PATVIRTINTA
NKSC prie KAM direktoriaus
2021 m. gruodžio 8 d.
įsakymu Nr. 1-79

NACIONALINIŲ KIBERNETINIO SAUGUMO PRATYBŲ „KIBERNETINIS SKYDAS 2021“ ATASKAITA VISUOMENEI

KIBERNETINIS SKYDAS 2021

TLP: WHITE

Turinys

1. SANTRAUKA

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Kauno technologijos universitetu, 2021 m. spalio 19-21 dienomis rengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2021“ (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 daugiau nei 670 asmenų iš 92 organizacijų. Didžiąją Pratybose dalyvaujančių organizacijų dalį – 87 organizacijos, sudarė valstybės informacinių išteklių arba ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai. Lyginant su ankstesniais metais, Pratybose dalyvaujančių valstybės informacinių išteklių arba ypatingos svarbos informacinių išteklių valdytojų arba tvarkytojų skaičius išaugo 35 proc. (2020 m. – 64 vnt.). Tačiau 87 organizacijos sudaro tik 21,7 proc. visų valstybės informacinių išteklių arba ypatingos svarbos informacinių išteklių valdytojų arba tvarkytojų, todėl šių metų pasiektas dalyvių skaičius buvo nepakankamas, kad būtų pasiekti Krašto apsaugos ministro 2021 kovo mėn. 17 d. įsakymu Nr. V-187 patvirtintame Lietuvos Respublikos krašto apsaugos ministro valdymo sričių 2021-2023 metų strateginiame veiklos plane nustatytas siektini kriterijai - 60 proc. (pasiekta 21,7 proc.) arba 200 organizacijų (pasiekta 87 vnt.).

Populiariausios, dažniausiai dalyvaujančių organizacijų pasirinktos pratybų siužeto linijos (toliau - SL) buvo susijusios su incidentais „Windows“ darbo stotimis (SL1 ir SL2) ir suklastotų laiškų siuntinėjimu (SL7). Tikėtina, kad dažnesnį SL1 pasirinkimą lėmė pastaraisiais metais stebėta „Emotet“ viruso veikla, SL2 - organizacijų susirūpinimas rizikomis, kurias įnešė poreikis dėl Covid-19 pandemijos darbą organizuoti nuotoliniu būdu. SL7 leido realiai patikrinti savo organizacijos personalo atsparumą suklastotiems (*phishing*) laiškams.

Pratybose pirmą kartą buvo surengtas Nacionaliniame kibernetinių incidentų valdymo plane numatytas koordinacinis susitikimas pavojingo incidento valdymui. Pratybų strateginio scenarijaus žaidimo metu paaiškėjo, kad dėl infrastruktūros buvimo kitose šalyse, NKSC turėtų ribotas galimybes perimti kibernetinių incidentų valdymą, taip pat valdymas remtųsi koordinavimu tarp skirtingų valstybių atsakingų CSIRT tarnybų. Koordinacinio susitikimo metu taip pat prieita išvados, kad siekdami turėti patikimą prieigą prie valstybės ar kitų elektroninių paslaugų naudotojai turi turėti daugiau negu vieną autentifikavimosi būdą.

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

96% vietinių instruktorių pritarė teiginiui, kad Pratybos jų organizacijai buvo naudingos.

2. 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 plano patvirtinimo.

D. Lietuvos Respublikos krašto apsaugos ministro įsakymas „Dėl Lietuvos Respublikos krašto apsaugos ministro valdymo sričių 2021-2023 metų strateginio veiklos plano patvirtinimo“.

3. ĮVADAS

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC), bendradarbiaudamas su Kauno technologijos universitetu (toliau – KTU), 2021 m. spalio 19-21 dienomis rengė kasmetines nacionalines kibernetinio saugumo pratybas „Kibernetinis skydas 2021“ (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 visuomenei, pratybų dalyviams ir vadovybei pristatyti Pratybų koncepciją, eigą, pasiektus rezultatus ir iš dalyvių gautą grįžtamąjį ryšį. Taip pat ataskaitoje pateikti statistiniai duomenys gali pasitarnauti ateityje vertinant praktinių informacinės infrastruktūros valdytojų kibernetinio saugumo įgūdžių formavimo progresą.

