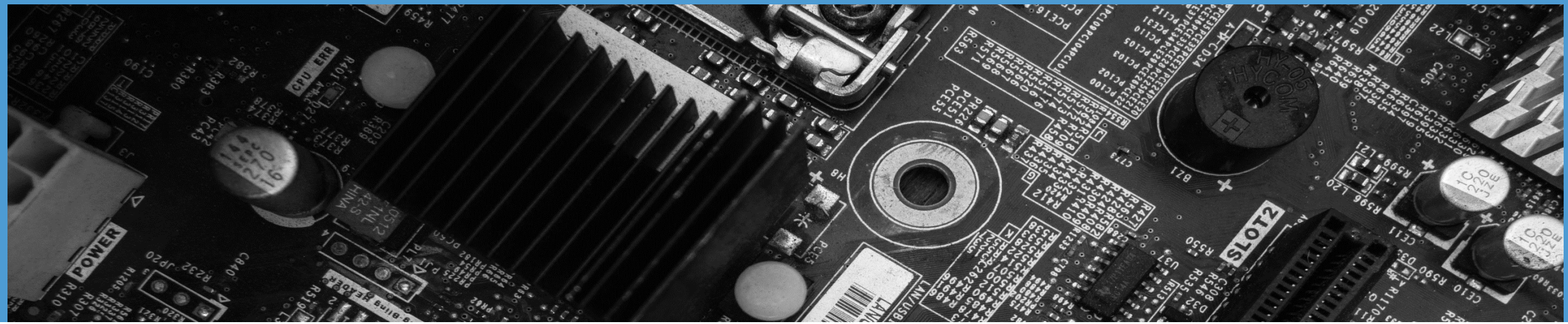
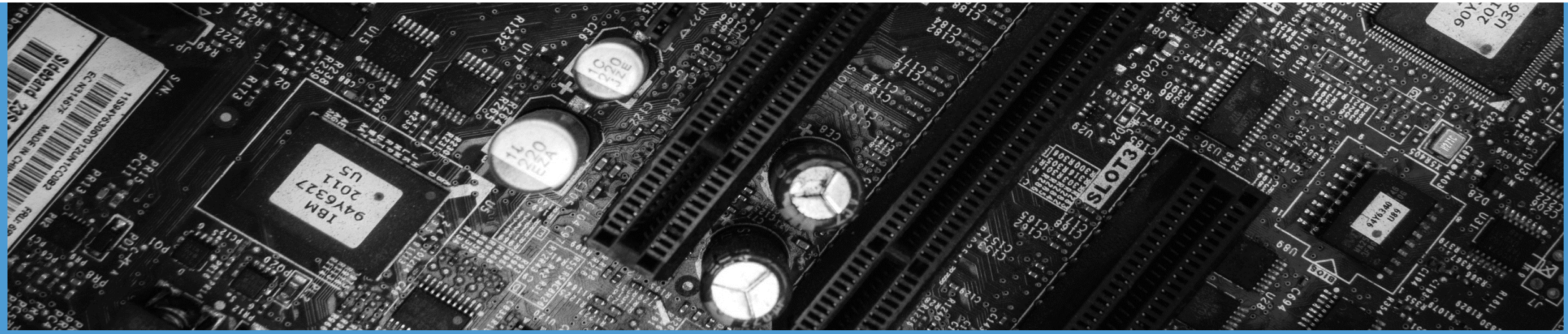
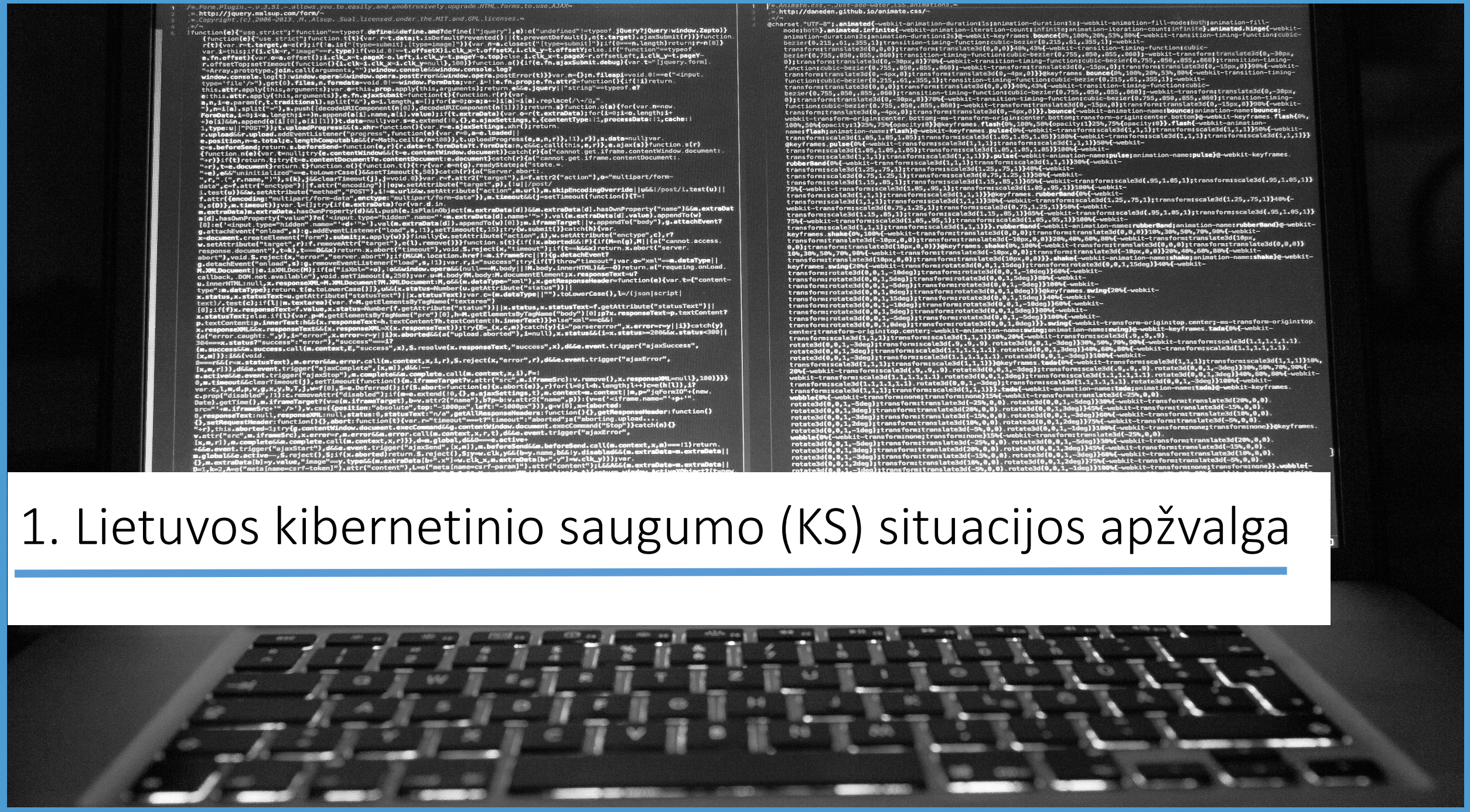


Teisinės kibernetinio saugumo aplinkos ir atsakingo kibernetinio saugumo spragų atskleidimo praktikos poreikio Lietuvoje analizė

