NACIONALINIS
KIBERNETINIO
SAUGUMO CENTRAS
PRIE KRAŠTO
APSAUGOS
MINISTERIJOS

NACIONALINIO KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

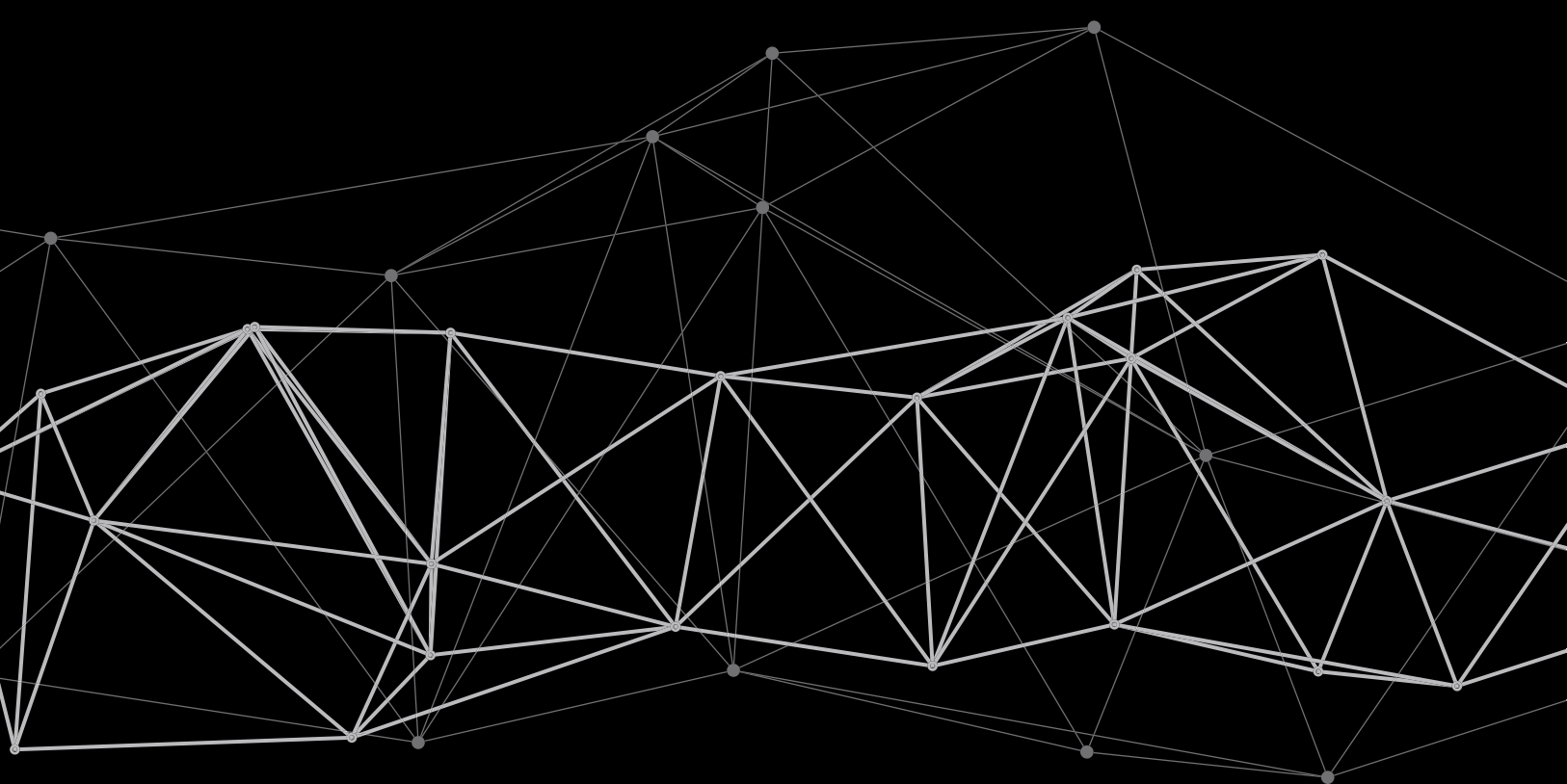
2018

MINISTRY OF NATIONAL DEFENCE
REPUBLIC OF LITHUANIA

2019, Vilnius

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

ISBN 978-609-412-168-5



TURINYS

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

DDoS – paskirstyto atsisakymo aptarnauti kibernetinė ataka

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

IT – informacinės technologijos

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

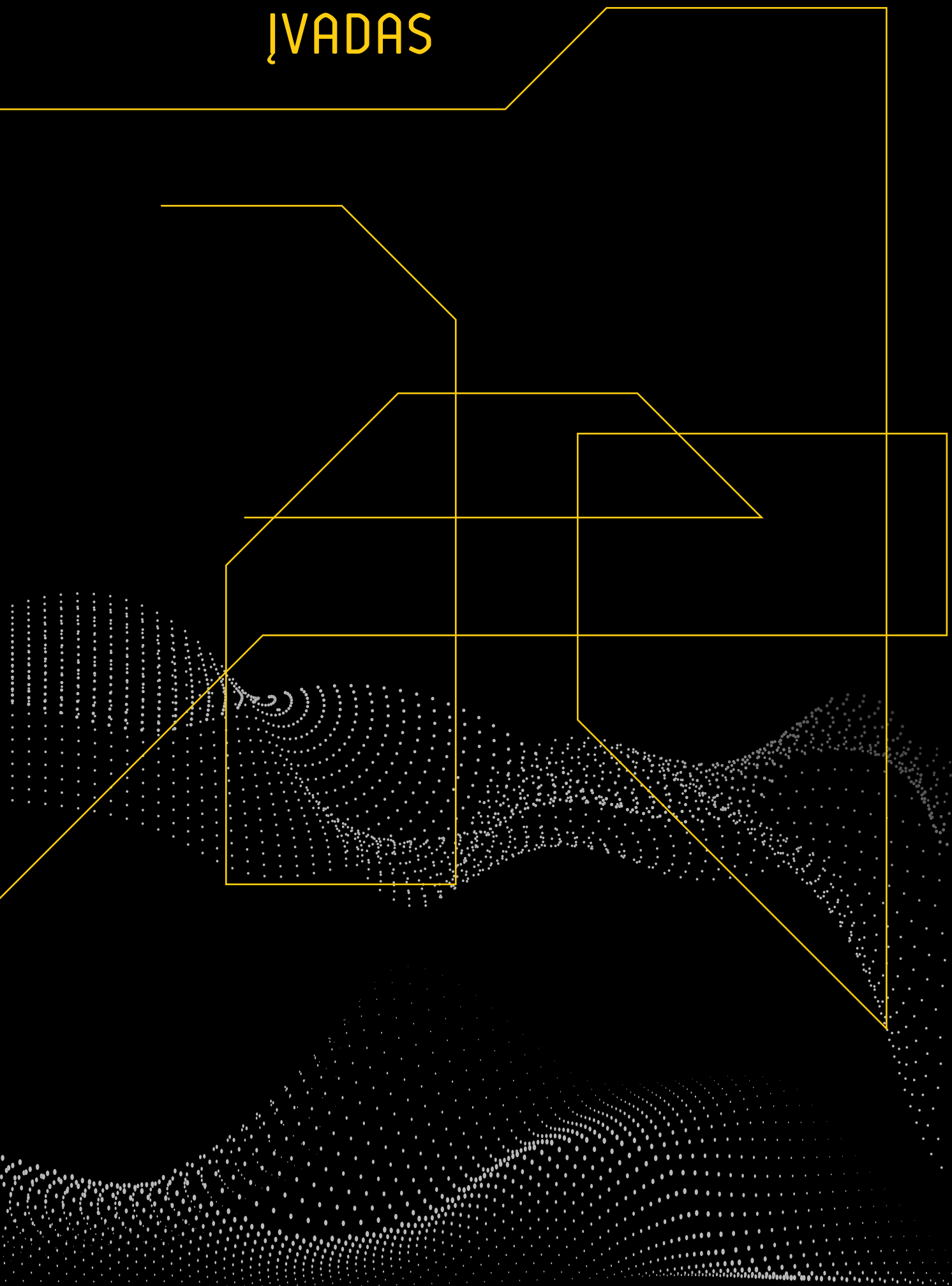
TLD – (angl. top level domain) aukščiausio lygmens domeno vardų sistema (pavyzdžiui, kuri baigiasi galūne „.lt“)

TS – tarnybinė stotis (serveris)

TVS – turinio valdymo sistema

VII – valstybės informaciniai ištekliai

ĮVADAS



Kibernetinio saugumo požiūriu 2018 m. Lietuvoje buvo gausu įvykių. 2017 m. gruodžio 19 d. Lietuvos Respublikos Seimui priėmus Kibernetinio saugumo įstatymo pataisas, buvo konsoliduoti Ryšių reguliavimo tarnybos CERT-LT[1], Vyriausybinių ryšių centro prie Krašto apsaugos ministerijos ir Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) pajėgumai. Nuo 2018 m. sausio 1 d. NKSC tapo pagrindine Lietuvos kibernetinio saugumo institucija, atsakinga už vientisą kibernetinių incidentų valdymą, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną ir kontrolę, ypatingos svarbos informacinės infrastruktūros (toliau – YSII) valdytojų ir kitų kibernetinio saugumo subjektų kibernetinio saugumo užtikrinimą. Visapusiškas dėmesys kibernetinio saugumo klausimams, bendros politikų ir ekspertų pastangos leido nacionaliniu mastu sutelkti gebėjimus, nustatyti aiškią kibernetinio saugumo stiprinimo kryptį ir konkrečius veiksmus, kuriuos reikia atlikti kelerių metų laikotarpiu. Lietuvos pastangos kibernetinio saugumo srityje neliko nepastebėtos – Lietuva yra tarp lyderių pagal nacionalinį kibernetinio saugumo indeksą (NCSI)[2].

Naujas kibernetinio saugumo gaires nustatė 2018 m. patvirtinta Lietuvos kibernetinio saugumo strategija, kuri formuoja vieningą kibernetinio saugumo stiprinimo kryptį iki 2023 m. Bendrasis duomenų apsaugos reglamentas paskatino subjektus aktyviau valdyti kibernetines rizikas, susijusias su asmens duomenų apsauga. Lietuva ir tarptautiniu mastu įsitraukė į gebėjimų užkardyti kibernetines grėsmes ugdymą. 2018 m. Lietuva pradėjo įgyvendinti dar 2017 m. inicijuotą Europos Sąjungos nuolatinio struktūrizuoto bendradarbiavimo projektą „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“. Prie kibernetinio saugumo Lietuvoje gerinimo svariai prisidėjo kibernetinio saugumo subjektų (ypač YSII valdytojų) organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas, NKSC stebėsenos pajėgumų plėtra.

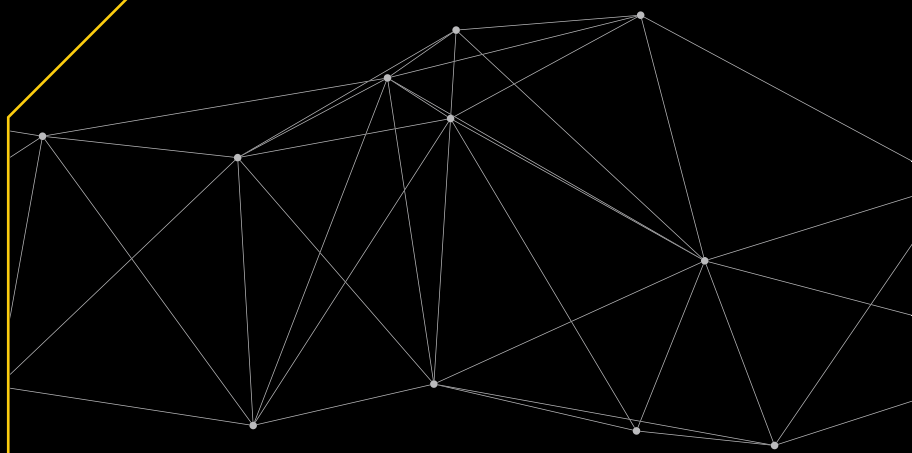
Technologijų plėtra, IoT populiarumas ne tik palengvina kasdienybę, tačiau taip pat sukuria naujus iššūkius. Antivirusinė PĮ, užkardos ir kitos kibernetinį saugumą turinčios užtikrinti priemonės nepajėgios užkardyti visų kibernetinių grėsmių. Technologiniai sprendimai negali visiškai apsaugoti ir neapsaugo nuo naujų pažeidžiamumų ir būdų, kaip juos galima išnaudoti, atsiradimo. Žmonių sąmoningumo, IT raštingumo didinimas bei kritinis mąstymas ir toliau lieka pagrindinis būdas kovoti su kibernetinėmis grėsmėmis. NKSC, siekdamas aktualizuoti kibernetinio saugumo klausimus ir informuoti visuomenę apie kibernetinio saugumo būklę ir grėsmes, teikia trečią nacionalinio kibernetinio saugumo būklės ataskaitą. Šioje ataskaitoje naudotojams yra pateikiamos pagrindinės rekomendacijos, kaip valdyti su kibernetinėmis grėsmėmis susijusias rizikas.

---

[1] CERT-LT – nacionalinė informacinių technologijų ekspertų grupė, pasirengusi reaguoti į kibernetinius incidentus nacionaliniu mastu (angl. Computer Emergency Response Team)

[2] Nacionalinis kibernetinio saugumo indeksas (NCSI – National Cyber Security Index), https://ncsi.ega.ee/

SANTRAUKA



Nacionalinio kibernetinio saugumo būklės ataskaita yra parengta remiantis NKSC valdoma informacija apie kibernetinius incidentus Lietuvoje, kibernetinio saugumo subjektų ir Lietuvos kariuomenės Strateginės komunikacijos departamento surinkta ir pateikta informacija. Toliau pateikiama santrauka apie esminius šios ataskaitos elementus.

Ilgą laiką augusi kibernetinių incidentų statistika 2018 m. mažėjo. Lietuvoje užregistruota 53 183 kibernetinio saugumo incidentai, t. y. 3 proc. mažiau nei ankstesniais metais. Tačiau išaugo kibernetinių incidentų sudėtingumas, atakos tampa vis labiau rafinuotos, o jas ištirti automatizuotomis priemonėmis yra neįmanoma. NKSC ištyrė 914 didelės ir vidutinės reikšmės kibernetinių incidentų, o tai 41 proc. daugiau nei 2017 m. Be to, 2018 m. registruota 21 proc. daugiau incidentų, įvykusių dėl įrenginių saugumo spragų, kas yra susiję su didėjančiu IoT įrenginių naudojimu.

2018 m. daugiausiai kenkimo programinės įrangos aptikta valstybės valdymo (39 proc.), energetikos (20 proc.) ir užsienio reikalų ir saugumo politikos (19 proc.) sektoriuose. Kenkėjiškos kibernetinės veiklos tendencija išlieka grėsminga, nes taikomasi į tuos kritinius sektorius, nuo kurių labiausiai priklauso Lietuvai svarbios paslaugos.

Socialinės inžinerijos metodais pagrįstų bandymų įsiskverbti į RIS 2018 m. NKSC užfiksavo 25 proc. daugiau nei 2017 m. Sukčiai, apsimesdami organizacijų vadovais ir naudodami socialinės inžinerijos metodus, ir toliau bando priversti organizacijų darbuotojus atlikti pinigines perlaidas. Piktavaliai taip pat bando išvilioti naudotojų pinigus siūlydami įsigyti prekes suklastotose interneto svetainėse. Socialinės inžinerijos metodai taip pat naudojami siekiant į organizacijų ir naudotojų kompiuterius įdiegti kenkimo PĮ.

