PATVIRTINTA
NKSC prie KAM direktoriaus
2022 m. gruodžio 5 d.
įsakymu Nr. 1-102

NACIONALINĖS KIBERNETINIO SAUGUMO PRATYBOS

„KIBERNETINIS SKYDAS 2022“

ATASKAITA

VISUOMENEI

TLP: WHITE

SANTRUMPŲ SĄRAŠAS

CR – virtualus kibernetinis poligonas (angl. *Cyber Range*)

KIVT – kibernetinius incidentus valdančios ir (ar) tiriančios institucijos

KS2022 – kibernetinis skydas 2022

KSS – kibernetinio saugumo subjektai

KTU – Kauno technologijos universitetas

NKIVP – kibernetinių incidentų valdymo planas

NKSC – Nacionalinis kibernetinio saugumo centras

SL – siužeto linija

VI – vietinis instruktorius

TURINYS

SANTRAUKA

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Kauno technologijos universitetu, 2022 m. spalio 18-20 dienomis rengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2022“ (toliau – Pratybos). Pratybomis buvo siekiama formuoti praktinius pratybų dalyvių kibernetinio saugumo įgūdžius, patikrinti kibernetinių incidentų valdymo procedūras, gerinti bendradarbiavimą tarp kibernetinius incidentus valdančių ir (ar) tiriančių institucijų ir kibernetinio saugumo subjektų.

Iš viso Pratybose dalyvavo 116 organizacijų (pratybose KS2021 dalyvavo 92 organizacijos). 107 dalyvavusios organizacijos yra valstybės informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai (KS2021 tokių buvo 87 vnt.). Didžiąją pratybose dalyvaujančių organizacijų dalį sudarė valstybinės institucijos (ministerijoms pavaldžios įstaigos), sveikatos priežiūros įstaigos, energetikos bendrovės, finansų institucijos, universitetai ir kt. organizacijos.

Pratybų dalyvių skaičius buvo nepakankamas, kad pasiekti Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarime Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ nustatytus vertinimo kriterijus. 4 kriterijus „Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų dalis, ne mažesnė nei nurodyta“ 2021 m. – 60%, 2023 m. – 70%, tad numanomas 65% kriterijus 2022 m. nebuvo pasiektas. Faktiškai pasiekta 32,1 proc. arba 107 vnt. (pratybose KS2021 – 21,7% arba 87 vnt.).

Šiais metais, populiariausia, dažniausiai dalyvaujančių organizacijų pasirinkta pratybų SL buvo *fišingo* simuliacija – (SL4), vykdyta per *GoPhish* platformą. Ja buvo siekiama patikrinti personalo atsparumą suklastotiems (*phishing*) laiškams. Pratybų metu SL4 dalyvaujančios organizacijos išsiuntė virš 56 tūkst. laiškų savo darbuotojams.

Pratybose identifikuotos pamokos yra užfiksuotos ir bus įvertintos tobulinant kibernetinio saugumo reglamentavimą.

97% vietinių instruktorių pritarė teiginiui, kad Pratybos jų organizacijai buvo naudingos.

NUORODOS

A. Lietuvos Respublikos Kibernetinio saugumo įstatymas (2014 m. gruodžio 11 d. Nr. XII-1428);

B. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“

C. Lietuvos Respublikos Vyriausybės 2019 m. liepos 3 d. nutarimas Nr. 709 „Dėl nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinio veiklos plano patvirtinimo“;

D. Lietuvos Respublikos krašto apsaugos ministro 2022 m. vasario 17 d. įsakymu Nr. V-137 „Dėl Lietuvos Respublikos krašto apsaugos ministro valdymo sričių 2022-2024 metų strateginio veiklos plano patvirtinimo“

ĮVADAS

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Kauno technologijos universitetu (toliau – KTU), 2022 m. spalio 18-20 dienomis rengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2022“ (toliau – Pratybos). Nacionalinių kibernetinių saugumo pratybų rengimas yra numatytas Lietuvos Respublikos Vyriausybės nutarimuose ir Lietuvos Respublikos krašto apsaugos ministro įsakyme (nuorodos B, C, D).

Šia ataskaita siekiama pristatyti pratybų koncepciją, eigą, pasiektus rezultatus..

