MYKOLO ROMERIO UNIVERSITETAS
EKONOMIKOS IR VERSLO FAKULTETAS

JONAS VAITKEVIČIUS
(KIBERNETINIO SAUGUMO VALDYMAS)

VALSTYBĖS INSTITUCIJŲ PORTALŲ APSAUGA KIBERNETINĖS SAUGOS VALDYMO PRIEMONĖMIS

Magistro baigiamasis darbas

Vadovas
Prof. dr. *Tadas Limba*

VILNIUS
2020

TURINYS

ĮVADAS **4**

1. PORTALŲ APSAUGOS KIBERNETINĖS SAUGOS VALDYMO PRIEMONĖMIS TEORINIAI ASPEKTAI **8**

1.1. Portalų apsaugos samprata ir portalų apsaugos elementų analizė 8

1.1.1. Portalų apsaugos samprata 8

1.1.2. Interneto svetainių ir aplikacijų architektūros analizė 9

1.1.3. Portalų konfigūracijos klaidų analizė 13

1.1.4. Dažniausiai pasitaikančių į žiniatinklio aplikacijas nutaikytų atakų analizė 15

1.2. Kibernetinės saugos grėsmių ir portalų apsaugos kibernetinės saugos priemonių analizė 17

1.2.1. Kibernetinės saugos grėsmės 17

1.2.2. Kibernetinės saugos priemonių rūšys 19

1.3. Kibernetinio saugumo valdymo priemonių įgyvendinimo problemų analizė 24

2. PORTALŲ APSAUGOS KIBERNETINĖS SAUGOS VALDYMO PRIEMONĖMIS PASAULINĖS PATIRTIES ANALIZĖ **28**

2.1. Kibernetinės saugos valdymo priemonių taikymas Jungtinėse Amerikos valstijose 28

2.1.1. Kibernetinės saugos vystymasis Jungtinėse Amerikos Valstijose 28

2.1.2. Kibernetinės saugos teisinis reglamentavimas Jungtinėse Amerikos Valstijose 30

2.1.3. Dabartinė kibernetinės saugos situacija JAV 35

2.2. Kibernetinės saugos valdymo priemonių taikymas Nyderlanduose 38

2.2.1. Kibernetinės saugos vystymasis Nyderlanduose 38

2.2.2. Kibernetinės saugos teisinis reglamentavimas Nyderlanduose 40

2.2.3. Dabartinė kibernetinės saugos situacija Nyderlanduose 44

2.3. Kibernetinės saugos valdymo priemonių taikymas Lietuvoje 47

2.3.1. Kibernetinės saugos vystymasis Lietuvoje 47

2.3.2. Kibernetinės saugos teisinis reglamentavimas Lietuvoje 49

2.3.3. Dabartinė kibernetinės saugos situacija Lietuvoje 52

2.4. Kibernetinės saugos valdymo priemonių taikymo lyginamoji analizė pasaulio šalių kontekste 55

3. VALSTYBĖS INSTITUCIJŲ PORTALŲ APSAUGOS KIBERNETINĖS SAUGOS VALDYMO PRIEMONĖMIS VERTINIMO METODOLOGIJA **57**

3.1. Empirinio tyrimo metodologija 57

3.1.1. Empirinio tyrimo tikslas ir uždaviniai 58

3.1.2. Empirinio tyrimo imtis 58

3.1.3. Empirinio tyrimo loginė eiga 60

3.2. Empirinio tyrimo duomenų analizė 60

IŠVADOS IR PASIŪLYMAI **67**

LITERATŪROS SĄRAŠAS **69**

ANOTACIJA **75**

ANNOTATION **76**

SANTRAUKA **77**

SUMMARY **78**

PRIEDAI **79**

LENTELIŲ SĄRAŠAS

1 lentelė Kibernetinės saugos įgyvendinimo etapai 26
2 lentelė Lietuvos pozicija pagal kibernetinį pasirengimą NCSI ir GCI indeksuose 54
3 lentelė Lyginamoji Jungtinių Amerikos Valstijų, Nyderlandų ir Lietuvos kibernetinės saugos valdymo priemonių taikymo analizė 55
4 lentelė Valstybinio ir privataus sektoriaus organizacijų portalų apsaugos situacija 62

PAVEIKSLŲ SĄRAŠAS

1 pav. Magistro baigiamojo darbo struktūros loginė schema 7
2 pav. Žiniatinklio programų komponentai 10
3 pav. Išorinės sistemos veikimas 12
4 pav. Galinės sistemos veikimo principas 13
5 pav. JAV už kibernetinę saugą atsakingų tarnybų sąveika 31
6 pav. Federalinių agentūrų pateikiama kibernetinių incidentų statistika 2006-2018 metais 37
7 pav. JAV 2005-2019 metais įvykusių duomenų saugumo pažeidimų ir nutekintų įrašų kiekiai 37
8 pav. Nyderlandų Nacionalinio kibernetinės saugos centro organizacija 41
9 pav. Koordinuoto spragų atskleidimo pranešimų statistika 46
10 pav. Koordinuoto spragų atskleidimo praneštos klaidos pagal tipą 46
11 pav. Duomenų saugumo pažeidimų kiekis Europos valstybėse 2018/05-2019/06 47
12 pav. Už kibernetinių nusikaltimų sprendimą atsakingos Lietuvos institucijos 50
13 pav. Populiariausios ryšių ir informacinių sistemų kibernetinės grėsmės 2019 metais 53
14 pav. Populiariausios identifikuojamos TVS Lietuvoje 54
15 pav. Ekspertų skaičiaus įtaka vertinimo patikimumui 59

ĮVADAS

Temos naujumas ir aktualumas. Interneto atsiradimo pradžioje įvairių valstybės institucijų ir organizacijų svetainės buvo kuriamos norint suteikti informaciją apie tam tikrą instituciją, žmonėms padėti suprasti įvairias jiems aktualias temas susijusiais su tų organizacijų veikla. Maždaug nuo 2000 metų institucijų portaluose be informacijos skelbimo buvo pradėtos teikti įvairios paslaugos: dokumentų šablonai, dokumentų parengimo užsakymas, prieiga prie įstaigų valdomų registrų, duomenų užsakymas iš duomenų bazių ir kt. Iki tol visos šios paslaugos buvo prieinamos tik fiziškai atvykus į pačią įstaigą. Šios interaktyvios paslaugos nuo pat savo atsiradimo pradžios traukė piktybiškai nusiteikusius žmones, kurių pagrindiniai siekiai - įsilaužti, sunaikinti, pakeisti ar tiesiog palikti savo žymę interneto puslapyje. Kadangi pradinis portalų sukūrimo tikslas buvo informacijos skelbimas, juos kuriant nebuvo mąstoma apie informacijos saugą ir portalų varikliai buvo nepritaikyti saugumo technologijų diegimui. Dažnai būdavo taip, kad pildant portalus naujomis funkcijomis ir paslaugomis, jos būdavo integruojamos tiesiogiai į seną ir nesaugų portalą, o ne kuriamas naujas patikimas sprendimas. Kiekvienas naujas portalo elementas didindavo portalo saugumo spragas.

Pasaulio ekonomikos forumo leidžiamame Globalinių rizikų vertinimo dokumente jau daugiau kaip penkis metus kibernetinių atakų grėsmė patenka į dešimties svarbiausiųjų sąrašą pagal tikimybę įvykti ir pagal jos poveikį, 2018 ir 2019 metais ši grėsmė buvo trečioje ir penktoje vietoje. Kaip rašoma šio tipo 2019 metų ataskaitoje šiuo metu daugiausia yra neteisingų naujienų skleidimo, asmens tapatybės vagystės, privatumo praradimo ir duomenų vagysčių tipo nusikaltimų (World Economic Forum, 2019). Dabar nepraeina nė diena be žinių apie kompiuterinius nusikaltimus ar kitus šio tipo įvykius: internetinių svetainių užvaldymas ir turinio pakeitimas (angl. *defacement*), tapatybės vagystės, niokojanti viruso ataka, pinigų nukreipimas iš banko sąskaitų, išpirkos reikalaujančios programos ir neskelbtinų duomenų vagystė. Saugumo profesionalai kaunasi nesibaigiančioje kovoje su nusikaltėliais, programišiais, teroristais ir užsienio žvalgybos agentūromis, kurie jaučia pasitenkinimą paleisdami virusus, trojanus, kirminus ir kitą kenksmingą programinę įrangą (Borky J. M., Bradley T. H., 2018).

Kai yra kuriami valstybės institucijų portalai daugiausiai dėmesio yra skiriama turiniui, prieinamumui ir naudojimo patogumui, o apie tinklalapio saugą pradedama galvoti tik vėliau. Dažni atvejai kai portalo spragos yra ištaisomos tik po įvykusių kibernetinių incidentų ar informacijos apie esamus pažeidžiamumus paviešinimo žiniasklaidoje. Nacionalinis kibernetinio saugumo centras (toliau – NKSC) savo 2019 metų nacionalinio kibernetinio saugumo būklės ataskaitoje rašė, kad atlikus Lietuvos (.lt) interneto svetainių kibernetinio saugumo vertinimą nustatyta, kad 63 % iš jų yra saugios ir 37 % pažeidžiamos. Analogiško 2018 metais NKSC atlikto tyrimo metu buvo nustatyta 48 % saugių svetainių ir 52 % pažeidžiamų, taigi situacija gerėja, bet vis dar yra daug pažeidžiamų svetainių. 2019 metų NKSC ataskaitoje taip pat rašoma apie atlikta viešojo sektoriaus interneto svetainių

pažeidžiamumų vertinimą, kurio metu paaiškėjo – į mažiau nei 1 % svetainių labai paprasta įsilaužti, į 17 % Lengva įsilaužti, į 4 % Sudėtinga įsilaužti, o 40 % svetainių yra saugios. Palyginus su 2018 metais NKSC atliktu analogišku tyrimu matosi gerėjanti tendencija, nes viešojo sektoriaus svetainių į kurias lengva įsilaužti kiekis mažėjo 4 %, svetainių į kurias sudėtinga įsilaužti kiekis mažėjo 1 %, o saugių svetainių kiekis padidėjo 11 %. Taigi situacija viešajame sektoriuje gerėja, bet vis dar yra nemažai tobulintinų sričių. Tuo tarpu CERT-LT savo metinėje 2017 metų veiklos ataskaitoje pažymi kad per 2017 metus CERT-LT gavo ir išnagrinėjo 54 414 pranešimus apie kibernetinius incidentus, atitinkamai 2016 metų ataskaitoje kalbama apie 49463, o 2015 metais – 41583 tirtus kibernetinius incidentus. Taigi kibernetinių incidentų kiekis didėją maždaug po 10% per metus, todėl valstybinės institucijos ir organizacijos privalo stiprinti savo informacinių sistemų ir portalų apsaugą ir būti pasiruošusios vis naujiems iššūkiams.

Mokslinės problemos ištyrimo lygis. Valstybinių institucijų ir organizacijų kibernetinę saugą nagrinėja: P. Petratos (2014), CH. Liu et al. (2010), G. Christou (2016), S. Baker, M. Schneck-Teplinsky (2010). Visi autoriai vieningai sutaria, kad labai svarbus aiškus ir teisingas teisinis kibernetinės saugos reglamentavimas, bei specializuoti kibernetinės saugos reikalavimai taikomi valstybiniam sektoriui ir ypatingos svarbos infrastruktūrai.

Kibernetinės saugos grėsmes ir kibernetinių incidentų pasekmės analizuojamos: S. Romanosky (2016), C. D. Heitzenrater, A. C. Simpson (2016), S. M. Bellovin et al. (2017), M. Choraś et al. (2017). Praktiškai visuose straipsniuose išskiriamos šios kibernetinės saugos grėsmės: kenksmingas programinis kodas, išpirkos reikalaujančios programos, paskirstytoji atsisakymo aptarnauti ataka, brukalai ir sukčiavimas pasitelkiant elektroninį paštą, bei tikslinės atakos.

Kibernetinės saugos valdymo priemonės aptariamos autorių: A. Stavrou et al. (2004), L. Wright (2017), B. Thuraisingham (2005), S. F. Hidhaya, A. Geetha (2012), H. Leopold (2015). Beveik visi autoriai straipsniuose kibernetinės saugos priemones skirsto į technines ar programines, teisines ir žmogiškąsias.

Nepavyko rasti straipsnių, kuriuose būtų kalbama apie kibernetinės saugos valdymo priemonių taikymą valstybinių institucijų ir organizacijų tinklų ir portalų apsaugai.

Mokslinė tyrimo problema. *Kaip apsaugoti valstybės institucijų portalus kibernetinės saugos valdymo priemonėmis?*

Tyrimo objektas – Valstybės institucijų portalų apsauga kibernetinės saugos priemonėmis

Tikslas – Įvertinus portalų apsaugos kibernetinės saugos valdymo priemones pateikti jų pritaikymo Lietuvos valstybės institucijų portalų apsaugai rekomendacijas.

Uždaviniai:

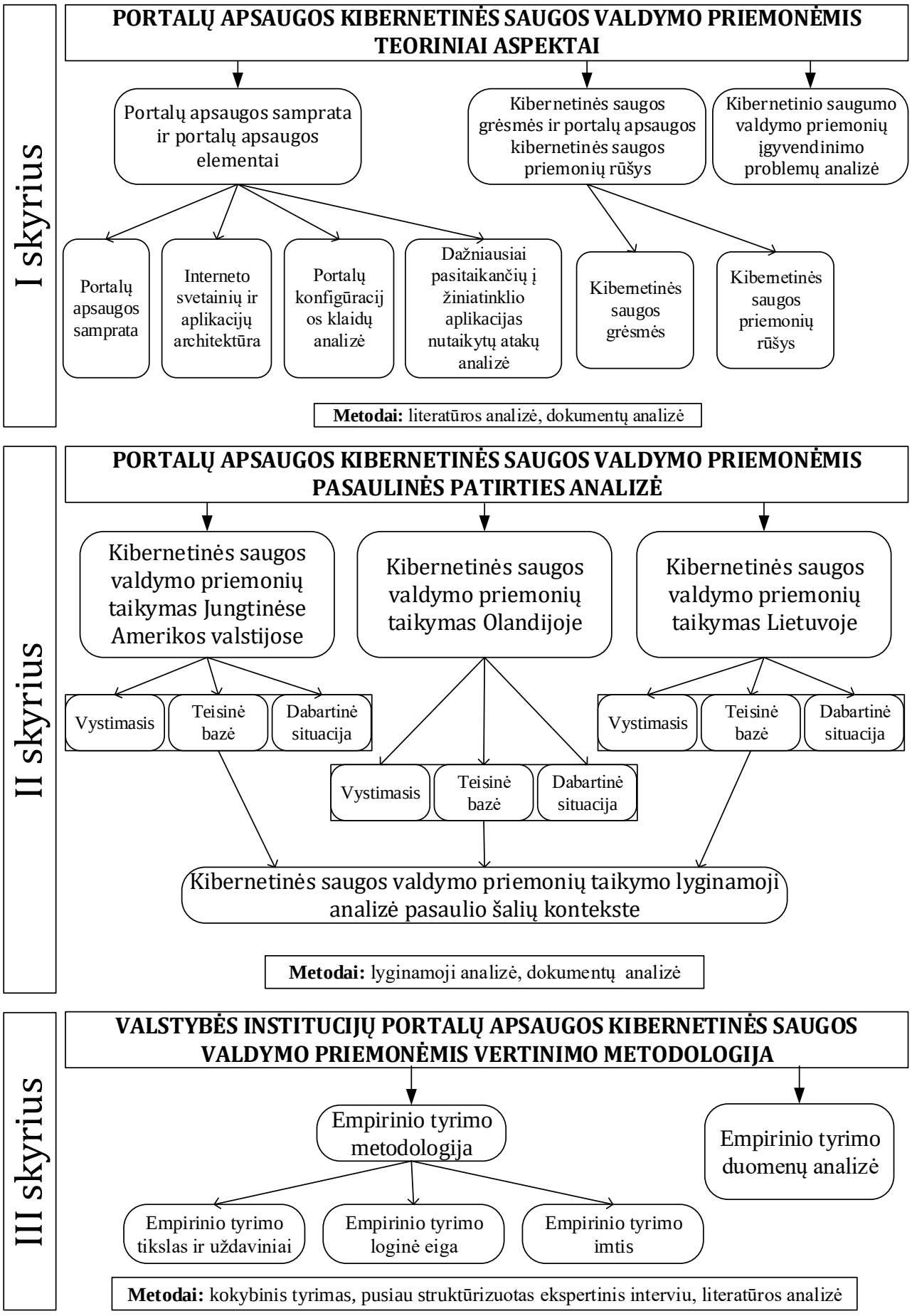
1. Išanalizuoti portalų apsaugos kibernetinės saugos valdymo priemonėmis teorinius aspektus

2. Išanalizuoti valstybinių institucijų portalų apsaugos kibernetinės saugos valdymo priemonėmis pasaulinę patirtį
3. Atlikti valstybinių institucijų portalų apsaugos kibernetinės saugos valdymo priemonėmis tyrimą

Tyrimo metodai: Literatūros analizė, dokumentų analizė, lyginamoji analizė, sisteminė analizė, kokybinis tyrimas, ekspertinis vertinimo metodas.

Darbo struktūra – darbą sudaro įvadas, trys pagrindiniai skyriai (žr. 1 pav.), išvados ir pasiūlymai, literatūros sąrašas, bei priedai.

Pirmame skyriuje yra analizuojami internetinių portalų apsaugos kibernetinės saugos valdymo priemonėmis teoriniai aspektai, analizė grįsta moksliniais straipsniais, knygomis, bei internetiniais duomenų šaltiniais. Antrajame skyriuje nagrinėjama portalų apsaugos kibernetinės saugos valdymo priemonėmis pasaulinė patirtis, lyginama Jungtinių Amerikos Valstijų, Nyderlandų ir Lietuvos kibernetinės saugos sritys. Trečiajame skyriuje pateikta pasirinkta tyrimo metodologija, aprašyta ir pagrįsta kodėl buvo pasirinktas būtent toks tyrimo metodas ir kokio tipo vertinimas bus atliekamas. Galiausiai pristatyta empirinio tyrimo rezultatų analizė, bei detaliai išnagrinėjami ekspertų atsakymai. Panaudoti 81 straipsnis, knyga ir kiti duomenų šaltiniai. Darbo apimtis – 68 puslapiai.



Šaltinis: sudaryta autoriaus

1 pav. **Magistro baigiamojo darbo struktūros loginė schema**

1. PORTALŲ APSAUGOS KIBERNETINĖS SAUGOS VALDYMO PRIEMONĖMIS TEORINIAI ASPEKTAI

1.1. Portalų apsaugos samprata ir portalų apsaugos elementų analizė

1.1.1. Portalų apsaugos samprata

Dabartinis pasaulis neįsivaizduojamas be interneto svetainių ir portalų. Kiekviena privati ar valstybinė įstaiga turi savo oficialią svetainę, reprezentuojančią jas, pateikiančią informaciją apie jų veiklą, susijusius įvykius ir sudarančią galimybę interesantams rasti kontaktus, kitą reikalingą informaciją, bei pasinaudoti specialiomis paslaugomis. Taip pat dažnai svetaines kuria ir privatūs asmenys, jose aprašydami savo veiklą, kūrybą arba kasdienio gyvenimo aktualijas. Atrodytų užsakius svetainės sukūrimą ar savo jėgomis ją sukūrus, patalpinus pas paslaugų tiekėją, galima ja nesirūpinti, tik naudotis ir kurti turinį. Neretai taip galvoja ne tik privatūs asmenys, bet ir privačių ar valstybinių įstaigų vadovai. Toks požiūris yra klaidingas, nes 2, 5, 10 ar daugiau metų neatnaujinant svetainių ir portalų vis labiau didėja grėsmė, kad bus įsilaužta ir svetainė ar portalas bus panaudoti piktybiškiems tikslams: neteisingos informacijos skleidimui, reklamai, virusų platinimui, pinigų kasimui ar tikslinėms atakoms vykdyti.

Viena iš svarbesnių priežasčių, kodėl svarbu rūpintis svetainių ir portalų sauga yra įmonės ar organizacijos reputacija. Tik dalis įsibrovimų į svetaines yra tiesiogiai sietina su noru suteršti organizacijos reputaciją ar paveikti visuomenės nuomonę, tačiau dažni atvejai, kai svetainės kode paslėpti virusai ar kita kenksminga programinė įranga, kurią įdiegdami nusikaltėliai siekia naudos sau, taip stipriai paveikia besilankančių asmenų kompiuterius, kad sulaukia atgarsio žiniasklaidoje ir prastina organizacijos reputaciją. Suprastėjusi privačių kompanijų reputacija mažina jais pasitikinčių klientų kiekį, puslapio lankomumą ir pelną, o prastėjanti valstybinių institucijų reputacija prastina bendrą pasitikėjimą valstybe ir didina gyventojų nepasitenkinimą.

Anot A. Telalev (2018) 56 % viso interneto srauto yra sukuriama automatinių šaltinių, tokių kaip laužimosi įrankiai, puslapių siuntėjai (angl. *scrapers*), brukalų siuntimo programos, apsimetinėtojai ir robotai. Dauguma kenksmingo kodo įdiegimo į svetaines atvejų yra įvykdyti ne rankiniu būdu, o automatiniais įrankiais. Šie įrankiai skenuoja visus išorinius IP adresus ir svetaines ir radę pažeidžiamumą automatiškai jį išnaudoja ir įdiegia kenksmingą kodą. Taigi bet kokiai neprižiūrimai ir neatnaujinti svetainei ar portalui kyla grėsmė būti išlaužtai. A. Telalev (2018) savo straipsnyje išskiria kelias priežastis kodėl svetainių sauga yra svarbus dalykas:

- **Išlaužtos svetainės taikosi į svetainės lankytojus**. Kenksminga programinė įranga yra panaudojama užkrėsti svetaines ar portalus, surinkti informaciją ir tam tikrais atvejais net

išnaudoti lankytojų kompiuterių resursus. Svetainė, prie kurios gavo prieigą programišius gali būti panaudota duomenų srauto nukreipimui ir lankytojų kompiuterių užkrėtimui kenksmingų programiniu kodu. Yra tūkstančiai skirtingų virusų ir tūkstančiai būdų užkrėsti svetainę.

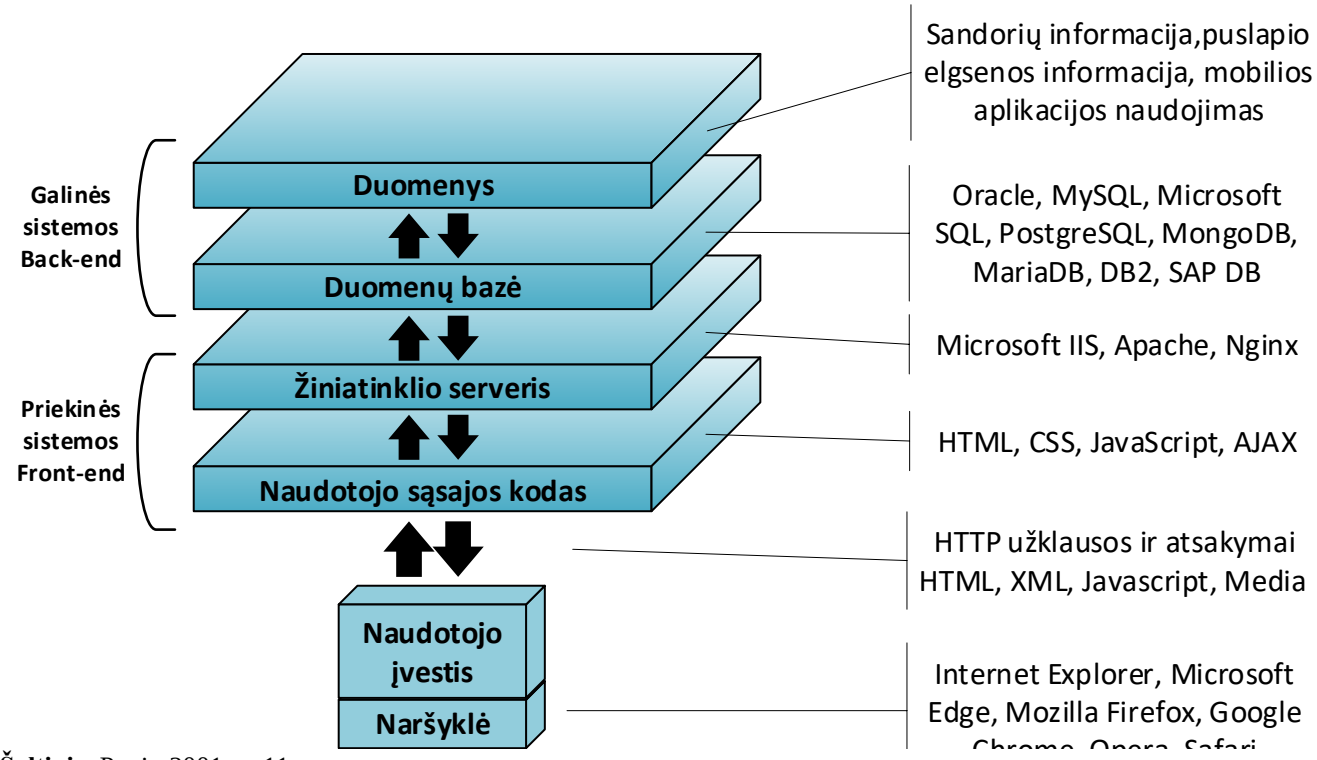
- **Nulaužtų svetainių kiekis didėja labai greitai.** 2017 metais Google paskelbė, kad lyginant 2016 metus su 2015 svetainių į kurias buvo įsilaužtą skaičius padidėjo 32 %. 2016 metų Google ataskaitoje skelbiama, kad pasaulyje yra 50 milijonų svetainių, kurios yra užkrėstos kenksmingu programiniu kodu. Taip pat šioje Google ataskaitoje skelbiama, kad 2017 metais paviešintų internetinių aplikacijų pažeidžiamumų kiekis buvo 212 % didesnis nei 2016 metais. Įmonės WebARX duomenimis jie nustatė apie 96 tūkstančius svetainių į, kurias buvo įsilaužta 2016 metais, o 2017 šis skaičius padidėjo beveik 6 kartus ir siekė 550 tūkstančių.
- **Nulaužtos svetainės sutvarkymas ir išvalymas kainuoja brangiau nei svetainės apsaugojimas.** Kai svetainės savininkas nustato, kad į jo svetainę ar portalą buvo įsilaužtą visų pirma jis ima ieškoti informacijos kaip tą svetainę sutvarkyti ir išvalyti ten paliktą kenksmingą ir nereikalinga informaciją. Daugelyje informacinių svetainių ir tinklaraščių rekomenduojama svetainės sutvarkymo ir išvalymo paslaugas užsisakyti iš profesionalų. Pašalinti kenksmingą kodą iš svetainės nėra paprasta, todėl ši paslauga nepigiai kainuoja ir ne visada yra garantija, kad svetainė bus tinkamai išvalyta. Kartais paprasčiau sukurti svetainę iš naujo ar atkurti iš atsarginės kopijos negu bandyti išvalyti.
- **Svetainė gali būti įtraukta į juoduosius sąrašus.** Anot Google skelbiamos statistikos jos turimi automatiniai įrankiai kas dieną nustato ir į juoduosius sąrašus įtraukia ne mažiau kaip 10 tūkstančių įtartinų svetainių. Google naudotojai bandydami patekti į tokią svetainę yra informuojami, kad „*ši svetainė gali pakenkti jūsų kompiuteriui*“, toks užrašas įspėja vartotojus nesinaudoti svetaine. Svetainės, kurios yra įtraukos į juoduosius sąrašus yra šalinamos iš Google paieškos ir praranda iki 95 % galimų naudotojų.

1.1.2. Interneto svetainių ir aplikacijų architektūros analizė

Taikomosios žiniatinklio programos yra sudėtingi dariniai. Vienas iš programinės įrangos apibūdinimų sako, kad programinė įranga yra “programa sukurta atlikti tam tikrą specifinę funkciją tiesiogiai naudotojui arba, tam tikrais atvejais, kitai programai. Programinės įrangos pavyzdžiai galėtų būti teksto redaktoriai, duomenų bazės, lentelių redaktoriai, interneto naršyklės ir daugelis kitų įvairios paskirties programų. Taikomoji programinė įranga naudoja kompiuterio operacinės sistemos paslaugas (angl. *services*) ir kitas pagalbines programas Trumpai tariant programa tai yra gabalas programinio

kodo, kuris daro kažkokią užduotį ir gali prieiti prie kitų kodo dalių tam, kad sėkmingai įvykdyti tą užduotį (Pettit, 2001).

Taikomosios žiniatinklio programos yra paremtos verslo logika, kuri leidžia naudotojams naršyti interneto svetainėje ir sąveikauti su visomis galutinės sąsajos (angl. *back-end*) duomenų sistemomis. Kaip pavyzdys galėtų būti žiniatinklio programos, kurios leidžia naudotojams peržiūrėti savo banko sąskaitos informaciją ir pervesti lėšas; programos, kurios leidžia naudotojams įsigyti daiktus internetu, tokios kaip pirkinių krepšelis ir pinigų perlaidų programinė įranga; prekių tiekimo grandinės programos, kurios jungia tiekėjus su gamintojais ir daugelis kitų. Visas šias programas sieja tai, kad jos sudarytos iš



Šaltinis: Pettit, 2001, p. 11

2 pav. **Žiniatinklio programų komponentai**

programinio kodo, kuris buvo parašytas specialiai žiniatinklio sąsajai ir kodo, kuris skirtas pasiekti vidinius svetainės duomenis ir su jais atlikti transakcijas. Svetainės duomenų bazė ir duomenys joje yra svarbiausi žiniatinklio programos elementai. 2 pav. yra parodyti žiniatinklio programų komponentai. Kaip galima matyti iš paveikslėlio žiniatinklio programinė įranga apima kodą esantį žiniatinklio serveriuose, programinės įrangos serveriuose, duomenų bazėse ir vidinėse organizacijos sistemose. Žiniatinklio programos, tai bet kokios programos, prieinamos bet kokiu būdu, pavidalu ar forma per žiniatinklį. Skirtingos žiniatinklio programų dalys dažnai yra kuriamos, palaikomos ir prižiūrimos skirtingų organizacijos padalinių. Nors termino „programa“ pagrindinė reikšmė yra vienas konkretus objektas, bet realybėje „programos“ naudojamos didžiųjų korporacijų, iš tikrųjų yra programinio kodo rinkiniai sudaryti iš atskirų kodo dalių, kurie atėjo iš skirtingų šaltinių: pavienių programuotojų ar trečiųjų šalių tiekėjų. Visi šie atskiri programinio kodo komponentai turi derėti tarpusavyje ir tinkamai funkcionuoti. Atskirų programos kodo dalių tarpusavio integravimas reikalauja visų organizacijos skyrių

įsitraukimo ir jei integracija tarp skirtingų žiniatinklio programos dalių nėra gera arba jei bent viena kodo dalių turi neužtaisytų spragų, visa žiniatinklio programa gali visiškai neveikti arba būti pažeidžiama išorinės atakos. Remiantis išdėstytais faktais ir tuo, kaip stipriai žiniatinklio svetainių kūrėjai yra spaudžiami kuo greičiau pabaigti užsakymus, bei dabartinį kvalifikuotų saugumo specialistų trūkumą, žmogiškosios klaidos tikimybė, dėl kurios sukurta žiniatinklio programa bus pažeidžiama, yra labai didelė (Pettit, 2001).

Naudotojo sąsajos kodas. Naudotojo sąsajos kodas yra interneto aplikacijos pristatomasis lygmuo. Šis kodas sukuria svetainės išvaizdą. Jis ne tik turi kodą, kuris tiesiogiai bendrauja su žiniatinklio serverio programine įranga, bet ir pateikia naudotojo pusės kodą, kuris gali pusiau automatiškai generuoti funkcijas ir atsakymus už naudotoją tiesiai į žiniatinklio serverį. Visa naudotojo įvedama informacija yra apdorojama per naudotojo sąsajos kodą.

Išskyrus trečiųjų šalių kodą, kurio klaidos yra ištaisytos, svetainių spragos daugiausiai yra taisomos rankiniu būdu ir tai laikoma vienu iš patikimiausių būdų apsaugoti naudotojo sąsają. Programuotojai turi Įsitikinti, kad į svetainę įvedami duomenys būtų tinkamai apdorojami, taigi svetainių sauga labai priklauso nuo programuotojo sugebėjimo ir žinių tinkamai apsaugoto svetainę.
Daugelis svetainių kūrėjų nėra programinės įrangos pažeidžiamumų ekspertai ir nežino dažniausiai pasitaikančių svetainių pažeidžiamumų, kuriuos hakeriai gali panaudoti įsibrovimui. Svetainių kūrėjai siekdami supaprastinti svetainės kūrimą arba sutaupyti laiko naudoja nesaugius metodus svarbiai informacijai saugoti, tokiai kaip prekių kainos, slaptažodžiai ar kita. Kai kuriais atvejais saugumo spragos būna svetainių naudojamose bibliotekose ir kodo tvarkylėse, tačiau programuotojai negali ištaisyti šių spragų patys ir turi naudotis gamintojų kuriamais ištaisymais. Pastovus bibliotekų ir pagalbinių įrankių atnaujinimas yra sistemos administratorių rūpestis.

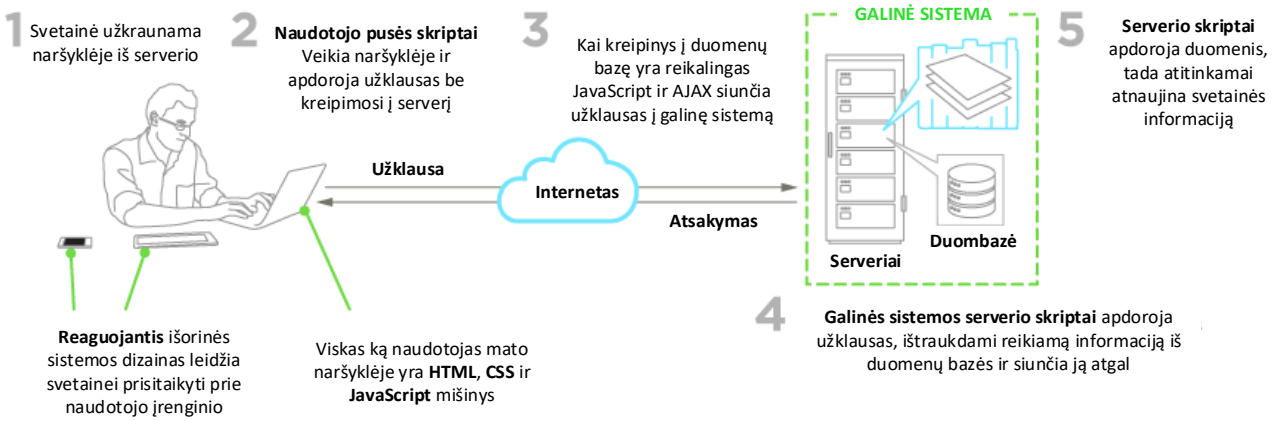
Dažniausiai pasitaikančios internetinių puslapių programavimo kalbos yra HTML, Java, JavaScript, Python ir CSS. Naudotojo sąsajos kodas gali būti parašytas trečiosios šalies arba sukurtas savarankiškai su grafinė vartotojo sąsajos įrankiais. Šis kodas siejasi tiesiogiai su naudotoju, žiniatinklio serverio programine įranga ir su išorinėmis sistemomis (angl. *Front-End*).

