Rekomendacijos

Kenkėjiškų interneto svetainių grėsmių valdymo tobulinimas

Programos „Kurk Lietuvai“ projekto „Kenkėjiškų interneto svetainių grėsmių valdymo priemonių kūrimas“ dalis

Parengė Renata Donauskytė ir Karolis Vyčius

2022 m. kovas

Kurk Lietuvai

KRAŠTO APSAUGOS MINISTERIJA

Įžanga

„Kurk Lietuvai“ projekto „Kenkėjiškų interneto svetainių grėsmių valdymo priemonių kūrimas“ metu atlikta esamos situacijos analizė parodė, kad kyla nemažai iššūkių siekiant užtikrinti saugesnę elektroninę erdvę gyventojams ir verslui. Lietuvoje vis daugėjant nukentėjusių asmenų dėl kenkėjiškų interneto svetainių, buvo iškeltas tikslas projekto metu pasiūlyti papildomas priemones, skirtas saugoti gyventojus ir verslą nuo kenkėjiškų interneto svetainių sumažinant tokių svetainių pasiekiamumą ir laiko tarpą, reikalingą prieigai apriboti.

Atsižvelgiant į kitų šalių taikomas praktikas bei atliktų viešųjų konsultacijų rezultatus, buvo sukurtas **pagrindinis projekto rezultatas – pasiūlytas modelis būsimai Blokuojamų domenų valdymo informacinei sistemai** (toliau – BDVIS). Centralizavus ir automatizavus interneto svetainių blokavimo procesą, BDVIS sudarys sąlygas greitai ir efektyviai užkardyti kenkėjiškas interneto svetaines ir interneto svetaines, išnaudojamas kitai nusikalstamai bei nelegaliai veikai internete vykdyti.

Atsižvelgiant į tai, kad kenkėjiškų interneto svetainių problema yra kompleksinė, greta BDVIS yra būtina imtis ir kitų priemonių siekiant palaikyti saugią elektroninę erdvę. Šių rekomendacijų tikslas – pasiūlyti gaires tolimesniems veiksmams kovojant su kenkėjiškomis interneto svetainėmis. Rekomendacijos skirtos kibernetinio saugumo politikos formuotojams bei institucijoms, atsakingoms už kenkėjiškų interneto svetainių užkardymą institucijoms.

I. Procesas

Kenkėjiškų interneto svetainių užkardymo procesas susideda iš keturių pagrindinių etapų: identifikavimo, tyrimo, sprendimo ir vykdymo (žr. pav. 1). Atkreiptinas dėmesys, kad skirtingose proceso dalyse veikia skirtingi dalyviai: identifikuoti kenkėjišką interneto svetainę gali tiek gyventojai, tiek elektroninę erdvę stebinčios institucijos, tačiau interneto svetainės blokavimą inicijuoja valstybinės institucijos pagal savo kompetencijas atlikusios tyrimą ir surinkusios reikalingus įrodymus; blokavimo sankciją skiria teismas, o vykdo valstybinės institucijos bei interneto prieigos paslaugų teikėjai. Kiekviena proceso dalis yra svarbi siekiant greitai ir efektyviai sustabdyti kenkėjiškų interneto svetainių daromą žalą gyventojams ir verslui, todėl turi būti užtikrintas koordinavimas tarp skirtingų proceso dalyvių bei nuosekliai peržiūrimas visas procesas.

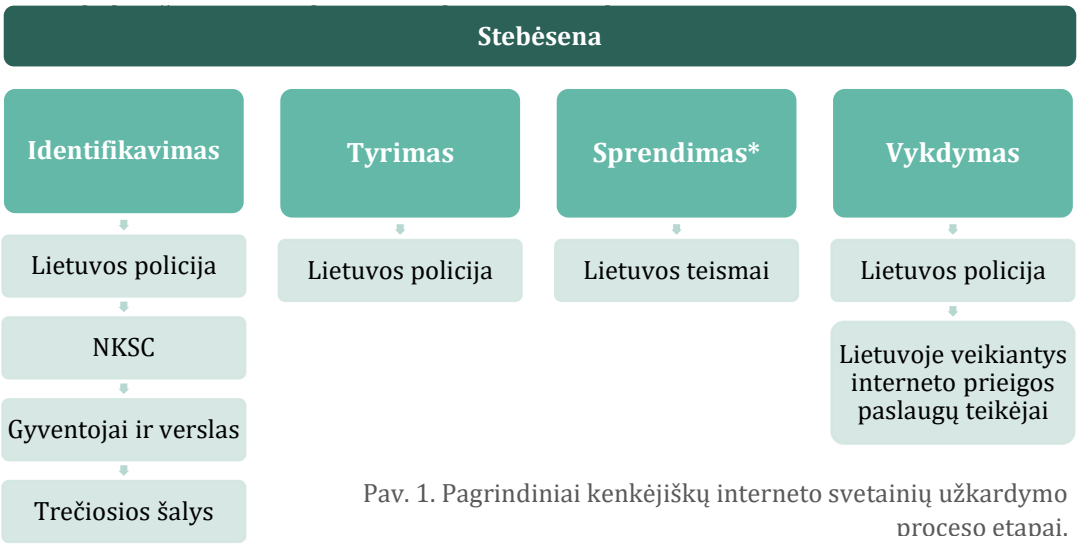
Rekomendacijos:

1.1. Siekiant didinti kenkėjiškų interneto svetainių identifikavimo greitį, yra būtina sukurti galimybę vieno langelio principu gyventojams ir verslui pranešti apie gautas įtartinas trumpąsias žinutes ir elektroninius laiškus bei pastebėtas įtartinas interneto svetaines atsakingoms institucijoms (žr. Jungtinės Karalystės pavyzdį, 13 psl.) ;

1.2. Atsakingoms institucijoms įtariant, kad interneto svetainė yra piktybiškai naudojama vykdyti nusikaltimams elektroninėje erdvėje, būtina kreiptis į teismą ne tik sankcijos blokuoti identifikuotą kenkėjišką interneto svetainę, bet ir būsimas veidrodines interneto svetaines pagal iš anksto aiškiai apibrėžtus kriterijus;

1.3. Kenkėjiškų interneto svetainių blokavimą vykdyti tik per BDVIS, kuri ne tik užtikrina centralizuotą blokavimą ir procesų automatizavimą, bet užtikrina blokavimo įgyvendinimą (plačiau žr. BDVIS modelis);

1.4. Atsakingos institucijos turi vykdyti proceso stebėseną, rinkti ir analizuoti duomenis siekiant nustatyti tendencijas, identifikuoti didžiausią žalą



Pav. 1. Pagrindiniai kenkėjiškų interneto svetainių užkardymo proceso etapai.

*Taip pat policijos pareigūnai taikydami 48 val. blokavimą arba institucijos, blokuojančios veidrodines svetaines pagal ankstesnes teismo nutartis.

II. Priemonės

Greitas kenkėjiškų interneto svetainių blokavimas yra būtina, bet nepakankama priemonė gyventojų ir verslo saugumui elektroninėje erdvėje užtikrinti. Nors interneto svetainės blokavimas sustabdo nusikalstamos veikos daromą neigiamą poveikį, tačiau tokios priemonės taikymas turi trūkumų: ne visais atvejais procesas yra pakankamai greitas, piktavaliai sukuria veidrodines interneto svetaines ir toliau tęsia nusikalstamą veiką, interneto vartotojai ne visada naudoja interneto prieigos paslaugų teikėjų numatytąjį DNS, per kurį yra įgyvendinamas interneto svetainės blokavimas.

Projekto metu atlikta užsienio praktikų analizė parodė, kad kitos Europos valstybės, kaip ir Lietuva, vykdo kenkėjiškų interneto svetainių blokavimą bendradarbiaujant su interneto prieigos arba prieglobos paslaugų teikėjais bei taiko kitas kompleksines priemones, kurios viena kitą papildo. Atkreiptinas dėmesys, kad skirtingų priemonių apsaugos lygis prieš kenkėjiškas interneto svetaines, pavyzdžiui, Google Safe Browsing perspėjimai, interneto svetainės blokavimas ar paties interneto vartotojo pasirinkta DNS ugniasienė, yra atvirkščiai proporcingas apsaugotai gyventojų daliai ir apsaugos greičiui (žr. pav. 2).