KIBERNETINIS SKYDAS 2022

1. Kibernetinio saugumo subjektų dalyvavimas

Pratybose buvo kviečiami dalyvauti kibernetinio saugumo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjai (toliau bendrai – kibernetinio saugumo subjektai, sutrumpintai - KSS), taip pat kibernetinius incidentus valdančios ir (ar) tiriančios institucijos (toliau KIVT institucijos) bei pavojingo kibernetinio incidento valdymą koordinuojančios institucijos (toliau – KIVK institucijos). Papildomai, NKSC sudarė sąlygas pratybose dalyvauti ir kitoms organizacijoms, išreiškusioms tokį poreikį. Toliau visi pratybų dalyviai bendrai vadinami Pratybų auditorija.

Iš viso Pratybose dalyvavo 116 organizacijų (pratybose KS2021 dalyvavo 92 organizacijos). 107 dalyvavusios organizacijos yra valstybės informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai (KS2021 tokių buvo 87 vnt.). Didžiąją pratybose dalyvaujančių organizacijų dalį sudarė valstybinės institucijos (ministerijoms pavaldžios įstaigos), sveikatos priežiūros įstaigos, energetikos bendrovės, finansų institucijos, universitetai ir kt. organizacijos.

Pratybų dalyvių skaičius buvo nepakankamas, kad būtų pasiektas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarime Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ nustatytas vertinimo kriterijus. 4 kriterijus „Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų dalis, ne mažesnė nei nurodyta“ 2021 m. – 60%, 2023 m. – 70%, tad numanomas 65% kriterijus 2022 m. nebuvo pasiektas. Faktiškai pasiekta 32,1 proc. arba 107 vnt. (pratybose KS2021 – 21,7% arba 87 vnt.).

Pavyzdžiui, iš keturiolikos LR ministerijų dalyvavo šešios, t.y. 43 proc. Esant tokiam ministerijų dalyvavimo lygiui, joms pavaldžios įstaigos irgi renkasi Pratybose nedalyvauti. Siekiant nustatyto kriterijaus įgyvendinimo, būtina rasti būdus, kaip KSS paskatinti dalyvauti nacionalinėse kibernetinio saugumo pratybose ateityje.

LR ministerijų dalyvavimas pratybose „Kibernetinis skydas“

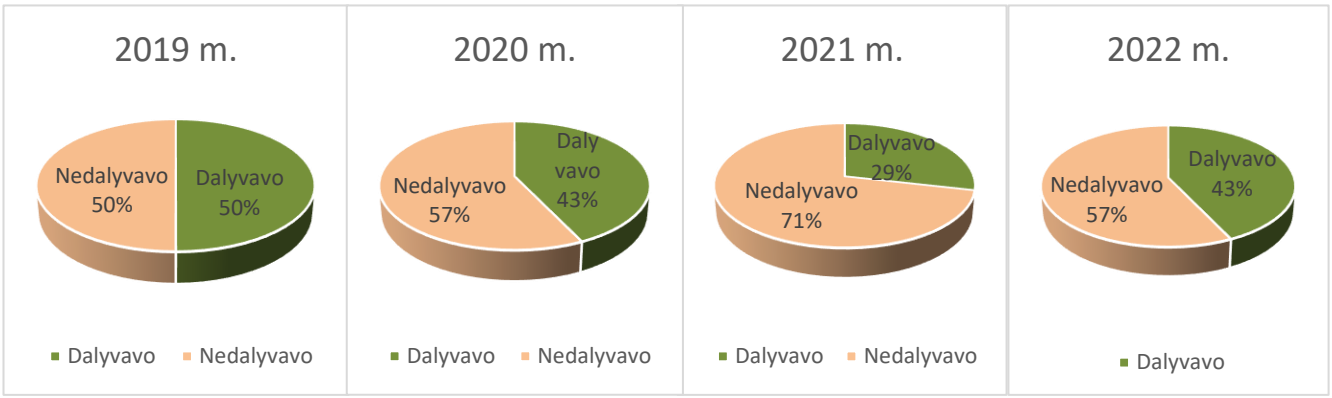


Diagrama 1: LR ministerijų dalyvavimas pratybose "Kibernetinis skydas" 2019 m., 2020 m., 2021 m., 2022 m.

2. Pratybų tikslas ir siekiniai

Pratybų tikslas

Pratybų dalyvių praktinių kibernetinio saugumo įgūdžių gerinimas.