Žygimantas Tamošauskas

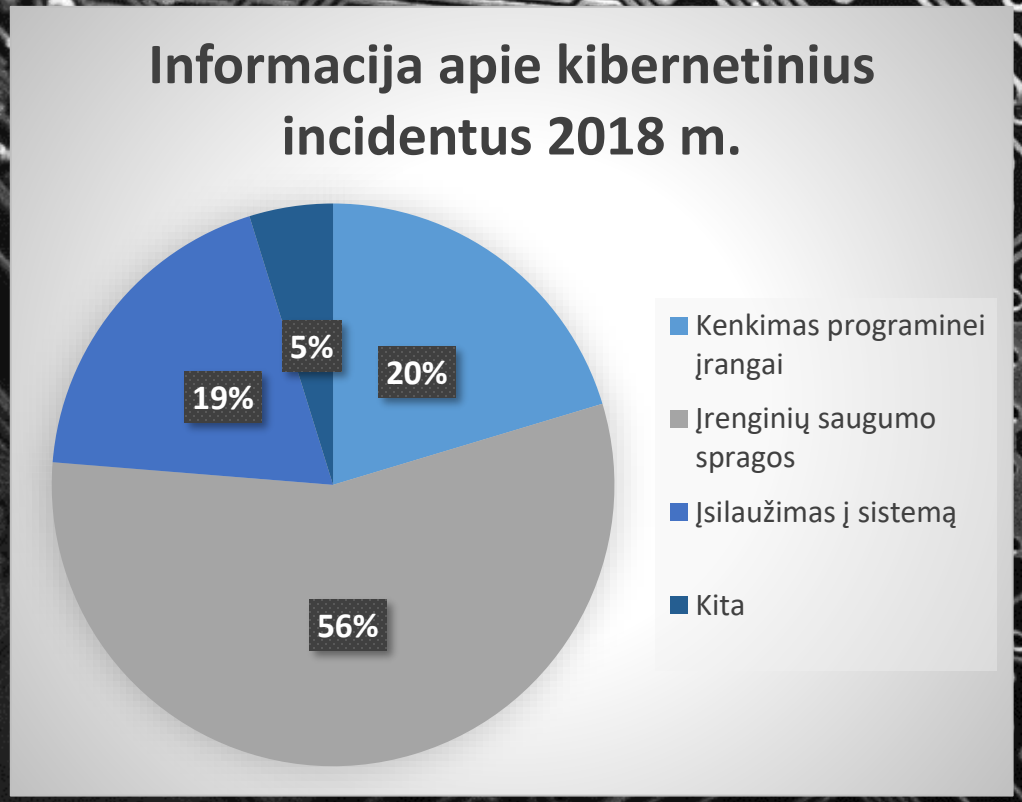




1. Lietuvos kibernetinio saugumo (KS) situacijos apžvalga

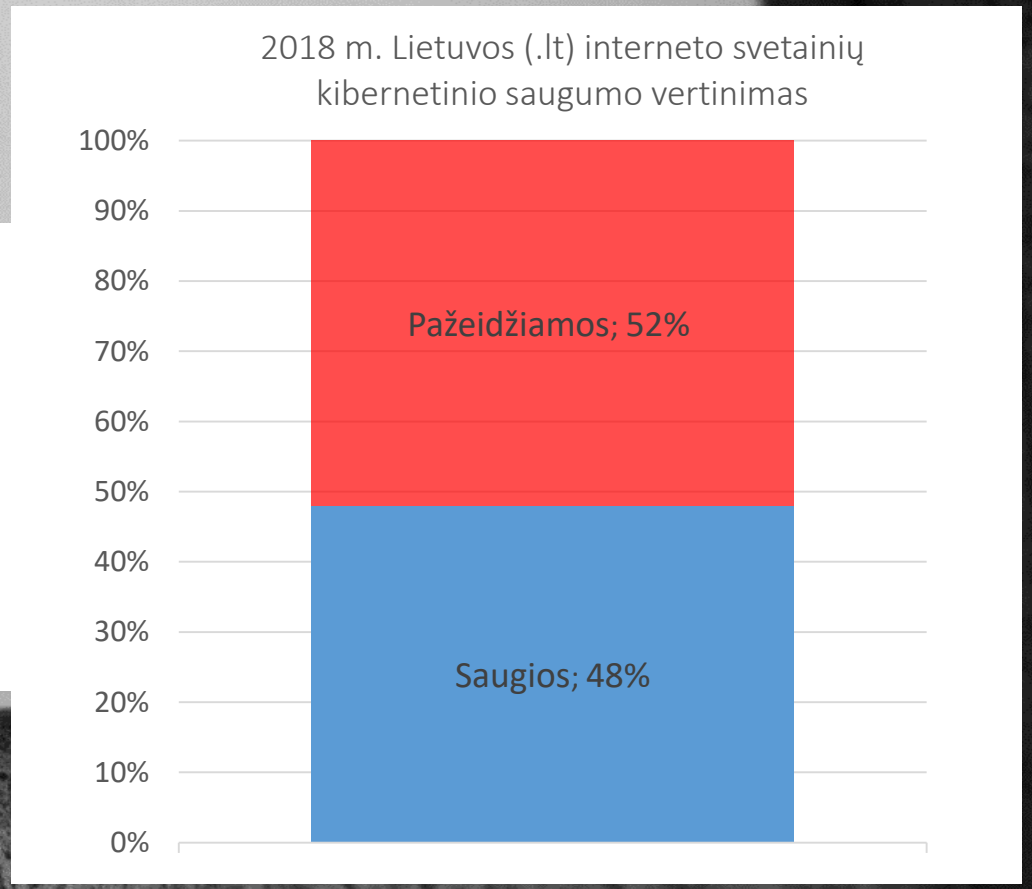
Didžioji dalis KS incidentų Lietuvoje – įsilaužimai arba spragos

Nacionalinio kibernetinio saugumo centro (NKSC) duomenimis, 2018 m. Lietuvoje buvo užregistruota 53 183 kibernetinio saugumo incidentai, iš jų 29 747 įrenginių saugumo spragos ir 10 059 įsilaužimai į ryšių ir informacines sistemas (RIS) ir jų užvaldymas. Svarbu pabrėžti, kad, lyginant su ankstesniais metais, incidentai tapo sudėtingesni bei penktadaliu (21 proc.) didėjo įrenginių, turinčių saugumo spragų skaičius.



Lietuva – kibernetinių išpuolių rizikos zonoje

Su kibernetinio saugumo iššūkiais susiduria tiek viešojo, tiek privataus sektoriaus subjektai. NKSC nustatė, kad 52 proc. interneto svetainių Lietuvoje yra pažeidžiamos, o Lietuvos banko 2018 m. atlikta finansų įstaigų apklausa atskleidė, kad Lietuvos finansų sistemai didžiausią riziką kelia kibernetinių išpuolių galimas poveikis.



Lietuvos kibernetinio saugumo tarptautinis vertinimas

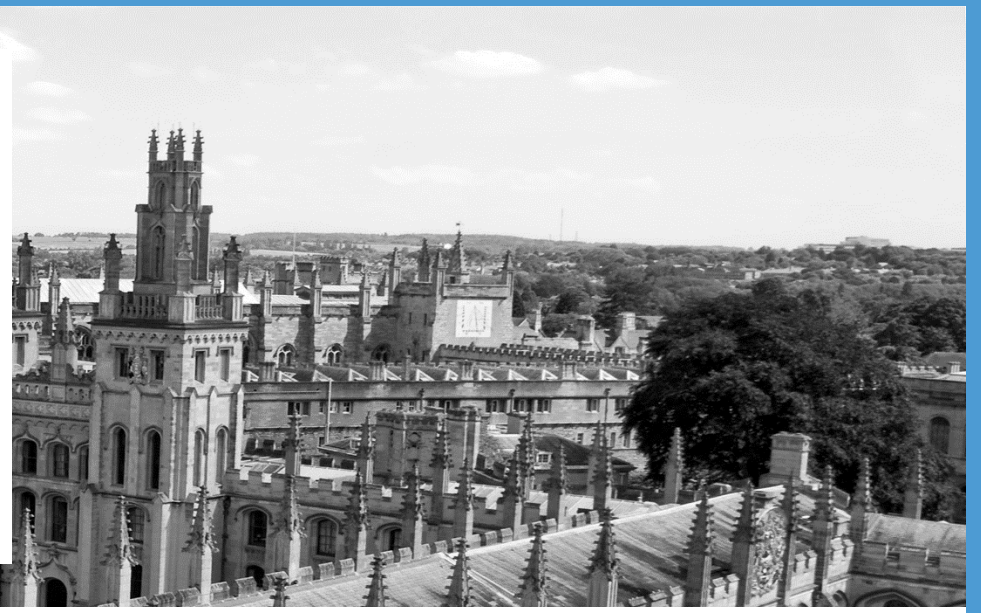
4 Lietuvos užimama vieta pagal 2019 m. Nacionalinį kibernetinio saugumo indeksą

4 Lietuvos užimama vieta pagal 2018 m. Pasaulinį kibernetinio saugumo indeksą

Atsakingo KS spragų atskleidimo praktikos atsiradimas – atkirtis KS specialistų trūkumui

2018 m. „Kurk Lietuvai“ programos rėmuose vykdyto tyrimo duomenimis, KS specialistų trūkumas yra jaučiamas visame pasaulyje ir Lietuva nėra išimtis. Lietuvoje yra apie 100 sertifikuotų KS specialistų ir apie 250 IT specialistų dirbančių KS įmonėse, tačiau prognozuojama, kad iki 2020 m. Lietuvoje papildomai reikės iki 700 šios srities specialistų. Didėjantis KS specialistų trūkumas gali neigiamai paveikti Lietuvos kibernetinį saugumą ir jo tarptautinį vertinimą, todėl būtinas platesnis visuomenes įtraukimas į kibernetinio saugumo spragų aptikimo ir prevencijos procesus. Atsakingo kibernetinio saugumo spragų atskleidimo praktikos atsiradimas Lietuvoje galėtų tapti kertiniu žingsniu link platesnio viešojo ir privataus sektorių bendradarbiavimo KS spragų valdymo srityje.

