Kenkėjiškų interneto svetainių užkardymas kitose šalyse

Užsienio praktikų analizė

Programos „Kurk Lietuvai“ projekto vadovai
Renata Donauskytė | Karolis Vyčius

Turinys

Įžanga

Kadangi kenkėjiškos interneto svetainės yra kompleksinė problema, neužtenka vienos priemonės siekiant jas užkardyti. Europos valstybės neretai taiko kompleksines priemones kovojant su kenkėjiškomis interneto svetainėmis. Siekiant apžvelgti visą priemonių spektrą, bus detaliai analizuojamos dviejų valstybių taikomos praktikos – Latvijos ir Jungtinės Karalystės. Antroje analizės dalyje daugiau dėmesio bus skiriama atskiroms priemonės palyginti ir įvertinti tarp skirtingų valstybių. Taigi, analizė susideda iš dviejų dalių:

I. Valstybių analizė;

II. Priemonių analizė.

Užsienio praktikų analizės **tikslas – apžvelgti Europoje taikomas skirtingas kenkėjiškų interneto svetainių užkardymo praktikas įvertinant jų stipriąsias ir silpnąsias puses**. Analizė buvo parengta remiantis viešai prieinamų dokumentų analize bei kokybiniais interviu su Šveicarijos ir Latvijos partneriais.

Užsienio praktikų analizė yra „Esamos situacijos analizė: Interneto svetainių saugumo būklė Lietuvoje“ tęsinys. Rekomenduojama pirmiau susipažinti su joje pateikiamomis Nacionalinio kibernetinio saugumo centro (toliau – NKSC) ir kitų Lietuvos institucijų taikomomis priemonėmis užkardant kenkėjiškas interneto svetaines.

I. Valstybių analizė

Šioje dalyje bus apžvelgiamas visas spektras saugumo priemonių, taikomų Latvijoje ir Jungtinėje Karalystėje

Latvija daugeliu atveju turi tokius pačius saugumo mechanizmus kaip ir Lietuva, tačiau taip pat turi papildomų priemonių tokių, kaip „Atsakingo interneto paslaugų teikėjo“ programa ir DNS Ugniasienę.

Jungtinė Karalystė pagal kibernetinio saugumo vertinimą yra pirmaujanti valstybė Europoje bei turi itin platų inovatyvių priemonių paketą verslui ir viešajam sektoriui.

Lietuva kibernetinio saugumo reitinguose yra tarp pirmaujančių Europoje ir pasaulyje

Pagal 2020 m. pasaulinio kibernetinio saugumo indekso duomenis Lietuva ne itin atsilieka nuo Jungtinės Karalystės, o Latviją netgi lenkia. Vis dėlto tiek Latvija, tiek Jungtinė Karalystė turi platesnį priemonių spektrą kovojant su kenkėjiškomis interneto svetainėmis nei Lietuva, todėl verta išanalizuoti tokių priemonių taikymo naudą ir rizikas. Detaliai analizei pasirinktas Latvijos atvejis dėl CERT.LV panašumo savo funkcijomis į Lietuvos Nacionalinį kibernetinio saugumo centrą, o Jungtinė Karalystė dėl ypač plačiai išplėtoto priemonių paketo, skirto kenkėjiškų interneto svetainių grėsmėms valdyti.

#1

Jungitnė Karalystė vertinama geriausiai Europoje

#4

Lietuva patenka tarp geriausiai vertinamų valstybių Europoje

#9

Latvija patenka į 10-uką geriausiai vertinamų valstybių Eurpoje

Global Cybersecurity Index, 2020 m.

Latvija

CERT.LV

CERT.LV misija – skatinti informacinių technologijų saugumą Latvijoje. Pagrindines fukcijos apima kibernetinių grėsmių stebėjimas; pagalbos teikimas valstybinėms institucijos dėl informacinių technologijų saugumo; prevencinės veiklos vykdymas fizinių ir juridinių asmenų atžvilgiu, kai incidente dalyvauja IP adresas iš Latvijos arba .LV domenas; viešojo sektoriaus, IT specialistų ir kitų asmenų švietimo veikla. Daugiausia dirbama su viešuojo sektoriaus ir kritinės infrastruktūros įmonėmis, bet, esant poreikiui ir galimybei, taip pat teikiama pagalba verslui ir gyventojams.

CERT.LV taiko įvairiapuses priemones siekiant užkardyti kenkėjiškas interneto svetaines. Didžiausias išskirtinumas – tokių svetainių įtraukimas į blokuojamų svetainių sąrašus per DNS ugniasienę.

Svetainės valdytojo informavimas

CERT.LV, aptikęs latviško domeno interno puslapį, užkrėstą kenkėjiška programine įranga, pirmiausia kreipiasi į svetainės valdytojus, kad jie pašalintų tokią programinę įrangą.

Paslaugų teikėjų informavimas

CERT.LV, aptikęs kenkėjišką internetinį puslapį (pirmiausia užsienio domeno, bet tam tikrais atvejais ir latviško domeno) kreipiasi į interneto arba prieglobos paslaugų teikėjus, kad jie savanoriškai apribotų prieigą prie tokio puslapio. Siekiant pagerinti bendradarbiavimą, CERT.LV iniciavo „Atsakingo interneto paslaugų teikėjo“ programą tiems paslaugų teikėjams, kurie įsipareigoja teikti informaciją savo klientams apie užkrėstus įrenginius ar jų dalyvavimą kibernetinėse atakose.

Informacijos perdavimas policijai

Nepavykus išspręsti problemos nė vienu aukščiau nurodytu būdu, CERT.LV renka įrodymus apie kenkėjišką interneto svetainės veiklą ir ją perduoda policijai. Atlikus tyrimą, policijos pareigūnai kreipiasi į teismą dėl sankcijos užblokuoti tokią interneto svetainę.

Informacijos perdavimas Google Safe Browsing

CERT.LV, aptikę naują kenkėjišką interneto svetainę (gautą ne iš trečiųjų šalių sąrašų), užpildo pranešimo formą Google Safe Browsing sistemoje. Rezultatai paprastai nėra stebimi.