Pratybų siekiniai

(1) Patikrinti ir treniruoti KIVT institucijų, KIVK institucijų ir KSS gebėjimus vykdyti Kibernetinių incidentų valdymo plane (toliau – Planas) nustatytus veiksmus; identifikuoti tobulintinas Plano sritis.

(2) Patikrinti KIVT institucijų ir KSS vidines kibernetinio incidento valdymo procedūras.

(3) Treniruoti Pratybų auditoriją aptikti ir analizuoti kibernetinius incidentus.

(4) Treniruoti Pratybų auditoriją dalintis kibernetinių incidentų informacija, gerinti bendradarbiavimą, naudotis Kibernetinio saugumo informacinio tinklo paslaugomis (MISP platforma).

3. Pratybų koncepcija

Organizuojant pratybas KS2022 remtasi NATO kibernetinės gynybos pratybų „Kibernetinė koalicija“ (angl. *Cyber Coalition*) modeliu. Vienas pagrindinių jų principų – kuo didesnis realistiškumas (angl. *train as you fight*). Buvo siekiama, kad pratybos vyktų aplinkoje, kuri yra kuo artimesnė kasdieninei Pratybų auditorijos aplinkai. Kitaip sakant, organizacija turėjo dalyvauti su tokiais pajėgumais, personalu, procedūromis, kuriuos realiai turi. Nebuvo formuojami laikini personalo dariniai, skirti specialiai pratyboms, kurie kasdien neegzistuoja, nebuvo perkama specialiai pratyboms skirta įranga. Pratybos vyko organizacijų patalpose, personalas dalyvavo iš savo darbo vietų, incidentus valdė, tyrė savo turimais įrankiais, pagal savo kasdienines procedūras.

Vietiniai instruktoriai savo nuožiūra parinko savo organizacijos įsitraukimo laipsnį, kuriuos pratybų organizatorių parengtus kibernetinius incidentus jų organizacija turėjo tirti ir valdyti pratybų metu. Atsižvelgiant į šį pasirinkimą, organizacijos struktūrą ir procedūras vietinis instruktorius turėjo pritaikyti tipinį pratybų scenarijų savo organizacijai.

Kibernetiniai incidentai buvo įvykdyti Kauno technologijos universiteto pratyboms parengtoje infrastruktūroje, o dalyviams pateikti techniniai artefaktai (darbo stočių, tarnybinių stočių diskų atvaizdai (angl. *image*), žurnaliniai įrašai (angl. *logs*), tinklo paketų kopijos, tinklo srauto įrašai (angl. *netflow*), sparčiosios atminties kopijos (angl. *RAM dump*). Informaciją apie įvykius ir incidentus pratybų erdvėje vietinis instruktorius pratybų auditorijai pateikdavo el. paštu remiantis iš anksto NKSC parengtais informaciniais įskiepiais.

Siekiant užtikrinti organizacijos sistemų saugą ir suteikti visus tyrimui reikalingus įrankius, šiais metais pratybų dalyviams buvo pasiūlyta naujovė – incidentus tirti kontroliuojamoje uždaroje interaktyvioje aplinkoje, naudojant NKSC virtualų kibernetinio saugumo poligoną (angl. Cyber Range). Remiantis techniniais artefaktais, virtualioje aplinkoje atkurtas pratybų scenarijus bei sukurtos išorinės darbo vietos skirtus tyrėjams.

4. Pratybų renginiai ir dalyviai

Pakvietimą dalyvauti pratybose ir į jų planavimą paskirti savo organizacijos atstovą (vietinį instruktorių) NKSC išsiuntė 312 ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojams ir tvarkytojams.

Iš viso į NKSC kvietimą atsiliepė ir savo atstovą – vietinį instruktorių - pratybų planavimui nurodė 169 organizacijos.

Dalis organizacijų, kurios ketino dalyvauti pratybose, vėliau dalyvauti pasirengime nustodavo, dėl tokio sprendimo pratybų organizatorių neinformavo.

Pratyboms pasibaigus, visoms nedalyvavusioms organizacijoms, buvo išsiųsta apklausa, kurią užpildė 105 organizacijos. Apklausos rezultatuose atsispindi dvi pagrindinės nedalyvavimo priežastys – personalo ir kompetencijų trūkumas. Dalis nurodė, jog norint dalyvauti kitų metų pratybose turėtų įgyvendinti pokyčius savo organizacijos viduje. Taip pat, nedalyvavusios organizacijos norėtų gauti daugiau pagalbos rengiantis pratyboms, pavyzdžiui, mokymus vietiniams instruktoriams, kurie dalyvauja pirmą kartą.

