku išskirti, ką reikia labiau, nes mūsų strategija orientuota ir į prevenciją - grėsmių aptikimą, užkardymą ir atsparumą, taip pat- veiklos tęstinumą, užkardymą, atstatymą, atsaką į ataką. Tai aš sakyčiau, nu ir į tą ir į tą;

Dominyka: tokia kombinacija, kad nėra išskiriama, kad vienas svarbiau, bet abu yra pakankamai svarbios dalys?.

Donatas: Jo, prioriteto nėra kažkuriam vienam

Dominyka: supratau. Supratau ačiū. O tada antras klausimas būtų: kaip apskritai šiuo metu vertintumėte savo organizacijos kibernetinio atsparumo lygį? Galbūt yra tam tikri netgi rodikliai, kuriuos išskirtumėte, kaip apskritai vertinate?

Donatas: O pagal ką matuotume?

Dominyka: Sakyčiau, aš, kadangi neturiu to techninio supratimo…

Donatas: jo, bet kaip bandome įvertinti, ar 10 balų sistemoje…?

Dominyka: turbūt pagal tikslus, kuriuos esate išsikėlę ir kiek esate įgyvendinę, bet su tikslu, kad va taip turėtų būti strategijoje.

Donatas: Sakyčiau tarp 75-80, 85 proc. Didelę dalį esame pasidarę, dar šiek tiek trūksta pilnam padengimui taip, kaip mes matytumėme, kad reikia pasidaryti dar šiek tiek trūksta.

Dominyka: Supratau: o tada gal turite kažką, ką išskirtumėte kaip pagrindinės tas atsparumo, kibernetinio saugumo dalis, ką tikrai organizacijos turėtų turėti šitoje srityje?

Donatas: Reikėtų turėti pirmiausia tai poveikio veiklai vertinimus (angl. Business impact analysis), analizes su aktualiais rodikliais - tai yra kritiniai procesai, kritiniai resursai, palaikantys procesai, palaikantys resursai. Tada indikuotos <RPO ir RTO> reikšmės - atstatymo laikas ir “Recovery Point Objective”. Iš to turi sekti veiklos tęstinumo planas, kur numatyti alternatyvūs veikimo būdai, poveikio mažinimo būdai, komunikacija, krizių komunikacija ir lygiagrečiai statymo planas (angl. disaster recovery). Tai yra detalios instrukcijos, kaip atstatyti, kur guli “backup’ai”, kokios instrukcijos, kokie prisijungimo duomenis. Tai nu, aš matyčiau, ką turėtų turėt. Aš manyčiau, kad mes visus tuos dalykus turim, bet dar kai kai kuriuos planus reikėtų atnaujinti.

Dominyka: Supratau. O jie (planai), neatnaujinami yra tiesiog, nes tam tikrų resursų ar ir išteklių nėra, ar tiesiog?
Donatas: jo tai viena prie viena priežasčių yra riboti resursai, bet čia bet kuriuo atveju yra kasdienybė, tiesiog yra prioritetų klausimas. Toliau, pačioje organizacijoje yra irgi prioritetų klausimas, dėl ko konkretūs resursai neskiriami tiems kažkokiems atnaujinimams. Kai kuriose įmonėse ir pokyčių buvo, tai tame pokyčių etape nevyko kažkokie atnaujinimai. Tai tiesiog tas užsitęsė laike.
Dominyka: Labai logiška, supratau ačiū. Tuomet dar norėčiau jūsų paklausti - kalbant apie konkrečias priemones, vėlgi, kokias organizacija imasi, tai, kokios buvo konkrečios priemonės, kurių organizacija imtųsi, kad pasiruoštų galimiems kibernetiniams incidentams? Čia gal konkrečiai kalbant, irgi aš labiau domiuosi vat prieš du metus buvo visai nemaža DDoS ataka, kurios auka irgi buvo ir „Ignitis“. Taip pat skaičiau, kad metų pradžioje vėlgi buvo vykdyta ataka prieš vieną iš grupės įmonių, dirbančių su saulės elektrinėms. Ataka labai gerai buvo atlaikyta. Man labai įdomu, iš tiesų, kokios priežastys, ko imasi organizacija, kad pati irgi pakankamai neblogai suvaldo šias grėsmes?

Donatas: Jo - tai priemonės, kurių imamės, aišku, yra planai ir planų testavimai, kai DDoS visada buvo įvardintas kaip galima grėsmė. Tiktai su DDoS, žiūrint iš techninės pusės, yra toks niuansas, kad yra pakankamai sunku. Gali ištestuoti, bet tas testavimas bus testavimas - ne reali ataka. Tai tuos scenarijus tu žinai, ką daryti, kai įvyksta DDoS ataka. Šiuo atveju tas suvaldymas jau turėjo būti mūsų interneto tiekėjo pusėje, duomenų centre. Ne pas mus. Atakos dydis buvo toks, kad tiesiog įprastai jau organizacijos tokių atakų nebevaldo, jos yra valdomos jau prieš organizaciją. Ir tos priemonės pas mus jos buvo suplanuotos, ir mes žinojome, kad tai turi suveikti, o praktika parodė, kad jos nesuveikė. Tai dėl to tai viena iš priežasčių, dėl ko tas DDoS buvo prieš du metus. O ką mes po to ėmėmės, tai nuolatinę stebėseną, 24-7h. Ji jau buvo ir iki to, nes po karo Ukrainoje pradėjom tą dalyką daryti. Tai mes pastebėjome pirmi pastebėjome <ataką>. Tiesiog srautas toks didelis, kad mūsų turimom priemonėm to suvaldyti nebegalėjom. Dabar, kalbant apie “Ignitis ON”, ten buvo ne DDoS ataka, ten buvo nutekinti slaptažodžiai. Tiesiog dėl žmogiškojo faktoriaus, pavadinkime, taip neatsargiai žmogus pasielgė - slaptažodis liko pas piktavalius, ir tiesiog po to buvo panaudoti.
Dominyka: Supratau dar kaip tik prie to paties skaičiau dabar, irgi rugsėjo mėnesį buvo straipsnis, kad buvo dar vieną ataka, kur „Ignitis“ irgi labai gerai atsilaikė prieš šitą.
Donatas: Tai čia analogiškus atvejis kaip su “Ignitis ON”. Tam, kad suprasti, tai pas mus yra keturi su puse tūkstančio darbuotojų ir d arome stebėseną dark web’o, monitoringo, visų slaptažodžių, ten tiek mūsų, tiek mūsų klientų “nuleakint’u” randam tikrai daug. Bet niekada šimtu procentų neužtikrinsi, kad sistemos būtų saugios. Tai, kas atsitiko rugsėjį, lygiai taip pat slaptažodis kažkur dark web’e plaukiojo, vėlgi - prisijungta, bet ten tiesiog poveikio nebuvo, nes tiesiog sistemą ties skirta ne valdymui, o monitoringu, stebėsenai, tai daugiau tokių reputacinė žinutė buvo. Bet vėlgi

priežastis tėra slaptažodžio nutekinimas, tiek “Ignitis ON”, tiek “I Solar” cloud’as (sistema), jos yra ne mūsų valdomos. Mes jas perkame, kai yra trečiųjų šalių, “klaudinės” paslaugos, kažkokių kitų produktų. Tai mūsų vat „Ignitis“ montuoja saulės elektrinės, o tam, kad galėtų stebėti didžiųjų klientų darbą, teikti pagalbą, inverterių gamintojas duoda įrankį, kuris iš saugumo pusės nėra pakankamai saugus, nes neturi dviejų faktorių autentifikavimo. “Ignitis ON” lygiai taip pat - stotelių tinklas yra mūsų, bet jų valdymas yra kito įrankio pagalba, kurį ne mes valdome. Tai tiesiog tokių išorinių įrankių negalime sukontroliuoti ir techninėm priemonėm apriboti.

Dominyka: Supratau tai vat čia vienas iš darbe mano irgi tiriamų tokių dalių yra, kad čia gaunasi vat ir yra tas, kad yra kibernetinės grėsmės ir yra tos išorės grėsmes ir šitoje vietoj, ką jūs šnekate, tikriausiai yra ta dalis, kur labiau reikia tada kreipti dėmesį šitoje vietoj kaip tos sistemos gali atsistatyti ir neturėtų tokio didelio poveikio. Jeigu nesuvaldysi.

Donatas: Pritariu nutūpėme jau šimtu procentų saugių sistemų nėra. Incidentas vis tiek įvyks. Klausimas, kaip greitai sureaguosi, kaip sukoordinuos darbus viduj, kaip iškomunikuosime, kaip atsistatysi iš po to incidento.

Dominyka: Aišku, ačiū. Tuo pačiu - kalbant, va tada apie tą, vėlgi, minėtą kibernetinį atsparumą ir kibernetinį saugumą grėsmių valdymą, tai, jūsų nuomone, kokie pagrindiniai iššūkiai pereinant nuo to rizikos grėsmių valdymo strategijos požiūri,o prie to atsparumo grindžiamo požiūrio. Ar čia iš tiesų, kaip aš išskyriau, kad yra perėjimas nuo vieno prie kito? Bet jūs minėjote, kad organizacija naudoja tam tikrą derinimą. Tai gal aš irgi tokį parašiau klausimą, kad yra iššūkiai, bet galbūt jų nėra? Galbūt tai tiesiog yra papildymas vienas kito?.

Donatas: Apie mūsų organizacija, tai perėjimo nebuvo, nes mes tiesiog visada, kiek aš pamenu, nuo pat pradžių statėme taip kad yra prevencija, aptikimas ir korekcinių veiksmai, atsistatymas. Visa strategija visada primenu nuo A iki Z, nuo aptikimo, nuo prevencijos aptikimas ir atsistatymas. Kitose organizacijose, kiek man tenka ar tekę matyt, bet kai taip iš kitų organizacijos organizacijų patirčių aš galėčiau išskirti, kad pagrindinis trikdis, tai yra vėlgi vadovų galvose, manant, kad jeigu aš jau investavau daug į kibernetinį saugumą, nusamdžiau geriausius ekspertus, supirkau brangiausią įrangą, kad incidento neatsitiks ir esu apsisaugojęs. Ir čia jokių atstatymo planų nereikia.

Dominyka: Labai sutinku šitoje vietoje. O tada, manot, kalbant apie tuos organizacijų iššūkius, jeigu organizacija imasi, tarkim, kibernetinio atsparumo strategijos didinimo ir gerinimo, įgyvendinimo, ar esat susidūręs, nebūtinai iš savo, bet iš kitų organizacijų, kokie dažniausiai iššūkiai būna, jeigu organizacijos, tarkim, nori, labiau suinvestuot dabar pinigus?

Donatas: Didžiausi iššūkiai yra vadovų dėmesys. Reikia “impact analysis” padaryti, poveikio veiklai vertinimą ir net jau čia pradedant daryto poveikio veiklai vertinimą,vadovai nenori įsitraukti. Reikia skirti laiko, “brainstorm’o” sesijų tam, kad identifikuoti, kokie resursai kritiniai. Tai vienas iš iššūkių,

kad vadovai to dėmesio nenori skirti, ir čia tada viskas gali pagriūti, nes ekspertai įvertins taip, kaip jie supranta poveikį veiklai. Jeigu neteisingai vertini - neteisingi prioritetai.

Dominyka: O kaip jūs suprantate patį poveikį veiklai?

Donatas: Tai yra tiesioginis poveikis dėl kažkokių sustojusių procesų. t.y. negautos pajamos, baudos, nuostoliai, ir tą žino tiktai verslas. Mes galime padėti užvesti ant kelių. Tarkim, įvyksta DDoS, neveikia savitarna, ir tiktai jau pats verslas galės žinot, verslas, aukštesnio lygio vadovus gali žinot, o ką tai reiškia įmonėje. Tarkim, šeštadienį neveikė savitarnos portalas. Arba didesni kokį objektą, kokia nors elektrinė. Kas, jeigu neveikia, vat nebegalime valdyti, kokį nors elektrinės katilą? Ką tai mums reiškia? Aš tai sakau dėl to, kad jei kaip mes, kaip prieš darydami pas save, prieš keletą metų, aš kažkaip galvojau, kad aš puikiai suprantu tą poveikį. Bet pasikalbėjusi su vadovais supranti, kad toli gražu ir tada tu žinai, kiek ką reiškia elektrinis stabdymas. Ką reiškia paleidimas, ką reiškia negaminti, tarkim, elektros priekinėm valandom ir pan.. Visai kitoks tas vertinimas. Ir tada tu jau sudėlioji prioritetus taip, kaip jie turėtų būti pagal poveikį verslui, veiklai. Ten, kad ten kokie nors Outlook neveiks, team'sai neveiks…Kas jiems..

Dominyka: Jo čia turbūt va tas ir yra įdomu, kad jūsų organizacija dar įtraukta į tą ypatingos svarbos infrastruktūrą, ir tikriausiai tas poveikis veiklai iš vienos pusės "outlookas" būtų nesvarbu, bet iš kitos pusės, jeigu kur nors kitur, ne ten nueitų ta ataka, tai tada tikrai didelis poreikis. Supratau, ačiū už išsamų atsakymą.

Prie to paties - tada norėčiau dar paklausti: Tai vat kokį vaidmenį būtent organizacijai ir ypač kai „Ignitis" yra kritinė infrastruktūra, kibernetinio, būtent, saugumo, arba šturmo, strategijose, sudaro bendradarbiavimas su išorės organizacija, tiek ir su viešom, ir privačiom, su kibernetinio saugumo centru ar yra jis kažkoks? Tikriausiai yra kažkoks vaidmuo šitam. Bet mano klausimas būtų koks?

Donatas: Pirmiausia jo, bendradarbiaujam su Nacionaliniu kibernetinio saugumo centru, Krašto apsaugos ministerija - tai čia pagrindiniai, pagrindinės šalys, su kuriomis mes bendradarbiaujame. Visa kita yra daugiau toks ekspertinio lygio bendradarbiavimas. Su kokia nors <neišgirdau>. Bendradarbiaujame su Lietuvos kariuomene, bet tas bendradarbiavimas ekspertiniame lygmenyje. Ne dėl to, kad čia įstatymai įpareigoja. Tai taip pasakyčiau.

Dominyka: O tada pasigilinant - tai šitoje vietoj gaunasi, kad ekspertiniam lygmenyje bendradarbiaujat labiau siekiant kažko išvengti. Be o, pavyzdžiui, jeigu įvyksta ataka, tarkim, tai ar būna koks nors <bendradarbiavimas>? Yra galiausiai protokolai?

Donatas: Jeigu įvyksta ataka… Jo, tai, tai mes bendradarbiavome gal daugiau tokioj prevencijos srityje - keitimosi gerąja praktika, dalyvavimui kibernetinio saugumo pratybose, o incidento atveju iš vienos pusės yra du, matyt, instrumentai, kuriuos galėtumėme pasitelkti - tai ekstra atveju Lietuvos kariuomenė ir ryšių batalionas, ir po to prie Krašto apsaugos ministerijos yra Europoje tiksliai

neįvardinsiu, bet greitojo reagavimo komanda. Nu ir NKSC, mes jau pagal įstatymą privalome informuoti.

Dominyka: Supratau, o čia dar šiek tiek užbėgsiu klausimams už akių, bet, jūsų manymu, vat tas kibernetinio saugumo centras, ar apskritai tas Nacionalinio kibernetinio saugumo įstatymas, jisai labiau žiūri ir nustato gaires prevencijai, kad išvengti atakų? va tas keitimasis gerosiom praktikom. Ar labiau tai yra vis tiek būtent nurodo ir padeda susidėlioti atsparumą, tuos punktus apie tai, kas įvykus atakai <vyktų>, aip turėtų veikti, kad tas keitimasis informacija, kad greičiau atsistatytų.

Donatas: Daugiausiai, mano nuomone, nustato daugiausiai prevenciją, tai nustato reikalavimus, priemones.

Dominyka: Manote, kad reikėtų papildyti?

Donatas: Sunku atsakyt.

Dominyka: labiau gal perfrazuosiu klausimą, ar to, kas yra dabar, užtenka, ar būtų tam tikrų dalių, sričių, kaip, tarkim, kibernetinis atsparumas, ką reikėtų įtraukti?

Donatas: Iš žvelgiant iš mūsų organizacijos, tai aš sakyčiau, užtenka, nes mum tai jokios įtakos neduotų. Mažom įmonėm gal tai būtų pagalba.

Na dabar, ką turime dabartiniame reguliavime, tai, kad organizacija turi turėti veiklos tęstinumo planą, statmenį, bet nėra detalizuojama, kas joje, kas juose turėtų būti arba kaip turėtų atrodyti geras tas planas. Kažkokių gairių, kaip ji pasirinkti.

Dominyka: Supratau.

Donatas: tai dažnai tie planai būna tokie formalūs, kur, atsitikus kažkokiam incidentui, į juos net nežiūrima.

Dominyka: Supratau aišku. Ačiū. Tada turėčiau sekantį klausimą - kaip ir aptarėme, kad „Ignitis“ grupė kaip organizacija įtraukia abu tiek atsparumą, tiek tą kibernetinių grėsmių valdymą, prevenciją į savo strategiją. Kalbant apie tą tikriausiai platesnę strategiją, tai tik pasitikslinimui, tai vėlgi ir būtų tikriausiai ta platesnė strategija, kuri susidaro iš tų dviejų komponentų? Ar vis dėlto, kai vat atrodo ta platesnę kibernetinę strategiją jūsų organizacijos?

Donatas: Jo yra šitie du komponentai. Dar trečias, gal pridėčiau: stebėseną. Išplėstinė, t. y. pažeidžiamumų paieškos, atakų ploto identifikavimas, t.y. ieškai, kokie išoriniai resursai pasiekiami internete. Pakankamai neseniai pradėjome daryti dar “web’o” stebėseną. Žiūri, ką apie tave kalba kažkur forumuose, kokie slaptažodžiai nutekinti, arba kur tas “Igničio” vardas atsiranda. Galbūt kažkur trečiosios šalys patyrė ataką, duomenys jau mūsų plaukioja. Tai mes dar šitą esam prasiplėtę.

Dominyka: o čia dabar įsivardytų, labiau vis tiek kaip kibernetinių grėsmių valdymas?

Donatas: Jo, jau jeigu tai priskirti - prie grėsmių valdymo.

Dominyka: Supratau mano, kaip tik sekantis klausimas turėjo būti - kaip visa organizacija sprendžia balansą tarp būtent duomenų saugumo ir to bandymo aptikti tas grėsmes visas ir nuolatinės tos

stebėsenos, ir būtent darbuotojų klientų privatumo? Bet čia tikriausiai, jūs ką kalbat, tai yra atskiras resursas kaip grupė, kuri stebi išorės dalykus. Nei nei klientų, nei darbuotojų čia nėra?

Donatas: Balansas tarp klientų darbuotojų privatumo - tai iš išorinių grėsmių, išorinių grėsmių aptikimui tai įtakos neturi, nes mes nerenkame papildomos informacijos nei apie darbuotojus, nei apie klientus. Tai aš sakyčiau, mes žiūrime duomenis, kurie jau dabar yra viešai prieinami. Nerenki papildomos informacijos, kuri galėtų, arba esamos informacijos, nei kategorizuoji, nei profiliuoji, iš tos vidinės informacijos, jos papildomai neagreguoji, renkant tik tai, kas yra prieinama iš išorės.

Dominyka: Tai šitoje vietoj gaunasi, kad grėsmės klientų duomenims ne tiek yra, kiek, realiai, vat tam nepertraukiamam elektros tiekimui ir pačiai sistemų veiklai?

Donatas: Grėsmes apie klientų duomenis renkame. Jeigu pastebime, kad yra nutekinta klientų duomenis, tai mes informuojame klientą, kad reikėtų pasikeisti slaptažodį. Tai, bet jo privatumas niekaip nėra įtakojamas. Mes nerenkame apie apie klientą duomenų arba apie darbuotoją duomenų. Mes renkame duomenis,iInformacija, kuri turi raktažodžių su mūsų interneto adresais, savitarna arba kitais resursais, IP adresais, domenais - tai techninė informacija ir šalia tokios informacijos randi, kad pardavinėjamas kokia nors didelė duomenų bazė, kurioje yra daug įrašų, tame tarpe ir <Igničio> klientų duomenų. Dešimt kokių klientų.Tuos klientus informuoja, kad reikia pasikeisti slaptažodį arba darbuotojams automatiškai tada. Aš kaip suprantu, klausimas yra balanso tarp grėsmių žvalgybos ir poveikio privatumui, tai vidinės žvalgybos mes nedarome, tai to poveikio privatumui kaip ir nėra. Tas balansas išlaikytas.

Dominyka: Čia mano pagrindinis klausimas buvo iš to, kad viena iš iššūkių tarp kibernetinių grėsmių valdymo, aš iškėliu, kad tas balansas ir tas iššūkis su tais duomenimis dirbti ir nepažeisti tam tikrų teisės aktų ir panašiai <etiškumas>, Tai mano klausimas dabar buvo labiau orientuotas į tai ar tai yra iššūkis, ar ne? Bet aš, kaip suprantu, ne?

Donatas: Ne nėra, nes tiesiog mes disponuojame viešai prieinama informacija.Tą pačią informaciją renka NKSC, kartais irgi mus informuoja.

Dominyka: Supratau, supratau. Dar norėjau paklausti - kalbant apie mokymo ir informatumo didinimo programas, tai kokios tos mokymo ir informuotumo didinimo programos padėjo, padeda įgyvendinti jūsų organizacijos kibernetinio saugumo / atsparumo ta strategiją? Arba nebūtinai kibernetinio atsparumo, bet apskritai kaip tos strategijos prisideda prie jūsų tos visos strategijos?

Donatas: Jo, tai mes turime tik kelis metodus, pavadinkime, taip - yra privalomi mokymai visiems darbuotojams, naujai priimtiems darbuotojams, kurie yra kasmetiniai, reguliarūs, na tokie baziniai info saugos mokymai visiems, jie yra reguliarūs. Tada turime visiems darbuotojams “phishingo” testus. Tada turime specifinius mokymus pagal pareigybes, ten administratoriai ir įvairių tų kritinių renginių inžinieriai.

Ir kas veikia, tai veikia, iš tikrųjų, praktiniai dalykai. Veikia “phishingo” simuliacijos. Karts nuo karto padarom sužaidybintus mokymus. Dažniausiai čia būna spalį, kaip kibernetinio saugumo mėnesio iniciatyva - tai įvairūs USB <flėšiukų> palikimai, perdavimai, stebėsena, ką su jais daro arba viktorinos esam darę, darėm protmūšius. Tai tokie praktiniai dalykai labiausiai veikia, nes ir po to, darant <fišingo> simuliacijas po tokių sužaidybintų mokymų tas “pakibusių” darbuotojų skaičius krenta.

Dominyka: Supratau, labai įdomu, pirmą kartą, tiesą sakant, girdžiu, apie tokias smagias veiklas. Supratau, o tada kyla klausimas - Šitas visas veiklas ir jų rezultatus, vaisius priskirtumėte labiau, kad tai didina organizacijos tą atsparumą ar labiau būtent prevenciją, grėsmių išvengiama?

Donatas: Prevencija. Beveik visos situacija yra prevencija. Kas didina atsparumą, tai didina veiklos tęstinumo planų testavimai ir atstatymo planų testavimai. Panašiai kaip ir su evakuoacijom. Evakuacijas, tarp kitko, irgi darom kartą per ketvirtį. Visas ofisas išsievakuojam su gaisro signalu. Tai tu jau žinai, ką daryti. Tai darome testavimus veiklos tęstinumo ir atstatymo planus.

Dominyka: Supratau ačiū, bet tikrai įdomus pasiruošimas.Labai toks įdomus požiūris į tą informuotumo didinimą. Tada mano irgi pakankamai platus klausimas. Bet irgi labai norėjau paklausti - kaip jūs, organizacija yra pasiruošusi reaguoti į galimus naujų technologijų kibernetinius iššūkius per būtent ateinančius penkerius metus? Ar čia gal siejant su tuo, kad ta kibernetinė erdvė labai greit keičiasi ir vystosi, ir vat įdomu, ar turite kažkokį pasiruošimo planą?

