PATVIRTINTA
NKSC prie KAM direktoriaus
2024 m. kovo 5 d.
įsakymu Nr. 1 - 18

NACIONALINĖS KIBERNETINIO SAUGUMO PRATYBOS

„KIBERNETINIS SKYDAS PHISHEX 2023“

ATASKAITA

PHISHEX
KIBERNETINIS
SKYDAS
2023

TLP: WHITE

SANTRUMPŲ SĄRAŠAS

KSS – kibernetinio saugumo subjektai

KS2023 PhishEx – kibernetinis skydas PhishEx 2023

NKSC – nacionalinis kibernetinio saugumo centras

VI – vietinis instruktorius

BITB – naršyklės modalinis langas (angl. *browser in the browser*)

PĮ – programinė įranga

TURINYS

ĮVADAS

Imitacinės socialinės inžinerijos pratybos yra kibernetinio saugumo mokymų dalis, orientuota į saugumo supratimo (angl. *security awerness*) stiprinimą. Šie mokymai skirti tobulinti organizacijos personalo kibernetinio saugumo supratimą ir gebėjimą atpažinti galimas grėsmes, taip pat patikrinti, ar darbuotojas žino, kokių veiksmų turi imtis gavęs įtartiną el. laišką ar SMS žinutę. Nacionalinis kibernetinio saugumo centras (NKSC) skatina organizacijas nuolatos ugdyti savo darbuotojų atsparumą kibernetinėms grėsmėms ir periodiškai organizuoti įvairias pratybas, tarp kurių turėtų būti ir imitacinės socialinės inžinerijos pratybos.

NKSC, siekdamas padėti organizacijoms, negalinčioms savarankiškai vykdyti socialinių inžinerijos pratybų, organizavo socialinės inžinerijos pratybas „Kibernetinis Skydas 2023 PhishEx“ (toliau – Pratybos). Šios pratybos leido kibernetinio saugumo subjektams (toliau – KSS arba Organizacijos) identifikuoti sritis, reikalaujančias papildomų saugumo priemonių, įvertinti esamą saugumo būklę ir incidentų valdymo procedūras. Be to, pratybomis siekta stiprinti dalyvaujančių organizacijų personalo gebėjimus atpažinti ir tinkamai reaguoti į duomenų viliojimo (angl. *phishing*) atakas, mažinti kibernetinio saugumo rizikas organizacijose.

Nacionalinio kibernetinio saugumo pratybų „KIBERNETINIS SKYDAS PHISHEX 2023“ ataskaita parengta siekiant išsamiai pristatyti pratybų planą, aptarti kampanijų eigą bei pateikti apibendrintus vykdytų pratybų apklausų rezultatus.

KIBERNETINIS SKYDAS PHISHEX 2023

2023 m. kibernetinio saugumo subjektai kartu su Nacionalinio kibernetinio saugumo centru prie KAM (NKSC) organizavo imitacines socialinės inžinerijos pratybas „Kibernetinis Skydas PhishEx 2023“ Lietuvos ypatingos svarbos informacinės infrastruktūros ir valstybės informacinių išteklių valdytojų ir tvarkytojų darbuotojams.

1. Pratybų tikslas ir siekiniai

Pratybų tikslas:

Stiprinti pratybose dalyvaujančių organizacijų personalo gebėjimus atpažinti ir tinkamai reaguoti į duomenų viliojimo atakas.

Pratybų siekiniai:

(1) Mažinti kibernetinio saugumo rizikas organizacijose.

(2) Padėti organizacijoms identifikuoti sritis, kurioms reikalingos papildomos saugumo priemonės.

(3) Sudaryti galimybę įsivertinti organizacijoms jų kibernetinio saugumo padėtį bei incidentų valdymo procedūras.

(4) Supažindinti organizacijos darbuotojus su praktikoje naudojamais piktavalių manipuliacijos būdais bei pateikti sistemos išnaudojimo pavyzdžių.