Balandžio, birželio ir rugsėjo mėnesį internetu vietiniams instruktoriams buvo surengtos pratybų planavimo konferencijos. Šiuose renginiuose buvo pristatyta tipinis pratybų scenarijus, kibernetiniai incidentai, paaiškinta vietinio instruktoriaus atsakomybė, pasirengimo pratyboms metu reikalingi atlikti darbai. Vietiniai instruktoriai tipinį pratybų scenarijų prisitaikė savo organizacijai.

Po pratybų surengti techniniai mokymai kibernetinio saugumo specialistams, dalyvavusiems pratybose. Į mokymus užsiregistravo 237 specialistai iš KSS, juose buvo pademonstruota, kokiu būdu buvo galima ištirti pratyboms KS2022 parengtus kibernetinius incidentus. Iš 237 dalyvių techninius mokymus ne tik išklausė, bet ir užduotis išsprendė bei vertinimui atsiuntė 39 dalyviai.

Pratybose spalio 18-20 dienomis iš viso dalyvavo 116 organizacijos. Laikoma, kad organizacija dalyvavo pratybose, jeigu pateikė pranešimą NKSC apie pratybų metu „įvykusį“ kibernetinį incidentą arba vykdė *fišingo* simuliaciją savo personalo atsparumo tokio tipo atakoms, patikrinti. Apklausos, kurią užpildė 92 vietiniai instruktoriai, duomenimis vidutiniškai pratybose kibernetinio incidento valdyme iš organizacijos dalyvavo 9 darbuotojai, įskaitant ne tik kibernetinio saugumo specialistus, IT administratorius, bet ir viešųjų ryšių specialistus, teisininkus, aukščiausio bei vidutinio lygmens vadovus.

5. Pratybų scenarijus

Vietiniai instruktoriai atsižvelgdami į organizacijos ambicijas pratybų scenarijų galėjo vystyti remdamiesi viena ar keliomis iš anksto paruoštomis siužeto linijomis (toliau – SL). Pasirinktas SL vietinis instruktorius turėjo pritaikyti savo organizacijai, atsižvelgdamas į jos struktūrą, procedūras ir/ar konkrečius poreikius. Atsižvelgiant į organizacijoms keliamas grėsmes, KS2022 pratyboms buvo paruoštos keturios SL:

(1) Organizacija yra informuojama, dėl internete pardavinėjamos galimai jų tinklaraščio duomenų bazės kopijos su piliečių/klientų asmens duomenimis. Atliekant tyrimą paaiškėja, kad piktavalis įsilaužė į organizacijos viešą tinklaraštį panaudodamas viešai žinomą pažeidžiamumą.

(2) Organizacija yra informuojama, dėl galimai nutekintų darbuotojų asmens duomenų (tapatybės kortelės ir atlyginimų suvestinė). Atliekant tyrimą, patvirtinamas asmens duomenų nutekėjimas iš organizacijos viešai prieinamų sistemų. Identifikuojami incidento paveikti asmenys.

(3) Organizacija yra informuojama, dėl galimai nutekintų asmens duomenų iš vidinių organizacijos sistemų. Atliekant tyrimą, nustatoma, kad piktavališki veiksmai pradėti vidinio organizacijos darbuotojo, kuriam buvo pasiūlytas atlygis iš trečiosios šalies.

(4) Organizacijos personalui surengta *fišingo* (angl. *phishing*) simuliacija. Jos metu buvo tikrinamas personalo atsparumas tokio tipo atakai, siunčiant el. laiškus ir prašant suvesti duomenis į svetaines, kurių domeno vardai ir dizainas yra panašūs į visuomenei žinomas paslaugas. Šiam tikslui buvo naudoti domenai: rnicrosoftonline.it, tyrimai.it, sodra.it, vrni.it, epolicija.it, epaslaugos.it, omvina.lt. Šios pratybų dalies metu surinkti duomenys nebuvo saugomi, buvo fiksuojamas tik nuorodos atidarymo ir duomenų suvedimo faktas.