Žiniatinklio serverio programinė įranga. Žiniatinklio serveris palaiko fizinę komunikaciją tarp naudotojo naršyklės ir žiniatinklio programų, kurias naudotojas turi pasiekti. Jis apdoroja visas vidun ir išorėn keliaujančias HTTP ir HTTPS užklausas, valdo naudotojo sesiją (jos nutraukimą, sesijos sausainiukus (angl. *cookies*) ir tikrina ar visos sesijos yra korektiškai apdorojamos.

Kadangi praktiškai visos kompanijos naudoja žiniatinklio serverių programinę įrangą sukurtą trečiųjų šalių gamintojų, tokių kaip Microsoft IIS, Nginx, Google ir Apache, kompanijos turi pasitikėti gamintojo sugebėjimu pateikti programinę įrangą be klaidų ir sukurti taisymus jei būna aptinkamos spragos. Nors kompanijos sistemų administratorius gali įsitikinti, kad žiniatinklio serverio programinė

įranga yra sukonfigūruota tinkamai, jie yra priversti dirbti svetainės aplinkoje, kurią jie prižiūri ir negali daryti kardinalių pakeitimų. Tam tikrais atvejais svetainės saugumo konfigūracija gali konfliktuoti su patogiu svetainės naudojimu ir stabiliu veikimu. Kadangi dažnai sistemos administratoriai yra vertinami pagal žiniatinklio puslapių stabilų veikimą ir atsako laiką, jie ne visada yra suinteresuoti naudoti tik saugią žiniatinklio serverio konfigūraciją. Be to, net jei kompanija pasisekė turėti sistemų administratorių, kuris yra ir saugumo ekspertas, kompanija vis tiek bus priklausoma nuo to ar jų naudojamo žiniatinklio serverio programinė įranga yra reguliariai atnaujinama. Nuo to laiko, kai pažeidžiamumas yra aptinkamas iki kol jam pataisyti išleidžiamas atnaujinimas dažnai praeina dienos ar net savaitės. Žiniatinklio serverio programinė įranga sąveikauja tiesiogiai su išorinėmis sistemomis, operacine sistema, tinklu ir naudotojo sąsajos programiniu kodu.

Išorinės sistemos. Išorinės sistemos (žr. 3 pav.) sąveikauja tiesiogiai su naudotojo sąsajos kodu, operacine sistema ir galinėmis sistemomis. Paprastai naudotojas nesąveikauja tiesiogiai su šiuo sluoksniu, tačiau duomenys, kuriuos naudotojas pateikia žiniatinklio puslapio sąsajos kodui yra persiunčiami per išorinę sistemą. Svetainę prižiūrintys darbuotojai norėdami išlaikyti išorinę sistemą saugią turi sekti viešai skelbiamas naudojamos programavimo kalbos klaidas, pažeidžiamumus ir laiku diegti jų ištaisymus ir atnaujinti bibliotekas, bei pagalbinius įrankius. Išorinių sistemų kūrėjai turi užtikrinti, kad naudotojui įvedus klaidingus duomenis ir neteisingą meta informaciją, jie bus tinkamai apdoroti ir nenutrauks sistemos darbo. Išorinių sistemų pavyzdžiai (Arsenal, 2018 ir Wappalyzer, 2018) tai Bootstrap, Microsoft ASP.NET, Ruby on Rails, Laravel, Google Web Toolkit, Material Design Lite, UIKit. Pačių suprogramuotų išorinių sistemų pavyzdžiai yra CGI, JSP, ASP. Dažniausiai CGI yra kuriama aukšto lygio programavimo kalbomis, tokiomis kaip PHP, Perl, C/C++, Python.

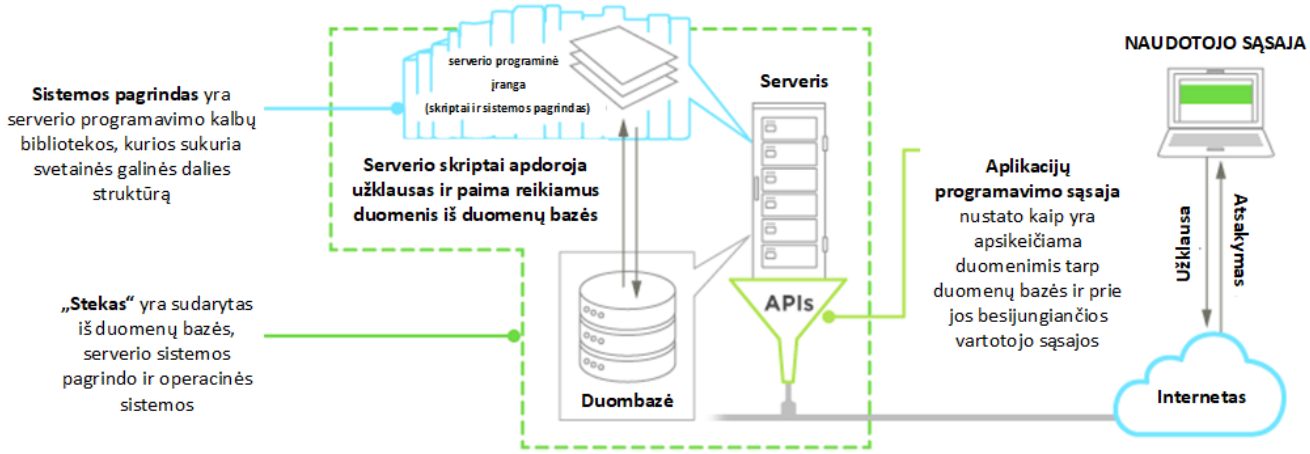


Šaltinis: Wodehouse, 2017

3 pav. **Išorinės sistemos veikimas**

Galinės sistemos yra pagrindinis žiniatinklio aplikacijų variklis. Verslas turi valdyti galines sistemas ir taip palengvinti internetinių transakcijų vykdymą. Naudotojų įvestis ir veiksmai atliekami žiniatinklio aplikacijoje yra perduodami į šį lygį per naudotojo sąsajos kodą ir išorines sistemas. Galinės sistemos (žr. 4 pav.) sąveikauja tiesiogiai su išorinėmis sistemomis, operacine sistema, duomenų baze ir

duomenimis. Galinės sistemos programinė įranga gali būti bendriniai produktai gaminami trečiųjų šalių arba pačių sukurti ar adaptuoti produktai. Galinės sistemos gali būti sudėtingos kaip pavyzdžiui bankinės ir finansų sistemos arba mažiau sudėtingos, tokios kaip interneto informacijos paslaugos, paieškos varikliai ir kt.



Šaltinis: Wodehouse, 2017

4 pav. **Galinės sistemos veikimo principas**

Galinės sistemos yra panašios į išorines sistemas, tuo, kad jas gali sudaryti kombinacija trečiųjų šalių kodo ir pačių kurto kodo. Darbuotojai prižiūrintys galines sistemas turi rūpintis, kad jose būtų įdiegti naujausi gamintojų pataisymai ir naudojama gamintojo rekomenduojama konfigūracija. Programuotojai turi užtikrinti, kad bet koks papildomas pačių sukurtas programinis kodas būtų saugus ir galės tinkamai apdoroti meta duomenis ir programinės įrangos triktis.

Duomenų bazė tai yra rinkinys duomenų, kurie suorganizuoti taip, kad jų turinys galėtų būti lengvai pasiekiamas, valdomas ir atnaujinamas. Duomenų bazė valdo duomenis, kuriuos naudoja žiniatinklio programa ir kontroliuoja kuriuos duomenis reikia pateikti. Dažniausiai žiniatinklio puslapiuose naudojamos duomenų bazės yra MySQL, Microsoft SQL, PostgreSQL, Oracle ir DB2 (angl. *SQL- Structured Query Language)*. Šio lygmens palaikymo komanda turi įsitikinti, kad sistemos parametrai yra nustatyti tinkamai ir jiems suteiktos teisės yra ne per didelės. Taip pat operacinės sistemos įrankiai turi būti teisingai sukonfigūruoti ir atnaujinti. Duomenų bazės administratoriai turi ne tik teisingai sukonfigūruoti bazę, bet ir įdiegti visus žinomus pažeidžiamumus ištaisančius atnaujinimus. Duomenų bazės programinės įrangos kūrėjai turi taip sukonfigūruoti ją, kad sistema gebėtų tinkamai reaguoti į neteisingas užklausas ir meta kodą. Duomenų bazė sąveikauja tiesiogiai su galinėmis sistemomis, duomenimis ir operacine sistema (Pettit, 2001).

1.1.3. Portalų konfigūracijos klaidų analizė

Kaip buvo kalbėta praeitame skyriuje portalų saugumas labai priklauso nuo to ar teisingai yra sukonfigūruotos išorinės, vidinės ir duomenų bazių sistemos, bei nuo to ar ryšiai tarp jų yra tinkamai

apsaugoti. Išorinėse sistemose naudojamas žiniatinklio serveris vaidina svarbų vaidmenį portalų saugoje, todėl labai svarbu jį tinkamai sukonfigūruoti ir nepalikti gamyklinių nustatymų. Dažniausiai pasitaikantys žiniatinklio serverių neteisingo konfigūravimo atvejai (Umesh Hodeghatta R., Umesha N., 2014):

- Numatytieji naudotojai ir numatytosios teisės yra nepakeistos
- Pavyzdinės bylos ir skriptai yra paliekami nekeisti
- Numatytoji konfigūracija paliekama nepakeista
- Teisės jungtis prie portalo direktorijų nėra tinkamai sukonfigūruotos
- Nesutvarkytos žiniatinklio serverio programinės įrangos saugumo spragos ir defektai arba operacinės sistemos neištaisyti pažeidžiamumai

Kiekvienas iš šių neteisingos konfigūracijos atveju turi savo specifiką, kurią reikia aptarti.

Nepakeisti numatytieji naudotojai ir numatytosios teisės. Dažniausiai pirmą kartą įdiegus žiniatinklio serverius, tokius kaip Microsoft IIS, Apache, Nginx, Tomcat ir kitus jų konfigūracija būna numatytoji: pradiniai vartotojai ir slaptažodžiai arba visiškas slaptažodžių nebuvimas ir numatytosios naudotojų teisės. Tik įdiegus žiniatinklio serverį svarbu nuspręsti kokių sistemos naudotojų ir jų teisių iš tikrųjų reikia, atitinkamai pakeičiant naudotojų identifikacinius vardus ir nustatant sudėtingų slaptažodžių politiką. Pradiniai leidimai turi būti pakeisti taip, kad nebūtų perteklinių teisių (Umesh Hodeghatta R., Umesha N., 2014).

Neištrinamos pavyzdinės bylos ir skriptai. Siekiant įgalinti paprastus naudotojus lengviau ir efektyviau sukonfigūruoti žiniatinklio serverį ir paleisti bazinį funkcionalumą dauguma žiniatinklio serverių ateina su pradinėmis pavyzdinėmis bylomis ir automatizavimo skriptais. Jie turi būti pašalinti, nes jie netinkami naudoti profesionaliems žiniatinklio serverio administratoriams. Jei šios bylos nebus pašalintos ir liks gulėti žiniatinklio serverio direktorijose, jos gali būti panaudotos hakerių atliekant atakas prieš žiniatinklio serverį (Umesh Hodeghatta R., Umesha N., 2014).

Nekeičiama numatytoji žiniatinklio serverio konfigūracija. Žiniatinklio serveris turi būti sukonfigūruotas remiantis gerosiomis praktikomis ir veikti patikimai. Pradinė konfigūracija turi būti įvertinta ir pakeista, priklausomai nuo organizacijos poreikių ir serveryje planuojamų diegti aplikacijų. Reikia nepamiršti nustatyti ir sukonfigūruoti šiuos parametrus: SSL sertifikatai, administratorių funkcijų nustatymai, duomenų ir slaptažodžių šifravimo politika, programavimo funkcijos. Nereikalinga ar nenorima serverio konfigūracija turi būti atitinkamai pakoreguota (Umesh Hodeghatta R., Umesha N., 2014).

Netinkamai nustatytos teisės prisijungti prie portalo direktorijų. Pasitaiko atvejų, kai žiniatinklio serverio administratorius nesukonfigūruoja prieigos teisių įvairių serverio bylų ir direktorijų pasiekimui. Naudojant nenustatytas ar neteisingai nustatytas bylų / direktorijų prieigos teises gali

atsirasti galimybė hakeriams lengvai keliauti per įvairias, įprastai jiems nepasiekiamas, žiniatinklio serverio direktorijas. Tokio tipo ataka yra vadinama direktorijų keliavimo ataka (angl. *Directory Traversal Attack*). Dažniausiai ši ataka veikia senuose Windows IIS serveriuose, kuriuose nėra įdiegti naujausi sistemos spragų ištaisymai (Umesh Hodeghatta R., Umesha N., 2014).

Saugumo spragos ir defektai žiniatinklio serveryje arba operacinėje sistemoje. Kasdiena atrandamos naujos žiniatinklio serverius ir pagrindines operacines sistemas galinčios pažeisti saugumo spragos ir defektai. Apie spragas ir defektus informuoja žmonės, kurie juos aptinka arba specializuotos kompanijos sekančios pažeidžiamumus. Po kiekvienos naujos spragos aptikimo žiniatinklio serverių ir pagrindinių operacinių sistemų gamintojai išleidžia programinės įrangos pataisas ir atnaujinimus, kurie ištaiso klaidas. Savalaikis žiniatinklio serverio ir operacinės sistemos pataisų ir atnaujinimų diegimas užtikrina, kad portalai bus saugų (Umesh Hodeghatta R., Umesha N., 2014).

1.1.4. Dažniausiai pasitaikančių į žiniatinklio aplikacijas nutaikytų atakų analizė

Kaip minėta anksčiau žiniatinklio programos suteikia reikiamą sąsają klientų prisijungimui ir reikalingų veiksmų atlikimui su siekiu gauti prieigą prie reikiamų duomenų. Remiantis OWASP Top 10 projekto (2017) pateikiama informacija ir Umesh Hodeghatta R., Umesha N. (2014) išleista knyga dažniausiai išnaudojami pažeidžiamumai žiniatinklio aplikacijose yra:

- Injekcijos atakos
- Buferio perpildymo atakos
- XSS (angl. *Cross-Site scripting*) pažeidžiamumai
- XML išorinių subjektų ataka
- Slapukų užnuodijimas
- Sesijos perėmimas
- Neapsaugotos jautrios informacijos perėmimas
- Netinkama autentifikavimo konfigūracija
- Web aplikacijose naudojami nesaugūs komponentai ar įskiepiai
- Nepakankamas web aplikacijų stebėjimas ir priežiūra

Didelė dalis prieš žiniatinklio aplikacijas nukreiptų atakų yra vadinamosios injekcijos atakos (angl. *injection attacks*). Šios atakos metus atakuojantysis pateikia nepatikrintą turinį programai, žiniatinklio aplikacijai ar interneto svetainei. Pateiktas turinys yra apdorojamas interpretatoriaus (angl. *interpreter*) kaip dalis žinomos komandos ar užklausos. Rezultate šios papildomos komandos pakeičia kompiuterio ar žiniatinklio aplikacijos veikimą. Injekcijos atakos yra vienos seniausių ir pavojingiausių atakų tipų nukreiptų į žiniatinklio aplikacijas. Sėkmingai įvykdžius šio tipo atakas gali būti pavogti ar prarasti

duomenys, pažeistas duomenų vientisumas, įvykdyta atsisakymo aptarnauji ataka arba visiškai sukompromituotas sistemos veikimas (Muscat, 2019). Remiantis Acunetix svetainėje pateikta informacija Injekcijos atakos skirstomas į keletą tipų:

- **Kodo injekcija**. Puolantysis įterpia aplikacijos kodą parašyta tos aplikacijos programavimo kalba. Šis kodas gali būti panaudotas paleisti operacinės sistemos komandas su naudotojo teisėmis.
- **CRLF injekcija** (angl. *Carriage Return and Line Feed*). Puolantysis panaudoja eilutės pabaigos simbolius (ASCII 13, \r ir ASCII 10, \n), tarpe įterpdamas nelauktas HTTP komandas. Ši ataka gali būti vykdoma kartu su XSS ataka.
- **XSS injekcija**. Puolantysis įterpia papildomą scenarijų (dažniausiai JavaScript kalbos) į žiniatinklio aplikaciją. Šis scenarijus yra paleidžiamas aukos naršyklės.
- **Kompiuterio antraštės injekcija.** Puolantysis išnaudoja aplikacijos pasitikėjimą naudotojo HTTP antrašte slaptažodžio pakeitimui.
- **Operacinės sistemos komandų injekcija.** Puolantysis įterpia operacinės sistemos komandas ir paleidžia jas su žiniatinklio aplikacijos naudotojo teisėmis.
- **SQL injekcija.** Puolantysis įterpia SQL kalbos komandas, kurios gali nuskaityti arba pakeisti duomenų bazės turinį. Tam tikrais atvejais puolančiajam gali pavykti kurti SQL byla žiniatinklio serveryje arba net paleisti operacinės sistemos lygio komandas.
- **XPath injekcija.** Panaši š SQL injekcijos ataką, tik šiuo atveju puolantysis naudoja XML kalbos komandas. Tų komandų pagalba galima pasiekti paprastai neprieinamą informaciją ir apeiti autentifikavimo mechanizmus.

Ne mažiau pavojingos yra XSS pažeidžiamumą išnaudojančios atakos. Kaip rašoma Litnet CERT straipsnyje (2015) XSS leidžia įsilaužėliui įterpti naršyklėje vykdomą kodą į kitų naudotojų peržiūrimą interneto portalą. XSS atakos metu savavališkai įterptas kodas yra vykdomas nieko nenutuokiančio vartotojo naršyklėje, šis kodas naudojasi papildomomis privilegijomis ir gali užgrobti naudotojo sesijas (angl. *session hijacking*), sudarkyti interneto puslapį, įterpti kenkėjišką turinį, nukreipti naudotojus į kitus puslapius ar turinį. XSS pažeidžiamumai skirstomi į tris tipus:

- **Atspindėtasis XSS** (angl. *reflected* arba *non-persistent*). Įterptas kodas „atsispindi“ pačioje žiniatinklio aplikacijoje. Toks kodas yra siunčiamas HTTP užklausos parametre, o žiniatinklio aplikacija nepakankamai išfiltruoja siunčiamus parametrus ir pateikia kliento naršyklei.
- **Išsaugotasis XSS** (angl. *stored* arba *persistent*). Papildomas kodas yra išsaugomas aplikacijoje, paprastai jos duomenų bazėje ir neprafiltruotas yra gražinamas kliento

naršyklei. Dažnai šio tipo pažeidžiamumas panaudojamas interneto forumuose, kurie leidžia lankytojams savo pranešimuose naudoti HTML kodą.

- **DOM XSS** (angl. *Document object model*). Šį pažeidžiamumą galima išnaudoti puslapiuose, kurie naudoja kliento pusės JavaScript scenarijus sąveikai su puslapio turiniu. Pažeidžiamumas leidžia panaudoti DOM naudojamus parametrus: *document.referer*, *window.name*, *location* ir vykdyti kenkėjišką kodą svetainės lankytojo kompiuteryje.

Norint apsisaugoti nuo injekcijos ir XSS tipo atakų reikia naudotis saugiomis sąsajomis ir nevykdyti pateikiamo kodo tiesiogiai interpretatoriuje. Kiti būdai yra atlikti svetainės lankytojų įvedamos ir išvedamos informacijos filtravimą ir nurodyti leistinus naudoti simbolius.

Dažnai svetainėse naudojami autentifikavimo mechanizmai yra nesaugūs. Kibernetiniai nusikaltėliai tokiose svetainėse gali panaudoti įvairiais prisijungimo duomenų nulaužimo technikas. Kaip rašoma OWASP Top 10 projekto (2017) puslapyje tokiose svetainėse dažniausiai pasitaikančios problemos:

- Leidžiamos automatizuotos vartotojų ir slaptažodžių rinkinių patikrinimo operacijos, kai puolantysis yra gavęs nutekintą naudotojų vardus ir slaptažodžius.
- Leidžiamos brutalios jėgos atakos (angl. *brute force*), kai puolantysis panaudodamas specialią programinę įrangą automatiškai parenka galimą naudotojo slaptažodį.
- Naudotojams leidžiama naudoti nesudėtingus ir trumpus slaptažodžius, kuriuos kibernetiniai nusikaltėliai gali parinkti iš dažniausiai naudojamų slaptažodžių sąrašo.
- Svetainėse naudojami nepatikimi būdai slaptažodžių atstatymui, tokie kaip žiniomis paremti atsakymai į klausimus.
- Naudotojų slaptažodžiai saugomi atviru tekstu, neužšifruojant.

Norint apsaugoti svetainę nuo tokio tipo atakų, reikia: svetainėse nenaudoti gamyklinių nustatymų, taikyti kelių faktorių autentifikavimą, riboti neteisingų prisijungimų kiekį, taikyti papildomas apsaugos priemones nukreiptas prieš automatizuotus prisijungimus, naudotojų prisijungimo duomenis saugoti užšifruotus.

1.2. Kibernetinės saugos grėsmių ir portalų apsaugos kibernetinės saugos priemonių analizė

1.2.1. Kibernetinės saugos grėsmės

Skaitmeninių technologijų naudojimas siekiant padaryti nusikalstamą veiklą, taip vadinamąjį „kibernetinį nusikaltimą“, egzistavo nuo pat kompiuterių technologijos atsiradimo. Tačiau terminas iki

pat 1990 metų buvo labiau siejamas su asmeniais kompiuteriais ir tik dešimtajame dešimtmetyje interneto tinklo atsiradimas sukūrė moderniųjų kibernetinių nusikaltimų terpę (Clough, 2012).

Didžiosios Britanijos Nacionalinio kibernetinės saugos centro išleistame dokumente „Dažniausiais pasitaikančios kibernetinės atakos: poveikio sumažinimas“ kibernetinės grėsmės skirstomos pagal atakos tipą (Great Britain National cyber security center, 2016):

- Netikslinės atakos
- Tikslinės atakos

Atlikdami netikslines atakas užpuolikai neišskirdami nei vieno, atakuoja kiek įmanoma daugiau įrenginių, paslaugų ar naudotojų. Norėdami atlikti tokio tipo atakas nusikaltėliai naudojasi įvairiomis technikomis, kurios išnaudoja interneto atvirumą:

- Sukčiavimas (angl. *phishing*) – naudojant šią techniką yra siunčiamas didelis kiekis elektroninių laiškų įvairiems adresatams prašant pateikti jautrią asmenę informaciją (tokią kaip vardas, pavardė, asmens kodas, banko prisijungimo duomenys ar slaptažodžiai) arba skatindami apsilankyti sufalsifikuotuose interneto puslapiuose
- Vandens girdyklos ataka (angl. *water hole*) – sukuriamos sufalsifikuotos svetainės atrodančios kaip originalai arba išnaudojant pažeidžiamumus legaliose svetainėse įdiegiamas kenksmingas programinis kodas, kuris leidžia pasiekti svetainėje besilankančius naudotojus ir apkrėsti jų kompiuterius
- Išpirkos prašančios programos (angl. *ransomware*) – platinamos kenksmingos programos, kurios užšifruoja kietąjį diską ir vėliau reikalauja sumokėti tam tikrą pinigų sumą, kad būtų išjungtas šifravimas
- Nuskaitymas (angl. *scanning*) – atakuojamas didelis kiekis interneto adresų atsitiktine tvarka ieškant pažeidžiamumų ir spragų.

Tikslinės atakos yra pritaikomos konkrečiai kompanijai, nes užpuolikas yra susidomėjęs būtent tam tikra organizaciją, jos verslu arba jam buvo sumokėta, kad atliktų specializuotą ataką prieš konkrečią įstaigą ar organizaciją. Pasiruošimas atlikti šio tipo atakas gali užtrukti daug laiko, nes reikia parinkti geriausią būda kaip patekti į organizacijos tinklą ar pasiekti konkretų darbuotoją. Dažniausiai tikslinės atakos padaro žymiai didesnę žalą, nei netikslinės, nes jos būna specifiškai pritaikytos tam tikram puslapiui, informacinei sistemai, procesui ar personalui. Atliekant tikslines atakas paprastai naudojamos šios technikos:

- Tikslinis sukčiavimas (angl. *spear-phishing*) – konkretiems individams siunčiami laiškai su prikabintomis kenksmingomis bylomis arba su laiško tekste esančia nuoroda į puslapį su kenksmingu kodu

- Bottinklas (angl. *botnet*) tinklo panaudojimas siekiant atlikti paskirstytąją atsisakymo aptarnauti (angl. – *distributed denial of service*. toliau DDOS) ataką
- Tiekimo linijos išnaudojimas – siekiama paveikti įrangą skirtą paslaugų teikimui į įstaigą ar organizaciją

1.2.2. Kibernetinės saugos priemonių rūšys

Kibernetinė sauga yra daugiau nei vien tik ugniasienės ir antivirusinės priemonės. Tai daugiau nei vien autentifikavimas ar saugos politikos. Negalima į Kibernetinę saugą žiūrėti kaip į monolitinę ir nedalomą struktūrą. Tai sudėtingas judančių dalių rinkinys. Norint užtikrinti patikimą kibernetinę saugą reikalingas bendradarbiavimas tarp visų organizacijos padalinių ir departamentų.

Kaip rašoma Liberty Center One straipsnyje (2019) kibernetinės saugos priemones galima suskirstyti į penkis tipus:

- Programinė įranga ir žiniatinklio aplikacijos
- Duomenys ir duomenų sauga
- Tinklas ir galiniai įrenginiai
- Žmonės ir procesai
- Fizinės prieigos kontrolė

Programinė įranga ir žiniatinklio aplikacijos. Šio tipo kibernetinės saugos priemonės užtikrina, kad įmonių ir organizacijų darbuotojai naudoja tik patikimą programinę įrangą ir tik tokią, kuri nekelia rizikos vidinėms sistemoms ir duomenims. Pačios organizacijos kuriamai programinei įrangai turi būti taikomas saugus testavimas, diegimas ir gyvenimo ciklo priežiūra. Kuriama programinė įranga visada turi būti patikima ir saugi, aptiktos spragos turi būti laiku užtaisomos. Visa organizacijoje naudojama programinė įranga ir kompiuterių operacinės sistemos turi būti reguliariai atnaujinamos, negali būti jokių išimčių (Liberty Center One, 2019). Anot WaterISAC Security Information Center (2015), The Capacity Group ir Federal Communications Commission leidinių įgyvendinant šio tipo kibernetinės saugos priemones reikia laikytis tokių gairių:

- Turi būti sudarytas organizacijoje leistinos naudoti programinės įrangos sąrašas
- Kompiuteriuose turi būti išjungti visos nenaudojamos tarnybos (angl. *services*) ir programėlės
- Paprastiems kompiuterių naudotojams turi būti apribota teisė diegti programinę įrangą
- Visų organizacijoje naudojamų kompiuterinių darbo vietų operacinės sistemos turi būti automatiškai atnaujinamos

- Visa organizacijos naudojama programinė įranga turi būti reguliariai atnaujinama
- Pačių kuriama programinė įranga turi būti testuojama dėl pažeidžiamumų ir reguliariai atliekamas pažeidžiamumų šalinimas
- Darbui naudojamų mobiliųjų įrenginių operacinės sistemos ir programėlės turi būti reguliariai atnaujinamos
- Žiniatinklio tarnybinės stotyse turi būti pašalinta visa gamyklinė konfigūracija ir pakeisti slaptažodžiai
- Turi būti reguliariai atnaujinama žiniatinklio tarnybinių stočių operacinės sistemos ir programinė įranga
- Žiniatinklio aplikacijose turi būti naudojami saugaus ryšio užtikrinimo protokolai

Duomenys ir duomenų sauga. Nesvarbu ar tai būtų klientų informaciją ar produktų brėžiniai, ar planuojamų organizacijos pertvarkų planai, ši informacija yra labai naudinga kibernetiniams nusikaltėliams. Dabar kai atviras bendradarbiavimas vyrauja visose srityse yra svarbu užtikrinti į dokumentus orientuotą saugą, kuri leistų organizacijai kontroliuoti darbinę informaciją ir jos judėjimą per visas organizacijos tiekimo grandis (Liberty Center One, 2019). Remiantis Federal Communications Commission ir Liberty Center One (2019) yra keli esminiai dalykai, kurie turi būti užtikrinami įgyvendinant šią kibernetinės saugos priemonę:

- Turi būti nustatyta ir pastoviai atnaujinama informacija apie organizacijos tvarkomus duomenis
- Turi būti žinoma kokie darbuotojai atsakingi už duomenų tvarkymą ir kokiais būdais viena ar kita informacija keliauja per organizaciją
- Informacija turi būti skirstoma pagal svarbą: konfidenciali, jautri ir vidinio naudojimo. Kiekvieno tipo informacijai turi būti nustatyti skirtingi saugos metodai
- Turi būti ribojama darbuotojų prieigą prie informacijos, negalima leisti visiems darbuotojams pasiekti visa informaciją
- Prieiga prie informacijos turi būti nustatoma pagal darbuotojų darbo roles
- Turi būti daromos svarbių organizacijos veiklai duomenų ir informacijos atsarginės kopijos
- Visa svarbi informacija, kompiuterių kietieji diskai ir mobilieji įrenginiai turi būti šifruojami
- Prieiga prie bendradarbiavimo platformų, tinklo laikmenų ir informacinių sistemų turi būti apsaugota slaptažodžiais ir autentifikavimo mechanizmais
- Visi veiksmai atliekami su informacija ir duomenimis turi būti stebimi ir saugomi žurnaliniuose įrašuose

- Duomenų sauga turi netrukdyti darbui, būti patogi ir nejuntama naudotojams ir darbuotojams

Tinklas ir galiniai įrenginiai. Šiuolaikinės organizacijos kompiuterinį tinklą sudaro staliniai kompiuteriai, daiktų interneto įrenginiai, biuro įranga, planšetės ir telefonai. Taip pat svarbi tinklo dalis yra tarnybinės stotys ir tinklo apjungimo įranga, bei tinkamos aplinkos užtikrinimo įrenginiai. Norint juos visus apsaugoti reikalinga užtikrinti tinklo ir galinių įrenginių saugą (Liberty Center One, 2019). Anot WaterISAC Security Information Center (2015) ir Federal Communications Commission rekomendacijų įgyvendinant šią kibernetinės saugos priemonę reikia:

- Priklausomai nuo tinkle veikiančių įrenginių segmentuoti tinklą, suskirstant į naudotojų, tinklo valdymo, tarnybinių stočių, demilitarizuotos ir kitas reikalingas zonas
- Riboti tiesioginį prisijungimą prie vidiniame tinkle esančių įrenginių
- Skirtingų tipų įrenginius ir skirtingų padalinių darbuotojų kompiuterių atskyrimui naudoti virtualius tinklus (angl. *Virtual LAN, VLAN*)
- Įdiegti ir visame tinkle naudoti tinklo prieigos kontrolės sistemą, prie tinklo duodant prieigą tik žinomiems ir patikimiems įrenginiams
- Skirtingus tinklo segmentus atskirti ugniasienėmis ir maršrutizatoriais
- Organizacijos turimas žiniatinklio tarnybines stotis ar kitas iš išorės pasiekiamas informacines sistemas apsaugoti žiniatinklio aplikacijų apsaugos ugniasiene (angl. *Web application firewall, WAF*)
- Ugniasienėse įjungti automatinės apsaugos nuo kenksmingos programinės įrangos, įsibrovimų, pažeidžiamumų ir žiniatinklio filtravimo (angl. *webfiltering*) funkcijas
- Nuotoliniam prisijungimui prie organizacijos vidinio tinklo arba sujungimui su kitais organizacijos padaliniais, ar debesų kompiuterijos paslauga naudoti šifruotus duomenų kanalus: sukuriamus SSL-VPN arba IPSEC VPN technologijų pagalba
- Visose kompiuterinėse darbo vietose įdiegti antivirusinę programinę įrangą ir reguliariai atlikti automatinius patikrinimus nuo virusų
- Organizacijos bevielį tinklą padalinti į svečių ir darbuotojų, su skirtingomis prieigos teisėmis ir prisijungimo būdu: svečių paprastesnis, darbuotojų - sudėtingesnis
- Rinkti žurnalinius įrašus iš visų serverių, tinklo įrangos ir ugniasienių, saugant juos žurnalinių įrašų tarnybinėje stotyje (angl. *syslog*) arba Saugumo įvykių valdymo sistemoje (angl. *Security information and event management, SIEM*)

Žmonės ir procesai. Jau senai yra žinoma, kad lyginant visas kibernetinio saugumo grėsmes, žmogiškasis faktorius yra darantis didžiausią poveikį. Kaip teigiama kompanijos Shred-it atliktame tyrime (2018) teigiama, kad net 47 % duomenų vagystės atvejų yra dėl darbuotojų aplaidumo ar žmogiškosios klaidos. Kad sumažinti žmogiškosios kilmės grėsmes, svarbu organizacijoje diegti efektyvias saugumo politikas, procesus ir technines kontrolės priemones. Reikia organizacijoje sukurti tokią kibernetinės saugos kultūrą, kuri skatintų darbuotojų atsakingumą ir atskaitomybę. Organizacijos vadovybė ir padalinių vadovai turi būti supažindinti su kibernetinės saugos problemomis ir svarba, skatinant savo kasdienėje veikloje diegti kibernetinės saugos procesus ir sprendimus (Liberty Center One, 2019). Apie saugos politikas ir procesus kalbama WaterISAC Security Information Center (2015) ir Federal Communications Commission, bei IDG Communications (2018) leidiniuose, nurodant organizacijoms laikytis tokių principų:

- Kelis kartus per metus vykdyti darbuotojų kibernetinės saugos mokymus, supažindinti darbuotojus su naujai atsiradusiomis grėsmėmis, dalintis svarbia tokio pobūdžio informacija elektroniniu paštu
- Instruktuoti darbuotojus kaip elgtis kibernetinio incidento atveju ir kokių veiksmų imtis pastebėjus įtartiną tinklo veikimą ar kitus elektroninio įsibrovimo požymius
- Techniniuose ir programiniuose sprendimuose naudoti saugių slaptažodžių politikos, nustatant minimalų slaptažodžio ilgį, galiojimo trukmę, keitimo dažnumą, paskutinių naudotų slaptažodžių atsiminimą, draudimą naršyklėms įsiminti slaptažodžius, slaptažodžių saugojimo principus
- Organizacijoje keistis naujomis kibernetinės saugos įžvalgomis ir tyrimais, kad visa organizacija būtų vienodai pasiruošusi galimiems išpuoliams
- Sudaryti veiklos tęstinumo ir veiklos atstatymo, įvykus kibernetiniam incidentui, planą ir kelis kartus per metus atlikti plano veiksmingumo testavimą ir pagal poreikį atnaujinti
- Sudaryti kibernetinių incidentų valdymo planą ir jo laikytis, bei atlikti plano išbandymus kelis kartus per metus
- Sudaryti kritinės infrastruktūros sąrašą su nurodytais svarbumo prioritetais
- Sudaryti mobiliųjų įrenginių naudojimo ir asmeninių mobiliųjų įrenginių naudojimo darbe (angl. *Bring your own device, BYOD*) politiką
- Sudaryti ir laikytis išorinių duomenų ir atmintinių naudojimo politikos
- Sudaryti ir laikytis nuotolinio prisijungimo prie organizacijos tinklo politikos

Fizinės prieigos kontrolė. Ši priemonė paskutinė, bet dėl to ji tikrai nėra mažiau svarbi nei kitos. Daugybė organizacijų pamiršta, kad jų fizinės sistemos lygiai kaip ir skaitmeninės gali būti lengvai

paveiktos ar sukompromituotos blogų veikėjų ir nusikaltėlių. Seni kietieji diskai su svarbia informacija gali būti pavogti arba neteisingai utilizavus perpirkti ir panaudoti informacijos rinkimui apie organizaciją. Ši informacija vėliau gali būti panaudotą naujų kibernetinių atakų prieš organizaciją atlikimui. Tinkamai nesaugant organizacijos patalpų ir duomenų centrų nusikaltėliai gali patekti į vidų ir gauti tiesioginę prieigą prie tinklo ar kompiuterinių darbo vietų (Liberty Center One, 2019). Norint sumažinti tokių ir panašių scenarijų tikimybę ir kiekį Federal Communications Commission ir Liberty Center One (2019) rekomenduoja imtis tokių veiksmų:

- Mobiliuosiuose įrenginiuose aktyvuoti nuotolinio išvalymo funkcionalumą ir jį panaudoti kai yra pametama ar kitais būdais netenkama mobiliųjų įrenginių
- Griežtai kontroliuoti fizinę prieigą prie organizacijos patalpų, sekant ir fiksuojant kokie žmonės, per kurį įėjimai įeina ir išeina
- Techninės paskirties patalpas ir duomenų centrus nuo bendrų patalpų atriboti papildomomis durimis, į vidų įleidžiant tik tokią teisę turinčius darbuotojus
- Visus įėjimus į organizacijos patalpas ir svarbiausias patalpų vietas stebėti kameromis
- Visada saugiai uždaryti langus ir duris
- Atsikratant senos nereikalingos techninės įrangos, ypač duomenų laikmenų turi būti atliekama duomenų sunaikinimo procedūra, kritines laikmenas sugadinant nepataisomai
- Aprūpinti darbuotojus sertifikuotais dokumentų smulkintuvais ir įpareigoti juos sunaikinti visus išmetamus dokumentus, kurie gali turėti jautrios informacijos
- Didinti darbuotojų sąmoningumą ir dėmesingumą, apmokant kaip apsisaugoti nuo socialinės inžinerijos atakų
- Jei organizacijoje yra viešai prieinamų patalpų, instruktuoti tokiose patalpose dirbančius darbuotojus nepalikti matomose vietose išorinių duomenų laikmenų, mobiliųjų įrenginių ir svarbių dokumentų
- Darbo vietas įrengti taip, kad per langus ar iš viešai prieinamų patalpų nesimatytų kompiuterio ekrano vaizdo

Kibernetinė sauga yra daugiau nei prieigos kontrolė, daugiau nei ugniasienės ir tinklo stebėjimas. Kibernetinė sauga tai sudėtingas darinys sudarytas iš daugybės komponentų. Tik supratę kibernetinę saugą kaip visumą užtikrinsime savo organizacijos apsaugą nuo kibernetinių nusikaltėlių, žmogiškųjų klaidų, bei apsaugosime savo sistemas ir duomenis nuo žalos. Fizinės kontrolės priemonės, dokumentų saugumas, aplikacijų sauga, tinklo stebėjimas, darbo procesai ir kultūra yra kritiniai dalykai, jei bent vieno iš jų neprižiūrėsime galiausiai sutriks ir likusių komponentų veikimas.

