Ataskaita

Viešosios konsultacijos dėl Blokuojamų domenų valdymo informacinės sistemos kūrimo inicijavimo

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

Parengė Renata Donauskytė ir Karolis Vyčius

2022 m. vasaris

Kurk Lietuvai

KRAŠTO APSAUGOS MINISTERIJA

Kontekstas

„Kurk Lietuvai“ kartu su Krašto apsaugos ministerija įgyvendinamo projekto „Kenkėjiškų interneto svetainių grėsmių valdymo priemonių kūrimas“ metu įvykdytos individualios konsultacijos su įstatymu nustatyta tvarka domenus blokuoti galinčiomis valstybinėmis institucijomis atskleidė poreikį rasti priemones efektyviau vykdyti domenų blokavimą.

Dabartinis procesas, kai apie reikalavimą blokuoti domeną 90 interneto prieigos paslaugų tiekėjų yra informuojami el. laiškais siunčiant raštą, reikalauja daug rankinio darbo tiek iš blokuojančių institucijų, tiek iš interneto prieigos paslaugų teikėjų, neišvengiama žmogiškųjų klaidų, nėra galimybės blokuoti domenus 24/7, taip pat nėra galimybės patikrinti, kurie interneto prieigos paslaugų teikėjai įvykdė domeno blokavimą. Tiek pastarųjų metų Lietuvos, tiek pasaulio tendencijos rodo, kad kenkėjiškų interneto svetainių ir toliau daugės, todėl augs ir blokuotinų domenų skaičiai. Dėl šių priežasčių yra siekiama sukurti Blokuojamų domenų valdymo informacinę sistemą (toliau – BDVIS), kuri būtų efektyvi, saugi, skaidri ir patogi naudoti jos vartotojams.

Siekiant kuo geriau atliepti būsimos informacinės sistemos vartotojų poreikius ir matomas rizikas, buvo numatyta įgyvendinti viešąją konsultaciją informacinės sistemos inicijavimo etape.

Tikslas

Suteikti galimybę suinteresuotosioms šalims išreikšti poreikį ir pateikti pastabas dėl *pagrindinių* Blokuojamų domenų valdymo informacinės sistemos (BDVIS) veikimo principų (techniniai sprendimai, rizikų valdymas, reikalingas teisinis reguliavimas, tolimesni žingsniai įgyvendinant).

Metodas

2021 m. spalis–2022 m. sausis: individualios konsultacijos su tikslinėmis grupėmis, pusiau struktūruoti interviu.

2022 m. vasario 2 d. 9.00-11.00 val.: nuotolinė apskritojo stalo diskusija su visomis suinteresuotosiomis šalimis (MS Teams platformoje).

2022 m. vasario 2-9 d.: laisvos formos pasiūlymų teikimas raštu.

Individualių konsultacijų ciklas (pusiau struktūruoti interviu pagrindu) buvo atliktas su visomis viešojoje konsultacijoje dalyvavusiomis šalimis siekiant pasirengti apskritojo stalo diskusijai. Apkritojo stalo diskusijoje vienu metu dalyvaujant visoms suinteresuotosioms šalims buvo pristatyti tarpiniai individualių konsultacijų rezultatai, kurie buvo pagrindas tolimesnei diskusijai. Po apskritojos stalo diskusijos visi dalyviai per savaitę laiko turėjo galimybę pateikti papildomus pasiūlymus raštu. Ši ataskaita parengta remiantis apskritojo stalo diskusijos metu išsakytais komentarais bei pasiūlymais pateiktas raštu.

Dalyviai

Keturias pagrininės tikslinės grupės:

- **Interneto svetainės blokavimą galinčios inicijuoti valstybinės institucijos** – tokios institucijos, kurios pagal jų veiklą reguliuojančius teisės aktus turi teisė esant teismo sankcijai duoti privalomus nurodymus interneto svetainę blokuoti per interneto prieigos pasgaulų teikėjų sistemas;
- **Interneto prieigos paslaugų teikėjai (IPPT)** – subjektai, kurie vykdo interneto svetainės blokavimą, kai yra gaunamas privalomi nurodymai iš blokavimą galinčios inicijuoti valstybinės institucijos;
- **Kitos valstybinės institucijos** – tiesiogiai ar netiesiogiai susijusios su interneto svetainių blokavimo procesu;
- **Nepriklausomi kibernetinio saugumo ekspertai** – švietimo įstaigų, nevyriausybinių organizacijų bei asociacijų atstovai.

