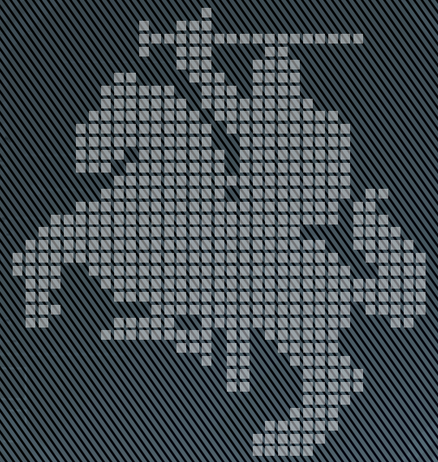
NACIONALINIO KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

2019

KRAŠTO APSAUGOS MINISTERIJA



Leidinio bibliografinė informacija pateikiama Lietuvos nacionalinės Martyno Mažvydo bibliotekos Nacionalinės bibliografijos duomenų banke (NBDB).

ISBN 978-609-412-192-0

Turinys

Dominančią temą galite pasiekti paspaudus ant jos pavadinimo

Sąvokos

Ypatingos svarbos informacinė infrastruktūra – ryšių ir informacinė sistema ar jos dalis, ryšių ir informacinių sistemų grupė, kurioje įvykęs kibernetinis incidentas gali padaryti didelį neigiamą poveikį nacionaliniam saugumui, valstybės ūkiui, valstybės ir visuomenės interesams.

Ypatingos svarbos paslauga – paslauga, kurios neteikimas ar teikimo sutrikimas padarytų didelį neigiamą poveikį nacionaliniam saugumui, šalies ūkiui, valstybės ar visuomenės interesams.

Kibernetinis incidentas – įvykis ar veika kibernetinėje erdvėje, galintys sukelti arba sukeliantys grėsmę arba neigiamą poveikį ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, galintys trikdyti arba trikdantys ryšių ir informacinių sistemų veikimą, valdymą ir paslaugų jomis teikimą.

Kibernetinio saugumo subjektas – subjektas, valdantis ir (arba) tvarkantis valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojas, viešųjų ryšių tinklų ir (arba) viešųjų elektroninių ryšių paslaugų, elektroninės informacijos prieglobos paslaugų ir skaitmeninių paslaugų teikėjas.

Ryšių ir informacinė sistema – elektroninių ryšių tinklas, informacinė sistema, registras, pramoninių procesų valdymo sistema ir jų valdymo, naudojimo, apsaugos ir priežiūros tikslais laikoma, tvarkoma, atkuriama arba perduodama elektroninė informacija.

Valstybės informaciniai ištekliai – informacijos, kurią valdo institucijos, atlikdamos teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma.

Sutrumpinimai

Botnet – užvaldytas kompiuterių ar daiktų interneto įrenginių tinklas, galintis vykdyti paskirstyto atsisakymo aptarnauti kibernetines atakas

ES – Europos Sąjunga

DDoS – paskirstyto atsisakymo aptarnauti kibernetinė ataka

IoT – (angl. *Internet of Things*) daiktų interneto įrenginiai, pavyzdžiui, išmanieji televizoriai, išmanieji telefonai ir pan.

IRT – informacinių ryšių technologijos

KAM – Lietuvos Respublikos krašto apsaugos ministerija

KVTC – Kertinis valstybės telekomunikacijų centras

YSII – ypatingos svarbos informacinė infrastruktūra

NKSC – Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos

OS – operacinė sistema

PĮ – programinė įranga

RIS – ryšių ir informacinė sistema

TLD – (angl. *top level domain*) aukščiausio lygmens domeno vardų sistema (pavyzdžiui, kuri baigiasi galūne „.lt“)

TS – tarnybinė stotis (serveris)

TVS – turinio valdymo sistema

VII – valstybės informaciniai ištekliai

VPN – (angl. *Virtual Private Network*) virtualus privatus tinklas

EDVINAS KERZA
KRAŠTO APSAUGOS VICEMINISTRAS

01
ĮŽANGA

Ketveri metai valstybės gyvenime nėra daug, bet nemažai, kai kalbame apie mūsų šalies kibernetinį saugumą, kai matuojame ir vertiname, kur buvome, kur esame ir planuojame būti. Pristatome ketvirtąją Nacionalinio kibernetinio saugumo būklės ataskaitą. Skaičiuojame jau antruosius metus, kai turime Nacionalinę kibernetinio saugumo strategiją su penkiais pagrindiniais tikslais. Kibernetinio saugumo srities pamatai padėti, svarbiausi sprendimai priimti ir jau galime kalbėti apie rezultatus. 2019-ieji buvo augimo metai. Stiprinti pajėgumus vertė ne tik naujos grėsmės, sudėtingesnės atakos ir naujesni jų vykdymo būdai, kartu augome kaip šalis, kuri jau yra pasirengusi pasirūpinti ne tik savo, bet ir prisidėti prie regiono kibernetinio saugumo. Įsteigėme Regioninį kibernetinio saugumo centrą, stiprinome partnerystę su Jungtinėmis Amerikos Valstijomis, kartu dirbsime, tirsime ir mokysimės su Ukraina ir Sakartvelu – esame patikimi partneriai.

2019-aisiais įgyvendinant Europos Sąjungos nuolatinio struktūrizuoto bendradarbiavimo (PESCO) Kibernetinės greitojo reagavimo grupės projektą pirmą kartą buvo užtikrintas greitojo reagavimo pajėgų budėjimas, sukurta tarptautinė komanda. Prisidedame prie NATO kibernetinės gynybos stiprinimo. Vienas iš svarbiausių sprendimų buvo sukurti Saugųjį valstybinį duomenų perdavimo tinklą. O tai reiškia didesnį šalies atsparumą ir saugumą. Priimtus sprendimus ir pasirinktus kelius pasitikrinome pratybose.

Galvojame ne tik apie kibernetinių incidentų suvaldymą, tačiau išplėtėme veiklą ir tyrimų srityje. Dalis tyrimų, tokie kaip „Yandex.Taxi“, „FaceApp“ mobiliųjų programėlių ir ryšio įrangos tyrimai, jau yra žinomi visuomenei, jų rezultatai pateikiami ir šioje ataskaitoje. Taip prisidedame ne tik prie Lietuvos žmonių saugumo didinimo, bet ir dalijamės informacija su kitų šalių partneriais. Kartu su „Kurk Lietuvai“ komanda pradėjome rengti kibernetinio saugumo vadovą smulkiajam ir vidutiniam verslui.

Ypač daug dėmesio buvo skirta naujoms hibridinėms grėsmėms, informacinėms atakoms, rinkimų saugumui užtikrinti. Čia prireikė sutelktų Lietuvos kariuomenės Strateginės komunikacijos departamento, Nacionalinio kibernetinio saugumo centro pastangų. Nors grėsmių pobūdis ir mastas 2019-aisiais augo, galima sakyti, kad kasdien stiprėjome ir mes. Ši ataskaita yra detalus šalies kibernetinio saugumo būklės paveikslas. Įvertinę jį galime sakyti, kad 2019-ieji buvo svarbių sprendimų, sustiprinusių kibernetinį saugumą, metai. Ataskaita taip pat siekiame parodyti, kad kibernetinės grėsmės aktualios ne tik valstybinėms institucijoms, verslui, tačiau ir kiekvienam Lietuvos gyventojui. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos ir toliau aktyviai plėtos savo veiklą, užtikrindamas ypatingos svarbos paslaugų saugumą, prisidėdamas prie piliečių sąmoningumo ugdymo ir saugesnės Lietuvos kūrimo, ir jei perskaitęs šią ataskaitą bent vienas žmogus susimąstys ir pasirūpins savo bei artimos aplinkos kibernetiniu saugumu – Lietuvos kibernetinė erdvė taps kur kas saugesnė.

Pagarbiai

Edvinas Kerza
Krašto apsaugos viceministras

02

SANTRAUKA

Santrauka

Lietuvoje ir pasaulyje kibernetinio saugumo aplinka 2019-aisiais išliko dinamiška. Kibernetiniai incidentai ir informacinės atakos buvo nuolatinės žiniasklaidos temos, o kibernetinio saugumo forumuose gausu specialistų įžvalgų apie kibernetinio saugumo grėsmes. Lietuva 2019 m. aktyviai įsitraukė ir į tarptautinį bendradarbiavimą užtikrinant kibernetinį saugumą – pradėti Regioninio kibernetinio saugumo centro, kaip operaciniame lygmenyje veikiančios tarptautinės kibernetinio saugumo bendradarbiavimo platformos, steigimo darbai. 2019 m. pasirašyti bendradarbiavimo susitarimai su Sakartvelu bei Ukraina, gauta Jungtinių Amerikos Valstijų finansinė parama vystomam naujos kartos sensorių projektui, tęsiamos diskusijos dėl tolesnės paramos plėtojant Regioninio kibernetinio saugumo centro infrastruktūrą. Lietuvos specialistai aktyviai dalyvavo kibernetinio saugumo pratybose. 2019 m. pabaigoje tarptautinėse pratybose „Cyber Shield 2019“ Nacionalinio kibernetinio saugumo centro specialistai užėmė antrąją vietą, o didžiausiose iki šiol Lietuvoje surengtose nacionalinėse pratybose „Kibernetinis skydas 2019“ dalyvavo daugiau nei 800 specialistų iš daugiau nei 100 viešojo ir privataus sektoriaus organizacijų. Atlikti nauji mobiliųjų aplikacijų ir iš rinkos paimtų tinklo maršrutizatorių kibernetinio saugumo tyrimai. Tyrimų rezultatai parodė, kad vartotojų asmens duomenys iš įrenginių ir programėlių iškeliauja į trečiąsias šalis, kur Europos Sąjungos Bendrasis duomenų apsaugos reglamentas negalioja, o programinė įranga gauna prieigą prie perteklinių, su jos funkcionalumu tiesiogiai nesusijusių, duomenų, paslaugų ir informacijos.

Buvo vykdomi prevenciniai veiksmai užtikrinant 2019 m. Lietuvoje vykusių rinkimų kibernetinį saugumą. Rinkimų metu buvo įsteigtas operacijų centras, o jo veiklos metu daugiausia kenkėjiškų IP adresų, kurie buvo blokuoti, fiksuota per Europos Parlamento rinkimus ir antrąjį Prezidento rinkimų turą – daugiau negu 900.

Didinami pajėgumai ir gerinama kibernetinio saugumo branda taip pat leido aiškiau identifikuoti kibernetines grėsmes. Lietuvoje 2019 m. registruotas 3 241 kibernetinis incidentas, kai jų tyrimams atlikti reikėjo tiesioginio specialistų dalyvavimo. Automatinėmis priemonėmis apdorotų kibernetinių įvykių skaičius Lietuvos IP rėžyje siekė daugiau kaip 300 000. Tokia klasifikacija, kai kibernetiniai įvykiai atskiriami nuo kibernetinių incidentų, įvesta siekiant suvienodinti klasifikavimą pagal suderintą Europos Sąjungos praktiką. Vertinant pagal incidentų tipus, pažymėtina, kad statistiškai sumažėjo paslaugų trikdymo incidentų ir techninėmis priemonėmis (sensoriais) aptinkamos kenkimo programinės įrangos skaičius ypatingos svarbos paslaugas teikiančių subjektų infrastruktūroje (sumažėjo 12 proc., palyginti su 2018 m.). Tačiau padidėjo krašto apsaugos sektoriuje aptiktos kenkimo programinės įrangos kiekis (49 proc.). Tuo tarpu energetikos sektoriuje matoma kenkimo programinės įrangos skaičiaus mažėjimo tendencija. 2019 m. taip pat registruotas ypatingas incidentas, kai duomenis šifruojantis kenkėjiškas kodas buvo užfiksuotas UAB „Kauno vandenys” informacinėse sistemose. Dėl to kilo rizika, kad bus paveikta technologiniu tinklu teikiama vandens tiekimo paslauga Kauno mieste. Kibernetinis incidentas buvo suvaldytas, tačiau ši situacija kelia nerimą dėl to, kad technologinius tinklus valdantys subjektai Lietuvoje yra kibernetinių incidentų taikiniai. Detalizuotas kibernetinių incidentų klasifikavimas, Lietuvos IP kibernetinių įvykių informacija ir kenkimo PĮ kibernetinių incidentų tendencijos leidžia konstatuoti – Lietuvoje kibernetinių incidentų poveikis vis dar yra nepakankamai įvertinamas.

Atgal į turinį

Opi kibernetinio saugumo problema yra interneto svetainių pažeidžiamumai. Interneto skenavimų metu iš 118 000 aukščiausiojo „.lt“ domeno interneto svetainių su turinio valdymo sistemomis identifikuota 56 400. Tyrimų duomenimis, 62 proc. iš jų naudoja neatnaujintą turinio valdymo sistemos programinę įrangą, kuri nėra saugi dėl publikuotų pažeidžiamumų. Be to, 37 proc. visų interneto svetainių turi atvirą prieigą prie svetainės valdymo skydo, todėl piktavaliai gali bandyti į jas įsilaužti, automatinėmis priemonėmis generuodami prisijungimo vardus bei slaptažodžius. Pozityvi tendencija viešajame sektoriuje – saugių interneto svetainių skaičius išaugo 11 proc. Tačiau dalis interneto svetainių vis dar nėra įteisintos kaip informacinės sistemos, nepaskirti saugos įgaliotiniai, o svetainių administratoriai neskiria pakankamai dėmesio kibernetinio saugumo klausimams. Statistiškai viešajame sektoriuje išlieka labiausiai pažeidžiamos savivaldybių institucijų, ministerijų ir joms pavaldžių įstaigų interneto svetainės. Apibendrinant galima teigti, kad viešajame sektoriuje interneto svetainių kibernetinio saugumo būklė gerėja, tačiau bendrąja prasme svetainių kibernetinio saugumo rizikos išlieka reikšmingos. Bendrai svetainių saugumo problematikai spręsti Nacionalinis kibernetinio saugumo centras 2019 m. publikavo nemokamą interneto svetainių pažeidžiamumų nustatymo įrankį, kuriuo praėjusiais metais sėkmingai pasinaudojo apie 120 subjektų.

2019 m. buvo užfiksuota reikšminga pažanga kibernetinio saugumo reikalavimų įgyvendinime – ypatingos svarbos informacinės infrastruktūros valdytojai įgyvendino 80 proc. nustatytų reikalavimų. Žengta toliau, įsibrovimų simuliavimo (angl. *penetration testing*) ir procesų auditavimo principais pradėti faktinių reikalavimų įgyvendinimo patikrinimai. Tokia praktika leido identifikuoti techninius trūkumus, o jų pašalinimo veiksmai buvo suderinti atsižvelgiant į nustatytas rizikas. Iš administravimo pusės nustatyta, kad subjektai yra linkę formaliai įgyvendinti reikalavimus, neskiriant pakankamai dėmesio praktiniams kibernetinio saugumo klausimų sprendimams. Valstybiniame sektoriuje ir toliau susiduriama su reikalavimų įgyvendinimo problemomis (2019 m. deklaruojamas įgyvendinimas šiame sektoriuje siekė apie 22 proc). Šį klausimą iš dalies turėtų išspręsti centralizuotas kibernetinio saugumo skėtis – Kertinio valstybės telekomunikacijų centro suteikiama saugi infrastruktūra daugiau nei 400 viešojo sektoriaus organizacijų.

2019 m. daugėjo hibridinių incidentų, susidedančių iš kibernetinės ir informacinės dalių, kurių tikslas – įsilaužimai, kenkimo programinės įrangos platinimas ir melagingos informacijos (angl. *fake news*) skleidimas. Lietuvos kariuomenės Strateginės komunikacijos departamento duomenimis, 2019 m. iš viso nustatyta 2 890 Lietuvai nedraugiškos informacinės veiklos atvejų, ketvirtis iš jų – konstitucinių pagrindų apsaugos srityje. Pabrėžtina, kad tokių žalingos veiklos atvejų skaičius pernai padidėjo 15 procentų. Lietuvos valstybingumas, nepriklausomybė ir demokratijos institutai pastaruosius keletą metų yra tapę vienais svarbiausių šaliai nedraugiškos žiniasklaidos taikinių.

03

KIBERNETINIO SAUGUMO ATSPARUMO DIDINIMAS

Kibernetinio saugumo aplinkos kūrimas

Po 2018 m. įvykusių reikšmingų organizacinių pokyčių ir teisės aktų pakeitimų 2019 m. kibernetinis saugumas Lietuvoje buvo stiprinamas ir plėtojamas toliau, įgyvendinant Kibernetinio saugumo įstatymą, teisės aktus bei vykdant įvairias iniciatyvas kibernetinio saugumo srityje. Formuodama kibernetinio saugumo politiką, KAM parengė keletą svarbių kibernetinio saugumo srities teisės aktų, kurių įgyvendinimas sustiprins kibernetinio saugumo sistemą ir padės apsisaugoti nuo kibernetinių grėsmių atsiradimo.

KAM, siekdama užtikrinti Nacionalinėje kibernetinio saugumo strategijoje, patvirtintoje Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" (toliau – Strategija), iškeltų tikslų ir uždavinių kibernetinio saugumo srityje įgyvendinimą, 2019 m. parengė Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstitucinį veiklos planą (toliau – Planas) 3 metams. Numatytos priemonės Strategijos tikslams ir uždaviniams įgyvendinti, nurodyti jiems skiriami asignavimai bei numatyti vertinimo rodikliai, matuojantys Strategijos tikslų, uždavinių pasiekimą ir priemonių įvykdymą atitinkamu laikotarpiu. Nors daugumą numatytų priemonių vykdo Plano koordinatorius – KAM ir jai pavaldūs padaliniai, tačiau prie Strategijos tikslų pasiekimo pagal savo kompetenciją prisideda ir kitos valstybės institucijos, įstaigos, ministerijos ir joms pavaldžios įstaigos. Tikimasi, kad Plane dalyvaujančių valstybės institucijų suinteresuotumas ir pastangos įgyvendinant numatytas priemones, pakankamas joms reikalingų lėšų skyrimas, aiškios Plano koordinatoriaus funkcijos, nuolatinė Plano priemonių įgyvendinimo ir vertinimo rodiklių reikšmių pasiekimo stebėsena bei geranoriška ir bendradarbiavimą skatinanti komunikacija leis sklandžiai įgyvendinti Strategijos tikslus.

2019 m. buvo priimti Valstybės informacinių išteklių valdymo įstatymui įgyvendinti reikalingi teisės aktai, kuriais sudarytos sąlygos veikti Saugiajam valstybiniam duomenų perdavimo tinklui (toliau – Saugusis tinklas), kad juo tinklo naudotojams būtų teikiamos saugios elektroninių ryšių paslaugos, nustatyti techniniai reikalavimai, kurių turi būti laikomasi įrengiant ir eksploatuojant valstybinius duomenų centrus.

Vadovaujantis Valstybinių duomenų centrų techniniais reikalavimais, 2019 m. lapkričio 18 d. patvirtintais krašto apsaugos ministro įsakymu, 2020 m. bus sudarytas ir patvirtintas patalpų, laikomų valstybiniais duomenų centrais, sąrašas.

Siekiant užtikrinti Saugiojo tinklo tvarkymą, nuo 2019 m. liepos 1 d. valstybės įmonė „Infostruktūra" buvo pertvarkyta į biudžetinę įstaigą KVTC, kuris užtikrina priskirtos naujos ir gyvybiškai svarbios valstybės funkcijos vykdymą. Saugusis tinklas yra nepriklausomas nuo viešųjų ryšių tinklų ir gali veikti krizės ar karo sąlygomis. Institucijos, įrašytos į Saugiojo tinklo naudotojų sąrašą, privalo naudotis tik Saugiuoju tinklu teikiamomis elektroninių ryšių paslaugomis ir jungtis prie viešųjų elektroninių ryšių tinklų tik per jį.

Šiuo metu į Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą, kuris yra skelbiamas viešai, yra įrašytos 463 valstybės ir savivaldybių institucijos ir įstaigos, valstybės įmonės ir viešosios įstaigos, atitinkančios bent vieną iš Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 432 straipsnio 2 dalyje nurodytų kriterijų.