Saugos naršymo ekosistema			
Priemonės pavyzdys	**Apsaugos lygis**	**Apsaugotų gyventojų dalis**	**Trūkumai**
Google Safe Browsing	Minimalus (pavyksta nustatyti tik akivaizdžiausius atvejus)	Labai didelė (apie 90 proc. gyv. vartoja Google produktus)	Gyventojai lengvai gali ignoruoti perspėjimą ir tęsti darbą tokiame interneto puslapyje; valstybinės institucijos neturi įtakos tam, kas yra blokuojama
Interneto svetainės blokavimas			
Priemonės pavyzdys	**Apsaugos lygis**	**Apsaugotų gyventojų dalis**	**Trūkumai**
BDVIS	Vidutinis (nustatomi ne tik akivaizdžiausi pažeidimai, bet užtrunka laiko)	Didelė (arba vid. tiek, kiek gyv. nekeičia DNS nustatymų)	Gyventojai nenaudoja interneto teikėjo numatytojo DNS dėl asmeninių priežasčių; sąlyginai ilgai užtrunka, kol teismo keliu priimamas sprendimas blokuoti
Interneto vartotojo įsidiegti/pasirinkti saugumo įrankiai			
Priemonės pavyzdys	**Apsaugos lygis**	**Apsaugotų gyventojų dalis**	**Trūkumai**
DNS ugniasienė	Aukštas (galimybė blokuoti automatiškai pagal nustatytus kriterijus, todėl greičiau apsaugoma)	Maža (kiek vartotojų žinos ir norės tokią priemonę taikyti)	Labiausiai pažeidžiamos gyventojų grupės nesinaudos dėl žinių ir kompetencijų trūkumo

Pav. 2. Skirtingų priemonių apsaugos lygio ir apsaugotų gyventojų dalies palyginimas.

Kiekviena priemonė prieš kenkėjiškas interneto svetaines turi savo stipriąsias ir silpnąsias puses:

- Google Safe Browsing sąlyginai greitai perspėją didelę populiacijos dalį apie galimą grėsmę, tačiau identifikuojama tik techninėmis priemonėmis nustatomos kenkėjiškos interneto svetainės (informaciją apdorojant techniniais įrankiais), o svetainės lankytojas gali lengvai nepaisyti perspėjimo lango ir tęsti naršymą interneto svetainėje;
- BDVIS pagreitina interneto svetainės blokavimo įgyvendinimą, tačiau blokavimo per interneto prieigos paslaugu teikėją procesas truks sąlyginai ilgai dėl tyrimo bei sprendimo priėmimo būtinybės. Taip pat piktavaliai lengvai sukuria naujas interneto svetaines, o blokavimas per interneto prieigos paslaugų teikėjų DNS nepasiekia tų vartotojų, kurie yra pasikeitę DNS nustatymus;
- DNS ugniasienė suteikia galimybę blokuoti kenkėjišką interneto svetainę šios priemonės vartotojams vos ją identifikavus. Toks veikimo modelis leidžia greitai ir nuo plataus spektro grėsmių apsaugoti šios priemonės vartotojus, tačiau pats interneto vartotojas turi apsispręsti, ar pasitiki institucijomis, siūlančiomis tokią paslaugą, ir naudoti įrankį savo įrenginyje. Taigi, nors suteikiamas aukščiausias apsaugos lygis, bet vartotojas turi imtis aktyvių veiksmų, todėl didelė tikimybė, kad tik maža dalis gyventojų ir verslo naudosis tokia priemone dėl žinių ir informacijos trūkumo.

Apibendrinant galima teigti, kad, nors kiekviena priemonė atskirai turi trūkumų, tačiau kuo daugiau skiritngo poveikio priemonių vienu metu yra taikoma skirtingoms tikslinėms grupėms, tuo didesnis bendras saugumo lygis elektroninėje erdvėje yra sukuriamas.

Rekomendacijos:

2.1. Sudaryti sąlygas blokavimą inicijuojančioms institucijoms blokuoti interneto svetaines per interneto prieigos paslaugų teikėjus ne tik DNS būdu domeno lygmenyje, tačiau ir per IP adresą atitinkamai sukuriant papildomą funkcionalumą BDVIS ir sutvarkant teisinę bazę;

2.2. Stiprinti atsakingų insitucijų bendrabardiavimą su Lietuvoje veikiančiais *prieglobos* paslaugų teikėjais, kurie, esant galimybei, galėtų nutraukti teikiamą paslaugą kenkėjiškai interneto svetainei tokiu būdu sustabdant žalingą poveikį gyventojams. Siekiant efektyvaus bendradarbiavimo galima remtis gerąją kitų institucijų ir valstybių patirtimi (žr. Ryšių reguliavimo tarnybos puslapį bei Nyderlandų taikomą modelį).