2. Pratybos ir jų planas

Iš anksto parengtas dokumentas, skirtas užtikrinti pratybų kontrolę, sklandų jų vykdymą bei koordinaciją su išorinėmis organizacijomis, numatant pratybų turinį ir auditoriją (toliau – Pratybų planas). Remiantis šiuo dokumentu pratybos yra išskaidytos į tris atskiras pratybų kampanijas, kurios vykdomas periodiškai kiekvieną ketvirtį, praleidžiant pirmąjį ketvirtį. Tokios atskiros pratybų kampanijos (žr. *3. Pratybų simuliacijos*) skirtos visiems dalyvaujančių Organizacijų darbuotojams arba pritaikytos atsižvelgiant į konkretaus darbuotojo (arba darbuotojų grupės) rolę, atsakomybes, keliamas rizikas organizacijos veiklai. Kurie organizacijos darbuotojai bus įtraukti į imitacinę socialinės inžinerijos pratybų kampaniją, nusprendžia organizacijos atstovas – vietinis instruktorius (toliau – VI).

Organizacijai nusprendus dalyvauti pratybose, Organizacija paskiria savo atstovą - vietinį instruktorių (toliau - VI) bei įgalioją šį asmenį atlikti pratybų kampaniją savo Organizacijoje. Planuojant pratybų kampaniją bei jų metu šie asmenys užtikrina glaudų bendradarbiavimą ir pratybų koordinaciją su kitais organizacijos padaliniais ir išorinėmis organizacijomis, kurios gali būti

paveiktos pratybų, užtikrina sėkmingą pratybų vykdymą ir kontrolę pagal iš anksto paruoštą NKSC planą.

Dalis darbuotojų apie gautus įtartinus el. laiškus informuoja ne tik savo organizacijos kibernetinio saugumo specialistą, bet ir kitas valstybines institucijas. Siekiant nesutrikdyti šių organizacijų veiklos, NKSC siekia identifikuoti visas organizacijas, kurioms pratybų simuliacija gali turėti įtakos ir bendradarbiauti su jomis, konsultuotis, iš anksto pristatant pratybų kampanijos scenarijus, derinant atsaką į pranešimus, kurie bus gaunami pratybų metu.

Vykdant pratybų kampanijas imituojamos realios grėsmės, su kuriomis susiduria organizacijos, todėl siekiant užtikrinti realią darbuotojų patirtį saugioje aplinkoje be glaudaus bendradarbiavimo pratybų metu naudojamas duomenų viliojimo atakoms vykdyti skirtas pratybų įrankis (toliau – Įrankis). Įrankyje įdiegti baziniai pratybų kontrolės sprendimai, neleidžiantys kampanijos vykdytojams rinkti asmeninius duomenis (pvz.: slaptažodžius, vardus, pavardes, telefono numerius, banko kortelės numerius ir pan.) bei užtikrinantys, kad žiniatinklio serveriui niekada nebūtų pateikta informacija (vartotojų pateiktos formos duomenys atmetami prieš juos pateikiant).

3. Pratybų kampanijos

Atsižvelgiant į duomenų viliojimo atakų tendencijas, pratybų kampanijoms paruoštos kelios duomenų viliojimo atakų simuliacijos (scenarijai), kurių metu laiškų gavėjai supažindinti su skirtingais piktavalių būdais išnaudoti el. laiško gavėjo emocijas ar PĮ, vykdant duomenų viliojimo atakas. Siekiant užtikrinti dalyvių privatumą bei išvengti netinkamos ar jautrios informacijos, pratybų simuliacijų turinį sudarė tik viešai prieinama informacija.

Vietiniai instruktoriai, įsivertinę savo organizacijos poreikius ir nustatę įsitraukimo laipsnį pratybų kampanijos metu, savo nuožiūra rinkosi, kurią iš simuliacijų taikyti savo organizacijos gavėjų auditorijai.