KAM yra atsakinga už Lietuvos Respublikos Vyriausybės nutarimo Dėl ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašo tvirtinimo projekto rengimą ir periodinį jo atnaujinimą. 2019 m. organizuotų konsultacijų metu dalyviams, atsakingiems už ypatingos svarbos informacinės infrastruktūros identifikavimą savo atstovaujamose valstybės institucijose ir įstaigose, pristatyti nuo 2019 m. pradžios įsigalioję Ypatingos svarbos informacinės infrastruktūros identifikavimo metodikos (toliau – Metodika) pagrindiniai pakeitimai. 2019 m. pagal atnaujintos Metodikos reikalavimus buvo renkama ir analizuojama informacija, bendradarbiaujama su atsakingomis institucijomis, siekiant atnaujinti ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą.

KAM 2019 m. tęsė iniciatyvas kibernetinio saugumo srityje, kurių tikslas buvo sustiprinti viešojo ir privataus sektorių bendradarbiavimą, plėtoti ir intensyvinti tarptautinį bendradarbiavimą, įgyvendinti ES rekomendacijas.

Siekiant stiprinti viešojo ir privataus sektorių bendradarbiavimą kibernetinio saugumo srityje Lietuvoje ir sudaryti galimybę IRT saugumo spragą suradusiam ir norinčiam ją ištaisyti asmeniui bendradarbiauti su kibernetinio saugumo subjektais, kurių IRT saugumo spraga buvo atskleista, 2019 m. buvo atlikta atsakingos viešojo ir privataus sektorių IRT saugumo spragų atskleidimo praktikos analizė ir pateikti siūlymai dėl reikalingų teisės aktų pakeitimų 2020 m.

Didinant Lietuvos matomumą tarptautinėje erdvėje, siekiant sudaryti platesnes tarptautinio bendradarbiavimo galimybes kibernetinio saugumo srityje, 2019 m. krašto apsaugos sistemos darbuotojai aktyviai dalyvavo įvairioje tarptautinių organizacijų, jų sudarytų darbo grupių veikloje, buvo intensyviai plėtojamas dvišalis bendradarbiavimas su Sakartvelo bei Ukrainos kompetentingomis kibernetinio saugumo srityje institucijomis, toliau stiprinamas glaudus bendradarbiavimas su JAV. 2019 m. pradėti Regioninio kibernetinio saugumo centro, kaip tarptautinio bendradarbiavimo kibernetinio saugumo srityje operaciniu lygmeniu platformos, steigimo darbai. 2019 m. pasirašyti bendradarbiavimo susitarimai su Sakartvelu bei Ukraina, gauta JAV finansinė parama NKSC vykdomam naujos kartos sensorių projektui, tęsiamos diskusijos dėl tolesnės JAV paramos plėtojant Regioninio kibernetinio saugumo centro infrastruktūrą bei su minėtomis šalimis pradėti derinti pasiūlymai dėl Regioninio kibernetinio saugumo centro veiklos prioritetų 2020-2021 metais. Planuojama, kad Regioninio kibernetinio saugumo centre 2021 m. bus vykdomi bendri tyrimai, kibernetinio saugumo pratybos, kartu dirbama ir keičiamasi informacija apie naujausias kibernetines grėsmes.

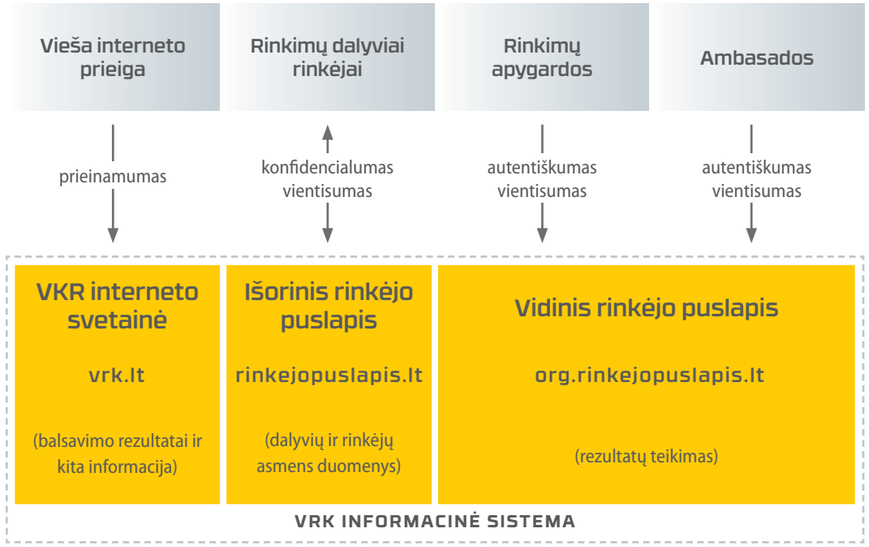
KAM 2019 m. toliau sėkmingai vykdė ir vadovavo ES nuolatinio struktūrizuoto bendradarbiavimo (angl. PESCO) projektui „Kibernetinės greitojo reagavimo grupės ir savitarpio pagalba kibernetinio saugumo srityje“ (toliau – Projektas). Vieni svarbiausių atliktų darbų 2019 m. – baigtas parengiamasis Projekto susitarimo memorandumo pasirašymo 2020 m. etapas, parengtos Projekto valdymo taisyklės, metodologija, kibernetinio saugumo pratybų „Gintarinė migla 2019“ metu toliau kuriamos kibernetinių greitojo reagavimo grupių veikimo procedūros, vykdomos veiklos, finansuojamos pagal Europos infrastruktūros tinklų priemonės (angl. CEF *Telecom*) dotacijos susitarimą, bei koordinuojami dalyvaujančių šalių narių ir privataus sektoriaus atstovų veiksmai siekiant gauti finansavimą iš Europos gynybos fondo.

KAM, įgyvendindama Europos Komisijos 2019 m. kovo 26 d. rekomendaciją dėl praktinių veiksmų ir priemonių, kuriomis siekiama visoje ES užtikrinti aukštą 5G tinklų kibernetinio saugumo lygį, rinkinio, 2019 m. birželio 26 d. parengė nacionalinę 5G ryšio tinklų infrastruktūros ir su ja susijusios rizikos vertinimo ataskaitą. Ataskaitoje nurodytos pagrindinės grėsmės ir jų šaltiniai, grėsmėms jautriausi subjektai, strateginės grėsmės rizikos ir galimi pažeidžiamumai. 2019 m. liepos 15 d. šią vertinimo ataskaitą patvirtino Lietuvos Respublikos Vyriausybės nacionalinio saugumo komisija. KAM 2019 m. liepos 17 d. perdavė nacionalinę 5G ryšio tinklų infrastruktūros ir su ja susijusios rizikos vertinimo ataskaitą Europos Komisijai ir ES kibernetinio saugumo agentūrai (ENISA). Padedant Europos Komisijai ir kartu su ENISA Lietuva atliko skaitmeninės ekosistemos bei 5G ryšio technologijų rizikos vertinimą. 2019 m. spalio 9 d. ES šalys kartu su Europos Komisija ir ENISA paskelbė bendrą ES rizikos, naudojant 5G tinklus, ataskaitą. Ji parengta remiantis visų ES šalių narių nacionaliniais kibernetinio saugumo rizikų vertinimais. Bendradarbiaudama su Europos Komisija Lietuva turės iki 2020 m. spalio 1 d. įvertinti ES rekomendacijų poveikį, kad būtų galima nustatyti, ar reikia imtis tolesnių veiksmų.

Plėtojant valstybės kibernetinės gynybos pajėgumus, 2019 m. pradėti veiksmai, siekiant numatyti resursus, reikalingus valstybės kibernetinės gynybos pajėgumams plėtoti, pradėti rengti dokumentai, siekiant nustatyti krašto apsaugos sistemos valstybės institucijų atsakomybę ir funkcijas valstybės kibernetinės gynybos pajėgumų plėtros srityje. Siekiant užtikrinti Lietuvos kariuomenės sąveiką su valstybės civiliniais pajėgumais, 2019 m. dalis LK karinio personalo integruota į Nacionalinį kibernetinio saugumo centrą, siekiant kartu su NKSC personalu keistis savo žiniomis ir patirtimi užtikrinant KAS valdomų informacinių sistemų kibernetinį saugumą taikos ir karo metu.

Atsparumo kibernetinėms grėsmėms didinimas

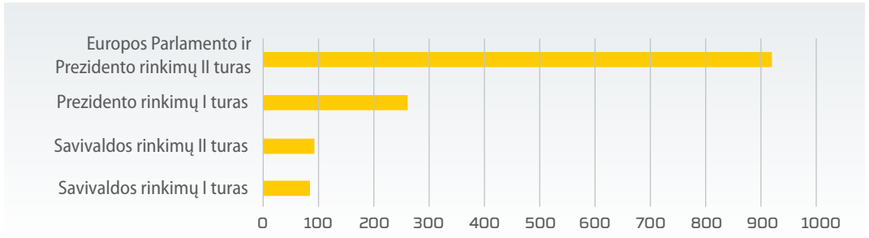
Siekdamas užtikrinti 2019 m. vykusių savivaldos, Lietuvos Respublikos Prezidento ir Europos Parlamento rinkimų kibernetinį saugumą, NKSC aktyviai įsitraukė ir bendradarbiavo su Lietuvos Respublikos Vyriausiąja rinkimų komisija bei jos valdomos informacinės sistemos (toliau – VRKIS) prieglobos bei priežiūros paslaugas teikiančiais rangovais bei subrangovais, identifikuojant kibernetines rizikas ir diegiant proporcingas jų valdymo priemones. Proaktyviam reagavimui į kibernetinius incidentus rinkimų kontekste NKSC įkūrė specialų operacijų centrą ir užmezgė aktyvų ryšį su kitų šalių organizacijomis, siekdamas užtikrinti tarptautinį reagavimą į potencialius kibernetinius incidentus. Operacijų centro veikla rėmėsi NKSC identifikuotomis rizikomis, kurios apėmė VRKIS kibernetinių rizikų valdymą informacijos konfidencialumo, autentiškumo, vientisumo ir prieinamumo kontekste (1 pav.).



1 pav. Supaprastintas VRKIS rizikos valdymo prioritetų modelis.

Papildomai NKSC rinkimų periodu nuolat stebėjo rinkimų dalyvių interneto svetainių prieinamumą ir turinio vientisumą. Operacijų centro veiklos metu NKSC specialistai blokavo IP adresus, vykdančius įtartiną veiklą, – daugiausia IP buvo užblokuota Europos Parlamento ir Prezidento rinkimų metu – daugiau negu 900 IP adresų (2 pav.).

Atgal į turinį



2 pav. Blokuoti IP adresai 2019 m. vykusių rinkimų metu.

NKSC, įvertinęs, kad rinkimų komisijų narių darbo stotys nėra centralizuotai valdomos ir prižiūrimos, nustatė, kad dėl šios priežasties gali būti paveiktas rinkimų rezultatų vientisumas arba sutrikdyta galimybė laiku perduoti rinkimų rezultatus. Dėl šios priežasties NKSC Inovacijų ir mokymų skyriaus specialistai paruošė specialiai rinkimams skirtą operacinę sistemą „KAMOS-VRKS“. Šios operacinės sistemos veikimo modelis – iš kompaktinio disko paleidžiama OS su įdiegtomis būtiniausiomis tvarkyklėmis ir PĮ. Papildomai NKSC vykdė švietėjišką veiklą – vedė mokymus rinkimuose dirbantiems darbuotojams bei partijų atstovams.

Siekiant stiprinti kibernetinės gynybos pajėgumus, 2019 m. buvo aktyviai dalyvaujama tarptautinėse kibernetinio saugumo pratybose. Vienos didžiausių – tarptautinės pratybos „Locked Shields 2019“, kuriose pagrindinis dėmesys buvo skiriamas ekspertų ir sprendimų priėmėjų bendradarbiavimui, kai techninis lygmuo integruotas į strateginį. „Blue OLEx 2019“ pratybose pagrindinis dėmesys skirtas ES institucijų ir valstybių narių bendradarbiavimui operaciniu lygmeniu valdant kibernetinio saugumo krizes. Lietuvos kariuomenės organizuotų tarptautinių kibernetinio saugumo pratybų „Gintarinė migla 2019“ tikslas – gynybinių kibernetinių operacijų vykdymas: priešiškų veiksmų kibernetinėje erdvėje vertinimas, kibernetinių grėsmių identifikavimas, potencialių kibernetinių atakų prevencija ir poveikio nukenksminimas. Šiose pratybose dalyvavo viešojo ir privataus sektorių organizacijos, Lietuvos kariuomenės, NATO sąjungininkai ir partneriai, Lietuvos inicijuoto ES Nuolatinio struktūrizuoto bendradarbiavimo (PESCO) projekto vystoma Kibernetinių greitojo reagavimo pajėgų komanda, rotaciją pradedanti 2020 m. sausio 1 d., o jai vadovauja Lietuva. Metų pabaigoje vykusiose tarptautinėse pratybose „Cyber Shield 2019“ buvo siekiama stiprinti šalių bendradarbiavimą ir reagavimą į dažniausiai pasitaikančius kibernetinius incidentus ypatingos svarbos informacinėse infrastruktūrose, šalies institucijose, organizacijose – NKSC specialistai šiose pratybose užėmė antrąją vietą.[1]

Metų pabaigoje didžiausiose iki šiol Lietuvoje surengtose nacionalinėse pratybose „Kibernetinis skydas 2019“ dalyvavo daugiau nei 800 specialistų iš daugiau nei 100 viešojo ir privataus sektoriaus organizacijų. Pratybos buvo paremtos NATO kibernetinės gynybos pratybų „Kibernetinė koalicija“ modeliu, t. y. kibernetinio saugumo subjektai realiomis sąlygomis – su turimais techniniais pajėgumais, personalu, procedūromis – savo organizacijose valdė kibernetinius incidentus, realiai išbandė vidinius kibernetinių incidentų valdymo planus, personalo gebėjimą aptikti, suvaldyti ir analizuoti kibernetinius incidentus. Net 90 proc. dalyvių teigė, jog pratybos jiems buvo naudingos, jos sudarė sąlygas pasitikrinti savo vidines procedūras, o patys dalyviai įgijo naujų žinių apie kibernetines grėsmes. NKSC planuoja pagal šį modelį ir toliau plėtoti pratybų koncepciją, kviesti vis įvairesnes organizacijas bei diversifikuoti pratybų scenarijus pagal sektorius.

[1] https://www.nksc.lt/naujienos/lietuviai_lipo_ant_pakilos_tarptautinesecyber_shie.html

3 pav. Kibernetinio saugumo pratybų „Gintarinė migla" akimirka. KAM nuotrauka.

NKSC 2019 m. sėkmingai įgyvendino Europos infrastruktūros tinklų priemonės (EITP) lėšomis iš dalies finansuojamą telekomunikacijų sektoriaus projektą „Įrankiai ir gebėjimų stiprinimas kibernetinės erdvės stebėsenai, analizei ir grėsmių aptikimui Lietuvoje ir ES gerinti". Projekto tikslas – stiprinti NKSC pajėgumus efektyviai koordinuoti ir valdyti kibernetinius incidentus, grėsmes, didinti darbuotojų kompetencijas, užtikrinti glaudesnį tarptautinį ir nacionalinį bendradarbiavimą, apsikeitimą informacija apie grėsmes.

Už projekto lėšas buvo atnaujinta NKSC naudojama incidentų valdymo infrastruktūra, įgyti nauji įrankiai grėsmėms aptikti, analizuoti ir dalintis informacija su partneriais. Dalį projekto sudarė aukšto lygio tarptautiniai kvalifikacijos kėlimo mokymai NKSC specialistams. Projekto veiklos padidino Lietuvos pasirengimo kibernetiniams incidentams lygį, inicijavo naujų saugumo priemonių atsiradimą, leido teikti platesnes ir veiksmingesnes kibernetinio saugumo paslaugas nacionaliniu lygmeniu bei suteikė galimybę dalyvauti bendrose europinėse bendradarbiavimo programose ir informacijos mainų platformose.

Projekto metu pagal NKSC praktinę patirtį (angl. *know-how*) buvo sukurta platforma, skirta viešųjų interneto tinklų infrastruktūrai vizualizuoti, infrastruktūros elementų pasiekimo stebėsenai ir grėsmėms aptikti. Platforma pagrįsta iš viešųjų šaltinių surinktais duomenimis, naudojant maršrutizavimo (BGP) ir kitus susijusius tinklo protokolus. Sistema pagal Lietuvos modelį pritaikyta kitoms šalims ir visiems ES nacionaliniams CERT padaliniams prieinama nemokamai, o joje saugumo specialistai gali stebėti savo viešai prieinamo nacionalinio tinklo topologiją ir susijusius saugumo įvykius.

Projekto metu buvo įgyta įranga, skirta saugumo vertinimo tikslams ir kenkimo kodo analizei. Specializuota kenkėjiško kodo analizavimo sistema vertina tiek bylas, tiek interneto svetaines, aptinka įvairių tipų atakas, geba analizuoti kenkėjiško kodo sukuriamą tinklo srautą, kodo analizės metu parsiųstas ar

Atgal į turinį

sukurtas bylas. Naudojant šį įrankį vykdoma nuolatinė visos Lietuvos tinklalapių (registruotų „.lt" zonoje) patikra, o apie rastus pažeidimus ir kenkėjišką veiklą informuojami šių svetainių prieglobos paslaugų teikėjai. Kiekvieną mėnesį įrankis išanalizuoja per 100 000 Lietuvos svetainių.

Plačiai visame pasaulyje kibernetinio saugumo komandų naudojama incidentų valdymo platforma – dar viena projekto metu įgyta sistema, kuri palengvino standartinių incidentų apdorojimo procesus, sutrumpino jų apdorojimo laiką ir labai padidino incidentų valdymo efektyvumą. Todėl NKSC specialistai gali daugiau laiko skirti prevenciniam darbui, išsamiems reikšmingų incidentų tyrimams ir naujų grėsmių aptikimui.

Nauja paslauga Lietuvos gyventojams, išvystyta projekto metu, – įrankis, skirtas vertinti interneto svetainių saugumą. Sistema yra viešai prieinama, vartotojai gali patys pasitikrinti savo svetainę dėl žinomų pažeidžiamumų.[2] Po atlikto saugumo audito svetainės valdytojas gauna ataskaitą apie konkrečias problemas ir rekomendacijas, kaip pagerinti savo svetainės saugumo būklę.

Dar viena naujiena – centrinė stebėjimo aplinka. Tai techninis sprendimas (vaizdo siena), leidžiantis realiu laiku stebėti NKSC valdomų ir prižiūrimų sistemų duomenis vienoje vietoje. Sistema naudojama kasdieniame analitikų darbe, o ypač buvo naudinga pastaraisiais metais vykusių rinkimų metu, kai vienoje vietoje reikėjo stebėti grėsmių indikatorius, siunčiamus iš daugybės skirtingų sistemų.

Europos Sąjungos finansavimas taip pat leido įsigyti aukšto lygio kompetencijos kėlimo paslaugas NKSC darbuotojams. Visame pasaulyje saugumo ekspertų vertinamuose mokymuose darbuotojai turėjo galimybę gilinti skirtingų kibernetinio saugumo sričių žinias ir įgūdžius. Tai leido praplėsti jų kompetencijas ir gebėjimus bei sudaryti sąlygas kompetentingesniam ir gilesniam kibernetinių saugumo incidentų tyrimui, užtikrinti aukštesnio lygmens pasirengimą ir padidinti kibernetinio saugumo atsparumą nacionaliniu lygmeniu.

[2] https://site-check.cert.lt/

04

DIDŽIAUSI 2019 M. KIBERNETINIO SAUGUMO IŠŠŪKIAI

Kibernetinių incidentų statistika

- NKSC 2019 m. užfiksavo 3 241 kibernetinį incidentą – triskart daugiau nei ankstesniu laikotarpiu.
- Kibernetiniai įvykiai Lietuvos IP rėžyje daugiausiai susiję su ryšių ir informacinių sistemų kibernetinėmis grėsmėmis ir kenkimo PĮ (5 pav.).
- Naudotojai ir subjektai vis dar negeba įvertinti ar nevertina realaus kibernetinių incidentų poveikio.