Donatas: Jo, kažkokio atskiro plano nėra, bet čia keli momentai yra. Taip, kibernetinėje erdvėje jinai keičiasi, bet principai saugumo ir atsparumo yra tie patys. Pažiūrėti, kas buvo apie kibernetinį saugumą kalbama prieš kokius trisdešimt metų, tai labai panašius dalykus visi kalbėjo ir darė, rašė, tai kažkokio perversmo tame nebus. Nu metodai tie patys. Tiktai turinį reikia žiūrėti. Kalbant iš to turinio perspektyvos, tai greičiausiai reikės įvertinti dirbtinio intelekto pritaikymą įvairiom atakom. Socialinės inžinierijos metodui, “deepfeiko” skambučiam ir t. t.. Taip pat reik įsivertinti, kad atakos, ar ten “cybercrimas”, ar “ransomware”, daro prieinamą tokias atakas bet kam. Taip pat kenkėjišką kodą, matyt, gali jau parašyti irgi bet kas su kokiu nors su kokiu “ChatGPT” ar kokių nors kitų GPT. Tai į šitą reikia atsižvelgti. Bet ar čia kažkokio perversmo tame reik, matyt, tiesiog reikia ir vienu ir kitu atveju reikia edukuoti žmones. Žmonės vis dar silpnoji grandis ir greičiausiai taip išliks. Tai aš kažkaip kažkokios revoliucijos per artimiausius 5 metus nematyčiau, kas kas keistų labai viską. Iš esmės tai tiesiog reikia palaikyti. Kokios grėsmės yra tai kaip darai grėsmių analizę, rizikų vertinimą, taip ir toliau darai ir tiesiog atsižvelgia į naujas grėsmes ir ieškai priemonių, kaip suvaldyti.

Dominyka: O vat grėsmių analizės ir tas strategijas jūs darote patys? Ar vadovaujatės tuo, ką paruošia?

Donatas: Mes darome patys, bet kaip šaltinį, tu vis tiek paėmi NKSC. Nors gal mažiau aktualus. Bet ten kokį ar ENISA "threat analysis" tai pasižiūri. Kokios tos grėsmės yra, pasižiūri, kas aktualu tavo organizacijai iš buvusių incidentų, įvykių kažkur.

Dominyka: O kodėl, kodėl sakote, kad ne taip aktualu kibernetinio saugumo centro?

Donatas: Jie daro apžvalgą buvusių metų. Apibendrina realiai apibendrintus duomenis, kuriuos mes jiems patys pateikiam. Kalbant apie energetikos sektoriumi, tai gali pasakyti, kiek įvyko incidentų energetikos sektoriuje. Tarkim, kokia nors ENISA pasisako, kas tikėtina, kad bus aktualu, ateinačiais metais.

Dominyka: Supratau, ją suskaičius. Aišku, Ačiū. Dabar turiu keletą klausimų būtent apie atsparumą, rizikos valdymą, techniniai apie pačią strategiją. Šiek tiek mes aptariamė, bet taip dar užtvirtinant - tai būtent kokią konkrečią atsparumo praktiką, sakytumėte, kad jūsų organizacija įgyvendina, kad užtikrinti būtent tą veiklos tęstinumą, tą nepertraukiamumą? Iš esmės ir yra tas atsparumas.

Donatas: Tai poveikio veiklai vertinamos veiklos tęstinumo planai, atstatymo planai. Tai čia ta procedūrinė dalis. Technologinė dalis, tai kritinių resursų dubliavimas. interneto ryšio dubliavimas, duomenų centrai dubliuoti. Alternatyvūs interneto tiekėjai, tada turi užsitikrinti, kad duomenų centrai, sistemos veiktų ten dėl elektros nutrūkimų, vėdinimo ir panašiai. O atsarginės kopijos, karštos atsarginės kopijos, archyvinės atsarginės kopijos, atsarginės kopijos kažkur tai debesyse, jeigu čia kažkas Lietuvoje nutiktų, ir tada testavimas - tų kopijų atstatymas, planų testavimas, kad darbuotojai žinotų, kaip reikėtų reaguoti, tai čia su planais. Prie atsparumą dar priskirčiau būtent tiek, kiek mes čia kalbame, tai incidentų valdymo planas - nuo aptikimo arba raportavimo incidentui. Tai yra vidinė komunikacija, tiek atsakingi žmonės, kas ką turi informuoti ir kiek laiko. Pratybas dėl kibernetinio saugumo galima pridėti, treniruojiesi. Ir treniruojasi nuo incidentų ir incidentų aptikimo analizę, bet ir valdymą, tą komunikacinę dalį.

Dominyka: Supratau, supratau. Aišku. O kai kaip manote, kiek veiksminga ši praktika žiūrint į jūsų tuos incidentus iš praeities, remiantis ankstesniais incidentais?

Donatas: Paprastai sakyčiau, kad labai veiksminga. Jeigu neteko dalyvauti kokiose nors pratybos, tai sunku suprasti, bet kai dalyvauji, vėlgi yea teoriškai ką tu turi žinoti, bet yra, kai atsitinka įvykis, šalia to, ką tu turi žinoti, atsiranda kiti faktoriai - kaip jaudulys, skubėjimas, kažkoks tai tada išorinis spaudimas, jeigu ti to nesi atidirbęs, tada labai sunku. Ramioje aplinkoje tu gali pasakyti, kad atsitiks incidentas, na, tai atsiversiu planą ten, tada…Praktikoje taip neįvyks. Tai mums…Aš teigiamai vertinčiau…Mes dalyvavome keliuose pratybose, ir ne tik Lietuvoje ir NATO. Tai ta pratybų atmosfera taip padeda suprasti, kad didelis incidentas tėra stresinė situacija ir turi step by stepjau žinot, ką tu turėsi daryti ir šaltai reaguoti. Ir tą leidžia treniruoti.

Dominyka: Prie to paties irgi mano sekantys klausimai turėjo būti - rai vat, jūsų nuomone, kas lemia, padeda užtikrinti vienų organizacijų sėkmingumą, kad jos susitvarko su incidentais, ir atvirkščiai - Kodėl kai kuriomis nesigauna? ir čia tikras ir būtų atsakymas?

Donatas: Tai du dalykai - aiškus planas ir testavimas padeda.

Dominyka: O tada iššūkiai - tai būna tikriausiai tas stresas ir nesivaldymas šito nebuvimas?

Donatas: stresas, tai natūrali būsena, aš irgi nuo savęs dar pridėčiau - jeigu nėra aiškaus plano, tai atsiras tikrai visi viską nori žinoti ir neatstoja. Tai aiškus komunikavimo planas, komunikavimo grandinę sudėlioja, kad incidentą valdanti komanda turėtų maksimaliai susikoncentruoti į incidentą, o ne į tūkstančio klausimų atsakymus. Į tūkstančius klausimų.

Dominyka: Supratau, o šitoje vietoj tada kyla klausimas - kur yra apibendrinamas tas, kad reikia to bendradarbiavimo su kibernetinio saugumo centru, kai vyksta, tarkim, ataka, tai tikriausiai tas reikalavimas, kad turi būti ir keitimasis informacija, šitoje vietoj kartais netgi pablogina situaciją, nes tada reikia atsakinėti į tuos tūkstantį klausimų, o ne iš tiesų spręsti problemą?

Donatas: nu ne, nesakyčiau taip, nes NKSC raportuoji apie situaciją, ir tu bet kuriuo atveju tu…Gal net ir padeda, nes tėra formalumas kaip turi atrodyti tavo tyrimo ataskaita. Tu turi atsakyti į tam tikrus klausimus - kas atsitiko, kada atsitiko, kodėl atsitiko ir taip… Ir tu raportuodamas NKSC turi privalomai surinkti tam tikrą informaciją, kurią tu galbūt praleistum toj stresinei būsenoj. Sakyčiau, kad netrukdo. NKSC nereikalauja nieko papildomai, kas būtų nereikalinga. Organizacija ir taip turėtų dėl savęs tą informaciją susirinkti.

Dominyka: Supratau aišku. Ačiū. Tada irgi kalbant toliau apie Nacionalinį kibernetinio saugumo centrą, aš jau buvau uždavus panašų klausimą pradžioje, bet tai, kokią įtaką organizacijos kibernetinio saugumo politikai daro NKSC, jeigu daro apskritai kažkokia. Tikriausiai tai, kad yra kažkiek tokie reikalavimai keitimosi informacijos, tai čia būtų teigiamą įtaką?

Donatas: Kokią įtaką daro politikai?

Dominyka: Ir ką tai keičia.

Donatas: Nu NKSC nustato formalius reikalavimus, kuriuos organizacijos turi atitikti. Uždeda, pavadinkime taip minimalų “backgroundą”, jau ką minimum organizacija turi atikti.

Dominyka: Nu tai čia toks pozityvus dalykas.

Donatas: jo, pozityvus dalykas, kad yra nustatomas visiems vienodas “baseline’as”. Taip pavadinkim.

Dominyka: Supratau, tada dar turiu klausimą apie tą naują kibernetinio saugumo įstatymo keitimą ir aš žinau, kad anksčiau buvo tas kibernetinio saugumo, kritinės infrastruktūros sudarytas sąrašas. Bet dabar jūs buvote įtraukti ir ypatingos svarbos infrastruktūrą. Tai mano klausimas būtų kaip būtent tie nauji pakitimai ir ar apskritai paveikė jūsų kasdienes praktikas ir planavimą?

Donatas: Ne mūsų nepaveikė, nes, kaip ir sakei, mes jau buvome įtraukti į jas. Dabar aš patikslinsiu dėl sąvokų. Priėmus naują įstatymą, nebelieka ypatingos svarbos infrastruktūros kaip tokios. Yra

svarbus subjektas ir esminis subjektas. Dabar mes greičiausiai dar tiktai gal būsime įtraukti prie tų esminių subjektų, bet mūsų šitas niekaip neįtakoja, nes mes ir iki tol buvome nu va tam kritinės infrastruktūros sąraše.

Dominyka: supratau. Tai formalumas. Aišku, Tada sekantis klausimas būtų - jūsų, kaip eksperto požiūriu, kokios būtų pagrindinės Lietuvos tos kibernetinės politikos sistemos stiprybės, siplnybės ir apskritai susijusios būtent su atsparumu galbūt arba apskritai - kurioje vietoj galėtų būti geriau? Ką galima būtų taisyti arba kaip tai, kas yra labai gerai?

Donatas: niekad negalvojau apie tai. Stiprybė - tai, kad turime vienodą "baseline'ą" visiems, o kas galėtų būti geriau - tai pagalba mažoms organizacijoms, regionuose. Mažom įmonėnm bet kurios daro kažkokią reikšmingą veiklą. Tai didelis organizacijos ir iki šiol investavo į kibernetinį saugumą, ir tikriausiai jų kibernetinio saugumo branda buvo, yra aukštesnė negu kitų subjektų. Bet kalbant apie tuos mažus, tai jiems reikėtų daugiau pagalbos, tos metodinės pagalbos, kaip įgyvendinti reikalavimus.

Dominyka: Supratau, bet čia labiau planavimo ar išteklių klausimas?

Donatas: bendrąja prasme yra išteklių ir resursų klausimas. Nes, įsivaizduokime, turime kokiam nors nežinau, ar rajone kokiose nors Prienuose kokius nors šilumos tinklus. Ten dirba dešimt žmonių, ir jiems dabar pagal įstatymą reikia turėti kibernetinio saugumo specialistą ir valdyti kibernetinį saugumą. Tai visų pirma ten pritraukt specialistai į rajoną yra sudėtinga. Tikriausiai taip, kažką galima surasti, bet vienas lauke ne karys, tai labai sudėtinga. Tai metodinė pagalba, aš manau, kad jinai gal atsiras, bet šiai dienai, sakyčiau, metodinės pagalbos dėl brandos, tom mažom organizacijom. Didelės organizacijos kaip Ignitis, Telia tai jos ir taip jau tą kibernetinio saugumo brandą turi.

Dominyka: Supratau,aišku,dar prie to paties irgi turėjau klausimą, irgi toks užtvirtinimui. Tai kai kalbėjome apie būtent viešojo - privataus sektoriaus bendradarbiavimą, tai, jūsų nuomone, šitoje vietoj kaip ir nebūtų labai kažko, ką reikėtų įtvirtinti, tikrinti, stiprinti, kad tai jau pakankamai sklandžiai yra aprašyta, nurodyta?

Donatas: aš manau ir kaip galima bendradarbiauti. Verslas kuria sprendimus, paslaugas, kalbant apie kibernetinį saugumą, tai manau, kad galėtų bendradarbiavimo principu dalytis ir su viešuoju sektoriumi. Sakykime taip.

Dominyka: O jūs, jūs, dalinatės?

Donatas: Taip, ekspertiniu lygiu, tai taip - kažkokiais sprendimais ar ten techniniais ne, apskritai paslaugų, kaip kibernetinio saugumo paslaugų, į išorę, į kitas organizacijas, neteikiam, bet konsultuojamės abi pusės ir mes konsultuojame, tiek NKSC, tiek kertinis valstybės telekomunikacijų tinklas. Su LRTC esame kažkada kalbėję arba ten per kibernetinių ekspertų bendruomenė. Tai ekspertiniame lygyje mes konsultuojamės, keičiamasi gerąja praktika. Bet ką aš turiu omeny apie verslo ir viešo sektoriaus bendradarbiavimą. Tai paimkite tuos pačius SOC, kas yra saugos operacijų

centras, kas yra privaloma pagal įstatymą kai kurioms įmonėms, tai valstybė šiai dienai neturi savo normaliai funkcionuojančių, užbaigtos SOC, kuris galėtų teikti paslaugas mažoms įmonėms, įstaigoms, o lygiagrečiai verslas turi ir teikia sau tokias paslaugas. Tai galbūt valstybei irgi nėra būtina išrasti, išradinėti dviračio. Bet ar čia kritiškai, tai ne.

Dominyka: o dabar noriu paklausti, kaip vyksta tas komunikacijos keitimasis tarp viešojo - privataus sektoriaus, ypač atakų atveju, kaip yra išvengiamomis miss-komunikacijos? vis tiek atsiranda tikriausiai ypač tokioje krizinėje stresinėje situacijoje tam tikrų klaidų, kaip yra su tuo tvarkomasi ar galbūt viskas taip gerai, kad nebūna?

Donatas: Gal sakyčiau, kad nėra ten tų atvejų tiek daug, kad čia ta komunikacija vyktų kažkaip labai dažnai. Yra dabar Lietuvoje, taip sakykime dvi iniciatyvos dėl formacijos keitimosi iniciatyvų. Tai pirmas į kibernetinio saugumo informacinis tinklas. Kitas yra Vilniaus miesto savivaldybė su, NRDCS, daro, darė projektą SOC-share, kur irgi kūrė įrankius ir metodiką dėl dalinimosi grėsmėmis - tai kaip išvengti tos miss-komunikacijos, tai yra susitarimo Protokolai ir tarpusavio pasitikėjimas. Jeigu tu nu kažkokį “briedą” komunikuoja, tai tave atitinkamai kiti dalyviai sureitinguoja. Bet to absoliučiai

Neišvengs.

Dominyka: nes dar yra viena tokia kita teorija, kuriai dažnai kaip “policy: formavimo srityje girdime, kad būtent dėl to, kad vis tiek yra tam tikros verslams baudos dėl tų atakų, kad yra vengiama tam tikrais atvejais dalintis su apskritais viešuoju sektoriumi apie tai, kad atakos įvyko.

Donatas: jo yra ta teorija. Aš manau, kad jinai egzistuoja ir Lietuvoje. Aš manau, kad čia ydinga, ydingas požiūris ir tikiu, kad su laiku tiesiog pasikeis, nes auga pačių organizacijų branda. Nu, aišku, visų pirma pati bendruomenė, jeigu žiūrėt plačiai, tą, kuris patyrė kibernetinę ataką nulinčiuoja taip formaliai. Tai čia yra minusas. Tai pagrinde, matyt, reikėtų komunikuoti tą žinutę, kad nu neišlaužiamu nėra, nes dabar dar dar didelė didelė dalis organizacijų galvoja, kad patirt, ataką yra labai blogai. Mes pas save esam grupėje pasisakė, kad mes, jeigu patiriame tokią reikšmingą ataką, tai mes patys ir euname komunikuoti viešai, šito neslėpėme. Kažkaip jau ir atitolom nuo to požiūrio, kad čia bando kažką taip paslėpti. Tiesiog aš galvoju, kad čia bendruomenei tos brandos šiek tiek reikia. Tas per laiką turi susiformuoti.

Dominyka: Supratau, bet kai sakote viešai komunikuoti, tai tikriausiai pirmiausia vyksta komunikacija su atitinkamom institucijom, ir tada bendra žinutė? Ir tada eini ir sakai?

Donatas: Lygiagrečiai. Lygiagrečiai ruoši pranešimą, teiki jį žiniasklaidai. Lygiagrečiai teiki institucijomm institucijom papildai kažkokios tos techninės informacijos. Nėra taip kad informuoja NKSC ir ten atsiklausė jų ar čia dabar galima komunikuoti? Ne tai, komunikuoji viską nuo pat pradžių, bent jau mes taip dirbam.

Dominyka: Aišku, kadangi liko aštuonios minutės, tai tik pora. Manau, gal spėsime, bet tokie labai baigiamieji bendriniai. Tai pirmas, kad apmąstydami vat savo patirtį ir apskritai savo ekspertizę, ką patartumėte kitoms Lietuvos organizacijoms, norinčioms padidinti savo kibernetinį atsparumą? Tai jau šiek tiek irgi aptarėme apie tas mažytes organizacijas, jų iššūkius. Bet čia toks irgi bendras nes užbėgant įvykiams už akių aš dar planuoju su KTU pasikalbėti, vilniaus universitetu, Rajono savivaldybe.

Donatas: noriu palinkėti, kad tikrai nuoširdžiai kalbėsis, nes sunku, sunku prakalbinti. Gal taip sakyčiau, jeigu pavyko sutarti.

Dominyka: Dar ne pažiūrėsime, bet bent jau čia yra šitos temos, toks tokia problema, kad daug organizacijų bijo šnekėtis apie tai, nors čia visas tas įrašinėjimas ir visa kita bus tiktai analizės principų. Mano darbe, kur aš nieko tenai labai necituosiu.

Donatas: tai koks palinkėjimas galėtų būtų, kaip padidinti atsparumą? Tai, taip, pirma tai nu nežinau, kaip tą reikėtų užrašyti, bet pirma, vadovai turi įsikalti, suvokti galvose, kad incidentas įvyks, anksčiau ir vėliau. Ir tada jau tu turi ruoštis realiai, o ne paukščiukui, kad atitiktum kažkokį reikalą. Čia yra šitas kritiška. Labai svarbu kokybiškas poveikio veiklai vertinimas, nes pagal tai tu tada planuoji visą kitą atstatymo, tęstinumo planą. Aišku, ten nuo to atsatymas, matyt, nelabai priklauso, bet tai leidžia toliau specialistams organizacijų įvertinti, kurie čia resursai yra svarbūs, ir atitinkamai skirti prioritetus ir pasiruošti. Tai tas suvokimas turi ateiti, kad vis tiek kažkada įvyks.

Dominyka: Supratau, o, jūsų manymu, tada kas padeda gerai įgyvendinti teisingai tą kibernetinio saugumo, kibernetinio atsparumo strategiją? Ar būtų kažkas? Ar čia yra tas?

Donatas: Liūdna, bet tiesa, kad greičiausiai įvykęs realus incidentas jau tada padeda įgyvendinti ir atsparumo strategiją. Dažnai taip yra, kad kol neužlėki, tol neįvertini. Tai padeda suvokimą atverti. O įgyvendinimo prasme, tai yra testavimas. Testavimas parodo, kiek galimai atsparumo strategija yra efektyvi.

Dominyka: Supratau. Mačiau, kad ir Vilniaus savivaldybė dabar turi programą, kur samdosi žmones, kviečia juos bandyti nulaužti sistemą ir taip žiūrėti, kur silpnos vietos. Tai čia tikriausiai ir būtų kažkas, kas padėtų geriau įgyvendinti?

Donatas: Čia gal daugiau skaičiau iš grėsmių aptikimo. Tu ieškai silpnų vietų sistemos. Iš tos klasifikacijos ką mes kalbėjome. Tai yra metodas, išorinių pažeidžiamumų paieška pasitelkiant bendruomenę. Ne, ne kompaniją samdant ne kažkokius įrankius naudojant. Šito rezultatas yra, kad savivaldybė žino silpnąsias vietas jų sistemos. Jie gali jau prevenciškai imtis veiksmų, kad tų skylių nebūtų.

Dominyka: Supratau, jūs vis tiek labiau su šituo susidūręs, nes aš iš pradžių interpretavau, galvojau, galbūt tai padeda suvokti, kiek iš tiesų žalos kažkas gali padaryti, ir tada susidėlioti vidinius procesus reagavimo?

Donatas: Ne, ten yra grynai grynai techninės skylės, kad, pavyzdžiui, galima prisijungti prie sistemos, tokiu ir tokiu būdu. radau atvirą prieiga. Slaptažodis silpnas, atspėjamas. Gimsta techninio pobūdžio skylės, pažeidžiamumai.

Dominyka: Bet jeigu tiktai vieną tokią strategiją taikyti, tai jau čia nebūtų gerai, nes vis tiek ta ataka kažkada įvyks.

Donatas: Vienareikšmiškai taikyti abi. Net nežinau iš tikrųjų. Niekur nebuvau girdėjęs, kad būtų siūloma arba svarstoma rinktis alternatyvą.

Dominyka: Aš kažkaip irgi esu čia gal tokia silpna vieta mano darbo, bet man pasirodė, kad labiau apskritai Lietuvoje yra bandoma parodyti, kad bandymas vat išvengti žalų, grėsmių, ir investavimas tas populiarus modelis, bet tai, kad tu atakų neišvengi ir jos vis tiek atsitiks, nėra toks populiarus. Ir pas mane yra bandymas parodyti, kad vis tiek reikėtų ir ten žiūrėti į abu. Tai ir teorija yra, kad vat jeigu paimsi, kad KTU ir Vilniaus universitetą, tai KTU, kadangi patyrė ataką, tai galbūt jau ne taip rūpinsis tuo atsparumo, o labiau buvo bandė išvengti tų atakų ir daryti prevenciją. O Vilniaus universitetas galbūt jau vykdo tam tikras programas.

Jonas Pidkovas (Vilniaus Savivaldybė), interviu, Vilnius, 2024m. Gruodžio 4d.

Dominyka: Jau įrašinėju. Kitas klausimas - ar Jūs būtumet nieko prieš, jeigu naudosiu jūsų vardą kur nors savo darbe.

Jonas: Nieko, nieko prieš.

Dominyka: Gerai. Tai tuomet - esu Dominyka, rašau darbą apie kibernetinio atsparumo konceptą. Interviu truks apie valandą. Pirmas klausimas yra būtent apie organizacijos kibernetinio saugumo/atsparumo strategiją. Taigi - kokia pas jus jį būtų? ar ji labiau orientuojasi į tą sistemų atsparumą (tam tikra nepertraukiamą sistemų darbą, neneigimas, kad ataka įvyks, visa esmė yra jai pasiruošti), ar vis dėlto labiau yra prioriterizuojama išvengti grėsmių, lopyti spragas, kad tik jos (atakos) neatsitiktų ir panašiai?

Jonas: Čia visko labai daug, bet gal pradedam truputį nuo pačios istorijos.

Dominyka: Gerai.

Jonas: Taip po ranka dabar neturiu, čia buvo prieš kelis metus. Darėme pratybas mes. Nežinau, gal pamenat Vilniuje bandėm ten geležinio vilko (gatvėj) autobusiukas su vaikais užstrigo, bandėm žiūrėti kaip eismą reguliuojam, ir esminė mintis buvo pažiūrėti mūsų ir savivaldybės įmonių atsparumą kibersaugoje. Tai pasitelkėm komandą tokią vieną ir viena iš tų komandos narių kaip ir užduotus buvo sutrikdyti būtent operacijas. ir gavosi iš to gimė, kad pamatėm, kokie mes neatsparūs, kaip įmonė. Tai nepabijojom pateikti tą ataskaitą būtent vadovybei. Ir palaipsniui pradėjom žiūrėti būtent tą savo higieną, tas pradinės rekomendacijas kaip įgyvendinti. Ir gavosi, kad pereinant žiūrim,

kad mes jau kaip ir truputėlį iššiugdėme kompetencijų ir sūkūrėmę tokią apie save organizaciją, aprašėme Vilniaus paslaugų krepšelį, ką mes darome. Truputėlį apsirašėme žingsnius nuo ko pradėsim ir kur judėsim, kad būtume atsparūs arba bent stebėtume ir matytume, kas vyksta pas mus. Kai jau apisrašėm šitą, tai stojom į tokią (neišgirdau pavadinimo) organizaciją, asociaciją, kuri ten dalinasi patirtimi ir skaitosi kaip standartą apsirašius, kibersaugos paslaugas savo viduje. Bet mes kuom skiriames nuo kitų truputėlį, kad mes ne pagal teoriją dirbam, mūsų komanda visa yra inovacijų ir technologijų grupė, yra, sakykim, visi adminai, tinklistas, darbo vietų priežiūros specialistas ir jie kaip komanda kažkiek valandų būtent skyrė kibersaugai. Ir sudaro būtent ekstrą atvejų, tas team'as, sudaro kibersaugos komandą. Dabar, kaip ir sakiau, plečiames, pradėjom žiūrėti ne tik savo būtent organizaciją, bet pradėjom konsoliduot ir žiūrėt poliklinikas, kaip pas juos situacija. tai gaunasi taip. O kas liečia labiau…koks ten klausimas buvo?
Dominyka: Ar galėtumet teigti, kad Jūsų organizacijos strategijoje daugiausia dėmesio skiriama atakų prevencijai ar tam sistemų prisitaikymui?
Jonas: Čia du lygiagretūs dalykai. Tik šiaip mes žiūrim būtent tą darbo resursų atstatymui, nes yra papildomai vykdomą programą "kas X atvejų atsitiktų", jeigu ne duok dieve karas, ar kažkas. Tai mes nagrinėjame sistemas, kurios yra kritinės, jeigu čia kažkas ar kur kitur atsistato, kas mums poreikis yra, ar tvarkingai darome backup'us. Sekantis dalykas - žiūrime, kas gali įvykti, prediction tokį darom mes, srautuose dalyvaujam komunikaciniuose, kokie būna "Telegramuose" ar "Twitter'yje", kur pataggina, dark web'uose žiūrim, kas gali vykti organizacijose iš tų raktinių žodžių, ar prisijungimai kokie organizacijoje. Ir kartu monitorinam, kas einamuoju metu vyksta. Bet papildomai, kadangi taip organizacijoje pagal metodiką negali būti tas saugumo centras kartu su IT, tai turime dalinį atitikties, atskirai prie, kuris nepriklauso nuo mūsų, arčiau prie administracijos direktoriaus, Adomo, ir jie būtent ieškos CISO specialisto, kuris ieškos atitiktį, kaip mes viską darom pagal patvirtintus teises aktus tuos dalykus, teises aktus, visus tuos dalykus. Tai ten labiau vykdo tą prevenciją, stebėjimą tokių dalykų.