Kiekvieną siužeto liniją sudaryta iš jau paruoštų techninių artefaktų (virtualių įrenginių disko kopijų, tinklo srauto kopija) skirtų tyrimui remiantis vidinėmis organizacijos procedūromis, bei informacinių įskiepių (el. pranešimų, tyrimo klausimų/atsakymų) skirtų inicijuoti kibernetinį incidentų valdymą ir informuoti NKSC, Valstybinę duomenų apsaugos inspekciją, policiją. Pratybų metu, 56 organizacijos iniciavo kibernetinio incidento valdymą ir informavo NKSC.

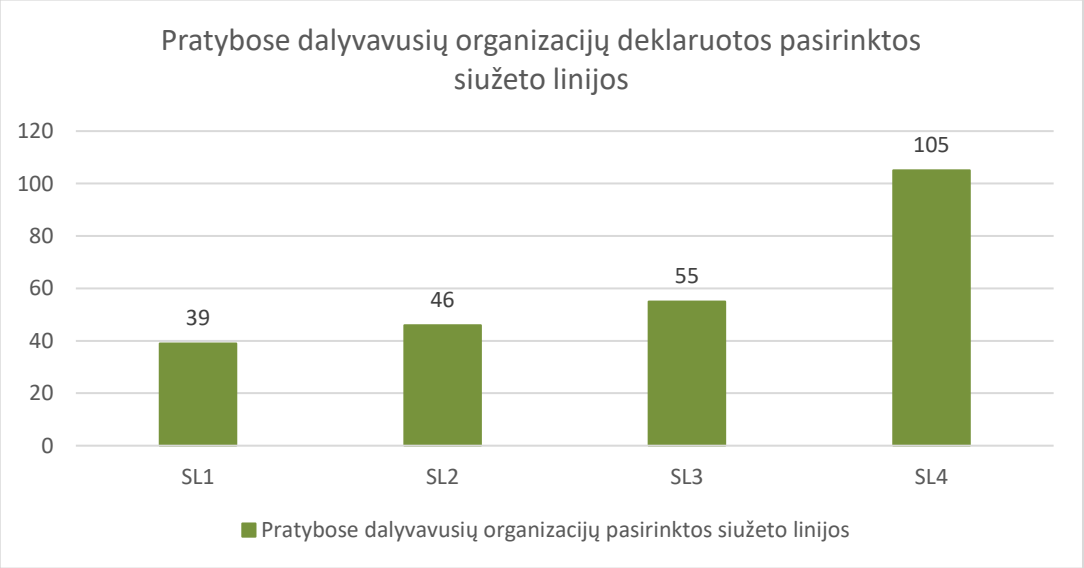


Diagrama 1: deklaruotas SL pasirinkimas*

*Dalyvavimą SL1 deklaravo 39 organizacijos, SL2 – 46 organizacijos ir t. t.