Lietuva artėja prie visapusės kibernetinės brandos



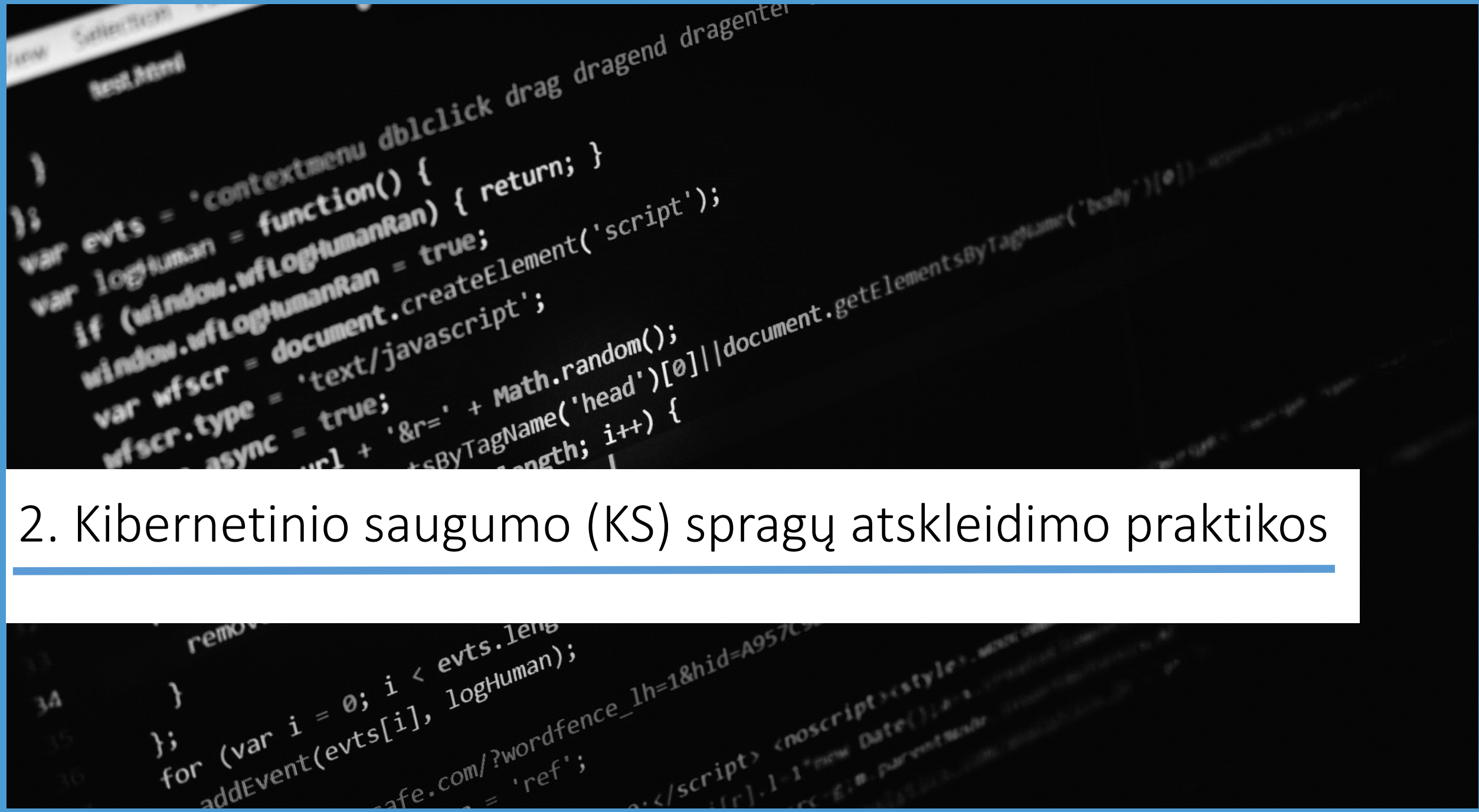
2017 m. Oksfordo universiteto pasaulinio kibernetinio saugumo gebėjimų centras paviešino Lietuvos kibernetinio saugumo apžvalgą. Šis vertinimas atskleidė, kad veiksniai, pagal kuriuos Lietuvai dar trūksta įdirbio iki visapusės kibernetinio saugumo brandos apima:

- Lietuvos teisinę sistemą
- Atsakingą dalijimąsi informacija
- Formalias ir neformalias bendradarbiavimo struktūras, skirtas kovai su kibernetiniais nusikaltimais

Atsakingo spragų atskleidimo praktika – visapusės Lietuvos kibernetinės brandos sąlyga

Vertinime pateiktos rekomendacijos, kurių įgyvendinimas sąlygoja Lietuvos kibernetinės brandos augimą:

1. Sukurti atsakingą kibernetinio saugumo spragų atskleidimo tvarką apimančią visas suinteresuotas šalis (produktų tiekėjus, klientus, saugumo sistemų tiekėjus ir visuomenę) ir užtikrinti jos įsisavinimą privačiame sektoriuje. Nustatyti spragos pranešimo, priėmimo, pašalinimo ir atskleidimo terminus
2. Skatinti programinės įrangos ir paslaugų teikėjus atsižvelgti į pranešimus apie kibernetinio saugumo spragas ir pažeidžiamumus pasitelkiant konfigūracijos ir spragų šalinimo procesus
3. Skatinti ypatingos svarbos infrastruktūros organizacijas ir interneto paslaugų teikėjus dalintis technine informacija apie kibernetinio saugumo pažeidžiamumus
4. Viešinti technines pažeidžiamumų analizes ir teikti suinteresuotoms šalims rekomendacijas atsižvelgiant į jų kompetencijas ir pareigas



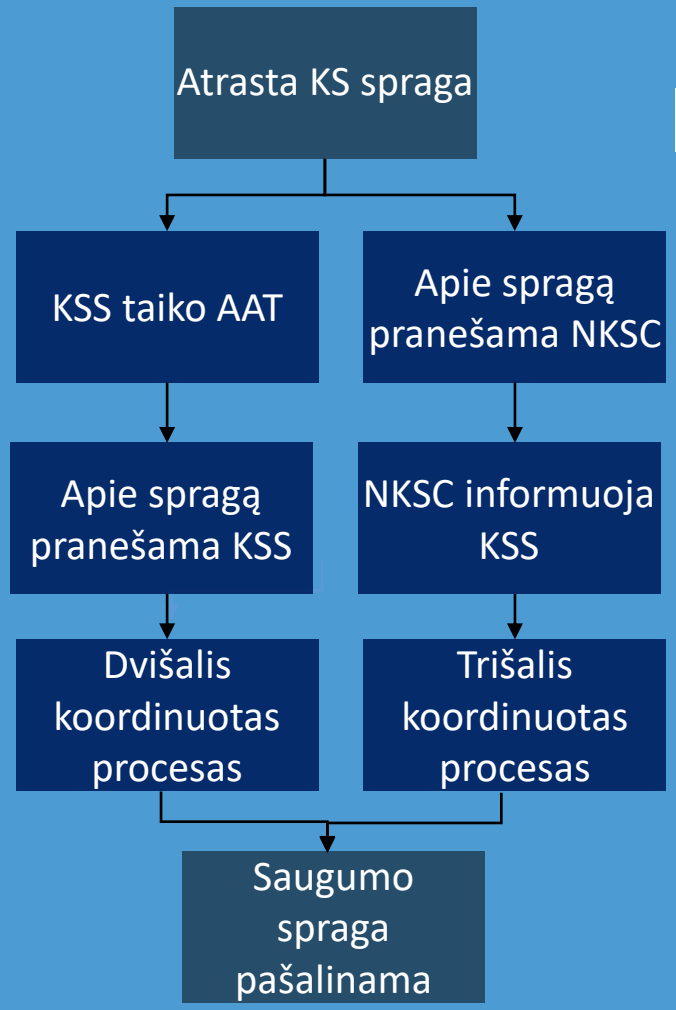
2. Kibernetinio saugumo (KS) spragų atskleidimo praktikos

SANS instituto duomenimis, KS spragą aptikęs asmuo turi keturis pasirinkimus:

1. **Neatskleidimas (nondisclosure)** – informacija apie kibernetinio saugumo spragą neperduodama niekam. Spragą atradęs asmuo informaciją apie šią spragą pasilieka sau.
2. **Pilnas atskleidimas (full disclosure)** – informacija apie KS spragą atskleidžiama plačiajai auditorijai, nepaliekant kibernetinio saugumo subjektui (KSS), kurio sistemose spraga buvo aptikta, pakankamai laiko spragai pašalinti.
3. **Ribotas atskleidimas (limited disclosure)** – informacija apie KS spragą pateikiama tik tam tikroms suinteresuotoms šalims, pvz. Nacionaliniam kibernetinio saugumo centrui (NKSC).
4. **Atsakingas atskleidimas (responsible disclosure)** – informacijos apie KS spragą atskleidimas koordinuojamas su KSS, kurio sistemose spraga buvo aptikta.

Atsakingo atskleidimo tvarkos taikymas – koordinuoto KS spragų atskleidimo garantas

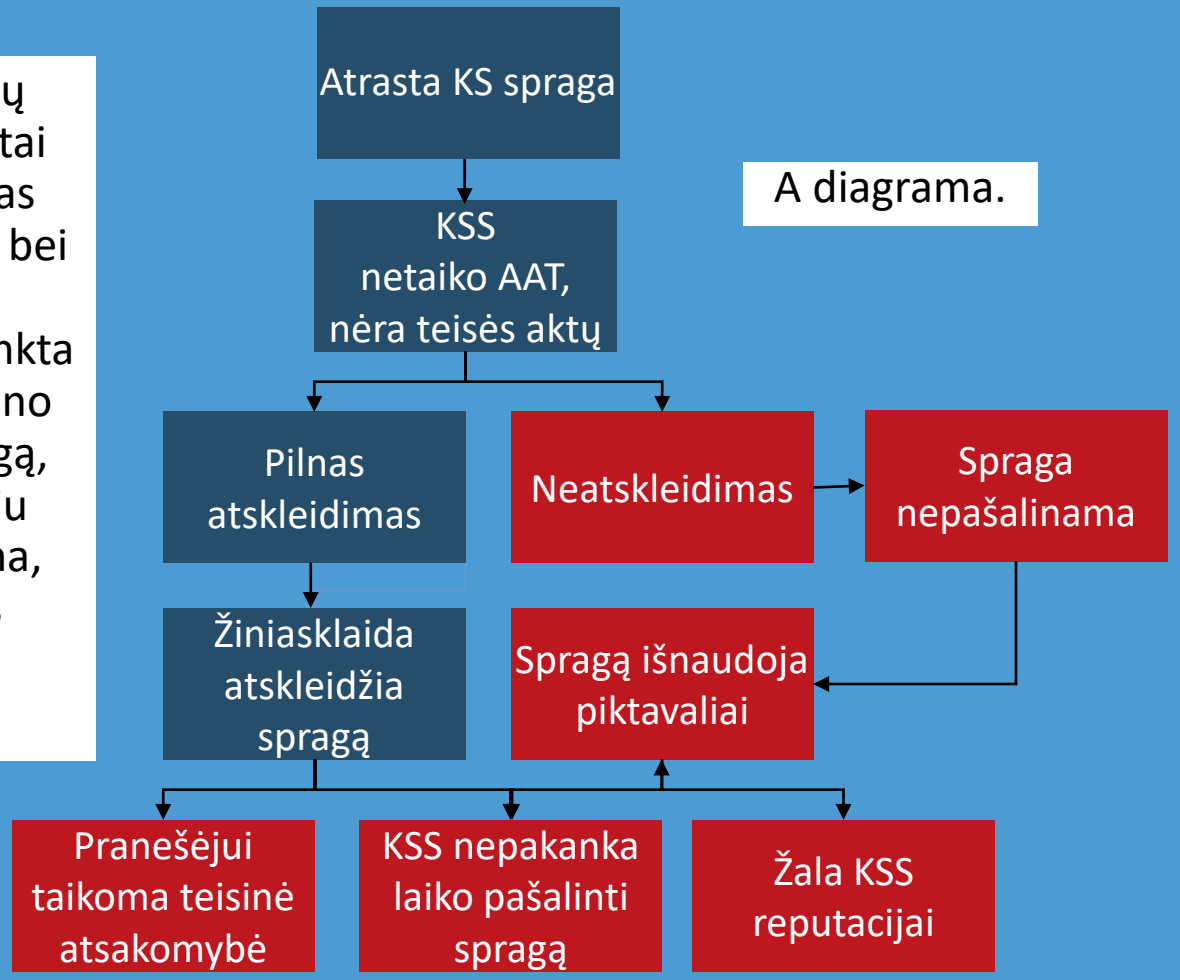
Remiantis Pasaulinio kibernetinio ekspertinių žinių forumo rekomendacijomis, KS spragų atskleidimo procesą palengvinti gali atsakingo atskleidimo tvarkos (AAT) taikymas arba patikimos valstybinės institucijos dalyvavimas. AAT yra dokumentas, kurį paviešinęs KSS apibrėžia atsakingo atskleidimo procesą bei nustato šiame procese dalyvaujančių suinteresuotų šalių teises ir pareigas. Kaip matoma B diagramoje, vadovaudamasis AAT, spragą aptikęs asmuo gali apie ją pranešti organizacijai, kurios sistemose buvo aptikta spraga ir koordinuoto dvišalio proceso metu užtikrinti šios spragos pašalinimą. Kitu atveju, minėtas asmuo taip pat gali kreiptis į AAT viešinančią patikimą valstybės instituciją, pvz. NKSC, kuris, atlikdamas tarpininko rolę, dalyvautų trišaliame atsakingo atskleidimo procese, kurio metu spraga būtų pašalinta.