1.3. Kibernetinio saugumo valdymo priemonių įgyvendinimo problemų analizė

Daugelio organizacijų vadovams kibernetinė sauga yra nepažintas pasaulis. Jie sunkiai supranta interneto saugos pagrindus ir tuo pačiu jiems sunku įdiegti kibernetinės saugos politikas, bei priemones savo organizacijose (SiriNiti, 2019). Anot KPMG grupės išleisto dokumento (2013) bet kurios organizacijos vadovybė susiduria su problema kaip garantuoti, kad jų organizacija tinkamai supras kibernetines grėsmes ir nustatys tinkamus prioritetus apsisaugojimui nuo jų. Atsižvelgiant į techninių terminų kitimą ir pokyčių spartą tai nėra lengva užduotis. Nebūnant kibernetinės saugos srities specialistu gali būti sunku nuspręsti nuo ko pradėti ir kaip susikoncentruoti į tai kas yra svarbu.

Tuo pat metu žiniasklaida prisideda prie baimės skatinimo sudarydami įspūdį, kad kiekviena organizacija yra lengvas taikinys kibernetiniams nusikaltėliams. Maža ar vidutinio dydžio kompanija turi visiškai kitokį saugumo profilį nei didelė ir dažniausiai netampa straipsniuose minimų kibernetinių incidentų aukomis. Žurnalistų rašomuose straipsniuose dažnai neatskiriami paprastų interneto sukčiautojai ir organizuotos nusikaltėlių grupės su gerai suplanuotomis strategijomis kaip vogti intelektinę nuosavybę. Puolančiojo prigimties supratimas yra labai svarbus vertinant, kokiu mastu organizacijos gali tapti kibernetinių nusikaltėlių taikiniu. Nors organizacijos vadovybė nebūtinai turi patirties ir supratimo apie kibernetinę saugą ir jos pritaikymą organizacijoje, tai netūrėtų būti priežastis visų su kibernetine sauga susijusių darbų perduoti ekspertams į rankas. Svarbu, kad kompanijos vadovybė prisiimtų atsakomybę šiose srityse (KPMG Advisory, 2013):

1. Išteklių paskirstymas kibernetinio saugumo problemoms spręsti
2. Vadovavimas ir sprendimų priėmimas
3. Kibernetinės saugos organizacinės kultūros kūrimas

Kaip rašoma Securityweek straipsnyje (2019) jau kelinti metai įmonėms yra rekomenduojami panašus kibernetinės sagos reikalavimai, tačiau vis dar labai didelis kiekis kompanijų daro klaidas bazinių saugos reikalavimų įgyvendinime. Pagrindiniai rekomenduojami saugos reikalavimai yra: pritaikyti kelių faktorių autentifikavimą (angl. *Multi Factor Authentication*), didinti matomumą ir gerinti žurnalinių įrašų surinkimą ir apdorojimą. Nors dauguma atakų gali būti sustabdytos panaudojus tinklo perimetro kontrolę, bet šios priemonės negali padėti prieš tinkle jau esančius įsibrovėlius. Norint sutramdyti tinkle jau esančius kibernetinius nusikaltėlius reikia stiprinti tinklo stebėjimą, tačiau reikia stebėti ne tik numanomus tinklo resursus, bet viską kas yra prijungta prie tinklo. Gan dažnai organizacijos daro klaidas stebėdamos savo tinklo resursus. Ekspertai kelia klausimą „Kaip organizacija gali apsaugoti savo turtą, apie kurį ji nežino“. Galima sakyti, kad kartais įsibrovėliai turi geresnį kompanijos tinklo suvokimą, nei patys kompanijos savininkai.

KPMG grupės išleistame aiškinamajame dokumente (2013) įvardinamos penkios dažniausiai pasitaikančios kibernetinio saugumo valdymo priemonių įgyvendinimo klaidos:

1. Organizacijos vadovybė išsikelia neįgyvendinamus tikslus, pavyzdžiui „Mes turime užtikrinti 100 % saugumą“, bet tokio lygio saugumo nėra. Supratus, kad tikslas sukurti 100 % apsaugą prieš kibernetinius nusikaltėlius nėra nei įgyvendinamas, nei tinkamas tikslas, reikia priimti tinkamą gynybinę poziciją. Tokia pozicija leistų geriau įvertinti priešininkus, sukuriant mechanizmus galimų ir tikrai įvykusių įsibrovimų aptikimui ir sukuriant tinkamus pajėgumus kovai su incidentu, kiek įmanoma labiau sumažinant nuostolius.
2. Mąstymas „Jeigu mes įsigysime geriausius techninius įrankius, mes būsime saugūs“ yra klaidingas. Dažniausiai efektyvi kibernetinė sauga yra mažiau priklausoma nuo technologijų, negu yra galvojama. Kibernetinės saugos pasaulyje yra pilna kompanijų siūlančių techninius sprendimus, kurie yra būtini bazinei saugai užtikrinti, bet jie nėra holistinės ir atsparios kibernetinės saugos pagrindas. Investavimas į techninius įrankius turi būti kibernetinės saugos strategijos išdava, o ne variklis.
3. Keliamas tikslas „Mūsų ginklai turi būti geresni nei programišių“, tačiau realybėje saugos politika turi būti nustatoma pagal organizacijos, o ne kibernetinių nusikaltėlių tikslus. Kova prieš kibernetinius nusikaltimus yra puikus amžinos kovos pavyzdys. Puolantieji kuria vis naujus puolimo metodus ir technologijas, o gynyba visada atsilieka vienu žingsniu. Vadovai turi žinoti apie naujus atakų mechanizmus, bet gynyba turi būti koncentruojama į svarbiausias kompanijos vertybes.
4. Yra manoma, kad atitikimas kibernetinės saugos reikalavimams yra grindžiamas tik efektyviu stebėjimu, tačiau galimybė mokytis yra tik toks svarbus kiek yra galimybių stebėti. Tik organizacija, kuri sugeba suprasti išorės pokyčius ir incidentų tendencijas, bei gali panaudoti šias įžvalgas formuojant kibernetinę strategiją ir politiką, bus sėkminga ilgajame laikotarpyje.
5. Yra manoma, kad jei organizacija pasamdys geriausius profesionalus, kurie ją saugos nuo kibernetini nusikaltėlių, ji bus saugi. Kibernetinė sauga dažnai yra matoma kaip vieno departamento ar skyriaus atsakomybė, tokia mąstysena sukelia klaidingą saugumo jausmą ir gali vesti prie didesnių problemų. Sunkiausia užduotis yra padaryti kibernetinę saugą visa ko pagrindu, pavyzdžiui kibernetinis saugumas turėtų tapti žmogiškųjų išteklių politikos dalis ir užimti pagrindinę vietą kuriant naujas IT sistemas.

Organizacijos daro klaidingas pradines prielaidas ir vėliau jomis grindžia savo tolimesniu sprendimus. Tokiu būdu susidaro visa grandinė klaidingų sprendimų (KPMG Advisory, 2013):

- Mes diegiame technines apsaugos priemones, tiksliai nesuprasdami kokį turtą turime saugoti

- Mes laikome kibernetinius nusikaltimus retai pasitaikančiais ir egzotiškais dalykais todėl stengiamės pasiekti 100 % saugumą
- Fokusuojamės į įrankius, kurie stabdo patekimą į tinklą, bet pamirštame drausti asmenims išsineši informaciją ir stebėti iš tinklo iškeliaujančius duomenis
- Mūsų saugos politika priklauso nuo to kokie įrankiai egzistuoja rinkoje, nors iš tiesų mes nežinome kas mums reikalinga
- Kai įvyksta gedimas ar incidentas, mes panikuojame
- Kibernetinę saugą siejame tik su specialistais profesionalais ir nenorime apkrauti likusios organizacijos
- Mes investuojame į įrankius, nes tai yra privaloma ir dėl to, kad žiniasklaida kas dieną praneša apie naujus kibernetinius incidentus

Siekiant išvengti ar iki minimumo sumažinti tokių ir panašių klaidų pasireiškimą įgyvendinant kibernetinės saugos valdymo priemones organizacijoje galima vadovautis Monchovitis C. straipsnyje (2019) nurodytais žingsniais. Straipsnyje aprašyti etapai buvo susisteminti ir perkelti į lentelę Nr. 1.

1 lentelė **Kibernetinės saugos įgyvendinimo etapai**

Etapas	**Kokie veiksmai turi būti atlikti?**	**Kokios dažniausiai daromos klaidos?**	**Ką reikia daryti, kad išvengti tipinių klaidų?**
1. Turto/resursų klasifikavimas ir įvertinimas	Šio etapo tikslas nustatyti kokius išteklius organizacijoje reikia saugoti (duomenys, technika, programinė įranga, procesai ir darbo eiga). Kiekvienam iš šių išteklių reikia nustatyti metaduomenis: savininkas, saugotojas, buvimo vieta, konfidencialumo lygį, poveikį, maksimalų toleruotiną su juo susijusią prastovą, atkūrimo laiką ir su juo susijusius kitus išteklius. Tai didelės apimties darbai, jiems atlikti turi būti atrinkti turto savininkas ir vadovaujantysis informacijos saugumo pareigūnas (angl. *CISO*)	Dažnai šiame etape neteisingai nustatomas turto savininkas, pavyzdžiui parenkant juo finansų departamento vadovą, nors galbūt toje organizacijoje daugiau informacijos turi materialiai atsakingas darbuotojas. Neteisingai parinkus atsakingą asmenį, analizės metu gali būti netinkamai suskaičiuotas resursų poveikio lygis ar maksimali leistina prastova, bei prie turto nepriskirti įmonės sertifikatų ar kitų svarbių dalykų..	Daugelio klaidų galima išvengti analizės atlikimui pasitelkti išorinius ekspertus. Atliekant pačią analizę reiktų bendrauti ne su vadovais, o darbuotojais, kurie atsakingi už verslui svarbias funkcijas. Reikia susipažinti su įmonės kultūra, pavyzdžiui išsiaiškinti koks asmuo geriausiai suteikia pagalba kritinių situacijų atveju kiekviename padalinyje. Galiausiai stengtis analizę daryti nuodugniai, pabūti detektyvu ir nepalikti nei vieno neapversto akmens.
2. Grėsmių ir pažeidžiamumų analizė	Šio etapo tikslas išsiaiškinti kokios grėsmės gali pakenkti mūsų organizacijai ir kokius pažeidžiamumus mūsų organizacija turi. Paprastai užduodami sau tokius klausimus kaip „Kas nori mums pakenkti“ arba „Kokia tokio puolimo tikimybė“ nagrinėjame	Šiame etape būna padaroma daug klaidų. Visų pirma organizacijos paskirti darbuotojai gali netinkamai įvertinti galimas grėsmes – „Mes esame maža įmonė, niekas mūsų nepuls, nėra jokios grėsmės“. Kitas dažnas atvejis pažeidžiamumo	Pirmo pavyzdžio atveju sprendimas nėra toks paprastas kaip kitų dviejų pavyzdžių atveju. Nenaudojamo serverio arba labai pažeidžiamos sistemos atveju reikia viską tiksliai aprašyti ir detaliai išsiaiškinti, tada samdyti išorės subrangovą, kuris

Etapas	Kokie veiksmai turi būti atlikti?	Kokios dažniausiai daromos klaidos?	Ką reikia daryti, kad išvengti tipinių klaidų?
	grėsmes. Tuo tarpu kai klausiame „Kaip lengvai galima mus užpulti?“ arba „Kaip jie gali mus pasiekti?“ nagrinėjame organizacijos pažeidžiamumus. Tokios analizės rezultatas – rizikų analizė ir sugeneruotas rizikų registras. Tokia analizė reikalauja specifinių žinių, todėl be organizacijos darbuotojų dar reiktų pasitelkti ir šios srities profesionalus.	ignoravimas pateisinant tuo, kad tai tik bandomoji sistemą ir ji daugiau nenaudojama. Arba sistemų administratoriaus pasiteisinimas, kad negalima ištaisyti tam tikro serverio pažeidžiamumų dėl senos duomenų bazės versijos, bet ar yra įgyvendintos kokios nors kontrolės priemonės, kurios apsaugo nuo šio pažeidžiamumo?	atliks pažeidžiamumų nustatymo testą. Tais atvejais kai kompanijos vadovybė nenori pripažinti grėsmių ir pažeidžiamumų, reikia stengtis įtikinti juos, kad analizė daroma dėl jų, kad svarbiausia geri lūkesčiai. Tokiais atvejais svarbu pasitikėjimas ir supratimas, o ne gerai išaiškint techninė pusė.
3. Kontrolė ir reagavimas į incidentus	Po to kai 1-2 etape surinkome visas reikalingas žinias, metas sukurti giluminę saugumo strategiją (angl. *defence-in-depth*), kurioje būtų prevencinio, taisomojo ir kompensacinio valdymo sluoksniai. Neatsiejamas nuo strategijos ir veiklos tęstinumo plano yra reagavimo į kibernetinius incidentus planas. Šiame plane turi būti aptariamas incidentų identifikavimas, suvaldymas, sprendimas ir atsistatymas po jų.	Šiame etape kylančios klaidos susiję su valdymu, ištekliais ir įgūdžių stoka. Dažniausiai daroma klaida kai Informacinių technologijų (toliau – IT) specialistams leidžiama parinkti ir įdiegti kontrolės priemones. To nereiktų daryti, nes kibernetinės saugos tikslas yra rizikų suvaldymas, o IT tikslas yra vertės sukūrimas. Kita dažnai daroma klaida parenkama netinkamos arba per didelis kiekis kontrolės priemonių. Arba parenkamos tinkamos kontrolės priemonės, bet jos sudiegiamos netinkamai, pvz. įsigyjamas brangus SIEM sprendimas, bet nesuplanuojamos lėšos pilnam jo sukonfigūravimui ir pritaikymui. Blogiausia galima klaida incidentų valdymo plano nebuvimas arba jo sukūrimas tik „ant popieriaus“, nedarant testų ir patikrinimų..	Visų pirma reikia teisingai sudėstyti atsakomybes – kokios yra galimos rolės ir kas už ką atsako. Vadovybė turi nepamiršti, kad IT kuria vertę, o kibernetinė sauga tą vertę saugo. Kai atsakomybės yra tinkamai nustatytos galima susikoncentruoti į labiau techninius dalykus, strategijos kūrimą, diegimą ir optimizavimą, bei realaus reagavimo į incidentus plano sudarymą. Nereikia bandyti visų šių veiksmų atlikti pačiai organizacijai, būtinai reikia pritraukti kibernetinės saugos profesionalus iš išorės, kurie dirbtų kartu su organizacijos darbuotojais. Šio etapo tikslas yra sukurti tinkamą, ištestuotą ir „gyvą“ incidentų valdymo planą, kuris užtikrintų, kad tuo atveju kai įvyks įsibrovimas jūsų organizacija būtų pasiruošusi.
4. Žmonių kibernetinė sauga	Net jei sėkmingai įvykdėme visus etapus iki šio reikia, nepamirši, kad pagrindinis pažeidžiamumo taškas yra žmonės. Šiame etape reikia kuo geriau iškomunikuoti, kad kibernetinė sauga turi būti diegiama visuose organizacijos sluoksniuose.	Didžiausias pažeidžiamumas – žmonės. Vadovai gali ignoruoti kibernetinę saugą ir skatinti darbuotojus slėpti šį faktą. Darbuotojai gali pažeidinėti nustatytą saugos politiką. Egoistiški IT ar saugos darbuotojai.	Labai svarbu gilus įsitraukimas. Užmezgate gilų ryšį – ugdote pasitikėjimą, užmezgate komunikacijos kanalus ir kuriate ilgalaikį pagarbos ryšį. Bendravime reikia naudoti psichologinį, sociologinį ir antropologinį metodus.

Šaltinis: parengta pagal Mochovitis C. straipsnį „Why do cyber security programmes fail?“, 2019

2. PORTALŲ APSAUGOS KIBERNETINĖS SAUGOS VALDYMO PRIEMONĖMIS PASAULINĖS PATIRTIES ANALIZĖ

2.1. Kibernetinės saugos valdymo priemonių taikymas Jungtinėse Amerikos valstijose

2.1.1. Kibernetinės saugos vystymasis Jungtinėse Amerikos Valstijose

Per paskutinius trisdešimt metų technologijos išaugo eksponentiškai. Mes kasdiena jaučiame technologijų teikiamus privalumus ir didiname savo priklausomybę nuo technologijų. Žiniatinklio aplikacijos, dronai, mobiliosios aplikacijos, industrinis automatizavimas, mašininio mokymosi aplikacijos ir kitos technologijos pakeitė mūsų gyvenimu. Bet šios technologijos atneša milžiniškas grėsmes. Dėl to Jungtinių Amerikos Valstijų (toliau – JAV) vyriausybė stiprinta savo kibernetinės saugos įstatymų bazę (Nelson O., 2019). Yra trys pagrindinės sritys į kurias koncentruojamasi: kibernetiniai nusikaltimai – pavieniai ar daugybiniai puolimai nukreipti prieš sistemas, siekiant finansinės naudos ar su tikslu sutrikdyti jų veiklą; kibernetinės atakos – dažniausiai susiję su politiškai motyvuotu informacijos rinkimu; kibernetinis terorizmas – apima veiksmus, atliekamus su tikslu pakenkti elektroninėms sistemoms ir sukelti paniką ar baimę.

JAV įstatymuose pirmosios užuominos į kibernetinę saugą atsirado 1987 metais patvirtinus Kompiuterių saugumo įstatymą (angl. *H.R.145 - Computer Security Act of 1987*). Šiame įstatyme nurodoma standartizuoti federalines kompiuterių sistemas, sukuriamos Kompiuterinių sistemų ir Privatumo patariamoji tarybos, nurodoma visoms agentūroms vykdyti kasmetinius darbuotojų kompiuterių saugos mokymus, bei visoms Federaline kompiuterių sistema besinaudojančioms agentūroms nurodoma sudaryti neskelbtinos informacijos saugumo ir privatumo planus.

Kaip rašoma Charlet K. parengtoje analizėje „Supratimas apie federalinį kibernetinį saugumą“ (2018) kongresas vaidina lemiamą vaidmenį federalinio kibernetinio saugumo srityje. Jis priima pagrindinius įstatymus susijusius su kibernetine sauga. Yra daugybė su kibernetine sauga susijusių įstatymų, bet esminiais galima laikyti šiuos:

- 1996 Clinger-Cohen įstatymas, taip pat žinomas kaip Informacijos technologijų valdymo reformos įstatymas (angl. *ITMRA*), pakeitė tai kaip federalinė valdžia valdė IT pastaruosius 20 metų. Įstatymas leido agentūroms įsigyti IT resursus savarankiškiau, taip pat įpareigojo agentūras paskirti vyriausiąjį informacijos pareigūną (angl. *CIO*).
- 2002 Federalinis informacijos saugumo valdymo pamatinis įstatymas (angl. *FISMA*), kuris apibrėžia federalinio kibernetinio saugumo roles ir atsakomybes, bei nurodo agentūroms parengti ir įgyvendinti savo informacijos ir informacinių sistemų apsaugojimo programas.

- 2003 Nacionalinė saugios kibernetinės erdvės strategija, pirmasis tokio tipo dokumentas JAV įstatyminėje bazėje – dokumento tikslas įtraukti ir paskatinti amerikiečius apsaugoti kibernetinės erdvės dalis, kurios jiems priklauso ir kurias jie valdo, kontroliuoja ar su kuriomis sąveikauja.
- 2014 Federalinės informacijos saugumo modernizavimo įstatymas, atnaujinęs 2002 įstatymą, aprašant Valstybės saugumo departamento (angl. *DHS*) ir Valdymo ir biudžeto tarnybos (angl. OMB) galias ir sąsajas su federalinių agentūrų informacijos saugumu.
- 2014 Nacionalinis kibernetinio saugumo įstatymas formalizavo Nacionalinio kibernetinės saugos ir komunikacijų integravimo centrą DHS (angl. *NCCIC*) ir paskatino kibernetinės saugos informacijos mainus tarp federalinių ir ne federalinių subjektų
- 2014 Federalinių informacinių technologijų įsigijimo reformos įstatymas (angl. *FITARA*) išplėtė CIO pareigūnų galias ir palietė tokius klausimus kaip IT investicijų rizikų valdymas, duomenų centrų konsolidavimas, IT mokymai ir įsigijimai/viešieji pirkimai.
- 2015 Kibernetinės saugos įstatymas paskatino dalijimąsi informacija tarp federalinės vyriausybės ir privačių įmonių per DHS. Taip pat nurodė visoms civilinėms agentūroms įgyvendinti EINSTEIN-DHS programą, skirtą aptikti ir užkirsti kelią federalinių tinklų grėsmėms

Anot Kurose M. straipsnio (2019) Per paskutinius dešimt metų, kartu su kibernetinių atakų didėjimu, kibernetinę saugą reglamentuojantys įstatymai vis dažniau atsiranda JAV vyriausybės akiratyje. Vien per 2018 metus, bent 35 valstijos, taip pat ir Vašingtono pateikė 235 įstatymų projektus ir nutarimus susijusius su kibernetine sauga: gerinantys vyriausybės saugumo praktikas, skiriantys lėšas kibernetinio saugumo programoms ir iniciatyvoms, apribojantys jautrios informacijos viešinimą, skatinantys darbo jėgą, mokymą ir ekonominę plėtrą.

Kalbant apie kibernetinių nusikaltimų ištyrimo lygį JAV, 2018 metai tam buvo palankūs. Kibernetinės saugos padalinys prie Saugumo ir keitimo komisijos (angl. *Cyber Unit at the Securities and Exchange Commission*) informavo nagrinėjanti 20 pavienių bylų ir atliekanti 225 besitęsiančių tyrimų susijusių su kibernetine sauga. Vienas iš labiausiai žinomų atvejų 2018 metais buvo šio saugos padalinio iškelta byla kompanijai Altaba (buvusi Yahoo Inc) ir pateiktas ieškinys 35 milijonams dolerių už tai, kad kompanija netinkamai ir vėluodama 2 metais paskelbė apie įsibrovimą į jų valdomą interneto puslapį ir šimtų milijonų jos naudotojų paskyrų duomenų vagystę (Craig A., 2019).

Kovodama su didėjančiu kibernetinių incidentų ir pažeidimų kiekiu JAV vyriausybė kas metai didina biudžeto dalį skiriamą kibernetinės saugos sričiai. 2018 metais tam buvo skirta 14,978 milijardų dolerių iš jų daugiau nei pusė sumos Gynybos departamentui (angl. *DOD*), 2019 metais 16,645 milijardų dolerių (DOD – 8,732 milijardų) ir 2020 metais – 17,435 milijardų dolerių (DOD – 9,643 milijardų).

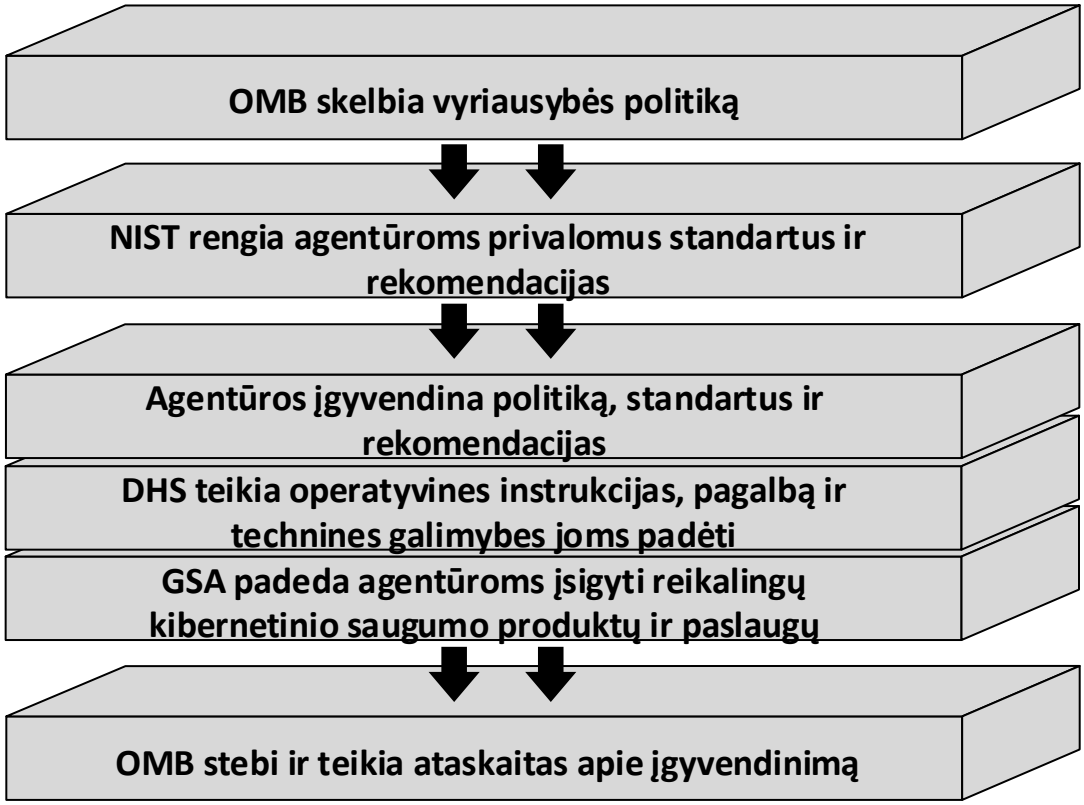
Antras pagal gaunamą kibernetinio saugos biudžeto dydį yra JAV Valstybės saugumo departamentas, kuriam 2018-2020 fiskalinių metų biudžete buvo numatyta po maždaug 1,9 milijardų dolerių (Cybersecurity funding, 2019).

2.1.2. Kibernetinės saugos teisinis reglamentavimas Jungtinėse Amerikos Valstijose

Jungtinėse Amerikos Valstijose kibernetinė sauga yra reglamentuota keliais pagrindiniais įstatymais ir yra paskirtos atsakingos institucijos tų įstatymų įgyvendinimui. Pagal įstatymus nustatyta, kad kiekviena federalinė agentūra yra pati atsakinga už savo kibernetinį saugumą. Tai kaip kokybiškai kiekviena agentūra rūpinasi savo kibernetine sauga kontroliuoja keturios pagrindinės institucijos (Charlet K., 2018):

- Valdymo ir biudžeto tarnyba (angl. OMB) – rengia informacijos saugumo politikas, principus ir gaires, bei prižiūri jų įgyvendinimą
- Nacionalinis standartų ir technologijų institutas (angl. *NIST*) – kuria standartus ir gaires nenacionalinėms federalinėms informacinėms sistemoms.
- Valstybės saugumo departamentas (angl. *DHS*) – užima lyderio ir operacijų valdymo rolę, teikia pagalba federalinėms civilinėms agentūroms atliekant jų kibernetinės saugos rizikų valdymą
- Bendrųjų paslaugų administravimo agentūra (angl. *GSA*) – teikia palaikymą federalinėms agentūroms parinkdama ir pateikdama tinkamus kibernetinio saugumo produktus ir paslaugas

Be išvardintų institucijų federalinėms agentūroms kritinę pagalba taip pat teikia keturios kitos įstaigos ir departamentai. Žvalgybos bendruomenės (IC) teikiama informacija yra gyvybiškai svarbi padedant civiliniams federalinės vyriausybės elementams nustatyti, blokuoti ir reaguoti į žinomas kibernetines grėsmes. Gynybos departamentas (angl. *DOD*) ir Nacionalinio saugumo agentūra (angl. *NSA*) paprašius gali padėti kitoms agentūroms gynybos pajėgumais ir techninėmis žiniomis. Po įvykusio įsilaužimo ar kibernetinių atakų prieš federalines informacines sistemas Federalinio tyrimų biuras (angl. *FBI*) vadovauja su tuo susijusiam federaliniam tyrimui. Visi šie subjektai sąveikauja kompleksiškai ir federaliniu būdu, pasiskirstydami vaidmenis ir atsakomybes. Supaprastintas jų sąveikos modelis pavaizduotas 5 paveikslėlyje.



Šaltinis: Charlet K., 2018, p. 10

5 pav. **JAV už kibernetinę saugą atsakingų tarnybų sąveika**

Jungtinės Amerikos Valstijos 2003 metais išleido savo pirmąja kibernetinės saugos strategiją, kurios poreikį suformavo per paskutinius metus internetinėje erdvėja stipriai išaugusios kibernetinės saugos grėsmės. 2018 metais, praėjus 15 metų nuo pirmosios strategijos išleidimo buvo išleista atnaujinta kibernetinės saugos strategija. Naujasis dokumentas glaudžiau integruojasi su kitomis strategijomis, tame tarpe ir JAV Nacionaline Saugumo Strategija išleista 2017 metais.

JAV kibernetinės strategijos vizija ir pagrindiniai iššūkiai. Nacionalinė kibernetinės saugos strategijos vizija – užtikrinti, kad Amerikos žmonės ir toliau naudotųsi saugios elektroninės erdvės pranašumais, kurie atspindi Amerikos principus, saugo Amerikos saugumą ir skatina Amerikos klestėjimą. Amerikiečiai tiki , kad interneto augimas kartu atneš visuotinius laisvos saviraiškos siekius ir asmens laisvę visame pasaulyje. Amerikiečiai naudojosi galimybėmis plėsti bendradarbiavimą, komerciją ir nemokamą galimybę keistis idėjomis. Tačiau Amerikos priešininkai pasirinko kitą kelią ir naudojosi interneto galimybės tuo pačiu metu apribodami savo piliečių teises jame. Jie slepiasi už savo suvereniteto, bet tuo pačiu įsitraukia į kenksminą ekonominį šnipinėjimą ir kenkėjiškas kibernetines veiklas, sukeldami didelius ekonominius sutrikdymus. Tokiais priešininkais strategijoje įvardijami Rusija, Kinija ir Šiaurės Korėją. Kaip dar vienas iššūkis įvardijamas privačių ir valstybės subjektų kova su kenkėjiškomis atakomis ir kenksminga veikla internete. Visoje JAV subjektai susidūrė su kibernetinio saugumo iššūkiais kaip efektyviai identifikuoti , apsaugoti ir užtikrinti jų tinklų, sistemų, funkcijų ir duomenų saugumą.