Apkritojio stalo diskusijoje (2022 m. vasario 2 d.) dalyvavo šių institucijų atstovai:

- Interneto svetainės blokavimą galinčios inicijuoti valstybinės institucijos:
  - Lietuvos Policija;
  - Lošimų priežiūros tarnyba;
  - Lietuvos bankas;
  - Lietuvos radijo ir televizijos komisija;
  - Valstybinė vartotojų teisių apsaugos tarnyba;
  - Narkotikų, tabako ir alkoholio kontrolės departamentas.[1]
- Interneto prieigos paslaugų teikėjai:
  - Telia;
  - Init;
  - Balticum;
  - Tele2;
  - Bitė;
  - Kertinio valstybės telekomunikacijų centras.
- Kitos valstybinės institucijos:
  - Krašto apsaugos ministerija;
  - Ryšių reguliavimo tarnyba;
  - Nacionalinis kibernetinio saugumo centas.
- Nepriklausomi kibernetinio saugumo ekspertai:
  - INFOBALT.

[1] NTAKD šiuo metu vykdo interneto svetainių blokavimą per prieglobos paslaugų teikėjus.

Konsultacijos apibendrinimas

BDVIS poreikis:

Diskusijos dalyviai buvo skatinami pasidalinti jiems kylančiais iššūkiais ir pagrindinėmis problemomis įgyvendinant teismo sankciją blokuoti interneto svetainę.

Blokavimą galinčios inicijuoti institucijos atkreipė dėmesį į šiuos iššūkius:

- Nėra efektyvių kontrolės mechanizmų, leidžiančių įsitikinti, kad domenas yra užblokuotas. Nurodytos kelios priemonės, kurios yra naudojamos: a) prašoma IPPT raštu patvirtinti, kad domenas yra užblokuota, o tai reikalauja daug žmogiškųjų resursų; b) prisiimama rizika ir tikrinami tik 10 didžiausių IPPT, kitus patikrinti yra sunku, nes reikia būti IPPT klientais;
- Didžiausia problema yra mažieji IPPT, nes nėra techninių būdų patikrinti, ar jie realiai blokuoja pagal privalomus nurodymus;
- IPPT sąrašas yra kintantis, todėl periodiškai reikia atnaujinti kontaktų sąrašus rankiniu būdu prieš siunčiant privalomus nurodymus;
- Lietuvos Policija nurodė, kad jie daugiausia blokuoja per IP adresus ir, jų nuomone, tai yra pasiteisinęs būdas. Vis dėlto centralizuotas blokavimas per IPPT būtų papildomas naudingas įrankis teisėsaugos rankose;

Interneto prieigos paslaugų teikėjai atkreipė dėmesį į šiuos iššūkius:

- Privalomi nurodymai blokuoti yra pateikiami padrikai, kiekviena institucija juos teikia skirtingai, ne visada tinkamai ir teisingai yra nurodomi reikalavimai. Nurodymams vykdyti užtenka pagrindinės informacijos;
- Šiuo metu yra daug insititucijų, kurios teisės aktuose yra nusimačiusios galimybę blokuoti interneto svetainę vienu ar kitu pagrindu. Gavus raštą dėl blokavimo, IPPT turi papildomai patikrinti, kokiu pagrindu yra teikiamas reikalavimas, taip pat skiriasi įvykdymo terminai, o tai sukuria papildomą administracinę naštą;
- Neegzistuoja vienas blokuojamų domenų sąrašas, kuris suteiktų galimybę IPPT patikrinti, ar viskas yra užblokuota. Tokia informacija taip pat būtų aktualu pateikti vienoje vietoje ir visuomenei;
- Valstybinės institucijos atlikdamos teisės aktų pakeitimus ir numatydamos galimybę teikti privalomus nurodymus blokuoti, ne visada atsižvelgia į technines galimybes įvykdyti tokius nurodymus. Dėl šios priežasties IPPT susiduria su sunkumais įgyvendinant kai kuriuos nurodymus;
- Laukiamas pokytis būtų, jeigu BDVIS naudotųsi visos institucijos, norinčios inicijuoti domeno blokavimą, t.y. tai darytų per vieną sistemą, tokiu pačiu principu, vadovautųsi tomis pačiomis taisyklėmis, tada tikrai sumažėtų administracinė našta ir klaidos tikimybė;
- Kertinis valstybės telekomunikacijų centras nurodė, kad jau darbar yra pusiau automatizavęs blokuojamų interneto svetainių sąrašo sudarymą, tačiau problema yra ta, kad ne visada yra atsiunčiami privalomi nurodymai iš valstybinių institucijų (net po tai, kai yra išiunčiami paklausimai). Blokuojant kelias interneto svetaines per savaitę, pusiau automatizuotas procesas yra gana efektyvus.