Dominyka: Supratau, aišku, irgi, tikriausiai, kai galvojat apie tą saugumą, tai išskiriat vienodai tuos dalykus, kad vienodai svarbūs, vienas lauke ne karys.

Jonas: Jo tai darėme net pratybas duomenų atstatymo ten savo didelės sistemos dokumentų valdymo. Ransomwarų kriptavimus žiūrim, kad galima būtų apsisaugoti. Netgi nagrinėjame technologinius sprendimus, kurie pigesni būtų, architektūriškai, kur eit, kad atsitatyt greitai. Lygavertiškai žiūrime, ir matau tame pliusą, kad pati komanda peržiūri kibersaugos architektūrą šitą, ir tuo pačiu dalyvauja savo konfiguravimuose, nes bendras susikalbėjimas ir vizija nepasimeta.

Dominyka: Supratau. O sekantis klausimas būtų - kaip apskritai vertintumet savo kibernetinio atsparumo lygį? Ar yra, konkrečiau, kokie kriterijai, pagal ką vertinat? ar yra išsiskirti stratrginiai planai, ir tikrinat kiek juos atitinkat, ar esat išsipildę savo KPIs?

Jonas: Tai iš tų sistemų veikimo yra tie KPIs, kiek jie gali veikti, atstatomumas ir taip toliau. Esam išsikėlę kriterijų irgi, netgi pasitvirtinę veiklos tiksluose ir metiniuose planuose. Kas liečia tą duomenų statymą ir veikimą. Kibersaugos kaip tik taip, turėjome prieš kokius tris mėnesius darbo grupelę kaip mes matuojame, pablikuot per savo organizacijas būtent pasilyginti ar mes gerai vykdome darbą, ar laiku sureaguojame, pamatuoti, pasižiūrėti tuos KPIs apskritai. Turimę pasidarę, kaip pasakyt, kartais pakliūna tokie dalykai, kur greit negali ištaisyt jų, kad ištaisyt reikia laiko. Tai būtent idėja per kiek laiko sureaguoji ir padaria planą, pradedi taisyti savo kažkokią ten dalį…būna kai darbo vietos, dabar stebim galinę įrangą…po to, taip mintinai nepasakysiu, bet kas ketvirtį pasižiūrim tuos rodiklius, pristatau, kai laiko lieka vadovybei, taip pat dabar vienas iš rodiklių tokių fishingo, tai mes darbuotojam siuntinėjam kartas nuo karto tokius bandymus paveikti, iš kiek laiškų jie…iš kiek darbuotojų įtartinai, pamatę, kad įtartinai ir persiuntė mums, kur mes ten į paštą atsakys robotukai. Tai šitą, tada kiek kas paspaudė ir suvedė savo duomenis ir t.t. iš strateginių turim, sakykim, kaip dabar poliklinikas konsoliduojam taip ir saugą, būtent ką mes tuo projektu sakysim, kad pasiekėm.

Dominyka: Supratau

Jonas: Nu rodikliai reikalingi, įdomiau dirbti ar pasiekei ar nepasiekei tikslų.

Dominyka: O čia dar klausimas į tą patį, o turit pasitvirtinę kažkokius tai planus, jeigu kuris nors iš darbuotojų suveda savo duomenis ir atsiranda pavojus breacho?

Jonas: Dėl sankcijų darbbuotojų dar ne, bet kai kažkas įvyksta su mūsų duomeni, turim sudelioję procedūra, turim team lead’ą, kuris kordinuoja procesą, pajungia viešiuosius ryšius, duomenų apsaugos pareigūnai, iš IT, kas reikia, iš tos veiklos ko reik. Tada vykdomas veiklos planas. Netgi darėm pratybas. Bet kol kas stalo pratybas.

Dominyka: Supratau, mano klausimas čia šiek tiek kartosis su Jūsų, bet gal turėsit ką papildyti, tai kokių konkrečių priemonių savivaldybė ėmėsi, kad pasiruoš galimiems kibernetiniams incidentams, bet jūs jau minėjot ir phishingo testus, ir pratybas tam tikras kartas nuo karto.

Jonas: Priemonių daug. Ių pat pradžių mes labai daug padarėme kai pradėjom žiūrėt, kad trūkstą įrankių. Priemonės pas mus atėjo per praktiką. Jau, kai nuiiminėjom žaliojo tilto skulptūras matėme, kad kažkas vyksta, įrangą kalibravom. Tada didelė priemonė buvo patikrinti kaip paslaugų tiekėjai testuoja ir daro sistemos patikras. Paleidom "hack me if you can", kurie nori legaliai įsilaužti į sistemas. Po to jau ta praktika ir iki vyriausybės nuėjo, po metų patvirtino. Tada jau piniginius prizus paleidom. Dar kas gerai, tai kai paleidi tokią programą, kai nesupranta jos esmės, tai gali lygiagrečiai kalibruotis įrangą, stebėsenos įranga. Kaip atlieka, kaip darbuotojai sureaguoja. Tada darėm pasiruošimą didelį prieš NATO, labai ilgą laiką turėjom veiksmų planą, per NATO summitus turėjom veiklų ir daug tvarkėmes. Gaunasi per praktiką viskas, ir geresni nei per popierius. Bet kas liečia darbuotojai, tai turim nerašytą tokią taisyklę pas save, jeigu darbuotojas matome, kad procentas sumažėja, tiksliau iš pradžių tik tą "paslystančią" auditoriją iš kibersaugos imdavome, dabar jau darome švietimą, kviečiame pas save į renginius iš praktinių pavyzdžiu kaip kas vyksta, negąsdinant jų realybėje, apie paprastus buitinius dalykus. Ir iš tiesų dar darome ketvirtinius tokius susirinkimus su kibersaugos bendruomene. Kas liečia jau technologinius dalykus, ketvirtinius susitikimus su tą kibersaugos bendruomeną.

Dominyka: O kas įeina į tą bendruomenę?

Jonas: SOC share, turim mes tą bendruomenę, į ją įeina kas nori, mes paskelbiam renginius, pasakojame apie realius atvejus, kad kiti galėtų iš to kažką pasimokyt, kaip vyko įsilaužimas, kaip užkardinama, bet ten ne tik mes pasakojame, per įmones, per kitus partnerius. Būtent šitas projektas gimė su privačiu partneriu. Buvo pirmas tiesiai mūsų iš europos projektas, kuriam nepabijojom teikti paraišką, prasifinansavom įrankių stebėsenas, tuo pačiu ten ir darbuotojų kompetencijų didinimas yra, tai gerai, kad galima tokius dalykus prasifinansuoti. Tai vat būtent su šiuo projektu pasiekem per du metus, kiek per keturis turėjom pasiekt.

Dominyka: O čia buvo projektas, aš skaičiau, su NRD security.

Jonas: taip taip, mes ieškojom su valstybinėm organizacijom su kuo eit į partnerius. Aš paskelbiau forume kas norėtų eit su mumis, jie atsiliepė ir pasirašėm sutartį, buvo geras bendradarbiavimo pavyzdys.

Dominyka: O tikslas projekto buvo, vėlgi prevencija ar atsparumas, ar abu?

Jonas: tikslas labiau prevencija, nes čia eina, buitiška mintis…nors gal ir atsparumas.

Dominyka: gali būti ir abu.

Jonas: nu čia tikslas būtent pasidalinti žiniomis, kad kiti suprastų kas vyksta, kas įsilaužia, kokie scenarijai. Nu aš čia buitiškai šneku, bet mes pradėjom kelti jau tarptautiniai įvairias būdais, kas vyksta pas mus ar bando vykdyti, keliam į tokią centralizuotą sistemą ir tada viskas sklinda po europą. Ir gaunasi, kad iš europos net NKS aplenkiam su tokiu pasidalinimu. Galvoju dabar ko čia daugiau. Nes gaunasi ir tas ir tas, nes jeigu reik rekomendaciją pasitvarkyti kokią metodinę, tai čia gaunasi gal labiau į kito vat kad įvykio išvengti, tai gal čia daugiau atsparumo, kad išvengti įvykio…nes prevencija jau būtų labiau….

Dominyka: Supratau. Kitas klausimas, vis tiek, kiek galit pasakoti, ar galit pasidalinti neseniai įvykusio incidento pavyzdžių, koks buvo organizacijos atsakas, kokie buvo dėliojami procesai? Nes aš jokių žymių pastaruoju metu neradau (apie jus), tai klausimas ar išvis pas jus buvo.

Jonas: Nu incidentas jau būna kai jau kažkas įvyksta, bet iki incidento…bet buvo prieš tai, prieš, tik laike nepasakysiu tiksliai, naujausias buvo čia kažkada, bet čia buvo užkardinta, tai ne incidentas, būtų incidentas, jeigu kažkur įeitų, bet prieš metus ar du buvo microsoft klaida ir buvo nusiurbti mūsų prisijungimai visi, bet kai pamatėm, kad klaida, tai paleidom slaptažodžių pakeitimus ir tik dabar prieš du mėnesius pamatėm, kad buvo bandyta su tais prisijungimais paveikti, prisijungti prie tam tikrų sistemų. Bandyta tik kažkodėl, bet susiję su žiniose, kas paskelbta buvo, Vilnius su Ukraina kažkas. Tai užkardinta buvo tokia. Tada…

Dominyka: bet čia labai įdomu, aš tik įsitarpsiu, darbe viena iš mano teorijų yra, kad labai gerai sekasi tvarkjytis, kad kažkas yra, kad jūs gerai susitvarkot, tai galit viską ką turit, pasakot.

Jonas: …Tada, tokie dalykai, dar papasakosiu, kai tu įsidiegi įrankius, kai vat darkwebo stebėjimus, tinklo stebėjimą, galinių įrenginių stebėjima, kompiuterių ir t.t. tu pradedi tiek daug ko matyt, tiek daug darbo padaugėja, nes vos ne kiekvieną dieną reikią užkardyt, didint tą atsparumą. Tai dabar buvo, bet pas mus nebuvo įvykio, su VPN klientu, kai pašte siuntinėjo, tik neatsiminsiu kuris, nes daug būna per paštą siuntinėja, ir kažkaip praleido tris pradžioj, nes nepamatė, kad per nuorodą virusas, keistai buvo padaryta. Tai…pastebėjom šitą, greitai pateikėm, kadangi bendradarbiaujam net su virusines gamintoju ESET'a, pateikėm jiem iškart tą turinį, informaciją, ko reik, jie tada iškart atnaujina tas tam tikras taisykles, vadinasi. Ir tuomet užkardėm kitose savo darbo vietose, ir tuos kompus mes iškart izoliavom ir sutvarkėm. bet pastebėjom tokį dalyką, vienas iš įdomesnių. Kitas

įdomesnis irgi įmonėje, tik jau ne pas mus, kai prieš gamintoją, čia buvo Teltonikos kažkokia kalida, jie neatnaujino ir š jų įrankius įsilaužė, bet pamatė, kad buvo įsilaužta, bandyta, bet laikų užkardyta, bet jau ten didesnes būtų buvusios pasekmės. Ir plius pačius vandens siurblius būtų tuščia eiga paleide, nes ten buvo tokie siurbliai, kur jeigu patvinsta kažkur, tai jie įsijungia. Tai net prie tų buvo pamatyta, kad prieinama. O taip tai vyksta, labai įdomu buvo kai per NATO summitą vyksta viskas, vos ne per karą, leadinti, komunikuot, išjunginėt. Bet čia buvo DDoS labiau atakos, turėjom NATO polapį, vieni iš gamintojų, gerų gamintojų, norėjo išbandyt, mes dažnai išbandom, tai mes naudojom organizacijoje vieną ir lygiagrečiai kitą įrankį, ir pamatėm, kad ryte buvo labai didelis suaktyvėjimas, jie ten pabandė, žinoma, nieko nepavyko padaryti, bet grįžo ketvirtą valandą, ir taip grįžo, kad net organizacija, kuri saugojo mus, ją pačia nulaužė, bet kadangi mes turėjom tu lygiagrečiai testuojamus daiktus, tai greit perjungėm į kitą, o jie buvo pasiruošė tai technologijai, tai jau nesuveikė jų visi tie poveikiai ir poveikių įrankiai, kur bandyta įsilaužti.

Dominyka: Supratau, o šitoj vietoj tik noriu pasitikslinti - turėjom kažkokį backup planą, jeigu taip atsitiktų.

Jonas: Jo, kai turi du planus, įrankius. Kas čia dar, gal aš atsidarysiu…pažiūrėsiu tuoj mūsų kanale, nes kažkaip labai neįsiminiau…direktyvos…

Dominyka: Tai jeigu ką prisiminsit, galit visuomet papildyti.

Jonas: gerai.

Dominyka: Noriu paklausti - ar esat apie tai galvoję apskritai, bet kaip jūsų organizacija yra pasiruošusi reaguoti į galimus naujų technologijų kibernetinius iššūkius per ateinančius penkerius metus? pagrindinė esmė, kad taip greit keičiasi technologijos ir kibernetinė erdvė, tai ar turit kokį pasiruošimo planą, ar tik metai į priekį ir po to žiūrėsim, tas pats AI.

Jonas: Labiau mes tokio ilgamečio plano neturime, nes labai kažkaip greit viskas kinta, tai mes stengiames dalyvauti, išklausyti patirčių su kitom organizacijom, kur būtent žiūri tokius trendus, bando, pilotuoja, kas vyksta rinkoje ir spėti su ja tuo pokyčių laiku. Dėl dirbtinio intelekto, tai dabar prie jo pratiname tik darbuotojus, bet vis tiek ten yra daug saugumo niuansų su duomenim. O kibersaugoje tie įrankiai yra dar pilotuojami, bet čia baisu pagalvot dabar, kuo daugiau, kai buvau vat vienoj pasualinėje konferencijoje, tai net su dirbtiniu intelektu įsilaužinėja su dirbtiniu intelektu per tuos pavyzdžius, vos ne kažkada AI su AI kovos ir mes vos ne ant popieriaus rašysimes. Baisu net

pagalvot, bet tokio vat kad ilgamečio ne, nes labai reaguoja greit viskas, mes kaip tik nagrinėjames tuos trendus, kažkada tas VPN buvo populairus, dabar Zero-trust, einame dabar kartu su rinka.

Dominyka: aišku, ačiū už atsakymą. Noriu pasiklausinėti apie Jūsų santykį su įstatymais ir viešosiom institucijom, vis tiek yra numatyti protokolai. Taigi, tai kokį vaidmenį Jūsų organizacijos kibernetinio saugumo stratrgijoje atlieka bendradarbiavimas su išoręs organizacijom, viešom ar privačom, tai čia tuo paties ir guidline, kad yra tam tikri įstatymai, kuriuos turit followin'ti, tain mano klausimas kiek įtakos tai Jums turi ir kaip tai veikia, ar apsunkina Jums situacijas ir reagavima?

Jonas: nu ar apsunkina, jeigu pavyzdžiui, jeigu nebūtume keletą metų ėję pažingsniui, tai galvotume, kad mus apsunkina ta direktyva nauja, bet mes tam ruošemės, ėjom, mum tai priimtina tiesiog. Tai tiesiog įpareigoja teises aktas visus tai daryti, tam tikra auditorija įpareigoja. Nes jau kaip ir buvom, kaip ir galvojom apie tai, buvom tam subrendę, mąstymas kitoks truputėlį kaip mūsų organizacijos.

Dominyka: O kaip vyksta pats reagavimas, kai Jūs turit pranešti apie tam tikrą ataką?

Jonas: Telefonu, paštu, jeigu kas ten baisesnio. Turim vidinius forumus, nacionalinis kabinetinis centras pradėjo jau kalbėtis, nebekiekvienas sau, pasiderinam strategijas. Nepasakyčiau, kad apsunkina.

Dominyka: Kitas klausimas tuomet - buvo čia, kur keitėsi pats įstatymas, tie subjektai, ar pavyzdžiui Jums kažką šitoj vietoj keitė? Nes aš kalbėjau ir su Igničiu ir jie užsiminė, kad jiems kažkas labai nesikeitė, jie ir prieš tai buvo vienoks objektas, dabar kitoks.

Jonas: Jo, tos organizacijos, kur turi kompetencijas, tai jos supranta, kad riek investuot i kibersaugą, tai kur laikėsi to, tai joms nieko, bet va dabar, kur kas nesiruošė tam, nedirbo ta linkme, tai liečia gan smarkiai, gan greit reik liesti. O mums tai jo, ten užregistruot į sistemą, neaišku kaip ten vieks, nes ten dar patys ruošiasi, bus sistemos, kur įrašytos į registrus. kai kas apsunkina - pvž., išleido teises aktą, kad kas valstybiniam tinkle, tai turi savo visas aplikacijas laikyti Lietuvos radijo ir televizijos valstybiniame duomenų centre. Tai nepažiūrėję ten šešiadešimt sistemų perkelti, kur kai kurias mes cloudinam Azure, dar kitur, ta prasme su technologijom, kurios šiom dienom veikia, ten kibernete sau vietų ten nepasiruošę, tai tokie nepasitarimai.

Domminyka: O tariamasi šiaip su specialistais?

Jonas: Nu va kažkaip šiuo įstatymu tai nesitarė, tik prieš tai atsiuntė raštu, kad va pateikite pastabas,bet va kaip tik dėl sistemų prvalumomo laikymo valstybiniam duomenų centre irgi nesitare. Tik tarėsi būtent tada, kai išleidinėjo, kad gali, kaip minėjau, kai turėjom įsilaužimo programą, kur sankcijų neteiksim ir gali įsilaužinėt, nesikreipsim mes į policiją, tam tikras procedūras, tai vat tada kreipesi, kaip išleist tas procedūras.

Dominyka: O va šita programa, kur minėjot vykdot, tai čia man kilo klausimas - ar čia skaitytųsi prevenvija, ar atsparumas? Ar pasižiūrėti kaip sulopyti spragas, ar reaguoti? ar abu?

Jonas: Pačioj pražd̄ioj buvo tikslas, kai išsidiskutavom, kai buvo pačios pirmos pratybos, kai pradėjom bendruomenėje skųstis, dėl tų visų programų, kur praneša ir gauna per galva, tada pradėjom mąstyti kaip tą bendruomenę, kuri irgi nori prisidėti, įtraukti, kad būtų tas atsparumas. Tai čia buvo pirmas tikslas, ir kai jau pavyko, ir pamatė ją nacionaliniu mąstu, tai jau pradėjom nebe padekas teikti, o piniginius lygius pagal tam tikrus pranešimo tipus, tai jau tada buvo toks atsparumas paszižiūrėti kaip mūsų sistemos iš tiesų ar tvarkingai padarytos, ar teisingai serveriai sukonfiguruoti. Bet mes nežinojome, kad bus ir pasižiūrėjimas į mūsų reagavimą, nes kai paleidom, kad bus atsiskaitoma už tas rastas spragas, kai kurie, nors ir negalima DDoS, pradėjo kiti leisti automatinius toolsus, ir pamatėm, kad mūsų kai kurios sitemos sunkiai dirba. Pradėjom tobulinti savo įrankius, kurie padeda tobulinti. Tai tuo momentu įsijungėm, sakėm ką darom dėl to, tai nusprendėm nerašyt tiem, kas daro tai, bet mes nenumatėm šito, tik įisijungė kaip mes konfiguriojam einamuoju momentu. Bet didesnė dalis atsparumo. Bet įsijungė kartu, mes nenumatėm, kad gali įsijungti ir dalis, kur kaip veikia mūsų procesai ir susikalbėjimas. Bet kadangi turėjom anksčiau patirtį ir su skulptūrom, ir su NATO…

Dominyka: Bet šiaip labai įdomus atvejis ta Jūsų programa. Jau ir anksčiau ir Jūs paminėjot, kad geriausia yra mokytis šito grynai per praktiką per atakas, bet jūs sugalvojot kaip mokytis ne per skaudžią praktiką.

Jonas: Jo ir dar gaunasi, kad ir tu dar kažką dar sužinai, nes susirašai su tais žmonėmis ir pasidalinai savo įžvalgomis dar ir gaunasi toks kompetencijų kelimas.

Dominyka: prie to paties, kokios praktikos padeda užtikrinti organizacijų, kurios sėkmingai susidoroja su kibernetiniais incidentais ir patiria minimalius trikdžius, sėkme? arba tam tikras rekomendacijas kaip ir į ką riek atkreipti dėmesį, kad sėkmingai tvarkytis su atsparumu ir kibernetinio saugumo iššūkiais? kalbam apie viso dydžio visokias organizacijas.

Jonas: Aš tik prisiminiau dar vieną į prieš tai atsakymą dėl tų tvarkų, užsiminsiu dar. Kad palengivinti mūsų organizaciją, būtent ką jie turi atitikti ir kaip tvarkytis, kaip čia pasakyti, yra daug visokių atitkčių ką turi atitkti organizaciją, kad atikti tą brandą atsparumo. Tai būtent mes kaip įmonė padarėm, kad mes esam įmonė, o apčioj mūsų dukretinės įmonės, ir bendrą politiką parengėm su keliais dokumentų šablonais, kad skaitomi jeigu atitiksti tuos punktus, darbo vietų, serveriu, žmonių ir t.t. tai tu skaitosi jau turi brandą ir atitiksi dalinai direktyvą ir būtent tau vyriausybės aktai, ką išleis ar išleido, mažai įtakos turės. tai tokią politiką dabar padarėm, kad būtų lengviau mūsų organizacijom, kad nereikėtų samdytis specialistų. Tai vat tu prie teises aktų ten kažką minėjai. O grįžtant prie šito klausimo - vis tiek viskas prasideda nuo nuo darbuotojų, nup žmonių kompetencijų, jų švietimas.

Dominyka: švietimas, tai ką turit konkrečiai omeny? ar kaip ko nepadaryt, ar kaip reaguoti?

Jonas: pradžia vis tiek yra kas tas yra ir kaip duomenų nenuleakinti nuo telefono ir rasto fleshiuko ant žemęs, kad jie labiau suvoktų ir juos sukrėstų. Tada, nežinau, ta higiena top dešimt, tas standartas organizacijos. vis tiek reikėtų pasitvirtinti. Eitų planas, mokymai, bent jau įsijungti, pamatyti, jeigu kažką turi mažos organizacijos, kur turim bent penkiasdešimt darbo bietų, kad srautus kokius nors tai matytų. Čia antivurisinės by default higiena, kopijos dar.

Dominyka: o kur dar reikia tobulėti?

Jonas: Aš manau, kad jeigu organizacijoje nėra brandos lygio, visuomet reikia pradėti nuo vadovo. Parodyti jam kaip yra ir kas gali būti.

Dominyka: O turit poveikio veiklai vertinimą?

Jonas: Ta prasme poveikio sistemai turi, bet, kadangi, labai daug, tai išrinkome TOP dešimt, tada rotuojame, dabar vėl darėm, tai išsirenkam, nes perdidelis scope gaunasi.

Dominyka: Mano kitas klausimas turėjo būti apie iššūkius, jeigu išsikeliat tam tikrus KPIs, kodėl jų nepasiekiat, ar tai išteklių, resursių klausimas? Tuo pačiu kokius iššūkius matote su kibernetiniu saugumu? Ar tai gali būti, kad mažesnės organizacijos neturi gerų specialistų, nėra gerų specialistų, nėra, kas išmanytų kibernetinį saugumą? Tarkim yra tik vadovai, kurie investuoja viską tik į prevenciją, bandydami išvengti atakų?