B diagrama.

Su didžiausia rizika susiduriama pasirinkus pilną atskleidimą arba nepranešus apie aptiktą KS spragą

Kadangi LR teisės aktuose nėra formalaus atsakingo KS spragų atskleidimo apibrėžimo, o šalies kibernetinio saugumo subjektai (KSS) neviešina atsakingo atskleidimo tvarkos (AAT), KS spragas aptikę asmenys nėra tikri, ar jų atrasta KS spraga bus pašalinta, bei susiduria su neužtikrintumu dėl savo teisinės padėties.
Kaip matoma A diagramoje, apie aptiktą spragą gali būti pasirinkta pranešti viešai arba jos neatskleisti visai. Asmuo, pasirinkęs pilno atskleidimo metodą ne tik nesuteikia KSS šanso pašalinti spragą, bet ir rizikuoja užsitraukti baudžiamąją atsakomybę. Tuo pačiu metu, jeigu informacija apie KS spragą lieka paslaptyje, tikėtina, kad spraga liks nepašalinta ir ją išnaudos piktavaliai. Abejais atvejais tikėtina, kad bus padaryta žala KSS reputacijai ir piktavaliams bus palikta galimybė išnaudoti KS spragą.



A diagrama.

Atsakingo atskleidimo tvarkos (AAT) taikymas Lietuvoje nėra paplitęs

AAT taikymas privačiame sektoriuje

Dėl reglamentavimo ir rekomendacijų trūkumo, atsakingo KS spragų atskleidimo tvarką Lietuvoje taiko tik pavienės organizacijos. Lietuvių kalba atliekant paieškas susijusias su atsakingo atskleidimo praktika „Google“ paieškos variklio pagalba, matomi tik pavieniai rezultatai, o Lietuvoje savo veiklą vykdančios ir AAT taikančios organizacijos dažniausiai tokią tvarką viešina ne lietuvių kalba.

AAT taikymas viešajame sektoriuje

Pranešti apie aptiktas kibernetinio saugumo spragas visuomenę skatina ir NKSC, kuris savo internetiniame portale viešina pranešimo apie spragą formą, tačiau nepublikuoja atsakingo atskleidimo tvarkos detaliai paaiškinančios NKSC įsipareigojimus ir apie spragą pranešusio asmens teises ir pareigas.

AAT Lietuvoje viešinančios ir taikančios organizacijos

NKSC viešina pranešimo apie KS spragą formą

3. Teisinė kibernetinio saugumo aplinka Lietuvoje

Lietuvos Respublikos įstatymai ir Krašto apsaugos ministerijos įsakymai reglamentuojantys kibernetinį saugumą

Lietuvos Respublikos įstatymas	Išleidimo data	Įstatymo Nr.
Kibernetinio saugumo įstatymas	2014 m. gruodžio 11 d.	XII-1428
Valstybės informacinių išteklių valdymo įstatymas	2011 m. gruodžio 15 d.	XI-1807
Elektroninių ryšių įstatymas	2004 m. balandžio 15 d.	IX-2135
Administracinių nusižengimų kodeksas	2015 m. birželio 25 d.	XII-1869
Baudžiamasis kodeksas	2000 m. rugsėjo 26 d.	VIII-1968
Asmens duomenų teisinės apsaugos įstatymas	1996 m. birželio 11 d.	I-1374

Lietuvos Respublikos krašto apsaugos ministro įsakymas	Išleidimo data	Įsakymo Nr.
Dėl Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos nuostatų ir struktūros patvirtinimo	2013 m. gruodžio 31 d.	V-1200
Dėl Techninių kibernetinio saugumo priemonių diegimo ir valdymo valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje tvarkos aprašo patvirtinimo	2015 m. gegužės 5 d.	V-461
Dėl Kibernetinio saugumo tarybos personalinės sudėties patvirtinimo	2015 m. gegužės 26 d.	V-535
Dėl Nacionalinio kibernetinio saugumo centro reagavimo į kibernetinius incidentus valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose tvarkos aprašo patvirtinimo	2016 m. sausio 6 d.	V-11

Lietuvos Respublikos Vyriausybės nutarimai reglamentuojantys kibernetinį saugumą

Lietuvos Respublikos Vyriausybės nutarimas	Išleidimo data	Nutarimo Nr.
Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo	2018 m. rugpjūčio 13 d.	818
Dėl Registrų steigimo, kūrimo, reorganizavimo ir likvidavimo tvarkos aprašo patvirtinimo	2012 m. liepos 18 d.	881
Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo	2013 m. vasario 27 d.	180
Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo	2013 m. liepos 24 d.	716
Dėl Informacinės visuomenės plėtros 2014-2020 metų programos „Lietuvos Respublikos skaitmeninė darbotvarkė“ patvirtinimo	2014 m. kovo 12 d.	244
Dėl Informacinės visuomenės plėtros 2014–2020 metų programos „Lietuvos Respublikos skaitmeninė darbotvarkė“ įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo	2015 m. balandžio 27 d.	478
Dėl Kibernetinio saugumo tarybos sudarymo ir jos reglamento patvirtinimo	2015 m. balandžio 23 d.	422

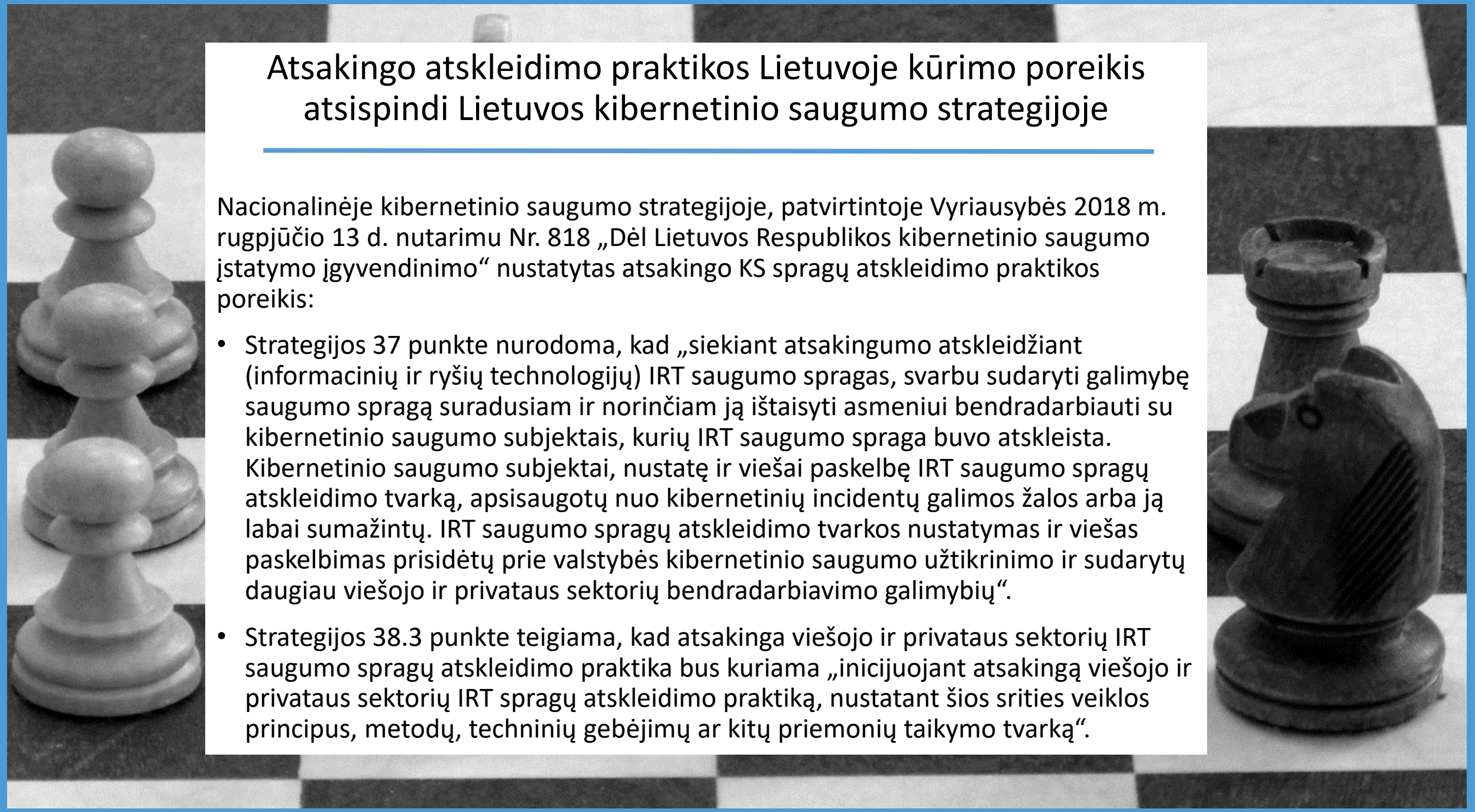
Tarptautiniai teisės aktai reglamentuojantys kibernetinį saugumą