Pernai NKSC atliko visos Lietuvos interneto svetainių (.lt) kibernetinio saugumo patikrinimus. Deja, net 52 proc. iš 52 000 interneto svetainių, turinčių TVS, Lietuvoje yra pažeidžiamos. Labiausiai pažeidžiamos interneto svetainės, turinčios „Wordpress" ir „Joomla" TVS.

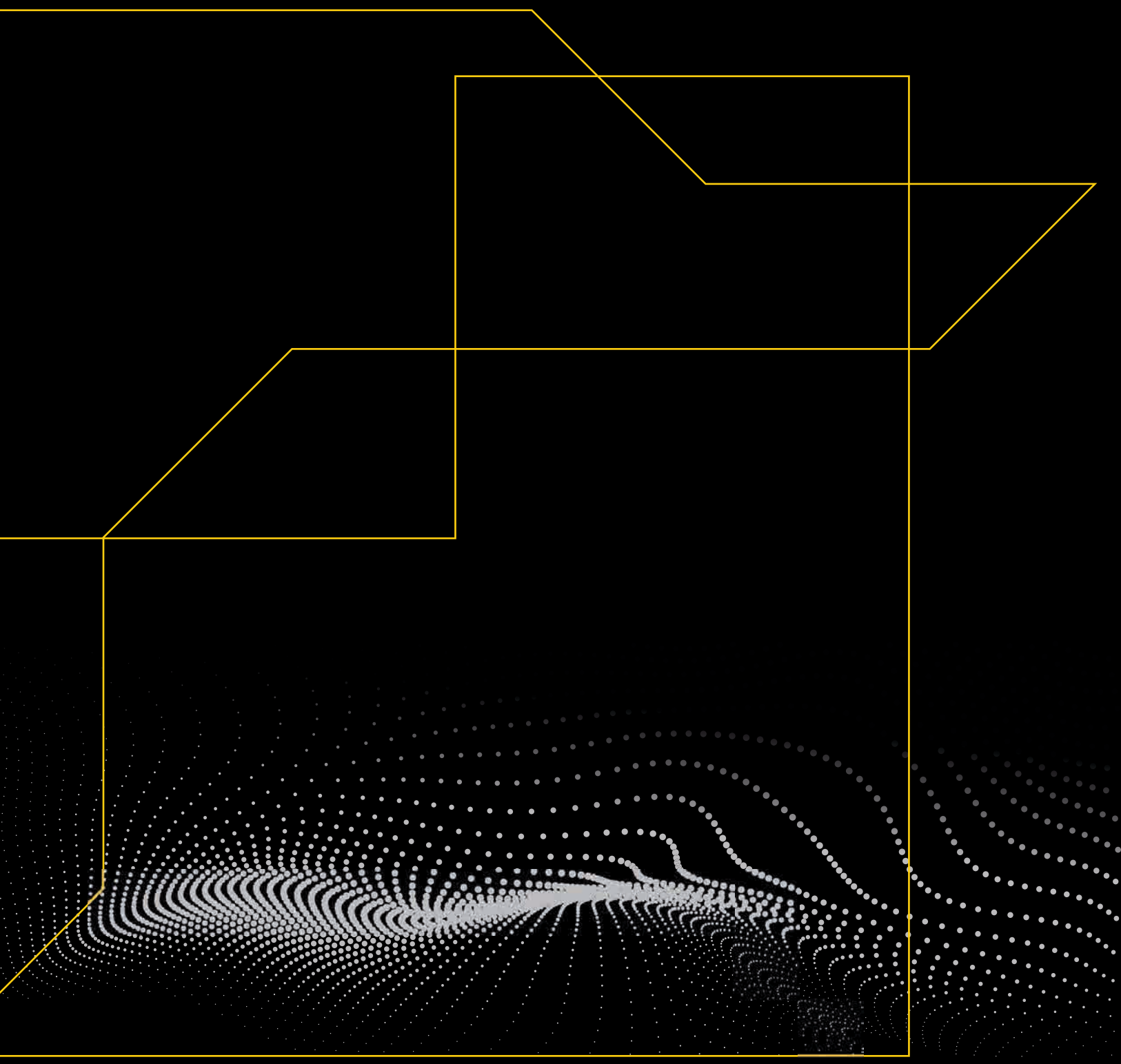
Programinis kodas gali būti saugus, tačiau mobiliosios programėlės dažnai prašo perteklinių duomenų arba prieigos prie įrenginio funkcionalumo. Prie tokios išvados prieita, kai NKSC inicijavo mobiliosios programėlės „Yandex.Taxi" analizę. Naudotojai dažniausiai tokią prieigą suteikia sutikdami su programų naudojimo taisyklėmis nesusimąstydami, kad jų duomenys, nesusiję su PĮ teikiama paslauga (pavyzdžiui, kontaktų duomenys, įrašai iš įrenginio mikrofono, nuotraukų galerija ir pan.), gali būti nutekinti ar prieinami trečiosioms šalims be jų žinios ir sutikimo.

2018 m. neigiama informacinė veikla buvo nutaikyta į svarbiausias Lietuvos nacionalinio saugumo sritis. Iš viso buvo nustatyti 2 456 atvejai, turėję neigiamos informacinės veiklos bruožų, t. y. vidutiniškai apie 205 atvejai per mėnesį. Didžiausias neigiamos informacijos aktyvumas buvo užfiksuotas gynybos srityje (29 proc.). Tokį intensyvumą lėmė ne tik įprastai Lietuvą veikiantis propagandos srautas, bet ir aktualūs šalies įvykiai, kurie buvo dirbtinai eskaluojami nedraugiškų šaltinių.

Tarp kibernetinio saugumo subjektų, įgyvendinančių Lietuvos Respublikos Vyriausybės nustatytus organizacinius ir techninius kibernetinio saugumo reikalavimus, YSII valdytojai įgyvendino 63 proc. organizacinių ir 50 proc. techninių kibernetinio saugumo reikalavimų (pernai YSII valdytojai buvo įgyvendinę tik 26 proc. organizacinių ir 6 proc. techninių kibernetinio saugumo reikalavimų).

Visokeriopai stiprindami kibernetinio saugumo aplinką, 2018 m. Krašto apsaugos ministerija ir NKSC pasirašė bendradarbiavimo susitarimą su žiniasklaidos priemonėmis. Taip pat pernai Krašto apsaugos ministerija, bendradarbiaudama su partneriais, pradėjo kurti Regioninį kibernetinio saugumo centrą Kaune. Priimtas sprendimas kurti Saugų valstybinį duomenų perdavimo tinklą, jungiantį gyvybines valstybės funkcijas užtikrinančias institucijas.

LIETUVOS KIBERNETINIŲ GRĖSMIŲ ŽEMĖLAPIS



1 lentelė. 2018 m. kibernetinio saugumo grėsmės ir tendencijos, palyginti su 2017 m.

↑	Didėjo	**Socialinė inžinerija**
→	Išliko didelė	**Kenkimo PĮ paplitimas**
→	Išliko didelė	**Pažeidžiamos interneto svetainės**
↑	Nauja	**Įrenginių saugumo spragos**
↑	Didėjo	**Elektroninių ryšių tinklų žvalgyba**
↑	Nauja	**Rangovų ir ar PĮ (ne)patikimumas**
↓	Mažėjo	**Elektroninių paslaugų trikdymas**

Socialinės inžinerijos metodais paremtų kibernetinių incidentų poveikis 2018 m. buvo didelis. Socialinės inžinerijos metodų, kai buvo manipuliuojama interneto vartotojų neapdairumu, patiklumu ar žinių trūkumu, naudojimo atvejų kibernetinėje erdvėje užregistruota 25 proc. daugiau. Ir toliau buvo siunčiami apgaulingi ir klaidinantys elektroniniai laiškai, rašomos žinutės socialiniuose tinkluose su kenkėjišku kodu ar nuorodomis į kenkėjiškas interneto svetaines. Šie metodai įgalino piktavalius įsiskverbti į kibernetinio saugumo subjektų, verslo ir gyventojų kompiuterius, rinkti informaciją arba įtraukti kompiuterius į Botnet ir vykdyti kenkėjišką veiklą. Didžiausia grėsmė kyla paprastiems naudotojams, kurių kibernetinio saugumo ir IT raštingumo stoka tampa pagrindine RIS užvaldymo priežastimi. Ši grėsmė taip pat labai aktuali ir verslo subjektams, kurie dėl socialinės inžinerijos metodais pagrįstų kibernetinių incidentų praranda konfidencialią informaciją arba patiria tiesioginius finansinius nuostolius (2 lentelė).

2 lentelė. Socialinės inžinerijos grėsmės įtaka

KIBERNETINĖ GRĖSMĖ	ĮTAKA		
	Nacionaliniam saugumui	Verslui ir VII	Gyventojams
Socialinė inžinerija		↓	↓

Kenkimo PĮ paplitimas taip pat susijęs ir su užvaldytais vartotojų ar IoT įrenginiais. Tai reiškia, kad apsaugos priemonės nesuveikė, buvo išnaudoti PĮ pažeidžiamumai, „įsilaužta“ ir paveiktas informacijos ir (ar) paslaugų konfidencialumas, prieinamumas ir vientisumas. Kenkimo PĮ paplitimo Lietuvoje grėsmė vertinama kaip didelė. Kenkimo PĮ aptikimas YSII sektoriuose kelia ypatingą riziką, kad bus paveiktos ypa-

tingos svarbos paslaugos, turinčios strateginę reikšmę ir galinčios daryti įtaką nacionaliniu ir regioniniu mastu (3 lentelė).

3 lentelė. Kenkimo PĮ grėsmės įtaka

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

Didelė dalis Lietuvoje esančių interneto svetainių yra pažeidžiamos daugiausia dėl neatnaujinamų TVS. Kibernetinio saugumo, verslo subjektai deramai neįvertina potencialios žalos, kurią patirtų dėl kibernetinio incidento, nevertina savo interneto svetainių, kaip svarbaus informacinio turto, reikalingo jų veiklai, taip pat neįvertina to, kad dalyje interneto svetainių yra saugomi asmens duomenys. Dėl šios priežasties kibernetiniai incidentai prieš kibernetinio saugumo subjektų interneto svetaines reikštų finansinius nuostolius dėl Bendrojo duomenų apsaugos reglamento nuostatų nesilaikymo (4 lentelė). Pažymėtina, kad, vertinant pagal vykdomą NKSC viešojo sektoriaus interneto svetainių stebėsenos sąrašą – galima teigti, kad padėtis viešajame sektoriuje gerėjo. 2018 m. interneto svetainių, į kurias yra labai lengva įsilaužti, skaičius mažėjo iki 1 proc.

4 lentelė. Pažeidžiamų interneto svetainių grėsmės įtaka

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

Įrenginių saugumo spragų NKSC 2018 m. aptiko 21 proc. daugiau nei 2017 m. Iš dalies tai susiję su IoT įrenginių paplitimu, be to, dėl šiuo metu esančio reguliavimo trūkumo tiek Lietuvoje, tiek Europos Sąjungoje, naudotojai įsigyja įrenginius, kuriems netaikomi papildomi saugos reikalavimai. Įsigyjami įrenginiai turi atvirus prievadus, nesaugius slaptažodžius, nešifruoja komunikacijų, turi nesaugią architektūrą ir programinį kodą (5 lentelė).

5 lentelė. Įrenginių saugumo spragų grėsmės įtaka

KIBERNETINĖ GRĖSMĖ	ĮTAKA		
	Nacionaliniam saugumui	Verslui ir VII	Gyventojams
Įrenginių saugumo spragos		✓	✓

Elektroninių ryšių tinklų žvalgyba yra susijusi su informacijos apie RIS rinkimu. Ši veikla gali būti nebūtinai piktavališka, tačiau dėl to, kad tokio pobūdžio informacijos rinkimas plinta, galima teigti, kad susido-

mėjimas RIS, kai įrenginiai ir informacija apie juos yra randama atlikus elementarius skenavimus, gali būti pirmas tokios veiklos vykdymo žingsnis. Ypatingą susirūpinimą kelia technologiniuose procesuose dalyvaujančių įrenginių sąsajos su internetu. Piktavaliai, surinkę informaciją apie tokius įrenginius gali bandyti trikdyti paslaugas, kurios turėtų ir fizinius efektus, darančius įtaką ne tik gyventojų namų ūkiams (pavyzdžiui, šildymui), verslui (pavyzdžiui, produktų gamybai), tačiau ir nacionaliniu mastu svarbioms paslaugoms (pavyzdžiui, elektros tiekimo, skirstymo ar vandens valymo procesams) (6 lentelė).

6 lentelė. Elektroninių ryšių tinklų žvalgybos grėsmės įtaka

KIBERNETINĖ GRĖSMĖ	ĮTAKA		
	Nacionaliniam saugumui	Verslui ir VII	Gyventojams
Elektroninių ryšių tinklų žvalgyba	✓	✓	

2018 m. Lietuvoje buvo pastebėta nauja kibernetinio saugumo grėsmė – rangovų patikimumo problema. 2018 m. dėl rangovų patikimumo problemos Lietuvos Respublikos Vyriausybė uždraudė naudotis „Kaspersky LAB" programine įranga VII ir YSII. NKSC atliko „Yandex. Taxi" programėlės vertinimą ir rekomendavo nenaudoti šios PĮ. Problemos aktualumas taip pat susijęs su tuo, kad technologiniu požiūriu produktai ar paslaugos gali būti saugios, tačiau įrangos ar paslaugų tiekėjai – ne. Turėdami perteklines prieigos galimybes, taip pat disponuodami konfidencialia informacija, subjektai informaciją apie pažeidžiamumus ar potencialius piktavališkos veiklos vektorius gali perduoti tretiesiems asmenims arba patys gali būti kenkėjiškos veiklos vykdymo tarpininkai (7 lentelė).

7 lentelė. Rangovų ir (ar) įrangos tiekėjų nepatikimumo grėsmės įtaka

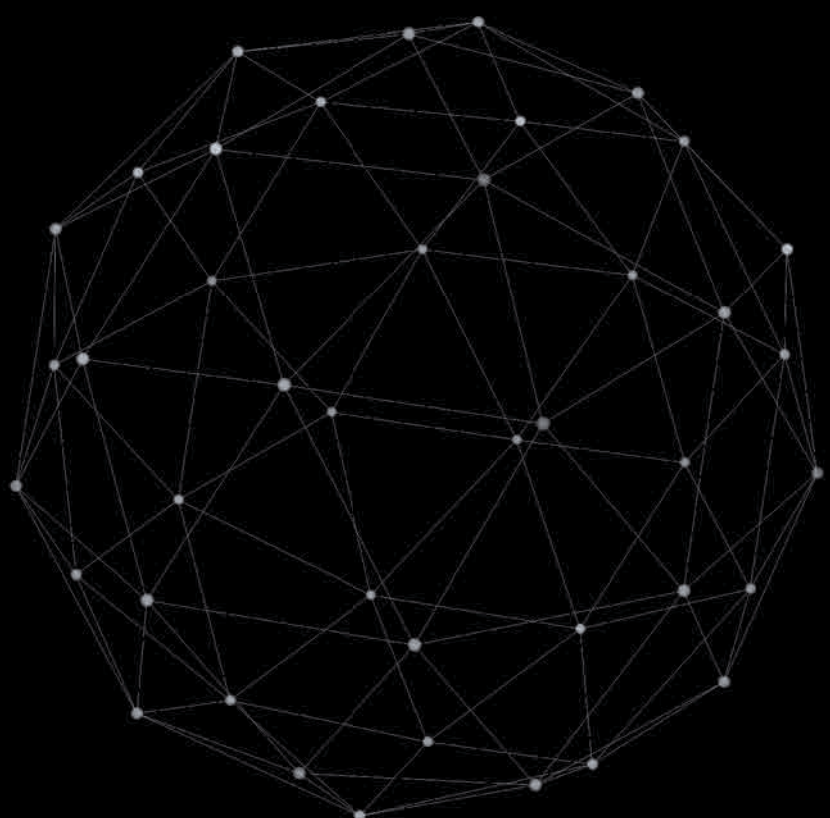
KIBERNETINĖ GRĖSMĖ	ĮTAKA		
	Nacionaliniam saugumui	Verslui ir VII	Gyventojams
Rangovų ir (ar) įrangos tiekėjų nepatikimumas	✓	✓	✓

Elektroninių paslaugų trikdymo grėsmės lygis 2018 m. mažėjo, DDoS atakų buvo užfiksuota 40 proc. mažiau. Tam įtaką darė anti-DDoS apsaugos priemonių naudojimas Lietuvos interneto infrastruktūroje, taip pat interneto paslaugų teikėjų siūlomos paslaugos ir kiti sprendimai, padedantys apsisaugoti nuo tokio pobūdžio kibernetinių incidentų (8 lentelė).