Jonas: Na, ką mes dabar matome, tai trūksta specialistų, nes reikėtų juos ugdyti. Bandome dabar mokyklose lygiagrečiai pilotinių, ne tik programavimo, bet ir kibersaugos mokome vaikus, įsilaužimų, kad truputėli kita programa juos ugdyti, jeigu kas pasirinktu sritį. Bet ką dabar matome, kad ir CISO specialistų nėra Lietuvoj, daug organizacijų susidurs su šia problematika, susidursim su kompetenciju problematika. Auditorius dabar gali nueiti į kursus ir tapti CISO specialistų, tai kompetencijų problematika. Su ką mes ir turime Lietuvoje, čia mažai tų specialistų, jie, dažniausiai, išeina į tarptautinius vandenis, mes negalime jų išlaikyti. Kita problematika - jeigu kai kurie, neapsimoka, arba per maža organizacija, samdo tą patį saugos įgaliotinį, arba paslaugą perka, tai kai pagalvoji, jeigu, pvž., tose pačiose oeganizacijose tas pats įvykis, nes ta pati sistema, tai irgi kaip jis sukordinuos? tokios vat rizikos yra. o dėl įgyvendinimo, tai tas truputėlį kartais, bet čia ir nuo vadovo priklauso, tas supratimas, kad jeigu jis supranta, kad jo duomenys svarbūs, nes jis gali nukentėti, per mediją, per kitus, tai jis investuos būtent į tą kibersaugą. Tai net nežinau, kas dar galėlėtų būt. Strateginiai tikslai nepasiekti, resursai taip pat, bet resursai atsiranda iš atlygio, nes maža rinka.

Dominyka: Ar jūsų nuomone, tas konceptas kibernetinio atsparumo, yra suvokiamas lietuvoj? Kibernetinis saugumas yra suvokiamas kaip pilnas konceptas, bet ar yra suvokiama skirtis kaip prenvencija, kur turi išvengti grėsmių, ir ar yra kur ivestuojama į atsistatymą? Ar į vieną suplakama?

Jonas: Į vieną suplakama,nes ir standartuose ir dokumentacijoje, visur dažnai į vieną suplakama.

Dominyka: O reikėtų išskirti?

Jonas: Nu mes kaip ir išskyrėm dokumentacijoje ir planuoose pas save, nes tai ir komandos kitos. Reikėtų išskirti, bet čia gaunasi dėl to, kad dokumentuose visur suplakta į vieną, bet tą atstatumomą dažnai pamiršta, kai orientuojasi į kibersaugą, galvoją įsidiegs vieną ar kitą įrankį ir bus atsparūs, bet kuo gilyn į mišką, tuo daugiau medžių, tu daugiau matai, daugiau resursų užkardyt tam, atnaujinti, arba turėt kontraktą su tiekėjais istemų palaikymui. Net ta programa mūsų nuo ko prasideda - kas iš to, kad turėsi rast tą spragą, o ją pataisyt negalėsi, tai mes seniai pradėjom tiekėjam kelti sąlygas, kad jeigu randam spragą, jie taiso už savo resursus. turi turėt įrankius pataisyt, nes jeigu mūsų vidinės sistemos, tai mūsų vidiniai darbuotojai pataiso. tai tu turi turėt tuos įrankius, ruoštis tam. O duomenų atstatymui, tai vis tiek daug kur suplakta į viena…

Domninyka: O dokumentuose, tai čia kur - įstatymuose?

Jonas: Standartuose, įstatymuose ir pas mus yra atitiktis gal…atiktys gal kitaip dar supranta, ar tu atitinki kažką, kaip pvž., yra patvirtintas kažkoks kibersaugos dokumentas ir ateina patikrinti kaip jį atitinki, ar mes neperkam tam tikrų prekių ar dar ko. Bet tas atsparumas ir…bet mano nuomone į vieną pusę viskas, bet čia tik mano nuomonė.

Domminyka: Dar jus mijėot, kad turi būti dvi komandos - čia dėl to, kad turi būti skirtingos kompetencijos?

Jonas: jo.

Dominyka: Supratau. O tai, kad kibernetinis saugumas vis dar krenta po IT skyriumi, tai ar tai yra tam tikra spraga, minusas, iššūkis, kad tai vis dar po IT, ir neturėtų būti?

Jonas: Nu kiti skaito, kas turi galimybę, kai vienas asmuo atitinka už vieną tam tikrą drinį, kaip kibersaugos centras, vienas žiūri architektūra, kitas log'us…nu gal nežiūri, bet stebi vis tiek toj srity turi dirbti, nėra, kad vien žiūri į monitorių. kiekviena persona turi savo funkcijas atskiras, tai reiškias turi turėti didelį labai organizacija didelę išlaidų dalį, tai aš tame matau pliusą, nes mes negalim to leisti, ir žmogus, kuri turi dirbti toj srity, tai jis dalinai, kaip pas mus, pavyzdžiui, vienas sistemas prižiūri ir infrastruktūrinę dalį, yra atsakingas už architektūrą visą kibersaugumo įrankių, jis žino visą mūsų architektūra ar kaip kas pas mus veikia, arba, sakykim, asmuo, kuris prižiūri n point dedection, galinių įrenginių kaip kas vyksta einamuoju momentu, gal kažkas blogai, gal neatsinaujinę windowsai, informuoja apie atsiradusią spragą, jis prižiūri darbo vietas aplamai ir plius prižiūri antivirusinių standarta ir tas įrankis plius surištas su antivirusine, tai tu optimizuoji procesą, tai ir taip optimizuoji, kad mažiau laiko sugaištų, bet tuo pačiu optimizuoju SOCą. tai aš matau daugiau pliusų, juolab, kad dabar padarė, kad virš mūsų bus asmuo, funkcija, kuri žiūrės, kaip mes tai darom. aišku, tas darinys tarpusavyj susikomunikavęs gaunasi, knolwedge sharingas, grupėje susikalbėjimas didesnis, nes tose kitose organizacijose, kur sako, kad atskirai yra gerai, bet numeta tą vieną problemą ir sako jūs IT - spręskit, tai kas gaunasi. O čia kaip komanda kartu psrendžia, reagavimas gretesnis gaunasi, nes jie ir tuos kitus dalykus prižiūri, tai matyčiau didesnę naudą to.

Dominyka: paskutinis klausimas - jus minėjot, kad stebit tuos kompiuterius, kaip derinat duomenų sekimo klausimus, darbuotojų? kaip sprendžiat etiškumo klausimą?

Jonas: pirmiausia dar čia nėra tas, kur mes stebim programos lygmeniu dar ką. bet jeigu truputėlį, tai vertina ar įsitraukia tas žmogus ir jo duomenys, kaip kameros ar dar kažkas, tai deirnama su duomenų

apsaugos poveikio vertinimu ir daromas žmonių informavimas. Bet mes dar nenuėjome šiuo atveju taip tolii, kaip galim susekti kur nuplaukė dokumentas su asmens duomenim. Dar, sakkykim, vertinam, kad jis nerenka asmens duomenų, nes jis stebi tik programinius įrankius ir jų koreliaciją, ar versija tam tikra. Nežiūri, kiek laiko koks softas atidarytas, nes yra standartinis softas ir jis įdiegtas. Koreliuoja, tu žiūri tą darbo vietą, jeigu kažkas blogai, tai žiūri, jeigu jungiesi prie vartotojo, tai išmeti perspėjimą ar sutinka, jeigu reguliuoji srautus tai žiūri kokie srautai iš jo eina. Ne žmogų matai, o darbo vietą ir pavadinimą, ir tada jungiesi prie žmogaus. Kažkada galvojom diegti prohraminę įrangą kuri matytų, jeigu nuteka asmens kodas su kompiuteriu. Buvo didelis politinis sukilimas, tai nenupirkom, o dark web'o scriptina grynai žiūri, kas atsitinka, turi mintyje, pvž., ar emalas atsirado dark web'e. Vienas įdomus atvejis buvo - žiūrim dar web'e atsirado mūsų vienos sistemos testinis accountas, o ta sistema prieinama tik iš vidaus. Tai pradėjom žiūrėti ir žiūrim, kad čia ne mūsų, o mūsų tiekėjo kompiuteris, projektų vadovo, tai mes pranešėm, jie ppažiūrėjo, kad tikrai nulaužtas kompiuteris ir susitvarkė. čia toks vienas iš įdomesnių kaip stebi ir gali paveigti ne tik nuo tavęs, bet nuo kitų.

Dominyka: trečios šalys yra tam tikra saugumo spraga, nes negali būti už juos atsakingas, bet jie lemia tavo saugumą.

Jonas: taip, dėl to savo procedūras įdiegė esam, kad jie net prie serverio neprieina, mes matome sąsajas ir t.t. Jeigu kiti mūsų tiekėjai kažką konfiguruoja, specifinį softą ar serverį, tai jungiasi per programą, kad matyt jo veiksmus ir ką darė. Daug kas priešinasi, nori senoviškai dirbti, tai kol išugdai. Tai didžiausia, gal net kelčiau į viršų, yra žmonių kompetencija, kuri dirba su vartotojų ar sis adminų, programuotojų kompetencijų išugdymas dirbti su saugumo įrankiais, kurie padeda tau užkardyti saugumo priemonėm, su tom priemonėm dirbti. Nes tu įjungti gali greit, bet kol išmokai, jie nemokės naudotis. o šiaip tai, kas liečia dar va kodėl neturim ilgalaikės strategijos, tai va neseniai laimėjom iš microsoft programą, kai pastebėjom, kad iš jų reik įrankio stebėjimui saugumo iš giliau, tai laimėjom, kad microsoft finansuoja tam tikras programas. viena iš programų - saugumo žymų sudėliojimo co pilot, kas kur gali prieiti, kaip teisingai tą politiką sukonfiguruoti, kad atitiktume, kad duomenys išeitų nuasmeninti į išorę, naudojant dirbtinį itelektą. Tai jeigu turėtume strategiją, negalėtume dabar greit į šitą persimesti. Reikia viduje jau greit diegti įrankius kaip viduje darbuotojai elgiasi su duomenim, tai va lygiagrečiai iškart paimam, mokomes ir diegiam sistemas, visumą, nes daug ten dalykų įeina.

Dominyka: O, tuomet, nesigauna čia irgi tam tikras iššūkis, kad jeigu pasirašot strategijas, jomis turit vadovautis, tai tam tikras iššūkis, kai reik greit reaguoti, nes yra dinamiška erdvė, ar nesigauna toks iššūkis tos strategijos valdyti gresmes?

Jonas: jo, būtent taip.

Dominyka: o ką jūsų darbo rolėje reiškia inovacijos?

Jonas: taip pavadinta inovacijų ir technologijų grupė.

Domiyka: o kokios tos inoovacijos?

Jonas: Inovacijų įvairiai yra, kartais tos invacijos labiau proceso veiklos pagerinimas, daug su veikla dirbam ir su sistemų diegimo sąsajom.

<...>

Jonas: buvo prieš du mėnesius pratybos Lietuvos mastu, kur su kariuomenė, kariuomenė važynėjo, mus įjungė, kaip būtent valstybinį ryšio operatorių, ir ką mes darytume, jeigu paveiktų, tai turėjom savo įrankius parodyt. buvo stalo pratybos kaip kas veikia. Kaip mūsų valstybės operacijų grupė veikia, ar iš IT, iš viešųjų ryšių, kaip, tarkim, nukritęs lektuvas, tai mes turėjom nusipirkę palydovinį ryšį, atrašėm, tai visi nustebo, kad mes palydovinį telefoną turim nusipirkę.

Viktoras Bulavas (Vilniaus Universitetas), virtualus interviu, 2024m. Gruodžio 10d.

Pasikeitė iš esmės požiūris į tai, kad anksčiau visi gynė kompiuterius namuose patys, o dabar yra NKSC, vyksta įvairios pratybos, ir mūsų žmonės dalyvauja tuose mokymuose. Esu ir aš juose dalyvavęs. Pasikeitė bendras mąstymas, nors jis dar nepasiekė kiekvieno žmogaus. Valstybė ir NATO jau priima sprendimus, kad reikia imtis centralizuotų veiksmų. Dalis sistemų jau perkelta į saugesnius tinklus.

Turime savo gynybos sistemas (pavyzdžiui, VU). VU, KTU ir Klaipėdos universitetas turi savo reagavimo centrą – virtualią organizaciją CERT. CERT ir CSIRT turi specifinius skirtumus.

Kadangi pasikeitė mąstymas, anksčiau universitete kiekvienas buvo atsakingas už savo darbo vietą. Dabar visi buvo pakviesti į "tvirtovę", tačiau ne visi prisijungė. Pasikeitė požiūris: įgyvendinama vidinė sauga administracijoms, o į vidinį potinklį kviečiami visi organizacijos nariai.

Strategija "kiekvienas už save" pasikeitė į bendrą apsaugą, bet tai nereiškia, kad žmogus neturi rūpintis savimi ir ginti savo sistemas. Kibernetinių paslaugų centras ieško spragų VU patikėtam paslaugų ruože. Vykdomas skenavimas, tikrinama, ar viskas saugu, ir, jei randama silpnų vietų (pvz.,

GMC), apie tai pranešama. Tos „skylutės“ stebimos, kad būtų užtaisytos. Aktyviai stebimas ir prižiūrimas perimetras.

Pagal naują direktyvą mes nesame kibernetinio saugumo objektas. Nauja įstatymo redakcija numato, kad iki balandžio 17 d. bus identifikuoti kibernetinio saugumo subjektai, tačiau VU kol kas į šį sąrašą nepatenka. Pagal kriterijus, mūsų veiklos išlaidos ir pajamos neatitinka reikalavimų. Nepaisant to, VU aktyviai įgyvendina saugos priemones, net jei direktyva mums yra tik rekomendacinio pobūdžio. Lygiai prieš metus KTU buvo masiškai užšifruoti. Iškeltas klausimas, ką daryti, kad mūsų to neištiktų, ir parengtas priemonių planas. Tie, kas yra vidiniame perimetre, turėtų jaustis saugiau. Tačiau per metus vyksta apie 25 milijonus atakų, siekiančių iššifruoti duomenis.

Dėmesys skiriamas vidinio atsparumo stiprinimui. Nors griežtų demarkacinių linijų nėra, pavyzdžiui, prieiga prie sistemų suteikiama tik iš autorizuoto tinklo. Atsarginės kopijos vis dar daromos – jei įvyktų užšifravimas.

DDoS atakos stabdomos įvairiais lygiais – ugniasienėmis, operatorių ar serverių lygiu. Taikomos konkrečios priemonės, kad užvaldytas serveris (pvz., kolegijos ar universiteto) nepatektų į užsienio agentų rankas ir neleistų jiems pulti iš vidaus tinklo.

Sprendimų priėmimas yra kolegialus – dalyvauja tarybos, LitNet atstovai ir CERT ekspertai. Vieni stiprina apsaugas, kiti rūpinasi reagavimu. Svarbu, kad daugiau žmonių mokėtų atskirti grėsmes ir reaguoti. Pratybos vyksta ne tik išorėje, bet ir viduje.

Budėjimas vyksta nuolat. Nauji sprendimai ir priemonės kyla reaguojant į išorines grėsmes. Pavyzdžiui, praėjusiais metais bibliotekos sistemos buvo atjungtos dėl KTU atakos, tačiau tai nesukėlė didelių nepatogumų.

VU turi veiklos tęstinumo planą – įvertintos didžiausios rizikos. Atsarginės kopijos, dubliuoti įrenginiai ir apkrovos balansavimas užtikrina sistemų veiklą. Geografinis pasiskirstymas leidžia apsisaugoti net nuo masinių trikdžių. Įrenginių autorizacija apsaugo nuo vagysčių – slaptažodį galima pavogti, tačiau fizinė prieiga prie kompiuterio ribota.

Žmonės raginami laikytis kibernetinės higienos. Komunikacija apie rizikas nuolat atnaujinama. Taip pat vykdomos socialinės inžinerijos pratybos – mokoma neatlikti veiksmų pagal abejotinus klausimynus ar prašymus. Didelė darbo įtampa kelia papildomų iššūkių, bet ugdomas žmonių atsparumas.

Nėra organizacijų, kurios nebuvo išlaužtos – yra tik tos, kurios apie tai laiku nesužinojo. Po rezonansinių atvejų, tokių kaip CityBee, VGTU ar KTU, visi siekia didinti atsparumą. Tačiau mūsų atveju negalima sakyti, kad turime stebuklingą sprendimą – bendruomenė turi tobulėti kartu.

Teorinis modelis neturi būti tik juoda ir balta. Reikia ieškoti balanso ir platesnių perspektyvų, įskaitant trečią ir ketvirtą dimensiją. Tik per tokį požiūrį galima užtikrinti organizacijos atsparumą ir efektyvumą.

Stanislav Sokolovskis (Vilniaus Rajono Savivaldybė), interviu sntrauka, interviu telefonu, 2024m. Gruodžio 10d.

1. *Kalbant apie jūsų organizacijos kibernetinio saugumo strategiją, ar pasakytumėte, kad ji labiau orientuota į atsparumą (tęstinumą/sistemų nepertraukiamumą ir gebėjimą prisitaikyti), ar į tradicinį rizikos ir grėsmių valdymą (atakų prevenciją ir žalos mažinimą)?*

Investuoja į nepertraukiamą darbą ir atsparumą; daug dėmesio skiriama tiek programinei, tiek techninei įrangai (hardware ir software), siekiant užtikrinti, kad nebūtų įsilaužimų. Ir ne tik prevencija, siekiant išvengti tokių situacijų, bet ir rengiamas veiksmų planas, kuris užtikrintų, kad įvykus atakai, būtų padaryta kuo mažiau žalos.

1. *Ar galėtumėte teigti, kad jūsų strategijoje daugiausia dėmesio skiriama atakų prevencijai, ar taip pat greitam sistemų atsistatymui ir prisitaikymui?*

2. *Kaip šiuo metu jūsų organizacija vertina savo kibernetinio saugumo atsparumo lygį?*
    1. *Kokie rodikliai ar metrikos naudojami atsparumui vertinti ir kaip dažnai šie vertinimai atnaujinami?*

3. *Kokių konkrečių priemonių ėmėsi jūsų organizacija, kad pasiruoštų galimiems kibernetiniams incidentams?*
    1. *Ar yra įdiegtos atsarginės sistemos arba atkūrimo protokolai? Kaip apie šias priemones komunikuojama organizacijoje?*

4. *Ar galite pateikti neseniai įvykusio kibernetinio incidento pavyzdį, jei toks buvo, ir apibūdinti savo organizacijos atsaką?*

Apie incidentus galiu pasakyti, kad gruodžio 5 d. buvo įvykdyta savivaldybės ataka (TELIA turi interviu apie šią ataką). Rajono savivaldybė tokiai atakai nebuvo tinkamai pasiruošusi – trūko specialistų, iš esmės dirbo tik du su puse žmogaus, atsakingų už 700 žmonių sistemą. Po šios atakos buvo suformuotas naujas skyrius, priimti papildomi specialistai ir glaudžiai bendradarbiauta su KVTC. Visa duomenų bazė ir serveriai buvo perkelti į duomenų centrą, o saugumui užtikrinti įsigyta naujos kartos antivirusinė programa.

Pirmiausia buvo suformuotas ir sustiprintas skyrius, siekiant išvengti visų atsakomybių sukoncentravimo vieno žmogaus rankose, nes vienam atsakingam darbuotojui buvo per sunku susitvarkyti su tokio masto iššūkiais. Ataka buvo įvykdyta labai profesionaliai, naudojant sudėtingas

programines priemones, todėl tai buvo rimtas ir sudėtingas incidentas. Manoma, kad jei būtų turėta daugiau žmogiškųjų išteklių, reakcija galėjo būti greitesnė, pavyzdžiui, laiku atjungti visus serverius nuo tinklo.

Šiuo metu įgyvendintos priemonės užtikrina, kad įvykus panašiai atakai būtų prarasta tik keletas dienų ar mėnesių duomenų, o ne metai, kaip buvo šios atakos metu. Visgi reikia pripažinti, kad įsilaužėliai taip pat tobulėja. Vieni kuria programinę įrangą su spragomis, o kiti tas spragas aktyviai ieško.

1. *Kokia buvo išmokta patirtis ir kaip ši patirtis paveikė jūsų organizacijos kibernetinio saugumo planavimą?*

5. *Kokie, jūsų nuomone, yra pagrindiniai iššūkiai pereinant nuo rizikos/gėsmių valdymo požiūrio prie atsparumu grindžiamo požiūrio?*

Atakos paprastai išsprendžiamos greitai – tereikia pasakyti, ko reikia, ir mes tai suteikiame. Visgi didžiausias iššūkis buvo komandos suformavimas ir efektyvus darbo pasidalijimas. Pirmas žingsnis buvo suburti komandą ir aiškiai paskirstyti atsakomybę: vieni atsakingi už vienas sritis, kiti – už kitas. Didžiausias darbo krūvis tenka aptarnavimui, nes žmonės nuolat skambina ir užkrauna IT skyrių netinkamomis problemomis. Dėl to nelieka laiko spręsti tikrųjų uždavinių.

Svarbu paminėti, kad IT ir saugumo skyrius turi būti atskirti. Dėl darbo krūvio neturėjome galimybės lankyti seminarų ar organizuoti mokymų. Tačiau dabar jau pradedame rengti spamo ir phishingo testus. Rezultatai buvo gana įdomūs: iš maždaug 200 žmonių apie 40% vis tiek užpildė netikras formas. Didžiausia grėsmė kyla būtent iš el. laiškų – žmonės nepatikrina, ką spaudžia, taip suteikdami prieigą prie savo kompiuterio ir mūsų tinklo.

Šiuo metu įgyvendinome papildomas saugumo priemones. Administravimo dalykai yra sprendžiami per aktyvią direktoriją – visi kompiuteriai turi administravimo slaptažodžius, todėl niekas negali savavališkai instaliuoti programų ar atlikti kitų nesankcionuotų veiksmų.

1. *Su kokiomis konkrečiomis kliūtimis susidūrėte įgyvendindami kibernetinio saugumo (ar atsparumo) strategijas, jei tokių yra?*

6. *Kokį vaidmenį jūsų organizacijos kibernetinio saugumo strategijoje atlieka atsparumas bei bendradarbiavimas su išorės organizacijomis (viešosiomis ar privačiomis)?*

Kai įvyko ataka ir darbuotojai pradėjo kreiptis pagalbos, nelabai atrodė, kad organizacija tiksliai žinojo, ką reikia daryti. Galbūt jie žinojo, ką reikia atlikti teoriškai, bet praktikoje – nelabai. Organizacija turi bazę ir instrukcijas, tačiau realiai daugiausia pagalbos suteikė „Telia“. Po atakos buvo skirtos baudos už tai, ko nepadarėme, bet niekas nesigilino į tikrąją situaciją. Be to, kai paprašai pagalbos, ne visada aiškiai pasako, ką ir kaip reikia daryti.

Krašto apsaugos sistema suteikia daugiau realios pagalbos, ypač organizuojant phishingo testus. „KVTC“ taip pat kažkiek padeda, bet trūksta kvalifikuotų žmonių. Jei reikia pagalbos iš tinklo specialistų, tai užtrunka labai ilgai, o patyrę specialistai brangiai kainuoja. Jei paimsime, pavyzdžiui, mažesnę savivaldybę, kaip Akmenės, sunku įsivaizduoti, kaip jie viską tvarkys. Reikalavimų daug, instrukcijos sudėtingos, o resursų ir žinių – mažai. Vilniuje vis tiek turime daugiau išteklių ir supratimo, bet net ir čia žmonių trūkumas labai jaučiamas. Jei giliniesi į licencijas, tai nelieka laiko tvarkyti kitų svarbių užduočių.

Turime dokumentų valdymo sistemą, tačiau dažnai kyla problemų. Pavyzdžiui, ateina žmonės ir sako, kad vienas ar kitas dokumentas neturėtų būti matomas tam tikram asmeniui. Mes siūlome sudaryti „medį“, kuris nurodo, kas ką gali matyti. Tačiau po to parašoma, kad IT skyrius turi tai įgyvendinti. Tuo metu mes dažnai nežinome, kas konkrečiai turi prieigą prie ko, nes nėra aiškių taisyklių. Dabar rašome taisykles, kurios padės viską struktūrizuoti. Kol taisyklės nėra pilnai parengtos, kyla daug klausimų ir netvarkos. Be to, IT skyriui tenka spręsti ne tik techninius, bet ir saugumo, prieigos bei kitus klausimus, kurių turėtų imtis skirtingi skyriai.

Kol taisyklės bus aiškiai apibrėžtos ir patvirtintos, problemos dėl prieigos ir saugumo išliks. Dėl to labai svarbu, kad kiekvienas vedėjas atsakingai spręstų savo srities klausimus ir nereikėtų visos atsakomybės užkrauti IT skyriui.

