PATVIRTINTA
NKSC prie KAM direktoriaus
2023 m. gruodžio 13 d.
įsakymu Nr. 1-99

NACIONALINĖS KIBERNETINIO SAUGUMO PRATYBOS

„KIBERNETINIS SKYDAS OPEX 2023“

ATASKAITA

VISUOMENEI

KIBERNETINIS SKYDAS 2023

TLP: WHITE

SANTRUMPŲ SĄRAŠAS

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

KIVT – kibernetinius incidentus valdančios ir (ar) tiriančios institucijos

KIVK – pavojingo kibernetinio incidento valdymą koordinuojančios institucijos

KS2023 OpEx – Kibernetinis Skydas OpEx 2023

KSS – kibernetinio saugumo subjektai

NKIVP – kibernetinių incidentų valdymo planas

NKSC – Nacionalinis kibernetinio saugumo centras

VU – Vilniaus universitetas

SL – siužeto linija

VI – vietinis instruktorius

TURINYS

SANTRAUKA

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Vilniaus universitetu, 2023 m. spalio 17-19 dienomis rengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas OpEx 2023“ (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 ir ugdyti viešosios komunikacijos įgūdžius.

Iš viso Pratybose dalyvavo ir kibernetinius incidentus valdė 82 organizacijos (pratybose KS2022 kibernetinius incidentus valdė 56 organizacijos). 77 dalyvavusios organizacijos yra valstybės informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai (KS2022 tokių buvo 53 vnt.). Didžiąją pratybose dalyvaujančių organizacijų dalį sudarė valstybinės institucijos (ministerijoms pavaldžios įstaigos), sveikatos priežiūros įstaigos, energetikos ir vandentvarkos bendrovės, finansų institucijos ir kitos 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. Kriterijus nr. 4 „Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų dalis, ne mažesnė nei nurodyta“ 2023 m. – 70%, reikšmė nebuvo pasiekta. Faktiškai pasiekta 25 proc. arba 77 vnt. (pratybose KS2022 – 17% arba 53 vnt.).

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

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 Krašto apsaugos ministro 2023 m. kovo 6 d. įsakymu Nr. V-180 „Dėl Lietuvos Respublikos krašto apsaugos ministro valdymo sričių 2023-2025 metų strateginio veiklos plano patvirtinimo“;

D. Lietuvos Respublikos valstybės kontrolės atlikto valstybės audito „Kibernetinio saugumo užtikrinimas“ ataskaita (2022 m. spalio 27 d. Nr. VAE-10).

ĮVADAS

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Vilniaus universitetu (toliau – VU), 2023 m. spalio 17-19 dienomis rengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas OpEx 2023“ (toliau – Pratybos). Nacionalinių kibernetinių saugumo pratybų rengimas yra numatytas Lietuvos Respublikos Vyriausybės nutarime ir Lietuvos Respublikos krašto apsaugos ministro įsakyme (nuorodos B, C).

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

KIBERNETINIS SKYDAS OPEX 2023

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 ir kibernetinius incidentus valdė 82 organizacijos (pratybose KS2022 kibernetinius incidentus valdė 56 organizacijos). 77 dalyvavusios organizacijos yra valstybės informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai (KS2022 tokių buvo 53 vnt.). Didžiąją pratybose dalyvaujančių organizacijų dalį sudarė valstybinės institucijos (ministerijoms pavaldžios įstaigos), sveikatos priežiūros įstaigos, energetikos ir vandentvarkos bendrovės, finansų institucijos ir kitos 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. Kriterijus nr. 4 „Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų dalis, ne mažesnė nei nurodyta“ 2023 m. – 70%, tad kriterijus 2023 m. nebuvo pasiektas. Faktiškai pasiekta 25 proc. arba 77 vnt. (pratybose KS2022 – 17% arba 53 vnt.).