Atsižvelgdamas į Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ pakeistą kibernetinių incidentų kriterijų sąrašą, taip pat siekdamas suvienodinti kibernetinių incidentų klasifikavimą pagal ES kibernetinio saugumo agentūros bei kitų šalių kibernetinių incidentų valdymo komandų taksonomiją, NKSC pakeitė ir suvienodino su bendra ES praktika kibernetinių incidentų skaičiavimo metodiką. Pagal Kibernetinio saugumo įstatymą kibernetiniu incidentu laikoma įvykis ar veika, galintys sukelti ar sukeliantys neigiamą poveikį ryšių ir informacinėms sistemoms ar perduodamai informacijai. Iki 2019 m. pradžios kibernetiniai incidentai buvo skaičiuojami atsižvelgiant į automatinėmis priemonėmis apdorotų ir išsiųstų pranešimų bei specialistų betarpiškai (rankiniu būdu) apdorotų kibernetinių incidentų skaičių. Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame 2018-08-13 Lietuvos Respublikos Vyriausybės nutarimu Nr. 818, incidentai klasifikuojami ne tik pagal jų požymius, tačiau ir pagal poveikį. Dėl šios priežasties NKSC, atsižvelgdamas į būtinybę incidentus klasifikuoti pagal poveikį, nuo 2019 m. kibernetiniais incidentais traktuoja atvejus, kada specialistai įvykius apdoroja betarpiškai – priskiria poveikio reikšmę bei nustato incidento kategoriją (4 pav.). Nuo šiol atskiriami automatinėmis priemonėmis ir programomis apdoroti procesai, kurie traktuojami kaip kibernetiniai įvykiai.

4 pav. Kibernetinio incidento nustatymo procesas.

Pagal atnaujintą kibernetinių incidentų klasifikavimą NKSC 2019 m. užfiksavo 3 241 kibernetinį incidentą. Tuo tarpu Valstybinės duomenų apsaugos inspekcijos duomenimis 2019 m. buvo užfiksuoti tik 34 kibernetiniai incidentai, susiję su asmens duomenų apsaugos pažeidimais. Įvertinus Policijos departamento prie Vidaus reikalų ministerijos informaciją apie nusikaltimų elektroninėje erdvėje tyrimus taip pat matyti – subjektai ne visada yra linkę kreiptis dėl nusikalstamos veikos ir poveikio identifikavimo. 2019 m., Informatikos ir ryšių departamento prie Vidaus reikalų ministerijos duomenimis, buvo užregistruotos tik 439 su elektronine erdve susijusios nusikalstamos veikos.[3] Dėl šios priežasties galima daryti prielaidą, kad Lietuvoje daugiausiai dėmesio skiriama prevenciniam kibernetinių incidentų užkardymui, o iš teisinės pusės bausmės už piktavališkos veiklos vykdymą yra sunkiai realizuojamos.

Kita automatiniu būdu apdorota ir interneto paslaugų bei prieglobos paslaugų teikėjams perduota iš trečiųjų šalių gauta informacija, kuriai pagal poveikį nebuvo priskiriama incidento kategorija, buvo traktuojama kaip kibernetiniai įvykiai. Ši informacija daugiausia susijusi su atskirų fizinių bei juridinių asmenų lietuviškais IP adresais, kurie, įtariama, buvo panaudoti kenkėjiškoje veikloje (5 pav.).[4]

Tipas	Kiekis
Ryšių ir informacinių sistemų kibernetinės grėsmės	199 828
Kenkimo PĮ	68 562
Informacijos rinkimas	37 363
Bandymai įsibrauti	2 987
RIS trikdymas (DoS)	355

5 pav. Kibernetiniai įvykiai, susiję su Lietuvos IP adresais.

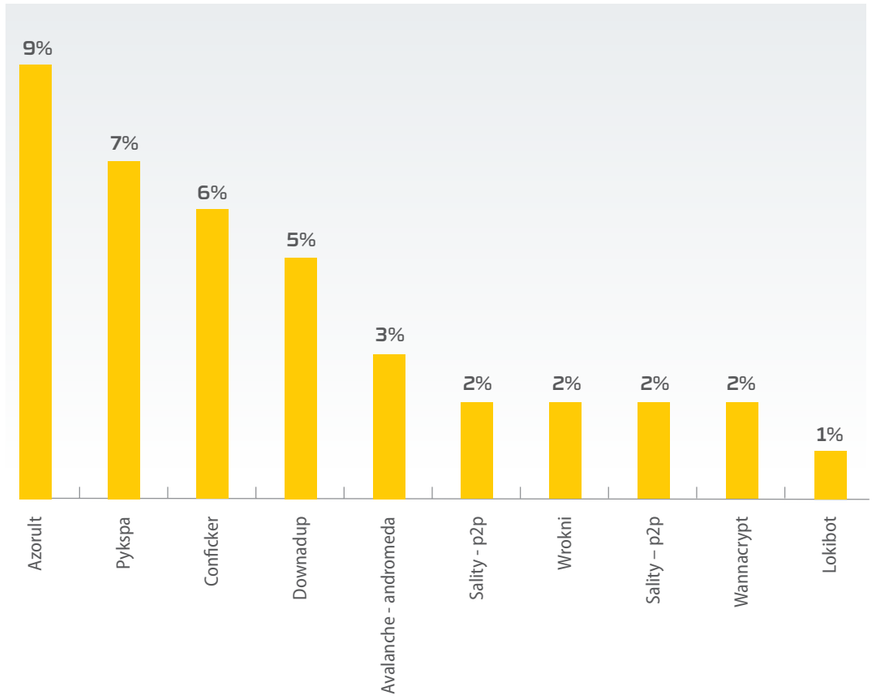
[3] https://www.ird.lt/lt/paslaugos/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-zinybinio-registro-nvzr-atviri-duomenys-paslaugos/ataskaitos-1/nusikalstamumo-ir-ikiteisminiu-tyrimu-statistika-1/view_item_datasource?id=8166&datasource=40853

[4] Pasitikrinti, ar IP naudojamas kenkėjiškoje veikloje, galima – https://www.nksc.lt/irankiai.html

Atgal į turinį

Vertinant kibernetinių įvykių informaciją, tarp dešimties populiariausių kenkimo PĮ pavyzdžių, aptiktų lietuviškuose IP, labiausiai paplitusios buvo *Azorult, Pykspa, Conficker* (6 pav.). Ši kenkimo PĮ susijusi su naudotojų darbo stočių užvaldymu, informacijos vogimu. Pavyzdžiui, *Azorult* žinoma dėl prisijungimo duomenų bei mokėjimo kortelių duomenų pasisavinimo.[5]

6 pav. Dešimt labiausiai plitusios kenkimo PĮ, susijusios su lietuviškais IP adresais.



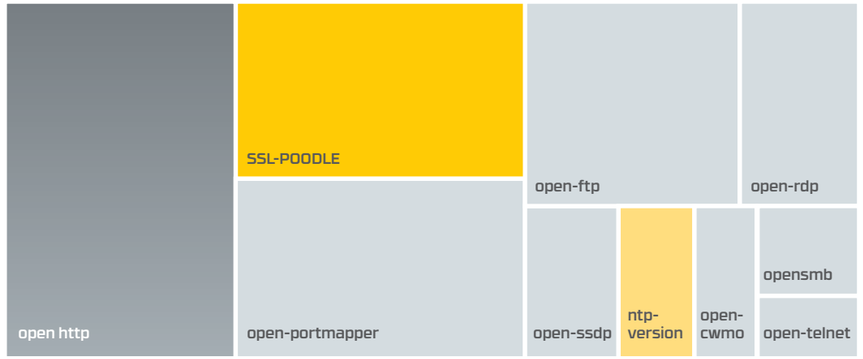
NKSC atkreipia dėmesį, kad dauguma antivirusinių programų, tarp jų ir nemokamų, geba lengvai aptikti labiausiai paplitusią kenkimo PĮ. NKSC taip pat periodiškai teikia rekomendacijas apie papildomus apsisaugojimo būdus bei priemones.[6]

Įvertinus iš trečiųjų šalių surinktą informaciją apie RIS grėsmes Lietuvos IP rėžyje, paaiškėjo, kad labiausiai paplitusios – atviri pertekliniai prievadai. Pavyzdžiui, atviru *http* prievadu vykdomą autentifikavimą galima nuskaityti ir tokiu būdu perimti prisijungimo duomenis. NKSC partnerių pateikta informacija taip pat leidžia pažymėti, kad Lietuvoje ypač paplitusi grėsmė – neatnaujintų interneto svetainės tapatumo nustatymo sertifikatų naudojimas. Tokios RIS grėsmės sukuria piktavaliams galimybes vykdyti *man-in-the-middle* kibernetines atakas, įsiterpiant į naudotojų ir internetu prieinamų RIS sesijas.

[5] https://success.trendmicro.com/solution/000146108-AZORULT-Malware-Information

[6] https://www.nksc.lt/rekomendacijos.html

Lietuvoje ir pasaulyje ypač populiarėjant IoT, išryškėja nuotoliniu būdu valdomų įrenginių rizikos. Tokie įrenginiai dažnai taip pat turi nešifruotos nuotolinės prieigos galimybes, kurias piktavaliai gali surasti be didesnių pastangų pasinaudodami laisvai prieinamais įrankiais.[7] Šios rizikos netiesiogiai taip pat atsispindi NKSC identifikuotoje kibernetinių grėsmių statistikoje (pavyzdžiui, *open-rdp, open-telnet*) (7 pav.).



7 pav. Populiariausios ryšių ir informacinių sistemų kibernetinės grėsmės Lietuvos IP rėžyje.

Apibendrinant kibernetinių incidentų ir įvykių statistiką, peršasi išvada, kad naudotojų kibernetinio saugumo sąmoningumas turėtų būti gerinamas – pavyzdžiui, labiausiai paplitusią kenkimo PĮ aptikti galima ir su nemokama antivirusine PĮ. Subjektams vis dar sunku įvertinti incidentų daromą žalą. Pagal oficialią Valstybinės duomenų apsaugos inspekcijos ir Policijos departamento prie Vidaus reikalų ministerijos informaciją, nedaugelis kreipiasi dėl atsakomųjų veiksmų taikymo kibernetinių incidentų vykdytojams.

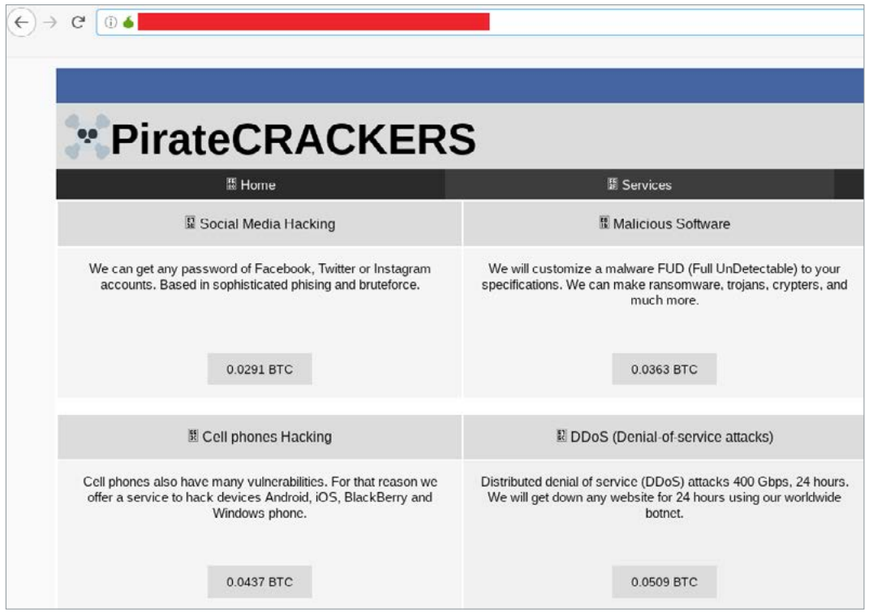
[7] https://www.shodan.io

Atgal į turinį

Kenkimo PĮ paplitimas

- Sensoriais aptinkamos kenkimo PĮ skaičius tarp ypatingos svarbos paslaugas teikiančių subjektų didžiausias buvo krašto apsaugos sistemos RIS (49 proc.).
- Energetikos sektoriuje užfiksuota mažėjantis kenkimo PĮ skaičius.

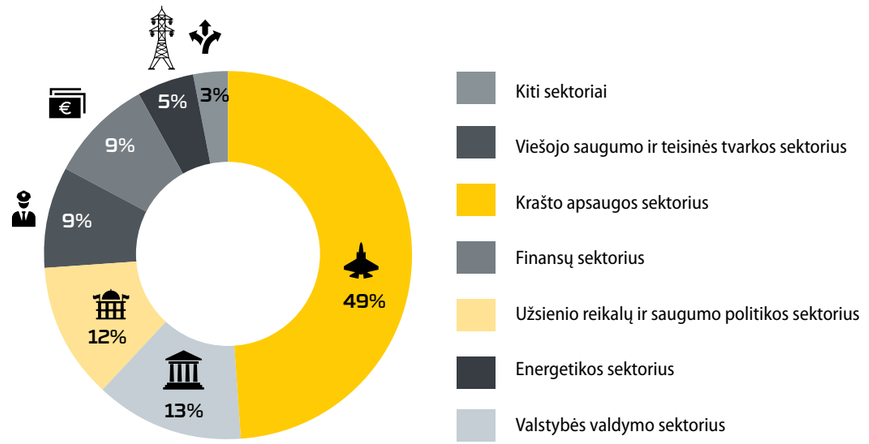
Kenkimo PĮ ir toliau išlieka didelė kibernetinė grėsmė, ypač pažangių ir tęstinių kibernetinių grėsmių (angl. *advanced persistent threat – APT*) kontekste. Grupuotės, kurios kuria APT, daugiausia susijusios su valstybių veikėjais ir yra politiškai motyvuotos. Kalbant apie pasaulinę APT grupuočių veiklą daugiausia minimos tos, kurios turi artimus ryšius su šalių vyriausybėmis, puoselėjančiomis kitokias negu vakarietiškos vertybes. APT grupuotės kibernetinių atakų metu geba efektyviai naudoti keletą atakų vektorių, nuolatos juos keičia. Tačiau esminis APT grupuotes vienijantis bruožas – tikslus taikinio pasirinkimas, efektyvus kibernetinės veiklos pėdsakų slėpimas ir įvairiapusiškas pažeidžiamumų bei kenkimo PĮ naudojimas. Vis dažniau pastebima, kad APT metodus naudoja ir kriminalinės grupuotės, kurių veiklos motyvai nėra priskiriami netiesioginiams valstybių veikėjams. Ši tendencija taip pat netiesiogiai yra susijusi su didėjančiu kenkimo PĮ prieinamumu. Pavyzdžiui, galimybe kenkimo PĮ naudotis kaip paslauga (8 pav.). Gebėjimas efektyviai išnaudoti pažeidžiamumus, modifikuoti ir naudotis kenkimo PĮ tampa galimybe nusikaltėliams užsidirbti.



8 pav. Nusikaltėlių siūlomos paslaugos tamsiajame internete.

2019 m. NKSC užfiksavo ir rankiniu būdu (specialistui tiesiogiai dalyvaujant) apdorojo 971 kibernetinį incidentą, susijusį tiesiogiai su kenkimo PĮ incidentų tipu. Šie kibernetiniai incidentai buvo nustatyti gavus kibernetinio saugumo subjektų pranešimus arba naudojantis specialiai šiai veiklai pritaikytomis NKSC techninėmis kibernetinio saugumo priemonėmis (sensoriais). Sensoriai kenkimo PĮ aptinka pagal nuolatos atnaujinamus kenkėjiškos veiklos indikatorius, kurie suteikia galimybę subjektams ir NKSC specialistams užkardyti jos šaltinį.

Įvertinęs kenkimo PĮ kibernetinių incidentų skaičių ypatingos svarbos paslaugas teikiančių kibernetinio saugumo subjektų RIS, NKSC nustatė iš viso 413 tokių kibernetinių incidentų (2018 m. buvo užfiksuota 470). Daugiausiai jų buvo užfiksuota krašto apsaugos sistemoje (49 proc.), valstybės valdymo (13 proc.) bei užsienio reikalų ir saugumo politikos (12 proc.) sektoriuose (9 pav.). Tokią kenkimo PĮ incidentų statistiką krašto apsaugos sistemoje sąlygojo padidintas šioje srityje dirbančių NKSC specialistų skaičius, aukšta jų kompetencija, papildomų kibernetinio saugumo priemonių naudojimas, dėl kurių CERT specialistai galėjo detaliau nei anksčiau identifikuoti kibernetinius incidentus.



9 pav. Kibernetinio saugumo subjektų ir NKSC techninėmis kibernetinio saugumo stebėsenos priemonėmis surinkta informacija apie kenkimo PĮ pagal ypatingos svarbos paslaugų sektorius.

Kitų kibernetinio saugumo subjektų RIS užfiksuoti 558 kenkimo PĮ incidentai, kurie buvo aptikti NKSC sensorių pagalba, o taip pat ir subjektams patiems taikant prevencines priemones, tinkamai sukonfigūravus ugniasienes, pradėjus naudoti įsibrovimo aptikimo ar prevencijos sistemas. Vis dėlto, kibernetinius incidentus aptikti tipinėmis priemonėmis, paremtomis taisyklių ir grėsmių indikatorių rinkiniais, tampa vis sudėtingiau. Pavyzdžiui, kenkimo PĮ gali šifruoti komunikacijas, taip apsunkindama galimybes aptikti kibernetinius incidentus pagal grėsmių indikatorius. Dėl šios priežasties rafinuotų kibernetinių incidentų valdymas reikalauja nuolatinės grėsmių stebėsenos, ypač pažangių ir tęstinių kibernetinių incidentų (angl. *advanced persistent threat*).

Taip pat yra pastebima, kad, nors kriptovaliutų vertė svyruoja, tačiau jų generavimas kitų interneto vartotojų resursų sąskaita, kai panaudojamos kenkėjiškos interneto svetainės bei *Botnet* tinklai, toliau vyksta internete, taip pat ir Lietuvoje.

Dėl didėjančio kenkimo PĮ prieinamumo, platesnių naudojimo galimybių galima teigti, kad jos grėsmė išlieka aktuali tiek nacionalinio saugumo ir verslo, tiek gyventojų informacijos saugumo požiūriu (10 pav.).

KIBERNETINĖ GRĖSMĖ	ĮTAKA		
	Nacionaliniam saugumui	Verslui ir VII	Gyventojams
Kenkimo PĮ paplitimas	✓	✓	✓

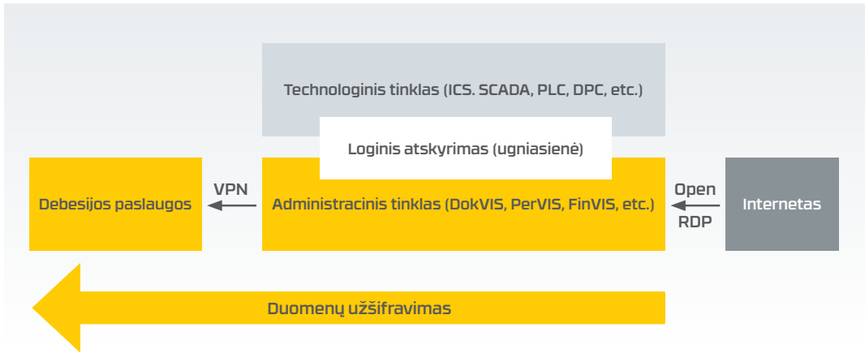
10 pav. Kenkimo PĮ grėsmės įtaka.