7. Kaip šis bendradarbiavimas paveikė jūsų organizacijos atsparumą?

8. Ar jūsų organizacija įtraukia atsparumo didinimo planavimą į platesnę strateginę sistemą? Jei taip, kaip?

Savo serverinės dar neperkėlėme, tačiau dabar pradedame organizuoti monitoringo sistemą. Sistema veiks taip, kad jei bus pastebėta ataka, visi rodikliai pradės žaliuoti arba raudonuoti, o budinčiam darbuotojui iš karto bus pateikta reikiama informacija.

Kalbant apie el. laiškus, visi neaiškūs laiškai turi būti siunčiami tikrinimui – klausiama, ar galima juos atidaryti, ar ne. Jei visgi įvyksta ataka, pagrindinis protokolas yra atjungti tinklą ir elektros tiekimą. Tai yra svarbiausias veiksmas, kuris taikomas tik masinės atakos atveju, kai įsibrovėlis jau būna patekęs į vidinę sistemą.

Svarbu pažymėti, kad įsilaužėliai veikia ne taip, kad tiesiog randa spragą ir iškart atakuoja. Jie gali „gyventi“ sistemoje pusę metų, ruošti savo sistemas, rinkti slaptažodžius ir ruošti ataką. Dėl to būtina stebėti anomalijas, kurios atsiranda sistemoje, pavyzdžiui, neaiškius prisijungimus iš nežinomų šaltinių. Stebėjimo programos yra tam skirtos – jos seka veiklą ir fiksuoja įtartinus veiksmus.

Įsilaužėliai yra gerai pasiruošę, daug išmano ir moka pasislėpti. Tai nėra atsitiktiniai žmonės, o profesionalai, kurie gerai supranta savo veiksmus. Todėl būtina ne tik stebėti sistemą, bet ir nuolat tobulinti saugumo priemones.

1. *Ar yra specialių komandų ar resursų, skirtų užtikrinti atsparumą atakoms, ir kuo šis požiūris skiriasi nuo tradicinio rizikos/grėsmių valdymo?*

9. *Kaip jūsų organizacija sprendžia balansą tarp duomenų saugumo, bandymo aptikti grėsmės, jų išvengti, kas reikalauja sistemos stebėjimo ir darbuotojų ar klientų privatumo?*

Su šia problema kol kas nelabai susidūrėme. Darbuotojų slaptažodžiai galioja tik konkrečiam darbuotojui ir jo paskyrai, niekas kitas jų nenaudoja. Tačiau netrukus įdiegsime monitoringo programą, kuri leis stebėti, kas ką veikia sistemoje, kad darbuotojai netyčia ar tyčia nenueitų ten, kur nereikia.

Taip pat yra darbuotojų, kurie dirba iš namų su savo asmeniniais kompiuteriais (notebookais). Dabar diegiame sistemą, kuri leis iš karto matyti, jei bus bandymai prisijungti prie tinklo. Bus aiškiai nustatytos leistinos ir neleistinos priemonės. Jei darbdavys nori prisijungti prie darbuotojo kompiuterio, pavyzdžiui, kad sutvarkytų technines problemas, darbuotojas turi suteikti leidimą. Tokiu būdu užtikrinamas saugumas ir išvengiama piktnaudžiavimo.

Be to, informacija ir dokumentų valdymo sistema yra apribota pagal prieigos lygius: kiekvienas darbuotojas mato tik tai, kas jam priklauso. Atlyginimus ir kitą jautrią informaciją mato tik buhalterija. Visa ši sistema dar tobulinama ir bus įdiegta artimiausiu metu.

1. *Kokią įtaką šiai pusiausvyrai turi teisės aktų laikymosi reikalavimai?*

10. *Kokios mokymo ar informuotumo didinimo programos padeda įgyvendinti jūsų organizacijos kibernetinio saugumo atsparumo strategiją?*
    1. *Ar šiomis programomis siekiama labiau skatinti rizikos/grėsmių mažinimą, ar jomis taip pat siekiama pagerinti atsparumą - reagavimą ir prisitaikymą po incidento?*

11. *Kaip jūsų organizacija pasiruošusi reaguoti į galimus naujų technologijų kibernetinius iššūkius per ateinančius penkerius metus?*

Šiuo metu jau turime aiškią viziją ir veiksmų planą, taip pat paruoštą penkerių metų strategiją. Plane numatyta, kokie projektai bus įgyvendinti, kokia įranga bus nupirkta, ir tam skirta konkreti biudžeto suma.
Vis dėlto, reikia pripažinti, kad per penkerius metus situacija gali pasikeisti, tačiau finansiniai resursai jau yra suplanuoti ir numatyti būsimiems veiksmams.

Lyginamieji klausimai apie atsparumą ir rizikos valdymą

10. *Kokią konkrečią atsparumo praktiką, pavyzdžiui, atsarginių kopijų sistemas, reagavimo protokolus ar tarpžinybinį bendradarbiavimą, įgyvendino jūsų organizacija, kad užtikrintų veiklos tęstinumą atakos metu?*
    1. *Kaip manote, kiek veiksminga ši praktika, remiantis ankstesniais incidentais?*

11. *Kokios praktikos, jūsų nuomone, padeda užtikrinti organizacijų, kurios sėkmingai susidoroja su kibernetiniais incidentais ir patiria minimalius trikdžius, atsparumą?*

Pirmiausia labai svarbus yra pačios organizacijos vadovo supratimas. Jei vadovas rimtai priims mūsų rekomendacijas, įvertins situaciją ir atsakingai į tai žiūrės, jau bus pasiekta 50% sėkmės. Likusią dalį galime užtikrinti mes – žinome, kaip auklėti darbuotojus, prižiūrėti, kad slaptažodžiai būtų tinkami, ir palaikyti bendrą kompiuterinės higienos standartą.

Dabar planuojame įdiegti „Google“ antrinę sinchronizaciją – tai yra būtinas žingsnis, kurį privalome atlikti. Tai yra pagrindas. Visa kita, pavyzdžiui, log'ų analizė, siekiant identifikuoti bandymus įsilaužti, taip pat bus sutvarkyta.

Esminis dalykas – užtikrinti kompiuterinę higieną. Turime priversti žmones laikytis šių taisyklių, paaiškindami, kodėl jos yra svarbios. Viskas turėtų būti pateikta labai paprasta kalba ir suprantamai, pabrėžiant, kad negalima naudoti lengvai atspėjamų slaptažodžių. Tinkamas švietimas ir aiškus komunikavimas yra raktas į sėkmę.

1. *Ar manote, kad tai yra praktika, kurią jūsų organizacija galėtų pritaikyti, o gal yra priežasčių, dėl kurių ji netaikytina?*

12. Priešingai, kodėl, jūsų nuomone, kai kurios organizacijos patiria didelį poveikį kibernetinių išpuolių metu, o kitoms pavyksta išvengti didelių trikdžių?
Vadovai nepastebi, kada ivyksta ivykis, o taip tai ne. O kita spraga tai darbuotoju higiena.

1. *Ar, remiantis jūsų patirtimi, tai visų pirma susiję su išteklių, planavimo ar reagavimo strategijų skirtumais?*

Su valdymu ir politika susiję klausimai

14. Kaip Nacionalinis kibernetinio saugumo centras (NKSC) daro įtaką jūsų organizacijos kibernetinio saugumo politikai ar atsparumo strategijoms?

Dėl įstatymų viskas priklauso nuo to, kiek vadovai yra pasirengę juos priimti ir įgyvendinti. Po mūsų praktikoje patirtos atakos į šiuos reikalavimus pradėjome žiūrėti labai rimtai. Suprantame, kad šie procesai yra brangūs, tačiau būtina vykdyti bent jau tai, kas įstatyme numatyta kaip minimalūs reikalavimai.

Tie, kurie rengia įstatymus, rašo juos remdamiesi maksimaliomis galimybėmis, tačiau įgyvendinti tai praktiškai yra sudėtinga, ypač mažesnėms organizacijoms. (Būtų verta pasidomėti, ar įstatyme yra numatyta diferenciacija tarp mažesnių ir didesnių organizacijų ir kaip jos turėtų vykdyti šiuos reikalavimus skirtingai.)

Mes tikriname, kaip suprantame įstatymą, ir lyginame, ar teisingai jį interpretuojame. Visgi lieka tam tikra erdvė interpretacijai, todėl svarbu nuolat vertinti savo veiksmus pagal keliamus reikalavimus.

1. *Ar NKSC gairės paskatino kokius nors konkrečius pokyčius, susijusius su kibernetinio saugumo incidentų valdymu?*

15. Ar jūsų organizacija privalo pranešti NKSC apie kibernetinius incidentus? Jei taip, kaip tai veikia jūsų kibernetinio saugumo planavimą ir reagavimą?

1. *Jei pranešti neprivaloma, ar manote, kad savanoriškas pranešimų teikimas galėtų būti naudingas, ar yra trūkumų?*

16. Pagal naująjį kibernetinio saugumo įstatymo keitimą, jūs priklausot ypatingos svarbos sektoriui. Kaip nauji kibernetinio saugumo įstatymo pakeitimai paveikė jūsų kasdienes praktikas ir planavimą?

17. Kokios, jūsų požiūriu, yra pagrindinės Lietuvos bendros kibernetinės politikos sistemos stiprybės ir silpnybės, susijusios su atsparumo palaikymu?

1. *Kokius patobulinimus siūlytumėte, kad būtų padidintas nacionalinis atsparumas, ypač viešojo ir privačiojo sektorių bendradarbiavimo srityje?*

Baigiamieji klausimai

18. Apmąstydami savo patirtį, ką patartumėte kitoms Lietuvos organizacijoms, norinčioms padidinti savo kibernetinio saugumo atsparumą?

irmiausia, reikia kantrybės ir tikslingo požiūrio bei gebėjimo paaiškinti vadovui, kodėl šie dalykai yra svarbūs ir kokios gali būti pasekmės. Reikia pateikti kuo daugiau konkrečių pavyzdžių. Jei tiesiog nueisite pas vadovą ir jis nesupras situacijos rimtumo, rezultatas bus neigiamas. Todėl svarbu aiškinti ir rodyti praktinius pavyzdžius, pavyzdžiui, organizuoti phishingo testus ir parodyti jų ataskaitas. Iš anksto perspėkite apie patikrinimą, o po to parodykite vadovui, kiek procentų darbuotojų neatpažino paprastų grėsmių. Tai padės vadovui suprasti problemos rimtumą ir gali paskatinti finansavimą.

Dažnai vadovai pradeda rimtai žiūrėti į šiuos dalykus tik po įvykusios atakos. Tačiau ar verta laukti, kol atsitiks incidentas, kad pradėtume veikti? (Ši idėja apie testus ir aktualumo parodymą yra labai įdomi, nes tai leidžia apeiti situaciją, kai tobulinama tik po atakų – per praktiką.) Dauguma vadovų mano, kad visa atsakomybė tenka IT specialistams, tačiau IT komanda jau turi daug svarbesnių užduočių, tokių kaip įstatymų peržiūra, kibernetinis saugumas, o ne „Word“ problemų sprendimas ar kursų organizavimas. IT specialistai turėtų turėti galimybę mokytis, tobulėti ir domėtis naujovėmis, nes kibernetinis saugumas yra labai sparčiai besikeičianti sritis.

Svarbu, kad vadovai suprastų šių klausimų rimtumą prieš įvykstant incidentui, o ne po jo. Investicijos į saugumą neturėtų būti daromos tik po krizės. Palaipsnis finansavimas yra daug efektyvesnis nei vienkartinis didelis biudžetas. Be to, yra daug įmonių Lietuvoje ir pasaulyje, kurios supranta saugumo svarbą ir yra pasirengusios už tai sumokėti.

Dar vienas geras pavyzdys – tai, ką padarė mūsų administracijos direktorius. Po atakos jis iš karto paskelbė pranešimą, kad rajonas buvo atakuotas, paslaugos sustabdytos, ir informavo visuomenę apie

situaciją. Tai buvo labai teisingas žingsnis. Informacijos neslėpimas padėjo sumažinti klausimų kiekį ir leido ramiai dirbti toliau. Pavyzdžiui, kai buvo pranešta, kad sistema nulaužta, buvo aiškiai pasakyta, kad šį mėnesį paramos mokėjimų nebus, o kitą mėnesį jie bus atnaujinti. Tokia komunikacija padeda sumažinti įtampą. Jei informacija būtų slepiama, žiniasklaida vis tiek ją atrastų, o tai sukeltų daug daugiau klausimų ir problemų.

1. *Ar manote, kad atsparumo strategijos užtikrina geresnius rezultatus nei tradiciniai į riziką ir grėsmių valdymą orientuoti metodai?*

19. *Kokie, jūsų nuomone, yra esminiai veiksniai, padedantys įgyvendinti veiksmingą atsparumo strategiją Lietuvos kontekste?*

    1. *Ar šie veiksniai yra pasiekiami pagal dabartinę politikos sistemą, ar jiems reikia papildomos reguliavimo ar išteklių paramos?*

Šiais klausimais siekiama atskleisti įžvalgas apie tai, kaip organizacijos pereina prie atsparumo, nustatyti sėkmingas atsparumo strategijas lemiančius veiksnius ir suprasti nacionalinės kibernetinio saugumo politikos įtaką vietos praktikai.

Adomas Bužinskas, Vilniaus Savivaldybė, Administracijos Vadovas, interviu, Vilnius, 2024 metų, Gruodžio 11d.

Dominyka: Kaip srepndžiat prioritetus būtent tarp kibernetinės saugos grėsmiu / rizikos valdymo, tos prevencijos, bandymo lopyti spragas, kad tos atakos neįvyktų, ir tos atsparumo, suvokimo, kad ataka įvyks, ir reik viską dayrti, kad jai pasiruošti?

Adomas: Jonas atsakinėjo iš techninės pusės…mes turim savivaldybėje, kad bendrai įsivaizduot, vien administracijoje apie 1050imt darbuotojų, visoj sistoj - 35is tūkstančius. Taip gaunasi, kad mes kaip didelis holdingas veikiam, žiūrint iš verslo pusės. Tai viena, ką mes čia turim savivaldybėje, man Jonas neleidžia sakyti, kad mes gerai susitvarkę, bet manau, kad mes gerai susitvarkę, yra šiek tiek kitas lygis kitose organizacjose. Labai skiriasi nuo pačios organizacijos ir kuriam lygyje esam, tai kas liečia savivaldybę, tia pačią administracija, tai tos atakos pastoviai vyksta, kiek aš suprantu, tai mes ruošiames tam preventyviai žinodami, kad tai įvyks, yra skirtingos programos, kur mokam, kad žmones patys įsilaužynetų ir rodytš spragas, tai pakankamai aišku, į kurią pusę išjudam. Įmonės grupėje daugiau aišku į kurią dalį eitų, į tą dalį kaip ir mes, stiprios pakankamai organizacijos, ir yra

dalis organizacijų, kurios dar su XP windowsais. Nu, ta prasme, labai neididelė dalis, bet ji irg yra. Ir techniškai, jeigu ji išteka iš mūsų sistemos duomenis, tai vis tiek esam atsakingi. Tai dabar, kad suprast, tvarkomes sistemiškai mes, tokį atsparumo skyrių šiais metais įkurėm, kuris turi ir cyber visą, tai jo tikslas yra visą grupę apjungti, ne tik vienuoliką įmonių, tai yra ir visas sveikatos sistemas, kad visi turėtų bent vienodą lygį.

Dominyka: Labai įdomu apie tą atsparumo skyrių paklausyti, nes jo, atsparumas yra tas konceptas, iš kurio aš vedu kibernetinį atsparumą. Kodėl čia sugalvojot jį sukurti?

Adomas: Tai čia yra keletas dalykų, tai pirmas yra vindikacija, toks, kuris, matyt, yra vienas iš pagrindų. Tai vindikacija yra susijusi su vidaus tvarka, kad neištekėtų pinigai ten, kur jie neturi ištekėti, bet dažniausiai niekas nekuria ten tik tai tų vindikacijos skyrių, jie priskiria jiems platesnę kompetenciją. Tai be tų auditų, preventyvių veiksmų, sankcijų kuravimo ir pan., jiems atitinka ir cyber security kaip atsparumo dalis. Anksčiau Jonas tai darydavo iki to laiko, dabar jie daro kol kas kartu. Faktas, kad įgyvendins Jonas, bet atsparumo skyrius jau visą sistemą, visą įmonių grupę nuleis bendrus reikalavimus, ten jau cyberio žmonės plėsis, kurie peržiūrės ir sveikatos įstaigas, vėliau mokyklas, ir jau mūsų įmonių grupės atsparumo skyrių vadovai su jais konsultuojas ir panašiai. tai čia yra toks noras apjungti, nes per NATO summit'ą aiškiai matėsi, kad, tarkim, mes kaip organizacija savivaldybės administraciją atlaikėm, bet pvž., Go Vilnius stend'ai buvo nulaužti, tai ten nelabai pasimatė. Dar buvo viena ataka, kur mūsų sistemos neatlaikė vilniaus apšvietimo. Buvo įsilaužta dienos metu ir atjungtas apšvietimas, tik kad dienos metu nebuvo aktualu, bet spėjom viską sutvarkyti iki vakaro ir atlaikyti. Tai gaunasi, kad vis tiek sistema….aš kaip vadovas administracijos negaliu pasakyti, kad viskas ok, kol mūsų subsidijos nėra pasiruošusios. Tai apie tai yra tas atsparumo skyrius, kad mūsų bendrą standartą pritaikyti kitur ir kai būna tos didesnės atakos, ir jie daro srautą, kad tas srautas nueitų į nepasiruošusias organizacijas, tai vat…bet iš tos pusės mes niekad nesakom, kad esam fully pasiruošę, bet čia yra neklausimas "ar gali įsibrauti?", o "per kiek laiko?". kol kiti yra silpniau pasiruošę, mes esam stiprūs.

Dominyka: supratau. tai kitas mano klausimas - kaip vertinate teiginį, kad išorinės grėsmės neišvengiamos, dėl to svarbu investuot į atsparumo stiprinimą ir ne tik į tą grėsmių prevenciją, tai jau ką tik pasakėt, kad neišvengiamos atakos, o toliau kalusimas būtų ar ši nuostata atsispindi jūsų vadovaujamame požiūryje? Tai aš, kaip suprantu, tai, kad yra tas skyrius kuriamas, viskas vis tiek ateina iš viršaus, tai tas požiūris, kad…

Adomas: nu tai mes iš vadybinės pusės, jeigu taip grynai, tai mano tikslas yra susamdyt gerus žmones savo srityse ir tas sritis padengti. Tai tas sritis nebuvo padengta, mes sukūrėm tą padalinį, aš iš esmės neateinu ir nenurodau jiems kaip ką daryt, jie ateina pas mane su sprendimais, biudžeto poreikiu ir panašiai, tai jau tą mes managinam. Bet faktas, kad įkūrę tą skyrių, ką as jau minėjau administracijai, kad tu pasidarysi auditą tam tikrų sričių, IT saugumo ir pamatysi, kur esam, tavo biudžeto poreikis smarkiai išaugs. Tai vat planuojant 2025ų metų poreikį jau yra daug cyber security dalių, kurias mes uždengiam ir jos eina milijonais, reik suprasti. šitoj dalyje yra prioritetas, ta prasme čia tiesiog aš tai vertinu net ne kaip prioritetą, bet kaip higieną, kaip užsirakinam duris vakare pastato, taip ir sistema turi mano būti be skilių visa. Tik kol mes ją sutvarkysim, tai daug kainuos, bet to pasitikėjimo, kasdieną gal tos paslaugos žmonės nejaučia, bet, jeigu kažkas nutiktų, tai labai kaltu per pasitikėjimą. Kaip ir visos savivaldos paslaugos - atliekų vežimo ten, karšto vandens - nejauti tol, kol paslauga veikia, bet jeigu jau kažkas sutrinka…

Dominyka: tikrai taip. Du klausimai iš to plaukia - pirmas, tai vienas dalykas, ką pastebėjau, kalbėdama su žmonėmis, kad jie išskiria kaip viena iš sunkumų, būtent kibernetinio atsparumo to viso, kad vadovai ne visuomet supranta poreikį, ir kad jiems reikia atnešti tam tikrą informaciją, nu pvž., tikriausiai pastebėjot po NATO summit;o, kad vyksta atvejis, tada pastebi vadovai ir tam tikrą rimtą reikalą, kad čia reikia kažką daryti. Nes kitas dalykas, ką išgirdau, ir kas buvo įdomu, tai kad būtinai reikia atakos, kad greičiausiai ir realiausiai mokaisi, kai įvyksta reali grėsmė, bet užtenka daryti tam tikrus testus ir rodyti rezultatus, kad yra prasti reikalai. Tai kas atkreipia dėmesį? kas būtent įtikina, kad reikia kažką daryti?

Adomas: nu tai man atrodo čia iš mano pusės žiūrinti apskritai svarbu turėt IT vadovą gerą, tiek tos vadybinės dalies, tiek tos CTO, kuris prioritetus padraftintų, ir tada natūraliai iš to pasitikėjimo kyla kiti prioritetai. Jie ateina su savo brangiais žaislais, kaip aš sakau, kur pasako, kad va nusipirksim šitą licenziją, kuri realiai organizacijos gyvenimo nepakeis, tu kaip eilinis darbuotojas ar vilnietis, ar paslaugos gavejas nepamatysi, tai tu turi įverinti, kas gali atsitikti, jeigu to nebus. Tai kažkaip man atrodo esmė yra, ypač to viešo adnistravimo tose įstaigose, versle tai tu viską vertini pagal tai, pasiskaičiuoji riziką, kiek pinigų gali prarasti, jeigu paslauga neveiks, arba ten duomenys nutekės. Viešam sektoriuje gal yra šiek tiek kitaip, daug kas vyksta ciklais, vertinama per politinę prizmę. Tai aš įsivaizduoju, kad kokiose mažose organizacjose tai yra daug sunkiau turėti , kokį biudžėta vien dėlto, kad to nemato žmonės. Tu neišasfaltuosi to IT saugumo, ar nepastatysi jo kažkaip tai. tai čia yra pasitikėjimo dalykas, me skažkaip neturim organizacijoje tos problemos. ir manau, kad tas atsparumo skyrius ir tam tikri sprendimai, kuriuos darys CTO ar apskritai jegų sutaupys. Tai mes esam tą šiek tiek su rezultatais surišę, per procesų tobulinimą ir apskritai, tai tas IT biudžetas mūsų

didelis, bet mes esam jau susigyvenę su tuo kaip su higiena. Va dabar yra didesnė išlaidų eilutė dvidešimt penktiem metam, nes kabinam kitas įstaigas, kurios niekad gyvenime nei licenzijų nesipirko nei ką, turėsim samdyt kokius keturis papildomus žmones, tai bus, bet kitu atveju…nu ta prasme iš mano puses tai aš suprantu, tai man…o kas tai įtikina, tai aš sakyčiau elementarus rizikų valdymas, nes jeigu kas ne taip nutiktų, tai būtų problema daug didesnę. Jeigu tu reaktyviai reaguoji, taip sakyčiau.

Dominyka: Supratau. O tada, tarkim mažesnės organizacijos, aš tik nežinau kaip vyksta tie viešieji valdymo procesai, ar jūs priversit jas susiimti ir daryt tam tikrus sprendimus ir jos bus pačios atsakingos ir turės priimti tam tikrus sprendimus, ar jūs ir patys finansuojat tas mažesnes įmones ir tuos sprendimus, kad jos turi susitvarkyti? Nes kitas klausimas turėtų būti, kad mažos organizacijos neturi nei resursų, nei pinigų tam.

Adomas: tai bendrai visa ta corporate valdymo logika mūsų veikia, kad mes išleidžiam akcininko lūkesčių laiškus, duodam jas valdybom, valdybos pagal akcininkų lūkesčių laiškus nustatinėja įmones metinius tikslus, veiklos strategiją draftina, tada tai atsigula į vieną veiklą. Tai cybersecurity yra vienas iš nedaugelio prioritetų įrašytų akcininkų lūkesčių laiške visose beveik organizacijose, ką rašėm, tai tokie beveik bendrinė dalis, tai ta peasme iš tos tokios korperatyvinės loogikos per tai implementuojam, jeigu žiūrėt per tą didelę organizaciją kaip mes ten priverčiam nepriverčiam, tai iš tos korperatyvinės logikos jau valdyba akcininkui atsakines tik pagal lūkesčių laiškus, kur jau yra parašytas mūsų prioritetas, ir jie formuodami biudžetas ir visą kita jau tam skirs dėmesio. kas liečia mažesnes organizacijas ir patį finansavimą, tai aš gal biški apskritai kitaip į tai žiūriu, man didelio skirtumo ar finansuojasi mažesnė organizacija pati, ar mes, ar dar kažkas, tai vis tiek yra miesto pinigai in general. Tai ar tu iš vienos kišenės, ar iš kitos ištraukti, tai nu didelio skirtumo nėra. faktas,k ad dalį dalykų centralizuotai daryt yra tiesiog pigiau. Pvž., ką mes dabar darysim, tai visas licenzijas, tai ten microsoft iki kitur pirksim centralizuotai. Tai paėmus ar ten perkkam tūkstantį licenzijų čia, ar ten dešimt tūkstančių licenzijų per įmonių grupę, aš čia iš palubės tuos skaičius imu, tai ta prasme kaina, sąlygos yra kita.Tai dalį dalykų pirkti centralizuotai, ne finansuot, bet pirkti, jau yra pigiau, o kas liečia mažesnes organizacijas, tai jau dalį organizacijų full time cybersecurit žmogaus net nereikia, tai mes jį smadom čia ir jis coverina penkias organizacijas. Tai kai yra tas pasirpiešinimas iš tos pusės, kad kažkas tai maži, neturi pinigų ir tada mes tieisiog pasidarom centralizuotai ir būna paprasčiau, nes mažos organizacijos gali sukurti didelę problemą, kuri vis tiek bus mūsų, o ne jų.