3.1. Pirmoji kampanija: naršyklė naršyklėje

Pirmoji kampanija skirta supažindinti gavėjus su praktikoje naudojamu fiktyviu modaliniu naršyklės langu (angl. *browser in the browser, BITB*), atvaizduojamu tinklalapyje. Toks modalinis langas leidžia piktavaliui imituoti bet kurią svetainę atvaizduojant jos tikrąjį domeno vardą bei turinį. Papildomai kampanijos simuliacijos naudoja homografinius (vizualiai panašius) simbolius, pakeičiant [l] į [I] simbolį bei panašius domenų vardus (angl. *Typosquatting).*

Bendradarbiaujant su *Policijos departamentu prie LR VRM* bei *UAB Omniva*, kurie pratybų tikslais leido naudoti į jų siunčiamus pranešimus panašias žinutes, sukurtos dvi pratybų simuliacijos:

(1) **Policija** – nuo *info@poIicija.lt* siunčiamas el. laiškas, informuojantis apie gautą administracinio nusižengimo protokolą su aktyvia nuoroda į paskirtos baudos mokėjimo

tinklalapį *https://poIicija.lt/*. Tinklalapyje pateikiamas į pagrindinį policijos tinklalapį (*https://epolicija.lt)* panašus turinys kartu su modaliniu langu, imituojančiu Elektroninių valdžios vartų prisijungimo mobiliuoju įrenginiu tinklalapį.

(2) Omniva – nuo *info@omvina.lt* siunčiamas el. laiškas, imituojantis siuntų bendrovės Omniva pranešimą apie gavėjams skirtą siuntą, kurios pristatymui kilus problemų prašoma patikslinti gavėjo duomenis tinklalapyje. Tinklalapyje pateikiamas netikras nukreipimo pranešimas, kuriame yra iškviečiamas modalinis naršyklės langas, vaizduojantis netikrą Omnivos tinklalapį su duomenų įvedimo forma.

Pirmoji pratybų kampanija vyko 2023 m. gegužės 17–26 d.. Pratybų savaitę 115 dalyvaujančių organizacijų bendrai išsiuntė 67038 kampanijos simuliacijų el. laiškus. Bendrai kampanijos scenarijų el. laiškų neatpažino bei riziką keliančius veiksmus (atidarė nuoroda ir/arba suvedė asmens duomenis) atliko 12 % (7943) gavusiųjų pratybų kampanijos el. laiškus.

lentelė 1

Pirmosios kampanijos rezultatai

		Riziką keliantys veiksmai	
Scenarijus	**Išsiųsta**	**Atidarė nuorodą**	**Pateikė asmens duomenis**
Policija	40867	11 % (4312)	5 % (1969)
Omniva	26171	14 % (3631)	6 % (1664)
Bendrai	*67038*	*12 % (7943)*	*5 % (3633)*

3.2.Antroji kampanija: failų išnaudojimas duomenų vagystei

Antroji pratybų simuliacija skirta parodyti Organizacijos gavėjams, kad piktavaliai naudodami socialinę inžineriją siekia ne tik išvilioti duomenis, bet ir psichologiškai manipuliuojant gavėją paskatinti jį atsisiųsti kenkėjišką programinę įrangą, atlikti piktavaliui reikalingus veiksmus ar priversti gavėją dalytis slapta ar asmenine informacija.

Pratybų kampanijai paruoštos keturios simuliacijos, skirstomos pagal jų tipą (vienos, dviejų pakopų) bei išnaudojamus PĮ plėtinius (*.ics, .html, .docx, .xlsx*). Vienos pakopos kenkėjiškos PĮ simuliacijos apsimesdamos teisėtomis programomis ar jų plėtiniais manipuliavo vartotojais atsisiųsti kenkėjišką programinę įrangą bei ją vykdyti. Dviejų ar keleto pakopų simuliacijos savyje talpino papildomas funkcijas bei reikalavo vartotojų atlikti papildomus veiksmus (pvz.: įgalinti turinį Microsoft Word dokumente).