Įtraukimas į blokuojamų svetainių sąrašus per DNS ugniasienę

CERT.LV bendradarbiaudamas su NIC (.LV domeno registro tvarkytoju) sukūrė DNS ugniasienę – nemokamą įrankį, skirtą apsaugoti atskirus vartotojus ir organizacijas nuo kibernetinių grėsmių, tokių kaip netikros bankų svetainės, nesąžiningos prekybos platformos, virusus platinančios svetainės ir kt. .

„Atsakingo interneto paslaugų teikėjo“ programa

(angl. *Responsible Internet Service Provider*)

Pagal šią programą yra suteikiamas kokybės ženklelis tiems paslaugų teikėjams, kurie įsipareigoja: a) teikti informaciją savo klientams apie užkrėstus įrenginius ar kitas saugumo spragas bei kokių veiksmų reikėtų imtis; b) bendradarbiauti su „Saugus internetas Latvijoje" ir efektyviai šalinti nelegalų ir žalingą turinį ir kt. Ši priemonė suteikia galimybę greitai informuoti galutinius vartotojus apie kylančias grėsmes ir efektyviai šalinti žalingą turinį.

10+

interneto paslaugų teikėjų yra suteiktas ženkliukas tokiu būdu padengiant didžiąją dalį interneto vartotojų.

59 %

nuo visų aptinkamų pažeidžiamų IP yra suisję su saugumo spragomis dėl netintamos konfigūracijos (2019 m.)

8 %

nuo visų aptinkamų pažeidžiamų IP yra užkrėsti kenkėjiška programine įranga (2019 m.)

Informacija iš cert.lv

CERT-Skydas

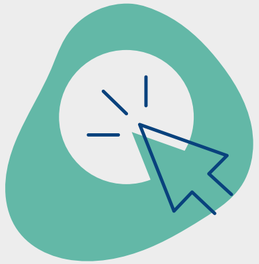
CERT.LV identifikuoja ir rankiniu būdu patikrina visas galimas grėsmes taip sumažinama tikimybė, kad neteisingai bus užblokuota interneto svetainė.

Kenkėjiška programinė įranga

Sąrašas interneto puslapių, kuriuose patalpinta kelnkėjiška įranga, generuojamas pasitelkiant automatines priemones, todėl yra nedidelė tikimybė užblokuoti neteisingą puslapį.

Duomenų viliojimas

Interneto svetainės, kuriose įtariama yra viliojami duomenys, taip pat į šį sąrašą patenka svetainės, kurios buvo nulaužtos.



Interneto kasyba

Be leidimo kriptovaliutas kasantys interneto puslapiai.

DNS ugniasienė

(angl. *DNS Firewall*)

Tai gyventojams ir verslui skirta nemokama priemonė, sauganti nuo suklastotų bankų puslapių, netikrų elektroninių prekyviečių ar virusus platinančių interneto svetainių. CERT.LV, stebėdamas kibernetinę erdvę ir gaudamas informaciją iš partnerių, identifikuoja kenkėjiškas interneto svetaines ir jas blokuoja DNS ugniasienės naudotojams. Kitaip tariant, vietoj to, kad DNS ugniasienės naudotojai pasiektų kenkėjišką interneto svetainę, jie yra nukreipiami į specialų puslapį (angl. *landing page*), kuriame nurodoma blokavimo priežastis ir kita svarbi informacija. DNS ugniasienė leidžia apsisaugoti nuo skirtingų grėsmių (žr. sąrašą dešinėje). Daugiau žr. 24-32 p.

Informacija iš dnsmuris.lv

Jungtinė Karalystė

National Cyber Security Centre (NCSC)

NCSC reaguoja į kibernetinio saugumo incidentus siekdamas sumažinti žalą organizacijoms ir visai Jungtinei Karalystei, teikia konsultacijas, priemones ir pagalbą viešajam, privačiam sektoriui ir gyventojams, kaip išvengti grėsmių susijusių su kibernetiniu saugumu bei rūpinasi šalies kibernetinės erdvės bei tinklų saugumu. Nuo pat įkūrimo 2016 m. NCSC skiria didelį dėmesį ne tik kritinei infrastruktūrai, viešajam sektoriui, tačiau ir finansų institucijoms bei privačioms įmonėms.

Jungtinės Karalystės NCSC plėtoja aktyvios kibernetinės gynybos priemonių sistemą. Nors pirmenybė yra teikiama viešajam sektoriui, tačiau dalis priemonių taip pat skirtos ir verslui. Toliau pateikiamos tik pagrindinės programos priemonės.

Pašalinimo priemonė
(angl. *Takedown Service*)

NCSC kartu su Netcraft (Netcraft – privati bendrovė, teikianti su kibernetiniais nusikaltimais susijusias paslaugas) identifikuoja kenkėjiškas interneto svetaines ir apie tai informuoja prieglobą bei originalios svetainės savininką.

Pranešimas apie įtartinus elektroninius laiškus
(angl. *Suspicious Email Reporting Service*)

Suteikia galimybę pranešti apie įtartinus elektroninius laiškus persiunčiant juos NCSC bei padedant greičiau identifikuoti kenkėjiškas interneto svetaines, kai el. laiškuose yra nuorodos į jas, ir jas pašalinti

DNS ugniasienė
(angl. *Protective Domain Name Service*)

NCSC inicijuota ir Nominet (Nominet – aukščiausio lygio .uk, .co.uk, .org.uk ir kitų domenų registro valdytoja) sukurta priemonė, skirta blokuoti kenkėjiškas interneto svetaines DNS būdų apsaugant viešojo sektoriaus įstaigų darbuotojus.

Kibernetinių grėsmių adapteris
(angl. *Cyber Threat Intelligence Adaptor*)

Leidžia įgaliotoms organizacijoms gauti aukštos kokybės, patikrintą informaciją apie įtartinas interneto svetaines bei IP adresus. Taip pat ši priemonė integruojama su organizacijų naudojamomis sistemomis (pvz., LME, Elastic, LogPoint, Splunk, Sentinel) bei teikia informaciją NCSC.

El. pašto patikra
(angl. *Mail Check*)

Mail Check padeda organizacijoms užtikrinti tinkamą el. pašto konfigūraciją apsisaugant nuo sukčiavimo, duomenų viliojimo atakų (SPF, DKIM, DMARC, TLS, MTA-STS). Taip pat veikia ir Web Check priemonė, skirta patikrinti viešojo sektoriaus įstaigų interneto svetaines dėl pažeidžiamumų siekiant užkirsti kelią svetainės nulaužimui.