Dominyka: noriu pasitikslinti - kai sakot, kad cyber žmogaus nereikia pilnu etatu, tai už ką tas cyber žmogus atsakingas, tik tai už tą strategijų deliojimą, žinių pasidalinimą?

Adomas: ne, tai as turiu omeny, nu jeigu tu esi, tarkim, nežinau, organizacija, kuri ten dirba kokioj nors centralizuotoj platformoj, kuri nuo tavęs nepriklauso, tarkim e-sveikata, ir ten pas tave yra kokių dešimt žmonių ir tu teiki tris paslaugas, tai tiesiog cyberistas neturės ką dirbti, iš tos pusės. pas mus tu gali 24/7 dirbti, ne iš tos pusės, kad scope darbų yra mažas, bet pačios organizacijos scope yra mažas. Tarkim, mokyklose kokiose, tai yra mokykla, yra tas IT ūkio dalį gali užkabint ant kokio paprastesnio žmogaus, bet, tarkim, cyberistas jis biški ktius dalykus daro, tai tau jo mokykloj full time tikrai nereikia. Dalis apskritai iš išorės perka tą paslaugą, kas irgi yra variantas išorinį jį turėt, kas irgi turi pliusų minusų, bet kol kas mes bandysim viduj jį turėti.

Dominyka: Jonas dar minėjo, kad IT skyrius rūpinasi ir saugumu, kas, iš esmės, yra sunku, nes tada sunku dėliotis prioritetus, nes tu gauni tuos tradicinius dalykus, kuriuos tvarko IT skyrius, kaip naudotis word ir pan.,, ir tada yra rimtesnis prioritetai, kaip saugumas, kuriems ne visada užtenka laiko. tai jis minėjo atskiro kibernetinio saugumo skyrių, kad bus, bet gal jis turėjo omenį šitą kibernetinio atsparumo skyrių?

Adomas: atsparumo, taip. Ne, tai dabar taip ir yra, kad taip buvo pas Joną ta visa atsparumo dalis, ir iš organizacinės pusės apskritai nėra gerai, kai tu perki, įgyvendini ir kontroliuoji. Nu ta prasme čia jau ir iš antikorupcinės pusės nėra gerai, bet ir bendrai net su tuo pačiu Jonu, kuris šiaip yra labai normalus vadovas, jis sako mes pasitarėm, tai gerai darom, bet nebūtinai mes ten gerai darom. dėl to ta cyber dalį atskiriam į ktią skyrių, kad gautų jie didesnį scope, kad nebūtų taip, kad cyber dalį suvalgo visa buitis, kaip sakant pajunginėt kompus. Bet nereiškia, kad mūsų IT skyrius, kuris darė šitą, ir darė gerai iki tol, dabar ten kažkur šone yra, bet kuriuo atveju visą tą sistemą JOnas su atsparumo skyriaus žmonėm ir kuria. Bet kuriuo atveju šitas yra ne pilni metai kaip įsteigtas, tai mes taip step by step žiūrim ir dėliojames sistema, ir Jonas bet kuriuo atveju visur dalyvauja kaip IT vadovas, bet tik rankas mes permetam į tą skyrių, kad įgyvendinias ten būtų, bet sprendimų priemime bet kuriuo atveju dalyvauja ir jis, nes jis yra kertinis žmogus visos sistemos.

Dominyka: Gerai, bet tada toliau einant toliau iš visų šitų daltkų, ką įvardinot, ką reikia pasidayrti, kaip galvojat, ką mąstot, tai kokie yra išskirami iššūkiai šito kibernetinio atsparumo, apskritai gal kiberetinio saugumo įgyvendinime? kaip, galbūt, vadovybė gali palengvinti tuos iššūkius, ar dalis tų iššūkių gali būti palengvinti vadovybės pasiraštymu?

Adomas: nu tai čia kaip ir visos ekonomikos dlema - kaip susidėlioti prioritetus ribotais ekonominiais ištekliais? tai čia man atrodo bendrinis toks prioritetas, man atrodo, aš kaip sakau, nenoriu girtis, kas

veikia pas mus organizacijoje, bet man atrodo pas mus ta atsparų sistema visai veikia. Mes ten tikrai neturim rolls royce, taip sakant, pagal visą saugumo dalį, ką galim daryt, bet tikrai ir ne su golfu važinėjam. Ta mes man atrodo esam visai sveikam viduriuke. Faktas, kad visad IT žmonės ateis ir neš geriausius ir saugiausius dalykus, bet man atrodo vadovo atsakomybė nepamesti proto A, o B skirti pakankamus resursus, tai vat ką mes dabar ir darom su sveikatos priežiūros įstaigom, tai man atrodo geras pratimas nuo A iki Z, kai buvo trys variantai pateikti kaip galima juos tvarkyt, ten bazinis, tada toks patenkinamas ir jau super mega. tai faktas, kad mes eisim link vidurinio, bet kai eisi blogoje padetyje, su XP windowsais važiuoji, tai nėra taip, kad nusiperki brangiausią ir turi dar labai daug step'ų pereit į priekį. Tai va čia man atrodo didžiausias iššūkis, kai niekas nedaryta yra ir tada pinigų reikia krūvą sukišt, tai pas mus buvo su sveikatos įstaigom daug iššūkių, kai ten jau eina tokie pinigai, kur renkiesi tarp naujos įrangos ir cyber security, tai įtampa atsiranda, bet čia jau yra vadovybės ir vadovų atsakomybė prieš juos atstovėti ir tas investicijas pasidaryt, nes kitu atveju tai vis tiek bus mūsų problema. Požiūrio klausimas. man atrodo svarbiausia yra ne kaip padėti,bet kiap netrukdyti jiems, nes jeigu atsirenki gerus žmones, tai jie visą darbą už tave padaro, tik reikia kertiniais momentais prilaikyti biųki arklius, kai jie nusprendžia aspispirkinėti, o jie visada atneš geriausią, kas yra ir jeigu jau iškyla įtampų politiniam lygmenyje, aš kaip vadovas turiu atstovėt, kad juos apginti, nes čia galima primanipuliuoti, ypatingai savivaldoje, ar statom naują darželį, ar IT skyriaus biudžetą didinam? nu aš hiperbolizuoju, nu bet visada taip bus.

Dominyka: supratau.

Adomas: Čia ir yra ta politinė dilema, kuo skiriasi nuo corporate levelio, kur tu apsigini biudžetą ir viskas, dirbi sau ramiai. Ir tave gali pushinti tik iš operacinių kaštų mažinimosi, bet visi ta cyber security mato iš biznio puses kaip tai, kad jeigu tu jo nepadarysi, tai tau in the end tai kainuos. tai čia yra biški kitaip yra, nes kita logika paremtas viešasis sektorius. tai šlovę daugiau dalykų atneša. bet kažkaip mes tvarkomes. Kadangi aš prieš tai šilumos tinklu valdybom vadovavau, tai žinau, ką reiškia daryti daug milijonų investicijų po žeme, jeigu to niekas nemato.

Dominyka: Tai gerai, Jono darbas yra atnešti patį geriausią ir saugiausią sprendimą, o jūsų darbas yra rasti kompromisą, kad nereikėtų daug išleisti, bet vis tiek būtų decent saugu.

Adomas: nu čia, ta prasme, yra šiaip vadovo pagrindinis dalykas. Turi visi išeit biški nepatenkinti, reiškias yra kompromisas. Bet šiaip tai taip. Bet čia veikia tai, kai yra pasitikėjimas. Aš taip galiu su Jonu dirbti, nes mes pakankamai esam atidirbę, vienas kitu pasitikim, ir jis neatnešinės man dalykų dirbtinai užsimetęs, kad paskui kažką dirbtinai cutnsiu, bet čia jau yra susidirbimo dalykas. bet jo,

mintis yra ta, kad aš bet kokiu atveju galiu atnešti tokius struktūrinius pokyčius kaip tą atsparumo skyrių ir visą kitą kur man atrodo kaip jau turi deliotis, bet ką jau čia verda viduj, tai jie jau man turi parodyti, o paskui jau sprendžiu aš ar tai yra problema ar ne. mes galėjom sakyti, kad su sveikatos priežiūros institucijom, kad jau gyvenat taip trisdešimt metų, galit dar dešimt metų pagyvent, bet kol tu nepasidarai audito ir nežinai realiai kaip blogai yra, tol tu gali biški ignoruot. Bet kai pakeli ta lavoną, tai pradeda jau smirdėt.

Dominyka: Yra kibernetinio saugumo įstatymai, yra tie visi keitimai, kur jis yra tvarkomas, koreguojamas, tai jie liečia ir vilniaus savivaldybę. Ar yra, kad jūs iš tiesų pastebit, kad yra kažkokių įstatymų pokyčių, kurie lemia tai, kad reikia sėsti, spręsti, atitkti tam tikrus reikalavimus, ar tai labiau toksai galiojantis, pvž., organizacijom mažesnėm, kuriom reik atitkti tam tikrą higieną?

Adomas: aš manau, kad jie šiaip, iš principo, veiksmingi, bet mes biški kitaip gyvenam. Aš čia nenoriu labai mandrai pasirodyti, bet nu mes nelabai lygiuojames į ta skitas valstybes įstaigas, mes vis tiek labiau save vertinam tiek atlyginimų, tiek specialistų prasme lyginames su rinka bendrai, o ne su kitom valstybinėm institucijom, tai tikėtina tai, kas išeina iš nacionalinių kažkokių reikalavimų, tai arba mes jau esamp adarę, arba esam padarę ir parekomendavę jiems padaryt. tai skamba, kad labai mandravojam, bet tiesiog esam didesni ir galim nsusimdayt gerensius žmones, ir taip veikia visa sistema. bet kad nu nacionalinių lygių ta bazė turi logiką ir veikia, tai faktas, tik nu iki tų savivaldybių jos kol ateina…ir yra dalykų kurie pakeisti prieš du metus, ir kuriuos kitos savivaldybės sužino apie tuos reikalavimus iš mūsų, kai mes kažaką bendrai darom, tai ta prasme yra ir tokių savivaldybių.

Dominyka: o ar yra kokių iššūkių interpretuojant tą įstatymą? Ir jonas man minėjo, kad tas įstatymas yra, ką jis pastebėjo, kad įstatymas reikalauja, kad viskas būtų gražiai apsiršyta ir dokumentuota, bet kol jūs veikiat ir bandot viską tvarkyti, ne visada spėjat apsidokumentuot.

Adomas: nu įstaymas taip veikia, jie eina dažnai forma prieš turinį, bet nu aš sakau, realiai tarkim kinikši visi dalykai, šitoj vietoj visiškai vieni esam, mes ten pvž., eidavom pas VSD, kad kažką padarytų, kad mes galėtumem kiniško šūdo nepirkti, galiausiai jie mum rekomenduoja nepirkti, bet įstatymiškai nieko nepakeičia, bbet jeigu įtraukiam tai į visšųjų pirkimų šitą, tai apskundžia mus ir užbanina pirkimą kaip nekonkurenciją. tai per kokius keturius metus išsimušėm, kad kameras išbrauktų. Dabar darom autobusų pirkimą, turėtų iki 2027m 400 naujų elektrinių autobusų atvažiuot. Nu mes paslaugą perkam, bet autobusam reikalavimus rašom. tai kiniško šūdo privežtų labai greitai, susisgribom, papushinom, įtraukėm viešojo vežimo paslaugas kaip kritines valstybei, dėl ko negalima kiniškos, tai mes daug ką darom patys, tą keitimą pats turi inicijuot, jeigu susiduri su problema. tai

viena yra, kas išeina, mes turim apsirašyt, sakau ten į tą mes žiūrim paparasčiau, bet daug ką patys ir pushinam. Nu tai va dabar kaip lektuvas, tarkim, nukrito - tai mes gale dienosa atsisėdom, jau viską principe padare ir sakom nu gerai, ar turi valstybė kažkokį mechanizmą avia katastrofos atveju. Tai kol visi susidrado, pasirodo, yra pasirašytas. Aštuoni punktai, ką reik daryt, tai viską principe padarėm. Bet kai yra kažkas tai tu neiškai šito, kad ar reikia žmones gelbėti ar ne? Su IT gal yra kitaip, bet ten surasšyti baziniai dalykai tam įstatyme.

Šarūnas Končius (KTU Domreg), virtualus interviu, 2024m. Gruodžio 12d.

Dominyka: Aha, įrašinėju. Tai vat tada trumpai papasakosiu truputį apie savo darbą, kad geriau suprastumėte bendrą idėją. Tai aš šiaip studijuoju Tarptautinių santykių institute ir rašau savo dabar magistro darbą iš to, kad turiu tokią teoriją, kad yra kibernetinis saugumas, kuris susidaro iš tam tikrų prevencijų atakų, t. Y. Visko, ką tu bandai padaryti, kad išvengti atakos. Ir tada yra kita dalis kibernetinis atsparumas, ir to dar kaip ir neneigia, kad ta ataka apskritai įvyks, negali išvengti išorinių grėsmių ir tada darai viską, kad apsisaugoti ir mažinti žalą ir vykdyti nepertraukiamą veiklą. Ir kadangi tas kibernetinis rizikų valdymas, ta prevencija ir bandymas apsisaugoti nuo atakų yra pakankamai "popular" dalykas, aš nusprendžiau patyrinėti, kiek atsparumas iš tiesų Lietuvos organizacijose išties yra toks dalykas, kuriuo kažkas apskritai užsiima ir kiek strategijose, tarkime, įmonių atsispindi arba kiek prioterizuoja tai, kad kažkas, kad buvo tas apsisaugojimas jau nuo pačios įvykusios atakos. Tam, kad paremti savo teoriją, tai aš atlieku tam tikrus atvejo studijas tai apie įvykusias jau anksčiau atakas ir tada kalbinu žmones, ekspertus, kurie su tuo dirba, kad pasižiūrėti, ką jie apskritai apie tai kalba. Jūs esate vienas iš ekspertų.

Šarūnas: Tai aš gal tada tik trumpai pasakysiu, kad pati idėja šita jinai nėra labai nauja, nes jeigu pažiūrėti, kur ji atsispindi, tai aš sakyčiau pats ISO 27001 standartas. Galbūt tas aiškiau dvidešimt antrų metų versijoje yra padaryta. Jisai siekia, kad organizacija turėtų, sakykim, tokius gal tuos savo resursus, skirtus kibernetiniam saugumui paskirstė į tris dalis. Viena dalis tai būtent siekti, kad neįvyktų įsilaužimas, tada antra dalis, kad pastebėti įsilaužimą, nes tu turi pastebėti, turi priemones turėti, nes gali gintis ir neturėti priemonių, kad pamatytum, jog pas tave jau kažkas nutiko. Ir tada trečia dalis būti pasiruošus tam įsilaužimui ir reaguoti, kada jisai vyksta, kad padarytum, sustabdytum žalingą veiklą ir atkurtų duomenis. Jeigu jie buvo pažeisti, tai kiekviena įmonė turėtų rasti tinkamą balansą tarp šitų trijų dalių. O ta idėja, kad tu turbūt negali apsisaugoti, tas įsilaužimas vis tiek įvyks. Tai ryškiausiai atsispindi ir zero-trust iniciatyvoje, iš kurios sekė ir labai techniniai dalykai, kurie

sako, kaip šiuolaikinėje šiuolaikiniai sistemoje visa tai reikėtų bandyti sieti jį į vieną visumą, tai daugelis technologijų šiuolaikinių Zero Trust idėjomis yra jau paremtos.

Dominyka: Supratau, o tada gal dar prieš išvis einant į klausimus norėjau paklausti, gal plačiau papasakotumet tai, ką jūs esate, kuo užsiimate ir KTU, Nes aš, kaip supratau, tai, ką jūs dirbate, yra šiek tiek kitaip. Su sistema, kurioje dirbate, tai galvoju pasitikrinimui.

Šarūnas: Tai gerai, tai mano darbas KTU yra susijęs su pirmąja versija Kibernetinio saugumo įstatymo Lietuvoje. Kada tas buvo padaryta? Kada atsirado Nacionalinis kibernetinio saugumo centras. Jie irgi svarstė, kam skirti savo resursus, ir nutarė, kad tai turėtų būti skirta ypatingos svarbos infrastruktūrai apsaugoti. Taip buvo sukurtas įstatymas, apibūdinantis, kas tai yra, ir jie, irgi rėmėsi ne, ne patys sugalvojo daugeliu atvejų, bet jie pasieme ta tinklo informacijos saugos direktyvą pirmąją versiją dabar, kur antroji versija Europos įsigaliojo ir įstatymas atitinkamai buvo atnaujintas, kad atitiktų antrą versiją, nes antrosios versijos apimtis ir turbūt gylis jie yra didesni ryškiai negu pirmosios ir negu pirmosios versijos lietuviško įstatymo. Tai aš sakyčiau ir į gylį labiau, ir į plotį labiau šiuo momentu, kas yra padaryta. Tai pagal pirmąjį įstatymą reikėjo neutralaus žmogaus, kuris būtų nu grubiai toks vidinis auditorius. Galbūt tai, KTU buvo įtrauktas Į tą ypatingos svarbos organizacijų sąrašą, nes turi registrą, kuris yra kritiškai svarbus. Tai tas registras yra taškas LT DNS vardų zona, nes KTU istoriškai valdo šitą zoną. Vadinasi, pats tas valdymas yra ganėtinai komplikuotas, nes pats KTU šitoj vietoj nedaro. Pakeitimų pakeitimai yra daromi per partnerius. Sakykim, jūs kreipėtės į kokį nors serverį.LT. Sakote aš noriu nusipirkti domeną, tai serveriai LT perduoda tą užsakymą, tinkamą formą, kad ši visai atsidurtų KTU tame registre. Tai tas, kuris valdo aukščiausio lygmens zoną, kaip ir taškas LT. Jisai turi laikytis tarptautinių standartų ICANN organizacijos, kuri kontroliuoja šituos dalykus ir sako, kaip viskas turėtų būti sutvarkyta. Kita vertus, žiūrint iš įstatymo pusės, tai yra ir tam tikra nuosavybė, ir visi tie dalykai, kas yra tame registre, jie yra nuosavybės įrodymas. Lygiai taip pat, kaip , pavyzdžiui, įvyktų, būtų sunaikintas koks nors registrų centras ir neturėtų rezervinės kopijos, pavyzdžiui, ten žemės nuosavybės dokumentų. Tai čia yra tas pats. Domenas priklauso. Tai teisiškai yra turtas. Tai vadinasi, šitie dalykai iš tikrųjų svarbūs. Nu ir teko vykdyti tuos įpareigojimus, kuriuos davė Nacionalinis kibernetinio saugumo centras. O tenai buvo, jeigu taip paimsim, tai va tie trys dalykai, kur pasakyta tai ką tu darai, kad apsisaugotų? Tai ten ta dalis apima rizikos valdymą ir tada tu turi turėti planą, kaip reaguosi, jeigu vyksta incidentas ir turi turėti būti atsparus, turi turėti rezervines kopijas, iš kurių atstatys duomenis ir atitinkamai. Ir reikia galvoti ne apie vieną duomenų centrą, apie keletą, nes žiūrint į tą atsparumo pusę po atsparumo slepiasi turbūt keli dalykai tiek pasiekiamumas angliškai availability, tiek veiklos tęstinumas - “Continuity”. Tai kaip jau tu sugalvosi tuos dalykus, taip. ta pati sistema, kuri katerių yra sugalvota

kaip tai veiktų? Tai buvo padaryta gana paprastai. Akivaizdu, kad tai nėra viso KTU reikalas. Negali puoštais reikalavimais pakišti, sakykim, bet kokios ten katedros ar ar viso fakulteto, bet tam tikras bendrai naudojamas dalis kitų, be jokios abejonės, tai liečia. Pavyzdžiui, jeigu vienas iš duomenų centrų, kurį naudoja Domregas, yra KTU duomenų centras, vadinasi auditas, kurį darys pagal ISO 27001. Jisai lies ir tą centrą. Tai taip ir buvo padaryta, kad tos vietos, kurios turi būti pakeltos iki to lygmens, juos buvo kilstelėjus pats Domrego padalinys, jisai buvo ištrauktas iš Informacinių technologijų departamento ir padarytas tame pačiame lygyje, nes kitaip vidinės tvarkos neleidžia sutvarkyti šitų dalykų. Ir, sakykim, tas mechanizmas, kuris leido vadovams įsitikinti, kad atitinka, sakykim, tą įstatymą, nes tokios atitikties NKSC neturi, kad ateitų tikrintų reguliariai. Jie patvirtina msako Taip, jūsų dokumentai geri jūsų procedūros, kurios numato ten, sakykim, reagavimą, jos yra geros. Įstatyme yra numatyti tam tikri kriterijai, sakykim, laikai, per kiek laiko turi sureaguoti, pranešti NKSC policijai, Valstybinei duomenų apsaugos agentūrai, inspekcijai, tai visi šitie dalykai yra, bet patikrinimo nedaroma ir buvo nutarta. Kitas mechanizmas, kuris leistų atitiktį užtikrinti, yra ISO 27001 standartas, kas padengia didžiąją dalį suteiktų reikalavimų. Tai tas buvo padaryta vat vieno padalinio lygyje, departamento lygyje. Ir aš manau, kad pasiteisino, nes privertė dokumentuoti tuos dalykus, kurie anksčiau nebuvo dokumentuojami ir privertė truputėlį kitaip pasižiūrėti į tas procedūras, kurios galbūt atrodė anksčiau. Tokios biurokratinės, reikia padaryti dėl varnelės. Tai, sakykim, tas pats rizikos valdymas. Jį gal aš ten truputėlį stumtelėjau į tinkamą vietą jau atėjęs, nes buvo daromas pagal metodikas, kas yra įprasta ir Lietuvoje viešajame sektoriuje naudoti. Bet vat, kad suvesti galus tai daroma labai paprastai. Informacija, išvados, kurios būna padaromos atitinkamo laikotarpio, jos turi pagrįsti biudžetą kitų metų, tai jeigu tau kažko reikia, tu turi parodyti, kad tai yra ne todėl, kad tu pats sugalvoji, o todėl, kad ir rizika galbūt išaugo, padidėja. Ir tai, aišku, yra šitie dalykai numatyti sudėtingiau ne vien tiktai biudžetavimo laikotarpiu. Yra tam tikras kaupiamas rizikos fondas, nes ten gali būti visokių kitokių teisinių aspektų ar dar kažko tokio, žodžiu, reikia turėti. Tai tas leidžia taip pat sureaguoti į kažkokias grėsmes, gerokai padidėjusias, kaip, pavyzdžiui, karas Ukrainoje. Tai tas leido daryti neeilinę peržiūrą ir pagalvoti, ko trūksta, kad mes būtume pasiruošę tai situacijai, nelaukiant finansinių metų pabaigos.

Dominyka: Supratau ačiū labai labai įdomu. Ačiū, kad išsiplėtėte. Dabar jau dalis klausimų, netgi gal ir persidengia, bet mano pagrindinis klausimas buvo vat kaip, kalbant apie jūsų, kaip pačios organizacijos saugumo strategiją arba kažkokius planus, kuriuos turit gaires, ar pasakytumėte, kad vat labiau orientuota yra, tarkim atsparumo sistemą, tas tęstinumas, sistemų nepertraukiamumą, ar vis dėlto labiau į gebėjimą, į tradicinį rizikos valdymą, tą grėsmių ir labiau gebėjimą vykdyti atakų prevenciją?