Pavyzdžiui, iš keturiolikos LR ministerijų dalyvavo penkios, t.y. 36 % visų LR ministerijų. 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“

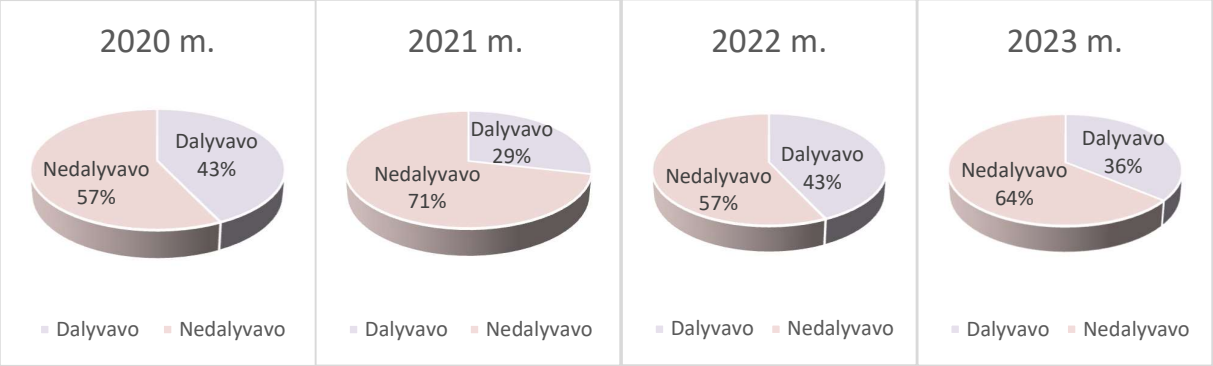

Diagrama 1: LR ministerijų dalyvavimas pratybose „Kibernetinis skydas“ 2020 m., 2021 m., 2022 m., 2023 m.

2. Pratybų tikslas ir siekiniai

Pratybų tikslas

Pratybų dalyvių praktinių kibernetinio saugumo įgūdžių gerinimas.

Pratybų siekiniai

(1) Patikrinti ir treniruoti KIVT institucijų ir KSS gebėjimus vykdyti Nacionaliniame kibernetinių incidentų valdymo plane (toliau – Planas) nustatytus veiksmus.

(2) Patikrinti KIVT institucijų ir KSS vidines kibernetinio incidento valdymo planus ir procedūras; planų ir procedūrų neturinčias organizacijas skatinti juos pasirengti.

(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 (toliau – KSIT).

(5) Patikrinti ir ugdyti KSS viešosios komunikacijos gebėjimus.

3. Pratybų koncepcija

Organizuojant ir vykdant pratybas KS2023 OpEx buvo siekiama užtikrinti kuo didesnį realistiškumą (angl. *train as you fight*), kad pratybos vyktų aplinkoje, kuri yra kuo artimesnė kasdieninei Pratybų auditorijos aplinkai. Pratybose dalyvaujančios organizacijos buvo skatinamos dalyvauti pratybose su tokiais pajėgumais, personalu, procedūromis, kuriuos realiai turi, neformuoti laikinų, specialiai pratyboms skirtų, personalo darinių, kurie kasdien neegzistuoja, nepirkti specialiai pratyboms skirtos įrangos. Pratybos vyko organizacijų patalpose, personalas dalyvavo iš savo darbo vietų, incidentus valdė, tyrė savo turimais įrankiais, pagal savo vidinius kibernetinio incidento valdymo planus ir procedūras.

Vietiniai instruktoriai įvertinę savo organizacijos poreikius ir nustatę įsitraukimo laipsnį, rinkosi 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 bazinį pratybų scenarijų savo organizacijai.

Kibernetiniai incidentai buvo įvykdyti NKSC virtualiame kibernetinio saugumo poligone, kuriame su Vilniaus universiteto specialistų parama buvo parengta pratybų infrastruktūra.

Dalyviai incidentus galėjo tirti pasirinktinai arba NKSC virtualiame kibernetinio saugumo mokymų poligone arba atsisiunčiant artefaktus (darbo stočių, tarnybinių stočių diskų atvaizdus (angl. *image*), žurnaliniai įrašus (angl. *logs*), tinklo paketų kopijas, tinklo srauto įrašus (angl. *netflow*), sparčiosios atminties kopijas (angl. *RAM dump*)) ir tiriant juos savo infrastruktūroje. Poligone incidentus tyrė 35 organizacijos. Informaciją apie įvykius ir incidentus, vykstančius pagal pratybų scenarijų, vietinis instruktorius pratybų auditorijai pateikdavo el. paštu remiantis iš anksto NKSC parengtais informaciniais įskiepiais.

4. Pratybų renginiai ir dalyviai

Pakvietimą dalyvauti pratybose ir į jų planavimą paskirti savo organizacijos atstovą (vietinį instruktorių) NKSC išsiuntė 303 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 161 organizacija.