8 lentelė. Elektroninių paslaugų trikdymo grėsmės įtaka

KIBERNETINĖ GRĖSMĖ	ĮTAKA		
	Nacionaliniam saugumui	Verslui ir VII	Gyventojams
Elektroninių paslaugų trikdymas		✓	

DIDŽIAUSI 2018 M. KIBERNETINIO SAUGUMO IŠŠŪKIAI



Kibernetinių incidentų statistika

- **NKSC per 2018 m. Lietuvoje registravo 53 183 kibernetinius incidentus, tai 3 proc. mažiau nei 2017 m.**
- **Išaugo kompleksinių atakų skaičius – NKSC atliko 914 didelės ir vidutinės reikšmės kibernetinių incidentų tyrimų, tai 41 proc. daugiau nei 2017 m.**
- **NKSC nustatė 21 proc. daugiau saugumo spragų interneto įrenginiuose.**

Įvertinus kibernetinių incidentų statistiką, 2018 m. užfiksuotas nežymus – 3 proc. – registruotų incidentų mažėjimas (9 lentelė). Ankstesniais metais kibernetinių incidentų skaičius Lietuvoje kasmet išaugdavo po 10–20 proc. 2018 m. pastebimai mažėjo elektroninių paslaugų trikdymo, elektroninių duomenų klastojimo ir vientisumo pažeidimų skaičius. Su šiais kibernetinių incidentų tipais palyginus kenkimo PĮ, informacinių sistemų užvaldymo ir įrenginių saugumo spragų kiekį, matyti, kad skirtumas didelis. Palyginti su 2017 m., per 2018 m. užfiksuotas penktadaliu (21 proc.) didesnis įrenginių, turinčių saugumo spragų, skaičius.

Nors bendra kibernetinių incidentų statistika rodo nedidelį registruotų incidentų sumažėjimą, kibernetiniai incidentai tapo labiau rafinuoti, t. y. didelės ir vidutinės reikšmės kibernetinių incidentų, kuriuos NKSC specialistai turėjo apdoroti rankiniu būdu, padaugėjo 41 proc., iki 914 incidentų (2017 m. – 536). Automatinėmis priemonėmis NKSC 2018 m. apdorojo 52 269 incidentus (2017 m. – 54 414). Kenkimo PĮ platinimo serveriai buvo bandyti išradingai paslėpti naudojant keletą „reverse proxy“.

Kibernetinių incidentų detektavimo įrankiai, veikiantys automatiniu būdu, apdorojo mažiau įvykių nei anksčiau, nes kenkimo PĮ kodai tapo pažangesni ir sudėtingiau aptinkami pagal iš anksto nustatytas taisykles bei indikatorius. Tokiems kibernetiniams incidentams ir kenkimo PĮ aptikti ir prevenciškai užkardyti yra reikalingi greitesni ir daugiau informacijos apdorojantys algoritmai.

9 lentelė. NKSC informacija apie kibernetinius incidentus 2018 m. ir pokytis, palyginti su 2017 m.

Tipas	Kiekis 2018 m.	Pokytis nuo 2017 m.
Kenkimo PĮ	10 822	–5 proc.
Įsilaužimas (RIS užvaldymas)	10 059	–8 proc.
RIS trikdymas (DoS)	31	–40 proc.
Elektroninių duomenų klastojimas	872	–30 proc.
Vientisumo pažeidimai	24	–50 proc.
Įrenginių saugumo spragos	29 747	+21 proc.
Įvairaus pobūdžio	1 628	–76 proc.
Iš viso incidentų:	**53 183**	**–3 proc.**

Socialinė inžinerija

- **Sukčiai socialinės inžinerijos metodais bandė išvilioti naudotojų pinigus prašydami atlikti pinigines perlaidas, apsimesdami organizacijų vadovais, siūlydami įsigyti prekes suklastotose interneto svetainėse.**

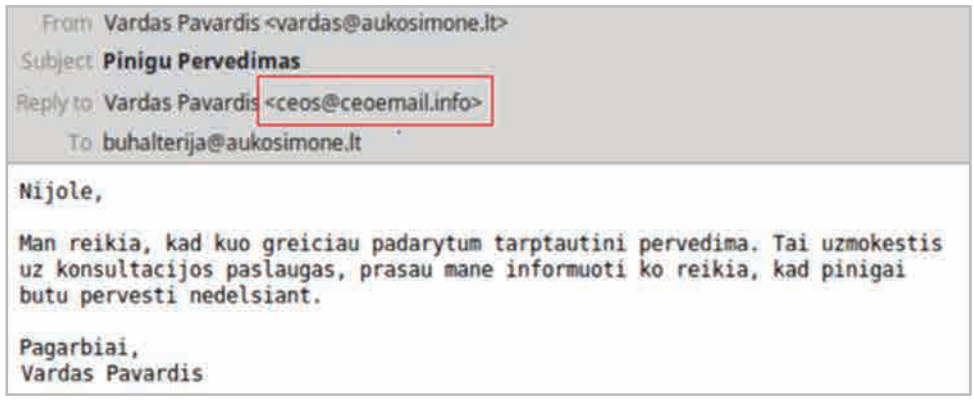
- **Šiuo metu socialinės inžinerijos metodai neapsiriboja elektroninių laiškų, suklastotų interneto svetainių kūrimu ar žinučių socialiniuose tinkluose siuntimu – piktavaliai gali paskambinti telefonu, bandyti susisiekti kitais būdais.**

Socialinės inžinerijos metodais paremti kibernetiniai incidentai susiję su manipuliavimu naudotojų veiksmais internete ir apgaule. Jų metu vyksta informacijos rinkimas, platinama kenkimo PĮ, išnaudojami pažeidžiamumai (1 pav.).

1 pav. Socialinės inžinerijos metodais pagrįstų kibernetinių incidentų klasifikavimas pagal Lockheed Martin „Cyber Kill Chain" modelį [3]

Populiariausi socialinės inžinerijos metodais pagrįsti kibernetiniai incidentai pagal 2018 m. statistiką Lietuvoje buvo slaptažodžių „žvejyba" elektroniniu paštu, žinučių socialiniuose tinkluose siuntimas arba naudotojų viliojimas į suklastotas interneto svetaines (angl. phishing). Piktavaliai šiais metodais taip pat dažnai siekia finansinės naudos. Ypač tokio pobūdžio kibernetinių incidentų padaugėja šventiniais periodais, kai naudotojai yra viliojami nuolaidomis, ir vertingai atrodančiais pasiūlymais ir pan. Dažnas atvejis, kai piktavaliai, apsimesdami įmonių vadovais, prašo buhalterių atlikti pinigines perlaidas (pavyzdys 2 pav.).

[3] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html



2 pav. „Direktoriaus" prašymas, gautas suklastotu elektroninio pašto adresu, pervesti pinigų

Kitas pavyzdys: dėl piktavališkų socialinės inžinerijos metodų naudotojai įdiegia kenkimo PĮ į RIS, pavyzdžiui, kuri pradeda veikti atidarius siunčiamą laišką ir įgalinus skaityti jo turinį (3 pav.).

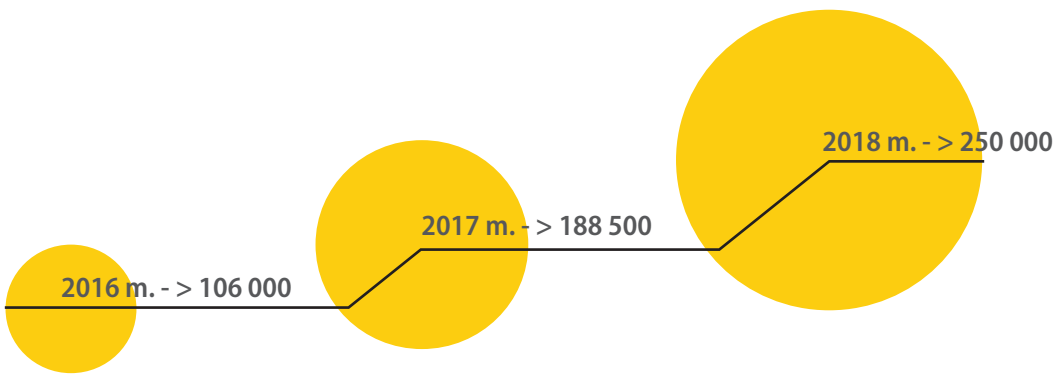
3 pav. Elektroniniais laiškais platintų dokumentų antraštė, kurią paspaudus yra aktyvuojama „macro" komanda, atsisiunčiama kenkimo PĮ

Piktavaliai taip pat gali skambinti telefonu ir prisistatyti RIS administratoriais arba, apsimetę dėkingais klientais, gali bandyti padovanoti ar įsiūlyti išorines atminties laikmenas su įdiegta kenkimo PĮ (10 lentelė).

Įvertinus stebėsenos duomenis, 2018 m. užfiksuotas 25 procentais didesnis socialinės inžinerijos metodais paremtų kibernetinių incidentų skaičius (4 pav.). To priežastis yra žmogaus veiksnio išnaudojimas kibernetinėms atakoms realizuoti. Kibernetinio saugumo subjektai skiria daug išteklių RIS atsparumui didinti, infrastruktūrai apsaugoti techninėmis priemonėmis, tačiau vis dar per mažai dėmesio skiriama darbuotojams šviesti ir sąmoningumui didinti. Deja, ir toliau yra laikomasi nuomonės, kad kibernetinis saugumas yra informacinių technologijų specialistų kompetencijos ir techninės įrangos klausimas. Įvykus kibernetiniam incidentui, atsakomybė dažniausiai yra perkeliama naudotojui, kuris iki įvykio dažniausiai deramai neinformuojamas ar nešviečiamas, kaip valdyti su kibernetiniu saugumu susijusias rizikas.

10 lentelė. Pagrindiniai socialinės inžinerijos grėsmių valdymo būdai

Nr.	Grėsmė	Patarimai naudotojui
1	Naudotojas paspaus nuorodą, vedančią į kenkėjišką puslapį.	Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar atvaizduojamas interneto svetainės adresas yra tikras, įsitikinti, kad adrese nėra įvelta gramatinių klaidų, adreso pavadinimas logiškas ir lengvai perskaitomas.
2	Naudotojas įves savo slaptažodį į suklastotą interneto svetainę.	Įsitikinti, kad sesija su interneto svetaine yra šifruojama, t. y. yra 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.	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 nelegalios PĮ platinimo šaltinių).
6	Naudotojas pasiduos piktavalio manipuliacijoms.	Neatlikti skubotų veiksmų, nepasiduoti emocijoms, iki galo išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą.



4 pav. Socialinės inžinerijos tendencijos 2016–2018 m.

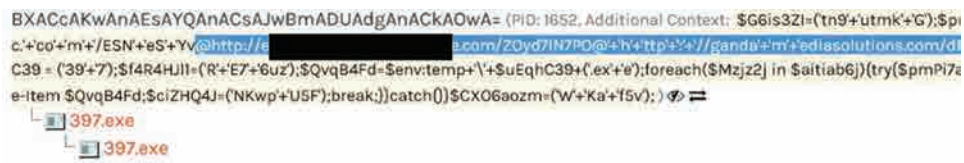
Kenkimo PĮ paplitimas

2018 m. daugiausiai kenkimo PĮ atvejų aptikta valstybės valdymo, energetikos, užsienio reikalų ir saugumo politikos sektoriuose.

Kenkimo PĮ paplitimas yra susijęs su RIS užvaldymu, kai piktavaliai, išnaudoję saugumo spragas bando įdiegti kenksmingą PĮ į RIS infrastruktūrą. Veikdama kenkimo PĮ sudaro sąlygas piktavaliui turėti prieigą prie infrastruktūros ir toliau vykdyti kitas kibernetines atakas (5 pav.).

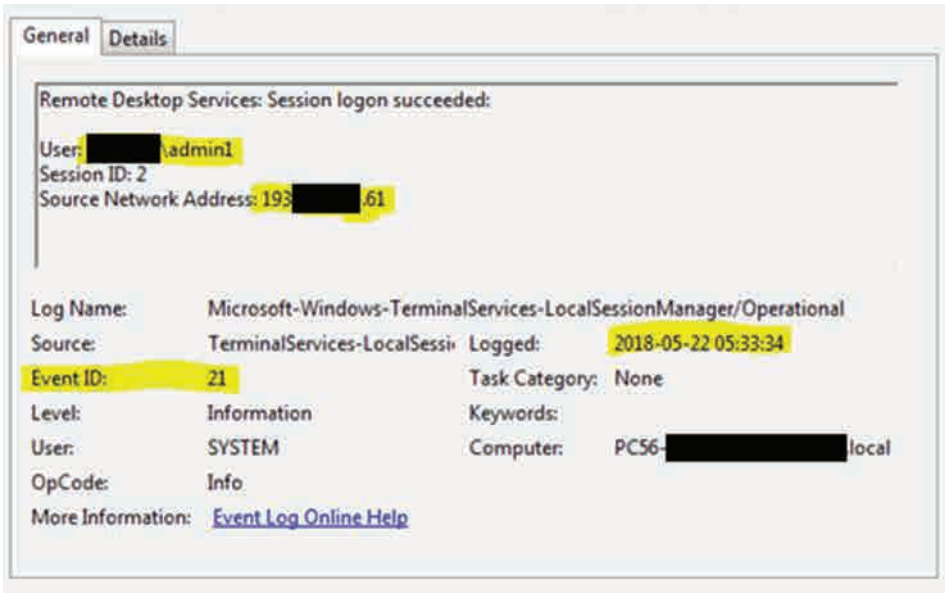
5 pav. Kenkimo PĮ klasifikavimas pagal „Cyber Kill Chain" modelį

NKSC naudojamos priemonės aptinka kenkimo PĮ veikimą prieš ją įdiegiant į infrastruktūrą, pavyzdžiui, aktyvuotas elektroninio laiško priedas bando užmegzti ryšį papildomai kenkimo PĮ atsisiųsti (6 pav.). Pastebėta tendencija, kai naudotojams yra siunčiamos nuorodos į debesijos paslaugų interneto svetaines (pavyzdžiui, onedrive.com, dropbox.com), kuriose yra įdėti failai su nuorodomis į kitas kenkėjiškas interneto svetaines.