National Cyber Security Center: Active Cyber Defence The fourth Year

Pašalinimo priemonė

(angl. *Takedown Service*)

99.6 %

identifikuotų duomenis viliojančių svetainių buvo sėkmingai pašalintos per 2020 m. (iš viso 166 710)

65.3 %

duomenis viliojančių svetainių buvo pašalinta per 24 val. laiko tarpą nuo identifikavimo momento 2020 m.

42 576

identifikuotų duomenis viliojančių atvejų buvo susijusę su svetainėmis, siekiančiomis atkartoti viešojo sektoriaus interneto puslapius, 2020 m.

NCSC, užfiksavęs įtartinas kenkėjiškas interneto svetaines ar IP adresus iš Jungtinės Karalystės, apie tai informuoja infrastruktūros paslaugų teikėją. Apsimestinių svetainių atveju informuojamas ir originalios svetainės savininkas. Imituojančių viešojo sektoriaus svetainių atjungimas inicijuojamas nepriklausomai nuo to, kurioje šalyje patalpinta svetainė.

National Cyber Security Center: Annual Review 2020

Pranešimas apie įtartinus elektroninius laiškus

(angl. *Suspicious Email Reporting Service*)

Ši priemonė leidžia gyventojams pranešti apie įtartinus el. laiškus paprastu būdu tiesiog persiunčiant juos į specialią NCSC el. pašto dėžutę. Tuomet NSCS analizuoja gautus el. laiškus ir identifikuoja kenkėjiškų interneto svetainių nuorodas bei inicijuoja jų pašalinimą. Analogiškos priemonės naudojamos įtartinoms SMS žinutėms, telefonų skambučiams, reklamoms ir svetainėms.

5.4 milijonai

pranešimų apie gautus įtartinus el. laiškus iš Jungtinės Karalystės gyventojų
(per 2020 rugsėjo – 2021 rugsėjo laikotarpį)

90 100

identifikuotų ir pašalintų kenkėjiškų interneto svetainių atvejų remiantis pranešimais
(per 2020 rugsėjo – 2021 rugsėjo laikotarpį)

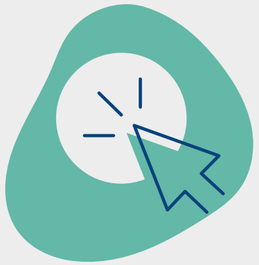
50 500

identifikuotų ir pašalintų kenkėjiškų interneto svetainių atvejų susijusių su sukčiavimu remiantis pranešimais
(per 2020 rugsėjo – 2021 rugsėjo laikotarpį)

National Cyber Security Center: Annual Review 2021

DNS ugniasienė

(angl. *Protective Domain Name Service*)



2.8 milijonai

viešojo sektoriaus darbuotojų saugomų nuo kenkėjiškų interneto svetainių per DNS ugniasienę 2020 m.

925 įstaigos

viešojo sektoriaus įstaigos naudojančios DNS ugniasienę 2021 m.

4.4 milijardų

užblokuotų DNS užklausų susijusių su potencialiai kenkėjiškomis interneto svetainėmis 2021 m.

DNS ugniasienė apriboja naudotojų prieigą prie NCSC identifikuotų kenkėjiškų interneto svetainių domenų. Blokuojamų domenų sąrašas yra sudaromas iš komercinių šaltinių bei NCSC surinktos informacijos. Verta paminėti, kad NCSC šią priemonę panaudojo ir SolarWinds situacijos analizei. Priemonę įgyvendinimo Nominet.

National Cyber Security Center: Annual Review 2020
National Cyber Security Center: Annual Review 2021

II. Priemonių analizė

Šioje dalyje bus apžvelgiamos dvi priemonės, kurios pasižymi dideliu kompleksiškumu, todėl reikalauja atskiros analizės

Įvairios bendradarbiavimo praktikos tarp atsakingų institucijų ir interneto bei prieglobos paslaugų teikėjų aptinkamos visose šalyse, tačiau jos labai skirtingos, todėl verta išanalizuoti, kokie yra pranašumai ir trūkumai skirtingų praktikų.

DNS ugniasienė šiuo metu yra taikoma ne tik Latvijoje ir Jungtinėje Karalystėje, bet ir kitose užsienio valstybėse. Taip pat šiuo metu Lietuvoje atliekamas DNS ugniasienės pilotas. Dėl šių priežasčių pravartu detaliau išanalizuoti jos taikymo niuansus.

Bendradarbiavimas su interneto ir prieglobos paslaugų teikėjais

Nuo neformalaus iki struktūruoto bendradarbiavimo modelio

Atliekant esamos situacijos analizę Lietuvoje bei nagrinėjant Europos šalių praktikas, buvo pastebėta, kad visose šalyse užkardant kenkėjiškas interneto svetaines pirmiausia yra bendradarbiaujama tarp atsakingų institucijų ir interneto bei prieglobos paslaugų teikėjų. Nuo sėkmingo šių institucijų bendradarbiavimo priklauso ir kenkėjiškų svetainių užkardymo greitis ir efektyvumas. Vis dėlto tarp Europos šalių nėra vieningo bendradarbiavimo modelio ir jis gali varijuoti nuo visiškai neformalaus (Vokietija) iki struktūruoto (Nyderlandai).

Skirtingas Europos šalių praktikas galima suskirstyti į tris teorinius modelius

Lietuva priskirtina prie neformalaus modelio, nes NKSC nėra teisiškai įpareigota užkardyti kenkėjiškas interneto svetaines. Pavienius atvejus NKSC perduoda prieglobos paslaugų teikėjams, tačiau kenkėjiškų svetainių sutvarkymas priklauso tik nuo prieglobos paslaugų teikėjo geros valios ir vidinių taisyklių. Vis dažniau NKSC perduoda informaciją policijai, kuri kreipiasi dėl teismo sprendimo svetainės blokavimui. Žemiau pateikiami kelių valstybių pavyzdžiai, kurie galėtų būti priskirti prie atitinkamo bendradarbiavimo modelio.