Svarbūs kibernetiniai incidentai

- Technologinius tinklus valdantys subjektai Lietuvoje tampa kibernetinių incidentų taikiniu.
- Ir toliau buvo fiksuojami hibridiniai incidentai, kurie susidėjo iš kibernetinės ir informacinės dalies.

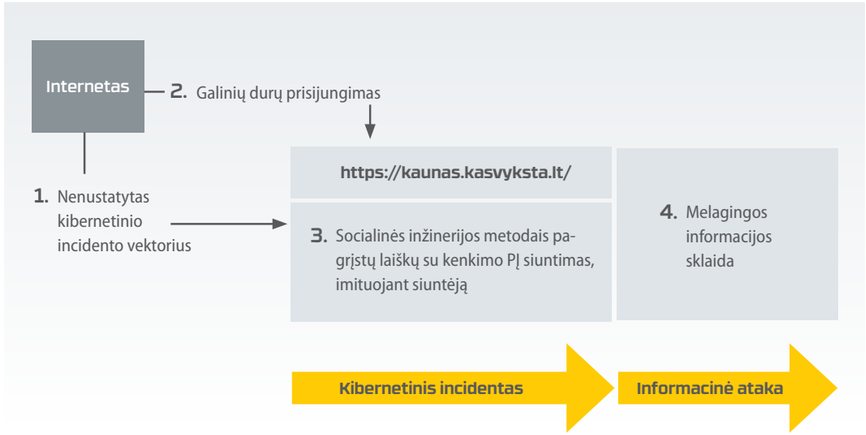
Ypatingas kibernetinis incidentas 2019 m. įvyko Lietuvoje – kibernetinė ataka prieš UAB „Kauno vandenys" informacines sistemas. Incidento metu kenkimo PĮ užšifravo duomenis administraciniame tinkle ir debesijos paslaugų ištekliuose, tačiau vandens tiekimas nebuvo sutrikdytas. UAB „Kauno vandenys" kibernetinio incidento atveju debesijos paslaugos buvo paveiktos per šifruotą VPN. Technologinius procesus atliekantys subjektai dažnai įgalina VPN prieigą per loginį atskyrimą iš administracinio į technologinį tinklą, tokiu būdu yra sukuriamas potencialus kibernetinės atakos vektorius į konkrečias ypatingos svarbos paslaugas. VPN prieiga yra tik vienas iš būdų, kaip iš administracinio tinklo gali būti pasiekiamas technologinis tinklas. Dėl šios priežasties būtina kaip įmanoma labiau izoliuoti technologinius procesus ir sistemas atskirti fiziniu būdu. UAB „Kauno vandenys" kibernetinės atakos vektorius – buvo išnaudota internetu pasiekiama ir automatinėmis priemonėmis aptinkama „open-rdp" nuotolinė prieiga (11 pav.). Tikėtina, kad laiku nesuvaldžius kibernetinio incidento būtų paveiktas vandens tiekimas Kauno mieste.

Atgal į turinį



11 pav. Duomenų užšifravimo kibernetinio incidento hipotetinis pavyzdys prieš technologinį tinklą valdantį subjektą.

Kitas rezonansinis kibernetinis incidentas 2019 m. – kibernetinės ir informacinės atakos, pasinaudojant „kaunas.kasvyksta.lt" interneto svetaine. Kibernetinės atakos specifika yra analogiška 2018 m. vykdytų kibernetinių atakų prieš „tv3.lt" interneto svetainę specifikai. Atakos pirminė fazė – įsilaužimas į interneto svetainę ir „galinių durų" prisijungimo galimybės sukūrimas. Atsižvelgiant į tai, kad nukentėjęs subjektas nepateikė NKSC išsamių žurnalinių įrašų, nepavyko nustatyti pirminio kibernetinio incidento vektoriaus. Piktavalis, gavęs prieigą prie interneto svetainės, paskelbdavo melagingą naujieną ir imituodamas tikrą siuntėją siųsdavo tikslingus elektroninius laiškus su kenkimo PĮ. Atkreiptinas dėmesys, kad šiuo konkrečiu atveju kibernetinė ataka yra susijusi su įsilaužimu į interneto svetainę ir kenkimo PĮ platinimu elektroniniu paštu, tuo tarpu informacinė ataka yra susijusi su melagingos informacijos platinimu (12 pav.). NKSC vertinimu, pakartotinos melagingos naujienos buvo skelbiamos prie interneto svetainės prisijungus per „galines duris", *de facto* tai yra susiję su interneto svetainės savininkų nepakankamu dėmesiu kibernetinio saugumo priemonėms, jų diegimui ir naudojimui.



12 pav. Kibernetinis incidentas ir informacinė ataka, pasinaudojant „kaunas.kasvyksta.lt" interneto svetaine.

Pažeidžiamos interneto svetainės

- Statistiškai viešajame sektoriuje labiausiai pažeidžiamos savivaldybių institucijų ir ministerijų bei joms pavaldžių įstaigų interneto svetainės.
- 37 proc. iš 118 000 interneto svetainių Lietuvoje turi atvirą iš išorinio tinklo administratoriaus ar naudotojų prieigą prie TVS.
- Saugių interneto svetainių skaičius viešajame sektoriuje 2019 m. augo 11 proc.

Interneto svetainių panaudojimas kibernetinėms atakoms deja dar nepakankamai įvertintas pavojus internete. Jos gali būti naudojamos informacinėms atakoms, pavyzdžiui, tikrovės neatitinkančiam turiniui (angl. *fake news*) skleisti. Taip pat gali būti vykdomos socialinės inžinerijos metodais paremtos atakos, bandant išvilioti naudotojų prisijungimo duomenis ar pinigus. Tokiais atvejais kibernetinės atakos vykdomos prieš interneto svetaines, išnaudojant jų pažeidžiamumus, įdiegiant kenkimo PĮ ir pan. Dažniausiai pasitaikantis atvejis – fiktyvios interneto svetainės su nemokamais arba įsigytais domeno vardais. Piktavaliai tokias interneto svetaines siekia įkelti į aukštą greitaveiką turinčią infrastruktūrą ir jos dažniausiai naudojamos socialinės inžinerijos metodais pagrįstai kenkėjiškai veiklai įgyvendinti.

2019 m. kibernetinio saugumo organizacija „Akamai" vykdė domeno vardų, naudojamų vykdant socialinės inžinerijos kibernetines atakas (angl. *baiting*), stebėseną (tyrimo imtis – daugiau negu 2 mlrd. interneto svetainių). Jos metu buvo fiksuojami domenų vardai (su galūnėmis „.com", „.tk", „.loan" ir pan.), kurių kenkėjiško veikimo aktyvumas nesiekdavo trijų dienų.[8] Trumpas aktyvumo laikotarpis susijęs su prieglobos paslaugų teikėjų pastangomis skubiai blokuoti tokias svetaines. Toks aktyvumas suponuoja nuolatines piktavalių pastangas ieškoti prieglobos paslaugų teikėjų, ignoruojančių priežiūros įstaigų nurodymus uždaryti kenkėjiškus išteklius. Su „Akamai" tyrimu susijusios interneto svetainės buvo agresyviai išnaudojamos ir *Botnet*, kenkimo PĮ platinti ir kriptovaliutų „kasimui" naudotojų sąskaita. Tokiu atveju kenkimo PĮ nebūtinai yra įdiegiama į svetainės lankytojų kompiuterius – kompiuterių resursai naudojami apdorojant

[8] https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

Atgal į turinį

interneto svetainėje įdėtą programinį kodą ir tokiu būdu generuojant kriptovaliutą. Pažeidžiamų interneto svetainių grėsmė aktualiausia verslui, viešojo sektoriaus organizacijoms bei gyventojams, nes nuo jų funkcionalumo tiesiogiai priklauso teikiamos paslaugos ir jų prieinamumas (13 pav.).

KIBERNETINĖ GRĖSMĖ	ĮTAKA		
	Nacionaliniam saugumui	Verslui ir VII	Gyventojams
Pažeidžiamos interneto svetainės		✓	✓

13 pav. Pažeidžiamų interneto svetainių grėsmės įtaka.

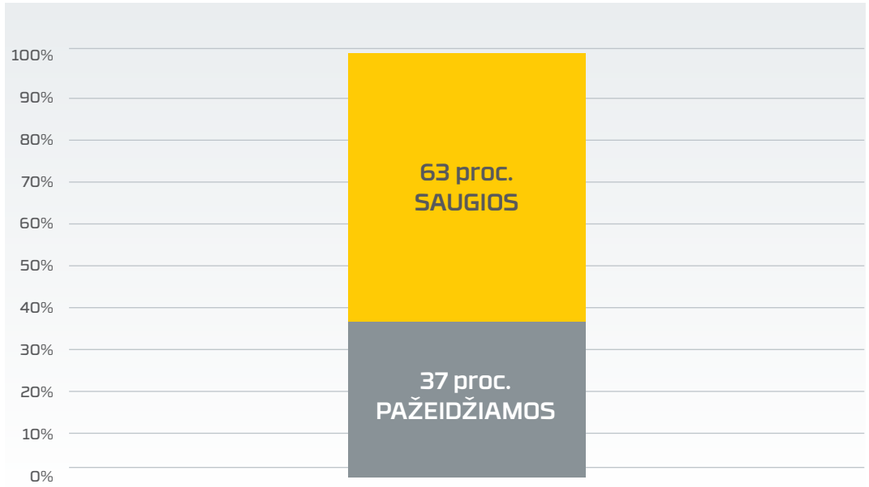
2019 m. NKSC tikrino daugiau nei 118 000 Lietuvos TLD interneto svetainių su galūne „.lt" ir daugiau nei 900 viešojo administravimo subjektų, vykdė VII ir YSII valdytojų interneto svetainių saugumo vertinimą. Identifikavus 56 700 (48 proc.) interneto svetainių su žinoma TVS, nustatyta, kad populiariausia atviro kodo TVS Lietuvoje yra *Word Press*, ji sudaro bendrą 34 proc. tikrintų svetainių imtį ir 33 proc. iš viešojo sektoriaus interneto svetainių aibės (14 pav.).

14 pav. Populiariausios identifikuojamos TVS Lietuvoje.

Nr.	Turinio valdymo sistema	Paplitimas Lietuvoje	Paplitimas viešajame sektoriuje
1	Wordpress	34 proc.	33 proc.
2	Joomla	4 proc.	13 proc.
3	Fresh Media	< 1 proc.	6 proc.
4	Idamas	< 1 proc.	5 proc.
5	Drupal	< 1 proc.	3 proc.
6	Kita	8 proc.	2 proc.
7	Nenustatyta	~ 52 proc.	38 proc.

Iš identifikuotų TVS (56 700 iš bendro 118 000 Lietuvos svetainių skaičiaus), nustatyta, kad net 63 proc. jų programinės įrangos versijos nėra naujausios, dėl to yra rizika, kad pasenusi TVS turės pažeidžiamumą, kurį išnaudojus piktavalis galės prieš svetainę atlikti kibernetinę ataką. Dar blogiau, 8 proc. identifikuotų interneto svetainių savininkų naudoja gamintojų jau nebepalaikomą TVS, todėl joms gali būti nepriei-namai atnaujinimai ir jos gali turėti saugumo spragų. Iš visų imties svetainių (118 000) beveik 44 000

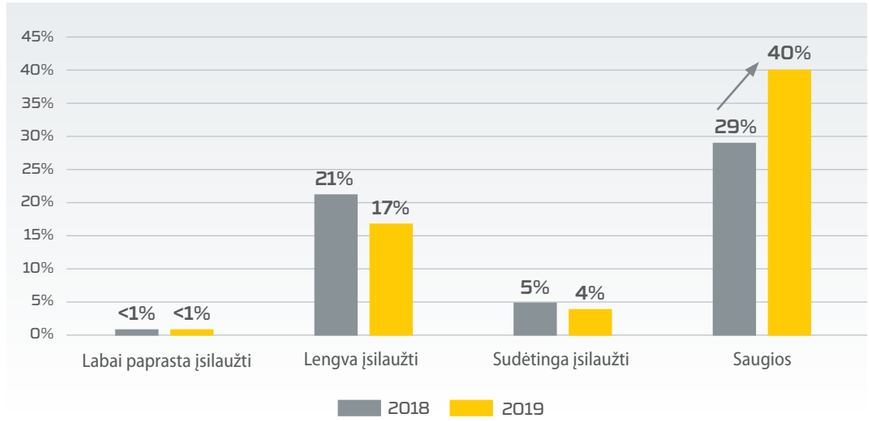
(37 proc.) turi atvirą prieigą iš išorinio tinklo prie interneto svetainės administravimo ir (ar) valdymo (15 pav.). Pažeidžiama TVS ir atvira prieiga prie interneto svetainės yra kibernetinio saugumo rizikos, didinančios įsilaužimo, svetainės valdymo perėmimo, turinio pakeitimo, kenkimo PĮ įterpimo ar nesankcionuoto patekimo į organizacijos vidinius tinklus tikimybę.



15 pav. 2019 m. Lietuvos (.lt) interneto svetainių kibernetinio saugumo vertinimas pagal prieigos prie interneto svetainės valdymo galimybes (imtis – 118 000 svetainių).

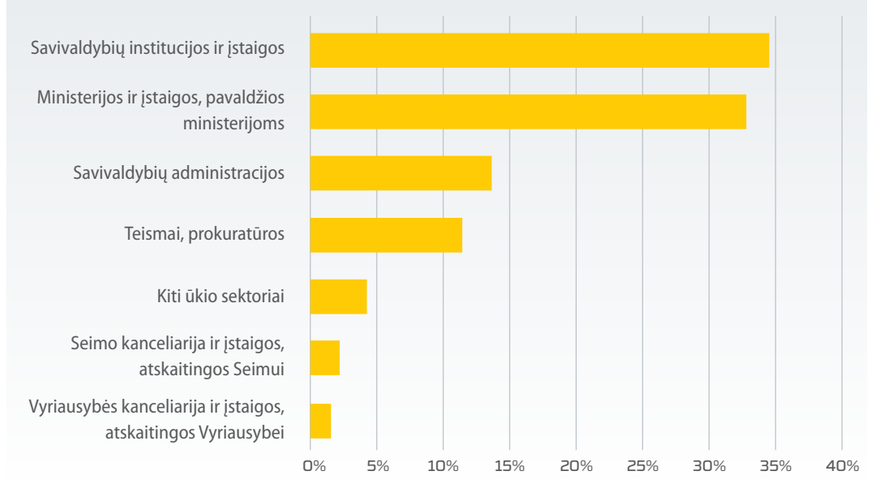
Atviro kodo TVS turinčios interneto svetainės, kurios nėra laiku atnaujinamos, yra labiausiai pažeidžiamas kibernetinių atakų taikinys. Situaciją papildomai blogina nepatikimi ir neatnaujinami TVS įskiepiai bei atviros iš išorinio tinklo naudotojų bei administratorių prieigos, nešifruota komunikacija arba netinkamas kriptografinių priemonių naudojimas – autentifikavimas be TLS/SSL sertifikatų, arba SSL 3.0 bei senesnių kriptografinių algoritmų naudojimas. Viešai iš išorinio tinklo prieinamas interneto svetainių administratoriaus langas (pvz., „.lt/admin“), NKSC vertinimu, nėra apribotas beveik pusėje atvirą prieigą prie TVS turinčių svetainių. Tokiu atveju, ypač jeigu nėra taikoma slaptažodžių keitimo politika bei nėra nustatytas ribotas bandymų prisijungti skaičius, piktavaliai įgauna galimybę techninėmis priemonėmis, išgavę naudotojų sąrašus, vykdyti slaptažodžių parinkimo kibernetines atakas (angl. *bruteforce*).

NKSC 2019 m. taip pat vykdė viešojo sektoriaus interneto svetainių pažeidžiamumų stebėseną, peržiūrėjo ir detalizavo viešojo sektoriaus interneto svetainių kibernetinio saugumo būklės vertinimą (1 priedas). Palyginus su ankstesniu laikotarpiu, viešojo sektoriaus interneto svetainių kibernetinio saugumo būklė gerėja, tačiau vis dar yra apie 17 proc. svetainių į kurias galima lengvai įsilaužti (16 pav.). NKSC, siekdamas pašalinti pažeidžiamumus, potencialiai pažeidžiamų svetainių valdytojus tiesiogiai informuoja ir koordinuoja aukšto prioriteto pažeidžiamumų pašalinimą. Remiantis patikrinimų informacija, NKSC teikia interneto svetainių valdytojams rekomendacijas apie dažniausius interneto svetainių bei informacinių sistemų trūkumus.



16 pav. Viešojo sektoriaus interneto svetainių kibernetinis saugumas 2018-2019 m. pagal pažeidžiamumų, tenkančiam vienam domenui, vertinimą.

Iš viešojo sektoriaus tyrimo matyti, kad daugiausia dėmesio turėtų būti skiriama savivaldybių institucijų, ministerijų bei joms pavaldžių institucijų interneto svetainėms apsaugoti (17 pav.).



17 pav. Bendras interneto svetainių pažeidžiamumas viešojo sektoriaus įstaigose.

Pastebėta tendencija, kada Lietuvoje sukurtos TVS buvo ypač pažeidžiamos kibernetiniams incidentams. Tokių pažeidžiamumų priežastis – nepakankamas kokybės užtikrinimas TVS gamybos arba jos komponentų programavimo metu. Vieno Lietuvos gamintojo TVS turėjo kritinį saugumo pažeidžiamumą, leidžiantį įterpti papildomą programinį kodą į vartotojų peržiūrimą puslapį (angl. *cross-site scripting* saugumo spraga). Lietuviškų interneto svetainių su šiuo pažeidžiamumu buvo užfiksuota 65. NKSC, rem-

damasis atsakingo informavimo principais, informavo TVS gamintoją bei pažeidžiamų interneto svetainių savininkus su nurodymais pažeidžiamumus šalinti.[9] NKSC atkreipia dėmesį, kad subjektai ne visada įsigyja interneto svetainių palaikymo paslaugas, arba į sutartinius įsipareigojimus neįtraukia nuostatų, įpareigojančių pašalinti dėl broko atsiradusias spragas. Interneto svetainės dažnai nėra įteisinamos kaip informacinės sistemos, nėra paskiriami saugos įgaliotiniai, administratoriai neskiria pakankamai dėmesio kibernetinio saugumo klausimams, o svetainėse skelbiama informacija nėra įvertinama kaip svarbi. Dėl šios priežasties nėra nusimatomos išlaidos svetainėms atnaujinti, o kartais dėl interneto svetainių senumo neįmanoma atnaujinti jos PĮ iki naujausios versijos. NKSC papildomai informuoja, kad interneto svetainių kibernetinio saugumo būklę galima pasitikrinti viešai prieinama nemokama priemone, esančia NKSC interneto svetainėje, kuria per trumpą laiką 2019-iais sėkmingai spėjo pasinaudoti 120 subjektų (18 pav.).

18 pav. Interneto svetainių pažeidžiamumų tikrinimo įrankis, pasiekiamas – https://site-check.cert.lt/

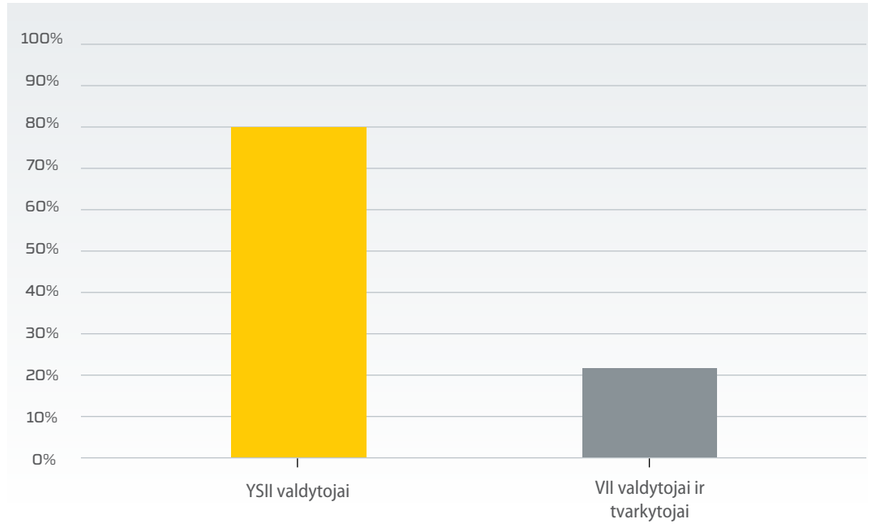
[9] TVS gamintojas neatskleidžiamas, kol yra vykdomas pažeidžiamumų šalinimas.