6 pav. Windows OS „.docx" dokumente suaktyvinta „macros komanda", kuri aktyvina „powershell" funkcionalumą ir bando atsisiųsti kenkimo PĮ į RIS

Kitas atvejis, kai vykdant kibernetinių incidentų tyrimus fiksuojamos aktyvios, jau pradėjusio veikti, kenksmingo kodo komunikacijos, kurios piktavaliui jau būna sukūrusios prieigą prie organizacijos RIS, yra perimta įrenginio kontrolė ir piktavalis gali netrukdomai prisijungti ir vykdyti kenkėjišką veiklą (7 pav.).

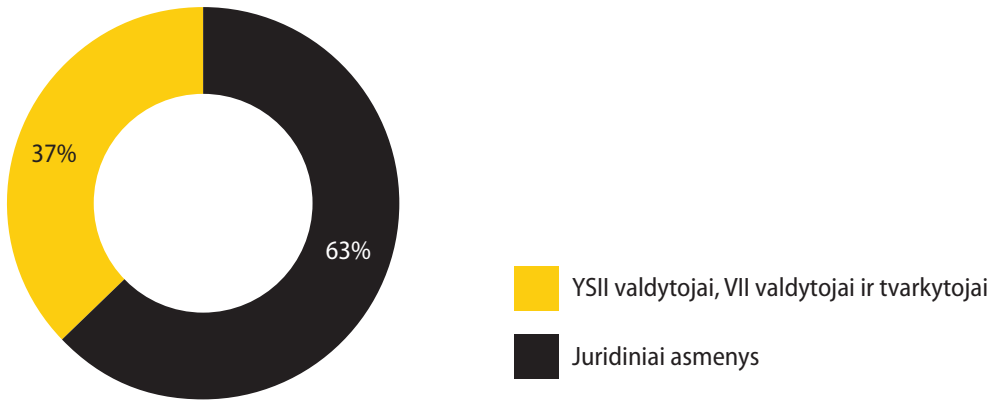


7 pav. Informacija apie sėkmingą piktavalio nuotolinį prisijungimą prie RIS

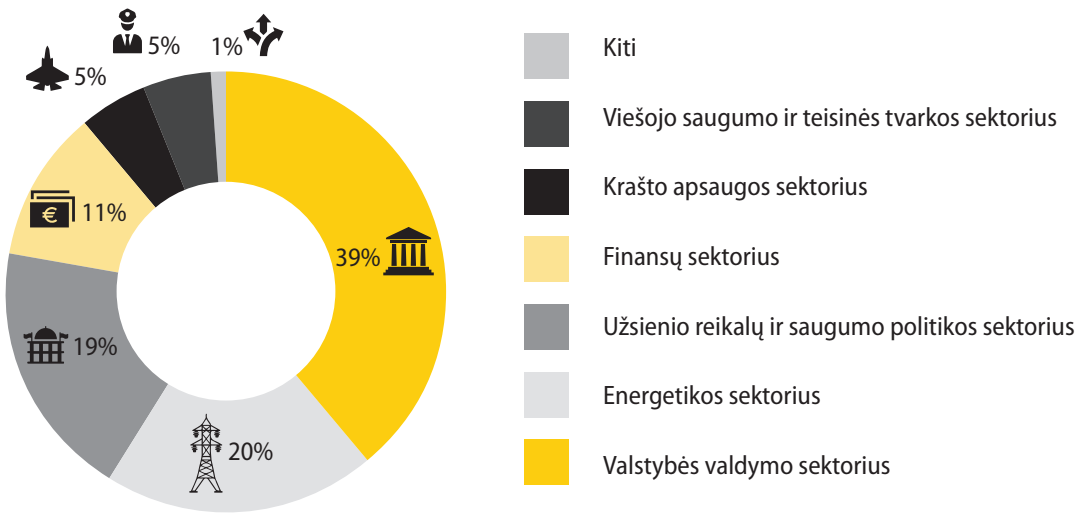
2018 m. NKSC užregistravo 10 822 kibernetinius incidentus su kenkimo PĮ. Palyginti su ankstesniais metais, šio tipo incidentų skaičius sumažėjo 5 proc. Pagal NKSC klasifikaciją vidutinės ir didelės reikšmės kibernetinių incidentų, susijusių su kenkimo PĮ aptikimu, NKSC užfiksavo 470, kai tuo tarpu 2017 m. buvo užfiksuoti 498 atvejai (8 pav.).

NKSC naudojamomis techninėmis priemonėmis 2018 m. daugiausiai kenkimo PĮ aptikta valstybės valdymo[4] (39 proc.), energetikos (20 proc.) taip pat užsienio reikalų ir saugumo politikos (19 proc.) sektoriuose (9 pav.). Tendencija tebėra grėsminga, nes ir toliau yra taikomasi į itin svarbias infrastruktūras, nuo kurių priklauso visuomenei svarbios paslaugos.

[4] Pagal Ypatingos svarbos informacinės infrastruktūros identifikavimo metodiką valstybės valdymo sektorių sudaro valstybės valdžios funkcijų atlikimo paslauga ir ypatingos svarbos valstybės informacinių išteklių (pirmos kategorijos informacinės sistemos ir registrai) tvarkymas



8 pav. Vidutinės ir didelės reikšmės kibernetiniai incidentai, susiję su kenkimo programinės įrangos aptikimu, pagal subjektus



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

11 lentelė. Pagrindiniai kenkimo PĮ grėsmių valdymo būdai

Nr.	Grėsmė	Patarimai naudotojui
1	Pasinaudojęs pažeidžiamumu, piktavalis įdiegs kenkimo PĮ į RIS.	Naudoti legalią OS ir PĮ, naudoti antivirusinę PĮ, ja profilaktiškai skenuoti duomenis įrenginyje, nedelsiant įdiegti gamintojo PĮ atnaujinimus jiems pasirodžius.
2	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.*
3	Kenkimo PĮ iš užkrėstos atminties laikmenos bus paleista automatiškai.	Nesinaudoti nepatikimomis, nepatikrintomis atminties laikmenomis. Nuolat jas formatuoti, išjungti automatinį failų paleidimą.
4	Kenkimo PĮ užšifruos kompiuteryje esančius duomenis.	Periodiškai daryti atsargines duomenų kopijas, saugoti atskirai, nuo tos vietos, kurioje jos buvo padarytos. Svarbią informaciją laikyti atskiroje laikmenoje ar laikmenose, neturinčiose tiesioginės sąsajos su internetu (pavyzdžiui, išorinėje laikmenoje).
5	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.
6	Kompiuteris bus užkrėstas per RIS tinklą.	Įstaigose naudoti tinklo segmentavimą, keletą filtravimo priemonių (pavyzdžiui, tinklo ir darbo stoties ugniasienę), svarbias RIS atskirti fiziškai.

* https://www.nksc.lt/irankiai.html

Pažeidžiamos interneto svetainės

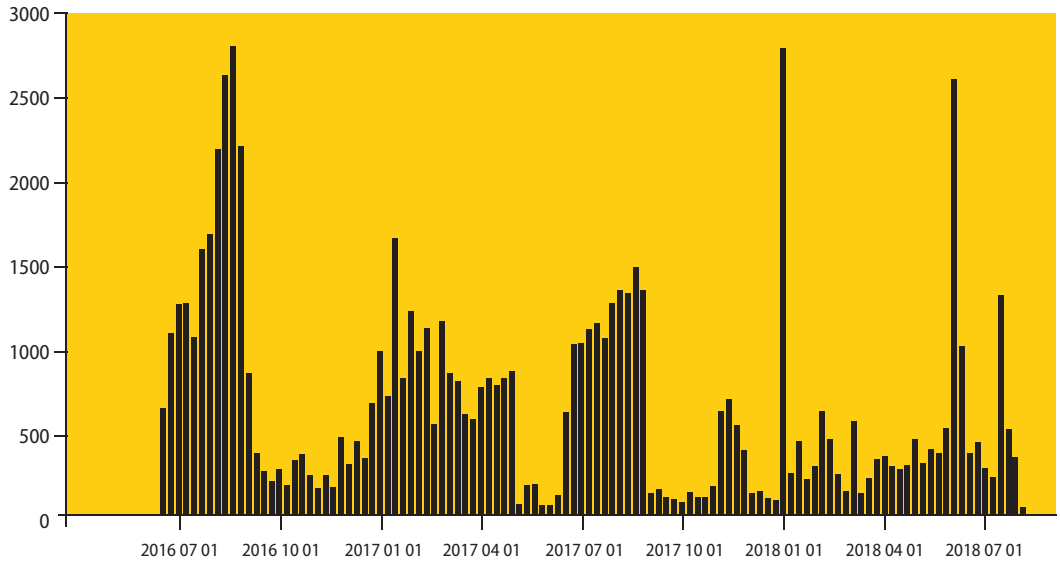
- **Pusė iš 52 000 interneto svetainių Lietuvoje su TVS yra pažeidžiamos.**
- **Labiausiai pažeidžiamos interneto svetainės, turinčios „Wordpress", „Joomla" TVS.**

Interneto svetainės, kurios turi pažeidžiamumų, gali būti panaudotos kenkimo PĮ įdiegti, įsilaužti ir prieigai prie duomenų įgauti, pavyzdžiui, per administratoriaus paskyrą. Pažymėtina, kad NKSC surinkta informacija apie pažeidžiamas interneto svetaines *de facto* nereiškia, kad jos yra užvaldytos ar pažeidžiamumai išnaudoti, tačiau tai rodo, jog egzistuoja reali tikimybė piktavaliams gauti neteisėtą prieigą prie svetainės TVS, ar joje saugomos informacijos (10 pav.).

Pavyzdys gali būti toks: 2018 m. NKSC tyrė įsilaužimą į Lietuvos Respublikos Seimo TS esančią interneto svetainę „skardzius.lt" (11 pav.). Interneto svetainių savininkai dažnai palieka atvirą prieigą prie interneto svetainių TVS administratoriaus paskyrų, neįjungia nesėkmingų bandymų prisijungti ribojimo, todėl piktavaliai gali automatinėmis priemonėmis įsilaužti į tokias interneto svetaines – įvykdyti vadinamą „brute force" kibernetinę ataką.

10 pav. Pažeidžiamų interneto svetainių kibernetinių incidentų klasifikavimas pagal „Cyber Kill Chain" modelį

Interneto svetainėms kibernetinės grėsmės kyla iš esmė dėl to, kad naudojamos populiariausios TVS, tokios kaip „Wordpress", ir su šia TVS susiję įskiepiai. Naudojant pasenusias TVS, tokios interneto svetainės tampa kibernetinių atakų taikiniais. Piktavaliai, radę pažeidžiamumų[5], gali pagal juos išnaudoti ir pritaikyti priemones kenkimo PĮ įdiegti[6].



11 pav. Bandymai prisijungti prie interneto svetainės skardzius.lt, pasinaudojant „wp-login.php" funkcionalumu

2018 m. NKSC atliko du interneto svetainių kibernetinio saugumo patikrinimus: visos Lietuvos (.lt) interneto svetainių TVS[7] saugumo vertinimą bei Lietuvos viešojo sektoriaus kibernetinio saugumo subjektų interneto svetainių saugumo vertinimą[8].

Buvo tikrinama daugiau kaip 110 000 Lietuvos aukščiausio lygmens domeno (angl. top level domain) interneto svetainių ir apie 1 200 viešojo sektoriaus interneto svetainių. Visos Lietuvos interneto svetainių TVS saugumo vertinimas buvo atliekamas identifikuojant pažeidžiamas TVS. Viešojo sektoriaus tyrimas buvo atliktas remiantis statistiniu modeliavimu, analizuojant įprasto svetainės naršymo metu gautą TS siunčiamą informaciją (GET request HTTP header banner), techninius duomenis, gautus iš viešųjų katalogų duomenų bazių, ir pasyvaus skenavimo priemonėmis gautą informaciją apie prieglobos serverius ir svetainės transliavimo tarnybų PĮ. Buvo vertinamos tinklo tarnybos, veikiančios TCP/IP protokolu, 80 ir 443 prievadais.

Tyrimo metu nustatyta, kad 32 proc. naudoja WordPress atvirojo kodo TVS, 5 proc. Joomla ir 9 proc. kitas TVS. Viešajame sektoriuje 25 proc. interneto svetainių naudoja Wordpress TVS ir 9 proc. Joomla TVS (12 lentelė).

---

5 https://www.cvedetails.com/

6 https://www.exploit-db.com/

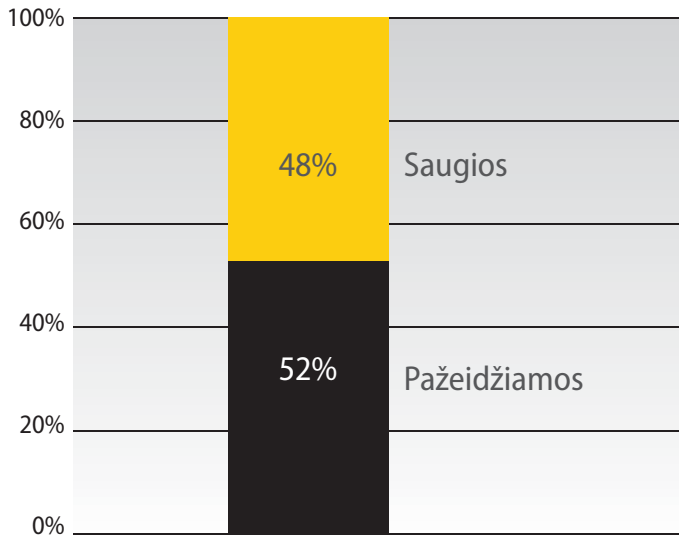
7 Tyrimo metu buvo vertintos tik tos svetainės, kurių TVS pavyko nustatyti ir kurios naudoja populiariausias atvirojo kodo TVS, nes šios sulaukia daugiausia piktavalių dėmesio ir jas yra masiškai bandoma užvaldyti jas pasitelkus automatizuotas priemones.