JAV kibernetinės saugos strategija yra sudaryta iš keturių pagrindinių skyrių:

1. Apsaugoti Amerikos žmones, tėvynę ir Amerikietišką gyvenimo būdą. Šiame skyriuje iškeliami tikslai apsaugoti tėvynę saugant kompiuterinius tinklus, sistemas, funkcijas ir duomenis.
2. Skatinti Amerikos gerovę. Šiame skyriuje skatinama puoselėti saugią, klestinčią skaitmeninę ekonomiką ir stiprinti namų ūkių inovacijas,
3. Išsaugoti taiką ir saugumą per Jėgą. Stiprinti Jungtinių Amerikos Valstijų gebėjimus kartu su sąjungininkais ir partneriais ir, jeigu reikia, nubausti tuos, kurie elektroniniai įrankiai naudojasi kenkėjiškais tikslais.
4. Plėsti Amerikietišką įtaką užsienyje. Skatinama išplėsti pagrindinius atviro, patikimo ir saugaus interneto principus.

Kiekvienoje iš strategijos dalių yra išskiriamos kelios svarbios sritys susijusios su portalų apsauga. Toliau pateikiamas sutrumpintas dalies jų apibūdinimas:

- **Saugus Federalinis tinklas ir informacija.** Užduotis: apsaugoti federalines informacines sistemas ir kompiuterinius tinklus paskirstant užduotis departamentams ir agentūroms, tuo pačiu nustatant standartą efektyviam kibernetinio saugumo rizikų valdymui. Iškeliami tikslai: toliau tęsti federalinės civilinės kibernetinės saugos valdymo ir priežiūros centralizavimą; paskirstyti rizikos valdymo ir informacijos technologijų veiklą.
- **Saugi kritinė infrastruktūra.** Užduotis: apsaugoti kritinę infrastruktūra ir valdyti jos rizikas privačiame sektoriuje ir federalinėje valdžioje. Iškeliami tikslai: Patikslinti roles ir atsakomybes; prioretizuoti veiksmus priklausomai nuo nustatytų nacionalinių rizikų; pasitelkti informacijos ir komunikacijos technologijų tiekėjus kaip kibernetinės saugos įgalintojus; skatinti investicijas į kibernetinę saugą.
- **Kova su kibernetiniai nusikaltimais ir pranešimo apie incidentus tobulinimas.** Užduotis: Teisėsauga turi bendradarbiauti su privačiomis įmonėmis ir tokiu būtu išspręsti iššūkius, kuriuos kelia technologinės kliūtys. Iškeliami tikslai: efektyvinti pranešimus apie kibernetinius incidentus ir gerinti reakcijas į juos; modernizuoti elektroninį stebėjimą ir kompiuterinių nusikaltimų įstatyminę bazę.
- **Gyvos ir atsparios skaitmeninės ekonomikos puoselėjimas.** Užduotis: modeliuoti ir skatinti standartų, kurie apsaugo ekonomiką ir sustiprina rinkos gyvybingumą, kūrimą. Iškeliami tikslai: paskatinti adaptyvios ir saugios technologijų rinkos atsiradimą; skatinti viso ciklo kibernetinę saugą.
- **Kibernetinio saugumo profesionalios darbo jėgos sukūrimas.** Užduotis: sukurti didelį Amerikos talentų fondą, pritraukiant geriausius ir ryškiausius užsieniečius

specialistus. Iškeliami tikslai: sukurti ir išlaikyti talentų tiekimo grandinę; išplėsti perkvalifikavimo ir mokymo galimybes JAV darbuotojams; sustiprinti federalinę kibernetinės saugos darbo jėgą; naudoti vykdančiąją valdžią talentingų darbuotojų apdovanojimui.

- **Kibernetinio stabilumo sustiprinimas per taisykles ir atsakinga valstijų elgsena.** Užduotis: JAV skatins atsakingos valstijos elgesio elektroninėje erdvėje sistemą. Iškeliami tikslai: skatinti visuotinį kibernetinių normų laikymąsi.
- **Nepriimtino elgesio elektroninėje erdvėja reglamentavimas.** Užduotis: užtikrinti pasekmes tiems, kas neatsakinga veikla padaro žalos JAV ir partneriams. Iškeliami tikslai: vadovautis objektyviomis žiniomis; nustatyti atsakomybes.
- **Skatinti atvirą, sąveikų, patikimą ir saugų internetą.** Užduotis: saugoti ir skatinti atvirą sąveikų, patikimą ir saugų internetą. Iškeliami tikslai: saugoti ir skatinti laisvą internetą; dirbti su bendraminčiais iš kitų šalių, industrijų, akademinės bendruomenės ir visuomenės.
- **Sukurti tarptautinius kibernetinius pajėgumus.** Užduotis: sustiprinti kibernetinių gebėjimo stiprinimo pastangas.

Be kibernetinės saugos strategijos JAV turi kelis kitus įstatymus nustatančius atsakomybes agentūroms ir departamentams už savo valdomus tinklus ir informacines sistemas. Vienas iš tokių yra 2017 metų gegužę patvirtintas vykdomasis įsakymas 13800 (angl. *Executive Order 13800*), jo pagrindinis tikslas Stiprinti kibernetinės saugos infrastruktūra federaliniuose tinkluose ir kritinėje infrastruktūroje. Portalų apsaugai svarbiausi skyriai: Kibernetinė federalinių tinklų sauga, Kritinės infrastruktūros kibernetinė sauga ir Tautos kibernetinis saugumas.

Kibernetinė federalinių tinklų sauga. Šiame skyriuje sakoma, kad nuo šiol vykdomųjų departamentų ir agentūrų vadovai yra tiesiogiai atsakingi už kibernetinio saugumo rizikos valdymo savo įstaigose, šią nuostatą taikant ir apimant kitus tai įstaigai pavaldžius padalinius. Agentūroms nurodoma laikytis šių principų:

- Agentūros privalo naudotis NIST sukurtą Kritinės infrastruktūros kibernetinio saugumo gerinimo sistemą (angl. *framework*), agentūros kibernetinio saugumo grėsmių suvaldymui.
- Agentūrų vadovai atlikdami IT pirkimus turi rinktis bendro naudojimo IT paslaugas (kiek leidžia įstatymai), įskaitant elektroninio pašto, debesijos ir elektroninio saugumo paslaugas.
- Kiekvienos agentūros vadovas privalo sudaryti ir DHS pateikti rizikų valdymo planą: plane turi matytis strateginės su kibernetine sauga susijusios biudžeto išlaidos ir visos prisiimto rizikos įskaitant nesutvarkytus informacinių sistemų pažeidžiamumus

Kibernetinės kritinės infrastruktūros sauga. Šis skyrius nustato kad vykdomoji valdžia remdamasi savo įgaliojimais ir galimybėmis privalo remti valstybės ypatingos svarbos infrastruktūros

objektų savininkus ir operatorius padėdama suvaldyti kibernetinės saugos rizikas. Šiame punkte taip pat nurodoma identifikuoti valdžios institucijas ir galimybes, kurias agentūros galėtų pasitelkti užtikrindamos ypatingos svarbos infrastruktūros kibernetinę saugą.

Tautos kibernetinė sauga. Siekiant užtikrinti, kad internetas išliktų vertingas ateities kartoms, vykdomosios valdžios politika turi skatinti atvirą, sąveikų, patikimą ir saugų internetą, kuris didina efektyvumą, inovacijas, komunikaciją ir ekonominę gerovę, gerbiant privatumą ir saugant nuo trikdžių, sukčiavimo ir vagysčių. Be to, JAV skatins kibernetinio saugumo ir susijusiose srityse kvalifikuotos darbo jėgos augimą ir išlaikymą, kaip pagrindą jų tikslams elektroninėje erdvėj pasiekti.

Be naujai išleistų įstatymų ir strategijos, vis dar galioja 2002 metais išleistas Valstybės saugumo įstatymas (angl. *The Homeland Security Act*) ir Federalinis informacijos saugumo valdymo pamatinis įstatymas (angl. FISMA), pirmajame agentūroms ir departamentams nurodoma atitikti antrojo reikalavimus. Kaip rašoma Nelson O. straipsnyje (2019) Nacionalinis standartų ir technologijų institutas pateikia tokius devynis žingsnius, kad įstaiga atitiktų FISMA įstatymo reikalavimus:

1. Reikia suklasifikuoti saugotiną informaciją
2. Pasirinkti minimalius pradinius kibernetinės saugos valdiklius
3. Patikslinti parinktas kontrolės priemones atliekant rizikų įvertinimo procedūrą
4. Dokumentuoti galutinai parinktas kibernetinės saugos valdymo priemones sistemos saugumo plane
5. Įdiegti kontrolės priemones atitinkamose informacinėse sistemose
6. Patikrinti įdiegtų saugumo kontrolės priemonių veiksmingumą
7. Nustatyti institucijos lygmens rizikas misijai ar verslo prielaidoms
8. Leisti tvarkyti informacinę sistemą
9. Nuolat stebėti kibernetinės saugos kontrolės priemonių efektyvumą

Be anksčiau paminėtų įstatymų, JAV departamentų ir agentūrų internetinių portalų ir svetainių saugą reglamentuoja (Digital.gov website checklist, 2020):

- Saugių jungčių reikalavimo federalinėse svetainėse ir žiniatinklio tarnybose politika (OMB M-15-13)
- 2014 metų Federalinis informacijos saugumo modernizavimo įstatymas (FISMA, Public Law 113-283)
- NIST viešųjų žiniatinklio tarnybinių stočių saugos gairės (2007)
- Federalinio informacijos saugumo valdymo įstatymo ataskaitų teikimo instrukcija (OMB M-04-15)

JAV turi galiojančius kelis įstatymus susijusius su atsakingų pažeidžiamų atskleidimu: Elektroninių galimybių stiprinimas panaudojant technologijų pažeidžiamumas įstatymas (H.R.7327) ir

Nulaužk savo valstijos departamentą įstatymas (H.R.5433). Kaip rašoma Tamošauskas Ž. R. analizėje (2019) šie JAV įstatymai apibrėžia premijų už spragų aptikimą iniciatyvą:

- Asmenims, organizacijoms arba įmonėms suteikiama laikina galimybė JAV vidaus saugumo departamento atitinkamose informacinėse sistemose identifikuoti spragas ir apie jas pranešti
- Tinkami asmenys, organizacijos arba įmonės gauna kompensaciją už tokius pranešimus

Taip pat įstatymuose reglamentuojama, kad įstatymas galioja asmenims ar organizacijoms pranešančioms apie saugumo spragas, įstatymas nustato atitinkamas departamento informacines sistemas, kuriose asmenims, organizacijoms arba įmonėms leidžiama ieškoti spragų.

JAV kibernetinės saugos ir informacijos saugos įstatyminė bazė yra gana plati ir paini, kartais ta pati informacija yra kelių skirtingų institucijų išleistuose įstatymuose ar tvarkose. Susiorientuoti ir nepasiklysti JAV įstatymų vingiuose padės Gynybos departamento Informacijos analizės centro (*DOD CSIAC, 2020*) parengta Kibernetinio saugumo diagrama (žr. 1 Priedas). Kadangi diagrama labiau orientuota į gynybos ministerijos padalinius, tai joje nėra visų civilinėms agentūroms skirtų įstatymų.

2.1.3. Dabartinė kibernetinės saugos situacija JAV

Po ankstesniame skyriuje minėtų įstatymų ir kibernetinės saugos strategijos išleidimo buvo atliktos kelios federalinių departamentų ir agentūrų rizikų analizės ir įstatymų laikymosi analizės. Šių analizių rezultatai parodė, kad ne visose srityse yra laikomasi teisinio kibernetinės saugos reglamentavimo.

Paties vykdomojo įsakymo 13800 įžangoje pažymima, kad per ilgai buvo nekreipiamas dėmesys į atgyvenusias ir sunkiai prižiūrimas, bei sunkiai apginamas IT sistemas. Taip pat atkreipiamas dėmesys į tai, kad didžiausi saugumo iššūkiai su kuriais susiduria departamentai ir agentūros yra operacinės sistemos ir aparatinė įranga, kurie nebeturi palaikymo ir gamintojo palaikymo gyvavimo ciklas yra pasibaigęs arba nenorą diegti išleistas šių sistemų ir įrangos pataisas. Kaip rašoma rizikos analizės ataskaitoje (Federal Cybersecurity Risk Determination Report and Action Plan, 2018), parengtoje pagal vykdomojo įstatymo 13800 nurodymus, išskirtinos tokios problemos susijusios su kibernetinės saugos įstatymų įgyvendinimu federaliniuose departamentuose ir agentūrose:

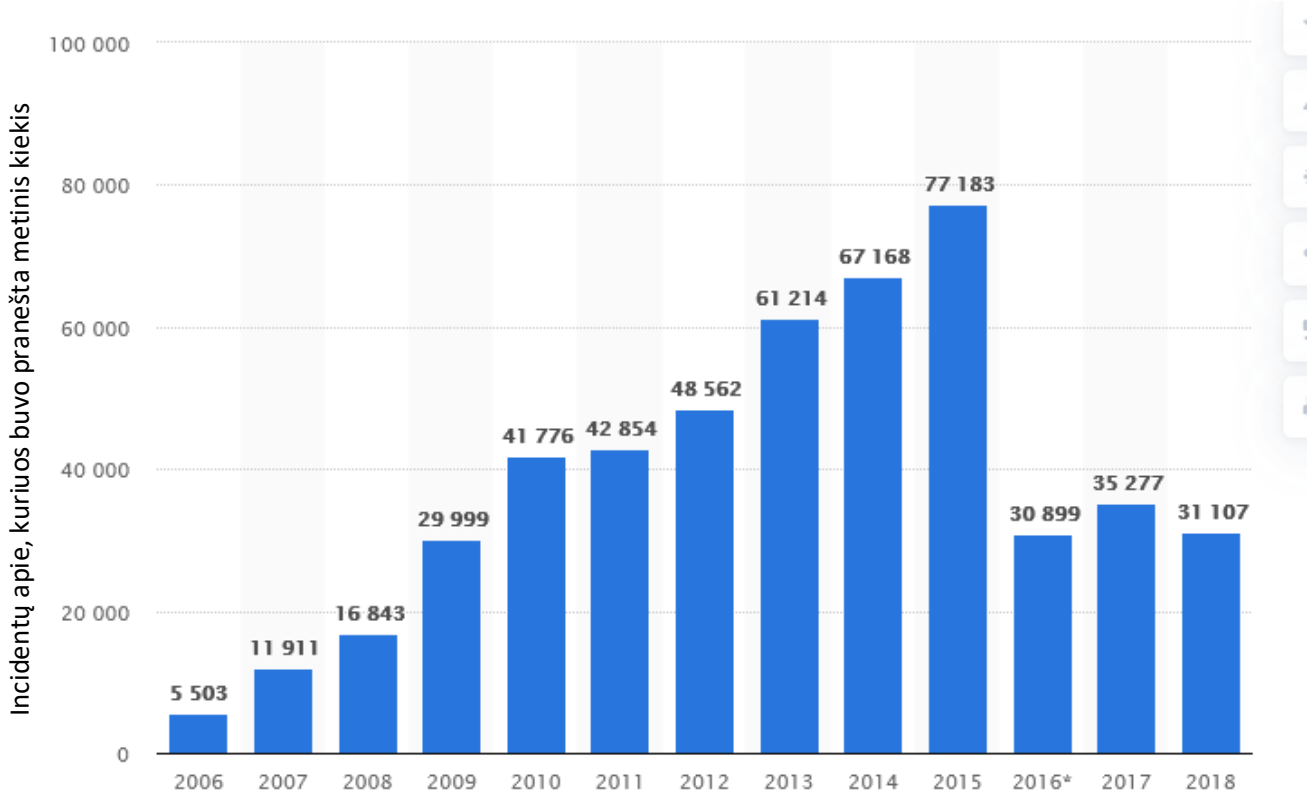
- Agentūros nesupranta dabartinės kibernetinių grėsmių aplinkos ir neturi reikiamų resursų kovai su jomis. 38% praneštų federalinių kibernetinių incidentų neturi aiškiai nustatyto atakos vektoriaus, kas rodo ribotą situacijos suvokimą. Tik 59% agentūrų informavo turinčios nustatytus procesus komunikavimui su padaliniais apie kibernetines rizikas.
- Agentūros neturi standartizuotų kibernetinio saugumo procesų ir IT galimybių, o tai daro įtaką jų gebėjimui efektyviai įgyti matyti jiems kylančias grėsmės ir efektyviai kovoti su jomis. Gerai, tai kad net 93% agentūrų darbuotojų naudoja asmeninio identifikavimo

korteles prisijungimui prie darbo vietos. Tik 49% agentūrų pažymėjo turintys galimybę nustatyti ir leisti arba neleisti naudoti programinę įrangą ant galinių įrenginių.

- Agentūros negeba stebėti kas vyksta joms priklausančiuose kompiuteriniuose tinkluose, joms ypač trūksta įrankių duomenų nutekėjimui nustatyti. Tik 27% agentūrų pažymėjo, kad jie turi galimybę nustatyti ir ištirti bandymus prieiti prie didelės apimties duomenų ir dar mažiau agentūrų pažymėjo, kad atlieka šiuos patikrinimus kas metai. Taip pat matomas nesubrendimas incidentų valdyme, nes tik 52% agentūrų turi patvirtintus incidentų valdymo planus ir tik 17% agentūrų iš tikro analizuojančių reagavimo į incidentus procesą. Daugelis agentūrų neturi sukurtų Saugumo operacijų centrų (angl. *SOC*), arba turi kelis tarpusavyje nekomunikuojančius tokius centrus.
- Agentūroms trūksta standartizuotų ir visą įstaigą apimančių procesų, skirtų valdyti kibernetinio saugumo rizikas.

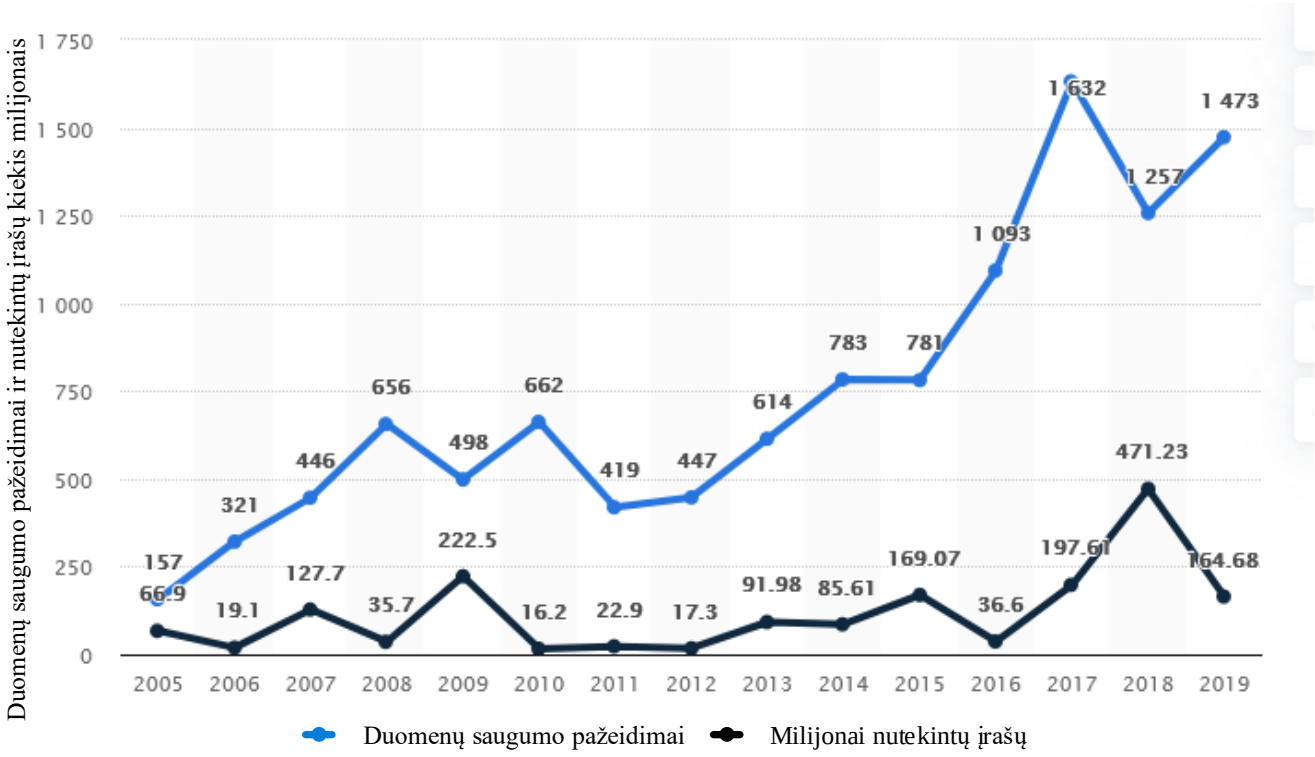
Ataskaitoje taip pat išskiriamos dvi reikšmingiausios rizikos sritys: senųjų informacinių technologijų (angl. *legacy IT*), kurias sunku ir brangu prižiūrėti ir apsaugoti, gausa, bei patyrusių ir pajėgių kibernetinio saugumo darbuotojų trūkumas. Anot Charlet K. (2018) nemaža dalis federalinės valdžios remiasi senomis IT sistemomis, kurias sunku apsaugoti ir jų priežiūra kainuoja brangiai. Charlet K. (2018) ataskaitoje rašoma, kad Vyriausybės atsakomybės tarnybos (angl. *GAO*) teikiamoje informacijoje matomos tokios dar JAV įstaigose naudojamos technologijos: senos programavimo kalbos (pvz. COBOL), senos IT techninės dalys (pvz. 8 colių magnetiniai diskeliai), nebepalaikoma techninė ir programinė įranga (pvz. Microsoft operacinės sistemos iš 1980-1990 metų). Dešimt seniausių dar naudojamų IT sprendimų amžius buvo nuo 39 iki 56 metų. Tokių sistemų išlaikymas kainuoja daug brangiau nei kainuotų naujų tokių sistemų priežiūra. Iš 80 milijardų dolerių per metu išleidžiamų federalinės valdžios, net 77% buvo panaudota senų IT sistemų priežiūrai.

Remiantis Statista.com svetainėje pateikiama kibernetinių incidentų statistika (pav. 6), federalinės agentūros per 2018 metus informavo apie 31 107 incidentus, palyginus su ankstesniais metais šis skaičius išliko panašus (atitinkamai 2017 – 35 277 ir 2016 – 30 899), tik matėsi stiprus sumažėjimas palyginus su 2015 metais (77 183 incidentai), nes nuo 2016 metų keitėsi incidentų apie kuriuos privaloma pranešti sąrašas (nebereikia pranešti apie prievadų skenavimus, nesėkmingus bandymus prisijungti ir pan.). Statista.com puslapyje tai pat pateikiama informacija apie JAV per metus įvykusių duomenų saugumo pažeidimų ir nutekintų įrašų kiekius, 2019 metais įvyko 1473 įsibrovimai ir buvo nutekinta 164,68 milijonai įrašų, tuo tarpu 2018 metais – 1257 įsibrovimai ir 471, 23 milijonai nutekintų įrašų (pav. 7).



Šaltinis: Statista.com, 2020

6 pav. **Federalinių agentūrų pateikiama kibernetinių incidentų statistika 2006-2018 metais**



Šaltinis: Statista.com, 2020

7 pav. **JAV 2005-2019 metais įvykusių duomenų saugumo pažeidimų ir nutekintų įrašų kiekiai**

2.2. Kibernetinės saugos valdymo priemonių taikymas Nyderlanduose

2.2.1. Kibernetinės saugos vystymasis Nyderlanduose

Nyderlandai viena iš pirmųjų šalių kuriose pradėjo veikti internetas arba jo pirminiai variantai. 1982 metais Nyderlandai prisijungė prie USENET tinklo (EUnet). Nyderlandų nacionalinis matematikos ir kompiuterių mokslų tyrimo institutas (dutch CWI) pamatė naujai gimstančiame tinkle didelį potencialą ir pradėjo kuri Nyderlandų kompiuterinį tinklą, kuris išsivystė į NLnet. Nors nebuvo tarptautinių interneto standartų, bet 1988 metais Nyderlandai kabeliu susijungė su Jungtinėmis Amerikos Valstijom. Nyderlandai pamatė strateginę vertę tapti interneto vartais į Europą ir 1990 metais įkūrė Amsterdamo interneto mainų mazgą (AMS-IX) kaip ne pelno siekiančią, neutralią ir nepriklausomą peering'o organizaciją (Hathaway M., Spidalieri F., 2017).

Nyderlandai taip anksti prisijungę prie pasaulinio tinklo turi vieną stipriausių ir didžiausio padengimo plačiajuosčio interneto ryšių visoje Europoje. Ši šalis tapo viena iš labiausiai technologiškai pažengusių valstybių ir labiausiai apjungtų kompiuteriniai tinklais. Interneto skvarba Nyderlanduose yra daugiau nei 93%, o daugiau nei 95% namų ūkių yra prijungti prie interneto. Be to Nyderlandai yra internetinės bankininkystės lyderiai, o jos piliečiai ir įmonės sudaro ketvirtą pagal dydį elektroninės prekybos rinką Europoje. Taip pat Nyderlandų informacijos ir komunikacijos technologijų (angl. *ICT*) sektorius generuoja 5% bendrojo vidaus produkto (toliau – BVP) ir šalis yra viena iš didžiausių šių paslaugų eksportuotojų pasaulyje. 2015 metais 22.9 procentai BVP sudarė skaitmeninė ekonomika. Be skaitmeninės ekonomikos Nyderlanduose taip pat yra vienas iš didžiausių uostų – Amsterdamas. Taigi Nyderlandai pripažįsta, kad nepaisant palyginti nedidelio šalies dydžio ir gyventojų skaičiaus šalis tampa vis labiau priklausoma nuo skaitmeninių technologijų ir turi spręsti kibernetinio saugumo klausimus (Hathaway M., Spidalieri F., 2017).

Nyderlandų valdžia suprasdama kiek jų ekonomika yra priklausoma nuo skaitmeninių technologijų ir atkreipdama dėmesį į 2010 metais Europos sąjungos (toliau – ES) paskelbtą „Europos strategija 2020" sudarė ir paskelbė 2011-2015 metų skaitmeninę strategiją (dutch *Digitale Agenda*). Šioje strategijoje nustatyti prioritetai ir konkretūs veiksmai, padedantys skatinti platesnį ICT naudojimą, skatinti nemokamą ir atvirą internetą, ir pašalinti tarptautinės prekybos barjerus internete, kad galėtų sukelti bent 4% ES BVP augimą. Nyderlandų skaitmeninė strategija patvirtinimo, kad yra visos būtinos sąlygos naudotis visomis ICT teikiamomis galimybėmis: saugi ir patikima ICT infrastruktūra; atviras ir prieinamas aukštos spartos internetas, kuriuo pasitiki naudotojai; gyventojai su reikiamai skaitmeninių technologijų naudojimo įgūdžiais. 2016 metais vyriausybė pateikė ataskaitą parlamentui, kurioje buvo teigiama, kad didžioji dalis strateginių tikslų numatytų 2011 metų skaitmeninėje strategijoje yra įgyvendinta ir pasiūlė atnaujintą skaitmeninę strategiją 2016-2017, kurios devizas inovacijos, pasitikėjimas ir pagreitis. 2016-2017 metų skaitmeninės strategijos tikslas buvo toliau skaitmenizuoti

kitus sektorius, pagrinde sveikatos apsaugą ir mobilumą (Hathaway M., Spidalieri F., 2017). 2018 metais buvo pristatyta Nyderlandų skaitmenizavimo strategija (Dutch Digitalisation Strategy, 2018), kuri įvardino tris pagrindiniu tikslus: 1. Būti priešakyje ir naudotis galimybėmis (tapti skaitmenizacijos lyderiu Europoje); 2. Visi prisijungia ir mes dirbame kartu (skaitmenizacija visom amžiaus grupėms, visam gyvenimo cikle); 3. Pasitikėjimas skaitmenine ateitimi – pasaulis skaitmenizuoja, bet bendros vertybės turi išlikti tokios pačios. 2018 metų pabaigoje Atstovų rūmams buvo pristatyta atnaujinta Nyderlandų skaitmenizacijos strategija (Dutch Digitalisation Strategy 2.0, 2018), nes dalis pradiniame strategijos variante iškeltų tikslų buvo pasiekti (pagrinde susiję su mokymo proceso skaitmenizavimu ir aukštos spartos interneto įdiegimu mokyklose). Atnaujintoje Nyderlandų skaitmenizavimo strategijoje be anksčiau minėtų temų, išskiriamos šios: dirbtinis intelektas, duomenų panaudojimas socialinėms problemoms spręsti ir ekonomikos augimui skatinti, skaitmeninė įtrauktis ir įgūdžiai, skaitmeninė vyriausybė, skaitmeniniai ryšiai, skaitmeninis atsparumas.

Anot Hathaway M., Spidalieri F. (2017) Nyderlandai, kaip ir kitos Europos šalys, susiduria su dideliu kibernetinių nusikaltimų kiekiu, industriniu šnipinėjimu, kritinių paslaugų teikimo sutrikdymais ir kita kenksminga veikla. 2010 metais Nyderlandų taikomųjų mokslinių tyrimo organizacija (dutch *Nederlandse Organisatie voor Toegepast Natuurwetenschappelijk Onderzoek, TNO*) pateikė analizę, kurioje buvo rašoma apie Nyderlandų patiriamą kibernetinių nusikaltimų žalą, kuri sudaro 1,5-2% BVP – apie 11 milijardų dolerių. Panašus tyrimas buvo atliktas 2016 metais – rezultatai rodė panašią patiriamą žalą, apie 10 milijardų dolerių. Dėl šių priežasčių Nyderlandų parlamentas pareikalavo sukurti Kibernetinės gynybos strategiją (dutch *Amendment Knops*). Iki dabar Nyderlandų vyriausybė yra parengusi ir paskelbusi tris Kibernetinės gynybos strategijos leidimus:

- 2011 metais paskelbta Nacionalinė kibernetinio saugumo strategija: Pasisekimas per bendradarbiavimą. Už šios strategijos įgyvendinimą buvo atsakingas Nacionalinis saugumo ir kovos su terorizmu koordinatorius (dutch *NCTV*). Strategija paskatino sukurti Nacionalinį kibernetinės saugos centrą (angl. *NCSC*), kuris tarnavo kaip platforma privataus ir viešo sektoriaus bendradarbiavimui kibernetinės saugos srityje. Galiausiai strategijoje buvo rekomenduojama sukurti Nyderlandų kibernetinės saugos tarybą, kuri tarnautų kaip nacionalinis ir strateginis patariamasis organas. Strategija buvo išbandyta, kai 2011 metais Nyderlanduose įvyko didžiausias kibernetinis įsibrovimas į sertifikatų išdavimo paslaugas teikiančią bendrovę DigiNotar.
- 2013 metais Nyderlandai paskelbė savo antrąją kibernetinės saugos strategiją. Nacionalinė kibernetinio saugumo strategija 2: nuo Sąmoningumo iki sugebėjimo, išplėtė šalies požiūri į kibernetinį saugumą, einant toliau už technologijų ir pavienių kibernetinių incidentų. Strategija bandė pasitelkti žmones, sakydama, kad kiekvienas Nyderlandų gyventojas atsakingas už šalies atsparumo užtikrinimą, užkertant kelią grėsmėms ateinančioms per

internetą ir užtikrinant, kad interneto gyvybingumas, patikimumas ir atsparumas bus kaip platforma laisvam prekių, paslaugų, kapitalo ir duomenų judėjimui per sienas.

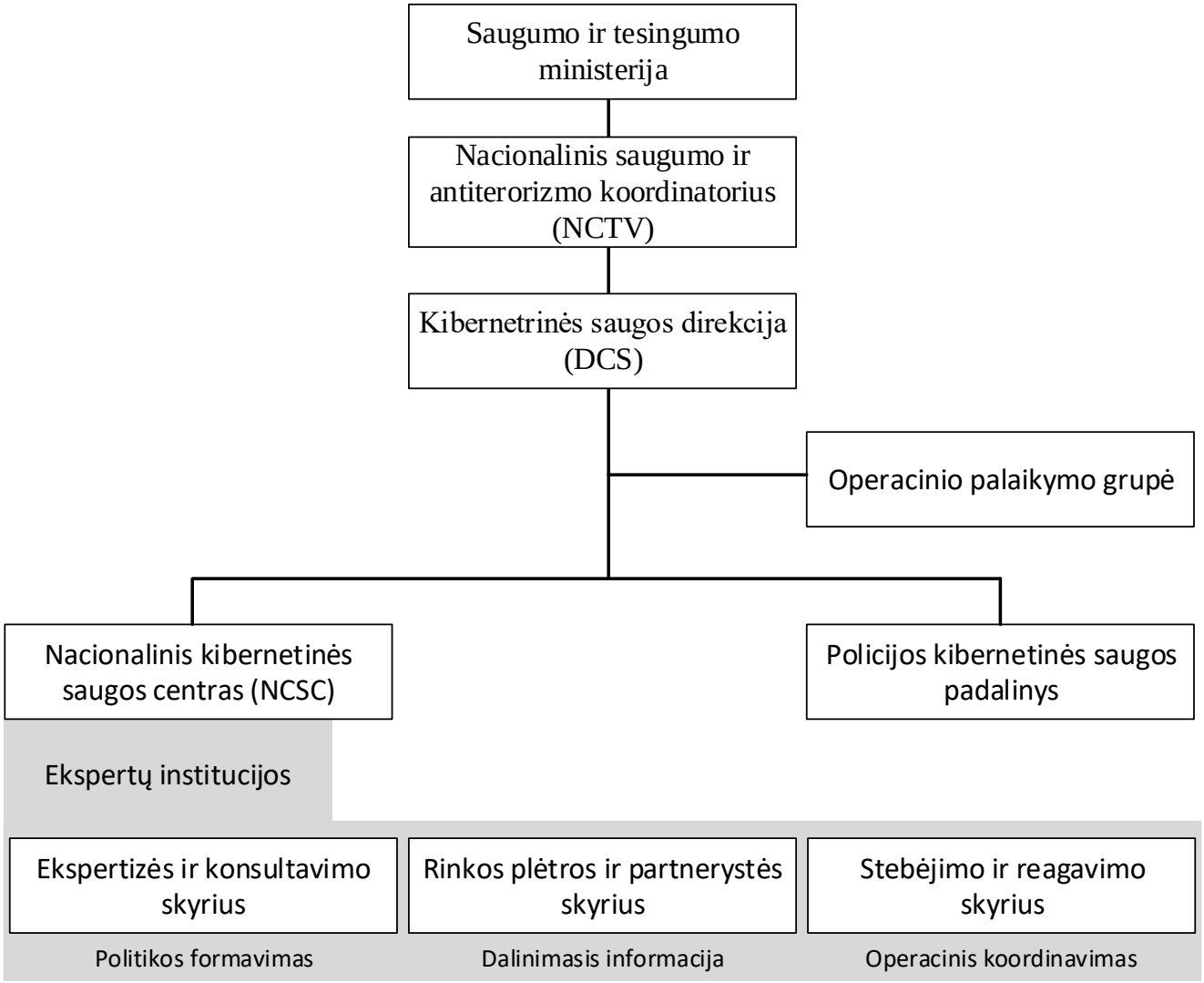
- 2018 metais Nyderlandai publikavo trečiąją strategijos versiją Pavadinta Nacionalinė kibernetinio saugumo dienotvarkė: Kibernetiškai saugūs Nyderlandai. Pagrindinis strategijos tikslas – Nyderlandai geba saugiai išnaudoti ekonomines ir socialines skaitmenizacijos galimybes ir apsaugoti nacionalinį saugumą skaitmeninėje srityje.