Vienos pakopos simuliacijos:

(1) Pasibaigęs galioti skaitmeninis sertifikatas (*.ics*) – siunčiamas el. laiškas, informuojantis gavėją apie pasibaigusį galioti skaitmeninį sertifikatą su raginimu atnaujinti sertifikatą, taip išvengiant paskyros pašalinimo. El. laiške „sertifikatas“ pateiktas universalaus kalendoriaus formatu (*.ics*). Gavėjui paleidus universalų kalendoriaus failą automatiškai pridedami keturi suasmeninti fiktyvūs kalendoriaus įvykiai su nuorodomis į suklastotas susitikimų svetaines.

(2) Nepristatytas el. laiškas (*.html*) – siunčiamas el. laiškas, informuojantis gavėją dėl nepristatyto el. laiško. Siunčiamo pranešimo gavėjas negali peržiūrėti, kol nėra paspaudžiama el. laiške pateikiama nuoroda arba atsisiunčiamas prisegtas (*.html*) failas su JavaScript kodu. Papildomai vartotojas yra nukreipiamas į fiktyvų pašto prisijungimo tinklalapį.

Dviejų pakopų simuliacijos:

(3) **Pažyma dėl finansinių įsipareigojimų (*.docx*)** – siunčiamas el. laiškas, imituojantis elektroninių siuntų pristatymo sistemą „E. Pristatymas“ bei informuojantis gavėją apie gautą elektroninę pažymą „dėl asmeninių finansinių įsipareigojimų nevykdymo“. Prie laiško pridedamas Microsoft Word dokumentas su dalinai paslėptais asmens duomenimis bei fiktyviu pranešimu, raginančiu vartotoją įgalinti redagavimą bei failo turinį, norint peržiūrėti duomenis.

(4) Pasikeitusi darbo užmokesčio tvarka (*.xslx*) – siunčiamas suklastotas laiškas nuo neegzistuojančios buhalterinės apskaitos programos „E. Pristatymai“. Laiške gavėjas yra informuojamas dėl pasikeitusio darbo užmokesčio neapmokestinamos dalies dydžio taikymo tvarkos ir raginamas susipažinti su darbo užmokesčio pakitimais prie laiško pridėtame dokumente. Pridedamas dokumentas yra Microsoft Excel failas su galimai suasmeninta informacija, tačiau informacija yra paslėpta, kol vartotojas neatlieka reikalaujamų veiksmų. Pirmuoju žingsniu vartotojas yra skatinamas įgalinti redagavimą bei išorinį turinio krovimą. Atlikus pirminius žingsnius išspausdinamas fiktyvus sistemos klaidos pranešimas su nuoroda į tinklalapį, kuriame pateikiama prisijungimo forma.

Antroji pratybų kampanija vyko 2023 m. spalio 2–6 d.. Bendrai kampanijos metu 121 dalyvaujanti organizacija išsiuntė 77417 kampanijos simuliacijų el. laiškus. Bendrai kampanijos scenarijų el. laiškų neatpažino bei riziką keliančius veiksmus atliko 18 % (13909) gavusiųjų pratybų kampanijos el. laiškus.

lentelė 2

Antrosios kampanijos rezultatai

Scenarijus	Išsiųsta	*Riziką keliantys veiksmai*		
		Atidarė kalendorinį įvykį	**Atidarė nuorodą**	**Pateikė duomenis**
Pasibaigęs galioti skaitmeninis sertifikatas (.ics)	4349	2 % (87)	1 % (27)	0 % (8)
Nepristatytas el. laiškas (.html)	29514	**Atidarė nuorodą**	**Pateikė asmens duomenis**	
		11 % (3352)	1 % (195)	
Pažyma dėl finansinių įsipareigojimų (.docx)	20535	**Įgalino dokumento turinį**		
		28 % (5769)		
Pasikeitusi darbo užmokesčio tvarka (.xslx)	23019	**Įgalino redagavimą**	**Įgalino išorinį turinį**	**Atidarė nuorodą**
		20 % (4701)	18 % (4076)	12 % (2698)
Bendrai	*77417*	*18 % (13909)*		