BDVIS veikimo principai:

Projekto vadovams trumpai pristačius siūlomos priemonės pagrindinius principus, diskusijos dalyviai buvo kviečiami išsakyti savo nuomonę dėl būsimos informacinės sistemos funkcionalumo, teisinių aspektų, rizikų valdymo bei svarstomų techninių įgyvendinimo alternavytų ir kt. klausimų.

Bendrieji komentarai:

- Iniciatyva yra gera, tačiau pats įgyvendinimas yra sudėtingas. Pirmiausia dėl to, kad DNS technologija nėra skirta blokavimui kaip ir pats internetas, todėl būtina užtikrinti, kad įrankis nebūtų naudojamas cenzūrai. Taip pat reikia įvertinti proporcingumą tarp tokio įrankio poreikio (užtikrinti, kad nebūtų pasiekiami nelegaliai veiklai vykdyti skirti puslapiai) ir jo galimo neigiamo poveikio (gyventojai ir verslas negalės pilnavertiškai naudotis interneto paslauga), jeigu įvyktų incidentas ir per klaidą būtų užblokuojama;
- Labai didelis postūmis būtų vien tai, kad valstybės institucijos sugebėtų ir galėtų pateikti vieną blokuojamų domenų sąrašą patogia forma IPPT, tada operatoriai galėtų lengviau vykdyti nurodymus bei užtikrinti tam tikro lygio kontrolę;
- BDVIS turėtų palaikyti ir domeno automatinę atblokavimo funkciją. Pavyzdžiui, teismui skyrus sankciją tik tam tikram laikotarpiui, IPPT neturėtų rūpintis ir sekti, kada domenas turėtų būti atblokuojamas;
- Siekiant užtikrinti, kad IPPT naudotųsi sistema, būtina sukurti patrauklią paslaugą, t.y. centraliuotai pateikti blokuojamų domenų sąrašus. Tam užtikrinti būtina toliau diskutuoti su visais proceso dalyviais ir siekti konsensuso;
- Domėtasi, kiek specifiškai bus nurodoma priežastis, dėl kurios domenas užblokuotas. Patikslinta, kad bus siekiama pateikti kuo tikslesnę informaciją, t.y. ne tik blokavimo priežastį, bet ir teismo nutarties numerį, taip pat ką daryti, jeigu manoma, kad puslapis per klaidą užblokuotas. Informacijos pateikimas turėtų būti suvienodintas (šiuo metu informaciniai puslapiai skiriasi), o susipažinti su informacija turėtų būti galimybė ir kitomis kalbomis pasikeitus nustatymus;
- Gretutinė BDVIS nauda būtų tai, kad visuomenei būtų pateikiama informacija vienoje vietoje, t.y. kokios institucijos gali inicijuoti interneto svetainės blokavimą, kokiais atvejais yra skiriama tokia sankcija, kokiam laikotarpiui blokuojama ir koks šiuo metu yra blokuojamų domenų skaičius. Šiuo metu nėra sistemingai pateikiama tokia informacija, todėl BDVIS suteiktų daugiau skaidrumo procesui bei galimybę analizuoti duomenis;

Teisiniai aspektai:

- Lietuva buvo įvardinta kaip valstybė, kuri visoje ES yra suteikusi teisę blokuoti interneto svetaines bene daugiausiai institucijų ir tai reglamentuoja apie 20 skirtingų teisės aktų. Nenorint, kad Lietuvoje atsirastų cenzūra, būtina užtikrinti, kad BDVIS nepažeistų saviraiškos ir žodžio laisvės bei verslo laisvės veikti. Kitaip tariant, tai neturėtų paskatinti plėsti blokuojamų interneto svetainių sąrašo keičiant įstatymus. Būtina užtikrinti tinkamą balansą tarp vertybių (saugumo ir laisves), todėl reikia sąžiningai diskutuoti viso BDVIS įgyvendinimo proceso metu;