Nors Nyderlandai yra parengę nemažai strategijų ir net tris kibernetinės saugos strategijas, tačiau jų kibernetinei saugai skiriamos lėšos sudaro tik nedidelę BVP dalį. 2014 metais kibernetinei saugai jie skyrė tik apie 0,0005% BVP, 2015 – jau apie 0,001%, tuo tarpu 2018 metais skiriama suma padidėjo iki 0,005% nuo BVP. Palyginimui Didžioji Britanija kibernetinei saugai skiria apie 0,01% BVP. 2015 metais Nyderlandų Nacionalinis kibernetinės saugos centras gavo 2.7 milijonus Eur finansavimo, Gynybos ministerija kibernetinei saugai išleido 5 milijonus Eur ir Nacionalinė Nyderlandų policija kovai su kibernetiniais nusikaltimas panaudojo 13,8 milijonų Eur. Žinant, kad Nyderlandai dėl kibernetinių nusikaltimų per metus praranda apie 1.5% BVP ir apie 10 milijardų Eur vertės praradimo dėl kibernetinių rizikų, atrodytų, kad Nyderlandai turėtų daugiau išleisti kibernetinei gynybai (Rademaker M. et al, 2016)

2.2.2. Kibernetinės saugos teisinis reglamentavimas Nyderlanduose

Kibernetinės saugos valdymo funkcija Nyderlanduose yra patikėta Saugumo ir teisingumo ministerijai (angl. *Ministry of Security and Justice*). Šiai ministerijai pavaldus Nacionalinis saugumo ir antiterorizmo koordinatorius (angl. NCTV), o pastarajam Kibernetinės saugos direkcija (angl. *DCS*) Pagrindinė institucija atsakinga už kibernetinę saugą yra Nacionalinis kibernetinės saugos centras (angl. *NCSC*), tiesiogiai pavaldus DCS (žr. Pav. 8). NCSC yra atsakingas už skaitmeninę saugą ir šalies kibernetinį atsparumą, daugiausiai dėmesio skiria centrinės valdžios ir ypatingos svarbos infrastruktūros procesams. Šio padalinio tikslas sukurti saugią, atvirą ir stabilią informacinę visuomenę atliekant tris pagrindines roles:

- Valstybinius ir privačius subjektus konsultuoti informacijos saugumo politikų ir veiklų klausimu, tiek paprašius, teik savo iniciatyva (Ekspertizės ir konsultavimo skyrius)
- Tarnauti kaip centrinis informacijos ir kibernetinio saugumo ekspertizės centras (Rinkos plėtros ir partnerystės skyrius)
- Teikti operacijų koordinavimo paslaugas didžiųjų ICT krizių metu ir teikti kibernetinių incidentų atsako priemones Nyderlandų vyriausybei ir ypatingos svarbos infrastruktūros objektų valdytojams (Stebėjimo ir reagavimo skyrius)
- Prižiūrėti kibernetinės saugos bendradarbiavimo platformą
- Teikti įžvalgas ir prognozes kibernetinės saugos tema



Šaltinis: Hathaway M., Spidalieri F.,, 2020, p. 11

8 pav. **Nyderlandų Nacionalinio kibernetinės saugos centro organizacija**

Nyderlandai būdami labai skaitmenizuota valstybė ir turėdami didelį interneto padengiamumą šalies mastu, susidurdavo su labai dideliais kiekiais kibernetinių atakų, taip pat patirdavo didelius nuostolius dėl jų. Dėl šios priežasties 2011 metais Nyderlandai išleido savo pirmąją kibernetinės saugos strategiją, kurią du kartus atnaujino – 2014 ir 2018 metais. Strategijose numatomi tikslas ir užduotys vis keisdavosi, nes Nyderlandų valdžia gana sėkmingai įvykdydavo didžiąją dalį suplanuotų tikslų.

Nyderlandų 2018 metų kibernetinės saugos strategijos pagrindiniai principai. Nyderlandai turi puikias galimybes išnaudoti skaitmeninimo ekonomines ir socialines galimybes. Tuo pat metu didėja kibernetinės spragos ir grėsmės skaitmeninėje srityje. Profesionalių nusikaltėlių keliama grėsmė auga ir toliau vystosi. Valstybės priešai daugiausiai dėmesio skiria skaitmeniniam, ekonominiam ir politiniam šnipinėjimui ir ruošiasi skaitmeniniam sabotažui. Didėja ne tik puolančių šalių kiekis, bet ir atakų sudėtingumas. Atsižvelgiant į šiuos dalykus Nyderlandų Nacionalinėje kibernetinės saugos strategijoje išskiriami šie principai:

- Kibernetinis saugumas neatsiejamai susijęs su nacionaliniu saugumu: dėl skaitmenizacijos nacionalinio saugumo interesai yra pažeidžiami skaitmeninių atakų.
- Viešojo ir privačiojo sektorių bendradarbiavimas yra Nyderlandų požiūrio į kibernetinį saugumą pagrindas.
- Vyriausybė pripažįsta grėsmes gyvybiniams interesams ir stiprina atsparumą, tokiu būdu kurdama skaitmeniškai saugius Nyderlandus Verslo bendruomenė ir piliečiai skatinami patys formuoti savo atsakomybę ir saugumą.
- Žinios yra labai svarbios kibernetiniam saugumui užtikrinti, reikia keistis turimomis žiniomis ir skatinti viešąjį, bei privatų sektorių keistis informacija. Be to būtina skatinti fundamentalius ir taikomuosius kibernetinės saugos tyrimus.
- Integruoti kibernetinį saugumą į kiekvienos organizacijos kasdienius procesus.
- Skaitmeninė sritis nėra ribojama valstybių sienų. Nyderlandų požiūris į kibernetinę saugą turi apimti tarptautinį aspektą, atsižvelgiant į duomenis, ryšius, interneto valdžią ir veikėjai, kurie atlieka skaitmenines kibernetines atakas.
- Įtampa tarp laisvės, saugumo ir ekonomikos augimo interesų yra neatsiejama nuo kibernetinio saugumo plėtros. Atsižvelgiant į tai Nyderlandai nori judėjimo kursą padaryti aiškų ir paremtą sprendimų priėmimu.

Nacionalinės kibernetinės saugos strategijos pagrindinis tikslas – „Nyderlandai gali saugiai išnaudoti ekonomines ir socialines skaitmeninimo galimybes ir apsaugoti nacionalinį saugumą skaitmeninėje srityje“. Kibernetinėse strategijoje iškeliami 7 uždaviniai:

1. Nyderlandai turi tinkamas skaitmenines galimybes aptikti, sušvelninti ir ryžtingai reaguoti į kibernetines grėsmes
2. Nyderlandai prisideda prie tarptautinės taikos ir saugumo skaitmeninėje srityje
3. Nyderlandai yra skaitmeniniu požiūriu saugios aparatinės ir programinės įrangos lyderiai
4. Nyderlandai turi atsparius skaitmeniniai procesus ir patikimą infrastruktūra
5. Nyderlandai turi veiksmingus barjerus prieš kibernetinius nusikaltėlius
6. Nyderlandai pirmauja elektroninių saugumo žinių kūrimo srityje
7. Nyderlandai turi integruotą ir stiprų viešojo ir privataus sektorių požiūrį į kibernetinį saugumą

Be kibernetinės saugos strategijos Nyderlandai vadovaujasi tokiais savo ir Europos sąjungos teisės aktais:

- Tinklų ir informacinių sistemų saugumo direktyva (angl. *NIS*), kuri Nyderlanduose buvo įgyvendinta Tinklų ir informacinių sistemų įstatymo (dutch *WBNI*) pagalba
- Dekretas dėl didelių avarijų rizikų (dutch *BRZO*)

- Kibernetinio saugumo įstatymas vyriausybei (dutch *WDO*)
- Europos sąjungos Bendrojo duomenų apsaugos reglamento Nyderlandų įstatymas (angl. *NL BDAR*)

2018 metais Nyderlanduose įsigaliojo pagal NIS direktyvą sukurtas Tinklų ir informacinių sistemų įstatymas. WBNI yra taikoma tik gyvybiškai svarbiai infrastruktūrai, taigi ne visoms įmonėms ir žmonėms Nyderlanduose. Įstatymas taikomas Nyderlandų vyriausybei, telekomunikacijų ir branduolinei pramonei, taip pat energetikos, transporto, bankininkystės, finansų, sveikatos priežiūros, vandens ir interneto paslaugoms. Bendroves, kurioms taikomas šis įstatymas vyriausybė raštiškai informavo, kad jos turi užtikrinti atitiktį. WBNI įstatyme taip pat yra įpareigojimas privalomai pranešti apie įvykusius kibernetiniu incidentus. Ataskaitos turi būti adresuojamos Nacionaliniam kibernetinio saugumo centrui (angl. *NCSC*). NCSC ir Skaitmeninio pasitikėjimo centras (angl. *DTC*) yra įpareigoti patarti privačiam sektoriui. NCSC teikia patarimus gyvybiškai svarbią infrastruktūrą valdančioms įmonėms, o likusioms pataria DTC.

Kibernetinės saugos įstatymas vyriausybei (dutch WDO) yra pakankamai naujas. WDO įstatymas sudarytas iš standartų, produktų ir paslaugų, kurie turi būti naudojami Nyderlandų vyriausybės, viešųjų organizacijų ir kai kurių privačių kompanijų, kurios dirba vyriausybei. Šiame įstatyme didžiausias dėmesys skiriamas tinkamumui/panaudojamumui, todėl jis yra pastoviai tobulinamas ir atnaujinamas.

Visos kompanijos, kurios dirba su sprogiosiomis medžiagomis, taip pat turi laikytis 2015 metais išleisto BRZO įstatymo. BRZO įstatymas tiek fizini, tiek kibernetinį saugumą laiko saugos dalimi. BRZO įstatymas įpareigoja:

- Keitimasis informacija tarptautiniu mastu, kad būtų išvengta ar sušvelnintos grėsmės pasekmės
- Organizacijos saugumo reikalavimai (pvz., Mokymas, prieiga)
- Personalo saugos reikalavimai (pvz., Gero elgesio pažymėjimas [VOG])
- Civilinės saugos reikalavimai (pvz., Sprogimui atsparios sienos)
- Elektroninės saugos reikalavimai (pvz., Vaizdo stebėjimas, praėjimo kontrolė)
- Informacijos ir komunikacijos technologijų reikalavimai (pvz. ugniasienės)
- Įrodyti, kad organizacija valdo kibernetinį saugumą

2013 metais Nyderlandų saugumo ir teisingumo ministras savo šalies parlamentui pateikė Atsakingo atskleidimo praktikos kūrimo strategiją (angl. *Guideline for responsible disclosure of IT vulnerabilities*). Iš šios pradinės strategijos išsivystė 2018 metais Nyderlandų vyriausybės patvirtintas Koordinuoto spragų atskleidimo gairės (NCSC, 2018). Šios gairės aprašo galimybę žmonėms aptikus pažeidžiamumus informacinėse sistemose ir portaluose apie jas informuoti savininkus ir sulaukti iš jų padėkos, o ne priekaištų. Gairėse pabrėžiama, kad koordinuoto spragų ieškojimo ir viešinimo procese

organizacija ir pranešėjas apie spragą gali vadovautis dvišaliu tarpusavio susitarimu, nustatytu pagal organizacijos skelbiamą koordinuoto atskleidimo tvarką. Ši tvarka turėtų apibrėžti koordinuoto spragų atskleidimo procese dalyvaujančių šalių veiklos ribas, teises ir atsakomybes. Tokiu būdu tvarka taptų atskleidimo procesą reguliuojančiu dokumentu. Laikantis dokumente nustatytų principų, šalys išvengtų baudžiamosios arba administracinės atsakomybės taikymo.

2.2.3. Dabartinė kibernetinės saugos situacija Nyderlanduose

2019 metais Nacionalinis saugumo ir kovos su terorizmu koordinatorius (angl. *NCTV*) atliko Nyderlandų kibernetinės saugos įvertinimą (angl. *CSAN*). Dokumente pateikiamos įžvalgas apie su kibernetine sauga susijusias grėsmes, interesus ir atsparumą bei šių veiksnių poveikį nacionaliniam saugumui. CSAN ataskaitą kasmet skelbia NCTV, ataskaita rengiama bendradarbiaujant su viešaisiais ir privačiaisiais partneriais.

Pirmajame ataskaitos skyriuje yra apžvelgiamos šaknines problemos, kurios išaiškėjo atliekant ankstesnes CSAN analizes ir kurios neturi lengvo sprendimo (NCTV, 2019):

1. Visuomenei būtinas skaitmenizavimas. Visuomenė tapo beveik visiškai priklausoma nuo skaitmeninių technologijų, procesų ir sistemų. Tai lemia, kad kibernetinė sauga yra būtina norint užtikrinti socialinį ir ekonominį augimą ir užkirsti kelią socialiniams neramumams:
    - Atsarginių priemonių ir paralelinių alternatyvų praktiškai nebėra. Praktiškai visi kritiniai procesai ir paslaugos yra pilnai priklausomos nuo informacijos ir komunikacijos technologijų. Taigi bet koks šių sistemų veikimo sutrikdymas gali sukelti socialiai trikdančią žalą.
    - Priklausomybė nuo riboto techninės ir programinės įrangos, skaitmeninių paslaugų ir platformų tiekėjų kiekio ir paslaugas teikiančių valstybių vis didėja. Dėl technologinių galimybių ar kainos ir našumo privalumų verslams, piliečiams ir valstybės organizacijoms gali kilti pagunda pirkti paslaugas iš tokių įmonių. Tokių paslaugų tiekėjai paprastai turi daugybines apsaugas nuo įsibrovimų ir paslaugų sutrikdymo, bet sutrikus šių paslaugų veikimui socialinis poveikis gali būti didelis.
2. Pastovios kibernetinės grėsmės. Grėsmė, kurią kelia valstybių finansuojami kibernetiniai nusikaltėliai ir toliau auga. Šalys ir toliau naudoja skaitmeninius resursus šnipinėjimo ar net sabotažo tikslais, kad pasiektų savo tikslus olandų interesų sąskaita:
    - Kibernetinių atakų vykdymas nesudaro didelės rizikos puolantiesiems. Yra didelė tikimybė, kad įvykdytos kibernetinės atakos dar ilgą laiką bus neaptiktos, o jas aptikus gali būti labai sudėtinga nustatyti atakos šaltinį. Net jei pavyksta nustatyti atakos

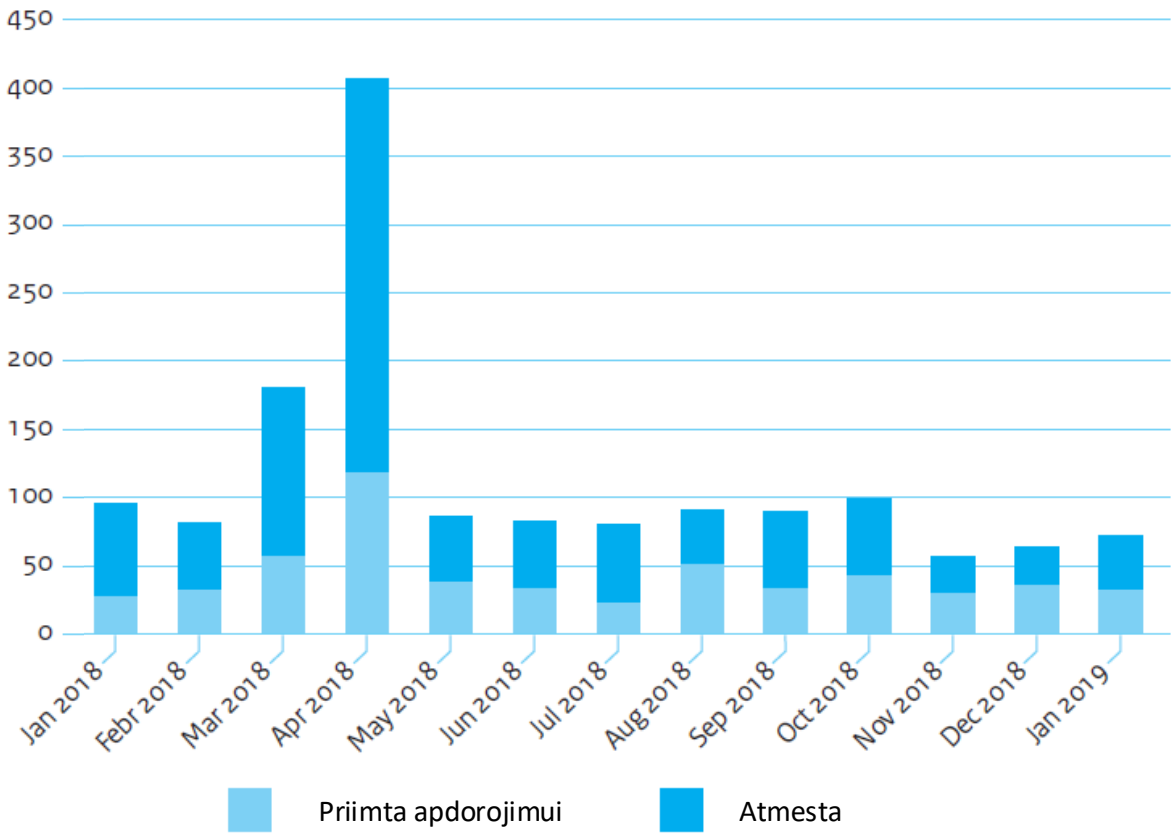
šaltinį, dažniausiai nėra jokių pasekmių, ypač jei tai susiję su kitos valstybės finansuojama ataka.

- Kibernetinių atakų vykdymo įrankius galima lengvai gauti per komercinius tiekėjus ir per didelį kibernetinių nusikalstamų paslaugų sektorių. Valstybės ir nusikaltėliai gali įsigyti kibernetinių atakų vykdymo mechanizmus, kitaip sakant jiems nebūtina tų atakų kurti patiems. Todėl atsiranda vis daugiau ir daugiau galimų atakos šaltinių, tai sudaro aukštą rizikos lygį.

3. Skaitmeninis atsparumas nėra visur tokio pat lygio. Organizacijos sėkmingai puolamos naudojant paprastus metodus. Daugybei tokių incidentų galėjo būti užkirstas kelias arba sumažinta žala, jei būtų buvę įgyvendintos bazinės saugos priemonės.

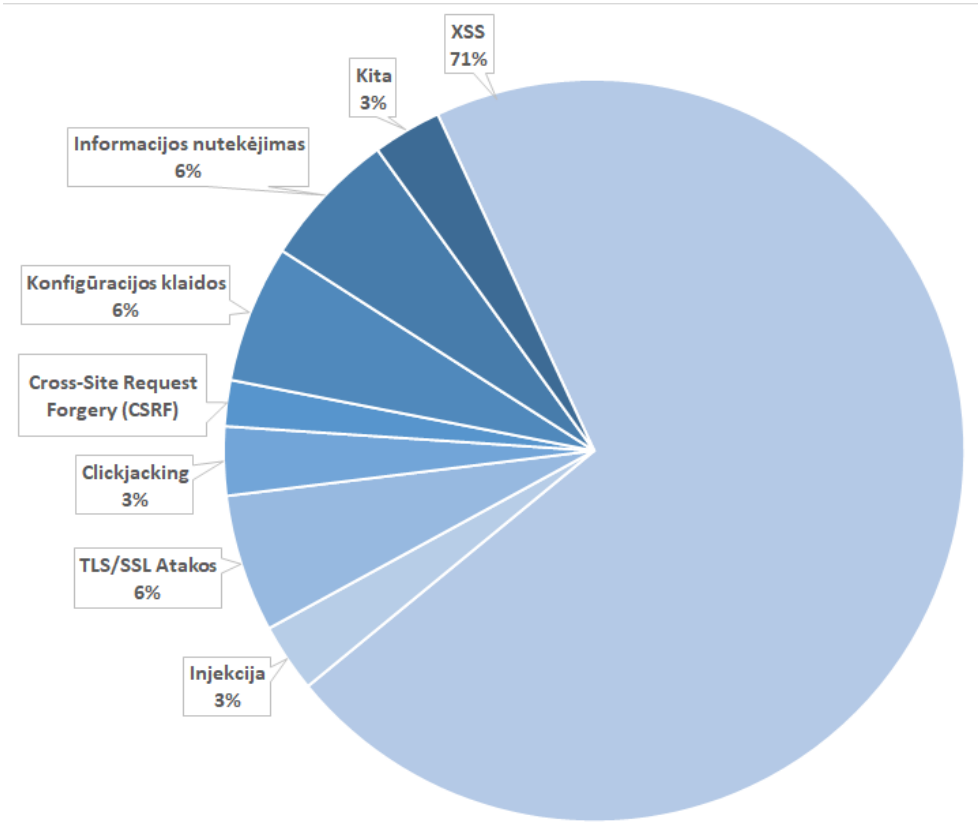
- Neigiamas sudėtingumo ir apjungimo poveikis. Darosi vis sunkiau užtikrinti patikimą ir atsparią skaitmeninę infrastruktūrą. Tam tikra programinė įranga, kurią naudoja programinės įrangos kūrėjai ir tiekėjai kaip statybinius blokus, jų teikiamoms paslaugoms, yra dešimčių metų senumo, todėl ji nėra atspari šiuolaikinėms kibernetinėms atakoms. Be to, dėl vis dažnesnio bendro naudojimo įrenginių naudojimo, tokių kaip daliniai produktai ar visos debesijos paslaugos, sunku susidaryti aiškų situacijos vaizdą ir prižiūrėti jo veikimą.
- Nesaugūs produktai ir paslaugos – kibernetinės saugos „Achilo kulnas“. Nesaugūs produktai ir paslaugos padidina paslaugų pasiekiamumą kibernetiniams nusikaltėliams, todėl jiems lengviau vykdyti kibernetines atakas. Saugumo praradimą gali sukelti tiekėjai, kurių produktuose yra nesaugios konfigūracijos, arba neteikia (arba nebeteikia) atnaujinimų, nes yra pažeisti atnaujinimo mechanizmai arba sunku įdiegti atnaujinimus. Be to, net jei atnaujinimų ir yra, organizacijos ne visada juos įdiegia.

NCTV CSAN 2019 ataskaitos prieduose pateikiama statistinė Nyderlandų Nacionalinio kibernetinės saugos centro (toliau – NCSC) informacija apie išnagrinėtus incidentus ir pranešimus gautus per Koordinuotą spragų atskleidimo programą (toliau – CVD). Ataskaitoje teigiama, kad CVD pranešimai vis dar išlieka naudingas įrankis pažeidžiamumų aptikimui. NCSC priima ir apdoroja CVD pranešimus tiek savo, tiek centrinės valdžios infrastruktūros labui. 9 paveikslėlyje pateikta gautų CVD ataskaitų statistika per 2018 metus (didelis atmestų ataskaitų kiekis buvo arba dėl to, kad nepavyko atkartoti minimų pažeidžiamumų arba dėl to, kad naujos ataskaitos dubliavo jau žinomus pažeidžiamumus). 10 paveikslėlyje pateikta diagrama su konkretesniais pažeidžiamumų tipais sužinotais iš CVD pranešimų.



Šaltinis: Cyber Security Assessment Netherlands, 2019

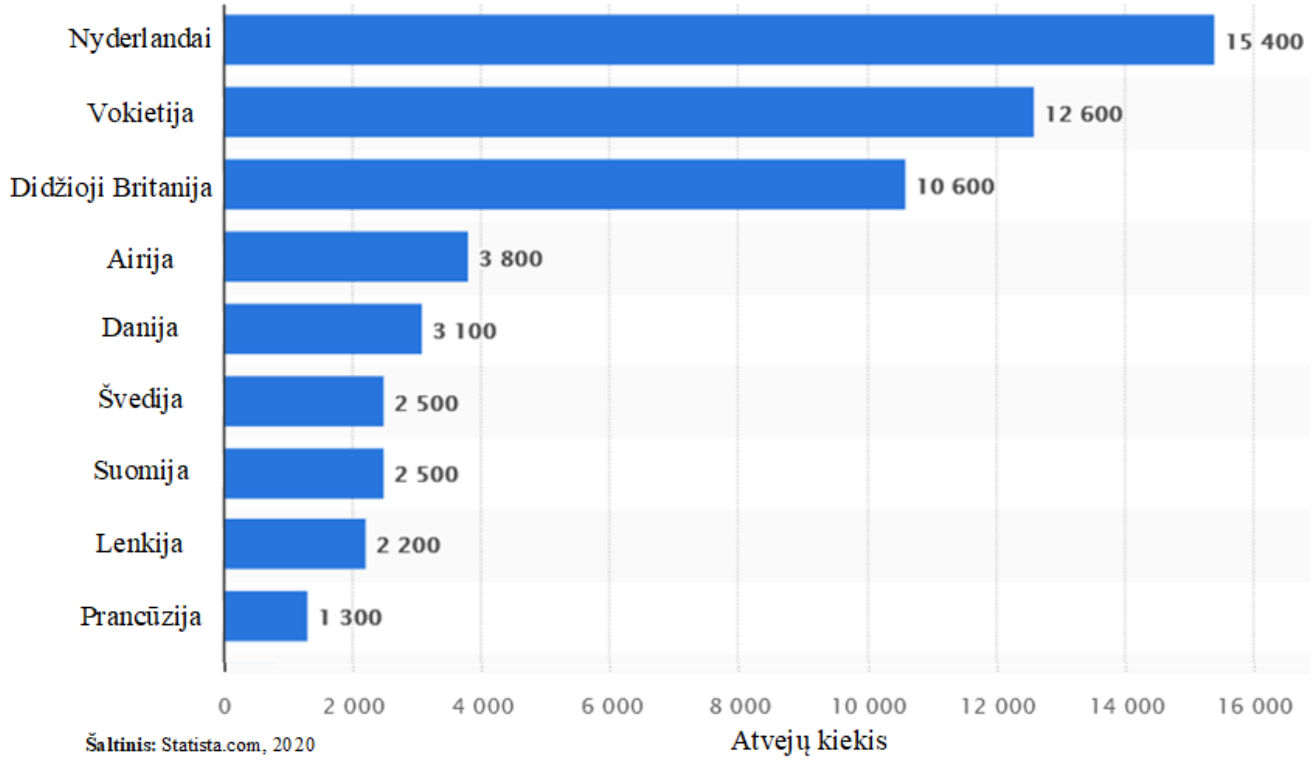
9 pav. **Koordinuoto spragų atskleidimo pranešimų statistika**



Šaltinis: Cyber Security Assessment Netherlands, 2019

10 pav. **Koordinuoto spragų atskleidimo praneštos klaidos pagal tipą**

Remiantis statistikos puslapiu Statista.com Nyderlanduose nuo 2018 gegužės iki 2019 birželio įvyko daugiausiai duomenų saugumo pažeidimo kibernetinių incidentų lyginant su kitomis Europos šalimis (žr. Pav. 11).



11 pav. **Duomenų saugumo pažeidimų kiekis Europos valstybėse 2018/05-2019/06**

2.3. Kibernetinės saugos valdymo priemonių taikymas Lietuvoje

2.3.1. Kibernetinės saugos vystymasis Lietuvoje

Lietuvoje ryšys su pasauliniu tinklu ir internetu atsirado beveik kartu su nepriklausomybės atgavimu – 1991 metais. Iš pradžių tinklu naudojosi tik Lietuvos Respublikos Seimas, o įkūrus Lietuvos mokslo ir studijų institucijų kompiuterių tinklą „Litnet“ prie šio tinklo ir vėliau prie interneto prisijungė Kauno technologijų universitetas ir Vilniaus universitetas. Iki 1994 metų prie interneto galėjo prisijungti tik „Litnet“ tinklo vartotojai (dauguma mokymo įstaigų darbuotojai ir studentai). Vėliau prisijungimo prie Interneto paslaugą per telefoninius modemus nemokamai teikė Atviros Lietuvos Fondas (ALF). Situacija pasikeitė 1999-2000 metais, kai „Lietuvos Telekomas“ nusprendė apmokestinti duomenų perdavimą telefoninėmis linijomis (Ikamas K., 2012).

Žinoma pačioje interneto naudojimosi pradžioje Lietuvoje nebuvo jokių įstatymų susijusius su kibernetine sauga. Pirmieji įstatymai ir nutarimai susiję su duomenų ir informacijos sauga buvo priimti 1996-1997 metais. Juose dar nebuvo kalbama apie internetą ir kibernetinę saugą, nes tie įstatymai buvo labiau skirti reguliuoti Valstybės institucijų informacinių sistemų ir duomenų bazių informacijos saugą. Toliau pateikiami keli svarbūs tuo metu išleisti įstatymai ir nutarimai:

- 1996 metais priimamas Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas. Įstatymas reguliuoja santykius, atsirandančius renkant, kaupiant, apdorojant, saugant, naudojant ir teikiant duomenis apie fizinius asmenis valstybės kompiuterizuotosioms informacinėms sistemoms, tarp jų ir valstybiniams registrams. Įstatymo tikslas – nustatyti duomenų subjektų teises ir šių teisių apsaugos tvarką.
- 1997 metais priimtas nutarimas dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose. Nutarimu siekiama užtikrinti duomenų esančių valstybės institucijų duomenų bazėse ir informacinėse sistemose patikimumą bei apsaugoti nuo neteisėto panaudojimo.
- 2003 metais patvirtinamas Nutarimas dėl bendrųjų reikalavimų valstybės institucijų interneto svetainėms. Nutarimo tikslas sudaryti visuomenei sąlygas gauti internetu visą viešą informaciją apie valstybės institucijas ir jų funkcijas, suvienodinti valstybės institucijų interneto svetaines, užtikrinti jų veiksmingumą, jose pateikiamos informacijos aktualumą, patikimumą, paieškos galimybes, svetainių kūrimą ir reguliarų informacijos atnaujinimą. Tiesa nutarime kalbama apie svetainių funkcinius, o ne saugos reikalavimus.

Taip pat nuo 2001 metų yra patvirtinamos dvi strategijos ir viena plėtros programa pilnai arba bent iš dalies susijusios su informacijos ir kibernetine sauga. Toliau išvadinamos tos trys strategijos su trumpu apibūdinimu:

- 2001 metais priimta Informacijos technologijų saugos valstybinė strategija. Šia strategija buvo siekiama nustatyti elektroninio verslo, elektroninio susirašinėjimo, kompiuterių tinklų, interneto tarnybinių stočių saugos reikalavimus. Taip pat strategija buvo norima įvesti duomenų saugos įgaliotinio pareigybę. Buvo planuojama sustiprinti svarbiausių valstybės informacinių sistemų saugą ir atlikti jų saugos atitikties vertinimo sistemos sukūrimą.
- 2002 metais patvirtinta Nacionalinio saugumo strategija. Strategijoje minimaliai užsimenama apie informacijos apsaugą – stiprinama svarbiausių valstybės informacinių sistemų sauga, užtikrinama tinkama informacijos technologijų ir duomenų saugos priemonių įgyvendinimo kontrolė.
- 2011 metais buvo patvirtinta Elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programa. Programos strateginis tikslas – plėtoti elektroninės informacijos saugą Lietuvoje, užtikrinti kibernetinį saugumą ir pasiekti, kad 2019 metais teisės aktų nustatytus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus atitinkančių valstybės informacinių išteklių dalis pasiektų 98 procentus visų valstybės informacinių išteklių, vidutinis ypatingos svarbos informacinės infrastruktūros incidentų likvidavimo laikas sumažėtų iki 0,5 valandos, o Lietuvos gyventojų, kurie saugiai jaučiasi kibernetinėje erdvėje, dalis pasiektų 60 procentų.

Deja nors paminėtoji Elektroninės informacijos saugos plėtros programa buvo labai ambicinga, jos tikslų įgyvendinti nepavyko – įvykdymas buvo tik apie 21%, o 2015 metais Valstybės kontrolė savo ataskaitoje „Kibernetinio saugumo aplinka Lietuvoje“ rašė:

„Nustatėme, kad penkerius metus vykdoma El. informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 m. programa nerezultatyvi: 2015 m. rugsėjo mėn. pasiekta tik 23 proc. planuotų rodiklių, 48 proc. pasiekti iš dalies, 29 proc. – nepasiekta. Esama būklė rodo, kad 2015 m. nebus pasiektas nė vienas programoje numatytas tikslų rodiklis, o bendras programos tikslų įgyvendinimas kol kas siekia tik 21 proc.“

Kalbant apie kibernetinės saugos vystymąsi Lietuvoje reikia paminėti ir jau skirtas bei dar planuojamas skirti lėšas kibernetinės saugos stiprinimui. Kaip rašoma 2015 metų Valstybės kontrolės ataskaitoje valstybės mastu nėra sukaupta tikslios informacijos apie išlaidas kibernetinei saugai, tačiau valstybinių auditorių vertinimu, 2011–2014m. kibernetinio saugumo ir el. informacijos saugos priemonėms įgyvendinti panaudota apie 20,9 mln. EUR, o nuo 2015 m. iki 2020 m. planuojama panaudoti dar apie 15,6 mln. EUR valstybės biudžeto asignavimų, ES ir kitos tarptautinės finansinės paramos lėšų. Papildant šią informaciją galima pasakyti, kad vykdant Kibernetinės saugos strategijos 2019-2021 metų planą numatoma skirti apie 7 mln. eurų iš valstybės biudžeto ir Europos Sąjungos paramos lėšų (LRV, 2019).