Atgal į turinį

Kibernetinio saugumo reikalavimų įgyvendinimas

Krašto apsaugos ministerijoje dirbantys „Kurk Lietuvai" specialistai 2019 m. vykdė smulkiojo ir vidutinio dydžio verslo subjektų apklausą dėl kibernetinio saugumo.[10] Apklausoje dalyvavo daugiau negu 200 respondentų. Išanalizavus duomenis paaiškėjo, kad trys iš keturių smulkiojo ir vidutinio verslo įmonių nėra pasiruošusios arba nežino, jog yra pasiruošusios, atremti kibernetines atakas. Net 72 proc. respondentų teigė, kad nežino, kaip reikia įsivertinti kibernetinio saugumo spragas ir rizikas. Respondentai taip pat nesupranta, kokios galėtų būti kibernetinių incidentų pasekmės. Dėl šios priežasties kibernetinio saugumo subjektams kyla sunkumų įgyvendinant Lietuvos Respublikos Vyriausybės nustatytus kibernetinio saugumo reikalavimus.

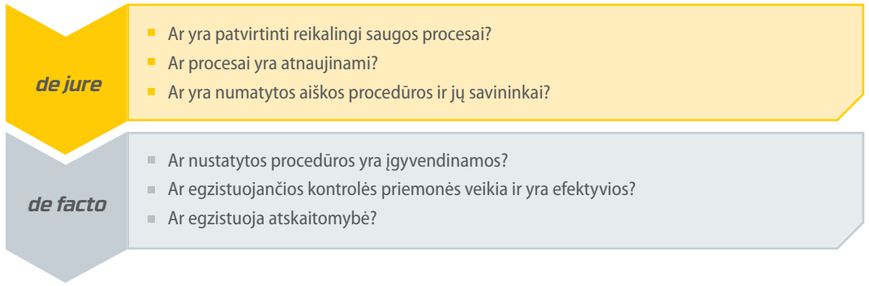
Vykdant kibernetinio saugumo reikalavimų įgyvendinimo stebėseną nustatyta, kad YSII valdytojų reikalavimų įgyvendinimas išaugo – 80 proc. YSII valdytojų 2019 m. buvo įgyvendinę kibernetinio saugumo reikalavimus (19 pav.). Deja VII valdytojams ir tvarkytojams ir toliau kyla keblumų su reikalavimų įgyvendinimu.



19 pav. Organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas

Kibernetinio saugumo strategijoje didelis dėmesys skiriamas ypatingos svarbos informacinės infrastruktūros valdytojų kibernetiniam saugumui. 2019 m. NKSC pradėjo naują veiklą – faktinius kibernetinio saugumo būklės patikrinimus. Patikrinimų rezultatai leidžia reziumuoti, kad deklaruojamas kibernetinio saugumo reikalavimų įgyvendinimas neatspindi realios organizacijų kibernetinio saugumo situacijos.

[10] http://kurklt.lt/2020/01/06/apklausa-lietuvos-svv-truksta-kibernetinio-saugumo-ziniu/

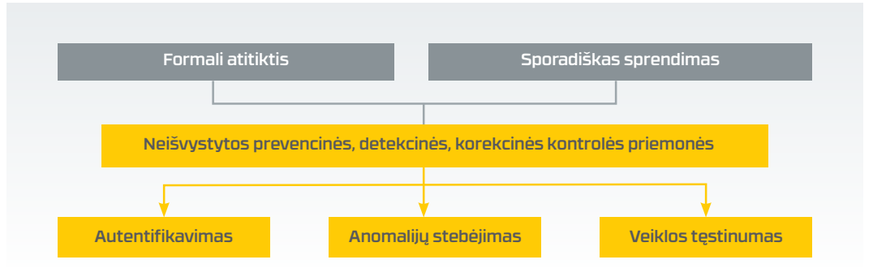


20 pav. Kibernetinio saugumo vertinimo procesas.

Organizacijos dažnai atitinka arba beveik atitinka saugos politikos *de jure* kriterijų. Tikrinami subjektai turi formaliai apsibrėžę saugos procesus, gaires, tačiau saugos užtikrinimas dažnai vertinamas kaip biurokratinė našta. Saugos dokumentai būna parengti formaliai, pagal nebegaliojančius Lietuvos Respublikos teisės aktus, o dokumentų turinyje apibrėžti procesai nebūna priskirti pagal kompetenciją. NKSC, analizuodamas kibernetinio saugumo reikalavimų įgyvendinimą, taip pat užfiksavo tendenciją, kad organizacijos yra linkusios informacijos bei kibernetinio saugumo dokumentų turinį apibrėžti abstrakčiai, tai leidžia formaliai pagrįsti reikalavimų įgyvendinimą, nereglamentavus reikalingų procesų. Dėl formalių ir abstrakčių procesų organizacijos faktinė sauga dažnai užtikrinama *ad hoc* principais, kada nėra aiškūs procesų savininkai ir jų atsakomybės. NKSC užfiksavo atvejų, kai atsakomybė už informacinę sistemą ir jos saugą buvo priskirta konkrečiam organizacijos struktūriniam padaliniui, tačiau praktiškai sistemos priežiūrą sporadiškai atlikdavo vienas iš administratorių. Fizinių patikrinimų metu taip pat paaiškėdavo, kad formali organizacinių ir techninių kibernetinio saugumo reikalavimų atitiktis *de facto* būdavo įgyvendinama iš dalies, neužtikrinant proporcingo teikiamų ypatingos svarbos paslaugų kibernetinio saugumo.[11]

Kita pasikartojanti tendencija, kurią NKSC užfiksavo patikrinimų metu, – rizikos valdymo kultūros trūkumas. Organizacijos vis dar nevertina informacijos kaip turto, todėl nesugeba deramai įvertinti kibernetinių incidentų poveikio. Dėl šios priežasties atsiranda tikimybė, kad organizacijos yra prisiėmusios per didelę riziką.

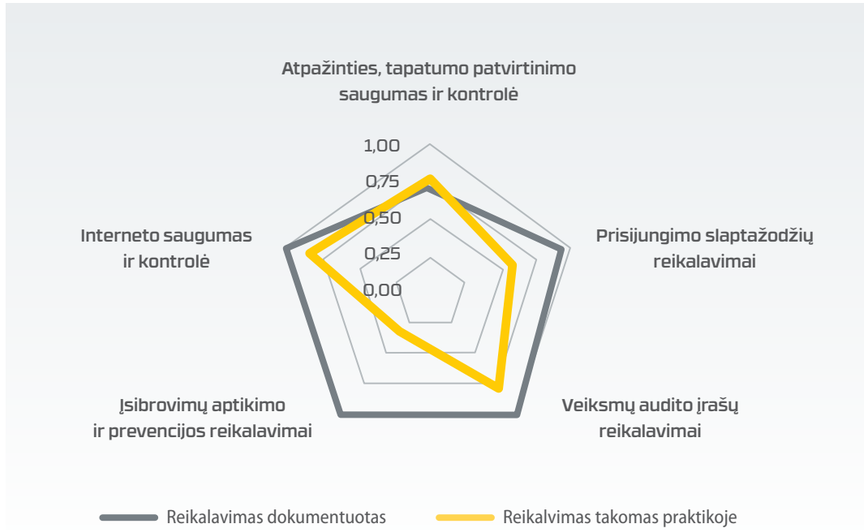
Dėl formalaus kibernetinio saugumo reglamentavimo NKSC patikrinimų metu fiksavo tipinius techninių kontrolės priemonių trūkumus (21 pav.).



21 pav. Tipiniai kibernetinio saugumo trūkumai.

[11] Atsižvelgiant į tai, kad NKSC pagal prioritetą tikrina ypatingos svarbos informacinės infrastruktūros valdytojus, kurių baigtinis sąrašas tvarkomas Valstybės ir tarnybos paslapčių įstatymo nustatyta tvarka, pateikiami nuasmeninti duomenys.

Pavyzdžiui, žiūrint iš prevencinės pusės, vis dar nėra skiriama pakankamai dėmesio prisijungimo duomenų saugojimui. Dažnai autentifikavimo informacija saugoma lokaliose darbo stotyse esančiose nešifruotose bylose, darbo vietų, sistemų naudojimosi instrukcijose, kurios kartais būna sukeltos į dokumentų valdymo sistemas viešai. Naudotojų, administratorių slaptažodžių sudarymo būdas įprastai apima tik dvi grupes (raides ir skaičius), o slaptažodžių keitimo reikalavimas palengvinamas iki vieno karto per pusmetį ar išvis netaikomas. Vis dar pasitaiko atvejų, kad pamirštama techninėje ir PĮ pakeisti gamintojo numatytus slaptažodžius. Kalbant apie detekcines priemones, dažnu atveju, nors naudotojų ir administratorių veiksmai informacinėse sistemose yra žurnalizuojami, tačiau įrašai nėra peržiūrimi, nėra stebimos anomalijos – sutrikus informacinės infrastruktūros arba jos struktūrinio elemento veikimui taikomas perkrovimo būdas. Vis dar nėra naudojamos įsibrovimo aptikimo sistemos, pagrindinėse tarnybinėse stotyse neįjungiamos saugasienės, turinčios blokuoti visą įeinantį ir išeinantį srautą, išskyrus susijusį su ypatingos svarbos informacinės infrastruktūros funkcionalumu ir administravimu. Dėl šios priežasties matoma didžiulė atskirtis tarp incidentų aptikimo reglamentavimo ir faktinio reikalavimų įgyvendinimo (22 pav.). Korekcinės priemonės dėl neholistiško kibernetinio saugumo įgyvendinimo taip pat sąlygoja papildomas rizikas. Neatliekami atsarginių kopijų atkūrimo testai, kurie parodytų, ar nėra sugadintų kopijų ir ar kopijose saugoma visa reikalinga informacija. Taip pat retai yra diegiami platformų PĮ, kuriose veikia infrastruktūros elementai, atnaujinimai.



22 pav. Techninių kibernetinio saugumo reikalavimų realus įgyvendinimas vienoje iš tikrintų organizacijų, kai 0 – neįgyvendinta, o 1 – reikalavimas įgyvendintas.

Paslaugų teikėjų bei įrangos patikimumas

- **Nustatyti programinės ir techninės įrangos pavyzdžiai, kurie yra nepatikimi, o vartotojų duomenys išsiunčiami į valstybes, kuriose ES duomenų apsaugos reikalavimai negalioja.**
- **Dažnai viešai platinamos programos ir aplikacijos turi akivaizdžiai perteklines prieigos teises prie įrenginyje esančių duomenų.**

Techninės ir PĮ patikimumas visų pirma susijęs su kibernetinio saugumo rizikomis. Didžiausia iš jų – įrenginių saugumo spragos. Įrenginių saugumo spragos didžiausią grėsmę kelia IoT aplinkoje. Gamintojai siekia sukurti santykinai pigius įrenginius mažiausiais kaštais, todėl neskiriama daug dėmesio tokių įrenginių kibernetiniam saugumui ir autentifikavimui valdyti, o dėl šiuos įrenginiuose esančių nedidelių skaičiavimo resursų atsisakoma šifravimo. Ši grėsmė yra aktuali ir tarptautiniu lygmeniu – dėl šios priežasties ES siekiama sukurti bendrą įrenginių ir paslaugų sertifikavimo mechanizmą.[12] NKSC turimais duomenimis, Lietuvoje tokios spragos daugiausiai yra susijusios su įgalintomis perteklinėmis paslaugomis ir atvirais prievadais. Dažnai atvirų prievadų funkcionalumas nėra būtinas ir naudotojai gali patys tokią prieigą užkardyti – keisti prieigos prie valdymo skydo naudotojų prisijungimo duomenis, prieigą iš išorinio tinklo užkardyti arba apriboti leisdami prisijungti tik iš tam tikrų IP adresų. Piktavalis, norėdamas atlikti kibernetinę ataką, gali ieškoti spragų IoT, tuo labiau kai tokiai veiklai atlikti nereikalingos specifinės žinios ir priemonės, pakanka viešai prieinamų įrankių.[13]

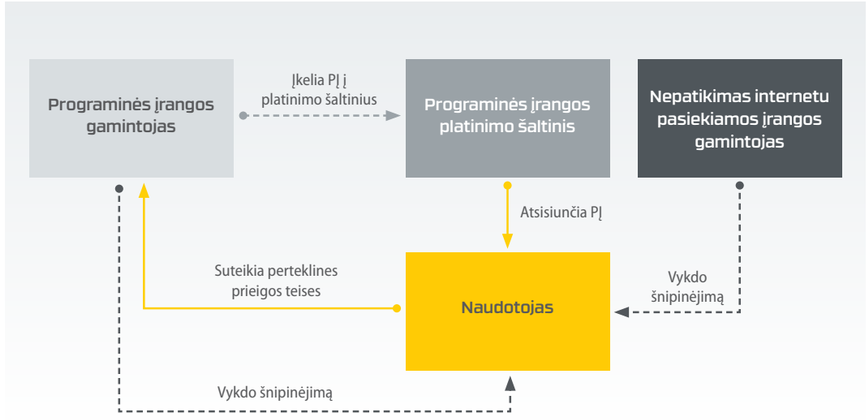
Kitas svarbus techninės bei PĮ patikimumo aspektas – paslaugų tiekėjų patikimumas (23 pav.). Šis klausimas yra daugialypis: iš vienos pusės, jis yra susijęs su miglota gamintojo reputacija, iš kitos – su nesankcionuotais pokyčiais gamybos procese. Kartais jos gali būti susijusios su skirtingu regioniniu ar valstybiniu reguliavimu. Dėl šios priežasties vieniems regionams skirta įranga gali neatitikti specifinių kokybės

[12] https://www.enisa.europa.eu/topics/standards/certification

[13] https://www.shodan.io/

Atgal į turinį

užtikrinimo reikalavimų, pavyzdžiui, taikomų ES šalyse. ES lygmeniu inicijuotas sertifikavimas turėtų sustiprinti kibernetinio saugumo požiūriu saugų įrenginių platinimą Europoje, tačiau kol kas esant nevienodam reguliavimui naudotojai patys prisiima rizikas, kurios kartais padidėja dėl taikomo mažiausios kainos principo. Dėl šios priežasties net ir patikimų gamintojų techninė įranga, kuri dėl mažesnės kainos surenkama nepatikimose šalyse, gali kelti grėsmę dėl paliktų pažeidžiamumų, „galinių durų“ prisijungimo galimybės ir pan.



23 pav. Programinės ir techninės įrangos patikimumo rizikų pavyzdys.

NKSC vertinimu, paslaugų tiekėjų ir įrangos patikimumo klausimas yra visapusiškas (24 pav.).

KIBERNETINĖ GRĖSMĖ	ĮTAKA		
	Nacionaliniam saugumui	Verslui ir VII	Gyventojams
Paslaugų tiekėjų ir įrangos patikimumas	✓	✓	✓

24 pav. Įrenginių saugumo spragų grėsmės įtaka.

NKSC, siekdamas užtikrinti saugios programinės ir aparatinės įrenginių naudojimą šalies viduje, vykdė kompleksinį Lietuvoje tiekiamų elektroninių sprendimų (mobiliųjų aplikacijų, taikomosios PĮ, aparatinės ryšio ir multimedijos įrangos) kibernetinio saugumo vertinimą. Tyrimai buvo vykdomi pagal naudotojams aktualiausias rizikos sritis, vertinant taikomąsias mobiliąsias aplikacijas, ryšio (maršrutizavimo ir komutavimo) bei multimedijos įrangą.

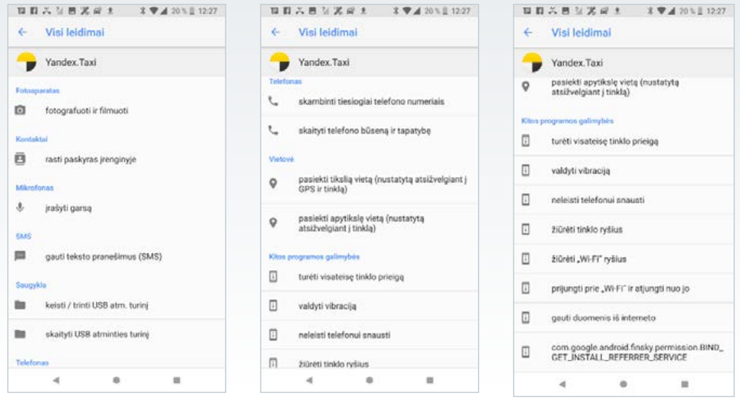
Vertinimo rezultatai atspindi rafinuotas kibernetinio saugumo rizikas, kurios išreikštos įvairios formos ir turinio paslaugomis, yra orientuotos į vartotojų duomenų (asmens, infrastruktūros ir kt.) perėmimą. Didžioji dalis programinių produktų yra nemokami, todėl Lietuvoje didelį vartotojų ratą. Nustatyta, kad ne NATO šalyse sukurti programiniai produktai yra aukštos funkcinės išbaigties, tačiau beveik visais atvejais kelia grėsmę šių produktų vartotojams – galimai atlieka perteklinės informacijos rinkimo procedūras, daugybinius šifruotus ryšio kanalų sujungimus su rytų šalyse esančiomis tarnybinėmis stotimis. Dažnai produktų gamintojai linkę nuslėpti tikrąją produkcijos kilmės šalį.

Taikomųjų mobiliųjų programėlių tyrimų rezultatai

Pastaruoju laikotarpiu buvo atlikti „Yandex.Taxi“, „FaceApp“, „ABBYY Business Card Scanner“ taikomųjų programėlių kibernetinio saugumo vertinimas. Išvadose pažymima, jog tirtos programėlės reikalavo prieigos teisių prie mobiliojo įrenginio, pasižymėjo plačiai interpretuotinomis naudojimo taisyklėmis ir turėjo galimybę duomenis iš mob. įrenginio perdavinėti į trečiąsias šalis, kuriose nėra taikomos Bendrojo duomenų apsaugos reglamento nuostatos.

„Yandex.Taxi“ mobiliosios programėlės tyrimas

NKSC įvertino Lietuvoje 2018 m. liepos 26 d. aktyviai pradėtą platinti programinį paketą „Yandex.Taxi“. Tymo metu buvo nustatyta, kad programėlė reikalauja prieigos prie didelio kiekio jautrių duomenų ir leidimo naudotis įrenginio funkcijomis. Minima programėlė turi galimybę aktyvuoti įrenginio kamerą ir mikrofoną (įrašyti naudotojo aplinką), naudoti kontaktų sąrašą (galimybė gauti telefonų knygos, naudojamų paskyrų informaciją), valdyti skambučius, nustatyti įrenginio tapatybę ir veiklos būklę, valdyti trumpųjų pranešimų paslaugas (galimybė perimti gaunamus pranešimus), modifikuoti turinį, saugomą išmaniojo įrenginio atmintyje, nustatyti tikslią (GPS) įrenginio buvimo vietą, valdyti tinklo prieigą (siųsti duomenis internetu, stebėti ir valdyti tinklo sujungimus, valdyti belaidžio tinklo (angl. *Wi-Fi*) prieigą) (25 pav.).



25 pav. „Yandex.Taxi“ nuostatų langai.

Pažymėtina ir tai, kad vėlesnės programėlės versijos ateityje gali padidinti reikalaujamų funkcijų prieigų kiekį. 2019 m. nežymiai modifikuota aplikacija pradėjo veikti Suomijoje *Yango* pavadinimu.

Tačiau, nepaisant gausių reikalaujamų prieigų prie įrenginio funkcionalumų, ji yra parengta kokybiškai, tinkamai optimizuota, duomenims perduoti naudoja šifruotus kanalus, standartinius protokolų prievadus.