3.3.Trečioji kampanija: naršyklės funkcijos

Trečioji pratybų kampanija Organizacijos darbuotojus supažindino su naršyklių funkcijų išnaudojimu, papildomai panaudojant į organizacijos el. laišką panašius domenų vardus bei homografinius simbolius.

Pratybų scenarijai sukurti bendradarbiaujant su *AB Lietuvos Paštas*, kurie pratybų tikslais leido naudoti į jų siunčiamus pranešimus panašias žinutes bei koordinavo atsakant į gaunamus pranešimus dėl galimų duomenų viliojimo atakų.

(1) Pilno ekrano vaizdas - Organizacijos subjektams siunčiamas Lietuvos paštą imituojantis el. laiškas informuoja gavėją dėl nepavykusios įteikti siuntos bei ragina patikslinti gavėjo duomenis savitarnos svetainėje. Tinklalapyje pateikiamas netikras nukreipimo pranešimas su nuoroda į tikrą Lietuvos pašto portalą, gavėjui per 5 sekundes neatlikus jokių veiksmų, atvaizduojamas fiktyvus Windows funkcijų naujinimo langas (tam, kad būtų iškviestas pilno ekrano vaizdas, reikalingas vartotojo paspaudimas). Pasirinkus bet kurią nuorodą ar mygtuką tinklalapyje yra iškviečiamas pilno ekrano vaizdas ir imituojamas Windows naujinimų procesas. Pasibaigus fiktyviam naujinimo procesui, atvaizduojamas Windows prisijungimo langas su duomenų įvedimo forma.

(2) **Naršyklės skirtukai** - Organizacijos subjektams prisistatant IT administratoriumi siunčiamas el. laiškas, prašantis gavėjus atnaujinti interneto naršyklę. Neatnaujinus naršyklės grasinama paslaugų teikimo sutrikdymu. Pateiktos naujinimo nuorodos nukreipia gavėją į tinklalapį, kuriame pateikiama bazinė vartotojo informacija (IP adresas, vietos informacija ir kt.), kurią tariamai norint apsaugoti reikalaujama atlikti papildomus veiksmus. Šie veiksmai apima „Patvirtinimas“ mygtuko nutempimą į skirtukų juostą bei diegimo užbaigimą paspaudžiant skirtukų juostoje atsiradusį patvirtinimą.

Trečioji kampanija vyko gruodžio 4–8d. Kampanijos metu 105 dalyvaujančios organizacijos bendrai išsiuntė 59110 kampanijos simuliacijų el. laiškų. Bendrai kampanijos scenarijų el. laiškų neatpažino bei riziką keliančius veiksmus atliko 12% (7009) subjektai, iš kurių asmens duomenis pateikė beveik 4% (2092) visų siųstų kampanijos laiškų.

lentelė 3

Trečiosios kampanijos rezultatai

		Riziką keliantys veiksmai	
Scenarijus	**Išsiųsta**	**Atidarė nuorodą**	**Pateikė asmens duomenis**
Pilno ekrano vaizdas	41689	14 % (5714)	5 % (1971)
Naršyklės skirtukai	17421	7 % (1295)	1 % (121)
Bendrai	*59110*	*12 % (7009)*	*4 % (2092)*

4. Pratybų dalyviai - kibernetinio saugumo subjektų dalyvavimas

Dalyvauti pratybose buvo kviečiami kibernetinio saugumo subjektai ir (arba) organizacijos, tvarkančios 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. Papildomai NKSC sudarė sąlygas pratybose dalyvauti ir kitoms organizacijoms, išreiškusioms tokį poreikį.