Šarūnas: aš sakyčiau, kad yra balansas. Nes negali tik į kažkurią vieną pusę nueiti, nes tada tavo tas brandos lygis jisai, nu tik vienoj vietoj bus užaugęs. Labai daug sudedamųjų dalių yra, nes čia yra ir žmonės, kuriuos turi turėti, kad jie tuos tas savo roles vykdytų, kur jų reikia Ir. Nes mes turim ir pasyvų budėjimą, ir iš tikrųjų kas 24/7 reaguotų, jeigu reikia, tie dalykai yra išbandomi, tikrinami. Tai vat kol nevyksta pratybos, tai aš galbūt nuošaly darau dalį, mes turim auditą kasmetinį pagal ISO standartą ir sakykim irgi, jeigu žiūrėti ar matom naudą iš to, tai aišku matom, nes jeigu darai ne, ne vien tiktai popieriais, bet sakykim, susieji tuos dalykus su praktiniais aspektais, ką tu turi pasidaryti, tai labai greitai ta tvarka pasidaro tinkama. Na, ne, ne vien tiktai popieriuose tai ir įskaitant kokia įranga naudoji. Kaip pirkimus vykdai? Galbūt dėl to pirkimai pailgėja, bet pirkimo, sakykim, tų gebėjimų turi ir vietiniai žmonės. Bet čia, sakykim, KTU su savo resursais prisideda gana stipriai ir tos vietos, kur persidengia, jos irgi yra daromos bendrai. Kas dėl duomenų centro patalpų, kitų dalykų tiesiog negali nebūni, sakykim, visai vienas ar ten kažkur tai vakuume, tai tie dalykai kur prisiliečia, aišku, stengiasi, kad tikrai minimumas būtų padarytas, nes taip šito dalyko reikia pagrinde domregui. Bet aš manau, kad pavyksta suderinti tuos interesus ir dabar pamačius, kad iš tikrųjų veikia gerai, tai yra galvojama, kad reikia išplėsti truputėlį veiklą, nes natūraliai dėl dėl veiklos specifikos KTU pats dromregas vysto ir daugiau veiklų, kurios nėra įtrauktos į ypatingos svarbos tą infrastruktūrą. Ir dabar, kada atėjo antroji ta tinklo informacijos direktyvą, tenai yra atsiradęs elementas, kuris verčia dar labiau dar plačiau pasižiūrėti, nes, sakykim, ko neturi rimtai, rimta apimtimi nei ISO standartas, nei prieš tai buvęs Kibernetinio saugumo įstatymas, tai tiekimo grandinės valdymo ir čia tiekimo grandinės valdymo klausimas yra iš dviejų pusių, nes, sakykim, net yra į tą sąrašą svarbių įmonių, NKSC tave gali įtraukti todėl, kad tu pats atitinka kriterijus. Bet gali būti taip, kad tavo klientai, kurie naudojasi tavo paslaugom tiesiogiai arba galbūt netgi per partnerius, rodo, kad tu esi tas svarbus ir tu būsi įtrauktas ne todėl, kad tu pats savaime esi svarbus, bet dėl to, kad tu esi dalis tiekimo grandinės. Tai buvo įvertinta, kad tos paslaugos, kurios anksčiau nebuvo įtrauktos į tą kritiškai svarbią, jos irgi paliečiamos dėl tos kritinės grandinės, nes tiesiog tie partneriai, kurie dalyvauja veikloj, jir naudojasi toms informacinėms sistemoms. Ir dėl tiekimo grandinės, sakykim, ta apimtis dabar didėja. Tai aišku tvarkos, kurios yra ir kadangi organizacijai patogu, jeigu jos veikia, jeigu jos nėra biurokratinės, tai tą išplėtimą padaryti ne taip jau ir sunku, bet žmonėms krūvis didėja. Na ir sakykim, tų pokyčių dar mes nematom visų iki galo ko ko reikės. Bet sakykim, tai, kas ateina, pavyzdžiui, ISO auditas ir atnaujinimas to standarto, tai jau tenai žiūrim plačiau, nes tas galiausiai nueis plačiau ir į rizikos valdymo dalį. Bet mes turim laiko metus dar gerus, tai manau, kad viską spėsim pasidaryti.

Dominyka: Tai tada kitas klausimas ta pačia tema. Tai dabar vistiek esate jau kažką dalį pasidarę, Kaip ir gal netgi kokius kriterijus KPIs turite išsiskyrė vertinti savo kibernetinio atsparumo lygį? Kaip apsibrėžti jo gėrį?

Šarūnas: Tai iš to turbūt vat ką ką pasakiau matosi, kad vadovai nutarė, kad tas indikatorius ar ten KPIs pagrindiniai yra atitiktis ISO standartui. Ir aišku, NKSC tai NKSC vykdo pratybas, tuose pratybose mes būtinai dalyvaujam ir jos leidžia pasitikrinti ir žmonių kompetenciją, kompetenciją ir kaip veikia pačios procedūros tai aišku, to tikrinimo mes turim pasidarę ir be to yra, yra tam tikri standartiniai veiksmai, kurie realiai kiekvieną mėnesį kažkas vyksta. Yra tiesiog išdėlioti patikrinimai, kad jie nebūtų kažkoks pikas specialiai tam, bet ir žiūrint į darbus, kad, pavyzdžiui, turi atsarginį duomenų centrą. Vat jeigu sutriktų veikla, nesvarbu technologijų ryšių kanalų pirmame duomenų centre, tu turi perkelti šitą savo veiklą aktyvų duomenų centrą į tą kitą vietą, tai tas gali būti Lietuvoje, tas gali būti užsienyje. Tai kaip daryti patikrinimą, tai patikrinimą turi daryti. Jis yra įpareigojamas daryti, pavyzdžiui, kartą per ketvirtį. Bet jeigu po momentu patikrinimas yra dalis procedūros ten netikėtos arba suplanuotos, nesvarbu. ir tu tiesiog padarei kaip dalį pratybų, tai užskaitoma, kad tą ketvirtį šitas tikrinimas jau buvo padarytas. Tai vat tas toks sujungimas tų tikrų kasdienių operacijų ir tų tikrinimų jisai leidžia nuo tik ne biurokratiškai žiūrėti. Ir jeigu nebuvo tikrinimo, tu jį turi padaryti todėl, kad tai yra dalis operacijų. Jeigu buvo tikrinimas, matosi, kad buvo, vadinasi, ataskaita ir pasižiūri, ar viskas veikia taip, kaip turėjo veikti. O aišku, visi visi šitie dalykai yra dokumentuoti, tai ir planas reagavimo NKSC turi būti patvirtintas, tai šitas dalykas yra padarytas. O pratybos pačios, kurios vyksta, jos rudenį, paprastai vyksta spalio mėnesį kažkur. Tai jos leidžia patikrinti komunikaciją su tomis organizacijomis, kuriom yra numatyta, kad tu jiems kažką turi atiduoti. Tai vat tas NKSC, policija. Ir tada dar dar be šito, sakyčiau, mes esame linkę pasitikrinti komunikaciją Išorei, tieisog komunikacijai, kuri išeitų iš kitų. Tai čia yra keletas žmonių, kurie tame dalyvauja. Kažkas domreg lygį, kažkas centralizuotam domrego lygyje. Šitie dalykai irgi yra sugalvoti, nes nu to to irgi reikia. Tai tokie dalykai kaip šablonų pasidarymas, kad jeigu reiktų kažką daryti netgi žmogui tiesiogiai su tuo nesusijusiems, bet minimaliai kažką išleisti, tai yra ir instrukcijos, ir šablonai, viskas paruošta. Taip, bet iš esmės tai yra dalis dalis plano, kaip tu reaguosi į incidentą.

Dominyka: Supratau, iškart atsakėte ir į mano sekantį klausimą apie tai, ką, ką darėte, kad pasiruošti kibernetiniam incidentams. Tai tada einam prie ketvirto klausimo - Ar turite kokį nors atvejį, pavyzdį, kuriuo galite pasidalinti, kuris neseniai, tarkim, įvyko būtent iš bandymo atakuoti arba atakosm kaip tvarketės, koks buvo atsakas? Gal jeigu į detales neinant, tai apskritai kaip viskas suveikė?

Šarūnas: Nebuvo pas mus tokių incidentų, sakykim kaip pačio KTU situacija čia buvo prieš prieš 2 metus su trupučiu. Bet grėsmės lenda nuolat. Tai yra, sakykim, stebėjimas vykdomas nuolat ir stebėjimas vykdomas tų kanalų, iš kur mes įvertinome, kad ta grėsmė galėtų galbūt būti netikėta, netikėtai didelė, nelaukta iki tol nežinota. Tai vat čia irgi labai daug turi remtis tiekimo grandinėm,

nes vienas iš tų stebėjimų kazkas vyksta, tai yra pranešimų gavimas iš partnerių, kieno įranga mes turim apie pažeidžiamumus, kuriuos jie sužinojo, tai partneriai. Bet jeigu mes matom, kad tos informacijos neužtenka, arba kažkurie partneriai pavėluotai tuos dalykus paskelbia, tai tada mes žiūrime į resursus, kurie yra nepriklausomi, trečių šalių ar bendruomenės. Tai tų šaltinių kiekis prisideda. Ir šitais dalykais rūpinasi ir centralizuota NKSC. Sakykim, mes dalyvaujam ten to vadinamo SITO veikloj, kur jie formuoja tą tinklą, nes tas tinklas vietinis, jisai gali duoti specifikos lietuviškos, ko kiti galbūt nemato. Jeigu tas kažkoks blogas veiksmas vyktų Lietuvoje, tai čia jau yra tokie, klausimas kiek tu nori matyti šitos informacijos, nes irgi turi būti balansas. Jeigu tos informacijos ateis labai daug, ir net jeigu, sakykim, viskas bus susiję su tavo turimais elementais infrastruktūrai, tai turi turėti žmonių komandą, kas tai reaguotų? Nes atėjęs pranešimas, į kurį niekas nesureagavo, jisai nenaudingas. Tai žiūriu, kad būtų tas balansas. Žiūrime, kad tie pranešimai būtų apdoroti, bent minimaliai dokumentuoti. Ir tada yra pastebimos kažkokios atakos, sakykim, tos atakos, jos reaguojama yra ir į vartotojų atakas, nes darbuotojas galėtų būti užpultas, sakykim, tiek tikslinę ataką naudojant, tiek ne tai vartotojų pusėje, mes irgi stebime labai įvairius resursus, įskaitant lietuviškus bendruomenės resursus. Tai, sakykim, kol kas aišku, tai labiau pratybos gaunasi, nes dalyvaujam tose pratybose, kur darbuotojai gauna laiškus. Tik mūsų atveju, įprasti laiškai jie nėra tokie, kad darbuotojai atsigautų. Mes turim savo dalykus organizuoti viduje su su mūsų pačių specifika susijusios, kad tą budrumą išlaikytume, nes bendri dalykai, kurie galbūt viso universiteto darbuotojams iš tikrųjų būtų neatpažinti. Mes truputėlį kitas sistemas naudojame ir ir kas ateitų tenai, mums nėra pavojinga.
Dominyka: Įdomu. Supratau. O dar gal irgi toks klausimas. Minėta, kad ataka buvo, bet kai atakuojamas, tarkime, yra KTU, tai jūsų sistemos yra atskiros ir jūsų nepaveikia tai, kas paveikė KTU?

Šarūnas: Taip, jeigu žiūrėsime į, pavyzdžiui, vartotojo autentifikavimą, mes naudojame KTU paštą, sakykime, KTU pašto dėžutės mano, pavyzdžiui, aš nesu Domrego darbuotojas, KTU pašto dėžutes naudoju, tai mano komunikacija per KTU, mano komunikaciją elektroniniu paštu buvo sutrikusi. Bet Domregas turi savo izoliuotas sistemas ir sakykim, jie naudoja ir tą į tą ir tą paštą, nes organizacijai reikia. Bet vat tiems visiems, sakykim, reikalams, susijusiems su registrų vidiniais dalykais, yra naudojamos atskiros izoliuotos sistemos, tai tas visiškai nepaveikia ta prasme nieko, nieko bendro, tik tai, kad atskiros spintos duomenų centre atskiri tinklo kanalai. Žodžiu, izoliacijos lygis yra didelis.

Dominyka: Supratau, o kadangi, KTU tikriausiai atskirai man pakalbinti nepavyks, nes atsisakė tenai. O gal tada žinot, irgi galit man paaiškinti skirtumą tarp -Tai gerai, tai jūs, jeigu tarkim į tam tikras saugumo sistemas, tai jūs esate atsakingas tik už domregą, ir tai ką KTUturi, tai irgi nėra?

Šarūnas: Jie jau manęs neklausytų. Sakytų, taip aš jiems taip pat dalinu patarimų truputėlį, bet viso labo tai yra rekomendacijos. Tai aš neturiu jokių įgaliojimų, kad spausti juos kažką daryti.
Dominyka: Supratau, supratau. Nu bet kuriuo atveju tikriausiai reikės priversti man juos atsakyti bent į klausimus, nes mano...
Šarūnas: Žinokit dabar galvoju, jeigu išeina gauti tą informaciją ir tada vadovas Žiliukas Darė prezentaciją. Dabar galvoja, kas tai galėjo būti. Gal Verslo žinių renginys ar kažkas tokio. Kur jid truputėlį pasakojo, kas tai vyko, kaip tai vyko, bet tiek, kiek leidžia situacija, nes dar vyksta tyrimas. Policija tiria. Tai jisai yra nesibaigęs, tai net ir tuos dalykus, kur jūs galbūt galėtų pasigirti, jis negalėjo pasigirti. Tai šiek tiek aptakiai. Tai vat, nežinau ar prieinamas video, bet man atrodo buvo daromas video, tai tik aš tiksliai neprisimenu koks kas darė renginį. Čia tas buvo prieš porą mėnesių.

Dominyka Turbūt pabandysiu susirasti. Nes aš irgi. Kadangi kita organizacija, kuri, su kuria kalbėjo, buvo Vilniaus universitetas, tai man buvo įdomu palyginti, kokias kokias funkcijas naudoja. Tiek KTU jau tiek VU. Buvau su idėja, kad gali kažkas skirtis, bet čia tikriausiai reikės jų pačių paprašyti.

Šarūnas: Tai žinokit, jie naudoja ir labai bendrus dalykus, nes universitetai turi, jie yra susijungę į tinklą, LITNET tinklą, LITNET ir KTU, žiūrint į patį KTU, Daugelis dalykų sutampa, tai gali būti, kad kažkurios savo vietose, pavyzdžiui, KTU CERT, tai yra ta jau saugumo tarnyba, kuri reaguoja į įvykusius incidentus, tuo pačiu yra dalis LITNET certo. Tai, pavyzdžiui, to padalinio vadovė Milda Mimienė. Tai šitie dalykai ka jinai pastebėjo, sakykim, kas bus viduje išleista, kaip komunikacija keliaus visam LITNET tinklui ir tą gaus visi universitetai Lietuvoje, plius jie mokykloms teikia paslaugas litneto, tai mokyklos irgi šituos dalykus turėtų pastebėti. Aišku, mokyklos ten minimaliai, nes savų resursų jos nelabai turi. Bet vat iš tokio hostinimo pusės LITNET šitoj vietoj savo darbą padarys tai truputėlį yra apgalvotai. Bet šitoje vietoje aš nežinau visų detalių kaip tos sąsajos atrodo, nes LITNET operacijos pagrinde yra padalintos tarp dviejų duomenų centrų Vilniaus ir Kauno. Ir Kaune už tai KTU yra labiau atsakingas, Vilniuje turbūt VU sakyčiau. Tai čia irgi dar tą sąsają jinai gali gal būt padėt kažką išsiaiškinti kaip jį, kaip jie dirba, nes ten jie tikrai ir resursais dalinasi.

Dominyka: Aš galvojau turėjau pradėjus rašyt darbą ir nekalbėjus dar su žmonėm, dariau teoriją, kad iš tiesų bus kažką, ką daro kitaip, tarkim, arba KTU, ką darė ir VU kažką turėjo. Bet dabar suprantu, kad vėlgi tų išorinių grėsmių nekontroliuoja ir KTU, tikriausiai, tiesiog nepasisekė šitoje vietoje, Nes vat kaip mano tirta sistema yra bendra ir...

Šarūnas: KTU užpuolė grupuotė, kurie fokusuojasi truputėlį į universitetus. Tai yra tarptautinė. Aš nemanau, kad čia kokiai nors vienai šaliai priklauso ir jie irgi dviračio neišradinėjo. Jie ėjo kanalais, kurie matosi, kad atviri. O kaip taisyklė, universitetai turi daugiau visokių atvirų dalykų, paliktų tiesiog todėl, kad ta akademinė laisvė ten dažnai Yra didesnė negu negu poreikiai, reikalavimai laikytis kibernetinio saugumo. Ir tiktai vat kažkokie tokie įvykiai, jie priverčia truputėlį tą laisvę apriboti, nes čia ne vien IT požiūris, nes jeigu jūs su Žiliuku irgi kalbėtumėte, tai jisai tą tą punktą labai pabrėžia. Aš aš jį suprantu, aš pats skaitau, mokiausi, bet aš prisimenu, ką aš išdarinėjo, kai studentas buvau, tai tie darbuotojai neturėjo labai džiaugtis. Bet yra kitas kitas momentas, kad kada tu vertini riziką, tu matydamas padidėjusią riziką, kuri išaugo dėl technologijos, dėl aplinkos, kad tiesiog dabar situacija tokia susiklostė. Tu turi priimti sprendimą nelaukdamas ir nebandydamas čia su visais susitarti. Nes jeigu, sakykim, kibernetinis saugumas yra kažkam paskirtas kad tai būtų ir to žmogaus atsakomybė, jisai turi galėti priimti sprendimą ir galbūt laikiną. Bet tos griežtos priemonės turi būti panaudotos greitai ir ryžtingai. Tai aišku, čia yra daug dalykų tokių klasikinių, susijusių su specifinėm technologinėm sritim. Turbūt didžiausia bėda ir didžiausias, didžiausia vieta, kurią atakuoja, yra kaip čia lietuviškai, paskyros, Identity Men komentaras. Tai slaptažodžiai, slaptažodžių politika, antro faktoriaus autentifikavimas. Visi šitie klausimai, jie turėtų būti išspręsti. Ir jeigu atsakyme tam pačiam domrege šitie dalykai yra išspręsti ir ten nuo labai senų laikų, tai šitas dalykas universiteto lygyje, ypač jeigu tu neturi didelės centralizacijos. Pavyzdžiui, tavo moodl'ą prižiūrės vienas padalinys, kuris savaip sprendžia, kaip viskas veiktų tai universiteto lygyje tą sunku padaryti. Turi atsirasti kažkokia labai stipri jėga, kuri sugebėtų parodyti, kad šitie dalykai yra svarbūs. Jeigu jūs pažiūrėsite į universitetus, Vilniaus universitetas turbūt yra išviso paskutinis, kuriame IT buvo centralizuotas kažkokiu kažkokiu mastu. Tai tas žmogus, kuris dabartinis eiti vadovas. Jisai atėjo iš Lietuvos energijos padalinių ir tuo momentu jis buvo labai pažangus. Vienas iš geresnių eiti vadovų, Tai jam šitą dalyką užtruko padaryti, aš manau, kokia penkiolika metų. Bet čia yra universiteto situacija. Ir iš tikrųjų VU buvo tas iki centralizuoto IT tarpas daug didesnis negu negu pas kitus. KTU ta centralizacija įvykusi anksčiau. Nežinau, kaip jiems pavyko. Aš ten gal irgi prisidėjau iš tokių architektūrinių sprendimų, bet kaip politiškai jie tuos dalykus sprendė, negaliu pasakyti. Tiesiog gal jiems pasisekė, gal LITNET svoris KTU pusėje buvo didesnis, gal pasitikėjimas padaliniu. Padalinys savo pastata labai nuo seno turėjo, tas gali reikšti. Žodžiu, daug daug labai aspektų. Žiūrint į kitus universitetus, kurie irgi tokie didelė jau ne Lietuva žiūrint, tai tas de centralizavimo klausimas yra iki šiol aktualus, nes ką tai reiškia? Tai reiškia, kad kiekviena katedra iš esmės, kuri sako man čia reikėtų daryti tyrimus. Aš turiu pinigų tyrimui, gali nusipirkti įrangos, įrangos, įsidėti į savo mažą infrastruktūrą, niekam nieko nesakyti, pradėti naudoti, nes jiems to reikia moksliniams tikslams ir jų, kaip ir niekas neturėtų drausti tai įsivesti tą drausmę IT pusėj universitete yra ganėtinai sunku.

Dominyka: Aha, supratau. Aišku, šiaip labai įdomu yra išgirsti. Aš tikriausiai, čia gal apie Bulavą mes ir šnekam. IT į vadovą VU?

Šarūnas: Bulavas iš akademinių sluoksnių. Čia man reiktų pasižiūrėti palaukit, ne Bulavas. Aš užmiršau pavardes.

Dominyka: Bulava esu kalbinus. Tai dėl to ir klausiu.

Šarūnas: Su Bulavu labai gerai pasikalbėti dėl visų dalykų, nes jis vat kaip nuleisti atėjusias, sakykim, kažkokias direktyvas, kurios turėtų veikti, tai jos per jį paprastai eina, garantuotai GDPR, pavyzdžiui, ėjo per jį Vilniaus universitete. Galiu, galiu garantuoti. O čia reiktų man pasižiūrėti labiau. IT Vadovas čia labiau, sakykim, ne aš iš operacijų Galbūt dalies anksčiau jis nebuvo matomas. Galėsiu elektroniniu paštu atsiųst vardą. Vardą, pavardę neturiu dabar greitai po ranka pasidėjęs supratau.

Dominyka: Tada dar noriu paklausti. Tai vat iš jūsų jau mes apie tai irgi šiek tiek aptariam apie tuos iššūkius. Iš jūsų, kaip eksperto, nuomonės. Kokie, jūsų nuomone, yra pagrindiniai iššūkiai? Vat bandant pereiti arba daryti pakitimus tarp rizikos ir grėsmių valdymo einant prie, tarkime, atsparumo grindžiamo požiūrio, tai čia gali būti netgi kelios vietos konkrečiai einant per techninius dalykus arba netgi kalbinau vieną organizaciją. Ir ji, tarkim, kalbėjo, kad kai kurios įmonės iš jų patirties apskritai turi problemų su vadovų, tarkim, suvokimu, kurie labiau eina prie prevencijos ir visko apsišarvavimo, kad tik neįvyktų ta ataka ir pamiršta visiškai atsparumą. Bet čia toks platus klausimas.