4. KIBERNETINIO SAUGUMO SUBJEKTŲ DALYVAVIMAS

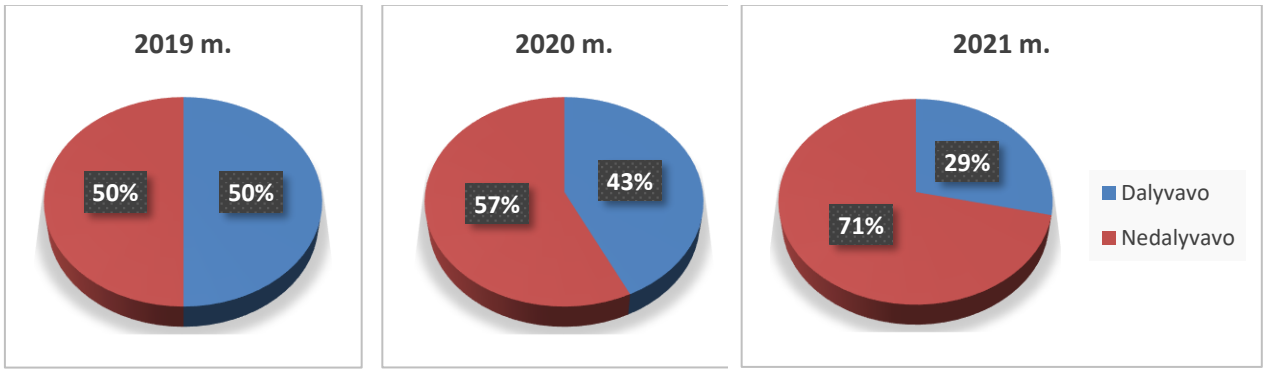
Pratybose buvo kviečiami dalyvauti kibernetinio saugumo subjektai, valdantys ir (arba) tvarkantys valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojai, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų 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 dalyvauti Pratybose kvietė organizacijas, priklausančias Lietuvos bankų asociacijai, taip pat kitas organizacijas. Toliau visi pratybų dalyviai bendrai vadinami Pratybų auditorija.

Iš viso Pratybose dalyvavo daugiau nei 670 asmenų iš 92 organizacijų (KS2020 dalyvavo 760 asmenų iš 73 organizacijų). 87 dalyvavusios organizacijos yra valstybės informacinių išteklių valdytojai ir ypatingos svarbos informacinių išteklių valdytojai arba tvarkytojai (KS2020 tokių buvo 64 vnt.). Didžiąją pratybose dalyvaujančių organizacijų dalį sudarė valstybinės institucijos (ministerijos ir joms pavaldžios įstaigos). Taip pat sveikatos priežiūros įstaigos, energetikos bendrovės, finansų institucijos, universitetai ir kt. organizacijos.

Pratybų dalyvių skaičius buvo nepakankamas, kad pasiekti Krašto apsaugos ministro 2021 kovo mėn. 17 d. įsakymu Nr. V-187 patvirtintame Lietuvos Respublikos krašto apsaugos ministro valdymo sričių 2021-2023 metų strateginiame veiklos plane nustatytus vertinimo kriterijus. Kriterijaus R-02-01-03-04 - „4. Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros valdytojų ir valstybės informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų dalis procentais nustatyta reikšmė - 60 proc., faktiškai pasiekta 21,7 proc. (pratybose KS2020 – 19,8%). Kriterijaus P-02-01-03-06-03 – „3. Nacionalinėse kibernetinio saugumo pratybose dalyvaujančių ypatingos svarbos informacinės infrastruktūros valdytojų ir valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų skaičius“ nustatyta reikšmė – 200 vnt., pasiekta – 87 vnt. (pratybose KS2020 buvo 64 vnt.).

Pavyzdžiui, iš keturiolikos LR ministerijų dalyvavo tik keturios, t.y. 29 proc.. Esant tokiam žemam ministerijų dalyvavimo lygiui, joms pavaldžios įstaigos irgi renkasi Pratybose nedalyvauti. Siekiant nustatyto kriterijaus įgyvendinimo, būtina rasti būdus kaip KSS paskatinti nacionalinėse kibernetinio saugumo pratybose ateityje.