8 Viešojo sektoriaus interneto svetainių sąrašas buvo sudarytas pagal ministerijų ir savivaldybių pateiktą informaciją

12 lentelė. Interneto svetainių TVS suvestinė

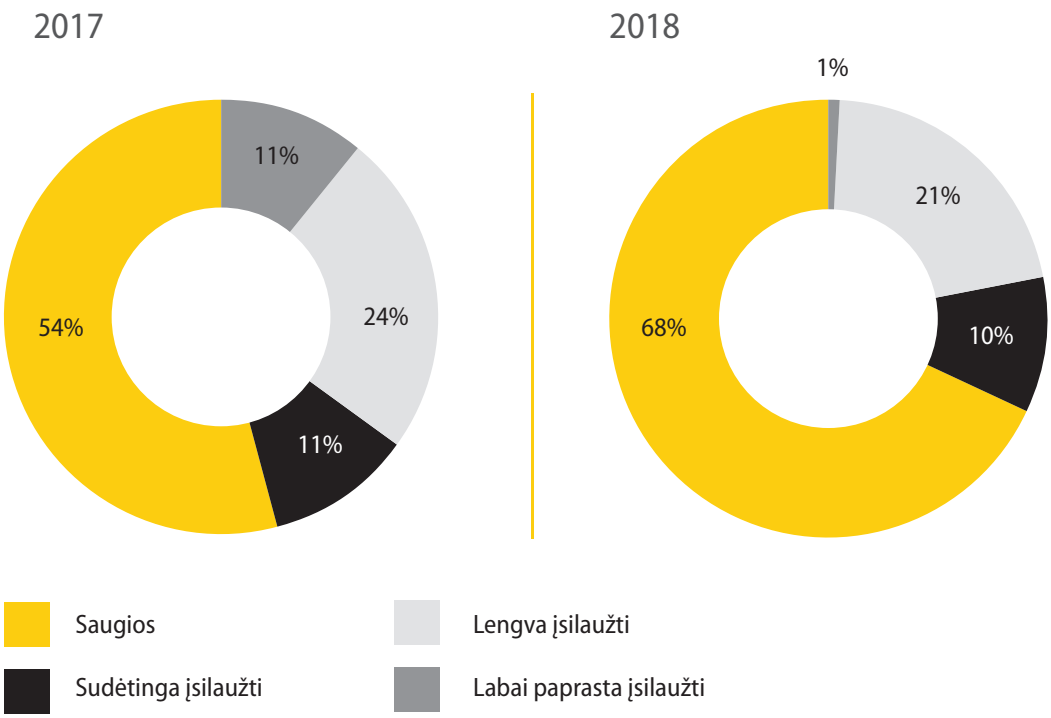
Turinio valdymo sistema	Paplitimas bendrai Lietuvoje	Paplitimas viešajame sektoriuje
WordPress	32 proc.	25 proc.
Joomla	5 proc.	9 proc.
Kita (Drupal, OpenCart, PrestaShop, Wix, Weebly, CMS Made Simple, Fresh Media, Idamas, CM4all ir pan.)	9 proc.	13 proc.
Nenustatyta	54 proc.	53 proc.

Įvertinus visos Lietuvos TVS tyrimo rezultatus, 52 proc. interneto svetainių Lietuvoje yra pažeidžiamos kibernetinėms atakoms (12 pav.). Kai kurios iš jų turi labai pavojingų saugumo spragų, o 9 proc. jų turi itin didelių pažeidžiamumų.



12 pav. 2018 m. Lietuvos (.lt) interneto svetainių kibernetinio saugumo vertinimas pagal TVS pažeidžiamumų informaciją

Nustatyta, kad tarp tirtų Lietuvos viešojo sektoriaus interneto svetainių 32 proc. yra pažeidžiamos kibernetiniams incidentams. Į didžiąją dalį (21 proc.) pažeidžiamų viešojo sektoriaus interneto svetainių, galima lengvai įsilaužti, nes internete yra prieinami tokio įsilaužimo metodai ir priemonės, todėl tikėtina, kad piktavaliai jomis gali pasinaudoti. NKSC dirbo tiesiogiai su administratoriais, kurių interneto svetainių pažeidžiamumai buvo kritinio lygio („blogiausi iš blogiausių“), informavo ir kontroliavo viešojo sektoriaus interneto svetainių savininkus dėl pažeidžiamumų užkardymo. Dėl to statistikoje atsispindi, kad svetainių, į kurias labai paprasta įsilaužti, 2018 m. sumažėjo iki minimumo (13 pav.).



13 pav. Viešojo sektoriaus interneto svetainių kibernetinis saugumas 2017–2018 m.*

*__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.

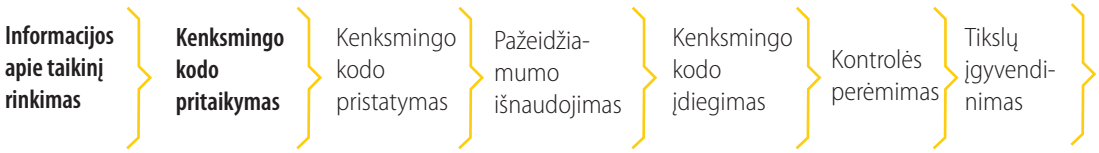
13 lentelė. Pagrindiniai pažeidžiamų interneto svetainių grėsmių valdymo būdai

Nr.	Grėsmė	Rekomenduojami grėsmės valdymo būdai
1	Piktavalis prisijungia prie TVS per naudotojo ar administratoriaus paskyrą.	Pakeisti interneto svetainės TVS administratoriaus ir naudotojų prisijungimo adresus, periodiškai keisti slaptažodžius, įgalinti ribotą bandymų prisijungti skaičių.
2	Piktavalis išnaudoja interneto svetainės pažeidžiamumus.	Nuolat atnaujinti TS OS, TVS ir susijusius įskiepius, nenaudoti nereikalingų TVS įskiepių, naudoti taikomųjų programų ugniasienę (angl. web application firewall), uždrausti nenaudojamus prievadus, skenuoti interneto svetainių pažeidžiamumus ir reguliariai tikrinti žurnalinius įrašus (angl. logs), įdiegti „reverse Proxy“ sprendimą, kad piktavalis negalėtų identifikuoti TVS.
3	Piktavalis į svetainę įdiegia kenkimo PĮ.	Sukonfigūruoti ugniasienes taip, kad prie interneto svetainių TVS būtų galima jungtis tik iš patikimų IP adresų (sudaryti taip vadinamąjį „baltąjį“ sąrašą).
4	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.
5	Prisijungimo prie interneto svetainės metu perimama informacija, įsiterpiama į ryšio srautą, perimami vartotojų duomenys ir (ar) prisijungimo slaptažodžiai.	Į interneto svetainę įdiegti SSL sertifikatą, kas užtikrins šifruotąjį ryšį. Tai viena efektyviausių interneto svetainių kibernetinio saugumo priemonių.
6	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 žvalgyba

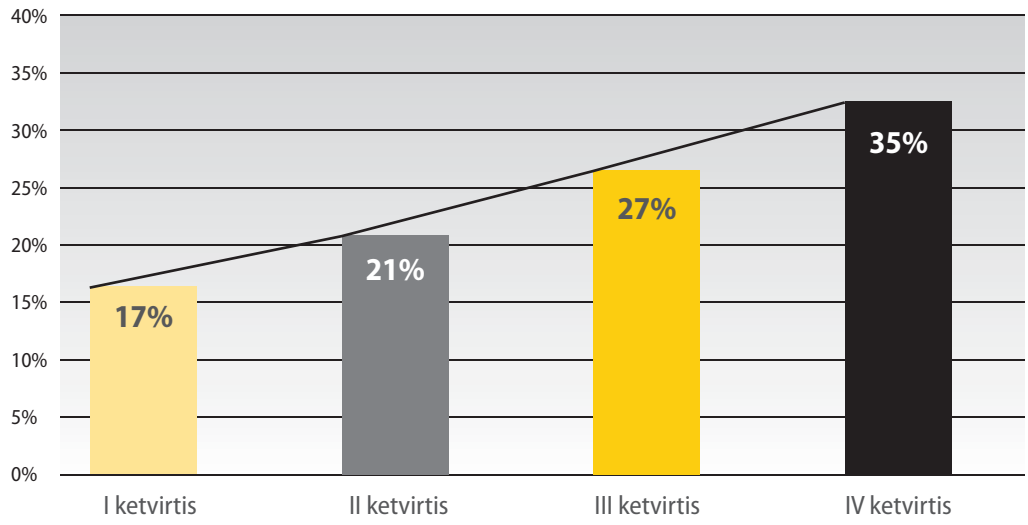
Lietuvoje labiausiai skenuojami energetikos, valstybės valdymo ir krašto apsaugos sektoriai.

Elektroninių tinklų žvalgyba susijusi su informacijos apie kibernetinio saugumo subjektų ar paprastų naudotojų RIS rinkimu. Populiariausias būdas – interneto skenavimo įrankiais, ieškant aktyvių, internetu prieinamų, paslaugų ir su jomis susijusių prievadų. Tokio pobūdžio elektroninių ryšių tinklų žvalgyba nebūtinai reiškia, kad bus vykdoma kenkėjiška veikla, tačiau dažniausiai tai yra pirmas žingsnis siekiant identifikuoti pažeidžiamas RIS vietas ir pagal jas pritaikyti kenksmingos PĮ platinimą.



14 pav. Elektroninių ryšių tinklų žvalgybos klasifikavimas pagal „Cyber Kill Chain" modelį

Pernai stebėtas didėjantis VII ir YSII valdančių subjektų elektroninių ryšių tinklų žvalgybos intensyvumas (15 pav.).



15 pav. 2018 m. ypatingos svarbos paslaugas teikiančių subjektų prievadų skenavimų intensyvumas

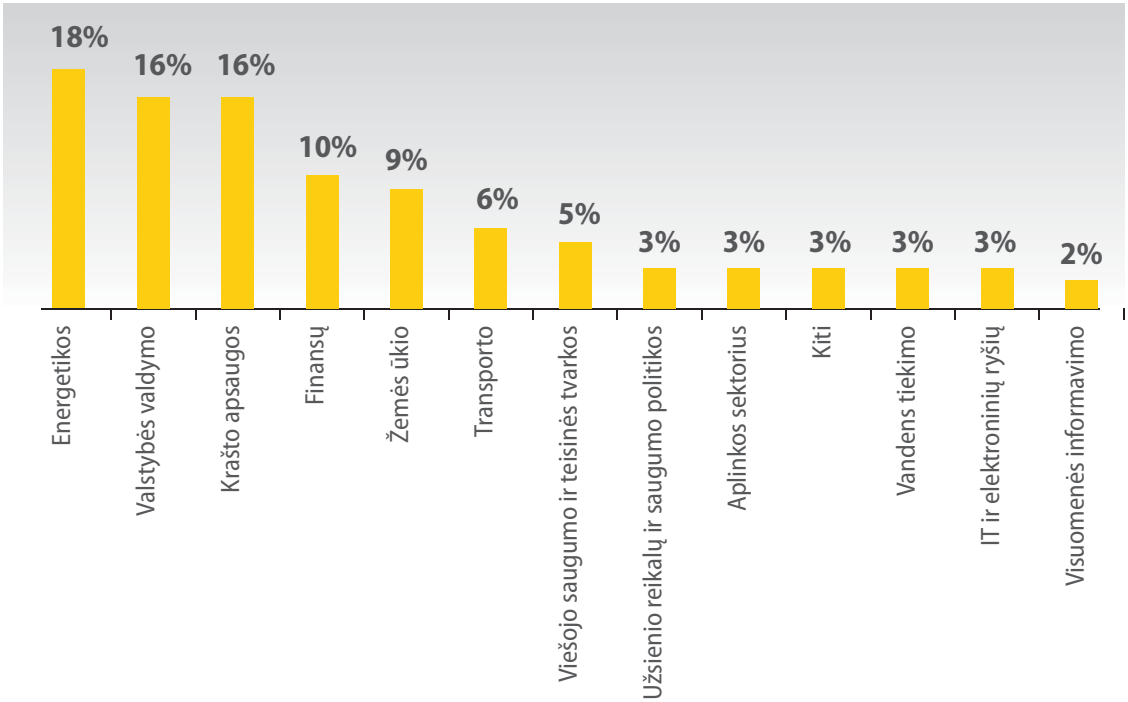
Skenuojant yra surenkama informacija apie organizacijų prie interneto prijungtus įrenginius, jų tipus, įgalintas paslaugas, pažeidžiamumus ar neuždarytus prievadus. Surinkus šią informaciją yra planuojamos tolesnės kibernetinės atakos arba – pasinaudojus viešai prieinama informacija ir įrankiais – bandoma įsilaužti į organizacijų infrastruktūrą. NKSC duomenimis, pagal pirminę informaciją populiariausi skenavimų šaltiniai yra – Rusija, Kinija, JAV (14 lentelė). Svarbu pažymėti tai, kad pirminis skenavimų šaltinis nebūtinai parodo tikrą geografinę vietą, iš kurios yra skenuojama.

14 lentelė. Elektroninių ryšių tinklų žvalgybos šaltinis pagal pirminę informaciją

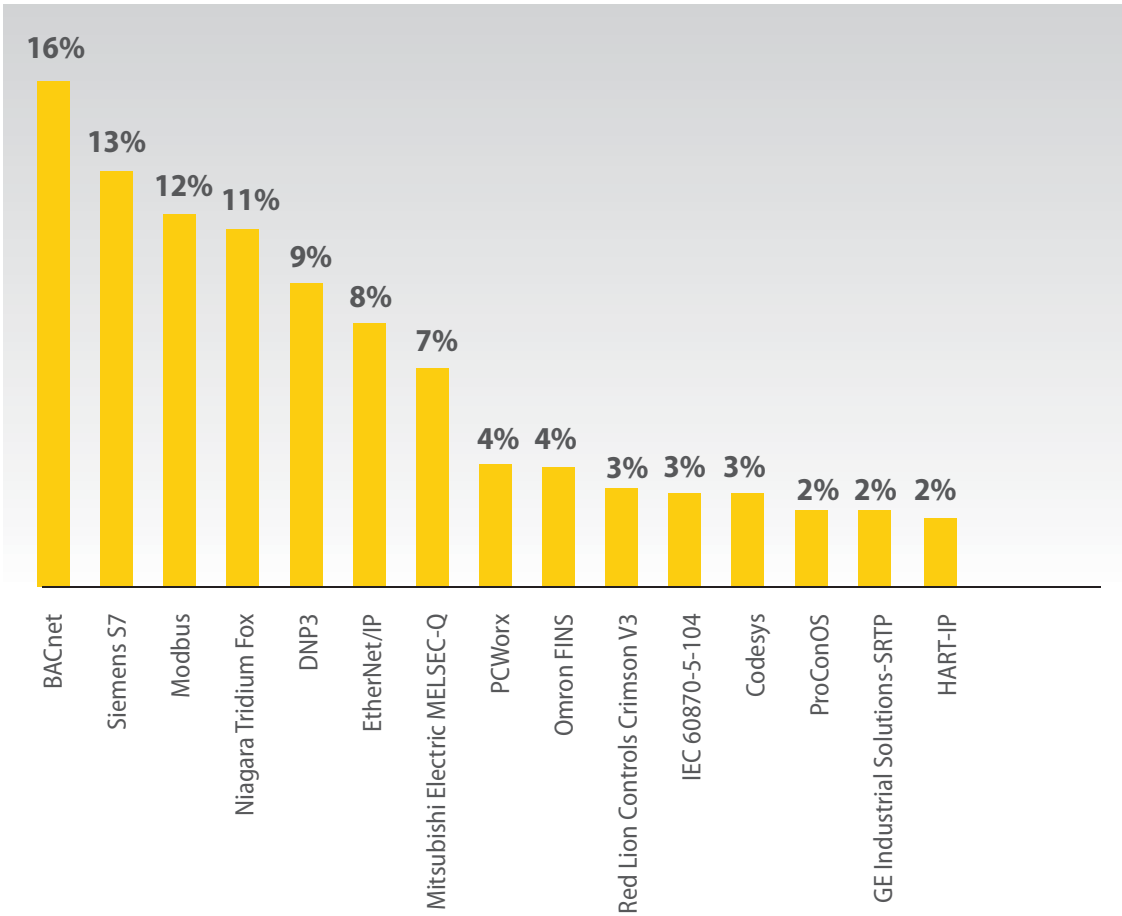
Valstybė	Kiekis (proc).
Rusija	17 proc.
Kinija	13 proc.
Jungtinės Amerikos Valstijos	12 proc
Lietuva	10 proc.
Nyderlandai	8 proc.
Ukraina	6 proc.
Kitos šalys (94)	34 proc.

2018 m. labiausiai buvo žvalgomi energetikos, krašto apsaugos, valstybės valdymo ir finansų sektoriuose ypatingos svarbos paslaugas teikiantys kibernetinio saugumo subjektai (16 pav.).