Neformalus modelis	Pusiau struktūruotas modelis	Struktūruotas modelis
CERT-Bund (Vokietija)	PROKI (Čekija)	Notice and Takedown Code (Nyderlandai)
NKSC (Lietuva)*	Responsible ISPs (Latvija)	Takedown Service (Jungtinė Karalystė)**

*Detali Lietuvos modelio analizė pateikiama „Esamos situacijos analizė Interneto svetainių saugumo būklė Lietuvoje“

**Dažniausia taikoma viešojo sektoriaus interneto svetainių imitavimo atvejais

Vokietija: CERT-Bund

Neformalus modelis

Bendradarbiavimo praktika, kai **nėra aiškių taisyklių**, kada ir kokiu būdu atsakingos institucijos perduoda informaciją interneto ar prieglobos paslaugų teikėjams apie kenkėjiškas interneto svetaines. Bendradarbiavimas yra grįstas informavimu, pasitikėjimu ir neformaliu bendravimu.

Pagrindiniai bruožai

CERT-Bund įstatymiškai nėra įpareigotas inicijuoti kenkėjiškų svetainių blokavimo, tačiau tokias svetaines aptikus apie jas yra pranešama interneto arba prieglobos paslaugų teikėjams.

Tik interneto ir prieglobos paslaugų teikėjai gali užblokuoti kenkėjiškas svetaines tai atliekant pagal savo vidaus taisykles ir tvarką. CERT-Bund neturi įtakos šiems procesams.

Tokiam bendradarbiavimo modeliui reikalingi geri **neformalūs santykiai tarp atsakingų institucijų ir interneto bei prieglobos paslaugų teikėjų**. CERT-Bund teigia turintys gerus darbinius santykius. Vis dėlto, tai neužtikrina, kad kenkėjiškų svetainių pasiekiamumas bus apribotas.

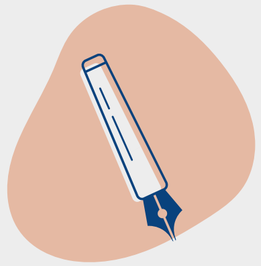
Parengta pagal 2021 m. gruodžio mėn. gautus atsakymus el. paštu

Čekija: CSIRT.CZ

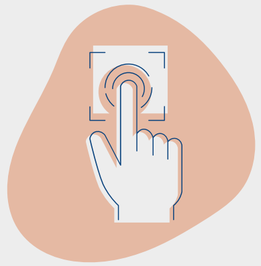
Pusiau struktūruotas modelis

Bendradarbiavimo praktika, kai **yra aiškios taisyklės**, kada ir kokiu būdu atsakingos institucijos perduoda informaciją interneto ar prieglobos paslaugų teikėjams apie kenkėjiškas interneto svetaines. **Nėra apibrėžta, kaip turi elgtis** su gauta informacija interneto bei prieglobos paslagų teikėjai

Pagrindiniai bruožai



CSIRT.CZ kartu su mokslininkų grupe 2015-2020 metais įgyvendinto projektą PROKI, kurio metu buvo sukurtas analitinis įrankis, skirtas rinkti informaciją iš įvairių šaltinių, ją apdoroti ir parengti ataskaitas apie galimai kenkėjiškas interneto svetaines.



Ataskaitos apie galimai kenkėjiškas veikas periodiškai yra perduodamos interneto paslaugų teikėjams ir kitoms susijusioms institucijoms, kurios pagal savo vidaus tvarką imasi veiksmų. **Siekiant efektyvesnio informacijos apsikeitimo, buvo sukurtas API**, kuris pakeitė informacijos siuntimą el. paštu.

Sistemingas informacijos apdorojimas leidžia aptikti net ir neakivaizdžius kenkėjiškų svetainių atvejus. Vis dėlto, interneto paslaugų teikėjai nėra įpareigoti uždaryti tokių svetainių, jie vadovaujasi savo vidaus politika.

Parengta pagal 2021 m. gruodžio mėn. gautus atsakymus el. paštu ir dokumentų analizę

Nyderlandai: NCSC

Struktūruotas modelis

Bendradarbiavimo praktika, kai **yra aiškios taisyklės**, kada ir kokiu būdu atsakingos institucijos perduoda informaciją interneto ar prieglobos paslaugų teikėjams apie kenkėjiškas interneto svetaines, o pastarieji **turi įpareigojimą atlikti atitinkamus veiksmus.**

Pagrindiniai bruožai

Notice and Takedown Code (NTD) – **taisyklių rinkinys, skirtas interneto ir prieglobos paslaugų teikėjams** (tiesiogiai galintiems šalinti turinį arba blokuoti svetainę), atsakingoms institucijoms ir trečiosioms šalims (gyventojams ir verslui) ir apibrėžiantis, kokiu būdu turi būti pateikiami ir išnagrinėjami pranešimai dėl kenkėjiškų svetainių.

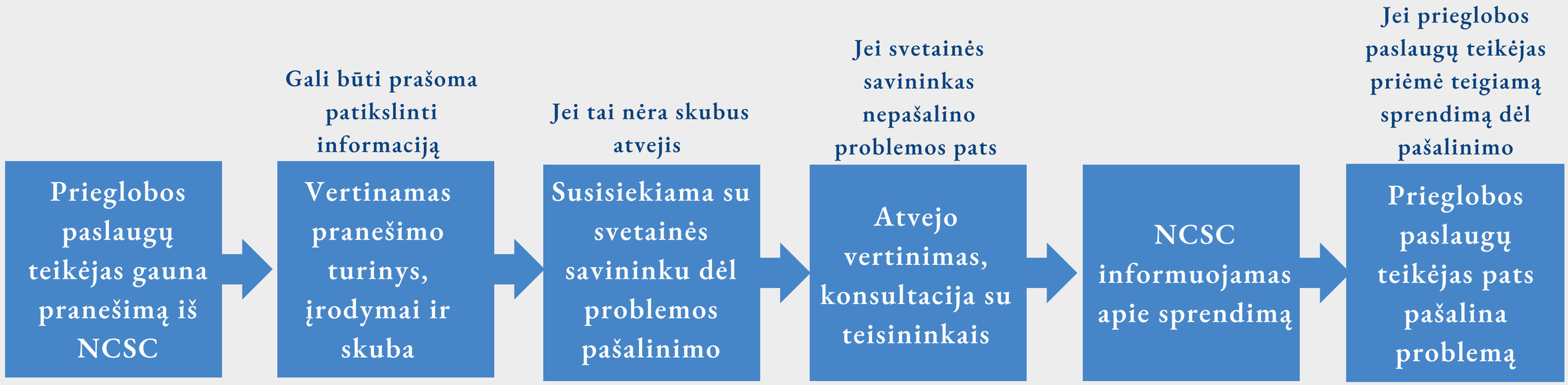
Sistema apima ne tik kenkėjiškas interneto svetaines, bet ir žalingą, nelegalų turinį ir kt. Tikslas – greitai ir efektyviai reaguoti į akivaizdžius pažeidimus internete, kai yra pateikiami pakankami įrodymai.