Šarūnas: Jeigu turbūt yra pirmiausia, tai yra labai didelė priklausomybė nuo to, kokio dydžio organizacija. Didesnei organizacijai paprastai tas suvokimas yra ir geresnis. Mažesnei vidutinei gali būti, kad jis atsiranda tiktai dabar todėl, kad aplinkui kažkas girdisi todėl, kad ta naujoji direktyva, kaip ir juos, jau turėtų liesti. Todėl, kad visi veiksmai, kuriuos darė NKSC, pastaruoju metu irgi atsisuka šiek tiek į smulkias ir vidutines įmones. Tai tas dydis jisai labai įtakoja, nes galbūt tos mažos organizacijos jos tiesiog dominuoja. Tas manymas, kad mes maži, mes niekam neįdomūs, Niekas čia pas mus neateis, kai tas yra netiesa, nes akivaizdu, kad tie nusikaltėliai, jie irgi nežaidžia žaidimų. Jiems ten kokia nors garbė ar dar kažkas tokio nebeįdomu. Klausimas pinigų pirmiausia yra, tai jie eina, tiesiog ima žemai kabančius vaisius, o tie maži, net jeigu jie galbūt iš jų tiek daug ne išpeši, bet jie yra puikus taikinys, kurį galbūt netgi visiškai automatizuotomis priemonėmis gali nulaužti. Tai čia vat šitas suvokimas šitą suvokimą taiso truputėlį ir dabartinis naujas kibernetinio saugumo įstatymas ir jisai perėmė šitą nis 2/3 2 direktyvos požiūrį, nes ten kas pasikeitė. Vat esminis pokytis ten yra ši įvardinta, kad kas turi susimokėti baudą, jeigu bus nustatyta, t.y. vadovas ir jau dabar nebėra jokių IT

vadovas, kažkas, tai įmonės vadovas. Tas yra tiksliai pasakyta ir čia yra vienas iš tokių didesnių pasikeitimų. Tai aš labai tikiu, kad jisai tą situaciją pradės keisti truputėlį ryškiau. Tada antras momentas. Antras momentas yra, kad iš tikrųjų partneriai, kurie teikia tas paslaugas mažiesiems, vidutiniams ir Nuo seniau Savo veiklą vykdantys šitoj srity specialistai laikosi įsikandęs senų dalykų, senų nuostatų todėl, kad jiems kažkada tas veikė ir nepasidairo kas yra naujo. Kaip keičiasi situacija? Aišku, jie pastebi tuos visiškai naujus dalykus ir pastebi, kad grėsmių kiekis ten daug greičiau auga ir panašiai, ir reaguoja į tai, bet labiau technologiškai pasižiūrėti, kad kažką reiktų daryti kitaip, va tas pats Zero Trust taikymas. Zero Trust pagrindinis skirtumas, kuris yra- Zero Trust sako galvok taip, kad jau tave nulaužė. Tai tas prasidėjo kokiais Du tūkstančiai antri du tūkstančiai ketvirti metai, turbūt, kai tai buvo pradėta. formuluoti pirmieji, kurie padarė pas save veikiantį sprendimą, buvo Googlas. Bet googlas tam reikalui skyrė labai daug pinigų. Ir kitiems atkartoti šitą sprendimą tuo momentu buvo labai sunku. Bet daugelis pasiėmė tuos principus. Ir šiaip Zero Trust principai jie kaip ir nieko nekainuoja. Ir vat tas, kad tu turėtum skirti kažkiek resursų ir turėti tikriausiai priemonių, kad pastebėtum, jog pas tave jau įsilaužė. Šis momentas yra labai svarbus, nes jeigu tu to nedarai, tas įsilaužėlis pas tave sėdės ramiai tol, kol susirinks pakankamai informacijos tol, kol gaus administratoriaus prieigą. Tai aš nežiūrėjau paskutinių statistikų, bet, sakykim, dar prieš porą metų buvo sakoma, kad po šešis septynis mėnesius įsilaužėlis sėdi ir stebi, kas kas vyksta, žiūri, ar galima nueiti kažkur tai giliau, toliau tai tu laiko turi, turėtum tikrai garantuotai pastoviai vyksta kažkokie dalykai, kurie ne tipiniai, tai tu turėtum priemones, kad tai pastebėti. Tai šita dalis jinai tikrai dar nėra tame lygyje, kur aš norėčiau matyti. Bet jeigu bandoma balansuoti, bandoma remtis kažkuo tuo pačių ISO standartų. Šitas dalykas ten jau yra parašytas. Dabar kas dar dėl tų senų naujų dalykų - kai kas yra į galvą įkalta taip stipriai toj pačioj saugumo srityje, kad dabar, kai išgirsti naujovę, tau gali atrodyti, kad čia tave tiesiog bando apgauti. Tai vienas iš tokių dalykų, tiesiog iliustruojančių tai, kad reikėtų daugiau lankstumo ir tokio greitesnio reagavimo į naujienas, kurios yra akivaizdžios, ištirtos ir net rekomenduotos, tai reguliarus reikalavimas vartotojui pasikeisti slaptažodį. Ar teko su tuo susidurti ten, darbe savo pavyzdžiui? jeigu mes jį paimsime, rekomendacinis madas diktuoja vis tiek amerikiečiai, tai jie turi tą tokį Nest institutą. Nacionalinis informacinių ir saugumo technologijų institutas. Jų rekomendacijos, išleistos dažnai tampa tiek ISO standartų dalimi, tiek įtakoja, garantuoju, kad šita europinė direktyva tikrai žiūrėjo į ten, kas yra rekomenduojama, Zero Trust palaikymo dalykai, tai, pavyzdžiui, jų išleista rekomendacija 2017-18 metai - sako, nebereiktų reikalauti iš vartotojo reguliariai keisti slaptažodį, nes tas maža, kad neduoda naudos, tas sukelia apgaulingą jausmą, kad tas slaptažodis yra saugus, nes tu jį neseniai pasikeitei. O kodėl? Todėl, kad vartotojai dabar vis tiek kada keičia slaptažodį, keičia turbūt paskutinę raidę ar paskutinį skaičiuką. Jeigu tas slaptažodis kažkur nutekėjo ir hashas jo buvo silpnai apsaugotas, tai iš esmės atkasti atgal koks buvo slaptažodis - galima. Tai atkasus tą, tada darant tokią labiau tikslią ataką, pakeisti paskutinę

raidę labai greitai galima, o jeigu tai yra skaičiukas, tai iš viso 10 pabandymui į tą 10 pabandymų, galbūt netgi kaip slenkstį nesureaguos apsaugos sistema, nes 10 pabandymui yra labai mažas slenkstis, tai paprasčiausiai net nepastebėsi. Antras faktorius ten yra apibrėžtas, kad jisai turi būti ir jisai yra tas, ką kuo dabar reikėtų rūpintis. Ir jeigu įsidiegė antrą faktorių, tai klausimas o kam reikia reguliariai keisti vartotojo slaptažodį? Tas galioja paprastiems vartotojams. Negalioja administratoriams administratorių prieiga ten kitas klausimas kaip ją apsaugoti, bet vat kas pakeitė šitą, sakykim, požiūrį ir nustojo iš vartotojo reikalauti slaptažodžio keitimo. Tai aš kai keliose organizacijose dirbu tai užsienietiška organizacija Skandinavijoje kurta, Crayon nustojo reikalauti slaptažodžio keitimo reguliariai, nes kaip ir pamatė, kad nebėra tikslo. KTU -nenustojo. Aš ką tik gavau priminimą, kad mano slaptažodžio galiojimas baigėsi. Turėčiau pasikeisti, tai aš dar kartelį nueisiu pas jų saugumo specialistus. Sakysiu, kad nėra čia geroji praktika šiuo metu. Bet tikiu, tai yra tik mano, mano siūlymas šitoj vietoj, o kitur irgi reikėtų žiūrėti, kaip į tai yra reaguojama, nes labai natūralu, kodėl tas negali veikti technologiškai? Todėl, kad per tinklą slaptažodis ne šifruotas niekada nėra siunčiamas, jeigu viskas gerai padaryta, vadinasi, kliento pusėje, kas tai bebūtų naršyklė ar tiesiog kompiuteris, kada tu suvedę naują slaptažodį ir nusiuntę jį nuvažiuoja hasho sistema jau serverio pusė, kuri tikrina ar geras slaptažodis, tai jis gali patikrinti pagal silpnų slaptažodžių sąrašą pagal paskutinius tavo dvidešimt keturis kokius naudotus slaptažodžius, ar tu kartais nebandai naudoti tokio paties? Bet ar pasikeitė paskutinė raidė is negali matyti hashas sukdamas iš maišo tą slaptažodį ir vienos raidės pakeitimas duoda visiškai skirtingą hashą, tu iš to negali suprasti, kiek daug vartotojas slaptažodį pakeitė. O technologiškai patį slaptažodį apsaugant mes šitoj vietoj serverio pusėj nežinom, kiek daug vartotojo slaptažodį pakeitė. O tai, kad jisai gudrauja ir tiktai paskutinį simbolį pakeitė dažnai labai dažnai dabar taip būna. Tai va, čia vienas irgi iš pavyzdžių, nes Nest rekomendacijos tikrai yra 2017-18 metų šitos, šitos dalies, šitos vietos ir per tą laiką, pajudėjimas įvyko, Crayon, pavyzdžiui, slaptažodžio keitimo atsisakė tiktai šiemet. Tai laikas labai labai didelis. Čia jeigu galvoti irgi apie tai, kas įtakoja - senas požiūris ir tas toks skeptiškas reagavimas į naujienas. Ir aišku, visada galvojimas, kad mes esame labai unikalūs, kitokie negu kiti. Čia tie standartiniai būdai pas mus netinka. Šitas irgi irgi veikia labai stipriai.

Dominyka: Jo, aš netgi kai skaitau tas teorijas ir ką rašo, tai sako, kad kai per daug, jau netgi pradedi visokių atsparumo ir prevencijos būdų naudoti, tai tiesiog jų pasidaro ir žmonės apatiški, ir labai sunku sumanaginti tą sistemą, tai deja, sutinku.

Šarūnas: Ir ir aišku, ypatingai, kai tas paveikia vartotojus. Aš esu matęs situaciją gyvai vienoje organizacijoje - naujas atėjęs administratorius pasakė, kad slaptažodžiai naudojami yra per silpni. Nors jie buvo aštuonių simbolių ilgio. Ir jisai įjungė, pasitarė su IT vadovu, reikalavimus ilgesniam

slaptažodiui. Man atrodo, 8 simboliai pasidarė minimumas ir iš karto slaptažodis turėjo pasidaryti sudėtingas. Tos didžiosios mažosios raidės, simboliai ir ir skaičiai turėjo būti. Tai tas irgi jeigu žiūrėti pagal Nestą, nerekomenduojama, tai kaip sakant iškarto kitą dieną, kadangi prievarta netgi visiems buvo pakeista ne tai, kad laukiama sekančio keitimo, visi turėjo pasikeisti. Pas daugelį ant monitorių atsirado priklijuotas lapelis su užrašytu naujuoju sudėtingu slaptažodžiu. Tas tas nutiko. Tai čia vat. O iš tokių labai baisių situacijų Lietuvoj aš esu matęs - realiai tai yra vidutinio dydžio gamybos įmonė. Regione esanti ne iš didžiųjų miestų ir dalykai ten ne super paslaptingi, pas juos ten euro paletės ir panašiai. Tai jie reikalavo vartotojų keisti slaptažodį kas dvi savaites ir aš nežinau, ar tas reikalavimas yra panaikintas, bet tiesiog tai visiškas neatitikimas to, kokie jie yra, ką jie pas save laiko, kokią informaciją, kaip reikėtų saugoti ir koks reikalavimas iškeltas slaptažodžiui.

Dominyka: Jei įdomu, įdomu. Tada turiu, matau, kad čia mūsų laikas irgi eina į pabaigą, Tai toks keletą dar klausimų užduosiu. Ar yra kažkokių nors informuotumo didinimo programų, kurias vat, nežinau savo duomenų Registrų centre, kuriuos dabar naudojate, kurios padeda gyventi, organizacijos saugumo, atsparumo strategiją? Bet jūs minėjote tuos laiškus, kad jie kitokio ir kitokio principo

Šarūnas: Gal gal aš ne nelabai supratau patį klausimą tu čia vartotojams, kad siųsti, kad jų budrumą didinti? Ar čia kažkas kito?

Dominyka Organizacija čia tie, kas dirba su tom, nu iš esmės teoriškai čia turėtų būt KTU kaip pačiai kaip organizacijai, bet čia jau dabar jūsų atskirai nuo KTU

Šarūnas: Pačios pačios sistemos gaunasi mūsų specifika irgi labai didelė, nes DNS'as jisai veikia labai žemame lygyje. Vartotojai, kurie kreipėsi į mus, į serverius mūsiškius, jie netgi neformuoja ryšio sesijos. Srautas gaunasi dėl to labai mažas. Tai technologiškai nieko visiškai sudėtingo ir netgi, tiesą sakant, iki mūsų tas tikrųjų vartotojų srautas neateina, nes yra įprasta, kad DNS'o paslaugą teikia interneto ryšio tiekėjas. Tai mes pas save dažniausiai to tokio nematome, kad tiesiogiai į mus kažkas kreiptųsi. Prevencinės priemonės, prie kurių prisidedame darydami, yra būtent kažkoks įrankis, kuris leistų panaudoti tą patį DNS kaip saugesnį įrankį, tai yra, sakykim turėti bazę įtartinų adresų ir jdigu kažkas kreipėsi ir sako koks čia tas IP adrsas, tai yrs DNS užklausą gavus blokuoti prasmę, neleisti nueiti į tą puslapį, tai šitas šita priemonė yra padaryta. Mes ją, domregas ją padarė kartu su NKSC ir pas NKS tai vadinasi užkarda. O realiai tai yra kaip tik padarytas tas tas dalykas, kuris leidžia blokuoti DNS. Bet tau reikia pasitikėti ir naudoti DNSužklausa siųsti į tą mūsų serverį, kuris tą daro. Arba dabar jau galima truputėlį ir gudriau tą dalyką daryti -naršyklė tavo gali būti saugesniu kanalu, nukreipta į tą. Tai tas yra rekomenduojama mokykloms kitiems, nes ten yra keli dalykai, kaip patenka.

Ta prasme, patikimos organizacijos turėtų daryti blokavimą, tai blokavimą daro NKSC suradę, vat, pradėjo vaikščioti kažkokie laiškai, kurie nukreipia tave į apgaulingą puslapį, kad suvestų slaptažodį. Jie užblokuoja tą puslapį DNS sistemoje ir tada jeigų vartotojai, kurie netgi negavo jokios informacijos. Sakykime, kad tai pavojinga, jie pabandys nueiti ten ir jų neįleis, parodys kitą puslapį ir sakys, kad ten yra blogai. Neik į tą puslapį. Tai vat tokio tipo priemonės jos yra. Jos kažkiek yra naudojamos, bet kitos organizacijos, kurios irgi ateina, jos saugo nuo žalingo turinio. Tai sakykim neprisimenu pavadinimo, bet ta organizacija, kuri lošimų bendrovėmis rūpinasi, tai jie dažnai blokuoja ten kažkokių lošimų bendrovės, kurios nelegalios. Kad pas jasnepakliūti, tai tau užkarda, jinai tave stabdys ne tik dėl to, kad ten yra kenkėjiška kažkas, bet ir turinys žalingas. Tas veikia kartu jungtyje. Tai vat tokios priemonės, aš manau jos padarytų teisingą darbą ir jas reikėtų plačiau naudoti. O jeigu kalbame apie organizacijų organizacijos vidų, tai tos priemonės jos yra reikalingos visose visose tose trijose srityse, kur mes apsaugą darom. Tai apsauga privalo prasidėti nuo nuo klasikos - atnaujinimai operacinei sistemai, programoms ką turi, ugniasienė, kompiuteryje turėtų būti įjungta kompiuterio nustatymai patys padaryti saugesnėj, ypač jeigu tu turėtum prisiliesti ar būti svarbesnės infrastruktūros dalis. Tai čia pradedam nuo to. Tada būtų labai gerai turėti kontrolės mechanizmą, kuris padėtų pamatyti tuos vat kompiuterius, vartotojų prisijungimus, tai yra stebėti, monitoringą daryti, kad tu galėtum sureaguoti, jeigu jeigu kažkas ne taip pagal Zero Trust, idealiu atveju, iekvienas ryšio seansas, kuris daromas, kiekviena ryšio sesija, kuri užmezgama, turėtų patikrinti, ar kažkada, ne vieną kartą per dieną adminas atėjo rankiniu būdu pasižiūrėjo ar ten viskas gerai, bet automatinės priemonės turėtų reaguoti. Tai vat būtų gerai turėti tas automatines priemones, tada antroji dalis pastebėti įsilaužimą, koks jis bebūtų, vadinasi, kažkur tinklo srautą sugaudyti arba bent jau turėti įvykius, užfiksuotussurinktų iš skirtingų vietų, daug įvykių užfiksuotų ir gebėtų juos sugretinti, sujungti, pažiūrėti, kurie yra susiję ir galbūt irgi pastebėtų seką, kuri rodytų, jog vyksta ataka. Tai tas tas momentas, bet čia yra pačių stebėjimo ar pas tave ne įsilaužia ir tada kiti dalykai, kurie leistų greitai reaguoti. Tai tas greitas reagavimas turbūt irgi lemia architektūra, kaip tu, kaip tu pasidarysi, kaip tu tinklą į segmentus sudėlios, kaip tu serverius sutvarkysi. Pavyzdžiui, jeigu tau ateina greitas poreikis perkelti savo operacijas iš vieno duomenų centro į kitą, kad aktyvus pasidarytų kitas, bet kiek laiko tai užtruks? Kas Kas tavo organizacijai yra priimtina? Tai čia tęstinumo tas klausimas, nes jisai kai kartu siejasi su prieš tai darytais veiksmais, nes tu jau turėjai pasidaryti rezervinę kopiją ir tikriausiai netgi skirtumų tą perdavimą organizuoti, transakcijas, replikuoti. Nesvarbu ką naudos, bet pagalvoti vat ar kokiu greičiu tu sugebėsi atkurti savo operacijas. Tai šitie dalykai jie turėtų būti apgalvoti ir išbandyti prieš tai, kada tau iš tikrųjų reikės jau tą panaudoti. Būtų gerai, kad tu žinotum, tai aš sakyčiau, reikia balanso tarp šitų trijų taškų. Bet aišku, gali būti, kad reikėtų dar kažko apie ką aš nesu pagalvojęs. Nes Šita tema labai fokusuota, tai žiūriu į kažką ir gali būti, kad plačiai nematau. Aš galvoju, kad bendrai tokius klausimus būtų galima pabendrauti su Viliumi Benečiu, kuris yra NRD

CS kompanijos vadovas ir tuo pačiu labai bendruomene palaiko lietuvišką kibernetinio saugumo šitoj vietoj, jis apie tuos dalykus garantuotai yra pagalvojęs.

Dominyka: O jūs turit dar 10 minučių, ar jūs bėgate į kitą susitikimą?

Šarūnas: Aš tuoj pasižiūrėsiu, kas matosi.

Dominyka: Nes aš turėčiau dar du tokius klausimus bendrinius, bet galvoju gerai.

Šarūnas: Aš, aš galiu dešimt minučių galiu. Gerai, galiu.

Dominyka: Tai kitas mano klausimas buvo, aš klausiau apie iššūkius tarp atsparumo ir rizikų valdymo. Dabar klausimas tai kąpastebėjote, kas yra gerai, o kas kokius, kokias geręsias praktikas, tarkim, organizacijos taiko bandydamos išlaikyti tą gerąjį balansą tarp rizikos valdymo ir atsparumo?

Šarūnas: Tai aš manau, kad rizikos valdymas savaime yra labai geras dalykas ir man labai patinka dabartinė tendencija, kad daug kur rizikos valdymu viskas prasideda. Tai pati ta vizdu direktyva irgi akcentuoja rizikos valdymą. Jeigu kas anksčiau to nedarė, žiūrėjo galbūt vien iš technologinės pusės dabar bus labai sveika pradėt daryti. Nes, man atrodo, šitie akcentai rizikos valdymo kaip tik irgi sudėti ir naujajame Kibernetinio saugumo įstatyme, nes jie nu persikelia praktiškai iš tos tos direktyvos. Tai šita dalis man man patiko, patinka, nes aš manau, kad tas kaip tik leidžia pamatyti, apie ką tu galvoji. Ar tu tikrai galvoji apie visas reikalingas sritis ir kaip kurią riziką tu vertini, tau padėtų atsirinkti tai, kas yra šiuo momentu prioritetas. Jeigu tą dalyką daryti ne tik todėl, kad vien lentelę nusipiešti, bet ir arčiau tų tikrų situacijų pritraukti. Tai man šita dalis, kad rizikos valdymas vis dažniau naudojamas vis labiau patinka.
Dominyka: O atsparumo?
Šarūnas: O atsparumas. Mes diskutuojam dėl kelių dalykų, jau čia ne KTU, turbūt, nors šie dalykai siejasi be jokios abejonės. Sakykim, modelis kaip dirba apskritai DNS zoną prižiūrinti sistema, jis yra nulemtas ICAAN organizacijos ir gerųjų praktikų reikalvimų. Ir ten yra tam tikri momentai, ko negali daryti. Ta vadinama split-brain konfiguracija kada, sikkim, ta pati zona taškas LT vienoj vietoj atrodytų vienaip, kitoj kitaip. Pagal dabartinį modelį taip nesidaro. Jeigu karas prasideda ir nutrūksta tarptautinis interneto ryšys, tai patį tą modelį, ką mes darysim tokioj situacijoj, jį reikia kurti, tai atsparumas vienos organizacijos, jisai iki tam tikrų sistemų, kurios neglobalios ir neturi ryšių su kitais, jos gali būti labai lengvai sugalvotos kaip padaryti ar netgi išbandytos. O kada tu darai ir galvoji apie tęstinumą kažkieno, kas sieja tave su kitom organizacijom, tą patį elektroninį paštą, kai galvoji kaip

darysi, tai kita organizacija turi naudoti tuos pačius būdus. Nes jeigu jie naudosis kitaip, tas neveiks. Pvž., jeigu remsimes, Ukrainos pavyzdys tą rodo, kad ir mobilų ryšį labai sunku užmusti, ir naudotis debesų kompiuteryje yra labai geri, nes tu nesi priklausomas nuo savo duomenų centro. Vadinasi tau reikia tada turėti kažkokių ryšio primeonių, kad nuo kurių bus taco dabartiniams kanalams, tu galėtum naudotis. Tai vat tas Starlinkas yra viena iš tų priemonių, kurią turbūt urėtum įsigyti ir patikrinti kaip naudoja ir veiktų. Jeigu darai kitą planą, kad pas save kažkur išsaugosi vieną kitą serverį ir tas serveris tada turėtų naudoti elektroniniam paštui siųsti čia Lietuvoje, kad kelios susijusios organizacijos veiktų, tas planas šiuo momentu atrodo niekiap nesuderinamas su tuo kitu, kas renkasi debesų kompiuteryje kaip variantą, kad čia neunaikinsi duomenų centro ir toliau galėsi naudotis, nes plačiai pasiskirstytą ryšį sunkiau nutraukti. Tai čia reikėtų pagalvoti. Aš suprantu, kad tos strategijos važiuoja labai skirtingas puses ir net gali būti, kad tarpusavyje nesudeirinamos. Tiesiog apie tai reikia galvoti. Ir yra variantų apie tą vidinę strategiją jinai turėtų įtraukti tavo partnerius, tiekejo kanalas arba partnerystės kanalas, kuris tau reikalingas irgi turėtų būti dalis to sprendimo. Tai tas sudėtinga. Vienas to sprendimo padaryti negali.

Dominyka: Tuomet paskutinis mano klausimas - minėjot ir tą kibernetinio saugumo įstatymą, kaip Jūs apskritai vertinat - Jau aš supratau, kad Jūsų požiūris yra visai teigiamas, kad jis veikia ir apskritai ką jis ten nurodo yra geras reikalas, bet girdėjau visokių nuomonių, kad ir interpratavimas užima laiko ir kad ta dokumentacija trukdo greit reaguoti į besikeičiančą dinamišką aplinką ir reaguot į grėsmės, kad negali iškart, reik viską apsirašyt ir tada veikti, tai kartais nespėji apsirašyti. Tai vat įdomu, koks būtų Jūsų požiūris į bendravimą su NKSC ir įstatymą.

Šarūnas: Tai aš galvoju, kad ir pirmasis kibernetinio saugumo įstatymas, kuris buvo skirtas ir ne mažoms organizacijoms, jis įtraukdavo kai kurias mažas organizacijas, nieko nepadarysi. Ir iš esmės tas reiškia, kad tose organizacjose turėtų atsirasti resursų, arba turėtų atsirasti galimybė outsourcinti tuos resusus, kad galėtum panaudoti. Tai pirmam įstatyme taip gerai nebuvo sudėliota viskas, šitas dalykas daug geriau sudėliotas dabar. Aš dar nemačiau žinutės, kurią NKSC skelbė mažom ir vidutinės organizacijoms, jie jau turėjo vieną susitikimą, žada pakartoti Sausį ar Vasarį, ta aš sakiau būtinai paklausysiu, nes šita mintis man šiaip yra įdomi, aš irgi galvoju, ką galima būtų padaryti, dairausi kitur, nes akivaizdu, kad sakykim viso to tokio formalumo šitos mažos organizavijos nepaeš. Didelėms organizacijoms tai yra atitikties klausimas, ir jeigu tu esi įpareigotas tą daryti, tai privalai rasti būdų kaip tą padarysi. O tai, kad NKSC ir KAMAS, kurie perkelinėjo šitą reglamentą, jie nebandė nieko išrasti Lietuviško. Jeigu iš esmės pažiūrėsim ten, tai tą patį ISO 27001 aprašytą, tai yra žiauriai gerai, nes jeigu tu jau šitą esi pasidaręs, tai tu jau 80-85 procentus būsi padaręs tai, ko reikia. Tai kad šita sistema padaryta dinamiška, tai tu būsi įtrauktas į tą sistemą svarbių organizacijų, jeigu atitiksi tam tikrus kriterius ir gali būti išbrauktas iš ten, tai tas yra labai gerai, tai mes jau turim reiškias pakankamai aiškius atrankos kriterijus ir tas rodytų kada reik įtraukti organizaciją ir jeigu dar

atsiras tos rekomendacijos, ką turėtų daryti maža ir vidutinė įmone, kurie ten gali patekti del tiekimo grandinės, tai viskas yra labai gerai, nes tu iš tiesų dalį šito viso veiksmo gali atiduoti kažkam, kas ten specializuojasi. Dabar turėti savo SOC ar CERT, tai yra operacijų lygmens padalinį, kuris reaguoja į incidentą, jeigu tas nedraudžiama, o sakoma - neturi resursų, pasiimk iš išorės šitą paslaugą, viskas tvarkoj. Nes ta organizacija, kuri ateis iš išorės, tai jie irgi norės apsižiūrėti, kaip jie galės reaguoti, nes tai yra natūralus bendradarbiavimas. Ir tu būsi priverstas kilstelėti savo branos lygmenį iki priimtino. Tai kaip kiekvienas galės, taip kiekvienas dirbs. Kaip patikrinti šitą atitktį - nežinau, nes šitą norėtųsi dayrit, nes visi tikrai nesugebės sudalyvauti pratybose, bet kuo toliau, tuo labiau pratybos tam branduoliui, kas įėjo į sąrašą tų kritiškai svarbios infrastruktūros, tai va ten yra, nes ten ta vieta, kurią iš tiesų labiausiai reikėtų saugoti. O kiti dalykai pasitemps. A manau labai teigiamai. Man labai patiko kaip šita naujoji direktyva buvo nuleista į lietuvišką įstatyma ir NKSC požiūris labai šiuo momentu patinka.