Vienas iš NKSC veiklos prioritetų yra technologinių tinklų (industrinių procesų valdymo sistemų) kibernetinis saugumas ir šiuose procesuose naudojamų įrenginių žvalgybos atvejai (17 pav.). Pažymėtina, kad nebuvo užfiksuota atvejų, kai tokie įrenginiai VII valdytojų ir tvarkytojų bei YSII valdytojų RIS turėtų tiesioginę sąsają su internetu. Nepaisant to, kad įrenginiai nėra tiesiogiai prijungti prie interneto, egzistuoja galimybė, kad sąsaja su internetu gali būti sukurta, pavyzdžiui, izoliuotame tinkle prijungus mobilųjį įrenginį, turėjusį arba turintį sąsają su internetu. 2018 m. labiausiai buvo ieškoma įrenginių, naudojančių BACnet, Siemens S7, Modbus, Niagara Tridium Fox protokolus (17 pav.).



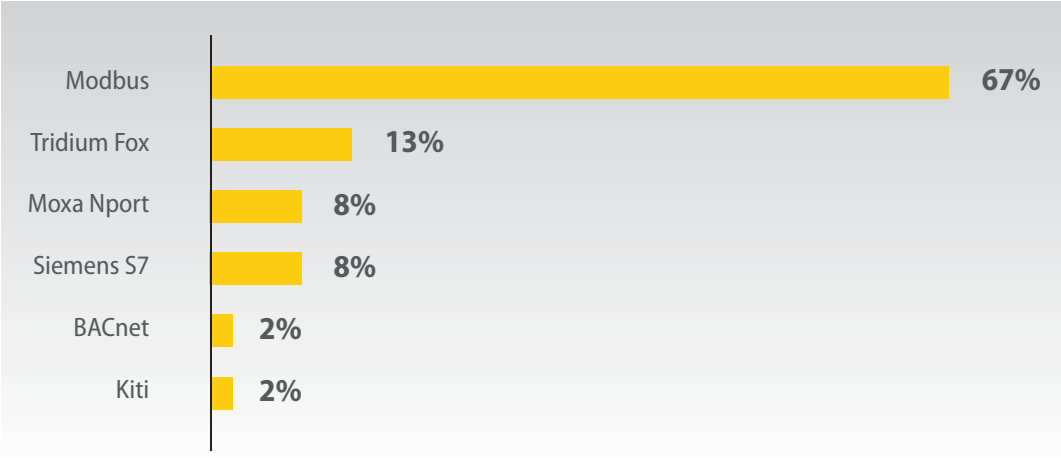
16 pav. Elektroninių ryšių tinklų žvalgyba pagal ypatingos svarbos paslaugų sektorius



17 pav. Įrenginių, naudojamų technologiniuose procesuose, žvalgybos statistika pagal protokolus ir (arba) įrangos gamintojus VII ir YSII valdytojų RIS 2018 m.

NKSC, siekdamas nustatyti kiek įrenginių, valdančių technologinius procesus, yra prijungta prie interneto Lietuvoje, atliko analizę, kurios metu buvo identifikuoti 486 įrenginiai, valdantys technologinius procesus.

Tyrimo metu nustatyta, kad 67 proc. įrenginių, turinčių tiesioginę sąsają su internetu, yra valdomi Modbus protokolu (18 pav.). Pavyzdžiui, tokie valdikliai gali būti naudojami namų vartotojams nuotoliniu būdu valdant namų šildymo, kondicionavimo ar signalizacijos sistemas. Pažymėtina, kad tokie įrenginiai yra ne visada atnaujinami, tokiu būdu piktavaliams yra paliekama galimybė, išnaudojus žinomus pažeidžiamumus, prisijungti prie įrenginių, perimti ir (ar) sutrikdyti jų valdymą.



18 pav. Technologiniuose procesuose dalyvaujančių ir internetu pasiekiamų įrenginių gamintojai ir (ar) komunikavimo protokolai

15 lentelė. Pagrindiniai elektroninių ryšių tinklų žvalgybos grėsmių valdymo būdai

Nr.	Grėsmė	Rekomenduojami grėsmės valdymo būdai
1	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.

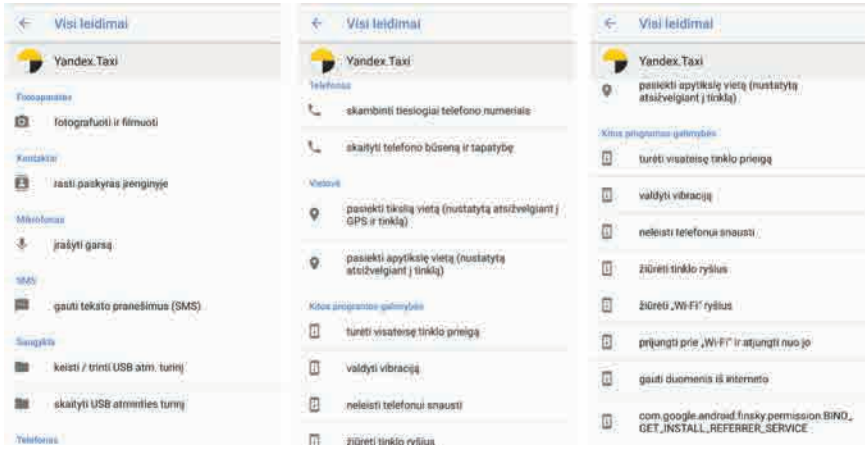
Rangovų ir PĮ patikimumas

Populiarios mobiliosios programėlės dažnai prašo perteklinių duomenų arba visokeriopos prieigos prie įrenginio funkcionalumo.

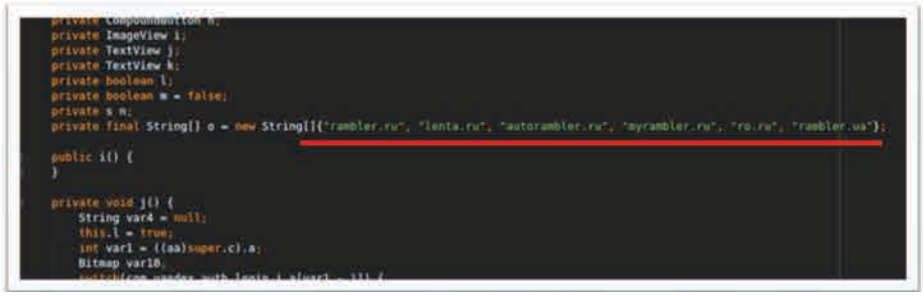
19 pav. Rangovų ir programinės įrangos patikimumo grėsmės klasifikavimas pagal „Cyber Kill Chain" modelį

NKSC atliktas tyrimas apie PĮ kilmę Lietuvos viešojo sektoriaus įstaigose, kurio apibendrinti rezultatai buvo publikuoti 2017 m. nacionalinio kibernetinio saugumo būklės ataskaitoje, sąlygojo Vyriausybės priimtus sprendimus dėl „Kaspersky Lab" PĮ pašalinimo VII valdytojų ir tvarkytojų bei YSII valdytojų sistemose. Problema dėl rangovų ir (ar) programinės bei techninės įrangos patikimumo ir toliau buvo keliama 2018 m. tiek viešojoje erdvėje, tiek atskirų subjektų iniciatyva kreipiantis į NKSC. NKSC inicijavo mobiliosios programėlės „Yandex. Taxi" analizę, kurios metu paaiškėjo, kad programa prašo perteklinių duomenų, reikalauja prieigos prie didelio kiekio itin svarbių duomenų ir leidimo naudotis įrenginio funkcijomis: galimybės aktyvuoti įrenginio kamerą ir mikrofoną (įrašyti naudotojo aplinką), naudoti kontaktų sąrašą (tai galimybė gauti telefonų knygos, naudojamų paskyrų informaciją), valdyti skambučius, nustatyti įrenginio tapatybę ir veiklos būklę, valdyti trumpųjų pranešimų paslaugas (tai 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 Wi-Fi prieigą (20 pav.). Taip pat, „Yandex. Taxi" palaiko aktyvų ryšį su 10 IP adresų Maskvos ir Jekaterinburgo serveriuose, taip sudarydama galimybę asmens duomenimis nutekėti už ES jurisdikcijos ribų, kur asmens duomenų reglamentavimas neatitinka ES standartų[9]. Programėlė turi galimybę šiais adresais (kurie, remiantis geolokacijos IP duomenų bazių informacija, išdėstyti skirtinguose regionuose) užmegzti ryšį nepriklausomai nuo to, ar ji dirba budėjimo, ar aktyviuoju režimu.



20 pav. Programėlės „Yandex.Taxi" prašoma prieiga prie išmaniojo telefono paslaugų ir informacijos



21 pav. NKSC tyrimo metu nustatyta informacija apie „Yandex.Taxi" komunikacijas

NKSC atkreipia dėmesį, kad, nepaisant saugaus programinio kodo, mobiliosios programėlės dažnai prašo perteklinių duomenų arba prieigos prie įrenginio funkcionalumo. Naudotojai dažniausiai tokią prieigą suteikia ir sutinka su programų naudojimo taisyklėmis nesusimąstydami, kad jų duomenys, nesusiję su PĮ teikiama paslauga (pavyzdžiui, ryšių duomenys, įrašai iš įrenginio mikrofono, nuotraukų galerija ir pan.), gali būti nutekinti ar prieinami trečiosioms šalims be jų žinios ir sutikimo.

Rangovų ir (ar) PĮ patikimumas taip pat glaudžiai susijęs su viešųjų pirkimų procedūromis, kai dėl kompetencijos stokos ar deramai neįvertinus grėsmių, vykdant viešąjį pirkimą pagal mažiausios kainos principą, yra įsigyjama ne pati saugiausia techninė ar PĮ. Piktavaliai, siekdami sutrikdyti ypatingos svarbos paslaugų teikimą, taip pat dažnai taikosi į tiekėjus, nes tokiu būdu galima tiesiogiai pasiekti nuo interneto atskirtą infrastruktūrą. Kaip pavyzdį galima įvardyti technologiniuose tinkluose esančios įrangos atnau-

[9] https://www.nksc.lt/naujienos/nacionalinis_kibernetinis_saugumo_centras_rekomend.html

jinimus, kai rangovas, prie technologiniame tinkle esančio įrenginio prijungęs nešiojamąjį kompiuterį su mobiliuoju ryšiu, įgalina nesankcionuotą technologinio tinklo sąsają su internetu. Tokiu būdu galima izoliuotame tinkle paskleisti kenkėjišką kodą, o įvertinus tai, kad technologiniuose tinkluose atnaujinimai nėra vykdomi nedelsiant jiems pasirodžius, kenkėjiškas kodas gali būti ir ne pats pažangiausias, nes pasitaiko atvejų, kai technologinių tinklų infrastruktūroje aptinkamos darbo stotys su pasenusia ir saugumo spragų turinčia „Windows XP" OS.

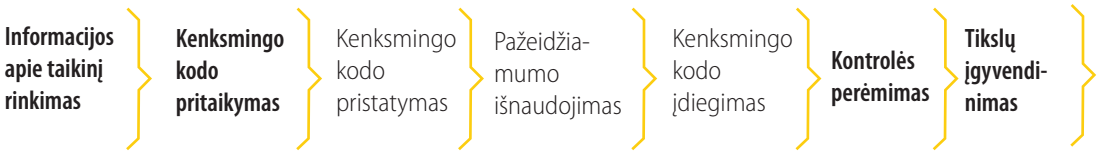
16 lentelė. Pagrindiniai grėsmių, susijusių su rangovų patikimumu, valdymo būdai

Nr.	Grėsmė	Rekomenduojami grėsmės valdymo būdai
1	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).
2	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.
3	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.

DDoS kibernetiniai incidentai ir įrenginių saugumo spragos

- **Registruota sąlyginai nedaug elektroninių paslaugų trikdymo atakų, 31 atvejis.**
- **Įrenginių, turinčių saugumo spragų, skaičiaus augimo tendencija yra reali grėsmė, kad šie įrenginiai gali būti įtraukti į Botnet tinklą ir naudojami DDoS kibernetinėms atakoms vykdyti.**

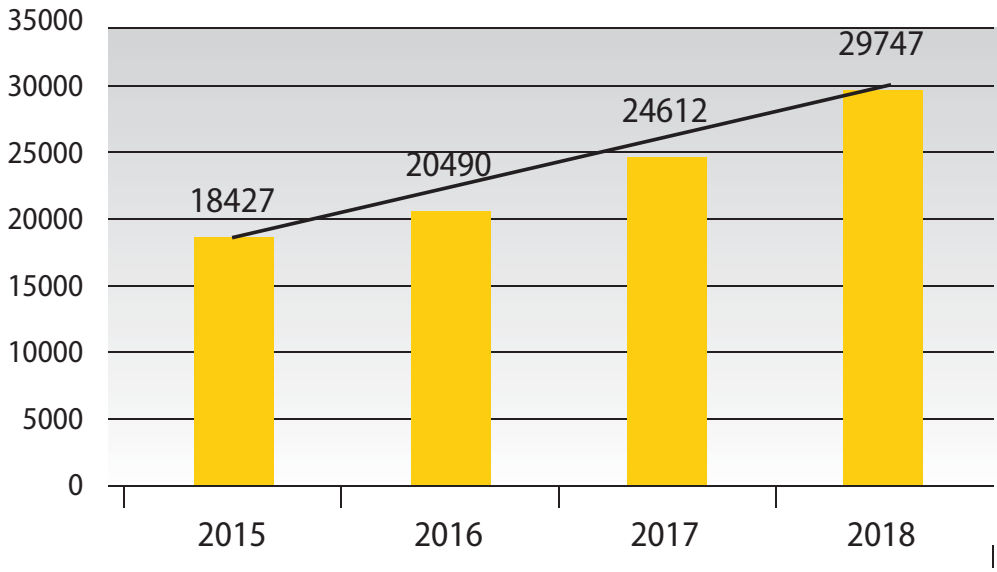
Elektroninio paslaugų trikdymo kibernetiniai incidentai dažniausiai vykdomi siekiant sutrikdyti RIS paslaugų prieinamumą. Populiariausias būdas – DDoS kibernetiniai incidentai per užvaldytą kompiuterių (Botnet) tinklą (22 pav.).



22 pav. Elektroninių paslaugų trikdymo kibernetinių incidentų klasifikavimas pagal „Cyber Kill Chain" modelį

NKSC 2018 m. užfiksavo 31 DDoS kibernetinį incidentą. Pagal svarbą, 20 iš jų buvo priskiriami vidutinei kategorijai. DDoS atakomis buvo taikomasi į Vidaus reikalų ministerijos, VĮ „Registrų centro", taip pat Lietuvos Respublikos Seimo RIS teikiamų paslaugų prieinamumą.

Pažymėtina, kad įrenginių, turinčių saugumo spragas, skaičius išaugo. Tokie įrenginiai gali būti užvaldyti ir įtraukti į Botnet tinklą, t. y. jais gali būti pasinaudota vykdant DDoS atakas. 2018 m. NKSC užfiksavo 28 630 įrenginių, turinčių saugumo spragų. Palyginti su ankstesniais metais, ši tendencija nuo 2015 m. kasmet padidėjo penktadaliu (atitinkamai 2015 m. užfiksuota 18 427, 2016 m. – 20 490, o 2017 m. – 24 612 įrenginių, 23 pav.). Įrenginių, turinčių saugumo spragų, skaičiaus augimas susijęs su sparčiai populiarėjančiais IoT.



23 pav. Įrenginių, turinčių saugumo spragų, daugėjimo tendencija 2015 – 2018 m.