- Pastebėta, kad labai svarbu dar teisėkūros etape sudėti saugiklius, neleisinčius piktnaudžiauti BDVIS. Teismai dažnai pasitiki valstybinėmis insitucijomis ir tvirtina jų prašymus, bet apskritai teisminė kontrolė lieka gana silpna, todėl IPPT gali gauti techniškai neįgyvendinamus nurodymus;
- BDVIS turėtų naudotis ne tik visi IPPT, bet ir visos valstybinės institucijos, norinčios blokuoti interneto svetaines per IPPT DNS. Jeigu atsirastų išimčių, tada BDVIS naudojimas prarastų esmę. Kad tai būtų užtikrinta, reikalingi teisės aktų pakeitimai. Sudėtingiausia dalis – kad nėra vieno teisės akto, kuris reglamentuotų visą nusikaltimų elektroninėje užkardymo procesą, todėl reikės ieškoti geriausio būdo numatyti prievolę naudotis BDVIS ir sankcijas nesinaudojant BDVIS;
- Domėtasi, kiek yra reikalinga į BDVIS pridėti blokavimo sankciją pagrindžiančius dokumentus, jeigu pati valstybinė institucija turėtų prisiimti atsakomybę, kad nebūtų užblokuojama neteisėtai. Patikslinta, kad tam tikrų pagrindžiančių dokumentų (vėlesniame etape būtų tiksliai apibrėžtas jų turinys) reikia dėl trijų pagrindų, kuriais yra blokuojamo domenai: 1) teismo sprendimu skirta sankcija blokuoti; 2) ikiteisminio tyrimo metu esant pagrįstiems įtarimams ir aiškioms rizikoms policijos pareigūnų sprendimų blokuojama 48 val.; 3) blokuojamos veidrodinės svetainės pagal aiškius kriterijus, kurie buvo numatyti ankstesniame teismo priimtame sprendime. Taip pat jie būtų reikalingi kaip papildoma saugumo priemonė (plačiau žr. dalyje apie rizikų valdymą);
- Per klaidą užblokavus domeną, BDVIS turi užtikrinti galimybę atsekti, kur buvo padaryta klaida, t.y. ar valstybinė institucija padarė klaidą įvesdama informaciją apie domeną ar informacinės sistemos tvarkytojas neįgyvendinimo visų kibernetinio saugumo reikalavimų. Įvykus incidentui ir padarius žalą gyventojams/verslui, už tai turės atsakyti konkreti institucija;

Rizikų valdymas:

- Pagrindinės rizikos – per klaidą užblokuoti domenai, kibernetinės atakos, geopolitinis kontekstas. Kadangi siekiama automatizuoti procesą, tai įvykęs incidentas paveiktų visus IPPT ir jų klientus, o ne tik vieno IPPT, taigi sukuriama viena vieta viskas užblokuoti (angl. *single point of failure)*. Atsižvelgiant į tai, yra būtina labai atsakingai vertinti rizikas, tačiau tai nereiškia, kad nereikia ieškoti sprendimų;
- Išreikštas susirūpinimas, kad net ir teisiškai numačius atsakingas institucijas dėl įvykusios klaidos, verslas gali patirti žalą ir kitais būdais, pavyzdžiui, klientų aptarvavimo centrai bus užkrauti daugybės skambučių;
- Viena iš svarstytų rizikos valdymo priemonių – papildomas informacijos patikrinimas valstybinės įstaigos specialistui pateikus informaciją per BDVIS. Tai galėtų atlikti: a) specialisto tiesioginis vadovas prisijungęs prie sistemos; b) informacinės sistemos tvarkytojo paskirtas darbuotojas. Būtina įvertinti, kiek toks procesas reikalaus žmogiškųjų išteklių ir laiko sąnaudų. Tikslas – minimizuoti klaidos galimybę, tačiau kiek įmanoma išlaikant proceso greitį. Konkretus būdas turėtų būti pasirinktas įgyvendinimo proceso metu vertinant galutinį BDVIS veikimo modelį ir visumą taikomų rizikų valdymo priemonių;
- Vienas iš rizikos valdymo būdų galėtų būti palikta galimybė rankiniu būdu patikrinti blokuojamus domenus patiems IPPT, pavyzdžiui, prieš juos

perduodant į DNS. Tokia galimybė galėtų būti kaip alternatyva tiems, kurie nori turėti didesnę kontrolę ir užtikrinti paslaugos teikimą savo klientams, kita vertus, dėl to neturėtų ženkliai nukentėti blokavimo sankcijos vykdymo greitis;

Techniniai sprendimai:

- Visiškai automatinis blokuojamų domenų perkėlimas į IPPT DNS yra gana invazyvus (vertinant Europos šalių kontekste) ir keliantis daug rizikų verslui, dėl šios priežasties IPPT tikriausiai reikėtų statyti tarpinę infrastruktūrą, kad nebūtų tiesioginės interakcijos tarp BDVIS ir IPPT infrastruktūros. Atkreiptas dėmesys, kad šiuo metu yra svarstomos dvi blokuojamų domenų perdavimo alternatyvos (ateityje gali būti pasiūlyta ir daugiau). Vienas iš variantų suteiktų daugiau kontrolės patiems IPPT ir nesudarytų galimybės gauti blokuojamus domenus į IPPT DNS tiesiogiai, kitas pasiūlytas perdavimo modelis remtųsi tiesioginiu domenu perdavimu į IPPT DNS bei užtikrintų didesnį domenų užblokavimo ir atblokavimo greitį. Kibernetinio saugumo ekspertų vertinimu abu variantai nekeltų pavojaus IPPT DNS (jau yra išbandyti kitose Lietuvos institucijų sistemose). Galutinis sprendimas dėl tinkamiausio techninio mechanizmo turėtų būti priimtas jau žinant daugiau detalių įgyvendinimo etape ir išsamiai įvertinus visas rizikas. Tikėtina, kad IPPT, įvertinę rizikas ir reikalingus pakeitimus, galės patys pasirinkti vieną iš kelių siūlomų prisijungimo variantų;
- Jeigu būtų galima automatiškai generuoti ir pateikti bendrą visų blokuojamų domenų sąrašą IPPT dar pilnai neįgyvendinus BDVIS, tokiu būdu proceso efektyvumas ir kokybė ženkliai pagerėtų;
- Įgyvendinant BDVIS yra būtina atsižvelgti ir į technologijų tendencijas, pavyzdžiui, kiek plačiai bus naudojami atviri DNS vietoj IPPT DNS.

Po diskusijos dalyvių pateikti klausimai[2]:

- Kas bus atsakingas už visų teisės aktų pakeitimus (20 skaidrė)?
- Kas bus BDVIS tvarkytojas?
- Pagal ką bus tvirtinami/atmetami domeno blokavimo atvejai?
- Jeigu visas blokuojamų domenų sąrašas bus skelbiamas viešai, ar bus galimybė filtruoti, pavyzdžiui, nelegalias investicines paslaugas siūlantys ar nelegaliai lošimų veiklai naudojami interneto puslapiai ir t.t.?
- Kadangi BDVIS bus talpinami tik su teismo sprendimu blokuojami domenai, ar yra numatoma galimybė ateityje tobulinti procesą, t.y. blokuojanti institucija per BDVIS pateikia dokumentus teismui, o, teismui priėmus sprendimą ir tai patvirtinus per BDVIS, sistema automatiškai perduotų privalomą reikalavimą blokuoti IPPT?

Apibendrinimas:

- Valstybinių institucijų problemos yra labai panašios, pagrindinė jų – kontrolės užtikrinimas. IPPT įvardijo, kad didžiausiais iššūkis yra padrikas nurodymų pateikimas ir besiskiriančios prakikos tarp nurodymus siunčiančių institucijų;
- BDVIS susidėtų iš dviejų pagrindinių dalių: a) centralizavimo – IPPT galėtų iš vienos vietos pasiimti visą blokuojamų domenų sąrašą ir tai būtų naudinga

[2] Pateikti klausimai/pasiūlymai raštu po apskritojo stalo diskusijos bus svarstomi ir į juos bus atsižvelgta rengiant galutinius projekto produktus.

visiems proceso dalyviams; b) automatizavimo – kai sumažėjus rankinio darbo pagreitėja užblokavimo įgyvendinimas. Būtent automatizavimas kelia daugiausia rizikų, todėl turi būti sudarytos sąlygos kiekvienam IPPT įsivertinti rizikas ir tolesnių viešųjų konsultacijų metu pasirinkti tinkamiausius sąrašo perdavimo į IPPT DNS būdus;

- BDVIS naudojimas turi būti privalomas tiek valstybinėms institucijoms, tiek IPPT ir tai turi būti reglamentuota teisės aktuose. Taip pat labai svarbu numatyti teisinę atsakomybę dėl padarytos žalos gyventojams/verslui per klaidą ar incidentą užblokavus interneto svetainę. Atsakomybę turi prisiimti institucija padariusi klaidą;
- Įgyvendinant BDVIS būtina skirti ypatingą dėmesį rizikų valdymui: a) pradedant tuo, kad įstatymiškai gali būti sukuriama galimybė piktnaudžiauti ir blokuoti daugiau negu reikia interneto svetainių, b) bei skiriant ypatingą dėmesį minimizuojant klaidų, gedimų bei sėkmingų kibernetinių atakų tikimybę.

Rezultatų panaudojimas

Konsultacijos metu surinktos pastabos ir pasiūlymai bus panaudoti rengiant BDVIS modelį ir teikiant rekomendacijas dėl sistemos įgyvendinimo. Taip pat galutiniuose projekto produktuose bus bandoma atsakyti ir į konsultacijų metu iškeltus klausimus.

Programos „Kurk Lietuvai“ kartu su Krašto apsaugos ministerija įgyvendinamas projektas „Kenkėjiškų interneto svetainių grėsmių valdymo priemonių kūrimas“

2021