NCSC neteikia privalomų nurodymų. Tai reiškia, kad **interneto ar prieglobos paslaugų teikėjai neprivalo blokuoti interneto svetainės, tačiau privalo įvertinti pateiktą informaciją ir informuoti apie savo sprendimą bei jį pagrįsti.**

Parengta pagal 2021 m. gruodžio mėn. gautus atsakymus el. paštu ir dokumentų analizę

Nyderlandų prieglobos paslaugų teikėjo veiksmai, kai yra gautas pranešimas iš NCSC

Notice and Takedown Code (sutr. NTD Code) suteikia galimybę tiek gyventojams, tiek atsakingoms institucijoms kreiptis į prieglobos paslaugos teikėjus tiek dėl turinio pašalinimo, tiek dėl interneto svetainės atjungimo. Nors procesas gali skirtis priklausomai nuo to, kas pateikia prašymą, bet visais atvejais išlieka pagrindinė proceso dalys. Žemiau esančioje schemoje pavaizduota, kaip atrodo pagrindiniai tokio proceso žingsniai, kai Nyderlandų NCSC praneša apie kenkėjišką interneto svetainę. Atkreiptinas dėmesys, kad pagal NTD Code sprendimą priima prieglobos paslaugų teikėjas. Nusprendus neatjungti svetainės, tiek gyventojai, tiek institucijos gali vėliau kreiptis į teismą ir gauti sankciją, kurią būtų privaloma vykdyti. Nepaisant to, NTD Code padeda išvengti kreipimosi į teismą ir ilgo proceso, kai yra akivaizdūs pažeidimo atvejai.



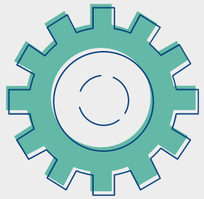
Apibendrinant, skirtingas Europos šalių praktikas galima suskirstyti į tris teorinius modelius

	Apibrėžtas informacijos perdavimo mechanizmas tarp atsakingos institucijos ir paslaugų teikėjų	Apibrėžti veiksmai, kurių turi imtis paslaugų teikėjas*
Neformalus modelis		
Pusiau struktūruotas modelis	✓	
Struktūruotas modelis	✓	✓

*Atkreiptinas dėmesys, kad tai nereiškia, jog duodami privalomi nurodytai interneto bei prieglobos paslaugų teikėjams blokuoti interneto svetainę, tačiau numatyta, kokius veiksmus būtina įvykdyti vertinant gautą informaciją,

Struktūruoto bendradarbiavimo modelio vertinimas

Galima teigti, kad neformalų bendradarbiavimo modelį taiko visos valstybės vienokia ar kitokia forma. Taigi, svarbu įvertinti, kuo galėtų būtų pranašesnis struktūruoto bendradarbiavimo modelis bei kokias rizikas reikia įvertinti norint taikyti tokį modelį.



Stiprybės

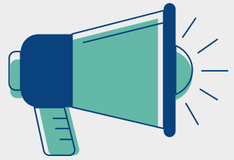
Akivaizdžių pažeidimų atveju yra daug **greičiau užkardomos grėsmės**. Aiškus mechanizmas, ką gali daryti atsakingos institucijos ir kaip turi elgtis paslaugų teikėjai pagal esamą teisinį reguliavimą. Paslaugų teikėjai turi suteikti grįžtamąjį ryšį, todėl **atsiranda daugiau skaidrumo**, kodėl yra arba nėra blokuojama interneto svetainė.

Silpnybės

Gerai veikia tik akivaizdžių pažeidimų atveju, **dalis pranešėjų vis tiek turi kreiptis į teismą**. Kadangi internto paslaugų teikėjai savanoriškai laikosi susitarimų, dalis jų gali nuspręsti neprisijunti, todėl gali kilti teisingos konkurencijos klausimai.

Galimybės

Aiškus ir skaidrus mechanizmas leidžia išsigryninti kriterijus, pagal kuriuos nustatomi pažeidimai, todėl **gali mažėti atvejų, patenkančių į teismą**. Paslaugų teikėjams lengviau pritraukti ir išlaikyti klientus, nes bendradarbiavimas su atsakingomis institucijomis kelia pasitikėjimą.