17 lentelė. Pagrindiniai grėsmių, susijusių su įrenginių saugumo spragomis, valdymo būdai.

Nr.	Grėsmė	Rekomenduojami grėsmės valdymo būdai
1	Prie įrenginio galima prisijungti su standartiniu slaptažodžiu.	Pakeisti IoT, pasiekiamų internetu ar per „bluetooth“ sąsają, prisijungimo slaptažodžius į saugius.
2	Prie įrenginio prisijungiama per neužkardytą pažeidžiamumą.	Reguliariai atnaujinti IoT taikomąją ir PĮ.
3	Piktavalis gali matyti įrenginyje saugomus slaptažodžius ir kitą neskelbtiną informaciją.	Išjungti slaptažodžių išsaugojimo įrenginyje galimybę.
4	Piktavalis gali perimti informaciją ar slaptažodžius įrenginių komunikacijos metu.	Įsigyti ir naudoti įrenginius, kurių komunikacijos sesija yra šifruojama.
5	Piktavalis pasinaudoja perteklinėmis įrenginių funkcijomis ir įgauna prieigą prie RIS.	Jeigu yra galimybė, reikia patikrinti, ar įrenginyje nepalaikomas perteklinis funkcionalumas (atviri prievadai).
6	Įrenginys komunikuoja su išore ir, galimas dalykas, yra nutekinama informacija.	Prieš įsigyjant įrenginį, reikia įsitikinti, ar jo gamintojas atitinka Bendrojo duomenų apsaugos reglamento reikalavimus, ar siunčiami duomenys yra saugomi ES teisės.
7	Įsigyjamas nesaugus įrenginys.	Vengti nežinomų gamintojų, kurių kilmės šalį ir patikimumą yra sudėtinga patikrinti.

Rezonansiniai kibernetiniai incidentai

2018 m. Lietuvoje rezonansą kėlė hibridiniai incidentai, kai kibernetinės atakos buvo priderintos prie melagingų naujienų.

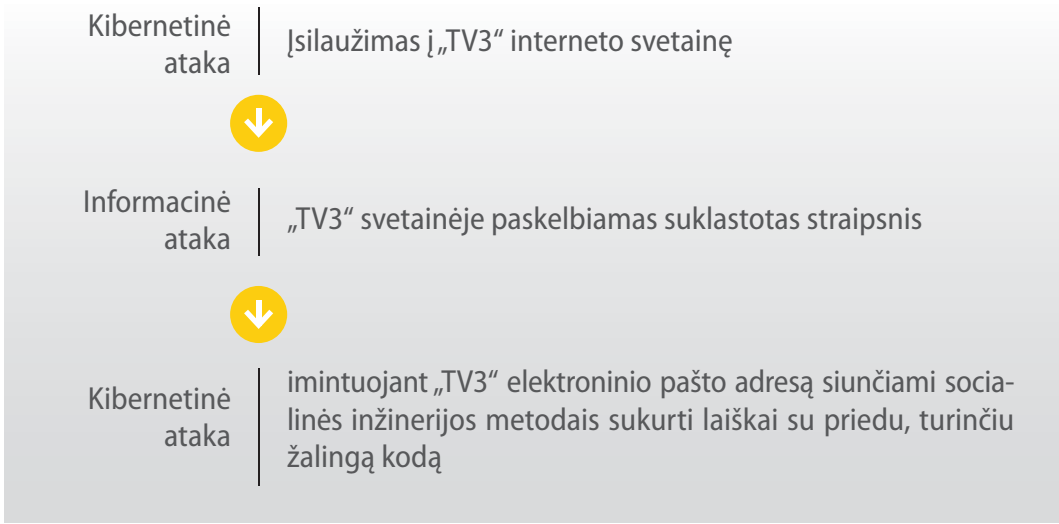
2018 m. vykę rezonansiniai kibernetiniai incidentai buvo susiję su RIS pažeidžiamumų atskleidimu, įdiegta kenkimo PĮ, užvaldytais įrenginiais ir su RIS vykdytais kenkėjiškais veiksmais.

24 pav. Rezonansinių kibernetinių incidentų klasifikavimas pagal „Cyber Kill Chain" modelį

2018 m. NKSC užfiksavo didelės reikšmės kibernetinius incidentus, kai pas kibernetinio saugumo subjektus buvo aptikta ilgą laiką veikusi pažangi šnipinėjimo įranga (angl. advanced persistent threat), sietina su užsienio valstybių žvalgybine veikla. Visuomenėje dažniausiai rezonansą kėlė kibernetiniai incidentai, savo pobūdžiu susiję su informacinėmis atakomis ir žinomų pažeidžiamumų išnaudojimu, nors dėl riboto poveikio pagal savo reikšmingumą nepriskirtini didelio poveikio arba pavojingiems kibernetiniams incidentams.

2018 m. taip pat buvo stebimi socialinės inžinerijos metodais paremti kibernetiniai incidentai, kurie buvo koreliuojami su informacinio pobūdžio atakomis (25 pav.). Kaip pavyzdį galima įvardinti 2018 m. „TV3"

interneto svetainės kibernetinį incidentą. Jo metu užvaldžius svetainės administratoriaus paskyrą buvo paskelbtas suklastotas skandalingas straipsnis, kuriuo remiantis ir imituojant TV3 elektroninio pašto adresą tikslinei auditorijai buvo siunčiami laiškai su dokumentu, kuriame buvo įterptas žalingas kodas, taip siekiant įsiskverbti į kitas RIS.



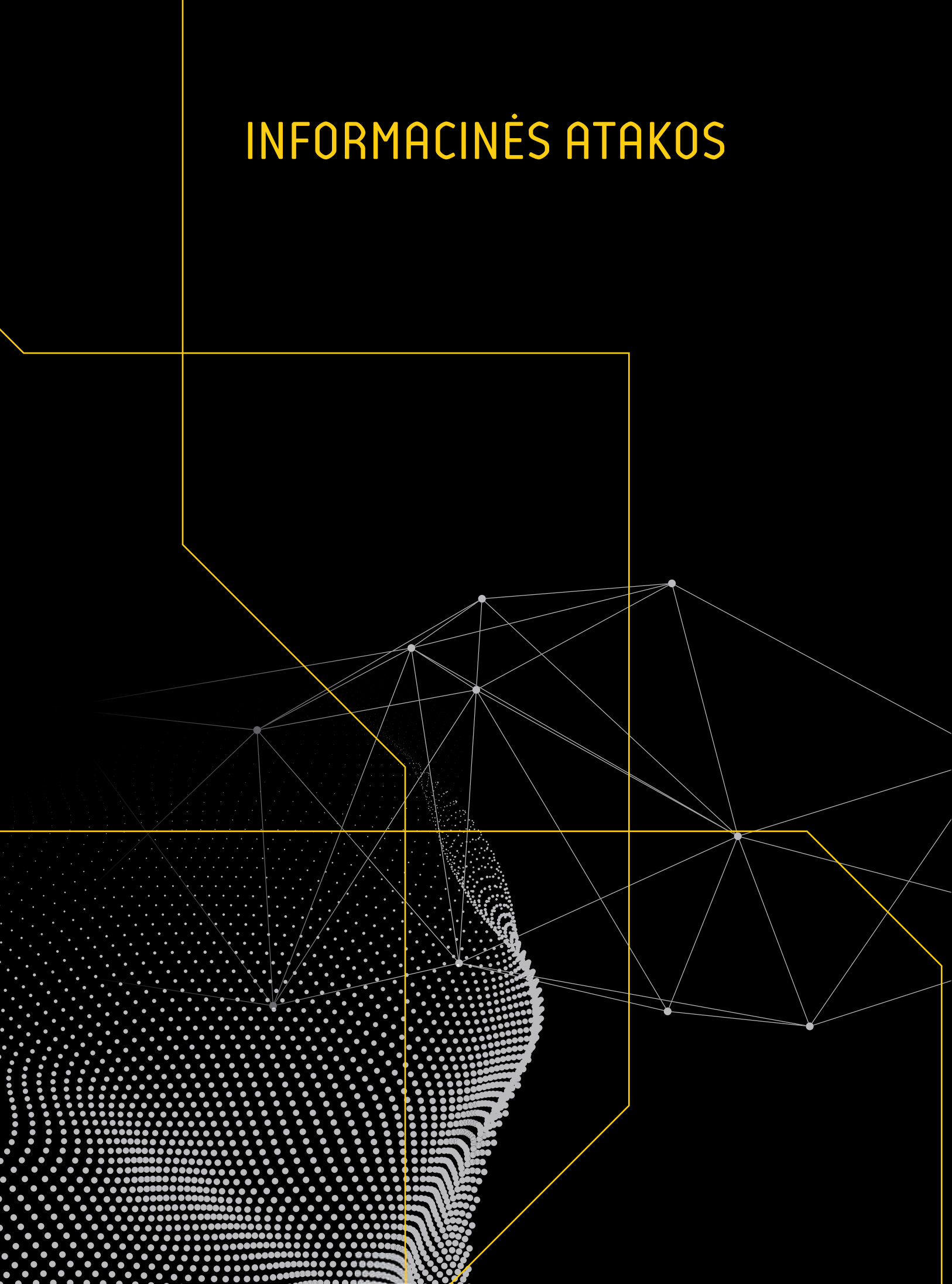
25 pav. Kibernetinės ir informacinės atakos, vykdytos įsilaužiant ir įsilaužus į „tv3.lt" naujienų portalo interneto svetainę

Svarbus ir rezonansą nacionaliniu mastu sukėlęs kibernetinis incidentas 2018 m. susijęs su informacinės sistemos *„e-sveikata"* pažeidžiamumo atskleidimu. Asmuo, pasinaudojęs programavimo klaida, viešai atskleidė pažeidžiamumą ir gavo prieigą prie asmens duomenų. Šis incidentas iškėlė atsakingo informavimo problemą, kai apie pažeidžiamumus yra informuojamos ne atsakingos institucijos, o trečiosios šalys, kurios viešindamos informacinių sistemų pažeidžiamus ir (ar) jų išnaudojimo būdus gali sudaryti sąlygas piktavaliams prieiti prie RIS saugomų asmens duomenų. NKSC atkreipia dėmesį, kad aptikus saugumo spragą pirmiausia apie tai reikėtų pranešti sistemos valdytojui ir NKSC, nesistengti išnaudoti saugumo spragos pažeistoje sistemoje, nebandyti pakeisti duomenų ar kitaip ją paveikti, nenaudoti kibernetinio saugumo įrankių pažeidžiamumams išnaudoti.

2018 m. pabaigoje, buvo vykdoma tikslinė brukalo (angl. spam) platinimo kampanija prieš valstybines institucijas, valdžios atstovus ir visuomenės veikėjus, kurios poveikis – elektroninio pašto paslaugų prieinamumo trikdymas, adresatų elektroninio pašto dėžutes užpildant tūkstančiais nepageidaujamų elektroninių laiškų. Kibernetinė ataka buvo vykdoma automatizuotu būdu įtraukiant asmenų elektroninio pašto adresus į įvairias reklamines naujienlaiškių prenumeratas, kurių siuntėjai nebūtinai buvo kenksmingi. NKSC teikia rekomendacijas, kaip apsisaugoti nuo tokio pobūdžio kibernetinių incidentų[10].

[10] https://www.nksc.lt/naujienos/apsaugos_priemones_kovai_su_brukalu.html

INFORMACINĖS ATAKOS



Informacinės atakos

Nustatyti 2 456 informacinių atakų atvejai, iš jų 29 proc. gynybos srityje.

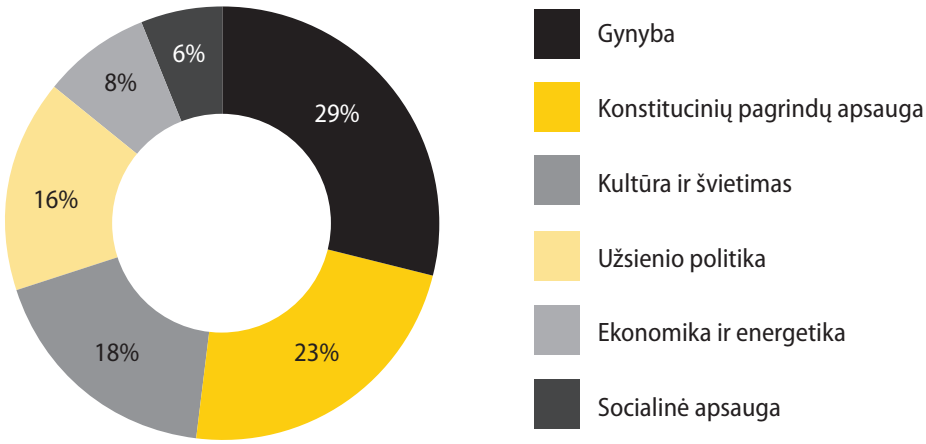
Lietuvos kariuomenės Strateginės komunikacijos departamentas vykdo įvykių, procesų ir tendencijų, susijusių su Lietuvos ir kitų šalių interneto vartotojų veikla kibernetinėje erdvėje, analizę. Pagrindinis dėmesys yra skiriamas per metus prieš Lietuvos visuomenę nukreipto neigiamos informacijos srauto, t. y. dezinformacijos, manipuliacijos, melagingų naujienų (angl. fake news) ir propagandos, svarbiausiems atvejams apžvelgti.

Dėl globalizacijos ir informacinių technologijų evoliucijos daugelis pasaulio šalių su skirtingu požiūriu į demokratines vertybes yra susijungusios į bendrą kibernetinę aplinką, kurioje keitimosi duomenimis ribos yra siauros arba visai neegzistuoja. Tai sukuria sąlygas informacinėmis operacijomis (pa)veikti demokratinių valstybių natūralų vystymosi procesą, manipuliuojant jų visuomenės nuomone suklastotomis ir provokuojančiomis naujienomis, skaitmeniniais pramoginiais produktais, kibernetinėmis atakomis siekiant neprileisti prie informacijos arba iškraipyti jos turinį, robotais socialiniuose tinkluose ir komentaruose bei samdomais nuomonės formuotojais, kurie kursto karą bei skatina tautinę, rasinę, religinę ir socialinių skirtumų nesantaiką.