NKSC analizės metu buvo nustatyta, kad programėlė šifruotais ryšio kanalais reguliariai jungėsi ir palaikė aktyvų ryšį su 11 unikalių IP adresų (iš kurių 10 priklauso Rusijos Federacijai). Duomenys perduodami skirtingais laiko tarpais.

Nustatyta, kad minima programėlė turi galimybę įvairiu laiku ir šifruotais ryšio kanalais užmegzti ryšį su skirtinguose Rusijos Federacijos regionuose esančiais adresais (remiantis geolokacijos IP duomenų bazių informacija) nepriklausomai nuo to, ar programėlė veikia budėjimo, ar aktyviuoju režimu. Pažymima, kad „Yandex. Taxi“ palaiko nuolatinį ryšį su trimis adresais (26 pav.).

Komercinis pavadinimas: Yandex. Taxi

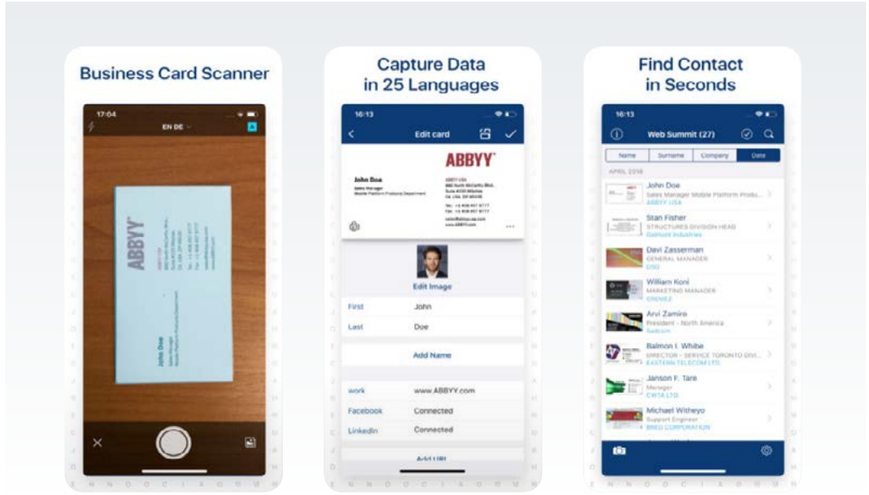
Sisteminis pavadinimas: **ru.yandex.taxi**

Eil. nr.		Miestas	Serverio vardas (angl. *Hostname*)	Perduodami duomenys programėlei veikiant budėjimo režimu	Perduodami duomenys programėlei esant aktyviai
1	AKTYVŪS PRISIJUNGIMAI	Maskva	*.yandex.net	Taip	Taip
2		Maskva	*.yandex.net	Taip	Ne
3		Maskva	*.yandex.net	Taip	Ne
4		New Jersey	*.linode.com	Taip	Taip
5		Jakaterinburgas	*.yandex.net	Taip	Taip
6		Maskva	*.yandex.ru	Ne	Taip
7		Jakaterinburgas	*.yandex.ru	Ne	Taip
8		Jakaterinburgas	*.yandex.net	Ne	Taip
9		Jakaterinburgas	*.yandex.net	Ne	Taip
10		Maskva	*.yandex.net	Ne	Taip
11		Maskva	*.yandex.ru	Ne	Taip

26 pav. Programinio paketo tinklo srauto analizė (Pastaba: IP adresai NKSC žinomi).

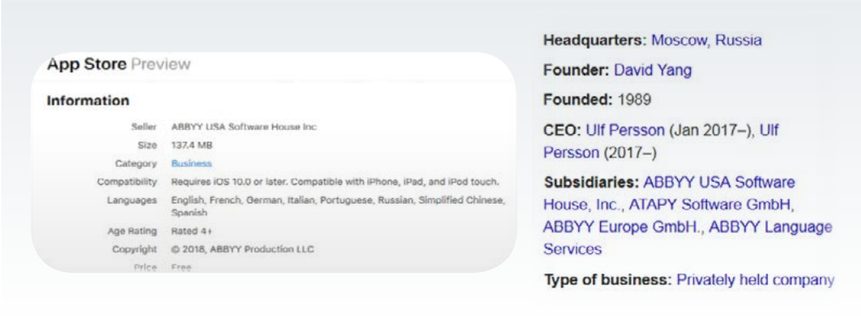
„ABBYY Business Card Scanner“ mobiliosios programėlės tyrimas

Mobilioji programėlė „ABBYY Business Card Scanner“ – programėlė, skirta vizitinėms kortelėms virtualizuoti. Mobiliuoju įrenginiu nufotografuota vizitinė kortelė yra išanalizuojama programėlės ir suskaitmeninama – iš kortelėje esančių duomenų išskiriamas asmens vardas, pavardė, atstovaujama įstaiga ir kiti kortelėje pateikti duomenys. Verta pažymėti, kad duomenų išskyrimas ir suskaitmeninimas remiantis vaizdine medžiaga (fotografija) yra santykinai sudėtinga procedūra (27 pav.).



27 pav. „ABBY Business Card Scanner“ taikomoji mobilioji programėlė.

Programėlės atsisiuntimo platformoje *Apple* „App Store“ nurodoma, kad programėlės pardavėjas (angl. *Seller*) yra *ABBY USA Software House Inc.,* kompanijos būstinė (angl. *Headquarters*) yra Milpite, Kalifornijoje. Generalinis direktorius (angl. *Chief Executive Officer, CEO*) – Ulf Persson (28 pav.).



28 pav. Gamintoją „ABBYY“ charakterizuojanti informacija.

Atlikus programėlės srauto dekompozicijos tyrimą nustatyta, kad „ABBYY Business Card Scanner“ atlieka sujungimus su 61 serveriu, esančiu Vokietijoje, Lenkijoje, Švedijoje, Airijoje, JAV ir Rusijoje. Galima vertinti, kad gamintojas „ABBYY“ nuosekliai vengia atskleisti kompanijos ištakas, nurodydamas JAV kaip komercinio vystymo šalį.

Remiantis Lietuvos Respublikos valstybės saugumo departamento ir Antrojo operatyvinių tarnybų departamento prie KAM 2018 m. grėsmių nacionaliniam saugumui vertinimu, „Rusijos žvalgybos ir saugumo tarnybos turi teisinius įgaliojimus ir techninių galimybių įgyti prieigą prie Rusijos ir užsienio valstybių piliečių, naudojančių rusiškas elektroninio komunikavimo platformas, duomenų“. Grėsmių vertinime taip pat nurodoma: „<...> grėsmė, kad asmeniniai duomenys nutekinami Rusijos žvalgybos ir saugumo tarnyboms, kyla visiems Lietuvos piliečiams, besinaudojantiems rusiškais socialiniais tinklais ir elektroninio pašto paslaugomis, pvz., odnoklasniki, mail.ru, yandex ir pan.“.

„FaceApp“ mobiliosios programėlės tyrimas

Mobilioji programėlė „FaceApp“ – Rusijos PĮ gamintojo „OOO Wireless Lab“ nuotraukų transformavimo programėlė, kuri specializuotais filtrais leidžia grafiškai modifikuoti nuotraukose užfiksuotų veidų savybes – juos pasendinti, atjauninti, pridėti šypseną ar pakeisti lytį charakterizuojančius veido bruožus. Remiantis „FaceApp“ naudojimo sąlygomis, programėle legalu naudotis nuo 18 m. amžiaus (nuo 13 m., jei atsakomybę prisiima tėvai ar globėjai).

Nagrinėtos *Android* („FaceApp“ versija „3.4.8“, konteinerio dydis 12,45 MB) ir iOS („FaceApp“ versija „3.4.7“, konteinerio dydis 153,1 MB) platformose veikiančios programėlės. Įdiegus programėlę į mobilųjį įrenginį, parodomas perspėjimas su informacija, nurodančia, kad pasirinktos nuotraukos bus apdorojamos nuotoliniu būdu mobiliosios programėlės kūrėjų tarnybinėse stotyse. Nesutikus su pateiktomis taisyklėmis, programėlė parodo langą su žinute apie tai, kad ji negali funkcionuoti, ir raginimu sutikti su nuotraukų apdorojimu nuotoliniu būdu.

Remiantis programėlės prieigos reikalavimais ir priėjimo prie įrenginio duomenų lygiu galima daryti prielaidą, kad reikalavimai prieigai yra skirti užtikrinti mobiliosios programėlės funkcionalumą, yra nepertekliniai ir neatsiejama programėlės veikimo dalis. Verta pažymėti, kad vartotojas, atsisiuntęs ir įsidiegęs „FaceApp“ programėlę, sutinka su programėlės naudojimo sąlygose nurodytomis taisyklėmis, kitu atveju galimybė naudotis teikiamomis paslaugomis nėra suteikiama: „<...> By accessing the FaceApp website or by downloading FaceApp's mobile application, you agree to these Terms. If you do not agree to these Terms, including the mandatory arbitration provision and class action waiver in Section 15, do not access or use our Services <...>“.

Naudojimo taisyklėse nurodoma, kad vartotojas turi sutikti neatlygintinai suteikti „FaceApp“ prieigą prie programėlės aplinkoje pasiekiamų duomenų – leisti „FaceApp“ juos naudoti, dauginti, modifikuoti, pritaikyti, skelbti, versti, kurti išvestinius kūrinius, platinti, viešai naudoti visais žinomais (ar tais, kurie bus sukurti ateityje) formatais ir kanalais: „<...> You grant FaceApp a perpetual, irrevocable, nonexclusive,

royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce, modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you <...>".

Kartu pažymima, kad vartotojas sutinka leisti „FaceApp" komercializuoti mobiliojoje programėlėje naudotus duomenis: „<...> By using the Services, you agree that the User Content may be used for commercial purposes. You further acknowledge that FaceApp's use of the User Content for commercial purposes will not result in any injury to you or to any person you authorized to act on its behalf <...>".

Nustatyta, kad mobiliuosiuose įrenginiuose atliekamos dalinės aktualiųjų duomenų (nuotraukų) modifikacijos procedūros (glaudinimas ir dalinis apdorojimas), ši iš dalies apdorota informacija siunčiama į nutolusį serverį galutinai apdoroti. Vartotojų nuotraukos yra modifikuojamos serveriuose, kurių dauguma registruoti Jungtinėse Amerikos Valstijose (iOS platformoje veikianti programėlė sujungimus atliko su 2 serveriais, registruotais Airijoje). Iš tarnybinės stoties duomenys atsiunčiami ir sukomponuojami mobiliajame įrenginyje, kuri vėliau parodomi vartotojui. Tyrimo metu pastebėta, kad *Android* platformoje veikianti programėlė į serverį vidutiniškai išsiunčia 560 kB duomenų, gauna 360 kB duomenų; iOS platformoje veikianti programėlė vidutiniškai išsiunčia 1,1 MB duomenų, gauna 176 kB duomenų. Manoma, kad šie duomenų mainų dydžių skirtumai išryškėja dėl *Android* ir iOS platformose naudojamų skirtingų duomenų glaudinimo mechanizmų.

Didžiausią susirūpinimą kelia programėlės naudojimo taisyklės, pagal kurias vartotojas turi sutikti neatlygintinai suteikti „FaceApp" prieigą prie programėlės aplinkoje pasiekiamų duomenų – leisti „FaceApp" juos naudoti, dauginti, modifikuoti, pritaikyti, skelbti, versti, kurti išvestinius kūrinius, platinti, viešai naudoti visais žinomais (ar tais, kurie bus sukurti ateityje) formatais ir kanalais. Vertinant tai, kad programėlė sukurta Rusijos PĮ gamintojo „ООО Вайрелез Лаб", šie reikalavimai sustiprina neproporcingumo įspūdį tarp programėlės teikiamų paslaugų profilio ir vartotojo patiriamų asmeninių duomenų kaštų.

Ryšio (maršrutizavimo ir komutavimo) įrangos tyrimų rezultatai

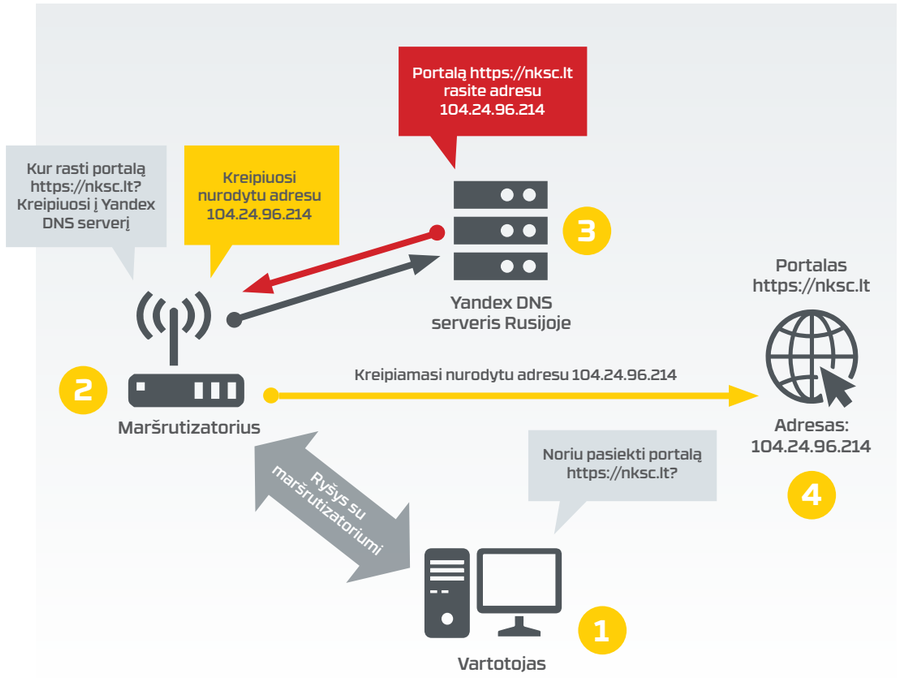
NKSC atliko ir 2019 m. birželio 10 d. paskelbė Lietuvoje parduodamos komunikacinės įrangos kibernetinio saugumo vertinimą. Šioje analizėje pateikti gamintojo „D-Link" maršrutizatorių ir komutatorių, skirtų namų ūkiams ir smulkiems verslo subjektams, vertinimo rezultatai. Analizuotų įrenginių kainų diapazonas nuo 20 Eur iki 200 Eur.

Tinklo įrangos gamintoja D-*Link Corporation (D-Link Systems, Inc.*) yra Taivano korporacija, 30 metų valdanti prekinį ženklą „D-Link", turinti 2000 darbuotojų, gaminamos produkcijos asortimentą tiekianti 60-čiai šalių. Korporacijos technologinė ašis – įvairios bendrų tinklo sprendimų realizacijos, kurios apima ryšio komutavimo, maršrutizavimo ir debesų kompiuterijos technologijas, sukuriančias didelės apimties ir didelio kompleksiškumo belaidžio ir plačiajuosčio tinklo plėtros galimybes. „D-Link" pasižymi plačiu tikslinių grupių diapazonu – namų ūkiai, mažo, vidutinio ir stambaus verslo sektoriai, ryšio ir elektroninių paslaugų teikėjai. Nepaisant „D-Link" prekinio ženklo žinomumo, korporacija 2014–2018 metais susidūrė su kuriamos įrangos saugumo iššūkiais: remiantis pažeidžiamumų duomenų bazių (angl. *Common Vulnerabilities and Exposures – CVE*) informacija, fiksuota 50 pažeidžiamumų, iš kurių 31 nustatytas 2018 metais. Pastebimai auganti „D-Link" produkcijos pažeidžiamumų tendencija kelia susirūpinimą ir yra neabejotinas NKSC atliekamų kompleksinių tyrimų objektas.

Nustatyta, kad tam tikri gaminiai, skirti namų ūkiams ir smulkiajam bei vidutiniam verslui, yra itin glaudžiai technologiškai susiję su Rusijos Federacija. Gaminiuose „D-Link DIR-842", „D-Link DIR-853", „D-Link DSL-2640U" ir „D-Link DSR-250N" nurodomas įrangos tiekėjas „D-Link Russia". Įrangoje veikia Rusijos DNS paslaugos „Yandex.DNS" ir „SkyDNS". DNS (angl. *The Domain Name System*) – sistema, konvertuojanti domeno žodinę išraišką į serverio skaitinį IP adresą. Maršrutizatoriuje nurodžius DNS serverio adresą, kiekviena domeno žodinė užklausa siunčiama į nurodytą DNS serverį, kuris pateikia skaitinį IP adresą, o maršrutizatorius vartotoją nukreipia reikiamu serverio IP adresu. Verta pažymėti, kad įrenginių PĮ atnaujinimas atliekamas iš Rusijoje esančių serverių (29 pav.).

„D-Link" įrenginiuose aktyvavus gamintojo nustatytą „Yandex.DNS" paslaugą, visos DNS užklausos siunčiamos į serverius, kurie valdomi Rusijos kompanijos „Yandex". Šiuose serveriuose registruojamos iš vartotojų atėjusios užklausos, leidžiančios nusakyti besikreipiančio vartotojo IP adresą, vartotojo šalį, užklausos laiką, adresus, kuriuos lanko vartotojas. Svarbu pažymėti, kad ilgalaikis vartotojo DNS užklausų stebėjimas ir stebėsenos rezultatų apdorojimas taikant šiuolaikinius duomenų analizės ir agregacijos metodus leidžia dideliu tikslumu apibendrinti vartotojo elgseną elektroninėje erdvėje ir tam tikrais atvejais nustatyti asmenį.

Kartu su „Yandex.DNS" paslauga gaminyje „D-Link DIR-853" veikia ir kita DNS paslauga „SkyDNS" – Rusijoje įsikūrusios įmonės produktas, teikiantis DNS ir DNS filtravimo paslaugas fiziniams ir juridiniams asmenims. „SkyDNS" yra Rusijoje įsikūrusi įmonė, kuri teikia DNS ir DNS filtravimo paslaugas fiziniams ir juridiniams asmenims. Įmonė nurodo, kad jos paslaugomis naudojasi vartotojai iš daugiau nei 40 valstybių, išskiriant Rusiją, Kazachstaną ir Ukrainą. „SkyDNS" valdo duomenų bazę su 90 milijonų puslapius charakterizuojančių įrašų, gautų iš DNS užklausų agregacijos. „SkyDNS" puslapiams charakterizuoti ir klasifikuoti naudoja dirbtinį intelektą, jį apmokant vartotojų elgsenos tyrimų rezultatais: *„Our research team works with bid data using such methods as continuous machine learning, AI and user behavior analysis to enrich SkyDNS DB and ensure high quality of web categorization."* Verta pažymėti, kad minėtos informacijos agregacijos, analizės ir taikymo specifiniams uždaviniams spręsti procesai gali veikti tik užtikrinant didelės apimties duomenų kaupimą, o netinkamas jų valdymas gali kelti grėsmę vartotojų privatumui.



29 pav. „Yandex.DNS" ir programinių atnaujinimų proceso blokinė schema.

NKSC pažymi, kad vartotojai, naudodami trečiųjų šalių iš anksto įdiegtas DNS funkciją užtikrinančias programas maršrutizatoriuose, rizikuoja, kad naršymo internete duomenys bus registruojami ir kaupiami nekontroliuojamai trečiųjų šalių. Rekomenduojama vartotojams domėtis įsigyjama programine ir aparatine įrangomis, kritiškai vertinti siūlomų paslaugų turinį.

Multimedijos įrangos tyrimų rezultatai

NKSC atliko Lietuvos radijo ir televizijos komisijos (toliau – LRTK) pateikto IPTV priedėlio „S-Box TX3 mini-H" (toliau – priedėlis) saugumo vertinimą. IPTV priedėlis „S-Box TX3 mini-H" – Lietuvoje platinamas Kinijos prekinio ženklo „Tanix" gamintojo „Oranth" projektuojamas ir gaminamas multimedijos produktas, skirtas televizijos transliacijoms žiūrėti internetu.