Bent vienoje pratybų kampanijoje dalyvavo **154** organizacijos. Didžiąją pratybose dalyvaujančių organizacijų dalį sudarė valstybinės institucijos (ministerijoms pavaldžios įstaigos), sveikatos priežiūros įstaigos, energetikos ir vandentvarkos bendrovės, finansų institucijos.

5. Pratybų subjektų apklausa

Siekiant įvertinti pratybų subjektų (el. laiškų gavėjų) požiūrį į NKSC organizuojamas pratybas, jų vykdymą bei identifikuoti papildomus pratybų siekinius pratybų dalyviams išsiųstas pranešimas su nuorodą į internetinę apklausą.

5.1. Bendras pratybų vertinimas:

Bendras pratybų vertinimas rodo labai teigiamą pratybų dalyvių požiūrį. Beveik 95% apklaustųjų teigiamai įvertino pratybas, pabrėždami, jog jos efektyviai padeda ugdyti kibernetinio saugumo sąmoningumą, moko atpažinti galimai įtartinus el. laiškus ir skatina kritiškai vertinti gaunamą informaciją. Dalyviai taip pat pažymėjo, kad pratybų temos yra labai aktualios ir atitinka realias grėsmes, suteikia galimybę saugiai mokytis iš savo klaidų. Nepaisant didžiulio teigiamų atsiliepimų skaičiaus, mažesnė dalis (5%) išreiškė tam tikrą nepasitenkinimą. Jie nurodė, kad pratybos vykdomos per dažnai ir jų formatas kartais būna pernelyg šabloniškas, kas, jų manymu, gali sumažinti pratybų efektyvumą ir/ar trukdo tiesioginiams jų darbams.

Svarbu pastebėti, kad, nors ir kai kurie respondentai išreiškė nuogąstavimus dėl pratybų, beveik visi (97%) remia organizacijos sprendimą dalyvauti pratybose, o likusieji 3% neturėjo aiškios nuomonės šiuo klausimu. Visa tai rodo, kad nepaisant tam tikrų susirūpinimų, dauguma dalyvių mano, jog pratybos teikia naudą ir yra vertos organizacijos dalyvavimo.

Bendrai vertinant pratybas svarbu įvertinti dalyvių reakciją į vykdomas tokio tipo pratybas. Apklaustųjų klausėme, kokias emocijas patyrė visų kampanijų metu. Didžioji dauguma (70%) nurodė, kad pratybos privertė juos susimąstyti. Tai rodo, kad pratybos yra pakankamai įtraukiančios ir efektyvios. Maždaug 12% nurodė, kad pratybos nekėlė jokių emocijų, o kiti 13% patyrė pozityvias emocijas. Nepaisant to, 2% dalyvių patyrė neigiamas emocijas, įvardijant kampanijas kaip nepatogias arba stresines.

5.2. Subjektų reakcija į kenkėjiškus laiškus

Iš apklausos duomenų matyti, kad didžioji dalis (74%) apklaustųjų susidūrę su galimai kenkėjiškais el. laiškais rodo atsakingą požiūrį ir praneša apie juos savo organizacijoje atsakingam asmeniui. Taigi, didžioji dalis apklaustųjų suvokia kibernetines grėsmes ir geba tinkamai reaguoti pastebėję galimai kenkėjišką el. laišką. Be to, daugiau nei pusė apklaustųjų aktyviai informuoja savo kolegas apie įtartinus laiškus, kas rodo bendradarbiavimą ir kolektyvinio saugumo požiūrį, kad saugumo klausimai yra svarbūs ne tik asmeniui, bet ir visos organizacijos lygmeniu.

Įdomu, kad 3% apklaustųjų nurodė informuojantys organizaciją, kuri yra imituojama kenkėjiškame el. laiške. Tai atspindi iniciatyvumą ir norą apsaugoti ne tik savo organizacijos, bet ir

kitų įstaigų interesus. 5% pranešė NKSC apie įtartinus el. laiškus. Tai gali rodyti tam tikrą nežinojimą šios institucijos vaidmenio kibernetinio saugumo kontekste.