Rizikos

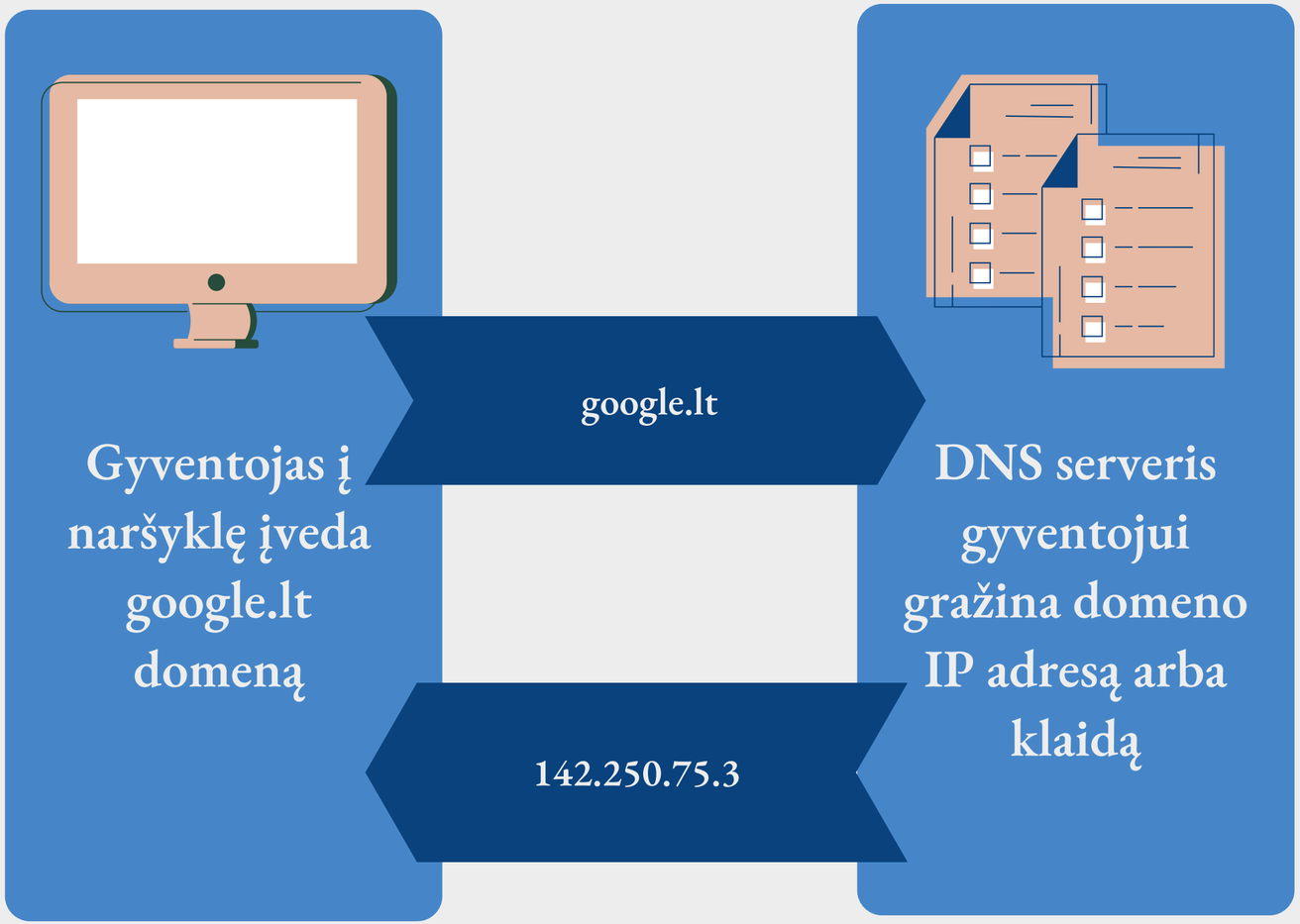
Balansuojant tarp efektyvaus grėsmių užkardymo ir žmogaus bei verslo teisių užtikrinimo, gali iškilti **„per didelio“ ir „per mažo“ blokavimo rizika**. Pirmu atveju, gali nukentė žmogaus teisės ir verslo interesai, antru atveju, nebus pasiektas norimas efektyvumo ir saugumo lygis.

DNS ugniasienė

Priemonė, skirta ypač greitai apriboti kenkėjiškų interneto svetainių domenų pasiekiamumą tikslinei auditorijai

DNS ugniasienės įgyvendinimas gali tapti viena iš priemonių ypač greitai apriboti kenkėjiškų interneto svetainių domenų pasiekiamumą, kol vyksta tolimesni administraciniai ir teisiniai procesai bei apsaugoti to norinčius gyventojus ar įstaigas nuo galimos tokių svetainių keliamos žalos.

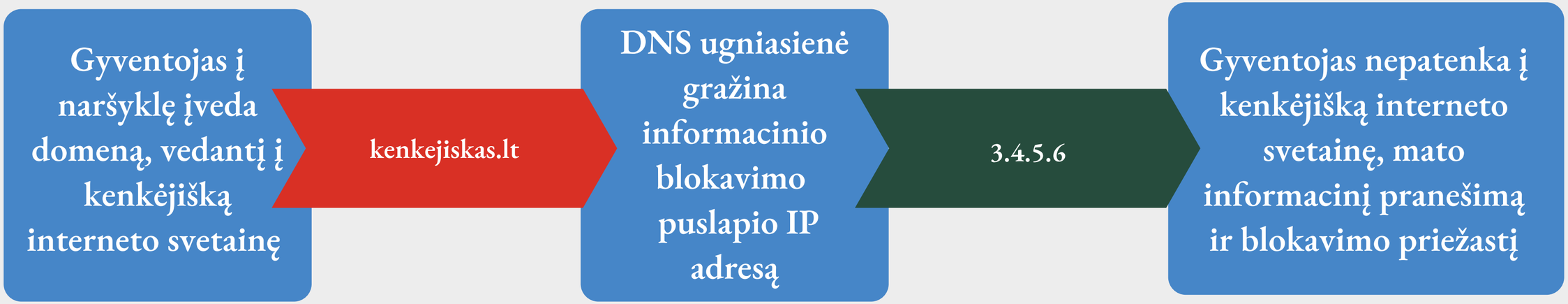
DNS (angl. *Domain Name System*) veikimas