LR ministerijų dalyvavimas pratybose „Kibernetinis skydas“:



5. 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 Kibernetinių incidentų valdymo plane (toliau – NKIVP) nustatytus veiksmus; identifikuoti tobulintinas NKIVP 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.

6. PRATYBŲ KONCEPCIJA

Organizuojant pratybas KS2021 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 paruoštus 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 KTU pratyboms paruoštoje infrastruktūroje, o dalyviams pateikti artefaktai (darbo stočių, tarnybinių stočių, mobilaus telefono diskų atvaizdai (angl. *image*), žurnalai (angl. *log*), perimtų tinklo paketų kopijos (angl. *pcap*), tinklo srauto įrašai (angl. *Netflow*)). Informaciją apie įvykius ir incidentus pratybų erdvėje vietinis instruktorius pratybų auditorijai pateikdavo el. paštu. Dalyviai darė prielaidą, kad kibernetiniai incidentai įvyko jų organizacijos IT infrastruktūroje.

7. PRATYBŲ RENGINIAI IR DALYVIAI

Pakvietimą dalyvauti pratybose ir į jų planavimą paskirti savo organizacijos atstovą (vietinį instruktorių) NKSC išsiuntė 401 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 195 organizacijos.

Dauguma organizacijų, kurios ketinimą dalyvauti pratybose buvo išreiškę, bet vėliau dalyvauti pasirengime nustodavo, dėl tokio sprendimo pratybų organizatorių neinformuodavo. Tos organizacijos, kurios apie nedalyvavimą informuodavo, dažniausiai tokio sprendimo priežastimis nurodydavo Covid-19 pandemijos sukeltas kliūtis.

Kovo ir birželio mėnesį internetu vietiniams instruktoriams buvo surengtos pratybų planavimo konferencijos. Rugsėjo mėn. surengtos trys scenarijaus rašymo konferencijos. Šiuose renginiuose buvo pristatyta tipinis pratybų scenarijus, kibernetiniai incidentai, paaiškinta vietinio instruktoriaus atsakomybė, pasiruošimo pratyboms metu reikalingi atlikti darbai. Vietiniai instruktoriai tipinį pratybų scenarijų prisitaikė savo organizacijai.

Po pratybų surengti mokymai kibernetinio saugumo specialistams, dalyvavusiems pratybose. Į mokymus užsiregistravo 400 specialistų iš KSS, juose buvo pademonstruota, kokiu būdu buvo galima ištirti pratyboms KS2021 parengtus kibernetinius incidentus.

Pratybose spalio 19-21 dienomis iš viso dalyvavo 92 organizacijos. Apklausos, kurią užpildė 86 vietiniai instruktoriai, duomenimis vidutiniškai pratybose kibernetinio incidento valdyme iš

organizacijos dalyvavo 8 darbuotojai (mediana – 6 darbuotojai), įskaitant ne tik kibernetinio saugumo specialistus, IT administratorius, bet ir viešųjų ryšių specialistus, teisininkus, aukščiausio bei vidutinio lygmens vadovus.

8. PRATYBŲ SCENARIJUS

Pratyboms paruoštas scenarijus susidėjo iš 7 dalių, siužeto linijų (toliau - SL). Vietiniai instruktoriai, atsižvelgdami į SL aktualumą ir organizacijos ambicijas pasirinko, kurios SL jų organizacija dalyvaus. Pasirinktas SL VI pritaikė atsižvelgdami į organizacijos struktūrą, procedūras ir poreikius Pratyboms buvo paruoštos tokios SL:

1. Suklastotas el. laiškas su kenkėjišku priedu suteikia prieigą prie organizacijos darbo vietos.

2. Prie nešiojamojo kompiuterio prijungus USB atmintinę į išorę nuteka failai su darbuotojų asmens duomenimis.

3. Įsilaužimas į „Windows“ IIS serverį. Suklastoto tinklapio patalpinimas organizacijos svetainėje.

4. Įsilaužimas į „Windows“ RDP serverį naudotojo teisėmis. Teisių eskalavimas. *Active Directory* duomenų nutekinimas.