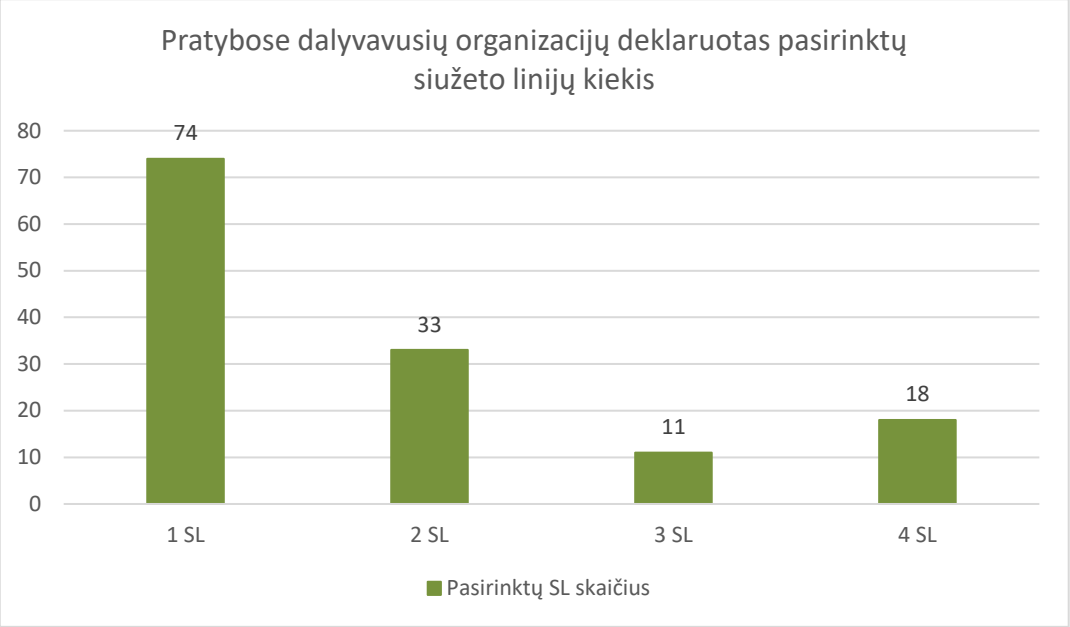
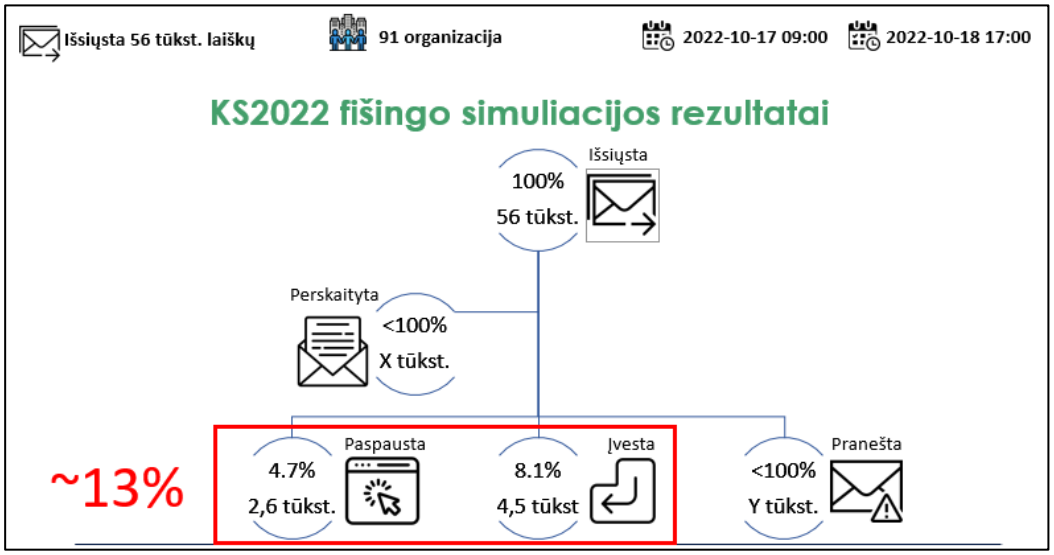


Diagrama 2: deklaruotas pasirinktų SL skaičius*

*74 organizacijos planavo dalyvauti vienoje SL, 33 organizacijos – dvejose SL ir t.t.

Šiais metais, populiariausia, dažniausiai dalyvaujančių organizacijų pasirinkta pratybų SL buvo *fišingo* simuliacija – (SL4), vykdyta per *GoPhish* platformą. Ja buvo siekiama patikrinti personalo atsparumą suklastotiems (*phishing*) laiškams. Pratybų metu SL4 dalyvaujančios organizacijos išsiuntė virš 56 tūkst. laiškų savo darbuotojams. 4,7% (2,6 tūkst.) paspaudė nuorodą, bet duomenų nesuvedė, o 8,1% (4,5 tūkst.) atidarė nuorodą ir įvedė duomenis. Iš viso nuoroda buvo paspausta arba duomenys suvesti beveik 13% atvejų.



Paveikslėlis 1: *fišingo* simuliacijos statistika

Atsižvelgiant į tai, kad fišingo simuliacija vyko tik tris dienas, darytina prielaidą, kad dalis iš 56 tūkst. siųstų laiškų likti neperskaityti. Vykdant fišingo simuliaciją ilgiau, ir tokiu

būdu padidėjus gavėjų, perkaičiusių laiškus daliai, rezultatas greičiausiai būtų dar didesnis (ir prastesnis).

Šios siužeto linijos rezultatai parodo, kad yra būtina stiprinti kibernetinio saugumo subjektų personalo atsparumą *fišingo* laiškams, nuolat vykdant personalo švietimą ir *fišingo* simuliacijas.

Pratybose buvo aktyviai imituojama žiniasklaidos rolė. Ją atliko Lietuvos kariuomenės KASP Didžiosios kovos apygardos 8-osios rinktinės kariai, kurie pratybų metu skambino incidentą valdančioms organizacijoms ir prašydavo jų pateikti visuomenę dominančią informaciją.