Nuo kenkėjiškų domenų apsaugomi tik gyventojai naudojantys DNS ugniasienę

Gyventojas, naudojantis įprastą DNS

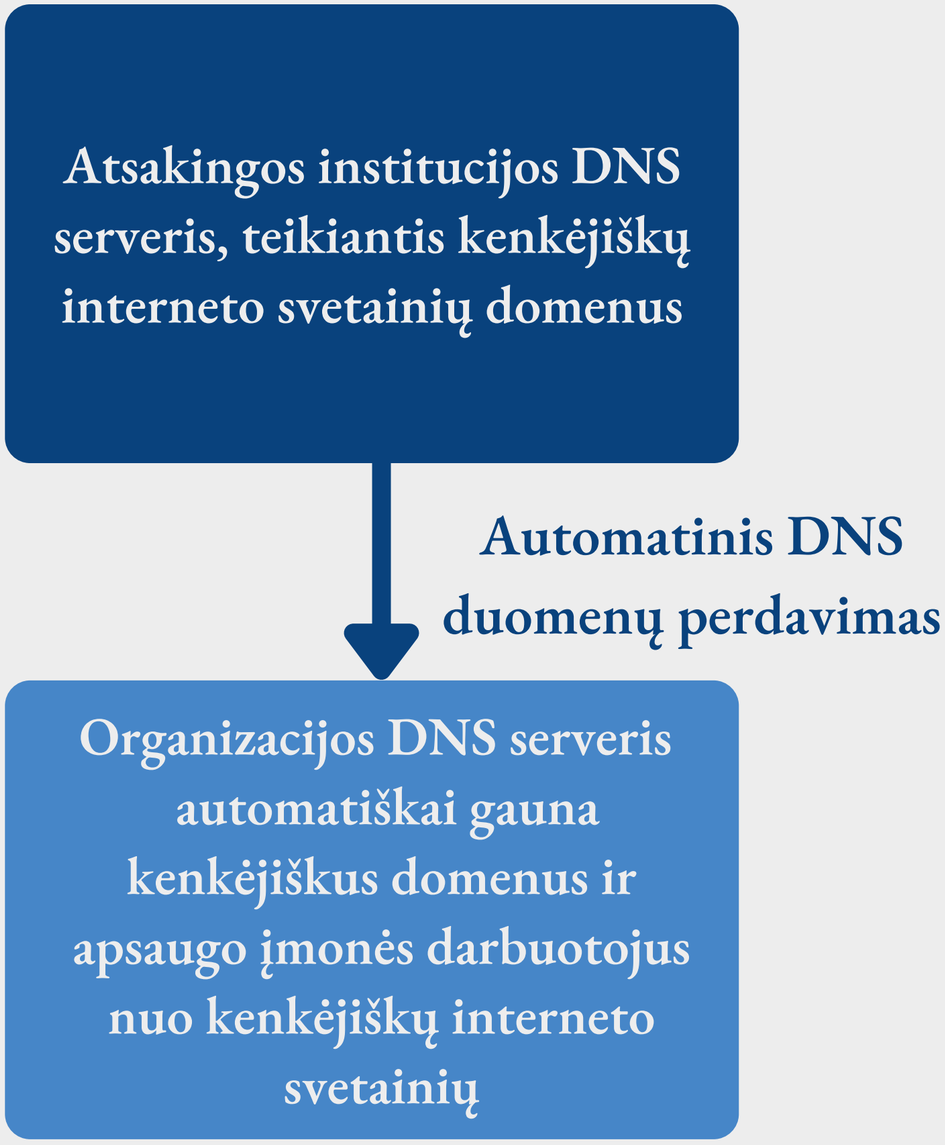
Gyventojas, naudojantis DNS ugniasienę



Apsauga nuo kenkėjiškų interneto svetainių įmonėms

Galimybė įmonėms gauti kenkėjiškų interneto svetainių domenus ir apsaugoti įmonės darbuotojus nuo galimos žalos

Kai kurios įmonės naudoja savo DNS serverius, tokiu atveju įmonei patogiau gauti informaciją apie kenkėjiškus domenus tiesiai į savo DNS serverius, o ne tiesiogiai naudoti DNS ugniasienę. Tai leidžia kenkėjiškus domenus įmonei blokuoti visiškai automatiškai per RPZ (angl. *Response policy zone*). Naujai identifikuoti kenkėjiški domenai gali tapti nepasiekiami darbuotojams per mažiau nei valandą.
Kitų šalių naudojamas perdavimo mechanizmas dažniausiai remiasi DNS zonų perdavimu (angl. *DNS zone transfer*), tačiau įprastai siūlomos ir alternatyvos.



DNS ugniasienės gerosios užsienio praktikos ir skirtingi naudotojai

Gyventojams ir organizacijoms

DNS ugunsmūris
(Latvija)

CIRA Canadian Shield
(Kanada)

SWITCH Public DNS ir
SWITCH DNS Firewall
(Šveicarija)

Tik viešojo sektoriaus įstaigoms

NCSC Protective Domain Name Service
(Jungtinė Karalystė)

Australian protective DNS service
(Australija)

DNS ugniasienės įgyvendinimo modeliai

Šalyse galime sutikti skirtingus DNS ugniasienės įgyvendinimo modelius: kūrimo patiems, kūrimo kartu su šalies domenų registro valdytojais ar pirkimo, kaip paslaugos, iš kompanijų (žr. *detalų pirkimo, kaip paslaugos produktų palyginimą*).

Latvija

CERT.LV DNS ugniasienę įgyvendino bendradarbiaudamas su NIC – aukščiausio lygio .lv domenų registro valdytojas, kuris yra valdomas Latvijos universiteto.

Jungtinė Karalystė

Nominet teikia DNS ugniasienės sprendimą Jungtinės Karalystės Nacionaliniam kibernetinio saugumo centrui (angl. *National Cyber Security Centre*). Nominet – aukščiausio lygio .uk, .co.uk, .org.uk ir kitų domenų registro valdytojas.

Australija

Kaip ir Jungtinės Karalystės atveju, Nominet teikia DNS ugniasienės sprendimą Australijos kibernetinio saugumo centrui (angl. *Australian Cyber Security Centre*).

Šveicarija

SWITCH-CERT DNS ugniasienę įgyvendino pati ir teikia paslaugą organizacijoms, universitetams bei gyventojams.

DNS ugniasienės pagrindinės rizikos

Kadangi ne visada yra lengva nustatyti, ar interneto svetainė yra tikrai kenkėjiška, kyla rizika, kad dalis domenų bus užblokuoti klaidingai

Svarbu apibrėžti labai **aiškius kriterijus**, kada domenas yra įtraukiamas į blokuojamų kenkėjiškų domenų sąrašą, kokiais būdais ir kada yra iš jo pašalinamas, **užtikrinti blokavimo proceso skaidrumą ir pasitikėjimą DNS ugniasienės valdytoju**. Taip pat naudotojas turi matyti detalų informacinį pranešimą apie blokavimo priežastį. Siekiant išvengti klaidingo blokavimo rizikos, visi blokuotini domenai Latvijoje yra patikrinami specialisto, o ne tik automatiniais įrankiais. Šveicarijos SWITCH-CERT atkreipia dėmesį į papildomų saugumo mechanizmų būtinybę ypač didelį dėmesį skiriant **baltųjų domenų sąrašų** (angl. *domain whitelist*) sudarymui bei būtinybei periodiškai peržiūrėti blokuojamų domenų sąrašą siekiant kuo greičiau atblokuoti jau sutvarkytus domenus.