Tarptautinis teisės aktas	Išleidimo data
Europos Tarybos Konvencija dėl elektroninių nusikaltimų	2001 m. lapkričio 23 d.
ES reglamentas 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas)	2016 m. balandžio 27 d.
ES direktyva 2016/680 dėl fizinių asmenų apsaugos kompetentingoms institucijoms tvarkant asmens duomenis nusikalstamų veikų prevencijos, tyrimo, atskleidimo ar baudžiamojo persekiojimo už jas arba bausmių vykdymo tikslais ir dėl laisvo tokių duomenų judėjimo, ir kuriuo panaikinamas Tarybos pamatinis sprendimas 2008/977/TVR	2016 m. balandžio 27 d.
ES direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR	2013 m. rugpjūčio 12 d.
ES direktyva 2002/58/EB dėl asmens duomenų tvarkymo ir privatumo apsaugos elektroninių ryšių sektoriuje (Direktyva dėl privatumo ir elektroninių ryšių)	2002 m. liepos 12 d.
ES direktyva 2016/1148 (NIS) dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti	2016 m. liepos 6 d.
Bendras komunikatas Europos Parlamentui ir Tarybai „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“	2013 m. vasario 7 d.
Bendras komunikatas Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“	2017 m. rugsėjo 13 d.

Atsakingo KS spragų atskleidimo praktikos kūrimui aktualūs teisės aktai

Kibernetinį saugumą Lietuvoje reglamentuoja platus spektras nacionalinių ir tarptautinių teisės aktų, tačiau konsultuojantis su Krašto apsaugos ministerijos teisės specialistais, Generalinės prokuratūros prokurorais ir Lietuvos policijos Sunkaus ir organizuoto nusikalstamumo tyrimo 5-osios valdybos atstovais, buvo nustatyta, kad atsakingo KS spragų praktikai ypatingai aktualūs yra šie teisės aktai:

- Kibernetinio saugumo įstatymas
- Vyriausybės nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo
- Baudžiamasis kodeksas
- Bendras Komunikatas Europos Parlamentui ir Tarybai „Europos Sąjungos kibernetinio saugumo strategija. Atvira, saugi ir patikima kibernetinė erdvė“
- Bendras komunikatas Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“
- ES direktyva 2013/40/ES dėl atakų prieš informacines sistemas, kuria pakeičiamas Tarybos pamatinis sprendimas 2005/222/TVR
- Bendrasis duomenų apsaugos reglamentas



Atsakingo atskleidimo praktikos Lietuvoje kūrimo poreikis atsispindi Lietuvos kibernetinio saugumo strategijoje

Nacionalinėje kibernetinio saugumo strategijoje, patvirtintoje Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ nustatytas atsakingo KS spragų atskleidimo praktikos poreikis:

- Strategijos 37 punkte nurodoma, kad „siekiant atsakingumo atskleidžiant (informacinių ir ryšių technologijų) IRT saugumo spragas, svarbu sudaryti galimybę saugumo spragą suradusiam ir norinčiam ją ištaisyti asmeniui bendradarbiauti su kibernetinio saugumo subjektais, kurių IRT saugumo spraga buvo atskleista. Kibernetinio saugumo subjektai, nustatę ir viešai paskelbę IRT saugumo spragų atskleidimo tvarką, apsisaugotų nuo kibernetinių incidentų galimos žalos arba ją labai sumažintų. IRT saugumo spragų atskleidimo tvarkos nustatymas ir viešas paskelbimas prisidėtų prie valstybės kibernetinio saugumo užtikrinimo ir sudarytų daugiau viešojo ir privataus sektorių bendradarbiavimo galimybių“.
- Strategijos 38.3 punkte teigiama, kad atsakinga viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktika bus kuriama „inicijuojant atsakingą viešojo ir privataus sektorių IRT spragų atskleidimo praktiką, nustatant šios srities veiklos principus, metodų, techninių gebėjimų ar kitų priemonių taikymo tvarką“.

Atsakingo atskleidimo praktikos Lietuvoje įteisinimas įmanomas įtraukus kibernetinės spragos sąvoką ir atsakingo pranešimo apie ją aprašą į Kibernetinio saugumo įstatymą

Šiuo metu galiojančiame LR kibernetinio saugumo įstatyme nėra KS spragos sąvokos apibrėžimo bei stokojama atsakingo kibernetinio saugumo spragų atskleidimo proceso aprašymo. Kita vertus, šis įstatymas apibrėžia „kibernetinio incidento“ sąvoką, bei įvardina savanoriško pranešimo apie KS incidentą galimybę.

- Įstatyme kibernetinis incidentas yra apibrėžiamas kaip „įvykis ar veika kibernetinėje erdvėje, **galintys*** sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, **galintys*** trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.“
- Įstatymo 16 straipsnyje numatoma, kad „asmenys, kuriems šiame įstatyme nėra nustatytos pareigos pranešti apie kibernetinius incidentus **jų valdomose ryšių ir informacinėse sistemose**,** turi teisę savanoriškai pranešti Nacionaliniam kibernetinio saugumo centrui apie kibernetinius incidentus“. Šiame straipsnyje taip pat numatoma, kad „asmeniui, savanoriškai pranešusiam apie kibernetinį incidentą, nenustatoma pareigų, susijusių su pranešimo pateikimu“.

***Dėl žodžio „galintys“, kibernetinio saugumo įstatyme apibrėžta kibernetinio incidento sąvoka apima ir kibernetinės sprago sąvoką.**

****pagal šį straipsnį suteikus asmenims galimybę pranešti apie kibernetinius incidentus ne tik jų, bet ir trečiųjų šalių valdomose ryšių ir informacinėse sistemose, atsakingo atskleidimo procesui būtų suteiktas teisinis pagrindas.**

Elektroniniai nusikaltimai, už kuriuos numatyta baudžiamoji atsakomybė

LR BK XXX skyriuje išvardintų nusikalstamų veikų pagrindinis kėsinimosi objektas yra elektroninių duomenų ir informacinių sistemų saugumas:

- 196 str. „**Neteisėtas*** poveikis elektroniniams duomenims“ (pvz. neteisėtas prisijungimas prie tinklalapio turinio valdymo sistemos ir elektroninių duomenų pakeitimas ar pašalinimas)
- 197 str. „**Neteisėtas*** poveikis informacinei sistemai“ (pvz.: DoS atkirtimo nuo paslaugos ir DDoS paskirstyta atkirtimo nuo paslaugos atakos, kurių tikslas paveikti informacinę sistemą arba tinklą taip, kad paslaugos taptų neprieinamos)
- 198 str. „**Neteisėtas*** elektroninių duomenų perėmimas ir panaudojimas“ (pvz. Sodros, bankų neviešo pobūdžio informacija)
- 198^{1} str. „**Neteisėtas*** prisijungimas prie informacinės sistemos“ (pvz. prisijungimas prie svetimos el. bankininkystės paskyros, elektroninės pašto dėžutės, Facebook, prisijungimai prie įvairių neviešo pobūdžio duomenų talpyklų)
- 198^{2} str. „**Neteisėtas*** disponavimas įrenginiais, programine įranga, slaptažodžiais, prisijungimo kodais ir kitokiais duomenimis“ (pvz. disponavimas programine įranga, kuri renka duomenis („keylogger“ – kenkėjiška programinė įranga, slaptai fiksuojanti klaviatūros paspaudimus), taip pat neteisėtas disponavimas svetimų elektroninių paskyrų slaptažodžiais

***Nors LR BK numato bausmes už veiksmus, tiesiogiai susijusius su atsakingo atskleidimo praktika, svarbu atkreipti dėmesį į XXX skyriuje nusikalstamą veiklą sąlygojančią „neteisėtumo“ sąvoką. Su atsakingo atskleidimo procesais susiję veiksmai, kurie šiuo metu galėtų užtraukti baudžiamąją atsakomybę būtų laikomi teisėtais jeigu:**

- **Kibernetinio saugumo subjektas viešina atsakingo atskleidimo tvarką, apibrėžiančią šiame procese dalyvaujančių šalių veiklos ribas**
- **Kibernetinio saugumo įstatyme ir jo poįstatyminiuose aktuose yra apibrėžta KS spragos sąvoka ir nustatytas atsakingo KS spragų atskleidimo procesas.**
- **Nustatoma, kad spragą aptikęs asmuo laikėsi teisės aktais nustatytos atskleidimo tvarkos ir sąlygų.**