2.3. Dalintis ir aktyviai skatinti naudotis juodaisiais sąrašais, kurie yra generuojami DNS ugniasienės funkcijai vykdyti, tiek su verslo įmonėmis, tiek su interneto prieigos paslaugų teikėjais, kurie naudoja savo DNS ir norėtų patys prevenciškai blokuoti įtartinas interneto svetaines;

2.4. Nuolat ir sistemiškai informuoti visuomenę apie kenkėjiškų interneto svetainių keliamas grėsmes, viešinti informaciją apie tai, kokiais atvejais yra apribojama prieiga prie interneto svetainių bei šviesti gyventojus apie priemones, skirtas apsisaugoti nuo kenkėjiškų interneto svetainių.

III. Atsakingos institucijos

Projekto metu atlikta esamos situacijos analizė parodė, kad kenkėjiškas interneto svetaines gali identifikuoti Lietuvos policijos pareigūnai, NKSC specialistai, gyventojai ar kt. subjektai, o tyrimą ir užkardymą vykdo Lietuvos policija (žr. pav. 1). Nors įstatymuose numatytos ribotos NKSC funkcijos ir atsakomybės ne kibernetinio saugumo subjektų interneto svetainių atžvilgiu, tačiau praktikoje NKSC specialistų ir policijos pareigų veiksmai persidengia bei reikalauja glaudaus bendradarbiavimo siekiant užkardyti kylančias grėsmes (plačiau žr. esamos situacijos analizė 24-31 p.).

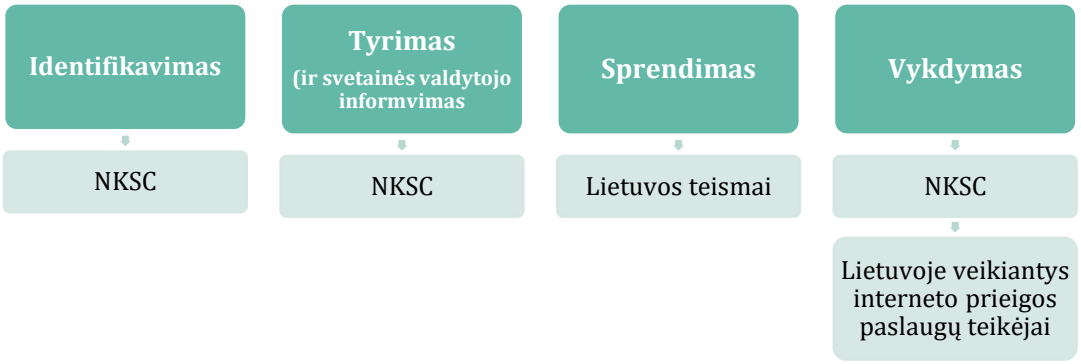
NKSC turi reikiamas technines galimybes ir kompetencijas anksti nustatyti atvejus, kai interneto svetainės yra išnaudojama kenkėjiškai veiklai vykdyti. Prireikus taikyti kraštutines priemones sutvarkant/užkardant tokią interneto svetainę, NKSC kreipiasi į policijos pareigūnus, kurie iš dalies dubliuoja jau atliktus NKSC veiksmus. NKSC, kaip ir policija, aptinka arba gauna informaciją apie duomenims vilioti ir kt. kenkėjiškai veikai sukurtas interneto svetaines, tačiau NKSC negali imtis savarankiškų veiksmų užkardant tokius atvejus.

Siekiant efektyviai kovoti su kenkėjiškomis interneto svetainėmis yra svarbu aiškiai apibrėžti institucijų atsakomybes pagal tai, kas greičiausiai ir efektyviausiai gali identifikuoti grėsmes bei pritaikyti reikalingas sankcijas ar priemones sustabdyti neigiamam poveikiui tokių svetainių lankytojams.

Rekomendacijos:

3.1. Įvertinti galimybę įstatymiškai suteikti NKSC teisę teikti privalomus nurodymus blokuoti interneto svetainę (žr. pav. 3) tais atvejais, kai interneto svetainė yra išnaudojama kenkėjiškai veiklai, tokiu būdu suteikiant daugiau įgaliojimų institucijai, kuri turi įrankius ir kompetencijas anksti identifikuoti grėsmes;

3.2. Peržiūrėti NKSC ir policijos atsakomybes užkardant kenkėjiškas interneto svetaines, sukurtas vykdyti nusikalstamą veiką elektroninėje erdvėje, bei numatyti efektyvius bendradarbiavimo mechanizmui, kai nėra įmanoma aiškiai atskirti atsakomybių.



Pav. 3. Kenkėjiškų interneto svetainių sutvarkymo/užkardymo procesas NKSC suteikus teisę teikti privalomus nurodymus blokuoti interneto svetainę.

Projekto eigos apibendrinimas