Kadangi DNS ugniasienės naudojimas gyventojams ir verslui nebūtų privalomas, kyla rizika, kad didžioji populiacijos dalis vis tiek liks neapsaugota, ypač ta dalis, kuri yra pažeidžiamiausia

Būtina įvertinti tokios priemonės populiarinimo kaštus, numatyti informacines kompanijas, **sklaidos strategiją**, kelti visuomenės pasitikėjimą šios priemonės valdytoja. Siekiant, kad didesnė populiacijos dalis būtų apsaugota nuo kenkėjiškų interneto svetainių, DNS ugniasiene galima skatinti naudotis ne tik gyventojus, bet ir verslo įmones ar viešojo sektoriaus įstaigas.

DNS ugniasienė: stiprybės ir silpnybės

Stiprybės

- Labai greitas kenkėjiškų interneto svetainių domenų blokavimas (per mažiau nei 1 val. nuo identifikavimo)
- Galima užblokuoti tiek Lietuvos, tiek užsienio interneto svetainių domenus
- Užtikrinamas skaidrumas, nes naudotojai gauna visą informaciją dėl domeno blokavimo priežasties
- Priemonei veikiant savanoriško naudojimo pagrindu (angl. *opt-in*) nėra reikalingas papildomas teisinis reguliavimas
- DNS ugniasienėje naudojamas DNS zonų mechanizmas leidžia kenkėjiškais domenais dalintis su verslu ir viešuoju sektoriumi

Silpnybės

- Galima blokuoti tik domenus ar subdomenus, tačiau neįmanoma užblokuoti tik konkrečių interneto svetainės puslapių
- Domenai užblokuojami tik daliai populiacijos, t.y tik gyventojams naudojantiems DNS ugniasienę
- Negalima įgyvendinti su turimais resursais (reikalingi papildomi serveriai ar paslaugos įsigyjimas)
- Negalima parodyti informacinio pranešimo su blokavimo priežastimi, kai svetainę bandomą pasiekti per HTTPS
- Negalima pakeisti DNS nustatymų naršamt per mobilųjį internetą Apple iOS operacinėje sistemoje,

DNS ugniasienės pilotai Lietuvoje

NKSC su partneriais savo iniciatyva pradėti DNS ugniasienių projektai

Remiantis Latvijos modeliu kuriama saugi ir patikima DNS infrastruktūra, kurios naudotojai būtų saugomi nuo kibernetinių atakų ir kenkėjiškų interneto svetainių. Siekiama užtikrinti naudotojų privatumą ir svetainių blokavimą per mažiau nei 1 val. nuo grėsmės identifikavimo.

DNS ugniasienės, skirtos viešojo sektoriaus įstaigų darbuotojams pilote dalyvauja 4 institucijos. Siekiama, kad ateityje ja naudotųsi visi KVTC klientai, YSII, VII valdytojai ir tvarkytojai.

Numatomas startas: 2022 m. II ketvirtis.

DNS ugniasienės, skirtos gyventojams ir organizacijoms įgyvendinimas

NKSC + DOMREG

DNS ugniasienės, skirtos viešojo sektoriaus įstaigų darbuotojams įgyvendinimas

NKSC + KVTC

Apibendrinimas

1. Latvija ir Jungtinė Karalystė taiko įvairias priemones užkardant kenkėjiškų svetainių grėsmes suprantant, kad vieno sprendimo neužtenka kompleksinei problemai spręsti. Taip pat neišvengiamai abiem atvejais tenka remtis į bendradarbiavimą su interneto ir prieglobos paslaugos teikėjais, nes jie vykdo patį interneto svetainės blokavimą ar atjungimą.

2. Interneto svetainės blokavimas su teismo sprendimu trunka per ilgai ypač tais atvejais, kai vykdomos didelio masto atakos. Sėkmingas atsakingų institucijų ir interneto bei prieglobos paslaugų teikėjų bendradarbiavimas gali prisidėti užtikrinant balansą tarp efektyvios gyventojų apsaugos ir galimo piktnaudžiavimo atvejų.

3. Nagrinėtos bendradarbiavimo praktikos rodo, kad tinkamai įgyvendintas struktūruoto bendradarbiavimo modelis gali suteikti greičio ir skaidrumo procesui bei turi potencialo sumažinti atvejų skaičių, kai yra kreipiamasi į teisėsaugos institucijas.

4. Tiek Latvija, tiek Jungtinė Karalystė naudoja DNS ugniasienę taip suteikdamos papildomą priemonę apsisaugoti nuo kenkėjiškų interneto svetainių. Esminis šių šalių skirtumas – skirtingi DNS ugniasienės naudotojai: Latvijos atveju tai gyventojai ir organizacijos, kai Jungtinės Karalystės atveju – viešojo sektoriaus įstaigos. DNS ugniasienė suteikia galimybę ypač greitai apriboti tikslinių auditorijų prieigą prie tokių svetainių.

5. Įgyvendinus priemones greitam kenkėjiškų interneto svetainių užkardymui, svarbu turėti ir priemones greitam grėsmių identifikavimui. Šiuo atveju verta atkreipti dėmesį į Jungtinės Karalystės taikomą pranešimų apie gautus įtartinus elektroninius laiškus priemonę.

Projekto gairės

Atlikta esamos situacijos analizė dėl interneto svetainių saugumo būklės Lietuvoje
2021 m. lapkritis

Projekto tarpiniai rezultatai ir svarstomos priemonės pristatyti kibernetinio saugumo tarybai
2021 m. gruodis

Atlikta gerosios užsienio praktikos analizė dėl priemonių, apribojančių kenkėjiškų svetainių prieigą
2021 m. gruodis

Atlikta viešoji konsultacija dėl siūlomų priemonių kenkėjiškų svetainių prieigos apribojimui
2022 m. sausis

Sukurtas kenkėjiškų svetainių prieigos apribojimo priemonių modelis remiantis užsienio praktikomis ir viešosios konsultacijos rezultatais
2022 m. vasaris

Pateikti pasiūlymai dėl reikalingų teisės aktų pakeitimų kenkėjiškų interneto svetainių priemonių modelio įgyvendinimui
2022 m. kovas

Projekto tarpinius rezultatus galima peržiūrėti ir progresą sekti: kurklt.lt

Kurk Lietuvai

Programos „Kurk Lietuvai“ kartu su Krašto apsaugos ministerija įgyvendinamas projektas

„Kenkėjiškų interneto svetainių grėsmių valdymo priemonių kūrimas“

2021