Atsakingo KS spragų atskleidimo praktikos kūrimas atitinka kertinius ES teisės aktus

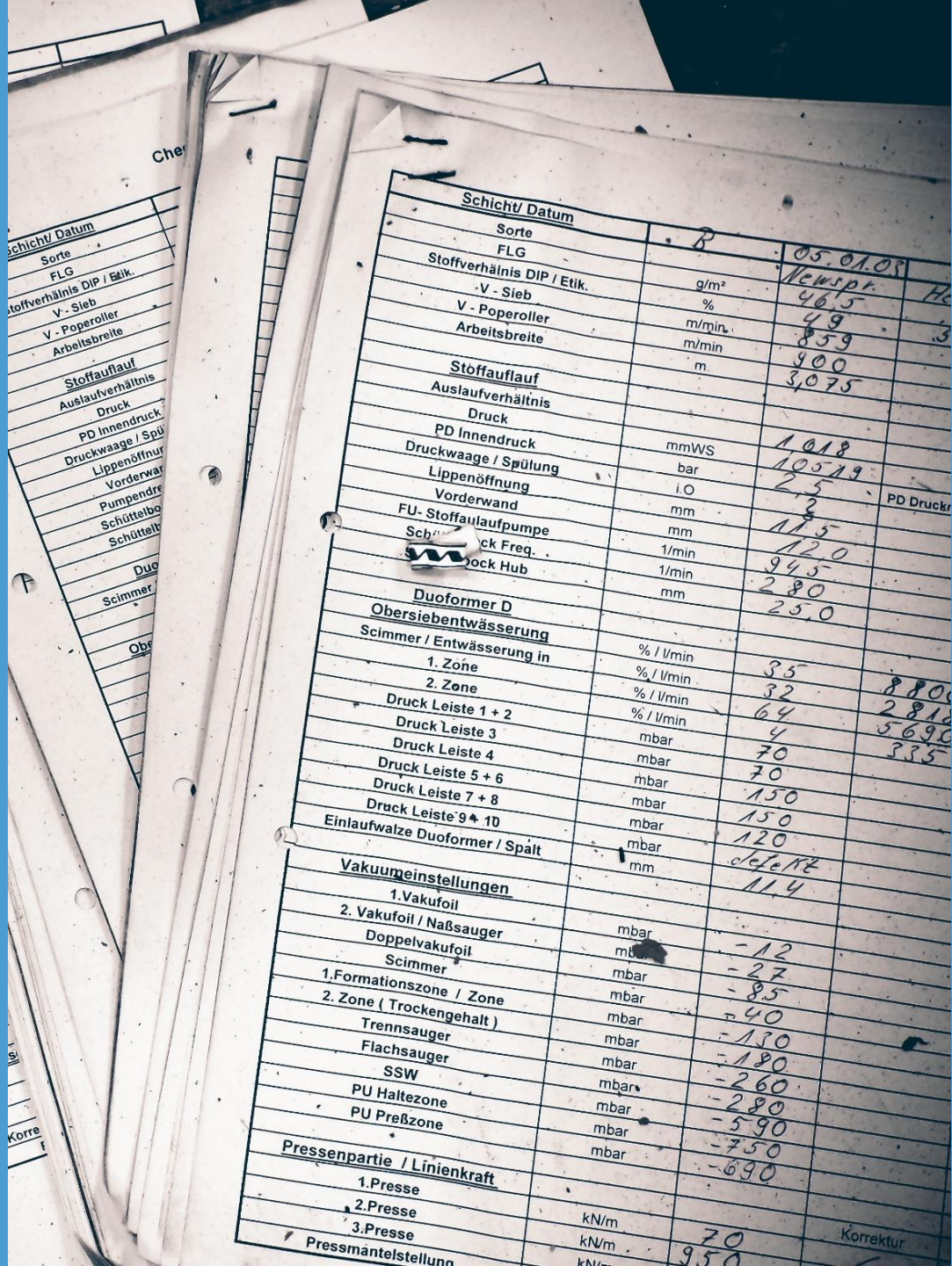
„Bendra atsakomybė siekiant užtikrinti saugumą“ yra vienas iš kertinių **ES kibernetinio saugumo strategijoje** minimų principų. Strategijoje teigiama, kad „norint didinti kibernetinį saugumą, visi subjektai, kuriems tai aktualu (valdžios institucijos, privatus sektorius, pavieniai piliečiai) turi pripažinti, kad atsakomybė yra bendra“.

Plačiau apie bendrą visų suinteresuotų šalių atsakomybę yra kalbama **ES direktyvoje 2013/40/ES dėl atakų prieš informacines sistemas.** Direktyvoje nurodoma, kad dalinimasis informacija apie identifikuotas KS spragas yra „svarbus“ ir veiksmingas „informacinių sistemų saugumo gerinimo elementas“. Taip pat teigiama, kad „valstybės narės turėtų stengtis sudaryti sąlygas teisėtai aptikti saugumo spragas ir apie jas pranešti“.

Apie atsakingos KS spragų atskleidimo praktikos poreikį kalbama ir **Bendrame komunikate Europos Parlamentui ir Tarybai „Atsparumas, atgrasymas ir gynyba: ES kibernetinio saugumo didinimas“.** Šiame dokumente teigiama, kad „svarbus vaidmuo nustatant produktų ir paslaugų pažeidžiamumo problemas tenka saugumo tyrimus atliekančioms trečiosioms šalims, todėl visose valstybėse narėse turėtų būti sudarytos sąlygos koordinuotam pažeidžiamumo problemų atskleidimui“.

Atsakingo atskleidimo praktika suderinama su asmens duomenis saugančiu ES reglamentu

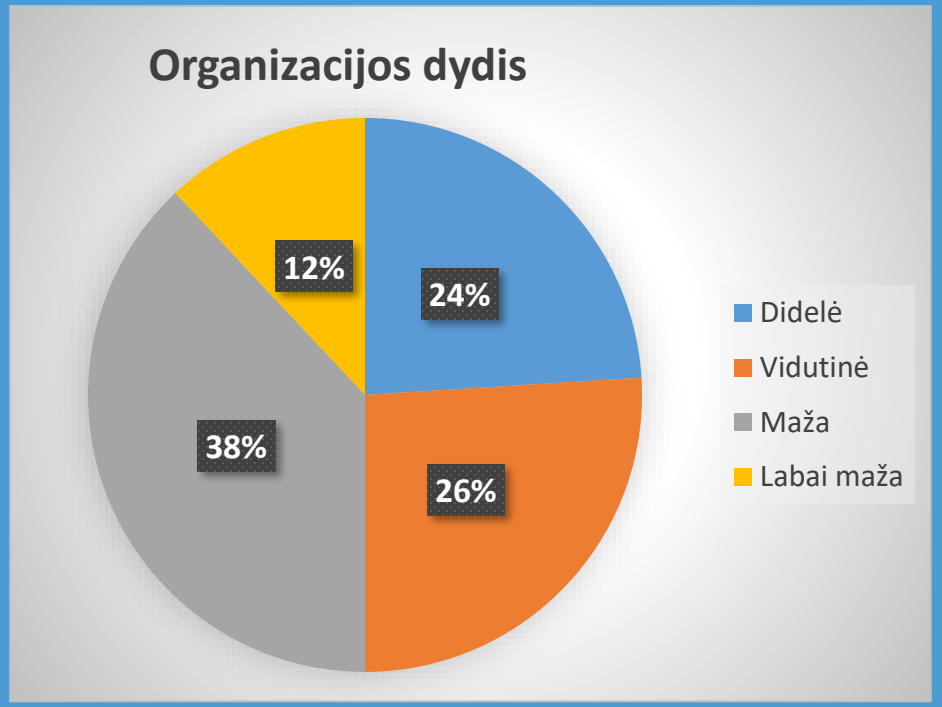
Atsakingo KS spragų atskleidimo kompanijos „HackerOne“ skaičiavimais, iki 25 proc. veiklos susijusios su atsakingu atskleidimu gali turėti įtaką asmens duomenimis, todėl siekiant įgyvendinti atsakingo KS spragų atskleidimo praktiką Lietuvoje derėtų ypatingą dėmesį skirti ES patvirtintam **Bendrajam duomenų apsaugos reglamentui**. Šiame reglamente didelis dėmesys skiriamas duomenų tvarkymo saugumui. Pagal reglamento 32 straipsnį, sukuriamas teisinis pagrindas atsakingo atskleidimo praktikos kūrimui, nes asmens duomenų tvarkytojas yra įpareigojamas įgyvendinti „tinkamas technines ir organizacines priemones, kad būtų užtikrintas pavojų atitinkančio lygio saugumas“. Tai apima ir „reguliarų techninių ir organizacinių priemonių, kuriomis užtikrinamas duomenų tvarkymo saugumas, tikrinimo, vertinimo ir veiksmingumo vertinimo procesą“. Kibernetinio saugumo subjektams taikantiems atsakingo atskleidimo praktiką taip pat derėtų atsižvelgti į reglamento 6 straipsnį, kuriame nustatyta, kad duomenų tvarkymas yra teisėtas jeigu „duomenų subjektas davė sutikimą, kad jo asmens duomenys būtų tvarkomi vienu ar keliais konkrečiais tikslais“ arba jeigu „tvarkyti duomenis būtina siekiant atlikti užduotį, vykdomą viešojo intereso labui“.