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

Pratyboms pasibaigus, visoms nedalyvavusioms organizacijoms, buvo išsiųsta apklausa, kurią užpildė 145 organizacijos. Apklausos rezultatuose atsispindi dvi pagrindinės nedalyvavimo priežastys – personalo ir kompetencijų trūkumas. Didelė dalis užpildžiusių

apklausą nurodė, jog pratybų vykdymą yra sudėtinga derinti su tiesioginėmis užduotimis dėl laiko trūkumo ir tai nulėmė jų apsisprendimą šiais metais nedalyvauti. 21% nedalyvavusių organizacijų nurodė, jog būtinai planuoja dalyvauti kitų metų Pratybose. 80% apklaustųjų nedalyvavusių organizacijų nurodė, kad turi patvirtintą incidentų valdymo planą.

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

Po pratybų surengti techniniai mokymai kibernetinio saugumo specialistams, dalyvavusiems pratybose. Į mokymus užsiregistravo 253 specialistai iš KSS, dalyvavo 222. Mokymų metu NKSC ir VU specialistai pademonstravo, kokiu būdu buvo galima ištirti pratyboms KS2023 OpEx parengtus kibernetinius techninius artefaktus – diskų atvaizdus. Iš 222 dalyvių techninius mokymus ne tik išklausė, bet ir užduotis išsprendė bei vertinimui atsiuntė 55 dalyviai.

Pratybose spalio 17-19 dienomis iš viso dalyvavo 82 organizacijos. Laikoma, kad organizacija dalyvavo pratybose, jeigu pateikė pranešimą NKSC apie pratybų metu „įvykusį“ kibernetinį incidentą. Apklausos, kurią užpildė 66 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.

Vietiniai instruktoriai atsižvelgdami į organizacijos kibernetinio saugumo brandą, pajėgumus ir ambicijas pratybų scenarijų galėjo vystyti remdamiesi viena ar keliomis iš anksto parengtomis 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, KS2023 OpEx pratyboms buvo parengtos trys SL:

(1) SL1 – pažeista internetinės svetainės turinio valdymo sistema. Tarptautinė grupuotė pažeidžia organizacijos turinio valdymo sistemą (TVS) ir geba skelbti kenkėjišką turinį organizacijos tinklalapyje.
(2) SL2 – pažeista pašto sistema. Vietinė grupuotė pažeidžia organizacijos pašto serverį ir geba perimti bei skaityti privačius organizacijos el. pašto pranešimus.
(3) SL3 – pažeistas organizacijos tinklas. Buvęs organizacijos darbuotojas įgyja neteisėtą prieigą prie organizacijos tinklo iš kurio geba pavogti konfidencialius

organizacijos dokumentus bei užšifruoja svarbius duomenis, reikalaudamas sumokėti išpirką duomenims atkurti.

Kiekvieną siužeto liniją sudaro parengti techniniai artefaktai (virtualių įrenginių disko kopijos) skirti tyrimui atlikti remiantis vidinėmis organizacijos procedūromis, bei informaciniai įskiepiai (el. pranešimai, socialinių tinklų pranešimai, bendravimo platformų įrašai, tyrimo klausimai/atsakymai) skirti inicijuoti kibernetinio incidento valdymą ir informuoti NKSC, Valstybinę duomenų apsaugos inspekciją, Policiją. Pratybų metu, 82 organizacijos iniciavo kibernetinio incidento valdymą ir informavo NKSC.