5. Įsilaužimas į „Linux“ web-serverį pasinaudojant įskiepio pažeidžiamumu. Duomenų bazės nutekinimas.

6. Į mobilaus ryšio telefoną (*Android*) suinstaliavus kenkėjišką programėlę nutekinamos nuotraukos.

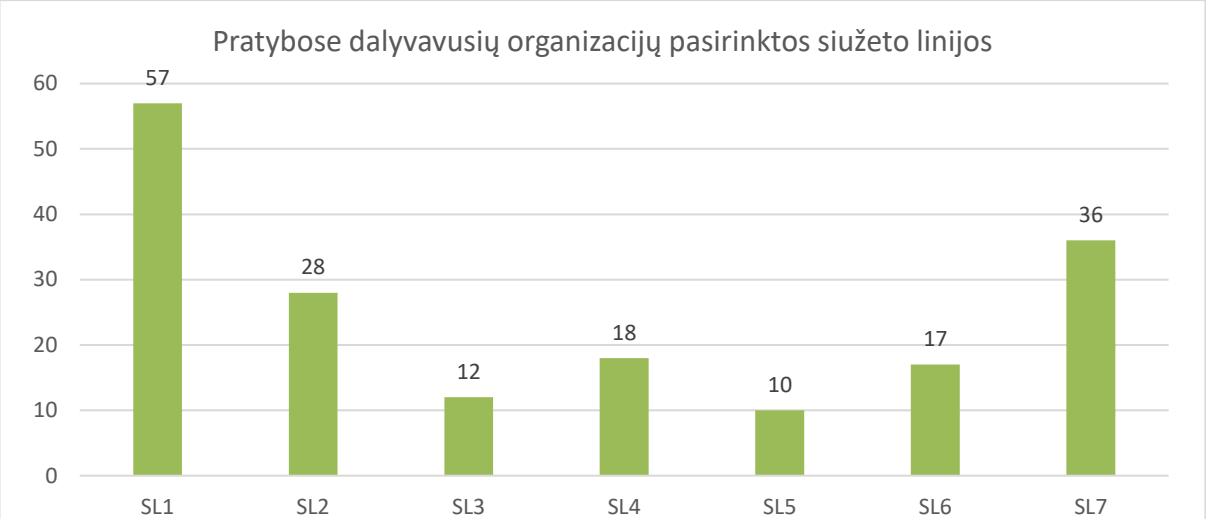
7. VI savo organizacijos personalui išsiunčia apsimestinius laiškus su prisegtu „Excel“ failu, kurio *Macro* komanda inicijuoja kreipimąsi į pratybų serverį arba laiškus su nuoroda į pratybų serverį. „Excel“ failo atidarymas su *Macros* komandų įgalinimu ir nuorodų atidarymas yra fiksuojamas pratybų serveryje. Šie įvykiai, iliustruojantys personalo kibernetinio saugumo sąmoningumo lygį, atiduodami VI vertinimui.

Visoms SL buvo paruošti techniniai artefaktai, kuriuos dalyviai galėjo ištirti ir remiantis vidinėmis organizacijos procedūromis pateikti tyrimo rezultatus savo organizacijos saugos personalui, kuris savo ruožtu turėjo informuoti NKSC, Valstybinę duomenų apsaugos inspekciją, Policiją.