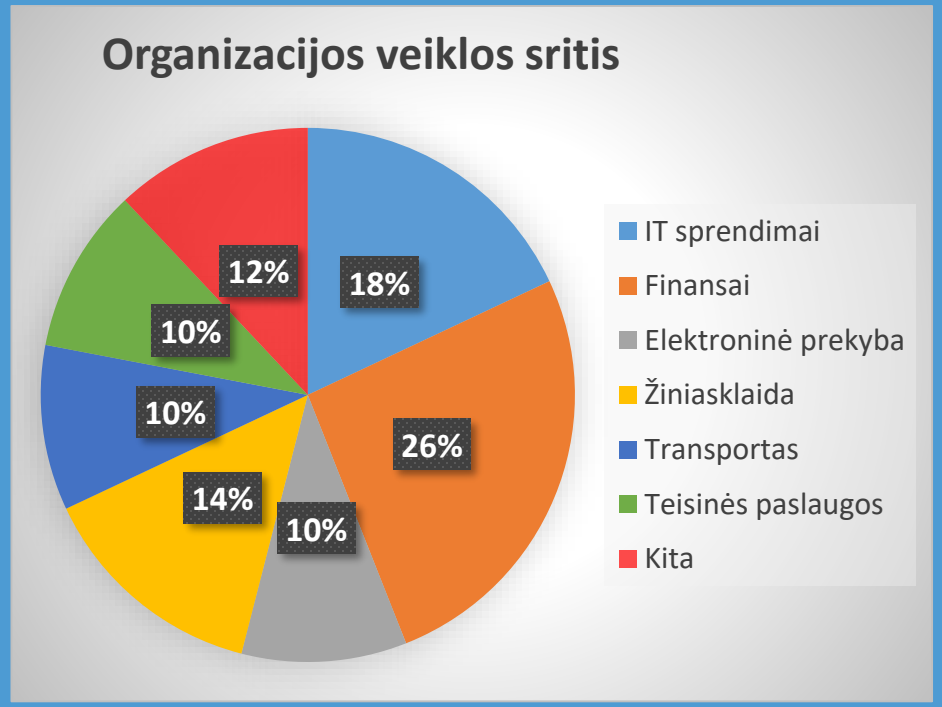


4. Privataus sektoriaus organizacijų apklausa

Apklausoje dalyvavo įvairaus dydžio organizacijos iš septynių veiklos sričių

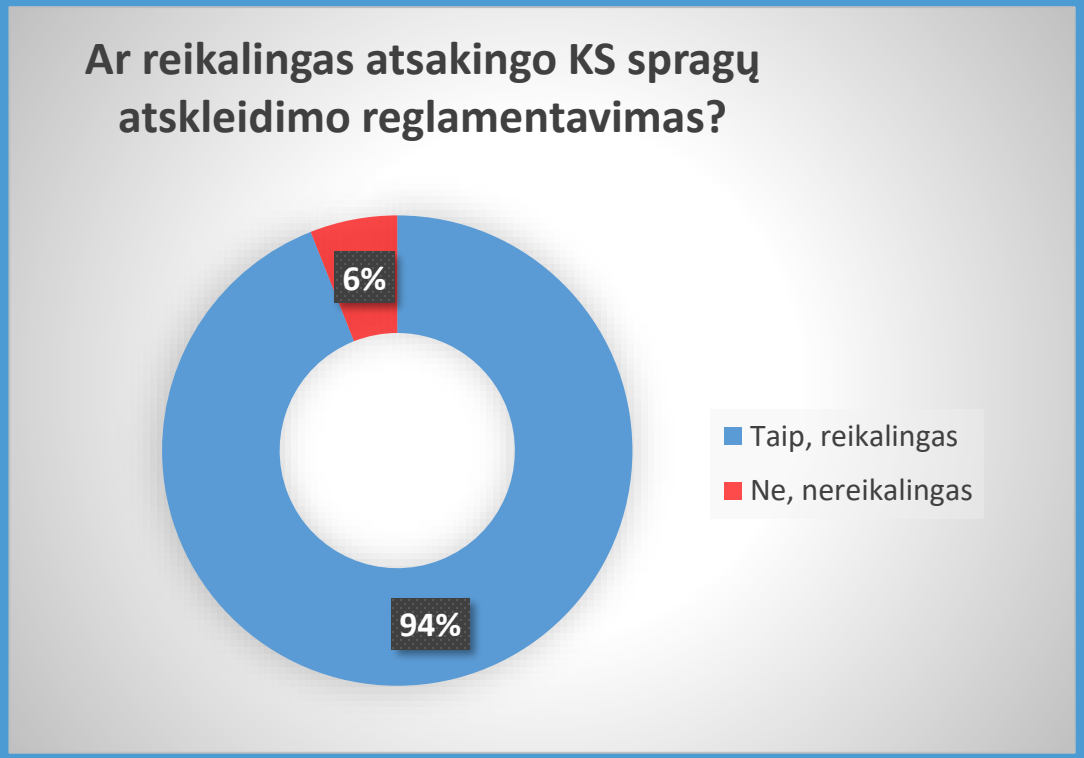
Siekiant nustatyti atsakingo KS spragų atskleidimo poreikį Lietuvoje, buvo atlikta privataus sektoriaus organizacijų apklausa. Šioje apklausoje dalyvavo 50 atstovų iš įvairaus dydžio organizacijų, kurių veiklos sritys apėmė IT sprendimų kūrimą, finansus, elektroninę prekybą, žiniasklaidą, transportą, teisines paslaugas ir kitas su IT arba ryšių technologijų naudojimu susijusias sritis.





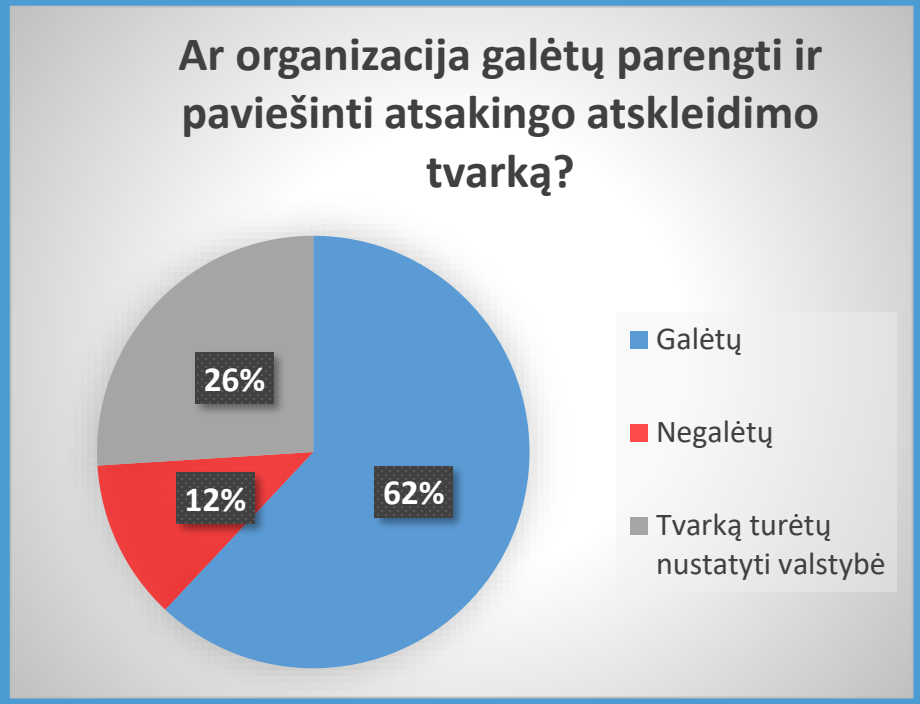
Informacinio turto apsaugą užtikrinti – svarbu, reglamentavimo – reikia

Visų apklausoje dalyvavusių organizacijų atstovai vienareikšmiškai teigė, kad jų atstovaujamoms organizacijoms svarbu užtikrinti maksimalią joms priklausančio informacinio turto apsaugą. Tuo pačiu metu, net 94 procentai apklausos dalyvių išreiškė palaikymą atsakingo KS spragų praktikos Lietuvoje reglamentavimui, kuris suteiktų galimybę spragą aptikusiam asmeniui apie ją pranešti organizacijai, kurios IT arba ryšių sistemoje ji buvo aptikta. Pasisakę už reglamentavimą asmenys taip pat atkreipė dėmesį į tai, kad atsakingo atskleidimo praktikos reglamentavimas neturėtų palikti vietos interpretacijoms.