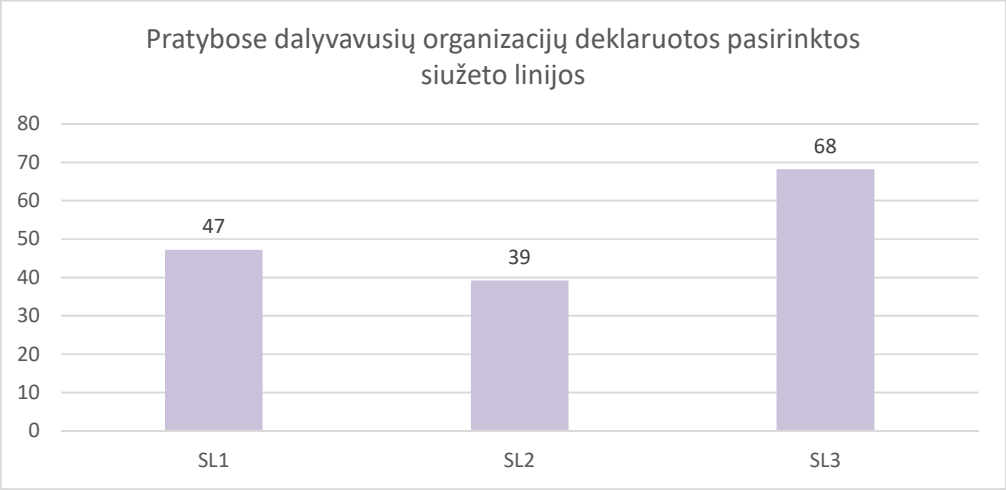

Diagrama 2: deklaruotas SL pasirinkimas

Dalyvavimą SL1 deklaravo 47 organizacijos, SL2 – 39 organizacijos, SL3 – 68 organizacijos.

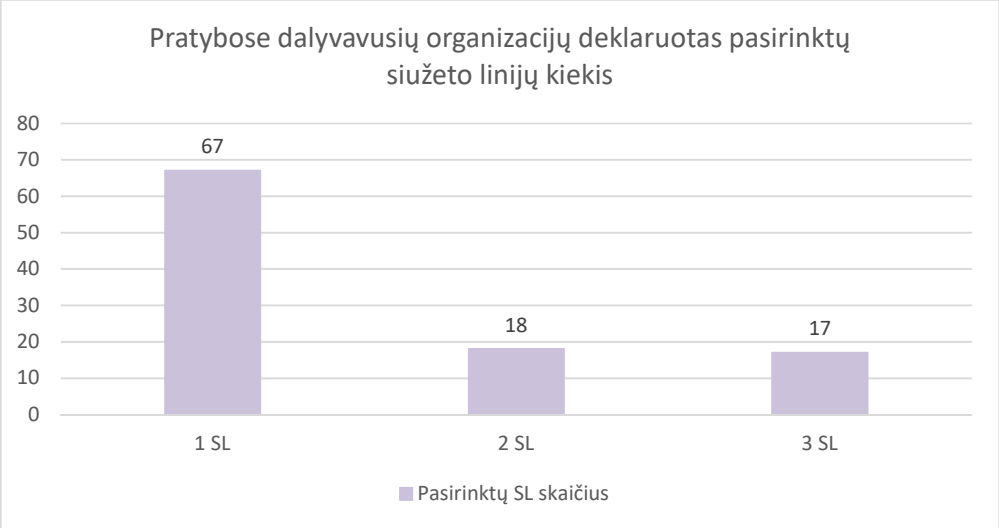

Diagrama 3: deklaruotas pasirinktų SL skaičius

67 organizacijos planavo dalyvauti vienoje SL, 18 organizacijų – dvejose SL ir 17 – trijose SL.

Populiariausia, dažniausiai dalyvaujančių organizacijų pasirinkta pratybų SL buvo SL3 – pažeistas organizacijos tinklas.

Šiais metais pratybose buvo skirta daugiau dėmesio organizacijų komunikacijos įgūdžių patikrinimui ir stiprinimui. Pratybų metu dalyvaujančių organizacijų viešosios komunikacijos ekspertai turėjo galimybę bendrauti su, žiniasklaidos rolė atliekančiais, Lietuvos kariuomenės KASP Didžiosios kovos apygardos 8-osios rinktinės kariais. 47 organizacijos iš 82 dalyvavusių pratybų metu pasirinko testuoti savo viešosios komunikacijos įgūdžius.

Bendravimas su žiniasklaidos atstovais vyko per įskiepius, trimis eskalavimo principo žingsniais kiekvienai SL:

(1) Žiniasklaidos atstovo užklausa el. paštu su klausimais. Organizacijai buvo skiriama valanda atsakymams pateikti, tai sudarė galimybę pasitikrinti komunikacijos įgūdžius turint ribotą laiką atsakymų pateikimui.

(2) Žiniasklaidos atstovo skambutis prašant papildyti ir patikslinti el. paštu pateiktą informaciją. Testuojami įgūdžiai gyvo telefoninio skambučio metu.

(3) Žiniasklaidos atstovo prašymas iki darbo dienos pabaigos atsiųsti pranešimą spaudai el. paštu, kuriame būtų pateikta visa informacija apie incidentą ir priemones, kurių organizacija ėmėsi, siekdama sumažinti reputacinę žalą.