2.3.2. Kibernetinės saugos teisinis reglamentavimas Lietuvoje

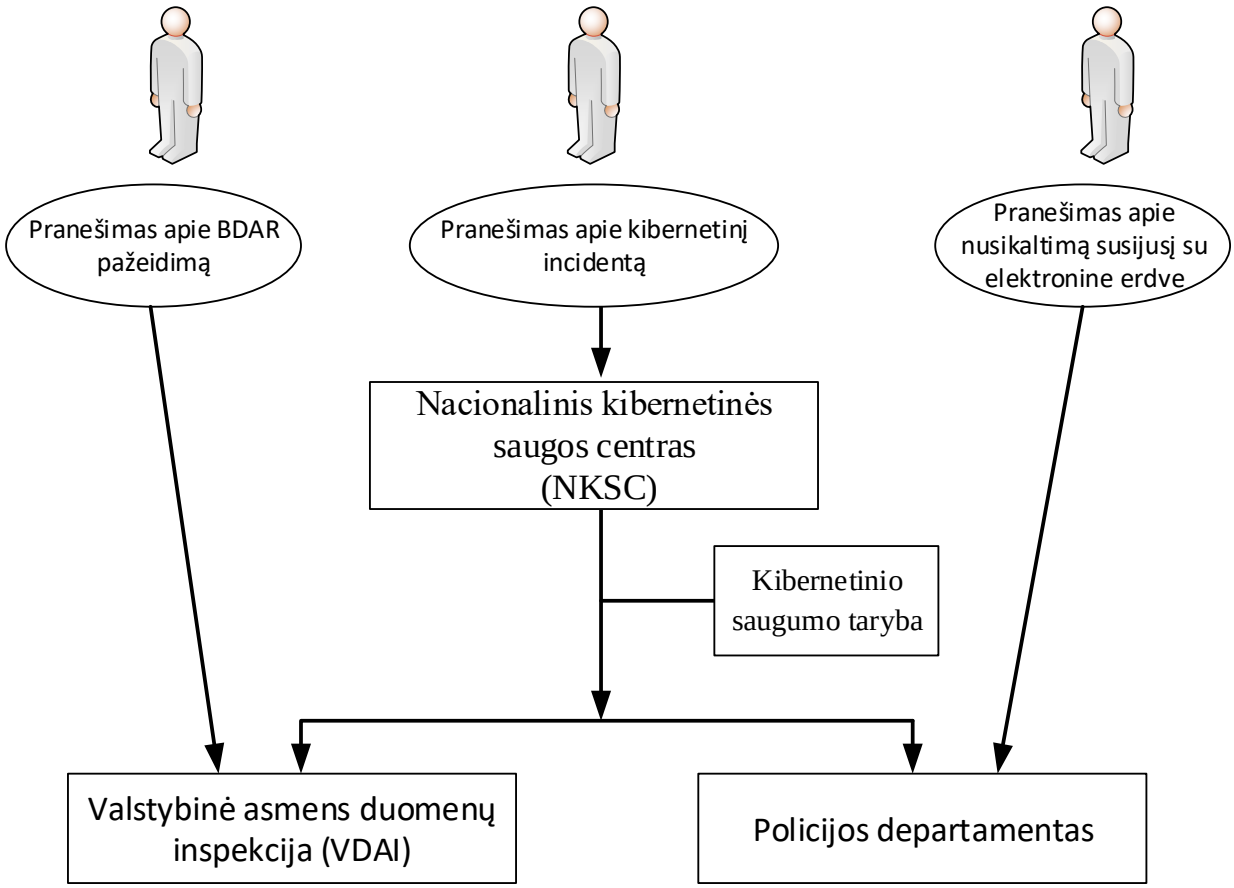
Lietuvoje Kibernetinės saugos valdymas vykdomas remiantis Kibernetinės saugos įstatymu ir Kibernetinių incidentų valdymo planu. Lietuvoje kibernetinės saugos funkcijas atlieka trys pagrindinės institucijos: Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija ir Policijos departamentas. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) yra pagrindinė Lietuvos kibernetinio saugumo institucija, atsakinga už vieningą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę, ypatingos svarbos informacinės infrastruktūros kibernetinį saugumą ir informacinių išteklių akreditaciją. Pagal NKSC nuostatas yra numatyti šie pagrindiniai institucijos veikos tikslai:

- Atlikti Saugumo priežiūros tarnybos funkcijas;
- Įgyvendinti nacionalinę kibernetinio saugumo politiką;
- Atlikti Nacionalinės komunikacijų apsaugos tarnybos funkcijas;
- Vykdyti informacijos sklaidos, tyrimų ir analizės kibernetinio saugumo klausimais veiklą.

NKSC struktūrą sudaro Kibernetinės gynybos ir Informacijos saugumo departamentai. Kibernetinės gynybos departamentas sudarytas iš trijų skyrių: Incidentų valdymo, Sistemų administravimo ir Kritinės

infrastruktūros saugumo. Informacijos saugumo departamentas sudarytas taip pat iš trijų skyrių: Bendrųjų reikalų, Inovacijų ir mokymo ir Akreditavimo. Kibernetinio saugos įstatymui ir Incidentų valdymo planui svarbiausi yra Incidentų valdymo ir Kritinės infrastruktūros saugumo skyriai.

Valstybinė asmens duomenų apsaugos inspekcija (toliau – VDAI) yra asmens duomenų apsaugos priežiūros institucija, kuri rūpinasi, kad būtų ginama žmogaus teisė į asmens duomenų ir privatumo apsaugą, tvarkant asmens duomenis profesiniais tikslais, kad asmens duomenų apsauga Lietuvoje atitiktų Europos Sąjungos teisinius reikalavimus ir būtų tinkamai užtikrinama informacinės visuomenės aplinkoje. Nuo 2018 metų įsigaliojus Europos sąjungos Bendrojo duomenų apsaugos reglamentui (toliau – BDAR) VDAI taip pat vykdo veiklą susijusią su BDAR ir priima skundus dėl BDAR pažeidimų. Lietuvos policija, o tiksliau Lietuvos kriminalinės policijos biuro 5-oji valdyba yra atsakinga už nusikaltimus elektroninėje erdvėje. 12 paveikslėlyje pavaizduotos už kibernetinių nusikaltimų valdymą ir sprendimą atsakingos Lietuvos institucijos ir jų tarpusavio sąveika.



Šaltinis: parengta autoriaus pagal kibernetinės saugos įstatyma ir kt dokumentus

12 pav. **Už kibernetinių nusikaltimų sprendimą atsakingos Lietuvos institucijos**

Schemoje taip pat vaizduojama Kibernetinio saugumo taryba, kurią sudaro įvairių valstybės institucijų atstovai, ji nuolatinė kolegiali nepriklausoma patariamoji institucija, analizuojanti kibernetinio saugumo užtikrinimo būklę Lietuvos Respublikoje ir teikianti kibernetinio saugumo politikos formavimo ir įgyvendinimo rekomendacijas.

Lietuvos 2018 metų kibernetinės saugos strategijos pagrindiniai tikslai. Iki pat 2018 metų Lietuva neturėjo vien kibernetinei saugai dedikuotos strategijos. 2002 – paskelbta bendro saugumo strategija, 2011 – paskelbta informacijos saugos programa, kuri iš dalies apėmė ir kibernetinę saugą. Galiausiai pastarosios nepavyko pilnai įgyvendinti. 2017 metais buvo nuspręsta sukurti pilnavertę Nacionalinę kibernetinės saugos strategiją. Šioje strategijoje išskiriami penki pagrindiniai tikslai ir juos įgyvendinti leidžiantys uždaviniai:

1. Stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, šio tikslo uždaviniai:
    a) Kurti sisteminį požiūrį į kibernetinį saugumą ir prevencinę veiklą – bus tobulinamas kibernetinio saugumo rizikos nustatymo, vertinimo ir prognozavimo būdus;
    b) Didinti kibernetinio saugumo politikos formavimo ir įgyvendinimo efektyvumą, mažinant administracinę naštą kibernetinio saugumo subjektams;
    c) Skatinti nacionalinių pratybų vykdymą ir dalyvavimą tarptautinėse pratybose;
    d) Plėtoti valstybės kibernetinės gynybos pajėgumus.
2. Užtikrinti nusikalstamų veikų kibernetinėje erdvėje prevenciją, užkardymą ir tyrimą, šio tikslo uždaviniai:
    a) Plėtoti valstybės pajėgumus ir gebėjimus kovoti su nusikalstamomis veikomis kibernetinėje erdvėje;
    b) Stiprinti nusikalstamų veikų kibernetinėje erdvėje prevenciją ir kontrolę.
3. Skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, šio tikslo uždaviniai:
    a) Plėtoti mokslinius tyrimus ir didelę pridėtinę vertę kuriančias veiklas kibernetinio saugumo srityje;
    b) Ugdyti kūrybiškumą, pažangius gebėjimus ir rinkos poreikius atitinkančius kibernetinio saugumo įgūdžius ir kvalifikaciją;
    c) Skatinti viešojo ir privataus sektorių bei mokslo ir studijų institucijų bendradarbiavimą, kuriant kibernetinio saugumo srities inovacijas.
4. Stiprinti glaudų viešojo ir privataus sektorių bendradarbiavimą, šio tikslo uždaviniai:
    a) Gerinti viešojo ir privataus sektorių bendradarbiavimo koordinavimą;
    b) Didinti viešojo bei mažų ir vidutinių privataus sektorių atstovų kibernetinio saugumo brandą;
    c) Kurti atsakingą viešojo ir privataus sektorių Informacijos ir ryšių technologijų saugumo spragų atskleidimo praktiką.
5. Stiprinti tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą, šio tikslo uždaviniai:

a) Plėtoti tarptautinį, tarpvalstybinį ir Baltijos regiono šalių bendradarbiavimą kibernetinio saugumo srityje;
b) Stiprinti tarptautinius kibernetinio saugumo pajėgumus ir gebėjimus;
c) plėsti dialogą su Jungtinėmis Amerikos Valstijomis kibernetinės gynybos srityje, siekti Jungtinių Amerikos Valstijų dalyvavimo Lietuvos kibernetinio saugumo užtikrinimo projektuose.

Be Kibernetinės saugos įstatymo ir strategijos Lietuvoje yra remiamasi anksčiau minėtu Asmens duomenų teisinės apsaugos įstatymu, tik 1996 versija buvo atnaujinta kelis kartus ir dabar galioja 2019 metų. Taip pat labai svarbūs yra kartu su Kibernetinės saugos įstatymu patvirtinti lydintys dokumentai:

- Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas
- Nacionalinis kibernetinių incidentų valdymo planas

Pirmajame labai detaliai aprašytos organizacinės ir techninės priemones, kurias privaloma ar rekomenduotina įgyvendinti Ypatingos infrastruktūros valdytojams ir kitoms institucijoms, o antrajame paaiškinama kibernetinių incidentų valdymo procedūra.

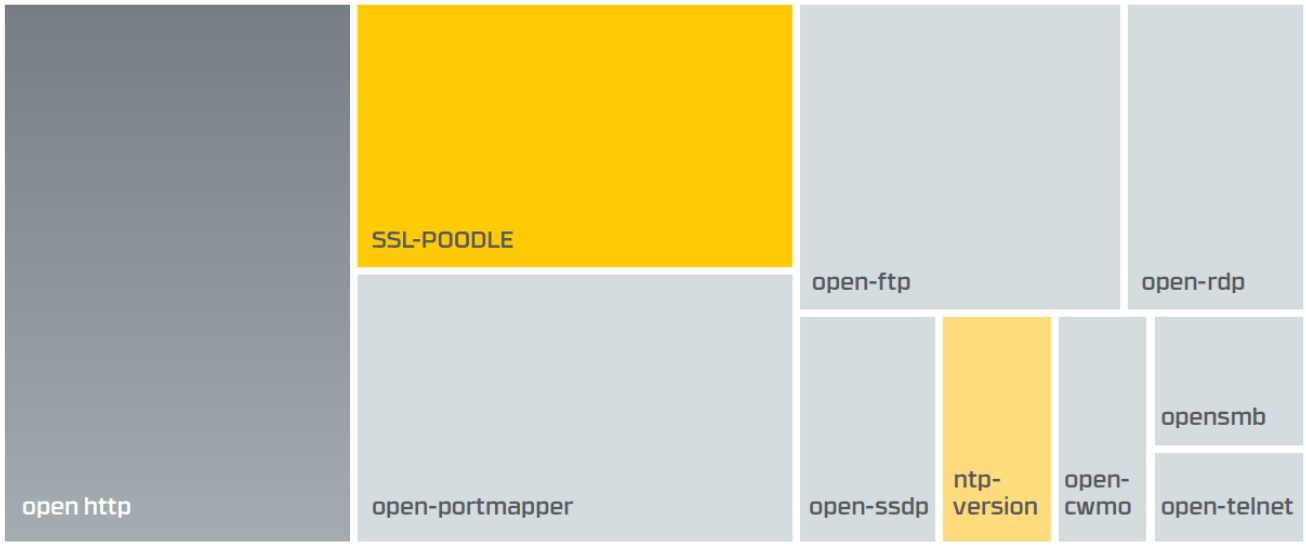
Lietuva vis dar neturi įstatyminės bazės susijusio su atsakingu pažeidžiamumų atskleidimu. Netūrėdama tokio įstatymo Lietuvos vyriausybė praranda puikų būdą neatlygintinai arba su minimaliomis išlaidomis sužinoti apie realiai Lietuvos valstybinių institucijų portaluose žiojinčias skyles. Tiesa NKSC savo 2019 metų kibernetinio saugumo būklės ataskaitoje pažymi, kad deda visas reikalingas pastangas tokio įstatymo atsiradimui ir Lietuvoje.

2.3.3. Dabartinė kibernetinės saugos situacija Lietuvoje

NKSC savo 2019 metų kibernetinio saugumo būklės ataskaitoje informuoja, kad NKSC 2019 metais užfiksavo 3241 kibernetinį incidentą, tris kartus daugiau nei ankstesniu laikotarpiu. Skelbiama, kad šie incidentai daugiausiai susiję su ryšių ir informacinių sistemų kibernetinėmis grėsmėmis ir kenkimo programine įranga. NKSC savo ataskaitoje pažymi, kad siekdami suvienodinti Lietuvos teikiamų kibernetinių incidentų ataskaitų klasifikavimo principus su Europos sąjungos naudojamomis. NKSC pakeitė kibernetinių incidentų skaičiavimo metodiką. Esant tokioms aplinkybėms nėra galimybės tiesiogiai palyginti 2019 metais įvykusių incidentų kiekį su 2018 ar 2017 metų kiekiu. Remiantis ankstesne metodika Kibernetiniais incidentais buvo laikomi ir rankinėmis ir automatinėmis priemonėmis nustatyti incidentai, o nuo šių metų automatinėmis priemonėmis nustatyti incidentai laikomi kibernetiniais įvykiais. Be pačios NKSC užfiksuotų incidentų, 2019 metais dar gauta informacija iš Valstybinės duomenų apsaugos inspekcijos apie 34 incidentus susijusius su asmens duomenų apsaugos

pažeidimais, o Informatikos ir ryšių departamento statistikos puslapyje skelbiamos apie 439 su elektronine erdve susijusios nusikalstamos veikos. Anot NKSC tokie skurdūs kitų tarnybų pateikti skaičiai rodo, kad Lietuvoje daugiausiai dėmesio skiriama prevenciniam kibernetinių incidentų užkardymui, o iš teisinės pusės bausmės už piktavališkos veiklos vykdymą yra sunkiai realizuojamos.

NKSC savo ataskaitoje taip pat skelbia populiariausias ryšių ir informacinių sistemų kibernetines grėsmes Lietuvos IP rėžyje (žr. Pav. 13)



Šaltinis: NKSC ataskaita, 2019

13 pav. **Populiariausios ryšių ir informacinių sistemų kibernetinės grėsmės 2019 metais**

Taip pat labai svarbi statistika skelbiama apie pažeidžiamas interneto svetaines. NKSC 2019 metais patikrino 118 000 svetainių bei portalų ir nustatė, kad net 37 % iš jų naudoja nesaugią turinio valdymo sistemą (toliau – TVS), kuri leidžia iš išorės prie jos prisijungti per administratoriaus paskyrą. Taip pat ataskaitoje teigiama, kad statistiškai viešajame sektoriuje labiausiai pažeidžiamos yra savivaldybių ir joms pavaldžių įstaigų interneto svetainės. Tuo tarpu saugių interneto svetainių kiekis viešajame sektoriuje augo 11%. Valstybinės institucijos vis dar nepakankamai vertina pavojų, kad jų svetainės spragos gali leisti nusikaltėliams skleisti tikrovės neatitinkančias naujienas (angl. *Fake news*) arba tokios svetainės gali būti panaudotos vykdant socialinės inžinerijos metodais paremtos atakos. Kaip rašoma NKSC ataskaitoje patikrinus minėtą kiekį interneto svetainių surinkta tokia informacija apie tuose puslapiuose naudojamas TVS sistemas (žr. Pav. 14). Iš identifikuotų TVS (56 700 iš bendro 118 000 Lietuvos svetainių skaičiaus), nustatyta, kad net 63 proc. jų programinės įrangos versijos nėra naujausios, dėl to yra rizika, kad pasenusi TVS turės pažeidžiamumą, kurį išnaudojus piktavalis galės prieš svetainę atlikti kibernetinę ataką. Dar blogiau, 8 proc. identifikuotų interneto svetainių savininkų naudoja gamintojų jau nebepalaikomą TVS, todėl joms gali būti neprieinami atnaujinimai ir jos gali turėti saugumo spragų. Kaip jau minėta įvade, per metus dar labiau sumažėjo viešojo sektoriaus Lengvai išlaužiamų interneto svetainių. Taip pat ataskaitoje pastebima, kad Lietuvoje sukurtos TVS buvo ypač pažeidžiamos kibernetiniams incidentams, dėl nepakankamai kokybiško TVS kūrimo.

Nr.	Turinio valdymo sistema	Paplitimas Lietuvoje	Paplitimas viešajame sektoriuje
1	Wordpress	34 proc.	33 proc.
2	Joomla	4 proc.	13 proc.
3	Fresh Media	< 1 proc.	6 proc.
4	Idamas	< 1 proc.	5 proc.
5	Drupal	< 1 proc.	3 proc.
6	Kita	8 proc.	2 proc.
7	Nenustatyta	~ 52 proc.	38 proc.

Šaltinis: NKSC ataskaita, 2019

14 pav. **Populiariausios identifikuojamos TVS Lietuvoje**

NKSC savo 2019 metų ataskaitos pabaigoje skelbia išvadas su jų nuomone svarbiausiomis problemomis ir pastebėjimais:

1. Lietuvoje nepakankamai vertinamas kibernetinių incidentų poveikis. Dažniausiai yra manoma, kad kibernetiniai incidentai yra nereikšmingi. Dėl šios priežasties susiduriama su kitomis problemomis, kurias NKSC fiksavo savo veikloje.
2. Viešajame sektoriuje interneto svetainių kibernetinio saugumo būklė gerėja, tačiau bendrąja prasme interneto svetainių kibernetinio saugumo rizikos išlieka reikšmingos.
3. Formalus kibernetinio saugumo reikalavimų įgyvendinamas didėja, tačiau kyla keblumų diegiant praktines kibernetinių incidentų rizikų kontrolės priemones.

Net kelių pasaulinių kompanijų kuriančių taip vadinamus kibernetinės saugos indeksus sąrašuose Lietuva užima labai gerą vietą. Daugiau informacijos pateikiama 2 lentelėje.

2 lentelė **Lietuvos pozicija pagal kibernetinį pasirengimą NCSI ir GCI indeksuose**

	National Cyber Security Index 2018		**Global Cybersecurity Index 2018**	
	Valstybė	**NCSI Taškai**	**Valstybė**	**GCI Taškai**
1	Graikija	92.21	Jungtinė Karalystė	0.931
2	Čekija	92.21	JAV	0.926
3	Estija	90.91	Prancūzija	0.918
4	Lietuva	88.31	Lietuva	0.908

Šaltinis: parengta autoriaus pagal Global Cybersecurity Index, 2019 ir National Cyber Security Index, 2018

2.4. Kibernetinės saugos valdymo priemonių taikymo lyginamoji analizė pasaulio šalių kontekste

3 lentelė **Lyginamoji Jungtinių Amerikos Valstijų, Nyderlandų ir Lietuvos kibernetinės saugos valdymo priemonių taikymo analizė**

Valstybė / Lyginamasis parametras	Jungtinės Amerikos Valstijos	Nyderlandai	Lietuva
Panašumai	JAV ir Nyderlandai panašūs tuo, kad pas juos internetas atsirado pakankamai senai, o kompiuteriniai tinklai egzistuoja daug laiko, todėl yra geras įdirbis šioje srityje. Ir JAV, ir Nyderlandai turi Atsakingo pažeidžiamumų atskleidimo įstatymus Ir Nyderlandų, ir Lietuvos kibernetinės saugos reglamentavimas yra nedidelės apimties, yra nesudėtinga orientuotis. Nyderlandų ir Lietuvos kibernetinės saugos srities organizacinė schema yra pakankamai panaši, abiejose yra palaikymo grupė/taryba, abiejose pagrindinė šios srities galia koncentruojasi į Nacionalinį kibernetinės saugos centrą. JAV ir Lietuva turi įstatymus reglamentuojančius interneto svetainių ir žiniatinklio tarnybinių stočių saugos reikalavimus		
Skirtumai	Skirtingai nuo JAV ir Nyderlandų Lietuva savo kibernetinės saugos strategiją suformavo pakankamai nesenai. JAV kibernetinės saugos teisinis reglamentavimas stipriai skiriasi nuo kitų dviejų valstybių, yra daug panašių įstatymų, o dalis funkcijų išskirstyta į kelis skirtingu metu išleistus įstatymus, kurie vienas kitą dalinai perdengia. Nyderlandai išsiskiria tuo, kad nuo pat pirmosios savo kibernetinės saugos strategijos laikosi nuoseklumo, įvykdo užsibrėžtus tikslus ir parengia naują strategiją. Nyderlandai stipriai skiriasi nuo kitų dviejų šalių savo didele visų sričių skaitmenizacija.		
Privalumai	Gerai paskirstytos atsakomybės tarp kibernetinės saugos sritį kuruojančių įstaigų. Kibernetinei saugai gali skirti didelį biudžetą Turi gerai paruoštą saugumo sistemą (security framework), kurios pagalba nesudėtinga bet kokioje įstaigoje optimizuoti kibernetinę saugą.	Turi labai gerai atidirbtą ir tinkamai funkcionuojantį Koordinuoto spragų atskleidimo įstatymą ir gaires.	Turi teisinį reglamentavimą beveik visoms kibernetinės saugos sritims. Per trumpą laiką sugebėjo pasitempti iki kitų šalių ir išspręsti daug vyravusių problemų

Valstybė / Lyginamasis parametras	Jungtinės Amerikos Valstijos	Nyderlandai	Lietuva
Trūkumai	Nepaslanki ir griozdiška teisinė bazė, joje sunku orientuotis, tas pats dalykas gali būti reglamentuotas iškart keliuose įstatymuose. Daug senų informacinių ir techninių sistemų, kurių nebeįmanoma atnaujinti, o jų išlaikymas kainuoja kelis kartus brangiau nei naujų sistemų.	Yra daug neužpildytų sričių teisiniame kibernetinės saugos reglamentavime. Daugelis sričių taip stipriai skaitmenizuota, kad nebeliko alternatyvių būdu kaip jas valdyti, ypač jei jos sutrikdomos kibernetinių atakų. Kibernetinės saugos sričiai skiria pakankamai mažą dalį nuo BVP.	Neturi galiojančio Atsakingo pažeidžiamumų atskleidimo įstatymo

Šaltinis: sudaryta autoriaus

3 lentelėje palyginamos Lietuvos, Nyderlandų ir JAV kibernetinės saugos sistemos atsižvelgiant į jų vystymąsi, valdymo organų struktūrą ir teisinę bazę. Nepaisant to, kad Lietuvoje sistema yra palyginti jauna, kokybiškai nėra per daug atitolusi nuo gerokai brandesnių ir ilgiau tobulintų sistemų, teisiškai ir pagal struktūrą , ji gerokai artimesnė Nyderlandams, kur akivaizdžiai pasiteisina tikslais neperkrautos kibernetinės strategijos modelis (trumpesnis laikotarpis, konkretūs struktūrizuoti tikslai). Vienas iš pagrindinių Lietuvos kibernetinės saugos teisinio reglamentavimo trūkumų – nėra Atsakingo pažeidžiamumų atskleidimo įstatymo.

3. VALSTYBĖS INSTITUCIJŲ PORTALŲ APSAUGOS KIBERNETINĖS SAUGOS VALDYMO PRIEMONĖMIS VERTINIMO METODOLOGIJA

3.1. Empirinio tyrimo metodologija

Renkantis kokio tipo tyrimas tinkamiausias šiam darbui, buvo nagrinėjami kiekybiniai ir kokybiniai tyrimai. Kiekybinis tyrimas buvo atmestas kaip netinkamas, nes nagrinėjama tema yra pakankamai nauja ir reikalaujanti specifinių žinių. Nėra pakankamai statistinės informacijos tinkamam kiekybiniam tyrimui atlikti, be to atliekant ankentinę apklausą nebūtų pavykę rasti didelės imties respondentų arba jų atsakymai būtų buvę neišsamūs, nepagrįsti patirtimi. Pagrindinis skirtumas tarp kiekybinių ir kokybinių tyrimų tai, kad kiekybinių tyrimų atveju gaunami rezultatai išreiškiami skaičiais, procentais ir statistiniai ryšiais, o kokybinio tyrimo rezultatas yra tekstinio pobūdžio, nestruktūrizuotas, neturintis reprezentatyvumo, bet pateikiantis gilesnę ir platesnę informaciją, nei kiekybinių tyrimų (Tidikis, 2003).

Tyrimo uždaviniams įgyvendinti buvo pasirinktas kokybinis tyrimas. Kokybinis tyrimas – tai toks tyrimas, kuris sociologijos, filosofijos, logikos ir individualaus stebėjimo priemonių pagalba padeda suprasti tam tikrą žmonių elgesį ir tokio elgesio priežastis (Tidikis, 2003). Kokybinis tyrimas atskleidžia ne tik akivaizdžiai matomus dalykus, bet nagrinėja ir giliau esančius požiūrius, įsitikinimus ir vertybes (Socialinės informacijos centras, 2020). Anot Tidikio (2003) tyrėjas atlikdamas kokybinį tyrimą savo dėmesį kreipia į subjektą ir jo veiksmus, bei kasdienę patirtį ir jo sąveiką su kitais individais. Informaciją tyrimui nuspręsta rinkti atliekant ekspertinį pusiau struktūrizuota interviu. Tokiam interviu parenkami ekspertai, kurie yra savo profesinės srities žinovai, turintys didžiausią kompetenciją analizuojamoje temoje ir galintys suteikti daugiausiai detalios informacijos apie tiriamą objektą, aptarti ir patikrinti tyrimo hipotezes, bei įvertinti įvairias tyrimo metodikas (Tidikis, 2003).

Pusiau struktūrizuotą ekspertinį interviu rekomenduojama naudoti kai tyrėjas turi pasirengęs temų sąrašą, bet nori turėti laisvės interviu metu paklausti neparuoštų klausimų, kurie kyla bendraujant su pašnekovu. Taikydami pusiau struktūrizuotą interviu tyrėjas gali lengviau suprasti tiriamą problemą ir atskleisti visiškai netikėtus ar nenumatytus problemos aspektus (Rupšienė, 2007). Šio tyrimo tikslinę grupę sudarė kibernetinės saugos ekspertai, turintys daug darbo ir užsiėmė, todėl buvo parinktas pusiau struktūrizuotas interviu.

3.1.1. Empirinio tyrimo tikslas ir uždaviniai

Tyrimo tikslas

Atlikti ekspertų nuomonės apie Valstybės institucijų portalų apsaugą kibernetinės saugos valdymo priemonėmis analizę ir pateikti priemonių pritaikymo Lietuvos valstybės institucijų portalų apsaugai rekomendacijas.

Tyrimo etapai

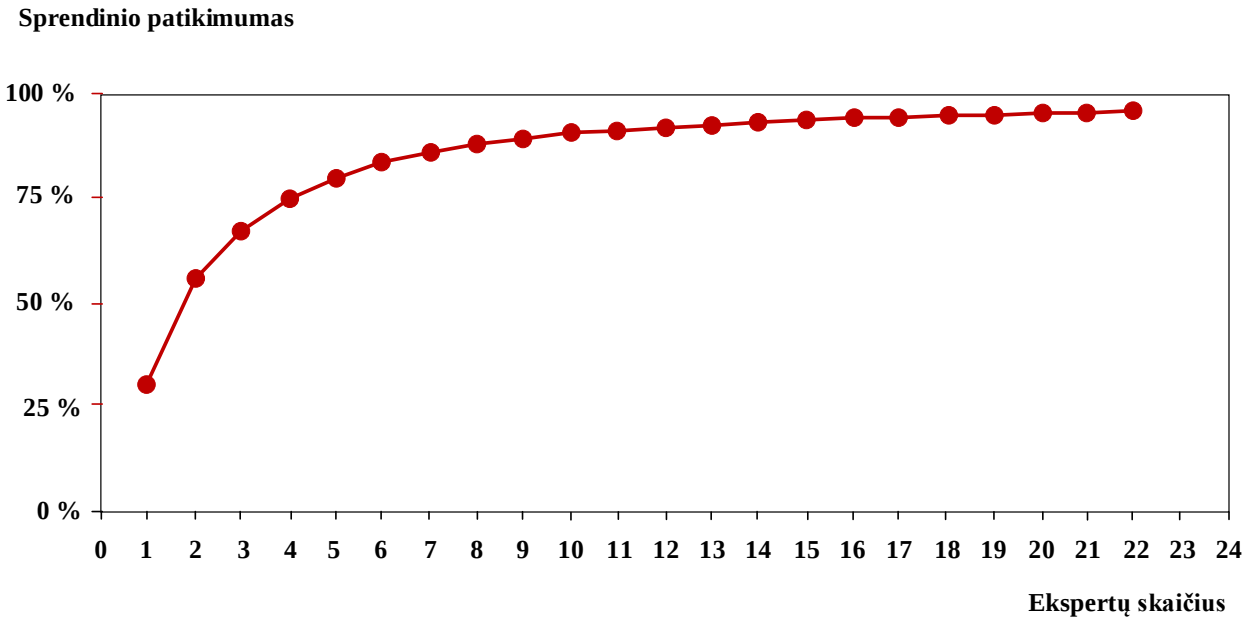
1. Atlikta mokslinių straipsnių, knygų ir teisės aktų bei ataskaitų analizė padėjo išnagrinėti tyrimo teorinius aspektus. Išnagrinėta portalų apsaugos samprata ir aptarta kodėl reikia saugoti internetinius portalus. Atlikta internetinių svetainių ir žiniatinklio aplikacijų architektūros analizė ir išskirtos dažniausiai kūrėjų daromos klaidos ir pažeidžiamiausios sritys. Išskirtos ir išanalizuotos kibernetinių nusikaltėlių dažniausiai atliekamos atakos ir nustatytos dažniausiai pasitaikančios kibernetinės grėsmės. Detaliai išnagrinėtos kibernetinės saugos valdymo rūšys ir rekomendacijos, bei reikalavimai jų įvykdymui.
2. Išanalizuota valstybės institucijų portalų apsaugos kibernetinės saugos valdymo priemonėmis pasaulinė praktika. Tais pačiais aspektais išnagrinėta kibernetinės saugos sritis Jungtinėse Amerikos Valstijose, Olandijoje ir Lietuvoje. Atlikus visų trijų valstybių detalias analizes rezultatai palyginti, lentelės pagalba.
3. Atliktas kokybinio vertinimo tyrimas panaudojant ekspertinio vertinimo metodą. Pusiau struktūrizuotam ekspertų interviu parinkti devyni kibernetinės saugos specialistai iš privataus ir valstybinio sektoriaus, turintys ne mažiau kaip 5 metų patirtį informacijos ir tinklų saugos srityse. Tyrimo metu surinkti duomenys išanalizuoti ir palyginti aprašomuoju būdu.

3.1.2. Empirinio tyrimo imtis

„Kokybiniame tyrime neverta siekti tikimybinės, atsitiktinai sudarytos imties, bet priešingai – reikia pasirinkti tokius atvejus, kurie informatyvūs tiriamuoju požiūriu. Kiekviename tyrime imties dydis ir konkretūs tyrimui pasirinkti imties vienetai iš esmės priklauso nuo tyrimo tikslų" (Rupšienė, 2007). Empiriniam tyrimui ekspertai buvo parinkti naudojant tikslinį grupių formavimą, remiantis jų patirtimi, kasdiene veikla ir darbo sritimi. Atkreiptas dėmesys į respondentų darbo stažo trukmę ir tai kaip aktyviai jie reiškiasi su darbu susijusiuose socialiniuose tinkluose. Renkantis galimus kandidatus buvo dalyvaujama įvairiose su kibernetine sauga susijusiuose seminaruose ir konferencijose, jų metu stebimi pranešėjai ir pasižymimi tie, kurių pranešimai labiausiai susiję su tiriama tema. Du respondentai buvo

parinkti, nes atstovavo žinomas valstybines ir privataus sektoriaus organizacijas užsiimančias veikla susijusia su kibernetine sauga ir jos valdymu. Taip pat vienas ekspertas buvo parinktas pagal kito eksperto rekomendaciją.

Sudarant ekspertų grupę tyrimui atlikti rekomenduojama įtraukti ne mažiau kaip 5 ekspertus. Daugelio mokslininkų nuomone, optimalus grupės dydis – nuo 8 iki 10 ekspertų. Yra įrodyta, kad nedidelės ekspertų grupės sprendimų ir vertinimų tikslumas nenusileidžia didelės ekspertų grupės sprendimų ir vertinimų tikslumui. Didinant ekspertų imtį tyrimo tikslumas didėja ir didžiausiu tampa 5-9 ekspertų grupėje. Kaip parodyta 15 paveikslėlyje agreguotų sprendimų patikimumą ir ekspertų kiekį sieja greitai slopstantis netiesinis ryšys (Augustinaitis ir kt., 2009).