Beveik 10% apklaustųjų nurodė, kad, susidūrę su įtartinu el. laišku, nieko neinformuoja. Tarp šių asmenų 20% nurodė nematantys tikslo tai daryti, kas rodo tam tikrą asmenų abejingumą ar nepakankamą suvokimą apie kibernetinių grėsmių rimtumą. Tuo tarpu 15% neinformuojančių teigia nežinantys, ką informuoti tokiose situacijose, kas rodo informacijos trūkumą ar neaiškumą organizacijos viduje. Taip pat nemaža dalis išreiškė baimę dėl galimos neigiamos organizacijos ar vadovų reakcijos, atviros komunikacijos ir saugumo kultūros trūkumą darbo aplinkoje.

5.3.Pratybų naudos

Dauguma apklaustųjų įvardina, kad pratybos suteikė jiems vertingos patirties ir kibernetinio saugumo žinių. Pirmiausia, beveik pusė (46%) apklaustųjų mano, kad dalyvavimas pratybose padėjo jiems geriau susipažinti ir atpažinti skirtingas socialinės inžinerijos atakas. Be to, beveik toks pats skaičius (47%) nurodė, jog pratybos padėjo susipažinti su organizacijos nustatytomis procedūromis, kaip reaguoti į duomenis viliojančius el. pašto laiškus, kas yra svarbu mažinant kibernetinio incidento rizikas.

Svarbu, kad didžioji dauguma apklaustųjų (68%) pabrėžė, kad pratybos paskatino juos laikytis bazinių kibernetinės higienos įpročių. Tai rodo, kad pratybos teikia ne tik teorines žinias, bet ir skatina jas taikyti praktikoje. Vis dėlto, nedidelė dalis (6%) apklaustųjų nurodė, kad pratybos jiems nebuvo naudingos. Tai rodo būtinybę toliau analizuoti ir tobulinti pratybų turinį bei informacijos pristatymo būdus, siekiant užtikrinti, kad pratybos būtų pritaikytos ir maksimaliai užtikrintų naudą kiekvienam dalyviui.

6. Pratybų rezultatai

Nacionalinio kibernetinio saugumo centro (NKSC) organizuotos pratybos sėkmingai įgyvendino jų siekiamas naudas, atspindėjo teigiamą poveikį dalyvių požiūriui ir elgsenai kibernetinio saugumo kontekste.

Pagrindinis pastebėtas pokytis, kuris tiesiogiai susijęs su pratybų siekiniu mažinti kibernetinio saugumo rizikas organizacijose, yra išaugęs NKSC pranešimų skaičius apie įtartinus duomenų viliojimo atvejus. Tai rodo dalyvių atsakomybės suvokimą ir aktyvumą. Be to, pastebėtas padidėjęs imituojamų organizacijų aktyvumas teikiant informaciją apie kibernetines grėsmes prisideda šviečiant piliečius apie kibernetines rizikas ir skatina efektyvesnį jų valdymą. Dalyviai, susipažinę su praktikoje naudojamais piktavalių manipuliacijos būdais, tapo atidesni ir pradėjo racionaliau reaguoti į internete pateikiamą informaciją, tokiu būdu saugodami ne tik organizacijų bet ir asmeninius interesus.

Visi šie pastebėjimai rodo, kad NKSC organizuotos pratybos įgyvendino savo tikslą stiprinti pratybose dalyvaujančių organizacijų personalo gebėjimus atpažinti ir tinkamai reaguoti į duomenų viliojimo atakas. Tai ne tik parodo pratybų sėkmę, bet ir pabrėžia sąmoningumo didinimo svarbą kibernetinio saugumo srityje bei rodo būtinybę toliau stiprinti organizacijų ir asmenų atsparumą kibernetinėms grėsmės.