Atlikus tyrimą nustatyta, kad pateiktame priedėlyje naudojama 7-tos kartos „Android 7.1.2" OS, kurios branduolio versija „3.14.29". Verta pažymėti, kad standartinė „Android 7.1.2" OS komplektuojama su naujesniu – „4.4" versijos branduoliu, todėl galima teigti, kad priedėlyje naudojamas specializuotas branduolys, skirtas konkretaus gaminio elektroninės elementinės bazės funkcionalumui užtikrinti. Naujausia „Android" OS yra 9-tos kartos, todėl įrenginys, kurio sisteminis pagrindas dviem kartomis atsilieka nuo dabartinės versijos, kelia abejonių dėl jo naudojamų saugumo sprendimų efektyvumo siekiant užkirsti kelią šiuolaikinėms kibernetinio saugumo rizikoms.

Atgal į turinį

Remiantis viešos pažeidžiamumų bibliotekos (angl. *Common Vulnerabilities and Exposures, CVE*) duomenimis, „Android 7.1.2" turi 433 įvairaus lygio kibernetinio saugumo spragas, kurių dalis leidžia perimti įrenginio valdymą nuotoliniu būdu. Perėmus valdymą, įrenginys gali būti panaudotas vartotojo tinklo sekimo procesams inicijuoti, dalyvauti formuojant kibernetines atakas.

Grafinės aplinkos funkcionalumas realizuotas 2016 m. sukurtu „Kodi 16.1" versijos programiniu paketu, kuris nebepalaikomas ir turi žinomų programinių saugumo spragų.

Tyrimo metu buvo aptikta prisijungimo prie 440 IP adresų, kurie išsidėstę 46 šalyse. Priedėlis kreipėsi į 5 Lietuvoje registruotus IP adresus. Iš nustatytos visos IP adresų imties 57 priklauso Rusijos Federacijoje registruotiems juridiniams asmenims: „Rostelecom" – 10 adresų, „YANDEX LLC" – 6 adresai, „JSC ER-Telecom Holding" – 4 adresai, „MnogoByte LLC" – 3 adresai, „PvimpelCom" – 3 adresai, „MnogoByte LLC" – 3 adresai, „Cronyx Plus Ltd." – 2 adresai, „2COM Co Ltd." – 2 adresai, „AVK-computer Ltd." – 1 adresas, „CDN-video LLC" – 2 adresai, „Start LLC" – 2 adresai, „CJSC Rascom" – 1 adresas, „CJSC SibTransTelecom" – 1 adresas, „CJSC TransTeleCom" – 1 adresas, „Ddos-guard Ltd." – 1 adresas, „Domain names registrar REG. RU, Ltd." – 1 adresas, „Fast Link Ltd." – 1 adresas, „Fly Telecom LLC" – 1 adresas, „Hosting Operator eServer. ru Ltd." – 1 adresas, „Iskratelecom CJSC" – 1 adresas, „LLC GlobalTelecomStroy" – 1 adresas, „LLC Multi-service" – 1 adresas, „LLC SETEL" – 1 adresas, „LLC Sip nis" – 1 adresas, „MTS PJSC" – 1 adresas, „National Telecom, CJSC" – 1 adresas, „OAO ASVT" – 1 adresas, „OOO Istranet" – 1 adresas, „OOO Trivon Networks" – 1 adresas, „Pskovline Ltd." – 1 adresas, „Quartz Telecom LLC" – 1 adresas, „RTK-Volga-Ural LLC" – 1 adresas, „Teleskan-Intercom Ltd." – 1 adresas.

Nustatyta, kad priedėlis vykdo kreipinius į IP adresus, registruotus ir šiose šalyse: Armėnijoje – į 1 adresą, Australijoje – į 5 adresus , Baltarusijoje – į 1 adresą, Belgijoje – į 4 adresus, Brazilijoje – į 1 adresą, Bulgarijoje – į 2 adresus, Kanadoje – į 10 adresų, Čilėje – į 1 adresą, Kinijoje – į 5 adresus, Čekijoje – į 5 adresus, Danijoje – į 2 adresus, Suomijoje – į 2 adresus, Pracūzijoje – į 28 adresus, Sakartvele – į 1 adresą, Vokietijoje – į 18 adresų, Graikijoje – į 1 adresą, Honkonge – į 2 adresus, Vengrijoje – į 5 adresus, Airijoje – į 5 adresus, Izraelyje – į 1 adresą, Italijoje – į 4 adresus, Japonijoje – į 4 adresus, Kazachstane – į 1 adresą, Kuveite – į 1 adresą, Latvijoje – į 2 adresus, Malaizijoje – į 1 adresą, Maroke – į 1 adresą, Nyderlanduose – į 25 adresus, Naujojoje Zelandijoje – į 1 adresą, Norvegijoje – į 3 adresus, Lenkijoje – į 10 adresų, Portugalijoje – į 2 adresus, Moldovoje – į 1 adresą, Rumunijoje – į 1 adresą, Slovėnijoje – į 3 adresus, Pietų Korėjoje – į 11 adresų, Ispanijoje – į 3 adresus, Švedijoje – į 6 adresus, Šveicarijoje – į 2 adresus, Taivane – į 1 adresą, Turkijoje – į 2 adresus, Ukrainoje – į 18 adresų, Junginiuose Arabų Emyratuose – į 1 adresą, Jungtinėje Karalystėje – į 22 adresus, Jungtinėse Amerikos Valstijose – į 151 adresą.

Dalis priedėlio programų turiniui perduoti naudoja *AceStream* būdą, pagrįstą P2P (angl. *Peer-to-peer*) tinklo modeliu, kuriame keitimasis informacija vyksta tiesiogiai tarp vartotojų – vartotojai vaizdo turinį (ar jį įprasminančius duomenis) siunčiasi vienas iš kito, įsitraukdami į žiūrimo turinio platinimą.

Atkreiptinas dėmesys į tai, kad priedėlio siunčiamos užklausos gali būti registruojamos jas aptarnaujančių sistemų, taip nustatant paties vartotojo IP adresą ir identifikuojant užklausas formuojančius įrenginius. Svarbus aspektas, kad priedėlis siunčia užklausas į šalis, kuriose netaikomas Bendrasis duomenų apsaugos reglamentas. Dėl šios priežasties veikiant priedėliui galimai sukurtų (ir (ar) infrastruktūroje dalyvaujančių) funkcinių vartotojų asmens duomenų saugumo lygis yra sunkiai apibrėžiamas.

05

INFORMACINĖS ATAKOS

Informacinės atakos

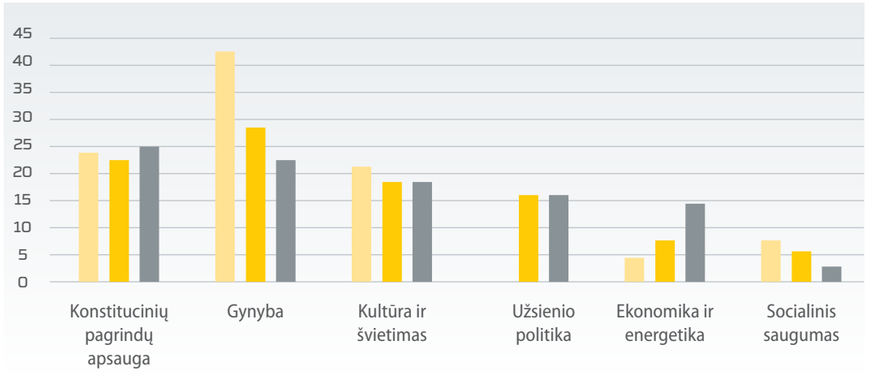
- Lietuvos valstybingumas, nepriklausomybė ir demokratijos principai pastaruosius keletą metų yra tapę vienais svarbiausių šaliai nedraugiškos žiniasklaidos taikinių.
- Nustatyti 2 890 Lietuvai nedraugiškų informacinės veiklos atvejų, ketvirtis jų – konstitucinių pagrindų apsaugos srityje.

Lietuvos kariuomenės Strateginės komunikacijos departamento duomenimis, 2019 metais dezinformacijos intensyvumo lygmuo Lietuvoje savo apimti bei turiniu išlaikė panašų lygį kaip ir ankstesniais metais. Pagrindiniu dezinformacijos šaltiniu išliko šalių, nepriklausančių Šiaurės Atlanto sutarties organizacijai (toliau – NATO) ir ES, bei nevalstybinių veikėjų vykdyta veikla, nukreipta prieš strateginius šalies tikslus ir demokratijos įrankius: Lietuvos narystę NATO ir ES, nacionalinių gynybos pajėgumų stiprinimą, šalies politinę santvarką, dvišalių ir daugiašalių santykių stiprinimą, pasitikėjimą valstybės institucijomis, teismų sistemą, šalies energetinį savarankiškumą, socialinę ir ekonominę gerovę bei istorinę atmintį. 2019 m. Lietuvos informacinėje erdvėje iš viso buvo nustatyta 2 890 žalingos informacinės veiklos atvejų (15 proc. daugiau nei 2018 m., vidutiniškai apie 241 atvejį per mėnesį), iš kurių daugiau nei 2/3 buvo inicijuojami ir vykdomi trečiųjų šalių.

Stebimu laikotarpiu išaugo rezonansinių daugiasluoksnių (angl. *multi-layered)* informacinių atakų, t. y. atakų, susidedančių iš kibernetinių ir informacinių elementų, skaičius. Šios atakos pasižymėjo pažangesniais techniniais ir turinio apipavidalinimo sprendimais, sudėtingesniu operaciniu veikimu, šio tipo išpuoliams vykdyti buvo skiriami didesni nei įprastai informaciniai ištekliai, technologiniai ir fiziniai pajėgumai. Pagrindiniu dezinformacijos veiksniu išliko Kremliaus režimo kontroliuojamos žiniasklaidos priemonės, skelbusios ir platinusios informaciją, neatitinkančią Lietuvos Respublikos visuomenės informavimo įstatymo nuostatų. Buvo formuojamas Lietuvos, kaip priešiškos ir nepatikimos valstybės, įvaizdis, nevengta

karo ir tautinės neapykantos skatinančio turinio, naudoti neskaidrūs turinio konstravimo bei apgaulės elementai: falsifikuoti faktai, tikslingai iškraipyti viešųjų asmenų pasisakymai, komentarai ar pranešimai spaudai, vaizdo redagavimo priemonėmis sufabrikuota vizualinė medžiaga, prisidengta kitų asmenų arba institucijų tapatybėmis. Neigiamos informacijos srautas koreliavo su reikšmingais įvykiais užsienio politikoje ir šalies viduje, kuriuos Lietuvai nedraugiški informacijos šaltiniai siekė išnaudoti formuodami neigiamą šalies įvaizdį Vakaruose, bei skatino tarpusavio susipriešinimą Lietuvos visuomenėje.

Konstitucinių pagrindų apsaugos srityje neigiamos informacijos srautas sudarė ketvirtadalį visų 2019 m. fiksuotų atvejų. Skelbiant nuosprendį Sausio 13-osios įvykių byloje, prieš Lietuvos teisinę sistemą ir visuomenės istorinę atmintį buvo vykdoma intensyvi dezinformacinė veikla. Gynybos srityje neigiamos informacijos srautas siekė 23 proc.: buvo siekiama mažinti šalies gyventojų pasitikėjimą šalies gynybos politika ir santykiais su NATO sąjungininkais, taip pat diskredituoti šalies nacionalinių gynybinių pajėgumų stiprinimą regione. Žalingos informacijos srautas gynybos sektoriuje aktyvėjo Lietuvai minint narystės NATO 15-ąsias metines, gegužę Baltijos jūroje vykstant NATO karinėms pratyboms „Spring Storm 2019“.

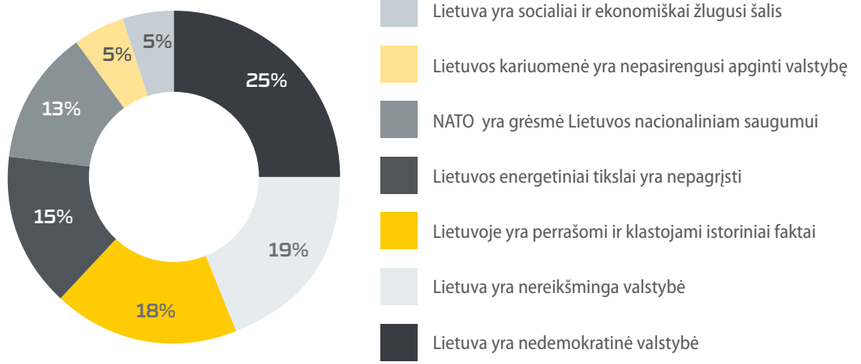


30 pav. Neigiamos informacijos koncentracija strateginių sričių atžvilgiu 2017-2019 m.

Kultūros ir švietimo srityje iš viso identifikuoti 522 (20 proc.) neigiamos informacinės veiklos atvejai. Kilus diskusijoms dėl Antrojo pasaulinio karo įvykių interpretavimo, buvo kurstomi ginčai dėl demokratijos, žmogaus teisių padėties užtikrinimo Lietuvoje, tuo suskubo pasinaudoti Lietuvai nedraugiškos žiniasklaidos priemonės – buvo siekiama formuoti Lietuvos, kaip ksenofobinės, diskriminacinės ir antisemitinės valstybės, įvaizdį tarptautinėje arenoje.

Užsienio politikos sektoriuje informacijos aktyvumą lėmė nacionaliniai ir tarptautiniai įvykiai: Lietuvos Respublikos prezidento Gitano Nausėdos susitikimas su NATO generaliniu sekretoriumi Jensu Stoltenbergu, JAV 1-osios kavalerijos divizijos bataliono dislokavimas Pabradėje bei vykusios karinės pratybos: „Baltijos saugotojas“ (*Baltic Protector 2019*), „Geležinis Vilkas“ (*Iron Wolf 2019*) ir „BALTOPS“.

Atgal į turinį



31 pav. Pagrindiniai 2019 m. Lietuvos interneto vartotojams skirti žalingos informacijos naratyvai.

Siekdami padidinti žalingos informacijos pasiekiamumą, suinteresuoti veikėjai vykdė neteisėtus kibernetinius įsilaužimus į interneto puslapius, naudodamiesi kitų asmenų ar institucijų duomenimis bei atvirkščiai – provokaciniu turiniu, interneto vartotojus skatinusiu atsidaryti konkretų dokumentą ar nuorodą, buvo maskuojami kibernetiniai veiksmai, kuriais siekta tiksliniams vartotojams daryti žalą bandant užvaldyti jų įrenginius ar juose įdiegti kenksmingą programinę įrangą.

Viena ryškiausių informacinių kibernetinių atakų vykdyta prieš „Delfi“ žurnalistą, kai prisidengus jo vardu buvo išsiųstos užklausos Lietuvos bei užsienio šalių institucijoms ir naujienų agentūroms pranešant apie tariamus NATO sąjungininkų viešosios tvarkos pažeidimus Lietuvoje. Kita informacinė ataka vykdyta prieš Kauno žydų bendruomenę: prisidengus šios bendruomenės pirmininko tapatybe atsakingoms tarnyboms buvo išplatinti melagingi pranešimai apie Lietuvoje dislokuoto NATO priešakinio bataliono karių Kaune tariamai įvykdytą antisemitinį nusikaltimą. Kibernetinė informacinė ataka vykdyta prieš KAM vadovybę paskleidus tikrovės neatitinkančią informaciją apie ministro gautą didelės vertės kyšį iš Jungtinių Amerikos Valstijų pareigūnų. Šios atakos metu įsilaužus į mažiausiai kelis interneto puslapius buvo paskelbtas ministrą diskredituojantis turinys, taip pat sukurtos nuorodos į specialiai šiam atvejui sumaketuotą ir Lietuvos Respublikos Specialiųjų tyrimų tarnybos interneto puslapį imitavusį portalą, kuriame buvo įkeltas sufabrikuotas melagingą informaciją patvirtinantis pranešimas.

06

IŠVADOS IR REKOMENDACIJOS

Išvados

01 Lietuvoje nepakankamai vertinamas kibernetinių incidentų poveikis.

Lietuvos Respublikos Vyriausybės nutarimu Nr. 818 patvirtintas kibernetinių incidentų klasifikavimas pagal poveikį leido NKSC diversifikuoti ir detalizuoti kibernetinių incidentų nustatymo procesą. Dėl šios priežasties, palyginti su ankstesniu laikotarpiu, NKSC specialistai apdorojo beveik tris kartus didesnį tokio pobūdžio kibernetinių incidentų skaičių – 3 241. Incidentų priskyrimas pagal poveikį leido nustatyti kitą iššūkį – jų efektai nepakankamai įvertinami. Dažniausiai yra manoma, kad kibernetiniai incidentai yra nereikšmingi. Dėl šios priežasties susiduriama su kitomis problemomis, kurias NKSC fiksavo savo veikloje. Naudotojai Lietuvoje dar nėra linkę naudoti elementarių kenkimo PĮ aptikimo priemonių – Lietuvos IP rėžyje labiausiai paplitusiai kenkimo PĮ aptikti nėra reikalingos komercinės priemonės. Kibernetinio saugumo subjektai taip pat dažniausiai pasikliauna tipiniais kibernetinių incidentų nustatymo įrankiais, nors pagal grėsmių indikatorius NKSC techninės kibernetinio saugumo priemonės kenkimo PĮ atvejų aptinka vis mažiau. Krašto apsaugos sistemoje analizuojamas platesnis metaduomenų spektras (ne tik sesijos lygmenyje) leido aptikti kur kas didesnį kenkimo PĮ atvejų skaičių, palyginus su kitais ypatingos svarbos paslaugų sektoriais. Kibernetinių incidentų poveikio nuvertinimas gali turėti reikšmingas pasekmes. Interneto svetainė „https://kaunas.kasvyksta.lt/“ 2019 m. net kelis kartus buvo išnaudota kibernetinėms informacinėms atakoms vykdyti. Kur kas didesnį rezonansą sukėlęs įvykis – 2019 m. UAB „Kauno vandenys“ kibernetinis incidentas. Nepakankamas dėmesys kibernetinių grėsmių atžvilgiu galėjo nulemti, kad duomenis šifruojantis virusas dėl nepakankamo technologinio ir administracinio tinklo atskyrimo būtų sutrikdęs ir vandens tiekimą Kauno mieste.

02 Viešajame sektoriuje interneto svetainių kibernetinio saugumo būklė gerėja, tačiau bendrąja prasme interneto svetainių kibernetinio saugumo rizikos išlieka reikšmingos.

NKSC 2019 m. betarpiškai bendraudamas su viešojo sektoriaus interneto svetainių savininkais padidino saugių interneto svetainių skaičių 11 proc. Tačiau įvertinus bendrą Lietuvos svetainių TVS būklę – identifikuotų neatnaujintų kiekis augo iki 63 proc. NKSC papildomai įvertino galimybę prisijungti prie visų „.lt“ interneto svetainių valdymo paskyros – nustatyta 37 proc. tokių svetainių. Papildomai NKSC specialistai viešajame sektoriuje aptiko vieno konkretaus gamintojo TVS su kritišku *cross-site scripting* pažeidžiamumu. NKSC vertinimu, kol svetainių savininkai nenusimatys lėšų interneto svetainių palaikymui, laiku nevykdys TVS ir įskiepių atnaujinimų, neįdiegs svetainių ugniasienių, patikimų kriptografinių priemonių, tol interneto svetainių pažeidžiamumų grėsmė išliks reikšminga.

03 **Formalus kibernetinio saugumo reikalavimų įgyvendinamas didėja, tačiau kyla keblumų diegiant praktines kibernetinių incidentų rizikų kontrolės priemones.**

Vykdant kibernetinio saugumo reikalavimų įgyvendinimo stebėseną NKSC fiksavo proveržį YSII valdytojų reikalavimų įgyvendinime. 2019 m. išplėtota NKSC patikrinimų vykdymo kompetencija leido konstatuoti faktą – reikalavimai dažnai įgyvendinami formaliai, neįdiegiant faktinių rizikos kontrolės priemonių. Formali atitiktis ir sporadiškas reikalavimų įgyvendinimas apsunkina subjektų gebėjimus stebėti anomalijas, aptikti kibernetinius incidentus ir, svarbiausia, užtikrinti veiklos tęstinumą kritinių kibernetinių incidentų atveju.