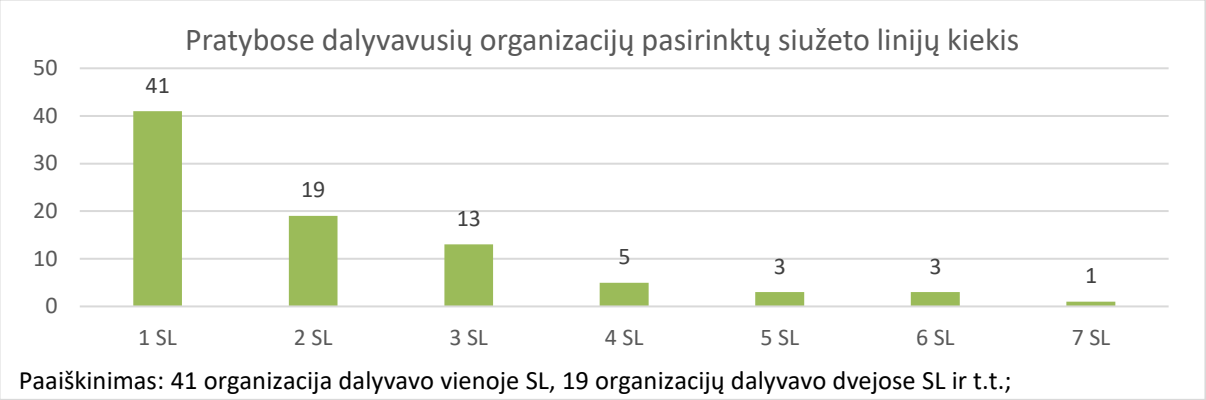
Visoms SL taip pat buvo pateikti el. laiškų pavyzdžiai, kuriais remiantis vietiniai instruktoriai galėjo inicijuoti kibernetinių incidentų valdymą ir tyrimą savo organizacijose.

Vietiniai instruktoriai dažniausiai rinkosi pratybų siužeto linijas, susijusias su incidentais Windows darbo stotimis (SL1 ir SL2) ir suklastotų laiškų siuntinėjimu (SL7). Tikėtina, kad pasirinkimą valdyti SL1 incidentą lėmė pastaraisiais metais stebėta „Emotet“ viruso veikla, kurią ši SL ir imituoja. SL2 pasirinkimas, galėjo būti lemtas organizacijų susirūpinimo rizikomis, kurias įnešė poreikis dėl Covid-19 pandemijos darbą organizuoti nuotoliniu būdu. galimybė pamatyti SL7 vietiniams instruktoriams leido realiai patikrinti savo organizacijos personalo atsparumą suklastotiems (*phishing)* laiškams (SL7). Tokius laiškus, kurių nuorodų ar priedų atidarymas buvo fiksuojamas pratybų serveryje, vietiniai instruktoriai išsiuntė daugiau

nei 12 tūkst. savo organizacijos darbuotojų. Tikslios tokiuose laiškuose buvusių nuorodų ar priedų atidarymo statistikos pratybų organizatoriai pateikti neturi galimybės, bet iš dalies vietinių instruktorių pateiktų duomenų galima daryti išvadą, kad naudotojų atsparumas tokio tipo atakoms yra prastas.



Paaiškinimas: SL1 pasirinko dalyvauti 57 organizacijos, A2 pasirinko dalyvauti 28 organizacijos ir t.t.



Paaiškinimas: 41 organizacija dalyvavo vienoje SL, 19 organizacijų dalyvavo dvejose SL ir t.t.;

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.

9. STRATEGINIO LYGMENS SCENARIJUS

Pratybose pirmą kartą buvo įtrauktas strateginio lygmens scenarijus. Pagal jį, vienas iš Lietuvoje veikiančių bankų patyrė didelio masto kibernetinę ataką, dėl kurios šio banko klientams tampa nepasiekiamos elektroninės bankininkystės paslaugos. Kartu šio banko klientams sutriko ir valstybės teikiamų el. paslaugų teikimas, nes prisijungiant prie jų dauguma klientų naudodavosi el. bankininkystės teikiamomis autentifikacijos paslaugomis.

Šiam incidentui suvaldyti NKSC, pasinaudodama NKIVP numatyta teise, sukvietė koordinacinį susitikimą.

Pratybų strateginio scenarijaus žaidimo metu paaiškėjo, kad dėl infrastruktūros buvimo kitose šalyse, NKSC turėtų ribotas galimybes perimti kibernetinių incidentų valdymą, taip pat valdymas remtųsi koordinavimu tarp skirtingų valstybių atsakingų CSIRT tarnybų.

Koordinacinio susitikimo metu taip pat prieita išvados, kad siekdami turėti patikimą prieigą prie valstybės ar kitų elektroninių paslaugų naudotojai turi turėti daugiau negu vieną autentifikavimosi būdą.

Tiek koordinaciame susitikime, tiek likusiose pratybose identifikuotos pamokos yra užfiksuotos ir bus įvertintos tobulinant kibernetinio saugumo reglamentavimą.