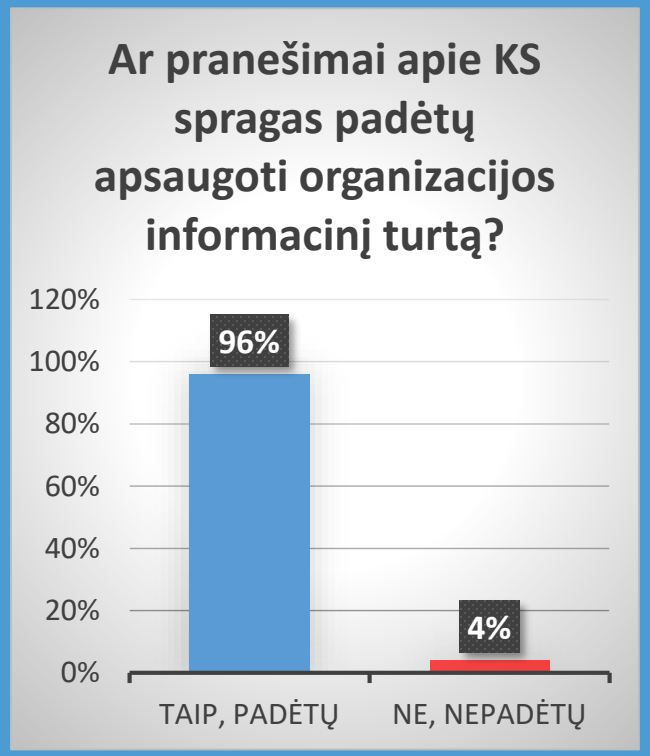
Atsakingo atskleidimo tvarkas viešinti galėtų, bet nuomonės išsiskiria dėl atlygio

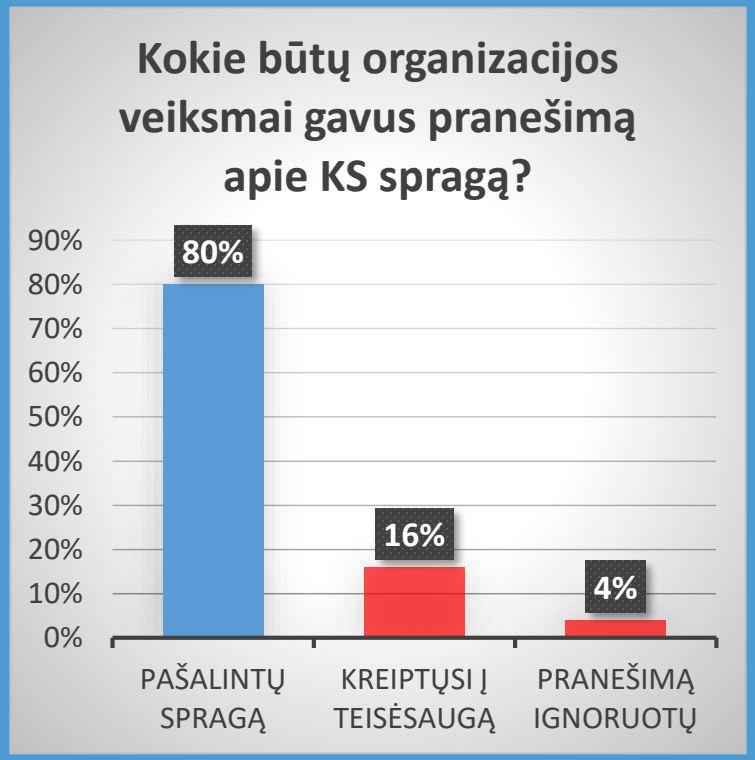
Dauguma apklausos dalyvių teigė, kad jų atstovaujamos organizacijos galėtų paviešinti savo atsakingo KS spragų atskleidimo tvarkas, tačiau pripažino, kad būtų naudinga jei valstybė publikuotų šių tvarkų ruošimo gaires. Nemaža dalis respondentų (26%) teigė, kad tokia tvarka turėtų būti bendra ir ją turėtų paruoši valstybė, tuo metu tie, kurie teigė, kad susilaikytų nuo tokios tvarkos viešinimo, savo pasirinkimą grindė manymu, kad atsakingo atskleidimo tvarkos atsiradimas skatintų nusikaltimus kibernetinėje erdvėje. Apklausos dalyviai išreiškė nuomonę ir dėl atlygio už geranoriškus pranešimus apie KS spragas. Nors daugelis respondentų teigė, kad jų organizacija suteiktų atlygį už pranešimus apie spragas, toks atlygis priklausytų nuo aptiktos spragos reikšmingumo ir dažniausiai apsiribotų organizacijos atributika. Daugiau nei ketvirtadalis respondentų, teigusių, kad aptinkantys spragas asmenys turėtų veikti neatlygintinai, baiminosi, kad atlygintina KS spragų atskleidimo praktika galėtų atverti kelią piktnaudžiavimui.



Į pranešimus apie KS spragas žiūri palankiai, jais dalintųsi su valstybe

Dauguma (96%) respondentų teigė, kad pranešimai apie KS spragas padėtų apsaugoti jų atstovaujamų organizacijų informacinį turtą, tačiau pabrėžė, kad kiekvieną pranešimo atvejį vertintų atskirai. Dauguma (80%) apklausos dalyvių teigė, kad jų organizacija pašalintų KS spragą ir apie tai praneštų ją aptikusiam asmeniui, o į teisėsaugą kreiptųsi tik tuo atveju jei šio asmens veiksmų teisėtumas keltų įtarimų. Tik maža dalis apklausos dalyvių (4%) teigė, kad pranešimus apie spragas ignoruotų, remdamiesi nuostata, kad didžioji dalis gaunamų pranešimų nebūtų reikšmingi. Sprendžiant pagal gautus atsakymus, didžioji dalis organizacijų (74%) dalintųsi gauta informacija apie spragas su atsakinga valstybine institucija, tačiau dažnai tai darytų pašalinus aptiktą spragą arba įsitikinus, kad ši informacija nebus platinama.





Išvados

- NKSC duomenimis, didžiąją dali Lietuvoje užregistruojamų KS incidentų sudaro įrenginių saugumo spragos bei įsilaužimai į RIS, o su KS iššūkiais susiduria tiek viešojo, tiek privataus sektorių subjektai.
- Lietuvos KS tarptautinis vertinimas yra itin aukštas, tačiau šaliai, siekiant visapusės kibernetinės brandos, svarbu sukurti sąlygas atsakingo KS spragų atskleidimo praktikos atsiradimui. Ši praktika ne tik prisidėtų prie augančio Lietuvos kibernetinio saugumo, bet ir duotų atkirtį KS specialistų trūkumui.
- Egzistuoja bent keturios KS spragų atskleidimo praktikos, tačiau siekiant suvaldyti potencialias rizikas ir užtikrinti maksimalią naudą visoms KS spragos atskleidimo procese dalyvaujančioms suinteresuotoms šalims, derėtų rinktis atsakingo atskleidimo praktiką.
- Šiuo metu trūksta teisinio reglamentavimo arba rekomendacinio pobūdžio dokumentų, apibrėžiančių atsakingo atskleidimo sąvokas, sampratą ir tvarką.
- Informacija apie atsakingo KS spragų atskleidimo praktiką Lietuvoje nėra paplitusi, o tokią praktiką taiko tik pavienės Lietuvoje veiklą vykdančios organizacijos.
- Nustatyta, kad iš visų kibernetinį saugumą Lietuvoje reglamentuojančių teisės aktų, septyni iš jų yra aktualūs atsakingo KS saugumo praktikos kūrimui.

Išvados

- Lietuvos Kibernetinio saugumo strategija yra vienintelis teisės aktas, kuriame užsimenama apie atsakingo KS spragų atskleidimo praktiką.
- Įvertinus esamą teisinę aplinką, atsakingo atskleidimo praktikos įteisinimui reikėtų įvykdyti LR kibernetinio saugumo įstatymo ir Vyriausybės nutarimo „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeitimus.
- Konsultacijų su Lietuvos teisėsaugos atstovais metu nustatyta, kad su atsakingo atskleidimo praktika susiję veiksmai galėtų būti laikomi teisėtais, jei kibernetinio saugumo subjektas, kurio IT arba ryšių sistemose aptinkama spraga, viešina atsakingo atskleidimo tvarką, apibrėžiančią šiame procese dalyvaujančių šalių veiklos ribas, o spragą aptikęs asmuo laikosi teisės aktuose nustatytų atsakingo atskleidimo sąlygų ir tvarkos.
- Tarptautinių teisinių nuostatų analizė atskleidė atsakingo atskleidimo praktikos suderinamumą su kertiniais ES teisės aktais.
- Atlikus privataus sektoriaus organizacijų apklausą, nustatyta nekvestionuojama informacinio turto svarba bei išsiaiškinta, kad dauguma privataus sektoriaus organizacijų palaikytu atsakingo KS spragų atskleidimo praktikos kūrimą ir reglamentavimą Lietuvoje.

Šaltiniai

- https://www.hackerone.com/blog/What-percentage-your-software-vulnerabilities-have-GDPR-implications
- https://www.nksc.lt/doc/biuleteniai/2019-04-11%20Imituot%C5%B3%20lai%C5%A1k%C5%B3%20ir%20svetain%C4%97s%20analiz%C4%97.pdf
- https://www.nksc.lt/pranesti-spraga.html
- http://kauno.diena.lt/naujienos/verslas/ekonomika/ivardijo-didziausias-rizikas-lietuvofinansu-sistemai-872344
- https://ncsi.ega.ee/country/lt/183/#details
- https://ltlife.lt/lt-life-english/lithuania-takes-the-4th-position-in-the-global-cybersecurity-index/
  https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/lithuania-cybersecurity-capacity-review-2017
- https://www.paysera.lt/v2/lt-LT/saugumas/pranesimai-apie-saugumo-spragas
- https://www.hostinger.com/responsible-disclosure-policy
- https://www.swedbank.se/om-oss/sakerhet/report-a-security-flaw.html
- https://www.visma.com/trust-centre/smb/security-and-privacy/operational/responsible-disclosure/
- https://spectrocoin.com/en/bug-bounty.html
- https://www.dokobit.com/compliance/vulnerability-disclosure-policy
- https://www.prokuraturos.lt/lt/veiklos-sritys/baudziamasis-persekiojimas/nusikaltimai-elektronineje-erdveje/185
- https://www.e-tar.lt/portal/lt/legalAct/TAR.2B866DFF7D43/asr
- https://www.nrdcs.lt/en/press-releases/lithuania-s-cyber-security-capacity-are-we-cyber-ready-to-embrace-digital-era-/80
- https://ncsi.ega.ee/country/lt/
- https://gdpr-info.eu/
- http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN
- https://www.sans.org/reading-room/whitepapers/threats/defineresponsible-disclosure-932
- https://www.thegfce.com/documents/publications/2017/11/21/coordinated-vulnerability-disclosure