04 **Naudotojai gali būti paveikti kibernetinių incidentų neatsižvelgiant į ryšių ir informacinių sistemų pažeidžiamumų išnaudojimą ar kenkimo programinės įrangos funkcionalumą.**

NKSC vykdyti techninės ir programinės įrangos tyrimai leido konstatuoti faktą, kad naudotojai gali nukentėti suteikdami programinei įrangai perteklines prieigos teises prie duomenų ar įrenginių funkcionalumo arba gali įsigyti programinę ar techninę įrangą, kurios duomenys gali būti perduoti į trečiąsias šalis, neužtikrinančias duomenų apsaugos.

05 **Hibridinės atakos sukelia didžiausią rezonansą visuomenėje. Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos ir toliau fiksavo hibridinius incidentus, susidedančius iš informacinės ir kibernetinės dalies.**

Kibernetinio saugumo požiūriu incidentai nebuvo rafinuoti, tačiau iš informacinės pusės buvo siekiama rezonanso eskaluojant ir didinant melagingos informacijos sklaidą.

Atgal į turinį

Rekomendacijos

NKSC, atsižvelgdamas į ataskaitoje aprašytas kibernetines grėsmes, teikia bazines kibernetinių rizikų valdymo rekomendacijas (32 pav.). Atkreipiamas dėmesys, kad rekomendacijos yra bendros. Detalesnes rekomendacijas NKSC teikia savo interneto svetainėje, joje taip pat galima rasti nemokamus įrankius pažeidžiamumams nustatyti.[14]

32 pav. Bazinės kibernetinių rizikų valdymo rekomendacijos.

Socialinės inžinerijos rizikų valdymo rekomendacijos		
Nr.	**Grėsmė**	**Rekomendacija**
1	**Naudotojas paspaus nuorodą, vedančią į kenkėjišką puslapį.**	Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar rodomas interneto svetainės adresas yra tikras, įsitikinti, kad adrese nėra įvelta gramatinių klaidų, adreso pavadinimas logiškas ir lengvai perskaitomas.
2	**Naudotojas įves savo slaptažodį suklastotoje interneto svetainėje.**	Įsitikinti, kad sesija su interneto svetaine yra šifruojama, t. y. naudojamas SSL sertifikatas (interneto svetainės adresas turi prasidėti „https“ žyma), naudoti kelių faktorių autentifikavimo įrankius (pavyzdžiui, slaptažodis, mobilusis įrenginys, piršto antspaudas).
3	**Naudotojas pats atskleis savo prisijungimo slaptažodžius piktavaliui.**	Naudoti mažiausiai dviejų faktorių autentifikavimą, saugoti savo prisijungimo slaptažodžius, jokiais būdais nelaikyti jų atviru tekstu darbo vietoje, kompiuteryje ar mobiliajame telefone.
4	**Naudotojas atliks piniginę perlaidą piktavaliams.**	Kritiškai vertinti reklamas internete ir elektroniniu paštu siunčiamuose laiškuose (ypač siūlomas dideles nuolaidas); prašymus atlikti pinigines perlaidas tikrinti kitais būdais, pavyzdžiui, pasitikslinti aplinkybes paskambinus telefonu.
5	**Naudotojas įdiegs kenkimo PĮ.**	Neatidarinėti dokumentų turinio, siunčiamų failų ir PĮ, kurie yra atsiųsti ar parsisiųsti iš nepatikimo šaltinio (pavyzdžiui, iš nelegalių PĮ platinimo šaltinių).
6	**Naudotojas pasiduos piktavalio manipuliacijoms.**	Neatlikti skubotų veiksmų, nepasiduoti emocijoms, detaliai išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą.

14 https://www.nksc.lt/rekomendacijos.html, https://www.nksc.lt/irankiai.html

Kenkimo PĮ rizikų valdymo rekomendacijos

7	**Pasinaudojęs pažeidžiamumu, piktavalis įdiegs kenkimo PĮ į RIS.**	Naudoti legalią OS ir PĮ, naudoti antivirusinę PĮ, ja profilaktiškai skenuoti duomenis įrenginyje, nedelsiant įdiegti naujus gamintojo PĮ atnaujinimus.
8	**Naudotojas parsisiųs kenkimo PĮ iš interneto šaltinių.**	Nesisiųsti failų iš nepatikimų šaltinių, naršyklėje įdiegti įskiepius kenkėjiškoms interneto svetainėms atpažinti, parsisiųstus įtartinus failus skenuoti antivirusine PĮ, tikrinti juos NKSC priemonėmis.[23]
9	**Kenkimo PĮ iš užkrėstos atminties laikmenos bus paleista automatiškai.**	Nesinaudoti nepatikimomis, nepatikrintomis atminties laikmenomis. Nuolat jas formatuoti, išjungti automatinį failų paleidimą, prieš atidarant laikmenoje esančius failus leisti antivirusinei PĮ nuskenuoti juos.
10	**Kenkimo PĮ užšifruos kompiuteryje esančius duomenis.**	Periodiškai daryti atsargines duomenų kopijas, jas saugoti kitame įrenginyje, atskirai nuo tos vietos, kurioje jos buvo padarytos. Svarbią informaciją laikyti atskiroje laikmenoje ar laikmenose, neturinčiose tiesioginės sąsajos su internetu (pavyzdžiui, išorinėje laikmenoje).
11	**Kenkimo PĮ sukurs piktavaliui prieigą prie konfidencialios informacijos.**	Šifruoti konfidencialią informaciją, jeigu būtina, apsaugoti ją saugiu slaptažodžiu. Informacijai perduoti naudoti kriptografines priemones, pavyzdžiui, elektroninių laiškų šifravimą.
12	**Kompiuteris bus užkrėstas per RIS tinklą.**	Įstaigose naudoti tinklo segmentavimą, keletą filtravimo priemonių (pavyzdžiui, tinklo ir darbo stoties ugniasienę), svarbias RIS atskirti fiziškai.

Interneto svetainių kibernetinių rizikų valdymo rekomendacijos

13	**Piktavalis prisijungia prie TVS per naudotojo ar administratoriaus paskyrą.**	Pakeisti interneto svetainės TVS administratoriaus ir naudotojų prisijungimo adresus, įgalinti prisijungimo galimybę pagal IP adresus, periodiškai keisti slaptažodžius, sudaryti ribotą bandymų prisijungti skaičių.
14	**Piktavalis išnaudoja interneto svetainės pažeidžiamumus.**	Įsigyjant svetainės programavimo paslaugas, pirkimo specifikacijoje įtraukti svetainės kodo patikrinimo pagal OWASP metodologiją reikalavimą. Nuolat atnaujinti TS OS, TVS ir susijusius įskiepius, nenaudoti nereikalingų TVS įskiepių, naudoti taikomųjų programų ugniasienę (angl. *web application firewall*), uždrausti nenaudojamus prievadus, pasitikrinti interneto svetainių pažeidžiamumus naudojantis viešai prieinamais įrankiais ir reguliariai tikrinti žurnalų įrašus (angl. *logs*), įdiegti „reverse Proxy“ sprendimą, kad piktavalis negalėtų identifikuoti TVS.
15	**Piktavalis į svetainę įdiegia kenkimo PĮ.**	Sukonfigūruoti ugniasienes taip, kad prie interneto svetainių TVS būtų galima jungtis tik iš patikimų IP adresų (sudaryti leidžiamų IP adresų sąrašą).
16	**Prieglobos paslaugų tiekėjas neužtikrina interneto svetainės kibernetinio saugumo priemonių.**	Perkant svetainės kūrimo, įdėjimo ir priežiūros paslaugas, į sutartį įtraukti reikalavimą paslaugų teikėjui, kad šis užtikrintų interneto svetainės kibernetinį saugumą, apsaugą nuo įsilaužimų, užtikrintų jos atitiktį Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams.
17	**Prisijungimo prie interneto svetainės metu perimama informacija, įsiterpiama į ryšio srautą, perimami vartotojų duomenys ir (ar) prisijungimo slaptažodžiai.**	Prieigai prie interneto svetainės naudoti HTTPS protokolą, tai užtikrins šifruotąjį ryšį. Tai viena efektyviausių interneto svetainių kibernetinio saugumo priemonių.
18	**Sutrikdomas prieinamumas prie interneto svetainės.**	Naudoti taikomųjų programų ugniasienę (angl. *Web application firewall*), užsisakyti didesnį pralaidumą, įsigyti papildomas. prevencines DDoS paslaugas, pavyzdžiui, iš interneto svetainės prieglobos teikėjo.

Elektroninių ryšių tinklų žvalgybos rizikų valdymo rekomendacijos

19	**Piktavalis identifikuoja aktyvias paslaugas ir įrenginius.**	Pakeisti įrenginių prievadus į rečiau naudojamus, išjungti nenaudojamus prievadus, įgalinti „reverse Proxy“, kad nebūtų įmanoma iš išorės identifikuoti aktyvių paslaugų ir techninės ar PĮ.

Techninės ar programinės įrangos patikimumo rizikų valdymo rekomendacijos

20	**Duomenų nutekėjimas ir (ar) paslaugų sutrikdymas.**	Rekomenduojama techninę ir PĮ įsigyti tik iš oficialių šaltinių ir tiekėjų, kurie veikia pagal Bendrojo duomenų apsaugos reglamento reguliavimą ir saugo duomenis NATO ar ES valstybėse, riboti techninės ar PĮ funkcionalumą ir informacijos bei paslaugų pasiekiamumą (pavyzdžiui, išmaniajame telefone išjungti galimybę įrašyti garsą, aktyvuoti kamerą, o organizacijoje – užkardyti bet kokią technologinio tinklo sąsają su internetu).
21	**Šnipinėjimas.**	Rekomenduojama įsigyti techninę ir PĮ iš šaltinių, kurie yra nepriekaištingos reputacijos ir nėra iškilusios rizikos dėl bendradarbiavimo su ne NATO ir ne ES užsienio žvalgybos tarnybomis.
22	**Nesankcionuota technologinio tinklo sąsaja su internetu.**	Suteikti ribotą rangovų prieigą prie RIS, vengiant suteikti nuotolinio prisijungimo prie RIS galimybę, stebėti ir audituoti komunikacijų žurnalinius įrašus.

23	**Prie įrenginio galima prisijungti su standartiniu slaptažodžiu.**	Pakeisti IoT, pasiekiamų internetu ar per „bluetooth“ sąsają, prisijungimo slaptažodžius į saugius.
24	**Prie įrenginio prisijungiama per neužkardytą pažeidžiamumą.**	Reguliariai atnaujinti IoT taikomąją ir PĮ.
25	**Piktavalis gali matyti saugomus slaptažodžius ir kitą neskelbtiną informaciją.**	IoT išjungti slaptažodžių išsaugojimo galimybę.
26	**Piktavalis gali perimti informaciją ar slaptažodžius įrenginių komunikacijos metu.**	Įsigyti ir naudoti įrenginius, kurių komunikacijos sesija yra šifruojama.
27	**Piktavalis pasinaudoja perteklinėmis įrenginių funkcijomis ir įgauna prieigą prie RIS.**	Jeigu yra galimybė, patikrinti, ar įrenginyje nėra perteklinio funkcionalumo (atvirų prievadų).
28	**Įrenginys komunikuoja su išore ir, galimas dalykas, yra nutekinama informacija.**	Prieš įsigyjant įrenginį, įsitikinti, ar jo gamintojas atitinka Bendrojo duomenų apsaugos reglamento reikalavimus, ar siunčiami duomenys yra saugomi ES teisės.
29	**Įsigyjamas nesaugus įrenginius.**	Vengti nežinomų gamintojų, kurių kilmės šalį ir patikimumą yra sudėtinga patikrinti.

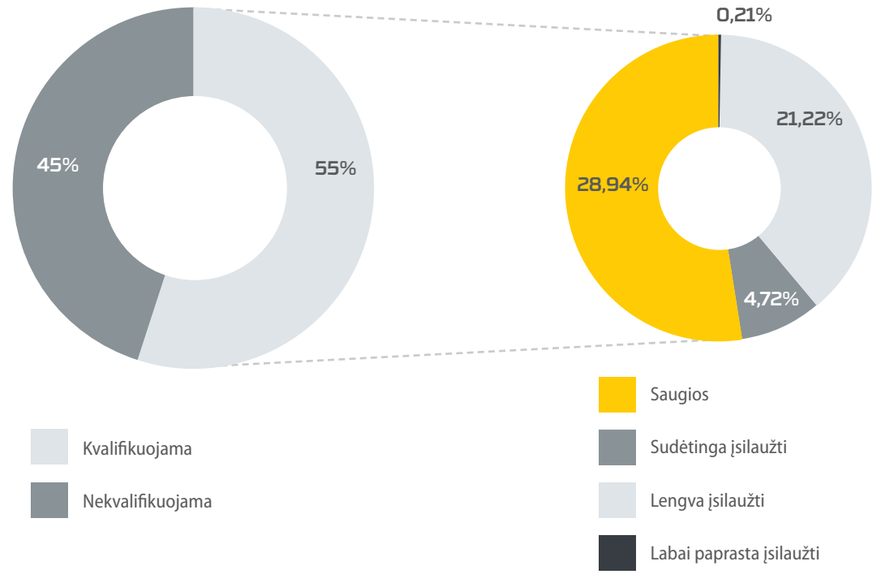
DDoS kibernetinių incidentų rizikų valdymo rekomendacijos

30	**Dėl išnaudotų resursų bus sutrikdytas RIS pasiekiamumas.**	Nuolat stebėti tarnybinių stočių, klasterių, aplikacijų ir duomenų bazių resursus, išskirti kritinius elementus, pagal poreikį vykdyti stebėjimą iš naudotojo perspektyvos (iš išorės), o prireikus – didinti pralaidumą, įsigyti papildomus resursus. Naudoti maršruto parinktuvus su *traffic-shaping* ir *rate-limiting* funkcionalumu.
31	**Dėl tiesioginio DDoS kibernetinio incidento bus sutrikdytas RIS pasiekiamumas.**	Įsigyti *anti-DDoS* paslaugas iš interneto paslaugų teikėjų. Įsigyti ugniasienes su *anti-DDoS* funkcionalumu, naudoti žiniatinklio aplikacijų ugniasienes. Esant galimybei naudoti įsilaužimo aptikimo ir užkardymo sistemas.
32	**Infrastruktūros išnaudojimas atakoms vykdyti (pvz., DDoS atakų sustiprinimas).**	Stebėti tinklo srautą (užklausos siuntėjo ir gavėjo IP adresus ir prievadus), analizuoti žurnalinius įrašus, siekiant nustatyti, ar infrastruktūra nėra išnaudojama DDoS atakoms. Nuolat atnaujinti PĮ.

Priedai

Viešojo sektoriaus interneto svetainių kibernetinio saugumo būklės vertinimas

Iki 2018 m. viešojo sektoriaus interneto svetainių būklė buvo vertinama pagal atskirų pažeidžiamumų išnaudojimo galimybes, neatsižvelgiant į bendrą svetainės pažeidžiamumo lygį. 2019 m. NKSC holistiškai vertino viešojo sektoriaus interneto svetainių kibernetinį saugumą pagal pažeidžiamumus, tenkančius vienam domenui. Pavyzdžiui, interneto svetainė, turinti du pažeidžiamumus pagal skirtingas jų išnaudojimo galimybes, buvo vertinama pagal lengviausiai išnaudojamo pažeidžiamumo grėsmę (pavyzdžiui, jei svetainė turi du pažeidžiamumus, kurių išnaudojimo kvalifikacija yra „lengva įsilaužti“ ir „sunku įsilaužti“, tai kvalifikacija yra traktuojama pagal „lengva įsilaužti“). NKSC taip pat įvertino, kad kai kurie pažeidžiamumai nėra kvalifikuojami – nėra aiškios informacijos ar jiems išnaudoti pakanka tipinių priemonių, ar yra būtinos ekspertinės žinios. Pagal šį metodą NKSC perskaičiavo 2018 m. tyrimų informaciją (33 pav.).



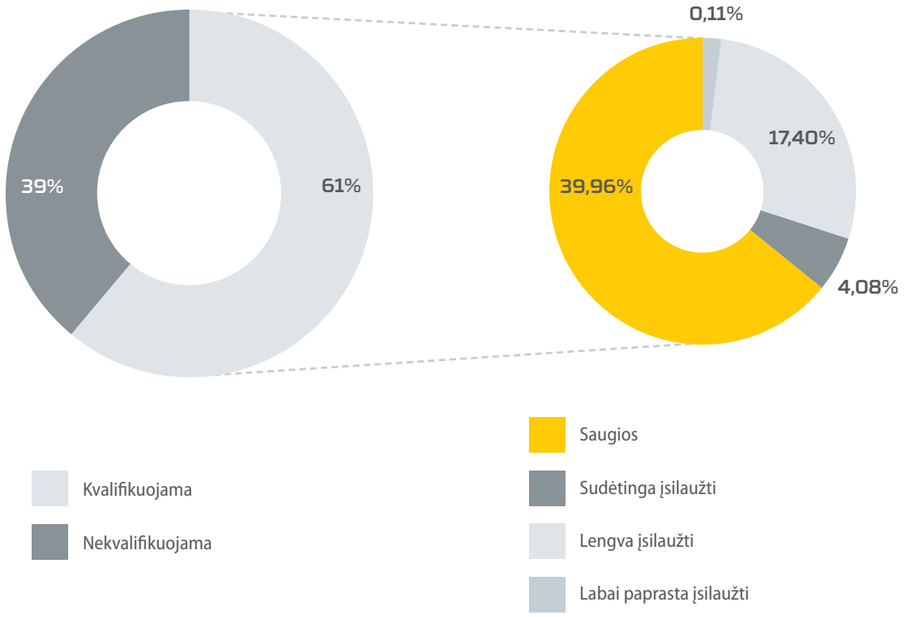
33 pav. Viešojo sektoriaus interneto svetainių kibernetinio saugumo būklė pagal domeno pažeidžiamumų kvalifikavimą 2018 m.[15]

Pagal atnaujintą interneto svetainių kibernetinio saugumo būklės vertinimą NKSC nustatė, kad 2019 m. padaugėjo interneto svetainių, kurių pažeidžiamumus yra įmanoma kvalifikuoti, o bendras saugių svetainių skaičius išaugo iki 40 proc. (34 pav.).

[15] **Labai paprasta įsilaužti** – įsilaužti nereikalingos techninės žinios ar ypatingi programavimo įgūdžiai. Sėkmingai atakai įvykdyti nesudėtingai atkuriami reikiami algoritmai, internete lengvai randamos reikalingų veiksmų instrukcijos.

Lengva įsilaužti – įsilaužti reikalingi įgūdžiai ir žinios, dažniausiai publikuojamos uždarose grupėse.

Sudėtinga įsilaužti – įsilaužti reikalingos kvalifikuotų specialistų, dažnai ne vieno atakuotojo, žinios, nes pažeidžiamumai dar nėra viešai publikuojami.



34 pav. Viešojo sektoriaus interneto svetainių kibernetinio saugumo būklė pagal domeno pažeidžiamumų kvalifikavimą 2019 m.

Atgal į turinį

Lietuvos Respublikos Krašto apsaugos ministerija,
Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos
ir Lietuvos kariuomenės Strateginės komunikacijos departamentas
Nacionalinė kibernetinio saugumo būklės ataskaita, 2019
Kalbos redaktoriai: Rasa Sirvydienė, Gintautas Pučinskas
Tiražas 500 vnt. Užsakymas Nr. GL-14
Išleido Lietuvos Respublikos krašto apsaugos ministerija,
Totorių g. 25, LT-01121 Vilnius, www.kam.lt.
Maketavo Krašto apsaugos ministerijos bendrųjų reikalų departamento
Vaizdinės informacijos skyrius, Totorių g. 25, LT-01121 Vilnius.
Spausdino Lietuvos kariuomenės Karo kartografijos centras,
Muitinės g. 4, Domeikava, LT-54359 Kauno r.