Šaltinis: Augustinaitis et al., 2009, p. 202

15 pav. **Ekspertų skaičiaus įtaka vertinimo patikimumui**

Remiantis šiais argumentais tyrimui buvo nuspręsta apklausti 9 ekspertus.

Prieš apklausiant ekspertus buvo paruoštas interviu scenarijus (žr. 2 Priedas). Scenarijaus pradžioje buvo aprašytas prisistatymas ir kreipimasis į ekspertus, paminėta rašomo darbo tema ir tyrimo tikslas Taip pat scenarijaus pradžioje paminėta, kad vykdant apklausą bus išlaikytas ekspertų anonimiškumas ir pateikiant rezultatus respondentams bus suteikti kodiniai pavadinimai.

Interviu klausimyną sudaro 7 klausimai, apimantys tokias temas:

- Bendra kibernetinio saugumo situacija Lietuvoje
- Kibernetinio saugumo valstybinėse institucijose būklė
- Kibernetinio saugumo teisinis reglamentavimas
- Tiriamos srities mokymai ir pratybos

- Visuomenės indelis į kibernetinį saugumą

3.1.3. Empirinio tyrimo loginė eiga

Empirinis tyrimas buvo atliekamas 2018 metų spalio 30 – lapkričio 20 dienomis. Tyrimui buvo parinkti kibernetine sauga, tinklų sauga ir informacijos sauga užsiimančių įmonių, bei valstybės institucijų darbuotojai. Tyrimui parinkti teoriniu, teisiniu ir praktiniu lygmeniu dirbantys specialistai. Atrenkant ekspertus buvo ieškoma specialistų, kurių darbo patirtis tiriamoje srityje yra ne mažesnė kaip 5 metai.

Su ekspertais buvo susiekta elektroniniu paštu arba per socialinius tinklus Linkedin ir Facebook, informuojant juos apie norimą atlikti tyrimą. Respondentai buvo informuojami apie tai, kad jų vardai, pavardės, darbovietės nebus viešinamos ir bus išlaikytas anonimiškumas. Visi ekspertai į kuriuos buvo kreiptasi sutiko dalyvauti tyrime. Kai respondentai sutikdavo dalyvauti interviu, jiems būdavo išsiunčiama papildoma informacija apie rašomą darbą, norimą sužinoti informaciją ir interviu klausimynas. šeši ekspertai pageidavo į interviu atsakyti el. paštu, pildant tekstinio redaktoriaus dokumento formą arba per Linkedin platformos susirašinėjimo modulį. Trys ekspertai pageidavo, kad interviu būtų vykdomas telefonu ir davė sutikimą, dėl pokalbio įrašymo. Tais atvejais kai su respondentu buvo bendraujama telefonu, pokalbio įrašas būdavo perklausomas ir jo stenograma perkeliama į tekstinio redaktoriaus dokumentą. Interviu telefonu trukmė nuo 20 iki 25 minučių.

Respondentų užpildytos anketos ir pokalbių stenogramos buvo kaupiamos ir pagal jas vėliau buvo daromas tyrimas. Šiame darbe nėra pateikiami visų anketų tekstai, 3 Priede galima matyti vienos užpildytos anketos pavyzdį. Kartu su anketos tiriamaisiais klausimais buvo fiksuojama eksperto asmens informacija: vardas, pavardė ir įmonė ar organizacija, kurioje jis dirba, tačiau šie duomenys darbe nėra pateikti siekiant užtikrinti ekspertų konfidencialumą. Patogumo dėlei respondentams buvo suteikti kodiniai pavadinimai nuo E1 iki E9, tyrimo rezultatuose būtent šiais kodiniai pavadinimais ir yra įvardijami ekspertai.

3.2. Empirinio tyrimo duomenų analizė

Pirmas klausimas – *Keliais sakiniais apibūdinkite dabartinę kibernetinio saugumo situaciją Lietuvoje – ar situacija gerėja/blogėja palyginus su tuo kas buvo prieš 5 metus?*

Respondentai E2, E6, E9 akcentuoja apie prastą kibernetinės saugos situacija prieš 5 metus ar anksčiau:

a) Privatus sektorius kažkiek rūpinosi saugumu
b) Viešas sektorius beveik nesirūpina tinklo saugumu

c) Valstybės lygmeniu nebuvo paskirta už kibernetinę saugą atsakingų žmonių ar institucijų
d) Egzistavo pavienės institucijos, kurios tik rinkdavo kibernetinių incidentų statistiką
e) Buvo prasta teisinė bazė: nebuvo įstatymais apibrėžta kieno tai yra atsakomybė, nebuvo informacijos paprastiems vartotojams

Septyni iš devynių ekspertų (E1, E2, E4-E6, E8, E9) teigia, kad kibernetinio saugumo situacija Lietuvoje pastaraisiais metais gerėja. Ekspertas E3 sako, kad situacija gerėja po truputį, o ekspertas E7 mano, kad kibernetinio saugumo situacija blogėja. Ekspertai apibūdindami dabartinę kibernetinės saugos situaciją išskiria tokius teigiamus bruožus:

a) Gerėja teisinė bazė: Įsigalioja kibernetinės saugos įstatymas ir BDAR reikalavimai
b) Atsiranda reikalavimai užtikrinti svetainių saugą, numatytos baudos už reikalavimų nevykdymą
c) Kibernetinės saugos priežiūros funkcijos sukoncentruotos vienoje įstaigoje
d) Parengta nacionalinė kibernetinės saugos strategija

Tuo tarpu ekspertas E5 dar paminėjo, kad šiuo metu Lietuva, Estų sukurtoje platformoje Nacionalines kibernetinės saugos indeksas (angl. *National cyber security index*), pagal kibernetinės saugos brandos lygį užimą 4 vietą pasaulyje.

Nors situacija gerėja, bet tuo pačiu stiprėja ir kibernetinės atakos, tobulėja kibernetiniai nusikaltėliai ir didėja bendras atakų kiekis. Ekspertas E4 pažymi, kad organizacijų tinkluose daugėja įvairios tinklo įrangos ir tarnybinių stočių, todėl atsiranda vis daugiau vietų kurias reikia saugoti nuo kibernetinių atakų. Respondentas E7 atkreipė dėmesį, kad nors atakos agresyvėja, bet biudžetas skiriamas šiais sričiai nedidėja. Eksperto E9 nuomonę galima būtų panaudoti kaip apibendrinimą šiam klausimui – Progresas džiugina, yra nuveikta labai daug, tačiau pasaulis nestovi vietoje ir reikalingas pastovus tobulėjimas.

Antras klausimas - *Jūsų nuomone, kokia būtų pagrindiniai skirtumai palyginant Lietuvos privataus ir valstybinio sektorių interneto portalų kibernetinės saugos aspektus - kokie pažeidžiamumai pasitaiko dažniausiai?*

Penkių ekspertų atsakymuose pažymima, kad didelių skirtumų tarp valstybinių institucijų ir privataus kapitalo įmonių interneto portalų ir jų pažeidžiamumų nėra. Tuo tarpu ekspertas E4 mano, kad valstybinių institucijų portalai paprastai būna susieti su duomenų bazėmis ir aplikacijomis, o privataus sektoriaus puslapiai dažniau būna reprezentacinio pobūdžio ir juose yra daugiau statinė informacija, be vartotojų duomenų. Respondentas E2 irgi mato tam tikrus skirtumus, jo nuomone privačiame sektoriuje nuo seno savo portalais privalėjo rūpintis finansų kompanijos, kurioms kibernetiniai incidentai siejasi su tiesioginiai finansiniai nuostoliais.

Kalbėdami apie portalų pažeidžiamumus beveik visi ekspertai išskiria dvi dažniausiai pasitaikančias klaidas: neatnaujinama tarnybinės stoties, bei turinio valdymo sistemos programinė įranga ir klaidos konfigūracijoje ar programiniame kode. Apibendrinant galima įvardinti tokius ekspertų aprašytus svetainių pažeidžiamumus:

- Žiniatinklio tarnybinių stočių pažeidžiamumai
- Programavimo kalbų, skirtų žiniatinkliui kurti, pažeidžiamumai
- Turinio valdymo sistemų pažeidžiamumai

Plačiau reiktų pakomentuoti eksperto E8 atsakymą, jis atkreipia dėmesį į Informacinių technologijų (toliau IT) skyrius privataus ir valstybinio sektoriaus organizacijose. E8 pažymi, kad privačiam sektoriuje IT skyrius dirba išvien su visa organizacija, o valstybiniame sektoriuje IT skyriai yra paprastai izoliuoti nuo likusios organizacijos veiklos ir jos poreikių, todėl IT ir saugos poreikiai turi žemą prioritetą ir negauna pakankamo finansavimo. Būtent toks IT skyriaus atsiribojimas nuo organizacijos sudaro prielaidas nesaugių žiniatinklio portalų egzistavimui valstybiniame sektoriuje.

Ekspertas E9 detaliau panagrinėja skirtingo tipo organizacijų kibernetinės saugos situaciją, siekiant aiškumo jo atsakymas buvo perkeltas į lentelę Nr. 4.

4 lentelė **Valstybinio ir privataus sektoriaus organizacijų portalų apsaugos situacija**

Organizacijos tipas / **Parametras**	**Valstybės įstaigos**	**Didelės privataus sektoriaus įmonės**	**Smulkus ir vidutinis verslas**
Kibernetinės saugos situacija	Gerokai pažengė į priekį (palyginus su tuo kas buvo prieš 5 ar daugiau metų)	Kaip ir anksčiau situacija yra gana gera	Situacija labai bloga
Išlaidos kibernetinei saugai	Didėja	Skiriamos lėšos auga	Lėšų neskiriama arba skiriama labai mažai
Puslapių talpinimas ir portalų sauga	Bendrinės svetainės/portalai yra gana gerai sutvarkyti Daugėja svetainių talpinamų bendroje vyriausybės platformoje Svetainės apsaugomos žiniatinklio aplikacijų ugniasienėmis (angl. WAF) Prasčiau su naujai kuriamomis sistemomis, jų konstravimu ir testavimu (E. sveikata, VRK atvejai).	Yra pakankamai priimtiname lygyje	Talpinama pas atsitiktinius debesijos paslaugų teikėjus Svetainės tinkamai nesaugomos ir neatnaujinamos

Šaltinis: parengta autoriaus pagal Eksperto E9 atsakymus į interviu klausimus

Ekspertas E2 atkreipė dėmesį, kad dabar kibernetiniai nusikaltėliai daugiau taikosi ne sutrikdyti svetainės darbą, o išnaudoti ją savo tikslams – panaudojant pažeidžiamumus perimti informaciją,

įsibrauti į organizacijos vidinį tinklą, pasiekti vidines duomenų bazes arba įdarbinti portalus kriptovaliutų kasimui. Tuo tarpu ekspertas E5 pabrėžia, kad šiuo metu portalų valdytojams nėra privalomų reikalavimų užtikrinti svetainės kodo higieną ir savalaikius programinės įrangos atnaujinimus, reikalingas įstatyminės bazės papildymas šiuo klausimu.

Trečias klausimas - *Kaip manote kas valstybinėms institucijoms ir organizacijoms labiausiai trukdo turėti patikimus ir saugius internetinius portalus? Kokiomis priemonėmis ir kokiais techniniais ir/ar organizaciniais kibernetinės saugos valdymo sprendimais siūlytumėte efektyvinti kibernetinį saugumą valstybinėse institucijose?*

Respondentų dažniausiai minimas valstybinių institucijų saugių internetinių portalų egzistavimo trikdis yra kompetentingų ir kvalifikuotų specialistų trūkumas (taip atsakė penki iš devynių ekspertų). Kitas dažnai ekspertų anketose pasitaikęs pastebėjimas buvo reikalavimų saugoti portalus nebuvimas organizaciniame ir teisiniame lygmenyje (taip atsakė ekspertai E1, E2 ir E5). Be šių dažniausiai pasitaikančių netobulumų valstybinėse organizacijose, respondentai taip pat paminėjo:

a) Saugos reikalavimų tiekėjams nebuvimas, perkant portalų kūrimo paslaugas
b) Reikalavimų periodiniam portalų saugumo patikrinimui nebuvimas
c) Nepakankama atsakomybė ir baudos už kibernetinės saugos priemonių nevykdymą ar nekokybišką įgyvendinimą
d) Kvalifikacinių reikalavimų testuotojams nebuvimą perkant pažeidžiamumų patikros paslaugas
e) Skiriamos nepakankamos lėšos esamų ir naujų darbuotojų atlyginimams
f) Profesionalus palaikymas iš išorės nėra perkamas
g) Kompetencijų išsklaidymas ir dedikuotų saugos specialistų nebuvimas

Kalbant apie technines ir organizacines priemones, kurios galėtų padėti pagerinti portalų kibernetinę saugą vieningo sutarimo tarp ekspertų nėra. Apibendrinant respondentų pasiūlymus, galima sudaryti tokį rekomendacijų sąrašą:

a) Valstybės lygmeniu turi būti kiek įmanoma detaliau aprašyti privalomi reikalavimai portalų saugumui
b) Valstybės lygmeniu galėtų būti patvirtintas sąrašas platformų, kurios tinkamos valstybės institucijų portalų kūrimui
c) Organizacijos vykdydamos naujų žiniatinklio aplikacijų ir portalų sukūrimo pirkimus turi į reikalavimus įtraukti principų „saugumą pagal dizainą“ ir „ numatytąjį saugumą“ (angl.

„*security by design*“ ir „*security by default*“) laikymosi punktus, bei numatyti tiekėjų atsakomybę jei bus pateiktas nesaugus produktas

d) Organizacijos turi periodiškai vykdyti portalų saugumo patikras. Patikras turėtų atlikti tik tam tikrus reikalavimus atitinkančios kompanijos. Per patikrinimus aptiktos portalų spragos ir pažeidžiamumai turi būti taisomi

e) Organizacijos turi skirti pakankamai lėšų saugos įrangai, paslaugoms ir jų palaikymui, bei techninėms konsultacijoms įsigyti

f) Portalus saugoti pasitelkiant žiniatinklio aplikacijų ugniasienę (WAF)

g) Dauguma valstybinių įstaigų turėtų savo portalus perkelti į specializuotą valstybės institucijų svetainių talpinimo platformą

h) Turi atsirasti įstaigos vadovo atsakomybė, tame tarpe ir finansinė, už saugos reikalavimų nesilaikymą. Turi būti reglamentuoti ir aprašyti darbuotojų veiksmai ir atsakomybės.

i) Turi būti didinamas atlyginimų fondas kibernetinės saugos specialistams ir skiriamos lėšos naujų darbuotojų įdarbinimui

j) Turi būti skiriamos lėšos kibernetinės saugos specialistų mokymams ir dalyvavimui konferencijose

Ketvirtas klausimas - *Ar šiuo metu Lietuvos vyriausybės ir ministerijų pradėtas vykdyti Valstybės informacinių išteklių infrastruktūros ir tinklų konsolidavimas turės įtakos valstybinių institucijų portalų kibernetinei apsaugai? Jeigu taip tai kokios?*

Šiuo klausimu ekspertų nuomonė buvo vieninga, net septyni iš devynių ekspertų apie valstybinių išteklių ir kibernetinės saugos konsolidavimą, atsiliepė teigiamai. Daugelio ekspertų nuomone konsolidavimas gali padėti išspręsti net kelias ankstesniuose klausimuose išskirtas problemas:

- Kvalifikuotų specialistų trūkumą, nes centralizuotai sistemai prižiūrėti reikės mažiau specialistų ir jų atlyginimams bus galima skirti didesnį lėšų kiekį
- Portalų talpinimo platformos suvienodinimas turėtų palengvinti saugumo užtikrinimą, nes vietoje šimtų skirtingų platformų reikės prižiūrėti tik vieną ar dvi
- Portalų priežiūrai bus taikomi vienodi saugumo reikalavimai, bus galima vieningai ir nuolatos vykdyti jų saugumo patikrinimus
- Esant centralizuotai tarnybinių stočių ir portalų kibernetinei apsaugai, kiekvienai organizacijai nebereikės atskirai pirkti saugumo techninės ir programinės įrangos, vykdyti jos nuolatinės priežiūros. Bus taupomos valstybės lėšos
- Organizacijoms reikės mažiau techninio personalo, nes nemažai atsakomybių persikels ant konsoliduoto duomenų centro valdytojo pečių

- Procesų kontrolė ir darbuotojų, bei vadovų atsakomybė už sistemų saugumą bus tiksliau reglamentuotos

Nežiūrint visų išvardintų konsolidavimo pliusų ekspertai E6 ir E9 atkreipia dėmesį, kad labai svarbu užtikrinti viso šio projekto saugą. Konsoliduojant viską po vienu stogu, reiškia, kad viskas dirba per vieną infrastruktūrą, vieną tarnybinių stočių rėžį, toks valstybinių resursų sukoncentravimas atkreipia kibernetinių nusikaltėlių dėmesį. Jei nusikaltėliams pavyktų išlaužti bent vieną iš portalų ar žiniatinklio aplikacijų, tikėtina jei galėtų patekti ir į kitas sukonsoliduotoje infrastruktūroje veikiančias sistemas. Sukompromitavus dalį sistemų galima padaryti neigiamą poveikį valstybės veikimui visos šalies mastu. Sukoncentruotą infrastruktūra gali būti sudėtinga ginti nuo išorinių atakų. Taigi labai svarbu šiame sprendime nepamiršti kibernetinės saugos ir ją kiek įmanoma labiau stiprinti.

Penktas klausimas - *Kokia jūsų nuomone yra situacija su teisiniu kibernetinės saugos reglamentavimu Lietuvoje? Ar pakankamai aiškiai yra aprašyta institucijų atsakomybė už savo valdomus informacinius išteklius ir internetinius portalus? Ką jūs siūlytumėte tobulinti?*

Dauguma į šį klausimą atsakiusių ekspertų (dėl žinių trūkumo trys ekspertai neatsakė) teigia, kad teisinio reglamentavimo užtenka ir jis su kiekviena diena gerėja. Ekspertai E1, E2 ir E6 atkreipia dėmesį į netinkamą valstybinių institucijų atsakomybės už padarytus ar nepadarytus veiksmus kibernetinės saugos klausimu reglamentavimą, formuluočių netinkamumą ir atnaujinimo poreikį. Ekspertas E6 taip pat sako, kad šiuo metu privačiam ir valstybės sektoriui nustatytos baudos ir atsakomybės už netinkamai ar iš vis neįvykdytus kibernetinius reikalavimus yra nevienodos, jas reiktų suvienodinti. Dabar nustatyti baudų dydžiai valstybiniam sektoriui yra mažesni ir taip skriaudžiamas privatus sektorius, o valstybės sektorius nėra skatinamas laikytis kibernetinės saugos įstatymo.

Respondentai E2 ir E8 siūlo tobulinti esamus kibernetinės saugos reikalavimus įstatymuose. Ekspertas E2 mano, kad dalis teisės aktų yra jau pasenę ir reikalingas jų atnaujinimus pagal dabartinę situaciją: turėtų būti peržiūrėtos internetinių portalų reglamentavimas, sistemų klasifikavimas, administracinės ir techninės priemonės kiekvienai kategorijai. Tuo tarpu ekspertas E8 mato daug neaiškių reikalavimų, kurių reikalingumas ir kaštų adekvatumas yra abejotini. Jo nuomone Lietuvoje akivaizdžiai trūksta teisininkų su kibernetinio saugumo ir informacijos saugos patirtimi arba saugos specialistų su teisės žiniomis.

Šeštas klausimas - *Ar Lietuvos Krašto apsaugos ministerijos organizuojamos kibernetinės saugos pratybos prisideda prie valstybės institucijų parengtumo atremti kibernetines atakas apsaugant interneto portalus didinimo? Ką šiuo atveju siūlytumėte tobulinti?*

Ekspertų atsakymus iš šį klausimą galima suskirstyti į tris grupes: didžiausia dalis (penki ekspertai – E1, E2, E5, E6 ir E9) laikosi nuomonės, kad šiuo metu organizuojamos kibernetinės saugos pratybos yra tinkamos ir teikia daug naudos; trys ekspertai (E3, E7 ir E8) mano, kad pratybų nauda minimali ar jos iš vis nėra; vienas ekspertas (E4) neturėjo informacijos apie pratybas ir į klausimą neatsakė. Ekspertų

E2, E6 ir E9 nuomone labai gerai, kad šiuo metu Krašto apsaugos ministerijos vykdomose pratybose yra tikrinamos ir techninės, ir organizacinės kibernetinės saugos žinios. Respondentai E2 ir E9 pažymi, kad dabar organizuojamų pratybų formatą labai papildytų ir išplėstų mokymų prieš pratybas organizavimas. Ypač gerai būtų, jei pratybose iš pradžių būtų mokoma kaip aptikti ir sustabdyti kibernetines atakas, kaip surinkti įkalčius ir kaip organizuoti kibernetinių incidentų sprendimo darbą, o po mokymų vyktų pačios pratybos, kurių metu organizacijų specialistai galėtų patikrinti įgytas žinias. Ekspertas E2 mano, kad pratybos galėtų vykti dažniau, o ekspertas E9 kaip tik rekomenduoja orientuotis ne į kiekybę, o į kokybę.

Respondentai E8 ir E9 atkreipia dėmesį, kad dabar organizuojamose pratybose dažnai imituojamos nerealistiškos situacijos. Jų nuomone reikėtų daugiau su tikromis situacijomis susietų pratybų užduočių, nes tik tokiu būdu bus galima įgyti naudingų žinių. Apibendrinant galima būtų pasakyti, kad tokios pratybos yra tikrai naudingos, ypač toms institucijom, kurios pačios nesugeba išmokyti savo darbuotojų tinkamai reaguoti į kibernetinius incidentus, pildyti nacionalinio kibernetinės saugos centro pateiktas formas ir rinkti informaciją apie incidentus.

Septintas klausimas - *Kaip prie valstybinių institucijų internetinių portalų kibernetinės saugos tobulinimo galėtų prisidėti Lietuvos visuomenė?*

Kalbant apie visuomenės indelį į portalų apsauga, daugelis ekspertų paminėjo Lietuvos teisinės bazės trūkumus susijusius su atsakingu pranešimu apie aptiktas spragas. Dabartiniame teisiniame reglamentavime yra aprašyta galimybė visuomenės atstovui pranešti apie pažeidimus aptiktus kažkokios organizacijos informacinėje sistemoje ar portale, tačiau nėra numatyta teisinio neliečiamumo pranešėjui. Ekspertas E5 siūlo įstatyme numatyti visuomenės atstovui aptikusiam spragą internetiniame portale ar informacinės sistemoje per 48 valandas informuoti NKSC ir jei informavimas vyko tinkamai (jei prieš kreipiantis į NKSC pažeidžiamumas nebuvo viešinamas internete) suteikti piliečiui teisinę neliečiamybę. Respondentai E3 ir E9 abejoja plačiosios visuomenės galimybėmis dalyvauti portalų spragų paieškose ir kibernetinio saugumo stiprinime, nes paprastai tai moka tik siauras specialistų ratas.

Ekspertas E9 detaliau nagrinėja ką dar reik padaryti norint pagerinti plačiosios visuomenės supratimą apie kibernetinę saugą:

- Visuomenės švietimas ir pasakojimas apie grėsmes yra labai svarbus
- Valstybinis sektorius galėtų labiau įsitraukti į visuomenės švietimą kibernetinės saugos klausimais
- Reikia mažinti žmonių neatidumą ir lengvatikiškumą, nes šie būdo bruožai yra dažniausiai išnaudojami kibernetinių nusikaltėlių
- Visuomenė turi išmokti atpažinti kibernetines grėsmes ir kilus įtarimui, kad portalas veikia netinkamai arba nukreipiama į kita svetainę nesisijusią su portalo tema – informuoti NKSC

IŠVADOS IR PASIŪLYMAI

1. Išanalizavus teorinius Portalų apsaugos sampratos, portalų apsaugos elementų, svetainių architektūros aspektus , bei atlikus dažniausiai daromų konfigūracijos klaidų, vykdomų atakų, ir kylančių kibernetinių grėsmių, bei priemonių toms grėsmėms tvarkyti analizę galima daryti išvada, kad daugelis problemų yra susiję su žmogiškuoju faktoriumi. Programuotojai pamiršta pakeisti gamyklinius programinės įrangos nustatymus, bei slaptažodžius arba klaidingai ir nesaugiai suprogramuoja svetaines ar jų elementus, nesilaiko gerųjų praktikų dažniausiai pasitaikančių atakų išvengimui. Įgyvendinant kibernetinės saugos valdymo priemones diegėjai pasirenka netinkamus metodus, padaro klaidingus pradinius sprendimus ir siekia iškart maksimaliai gero rezultato, prieš tai tinkamai nepasiruošę.
2. Atsižvelgiant į užsienio šalių (Jungtinių Amerikos Valstijų ir Nyderlandų) praktiką, kibernetinės saugos valdymo vystymąsi, esamą teisinį reglamentavimą ir realią kibernetinės saugos padėtį, bei atlikus lyginamąją analizę, galima daryti išvadą, kad norint pasiekti draugiškų gyventojams, patikimų ir atsparių kibernetiniams įsibrovimams valstybės portalų būseną nebūtina investuoti didelių lėšų ir pasitelkti daugybę specialistų (Jungtinių Amerikos Valstijų atvejis), nebūtina kurti sudėtingų valdymo schemų, bei sunkiai suprantamų įstatymų (Lietuvos atvejis), o galima viską pasiekti per minimalizmą, žengiant į priekį mažais žingsneliais, bet patikimai (Nyderlandų atvejis). Reikia pasimokyti iš Nyderlandų kibernetinės saugos modelio: Kibernetinės saugos strategija kuriama trumpam laikotarpiui, su realistiškais įvykdomais uždaviniais, naudojamas minimalus užtektinas teisinis reglamentavimas ir gyventojams sudaroma galimybė prisidėti prie svetainių saugos tobulinimo per Koordinuoto spragų atskleidimo programą.

3. Analizės išvados labai nenutolo ir nuo ekspertų apklausos rezultatų. Apklaustų ekspertų nuomone, Lietuvos kibernetinės saugos situacija yra gerame stovyje ir matomas akivaizdus tobulėjimas per pastaruosius 5 metus (įsigaliojo Kibernetinės saugos įstatymas ir BDAR reikalavimai, parengta Nacionalinė kibernetinės saugos strategija, kibernetinės saugos priežiūra sukoncentruojama vienose rankose). Nepaisant to, vos ne vieningai pastebėta, jog vis dar skiriama nepakankamai dėmesio didžiajai daliai esminių ir labai paprastu žiniatinklių serveriuose ir turinio valdymo sistemose sutinkamu klaidų (neištaisomi žiniatinklio tarnybinių stočių pažeidžiamumai, neatnaujinama turinio valdymo sistema, konfigūruojant svetaines nesilaikoma rekomendacijų).

Pagal padarytas išvadas teikiami tokie pasiūlymai:

- Siūlytina kuriant naują ar atnaujinant esamą Nacionalinę kibernetinės saugos strategiją sumažinti strategijoje numatytų uždavinių kiekį, padaryti juos realistiškesnius ir sutrumpinti galutinį įvykdymo terminą arba padaryti kelis trumpesnius etapus ties kuriais būtų patikrinama pasiekti rezultatai. Tokį Nacionalinės kibernetinės saugos strategijos modelį taiko Nyderlandai ir jiems gerai sekasi įvykdyti užsibrėžtus tikslus ir laiku ją atnaujinti.
- Siūlytina kuriant Atsakingo pažeidžiamumų atskleidimo įstatymą ar tvarką pasiremti geruoju Nyderlandų pavyzdžiu šioje srityje. Galima būtų pasinaudoti Nyderlandų įgyta patirtimi su teisinga formuluote, ankstesniame jų įstatyme buvo naudojamas terminas „Atsakingas atskleidimas“ (tokiu būdu perkeliant atsakomybę tik ant pranešančiojo), o naujajame naudojamas terminas „Koordinuotas atskleidimas“, tokiu būdu perkeldamas atsakomybę abiem dalyvaujančioms pusėms. Tokiame įstatyme ar tvarkoje turėtų būti numatyta visi Atsakingo atskleidimo dalyviai: organizacija, kuriai priklauso informacinė sistema ir kuri paskelbė informacija apie vykdomą Atsakingo atskleidimo programą; Pranešančioji pusė, atsakinga už savo pačios veiksmus ir besilaikanti proporcingumo principo (tikrinimo metu nedaryti nieko daugiau nei reikia tam, kad surinktum informaciją apie pažeidžiamumą); Nacionalinis kibernetinės saugos centras dalyvauja informacijos mainuose arba jei pranešančioji pusė to nori, gali būti tarpininku tarp pranešančiojo ir Atsakingo atskleidimo programą rengiančia organizacija.
- Siūlytina įpareigoti naujų informacinių sistemų ar portalų kūrėjus taikyti principus Saugus pagal nutylėjimą (Secure by default) ir Saugus pagal dizainą (Secure by design), kas leistų išvengti dažnai pasitaikančių klaidingos konfigūracijos sukuriamų pažeidžiamumų.
- Būtų naudinga jei Lietuvoje už kibernetinę sauga atsakingos institucijos irgi parengtų tokia kibernetinės saugos, informacijos saugos ir fizinės saugos įstatymų, tvarkų ir rekomendacijų rodyklė kokią yra parengęs Jungtinių Amerikos Valstijų Gynybos ministerijos Informacijos analizės centras (1 Priedas). Tokiame dokumente galėtų būti patogiai pateiktos nuorodos į visus Lietuvoje galiojančius teisės aktus, strategijas, nutarimus ir rekomendacijas. Tokio dokumento atsiradimas palengvintų institucijų prižiūrinčių ir saugančių savo informacines sistemas, duomenų bazes ir portalus darbą. Dokumentas turėtų būti skelbiamas jį parengusios institucijos portale ir atsiradus pakeitimų atnaujinamas.

LITERATŪROS SĄRAŠAS

1. *10 Basic Cybersecurity Measures. Best Practices to Reduce Exploitable Weaknesses and Attacks*, WaterISAC Security Information Center, 2015. Prieiga per internetą https://www.waterisac.org/sites/default/files/public/10_Basic_Cybersecurity_Measures-WaterISAC_June2015_0.pdf
2. *10 Ways to Prevent Cyber Attacks*, The Capacity Group. Prieiga per internetą https://capcoverage.com/index.php/10-ways-to-prevent-cyber-attacks/
3. 2015 metų CERT-LT veiklos ataskaita. Prieiga per internetą: https://www.nksc.lt/doc/2015.pdf
4. 2016 metų CERT-LT veiklos ataskaita. Prieiga per internetą: https://www.nksc.lt/doc/2016.pdf
5. 2017 metų CERT-LT veiklos ataskaita. Prieiga per internetą: https://www.nksc.lt/doc/2017.pdf
6. 2018 metų NKSC nacionalinio kibernetinio saugumo būklės ataskaita. Prieiga per internetą: https://www.nksc.lt/doc/NKSC_ataskaita_2018.pdf
7. 2019 metų NKSC nacionalinio kibernetinio saugumo būklės ataskaita. Prieiga per internetą: https://www.nksc.lt/doc/Nacionalinio_kibernetinio_saugumo_bukles_ataskaita_2019.pdf
8. *A Layered Approach to Cybersecurity: People, Processes, and Technology*, IDG Communications, Inc, 2018. Prieiga per internetą https://www.csoonline.com/article/3326301/a-layered-approach-to-cybersecurity-people-processes-and-technology.html
9. *Annual number of data breaches and exposed records in the United States from 2005 to 2019*, Statista, 2020. Prieiga per internetą https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/
10. Augustinaitis A. et al. *Lietuvos E. Valdžios gairės: Ateities įžvalgų tyrumas*, Mykolo Romerio universitetas, 2009
11. Baker S., Schneck-Teplinsky M. *Spurring the Private Sector: Indirect Federal Regulation of Cybersecurity in the US*. In: Ghosh S., Turrini E. (eds) Cybercrimes: A Multidisciplinary Analysis. Springer, Berlin, Heidelberg, 2011
12. Bellovin S. M. et al. *Limiting the undesired impact of cyber weapons: technical requirements and policy implications*, Journal of Cybersecurity, Volume 3, Issue 1, 1 March 2017, Pages 59–68
13. Borky J. M., Bradley T. H. *Protecting Information with Cybersecurity*. In: Effective Model-Based Systems Engineering. Springer, Cham, 2018

14. *Challenges In Implementing Cyber Security*. SiriNiti, 2019. Prieiga per internetą: http://siriniti.net/challenges-in-implementing-cyber-security.php
15. Charlet K. *Understanding Federal Cybersecurity,* The Cyber Security Project, 2018. Prieiga per internetą: https://www.belfercenter.org/sites/default/files/files/publication/Understanding%20Federal%20Cybersecurity%2004-2018_0.pdf
16. *Checklist of Requirements for Federal Websites and Digital Services. The relevant laws, policies, and regulations for federal agencies,* Digital.gov, 2020. Prieiga per internetą: https://digital.gov/resources/checklist-of-requirements-for-federal-digital-services/
17. Choraś M. et al. *Cyber Threats Impacting Critical Infrastructures*. In: Setola R., Rosato V., Kyriakides E., Rome E. (eds) Managing the Complexity of Critical Infrastructures. Studies in Systems, Decision and Control, vol 90. Springer, Cham. 2016
18. Christou G. *National Cybersecurity Approaches in the European Union: The Case of the UK. In: Cybersecurity in the European Union. New Security Challenges Series*. Palgrave Macmillan, London, 2016
19. *Coordinated Vulnerability Disclosure: The Guideline*, Nationaal Cyber Security Centre, 2018. Prieiga per internetą: https://english.ncsc.nl/publications/publications/2019/juni/01/coordinated-vulnerability-disclosure-the-guideline
20. Craig A. *SEC Cyber Briefing: Regulatory Expectations for 2019,* Harward Law School Forumo n Corporate Governance, 2019. Prieiga per internetą: https://corpgov.law.harvard.edu/2019/01/02/sec-cyber-briefing-regulatory-expectations-for-2019/
21. *Cyber Security Assessment Netherlands,* National Coordinator for Security and Counterterrorism, 2019. Prieiga per internetą: https://english.ncsc.nl/topics/cybersecurity-assessment-netherlands/documents/publications/2019/09/13/cyber-secrurity-assessment-netherlands-2019
22. *Cyber Security Planning Guide*, Federal Communications Commission. Prieiga per internetą https://transition.fcc.gov/cyber/cyberplanner.pdf
23. *Cybersecurity funding,* White house, 2019. Prieiga per internetą: https://www.whitehouse.gov/wp-content/uploads/2019/03/ap_24_cyber_security-fy2020.pdf
24. *DoD Cybersecurity Chart, DOD CSIAC, 2020.* Prieiga per internetą: https://dodiac.dtic.mil/wp-content/uploads/2020/04/ia-policychart-1-Apr-20-DoDIN.pdf

25. *Dutch Digitalisation Strategy 2.0,* 2018. Prieiga per internetą: https://www.nederlanddigitaal.nl/english/dutch-digitalisation-strategy-2.0
26. *Dutch Digitalisation Strategy,* 2018. *Prieiga per internetą:* https://www.nederlanddigitaal.nl/english/dutch-digitalisation-strategy
27. *Dutch National Cyber Security Agenda*, ENISA, 2018. Prieiga per internetą: https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/strategies/national-cyber-security-strategy-1/@@download_version/82b3c1a34de449f48cef8534b513caea/file_en
28. *Executive Order 13800 Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, Federal Register/Vol. 82, No. 93/Tuesday, May 16, 2017. Prieiga per internetą: https://fas.org/irp/offdocs/eo/eo-13800.pdf
29. *Federal Cybersecurity Risk Determination Report and Action Plan,* White house, 2018. Prieiga per internetą: https://www.whitehouse.gov/wp-content/uploads/2018/05/Cybersecurity-Risk-Determination-Report-FINAL_May-2018-Release.pdf
30. *Global Cybersecurity Index 2018 (GCI),* ITU Publications, 2019. Prieiga per internetą: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
31. Great Britain National cyber security center. White paper *Common cyber attacks: reducing the impact* 2016. Prieiga per internetą: https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/common_cyber_attacks_ncsc.pdf
32. *Guideline for responsible disclosure of IT vulnerabilities*, 2013. Prieiga per internetą: https://www.government.nl/latest/news/2013/01/03/guideline-for-responsible-disclosure-of-it-vulnerabilities
33. *H.R.145 - Computer Security Act of 1987*, 100th Congress (1987-1988). Prieiga per internetą: https://www.congress.gov/bill/100th-congress/house-bill/145
34. Hathaway M., Spidalieri F., *The Netherlands Cyber Readiness at a Glance,* Potomac Institute For Policy Studies, 2017. Prieiga per internetą https://www.potomacinstitute.org/images/CRI/FinalCRI20NetherlandsWeb.pdf
35. Heitzenrater C. D., Simpson A. C. *Policy, statistics and questions: Reflections on UK cyber security disclosures*, Journal of Cybersecurity, Volume 2, Issue 1, 1 December 2016, Pages 43–56
36. Hidhaya S.F., Geetha A. *Intrusion Protection against SQL Injection and Cross Site Scripting Attacks Using a Reverse Proxy*. In: Thampi S.M., Zomaya A.Y., Strufe T., Alcaraz Calero J.M., Thomas T. (eds) Recent Trends in Computer Networks and Distributed Systems

Security. SNDS 2012. Communications in Computer and Information Science, vol 335. Springer, Berlin, Heidelberg, 2012

37. Ikamas K., *Interneto istorija Lietuvoje: kodėl mes turime greičiausią internetą*, DELFI, 2012. Prieiga per internetą: https://www.delfi.lt/projektai/archive/interneto-istorija-lietuvoje-kodel-mes-turime-greiciausia-interneta.d?id=59731045
38. Jonathan Clough. *The Council of Europe Convention on Cybercrime: Defining `Crime' in a Digital World.* Criminal Law Forum 2012, Volume 23, Issue 4, pp 363–391. Springer
39. *Kibernetinio saugumo aplinka Lietuvoje* Valstybės audito ataskaita, 2015. Prieiga per internetą: https://www.vkontrole.lt/failas.aspx?id=3497
40. *Kokybiniai tyrimai*, Socialinės Informacijos Centras, 2020. Prieiga per internetą http://www.sic.lt/index.php/lt/p/tyrimu-metodai/kokybiniai-tyrimai
41. Kurose M., *Cybersecurity Regulation – How are U.S. Policies Evolving to Combat New Threats?* Envision,*2019.* Prieiga per internetą: https://www.envisionsuccess.net/blog/cybersecurity-regulation
42. Leopold H. *Cyber Situational Awareness*, 132: 97, Springer, Vienna, 2015
43. *Lietuvos Respublikos Asmens duomenų teisinės apsaugos įstatymas* // Valstybės žinios, 1996-07-03, Nr. 63-1479.
44. *Lietuvos Respublikos Kibernetinio saugumo įstatymas* // TAR, 2014-12-23, Nr. 20553
45. Liu CH. et al. *The Enhancement of Security in Healthcare Information Systems*. J Med Syst (2012) 36: 1673, Springer, US
46. Moschovitis C. *Why do cyber security programmes fail?* Cyber Security: A Peer-Reviewed Journal, Vol. 2, 4 303–309, 2019
47. Muscat I., *What Are Injection Attacks,* Acunetix, 2019. Prieiga per internetą: https://www.acunetix.com/blog/articles/injection-attacks/
48. *National cyber strategy of United States of America*, 2018. Prieiga per internetą: https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
49. Nelson O. *Cybersecurity Laws – A Complete Overview*. Cyberexperts, 2019. Prieiga per internetą: https://cyberexperts.com/cybersecurity-laws
50. *NL – Cybersecurity Legislation in the Netherlands*. Prieiga per internetą: https://tedangevaare.nl/nl/
51. *Number of cyber security incident reports by federal agencies in the United States from FY 2006 to 2018*, Statista, 2020. Prieiga per internetą https://www.statista.com/statistics/677015/number-cyber-incident-reported-usa-gov/
52. *Nutarimas dėl bendrųjų reikalavimų valstybės institucijų interneto svetainėms patvirtinimo* // Valstybės žinios, 2003-04-24, Nr. 38-1739

53. *Nutarimas Dėl duomenų apsaugos valstybės ir vietos savivaldos informacinėse sistemose // Valstybės žinios, 1997-09-10, Nr. 83-2075*
54. *Nutarimas dėl elektroninės informacijos saugos (kibernetinio saugumo) plėtros 2011–2019 metais programos patvirtinimo* // Valstybės žinios, 2011-07-09, Nr. 83-4033
55. *Nutarimas dėl informacijos technologijų saugos valstybinės strategijos ir jos įgyvendinimo plano patvirtinimo* // Valstybės žinios, 2001-12-29, Nr. 110-4006
56. *Nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo* // TAR, 2018-08-21, Nr. 13252
57. *Nutarimas dėl nacionalinio saugumo strategijos patvirtinimo* // Valstybės žinios, 2002-06-07, Nr. 56-2233
58. *OWASP Top 10 – 2017 The Ten most Critical Web Application Security Risks*, OWASP Foundation, 2017. Prieiga per internetą https://owasp.org/www-pdf-archive/OWASP_Top_10-2017_%28en%29.pdf.pdf
59. *Pagrindiniai web sistemų pažeidžiamumai ir saugos būdai,* Litnet CERT, 2015 Prieiga per internetą https://cert.litnet.lt/2015/05/pagrindiniai-web-sistemu-pazeidziamumai-ir-saugos-budai-5/
60. *Patvirtintos artimiausių metų valstybės kibernetinio saugumo stiprinimo priemonės,* LRV, 2019. Prieiga per internetą: https://lrv.lt/lt/naujienos/patvirtintos-artimiausiu-metu-valstybes-kibernetinio-saugumo-stiprinimo-priemones
61. Petratos P. *Cybersecurity in Europe: Cooperation and Investment.* In: Carayannis E., Campbell D., Efthymiopoulos M. (eds) Cyber-Development, Cyber-Democracy and Cyber-Defense. Springer, New York, NY, 2014
62. Pettit S., *Anatomy of web application: Security considerations*, Sanctum Inc, 2001
63. Rademaker M. et al, *Dutch investments in ICT and cybersecurity. Putting it in perspective.*, The Hague Centre for Strategic Studies, 2016
64. Rikk R., *National Cyber Security Index 2018,* e-Governance Academy, 2018. Prieiga per internetą: https://ncsi.ega.ee/country/lt/
65. Romanosky S. *Examining the costs and causes of cyber incidents.* Journal of Cybersecurity, Volume 2, Issue 2, 1 December 2016, Pages 121–135
66. Rupšienė L *Kokybinio tyrimo duomenų rinkimo metodologija*, Klaipėdos universitetas, 2007
67. *Shred-it Study Exposes Employee Negligence as Top Information Security Risk to U.S. Businesses,* Shred-it, 2018. Prieiga per internetą <https://www.shredit.com/en-us/about/press-room/press-releases/sacking-employees-for-data-breach-negligence>

68. Stavrou A. et al. *A Pay-per-Use DoS Protection Mechanism for the Web*. In: Jakobsson M., Yung M., Zhou J. (eds) Applied Cryptography and Network Security. ACNS 2004. Lecture Notes in Computer Science, vol 3089. Springer, Berlin, Heidelberg, 2004
69. Tamošauskas Ž. R., *Pamokos iš užsienio: atsakingo kibernetinio saugumo spragų atskleidimo praktika*, KURKIT, 2019. Prieiga per internetą: http://kurklt.lt/wp-content/uploads/2019/03/U%C5%BEsienio-praktik%C5%B3-dokumentas-.pdf
70. Telalev A., *5 reasons why website security is important in 2018*, WebARX, 2018. Prieiga per internet https://www.webarxsecurity.com/5-reasons-website-security-important-2018/
71. *The five most common cyber security mistakes. Management's perspective on cyber security*. KPMG Advisory, 2013. Prieiga per internetą: https://assets.kpmg/content/dam/kpmg/tr/pdf/2017/01/five-most-common-cyber-security-mistakes.PDF
72. *The Global Risk Report 2019*, World Economic Forum, 2019. Prieiga per internetą https://www.weforum.org/reports/the-global-risks-report-2019
73. Thuraisingham B. *Managing Threats to Web Databases and Cyber Systems*. In: Kumar V., Srivastava J., Lazarevic A. (eds) Managing Cyber Threats. Massive Computing, vol 5. Springer, Boston, MA. 2005
74. Tidikis R. *Socialinių mokslų tyrimų metodologija*, Lietuvos teisės universitetas, 2003
75. *Top 10 Frontend Frameworks of 2018*, Cody Arsenault, 2018. Prieiga per internetą https://www.keycdn.com/blog/front-end-frameworks
76. Townsend K., *Failures in Cybersecurity Fundamentals Still Primary Cause of Compromise: Report*, Securityweek, 2019. Prieiga per internetą https://www.securityweek.com/failures-cybersecurity-fundamentals-still-primary-cause-compromise-report
77. Umesh Hodeghatta R., Umesha N., *The InfoSec Handbook An introduction to Information Security*, Apress open, 2014
78. *Understanding the five types of cybersecurity*, Liberty Center One, 2019. Prieiga per internetą https://libertycenterone.com/blog/understanding-the-five-types-of-cybersecurity#
79. *Web frameworks Market Leaders*, Wappalyzer, 2018. Prieiga per internetą https://www.wappalyzer.com/categories/web-frameworks
80. Wodehouse C., *A Beginner's Guide to Front-End Development*, UpWork, 2017. Prieiga per internetą https://www.upwork.com/hiring/development/beginners-guide-to-front-end-development/
81. Wright L. *Managing Cyber Security*. In: People, Risk, and Security. Palgrave Macmillan, London, 2017

Vaitkevičius J. Valstybės institucijų portalų apsauga kibernetinės saugos valdymo priemonėmis / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas prof. dr. T. Limba – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir verslo fakultetas, 2020

ANOTACIJA

Magistro baigiamajame darbe išnagrinėjus portalų apsaugos sampratos ir apsaugos elementų teorinius aspektus, išanalizavus kibernetinės saugos grėsmes ir kibernetinės saugos valdymo priemonių taikymo rekomendacijas, išanalizavus kibernetinės saugos valdymo priemonių taikymo ypatumus pasaulyje ir Lietuvoje, atlikus kokybinį tyrimą, buvo pateiktos kibernetinės saugos valdymo priemonių pritaikymo Lietuvos valstybės institucijų portalų apsaugai rekomendacijos. Pirmoje darbo dalyje yra analizuojami internetinių portalų apsaugos kibernetinės saugos valdymo priemonėmis teoriniai aspektai, analizė grįsta moksliniais straipsniais, knygomis, bei internetiniais duomenų šaltiniais. Antroje darbo dalyje nagrinėjama portalų apsaugos kibernetinės saugos valdymo priemonėmis pasaulinė patirtis, lyginama Jungtinių Amerikos Valstijų, Nyderlandų ir Lietuvos kibernetinės saugos sritys. Trečioje darbo dalyje pateikta pasirinkta tyrimo metodologija, aprašyta ir pagrįsta kodėl buvo pasirinktas būtent toks tyrimo metodas ir kokio tipo vertinimas bus atliekamas. Galiausiai atlikta empirinio tyrimo rezultatų analizė, bei detaliai išnagrinėjami ekspertų atsakymai.

Pagrindiniai žodžiai: kibernetinio saugumo valdymo priemonės, kibernetinio saugumo grėsmės, internetinių portalų apsauga, valstybės institucijos, kibernetinės saugos strategija, svetainių pažeidžiamumai, kibernetinės saugos įstatymas

Vaitkevičius J. Protection of public authorities portals by cyber security management tools / Master‘s Work in Cyber security Management. Head of the prof. dr T. Limba. - Vilnius: Mykolas Romeris University, Faculty of Economics and business, 2020

ANNOTATION

In the master's thesis after analyzing the theoretical aspects of portal security concept and security elements, analyzing cyber security threats and recommendations for the application of cyber security management measures, analyzing the peculiarities of the application of cyber security management measures in the world and in Lithuania, following a qualitative study, recommendations for the application of cyber security management measures to the protection of portals of Lithuanian state institutions were provided. The first part of the work analyzes the theoretical aspects of the protection of Internet portals by cyber security management tools, the analysis is based on scientific articles, books, and online data sources. The second part of the work examines the global experience of portal security using cyber security management tools, compares the areas of cyber security in the United States, the Netherlands and Lithuania. The third part of the work presents the chosen research methodology, describes and substantiates why this research method was chosen and what type of assessment will be performed. Finally, the analysis of the results of the empirical research is performed, and the answers of the experts are analyzed in detail

Key words: cyber security management tools, cyber security threats, protection of web portals, public authorities, cyber security strategy, website vulnerabilities, cyber security law

Vaitkevičius J. Valstybės institucijų portalų apsauga kibernetinės saugos valdymo priemonėmis / Kibernetinio saugumo valdymo magistro baigiamasis darbas. Vadovas prof. dr. T. Limba – Vilnius: Mykolo Romerio universitetas, Ekonomikos ir verslo fakultetas, 2020

SANTRAUKA

Magistro baigiamojo darbo tikslas - Įvertinus portalų apsaugos kibernetinės saugos valdymo priemones pateikti jų pritaikymo Lietuvos valstybės institucijų portalų apsaugai rekomendacijas. Taip pat siekiama išanalizuoti kibernetinės saugos grėsmes ir kibernetinės saugos valdymo priemonių taikymo teorinius aspektus, išanalizuoti kibernetinės saugos valdymo priemonių taikymo ypatumus pasaulyje ir Lietuvoje.

Kai yra kuriami valstybės institucijų portalai daugiausiai dėmesio yra skiriama turiniui, prieinamumui ir naudojimo patogumui, o apie tinklalapio saugą pradedama galvoti tik vėliau. Dažni atvejai kai portalo spragos yra ištaisomos tik po įvykusių kibernetinių incidentų ar informacijos apie esamus pažeidžiamumus paviešinimo žiniasklaidoje. Magistriniame darbe, remiantis užsienio šalių patirtimi ir teorine informacija, bus siekiama pateikti rekomendacijas dėl kibernetinės saugos priemonių taikymo internetinių portalų apsaugai.

Darbe taikyta literatūros ir dokumentų analizė siekiant išanalizuoti portalų apsaugos sampratą, kibernetinės saugos grėsmių ir kibernetinės saugos priemonių teorinius aspektus. Lyginamoji analizė atlikta siekiant palyginti pasaulio ir Lietuvos patirtį kibernetinės saugos valdymo srityje. Taip pat atliktas kokybinis ekspertų nuomonės tyrimas, kurio metu buvo apklausti 9 ekspertai. Tyrimu siekta išsiaiškinti bendrą kibernetinio saugumo situaciją Lietuvoje, kibernetinio saugumo būklę valstybinėse institucijose, kibernetinio saugumo teisinį reglamentavimą Lietuvoje, galimas visuomenės indėlis į kibernetinį saugumą. Apibendrinus visais metodais surinktus duomenis pateiktos rekomendacijos dėl kibernetinės saugos valdymo priemonių taikymo.

Darbą sudaro 3 dalys: Pirmoje darbo dalyje yra analizuojami internetinių portalų apsaugos kibernetinės saugos valdymo priemonėmis teoriniai aspektai, analizė grįsta moksliniais straipsniais, knygomis, bei internetiniais duomenų šaltiniais. Antroje darbo dalyje nagrinėjama portalų apsaugos kibernetinės saugos valdymo priemonėmis pasaulinė patirtis, lyginama Jungtinių Amerikos Valstijų, Nyderlandų ir Lietuvos kibernetinės saugos sritys. Trečioje darbo dalyje pateikta pasirinkta tyrimo metodologija, aprašyta ir pagrįsta kodėl buvo pasirinktas būtent toks tyrimo metodas ir kokio tipo vertinimas bus atliekamas. Galiausiai atlikta empirinio tyrimo rezultatų analizė, bei detaliai išnagrinėjami ekspertų atsakymai

Vaitkevičius J. Protection of public authorities portals by cyber security management tools / Master‘s Work in Cyber security Management. Head of the prof. dr T. Limba. - Vilnius: Mykolas Romeris University, Faculty of Economics and business, 2020

SUMMARY

The aim of Master’s thesis - After evaluating the cyber security management measures of portal security, to provide recommendations for their application to the security of portals of Lithuanian state institutions. Also, the aim is to analyze cyber security threats and theoretical aspects of the application of cyber security management measures, to analyze the peculiarities of the application of cyber security management measures in the world and in Lithuania.

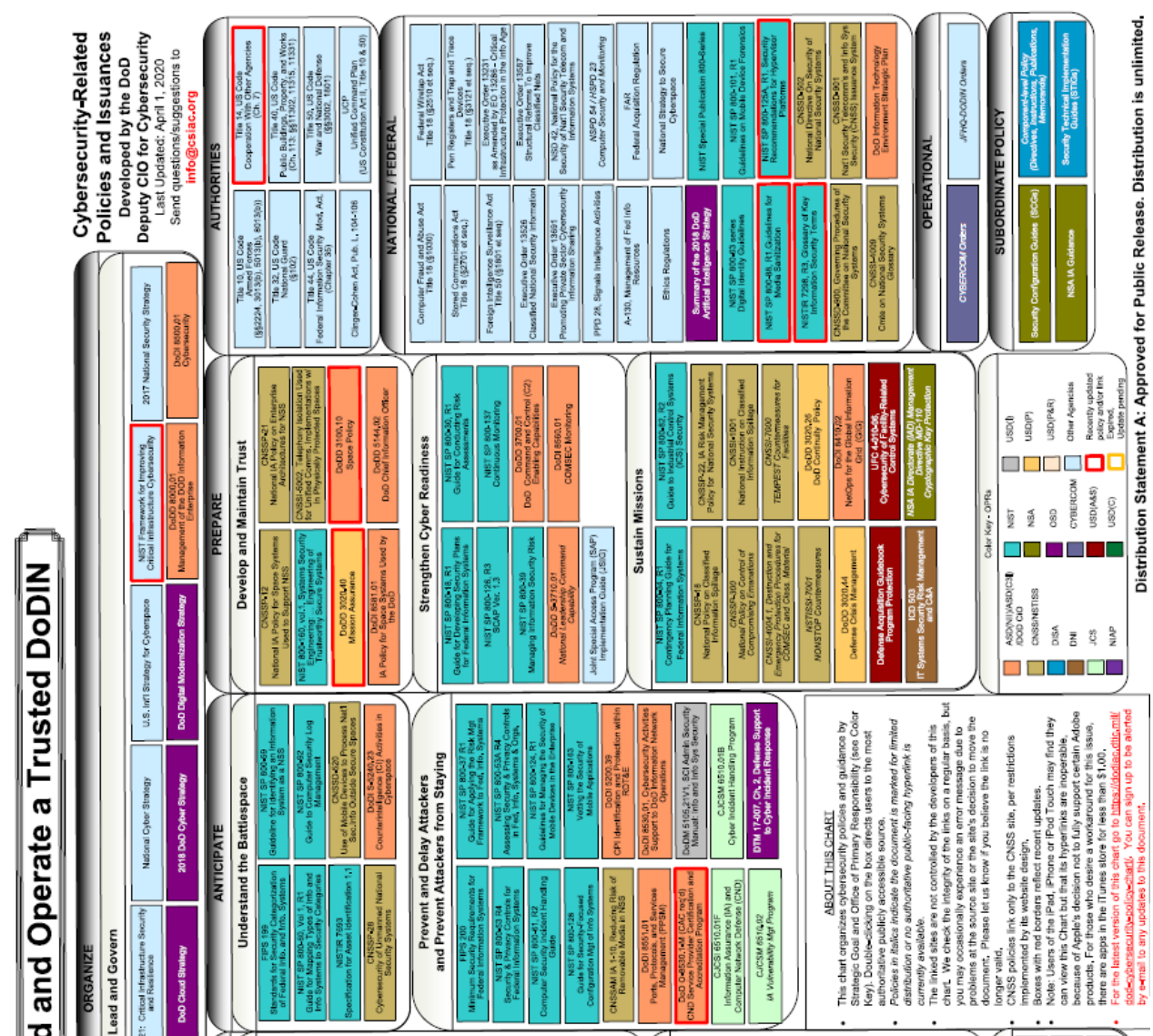
When public authorities' portals are created, the focus is on content, accessibility and ease of use, and the safety of the website is only considered later. Frequent cases where vulnerabilities in the portal are remedied only after cyber incidents or the disclosure of information about existing vulnerabilities in the media. In this work, based on the experience of foreign countries and theoretical information, recommendations on the application of cyber security measures to the protection of Internet portals will be provided.

The analysis of literature and documents was applied in the work in order to analyze the concept of portal security, theoretical aspects of cyber security threats and cyber security measures. The comparative analysis was performed in order to compare the world and Lithuanian experience in the field of cyber security management. A qualitative survey of expert opinions was also conducted, during which 9 experts were interviewed. The aim of the research was to find out the general cyber security situation in Lithuania, the state of cyber security in state institutions, the legal regulation of cyber security in Lithuania, the possible contribution of the society to cyber security. After summarizing the data collected by all methods, recommendations for the application of cyber security management measures are provided.

The first part of the work analyzes the theoretical aspects of the protection of Internet portals by cyber security management tools, the analysis is based on scientific articles, books, and online data sources. The second part of the work examines the global experience of portal security using cyber security management tools, compares the areas of cyber security in the United States, the Netherlands and Lithuania. The third part of the work presents the chosen research methodology, describes and substantiates why this research method was chosen and what type of assessment will be performed. Finally, the analysis of the results of the empirical research is performed, and the answers of the experts are analyzed in detail

PRIEDAI

1 Priedas. Kibernetinio saugumo diagrama-rodyklė (DOD CSIAC, 2020)



2 Priedas. Pusiau struktūrizuoto interviu scenarijus

Laba diena,

Esu Jonas Vaitkevičius, šiuo metu studijuoju Mykolo Romerio universitete Kibernetinio saugumo valdymą ir rašau Magistrinį baigiamąjį darbą. Mano MBD tema „Valstybės institucijų portalų apsauga kibernetinės saugos valdymo priemonėmis“.
Darbo tyrimą nusprendžiau daryti kokybinį – atliekant ekspertų apklausą. Planuoju apklausti 7-9 ekspertus. Jus pasirinkau vienu iš ekspertų.
Darbe nebus minimos tikrosios ekspertų pavardė ir vardai, jie bus sužymėti numeriais.
Prašau užpildyti anketą, atsakant į atviro pobūdžio klausimus.

Ekspertų apklausos klausimynas

1. Keliais sakiniais apibūdinkite dabartinę kibernetinio saugumo situaciją Lietuvoje - ar situacija gerėja/blogėja palyginus su tuo kas buvo prieš 5 metus?
2. Jūsų nuomone, kokia būtų pagrindiniai skirtumai palyginant Lietuvos privataus ir valstybinio sektorių interneto portalų kibernetinės saugos aspektus - kokie pažeidžiamumai pasitaiko dažniausiai?
3. Kaip manote kas valstybinėms institucijoms ir organizacijoms labiausiai trukdo turėti patikimus ir saugius internetinius portalus? Kokiomis priemonėmis ir kokiais techniniais ir/ar organizaciniais kibernetinės saugos valdymo sprendimais siūlytumėte efektyvinti kibernetinį saugumą valstybinėse institucijose?
4. Ar šiuo metu Lietuvos vyriausybės ir ministerijų pradėtas vykdyti Valstybės informacinių išteklių infrastruktūros ir tinklų konsolidavimas turės įtakos valstybinių institucijų portalų kibernetinei apsaugai? Jeigu taip tai kokios?
5. Kokia jūsų nuomone yra situacija su teisiniu kibernetinės saugos reglamentavimu Lietuvoje? Ar pakankamai aiškiai yra aprašyta institucijų atsakomybė už savo valdomus informacinius išteklius ir internetinius portalus? Ką jūs siūlytumėte tobulinti?
6. Ar Lietuvos Krašto apsaugos ministerijos organizuojamos kibernetinės saugos pratybos prisideda prie valstybės institucijų parengtumo atremti kibernetines atakas apsaugant interneto portalus didinimo? Ką šiuo atveju siūlytumėte tobulinti?
7. Kaip prie valstybinių institucijų internetinių portalų kibernetinės saugos tobulinimo galėtų prisidėti Lietuvos visuomenė?

3 Priedas. Eksperto atsakymų aprašymas. Pavyzdys.

Ekspertas E9

1. Keliais sakiniais apibūdinkite dabartinę kibernetinio saugumo situaciją Lietuvoje - ar situacija gerėja/blogėja palyginus su tuo kas buvo prieš 5 metus?
   Progresas be abejo matosi. Lyginant prieš 5 metus yra labai pasistūmėta teisinėje bazėje. NKSC sukūrimas ir kompetencijų ten atsiradimas yra dideli žingsniai į priekį. Taigi iš esmės tikrai galima pripažinti, kad progresas yra, bet reikia suprasti, kad ir grėsmės nestovi vietoje, jos taipogi sparčiai vystosi. Jei lygintume tas grėsmes, kurios buvo prieš 5 metus ir kokios yra dabar tai galime matyti, kad dabar grėsmės yra stipriai išaugusios. Progresas džiugina, bet tikrai dar nesame pasiekia tokią stadiją, kad galėtume pasakyti, kad viskas tikrai jau yra gerai ir bus gerai rytoj.

2. Jūsų nuomone, kokia būtų pagrindiniai skirtumai palyginant Lietuvos privataus ir valstybinio sektorių interneto portalų kibernetinės saugos aspektus - kokie pažeidžiamumai pasitaiko dažniausiai?
   Reikėtų išskirti 3 grupes:
   Valstybės įstaigos, gerokai pažengę į priekį (jei lyginti kas yra dabar ir kas buvo prieš 5 metus), daug svetainių yra sukonsoliduota į vieningą sistemą. Valstybės įstaigos atkreipė dėmesį į Vyriausybės nutarimus ir pradėjo diegtis pas save internetinių aplikacijų ugniasienės (WAF), sauga ženkliai pagerėjusi, dar yra spragų su naujai kuriamomis sistemomis (Esveikata, VRK atvejai). Tai labiau susiję ne su techninių saugumo sprendimų trūkumu, bet labiau su pačių naujų sistemų konstravimu ir testavimu, čia saugumas yra nepakankamas. Bendrinės svetainės (portalai) jau yra gana gerai sutvarkyti ir saugūs.
   Didelės įmonės (enterprise). situacija yra gana gera, ji buvo gan nebloga ir anksčiau, išlaidos kibernetiniai saugai auga, yra pakankamai priimtiname lygyje.
   Smulkus ir vidutinis verslas. situacija labai bloga, nes mažos įmonės neturi savo informacijos saugumo specialistų, puslapius talpina pas atsitiktinius debesijos paslaugų teikėjus. Paprastai tokie tiekėjai nesiūlo turinio valdymo įrankių diegimo ir priežiūros arba tos paslaugos yra per brangios. todėl didžiausias kiekis įsilaužimų ir duomenų nutekėjimo įvyksta šiose įmonėse. Pvz. grožio chirurgijos klinikos atvejis.

3. Kaip manote kas valstybinėms institucijoms ir organizacijoms labiausiai trukdo turėti patikimus ir saugius internetinius portalus? Kokiomis priemonėmis ir kokiais techniniais ir/ar organizaciniais kibernetinės saugos valdymo sprendimais siūlytumėte efektyvinti kibernetinį saugumą valstybinėse institucijose?

Didžiausias trūkumas yra specialistų trūkumas, gana sunku pritraukti ir išlaikyti kibernetinio saugumo specialistus, pagrinde dėl atlyginimų skirtumo privačiam ir valstybiniam sektoriui skirtumo. Saugos sprendimus įsigyja gerus, bet nėra kam administruoti. Paprastai saugumo sprendimo paslaugų pirkimas iš išorės nėra daromas, dėl tam tikrų susiklosčiusių aplinkybių.
Kita problema, kad tie patys žmonės turi rūpintis ir IT infostruktūra ir kompiuteriniais tinklais ir duomenų saugumu.
Efektyvinimui:
Tinkamus techninius ir programinius sprendimus galėtų parinkti kvalifikuoti specialistai. Reiktų daugiau dėmesio skirti vidiniams mokymams, specialistų tobulinimui, komandiruotėms į konferencijas.
Taip pat reiktų daugiau lėšų skirti naujiems specialistams įdarbinti ir apmokyti.

4. Ar šiuo metu Lietuvos vyriausybės ir ministerijų pradėtas vykdyti Valstybės informacinių išteklių infrastruktūros ir tinklų konsolidavimas turės įtakos valstybinių institucijų portalų kibernetinei apsaugai? Jeigu taip tai kokios?
   Reiktų išskirti du atskirus konsolidavimo etapus:
   Valstybės informacinių išteklių konsolidavimas
   Kibernetinio saugumo konsolidavimas.
   Kibernetinio saugumo konsolidavimas yra svarbus ir reikalingas, nes sukoncentravus žmones turinčius kompetencijas į vieną vietą jie gali potencialiai padaryti daugiau darbų, gauti daugiau lėšų mokymams.
   Yra kitas aspektas dėl ryšių konsolidavimo, nes sukoncentravus tinklą į vienas rankas, jį gali būti sunkiau ginti ir jis tampa lengvesniu taikiniu. Sukoncentruota infrastruktūra yra daug įdomesnė nei pavieniai taikiniai, nes sukompromitavus vieną įstaigą galima būtų sukompromituoti visą saugumo sistemą visoje šalyje.
   Visų klausimų sprendimas ir tinklų valdymas atiduodama vienai ministerijai ir vėliau pasikeitus valdžiai politikai galėtų lengviau kontroliuoti prieigas prie duomenų.

5. Kokia jūsų nuomone yra situacija su teisiniu kibernetinės saugos reglamentavimu Lietuvoje? Ar pakankamai aiškiai yra aprašyta institucijų atsakomybė už savo valdomus informacinius išteklius ir internetinius portalus? Ką jūs siūlytumėte tobulinti?
   Neturiu kompetencijos šiuo klausimu.

6. Ar Lietuvos Krašto apsaugos ministerijos organizuojamos kibernetinės saugos pratybos prisideda prie valstybės institucijų parengtumo atremti kibernetines atakas apsaugant interneto portalus didinimo? Ką šiuo atveju siūlytumėte tobulinti?

   Pratybos yra labai reikalingos, kalbant su pratybų dalyviais gan dažnas atsakymas buvo toks, pratybos kas metai didėja dalyvių skaičiumi, bet atliekamos užduotys ir įgyjamos patirtys negerėja. Yra išsakytos nuomonės, kad norėtųsi sudėtingesnių užduočių, labiau realistiškų, labiau praktiškų.

   Daugiau koncentruotis ne į kiekybę, o į kokybę ir sudėtingesnes užduotis.

7. Kaip prie valstybinių institucijų internetinių portalų kibernetinės saugos tobulinimo galėtų prisidėti Lietuvos visuomenė?

   Visuomenės edukacija yra labai svarbus dalykas. Abejoju ar visuomenė galėtų prisidėti prie saugomo tiesiogine prasme. Svarbu, kad visuomenė išmoktų atpažinti kibernetines grėsmes ir kilus įtarimui, kad portalas veikia netinkamai arba nukreipiama į kažkokią svetainę ir prašoma įvesti savo asmeninius banko prisijungimo ar kitus duomenis. Kad apie tai būtų pranešama ir kuo mažiau žmonių užkibtų ant tokių atakų kabliuko. Tokiu atveju ir įvykus kibernetiniam incidentui poveikis nebūtų per sudėtingas. Visuomenės švietimas, mokymas ir pasakojimas apie grėsmes yra labai svarbus.

   Manau, kad labai trūksta plataus mąsto tiek valstybinio sektoriaus, tiek visuomenės mokymų.

   Tai yra pirmas ir pagrindinis dalykas padedantis atremti kibernetines atakas.

   Žmonių neatidumas ir lengvatikiškumas yra dažniausiai naudojami įrankiai, kuriais kibernetiniai nusikaltėliai bando pasiekti savo tikslų.

PATVIRTINIMAS APIE ATLIKTO DARBO SAVARANKIŠKUMĄ

2020 - 04 - 28
Vilnius

Aš, Mykolo Romerio universiteto (toliau – Universitetas),

Ekonomikos ir verslo fakulteto, Kibernetinės saugos valdymo programos
(fakulteto / instituto, programos pavadinimas)

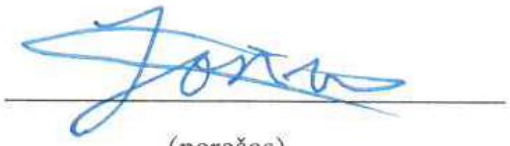
Studentas (-ė) Jonas Vaitkevičius,
(vardas, pavardė)

patvirtinu, kad šis rašto darbas / bakalauro / magistro baigiamasis darbas

„Valstybės institucijų portalų apsauga kibernetinės saugos valdymo priemonėmis“:

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

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



(parašas)

Jonas Vaitkevičius
(vardas, pavardė)