2018 m. didžiausiu neigiamos informacijos šaltiniu Lietuvoje išliko Rusijos Federacijos vyriausybės kontroliuojama žiniasklaida ir su ja netiesiogiai siejamų bei Lietuvos teritorijoje veikiančių informacijos kanalų veikla. Vykdydami informacinius išpuolius su Kremliaus režimu siejami naujienų portalai, socialinių tinklų vartotojai ir televizija vadovavosi ilgalaikėmis medijų vartojimo įpročių tendencijomis Lietuvoje

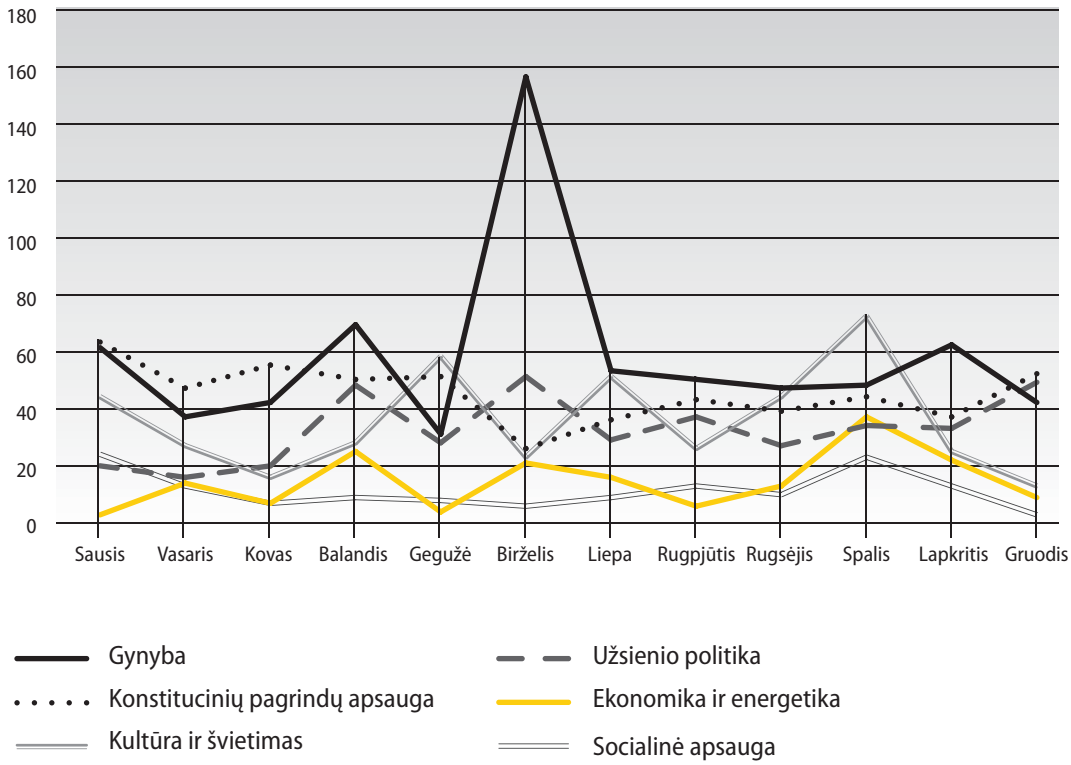
ir veikė tikslingai. Kaip ir ankstesniais laikotarpiais, pagrindinės Rusijos vykdomos informacinės veiklos kryptys išliko nepakitusios ir daugiausiai buvo nukreiptos į Lietuvai strategiškai svarbių bei socialiai jautrių klausimų, tokių kaip istorinės atminties ar socioekonominių gyventojų problemų, eskalavimą. Šių temų tikslingumas atspindi ilgalaikius Rusijos Federacijos strateginius interesus ir siekius išlaikyti savo informacinės erdvės kontrolę bei įtaką kitų valstybių informaciniuose laukuose, t. y. turėti politinius, ekonominius, informacinius ir kt. svertus jų vidaus procesų darbotvarkėje.

Iš viso praėjusiais metais buvo identifikuoti 2 456 nedraugiškos informacinės veiklos atvejai (arba vidutiniškai apie 205 per mėnesį). Jų procentinis pasiskirstymas pagal strategiškai svarbias sritis: gynyba – 29 proc.; konstitucinių pagrindų apsauga – 23 proc.; kultūra ir švietimas – 18 proc.; užsienio politika – 16 proc.; ekonomika ir energetika – 8 proc.; socialinė apsauga – 6 proc. (26 pav.).



26 pav. Neigiamos informacijos koncentracija strateginių sričių atžvilgiu 2018 m.

Didžiausias neigiamos informacijos aktyvumas fiksuotas gynybos srityje (beveik trečdalis iš visų atvejų). Taip pat nemaža dalis atvejų pasiskirstė tarp konstitucinių pagrindų apsaugos, kultūros ir švietimo bei užsienio politikos sričių. Kiek mažiau propaganda pasireiškė ekonomikos ir energetikos bei socialinės apsaugos srityse. Visgi būtų neteisinga manyti, kad, pavyzdžiui, socialinės apsaugos klausimai buvo mažiau svarbūs, nei tie, kurie buvo susiję su gynyba. Verta pabrėžti, kad kiekviena tema skleidžiama propaganda buvo suprantama individualiai, bet neatsietai nuo bendro vaizdo, o jos daromos žalos įvertinimas neapsiribojo vien kiekybine išraiška (pavyzdžiui, spalio mėnesį socialiniai klausimai buvo daug svarbesni negu gynybos, bet jų bendrame sraute užfiksuota kiekybiškai mažiau nei susijusių su gynybos temomis). Atsižvelgiant į propagandos aktyvumą, galima išskirti sausio, balandžio, birželio, spalio mėnesius, kuomet buvo identifikuota daugiausiai nedraugiškos informacinės veiklos atvejų (27 pav.). Tai sutapo su reikšmingais užsienio politikos ir šalies vidaus įvykiais, kuriuos Lietuvai nedraugiški informacijos šaltiniai siekė išnaudoti formuodami neigiamą šalies įvaizdį Vakaruose, bei skatino Lietuvos visuomenės auditorijų tarpusavio susipriešinimą.



27 pav. Neigiamos informacijos srauto dinamika valstybės strateginių sričių atžvilgiu 2018 m.

Ryškiausias tokio veikimo Lietuvoje pavyzdys – birželį karinių pratybų „Kardo kirtis 2018" metu internetiniame puslapyje gelezinisvilkassite.wordpress.com paskelbta informacija, kad JAV karinių šarvuočių „Stryker" avarijos metu žuvo vaikas (28 pav.).

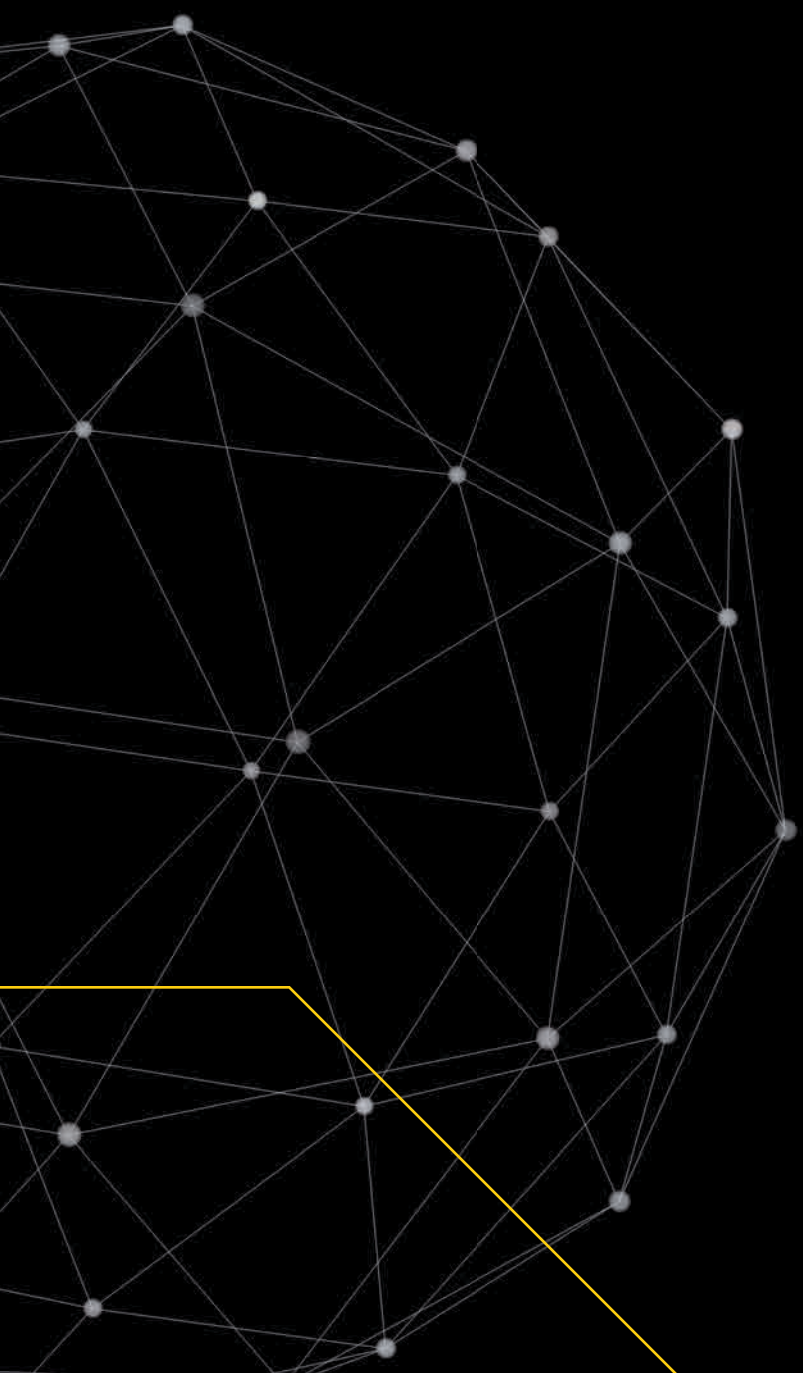

Lietuvoje NATO pratybose „Saber Strike 2018" žuvo vaikas

DELFI Žinios › Dienos naujienos › Kriminalai ir nelaimės

Lietuvoje NATO pratybose „Saber Strike 2018" žuvo vaikas (703)

28 pav. Melaginga naujiena – JAV karinių šarvuočių „Stryker" avarijos metu neva žuvo vaikas (2018 m. birželis)

KIBERNETINIO SAUGUMO ATSPARUMO DIDINIMAS



Kibernetinio saugumo organizavimas

- **2018 m. Lietuvos Respublikos Vyriausybė patvirtino Nacionalinę kibernetinio saugumo strategiją, kurioje iki 2023 m. buvo nustatytos svarbiausios nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptys.**
- **Priimtas sprendimas kurti saugų valstybinį duomenų perdavimo tinklą, jungiantį gyvybines valstybės funkcijas užtikrinančias institucijas (toliau – Saugusis tinklas).**

2018 m. buvo patvirtinta pirmoji Lietuvoje Nacionalinė kibernetinio saugumo strategija – esminis dokumentas, kuriame, atsižvelgiant į aplinkos analizės išvadas, Lietuvos ir Europos Sąjungos teisės aktus, gerąją kitų šalių patirtį bei viešojo ir privataus sektorių atstovų pasiūlymus, buvo įtvirtinti viešojo ir privataus sektorių, Lietuvos mokslo ir studijų institucijų penkerių metų tikslai ir uždaviniai kibernetinio saugumo srityje. Įgyvendinant strategiją yra siekiama stiprinti valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, užtikrinti nusikalstamų veikų prevenciją, užkardymą ir tyrimą, skatinti kibernetinio saugumo kultūrą ir inovacijų plėtrą, stiprinti glaudų viešojo ir privataus sektorių, tarptautinį bendradarbiavimą ir užtikrinti tarptautinių įsipareigojimų kibernetinio saugumo srityje vykdymą. Kartu buvo patvirtinti strategijos įgyvendinimo vertinimo kriterijai ir siekiamos jų reikšmės, o pati strategija bus įgyvendinama per tarpinstitucinius veiklos planus, kuriuose nustatomos strategijos įgyvendinimo priemonės ir lėšos joms įgyvendinti. 2018 m. taip pat buvo užbaigta dar 2017 m. viduryje pradėta šalies kibernetinio saugumo funkcijų ir pajėgumų konsolidacija, t. y. buvo sujungtos informacinių išteklių saugos, elektroninių ryšių tinklų ir informacijos saugumo bei kibernetinio saugumo politikos formavimo ir jos įgyvendinimo funkcijos ir perduotos Krašto apsaugos ministerijai.

2018 m. nauja redakcija buvo išdėstytos Kibernetinio saugumo įstatymo nuostatos, priimti Lietuvos Respublikos administracinių nusižengimų kodekso pakeitimai, atnaujintos Kibernetinio saugumo įstatymą įgyvendinančių teisės aktų nuostatos. Visi šie teisės aktų pakeitimai buvo atlikti ne tik siekiant į nacionalinę teisę perkelti 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyvą 2016/1148 „Dėl priemonių

aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti“, bet tai taip pat sudarė galimybę patobulinti kibernetinio saugumo sistemos organizavimą ir kontrolę, patikslinti kibernetinio saugumo politiką formuojančių ir įgyvendinančių institucijų funkcijas, kibernetinio saugumo subjektų pareigas bei atsakomybę ir nustatyti papildomas kibernetinio saugumo užtikrinimo priemones. Pakeitus minėtus teisės aktus, buvo praplėsta NKSC kompetencija, suteikta daugiau teisių kibernetinio saugumo subjektų kontrolei ir priežiūrai vykdyti – NKSC tapo ne tik prižiūrinčia, tačiau ir nacionaliniu mastu kibernetinio saugumo subjektus kontroliuojančia ir administracinę atsakomybę taikančia institucija.

2018 m. buvo priimtas Bendrasis duomenų apsaugos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo (toliau – Reglamentas). Organizacijos, siekdamos išvengti Valstybinės duomenų apsaugos inspekcijos taikomos atsakomybės už Reglamento nuostatų nesilaikymą, aktyviau ėmėsi tvarkyti savo IT ūkį, t. y. ne tik pradėjo reglamentuoti asmens duomenų naudojimą savo veikloje, tačiau pradėjo planuoti ir diegti kibernetinio saugumo priemones asmens duomenims apsaugoti.

Siekdama pakelti kibernetinio saugumo būklės lygį Lietuvoje, Krašto apsaugos ministerija 2018 m. antroje pusėje parengė Valstybės informacinių išteklių valdymo įstatymo pakeitimą ir pasiūlė nustatyti pareigą valstybės ir savivaldybių institucijoms ir įstaigoms, vykdančioms valstybines mobilizacines užduotis gyvybiškai svarbioms valstybės funkcijoms atlikti, naudoti Saugųjį tinklą. Saugusis tinklas būtų atskirtas nuo viešųjų ryšių tinklų ir galėtų veikti krizės ar karo sąlygomis. Minėtą įstatymą Lietuvos Respublikos Seimas priėmė 2018 m. gruodžio 20 d. Šio įstatymo įgyvendinimas sudarys galimybę ne tik užtikrinti greitesnį ir efektyvesnį reagavimą į kibernetinius incidentus, bet bus taupomi kibernetiniam saugumui skiriami ištekliai, nes bus centralizuojamas kibernetinės saugos užtikrinimas, bus sudarytos sąlygos efektyviau taikyti kolektyvinės gynybos priemones.

Kibernetinio saugumo aplinkos kūrimas

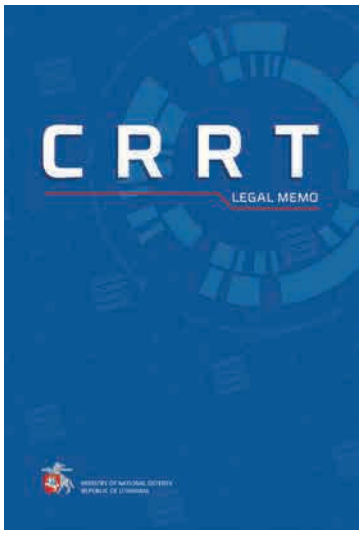
- **2018 m. Krašto apsaugos ministerija ir NKSC pasirašė bendradarbiavimo su žiniasklaidos priemonėmis susitarimą.**
- **2018 m. Krašto apsaugos ministerija, bendradarbiaudama su partneriais, pradėjo kurti Regioninį kibernetinio saugumo centrą Kaune.**
- **2018 m. Lietuva pradėjo įgyvendinti dar 2017 m. inicijuotą Europos Sąjungos nuolatinio struktūrizuoto bendradarbiavimo projektą „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ (angl. Cyber Rapid Response Teams and Mutual Assistance in Cyber Security).**

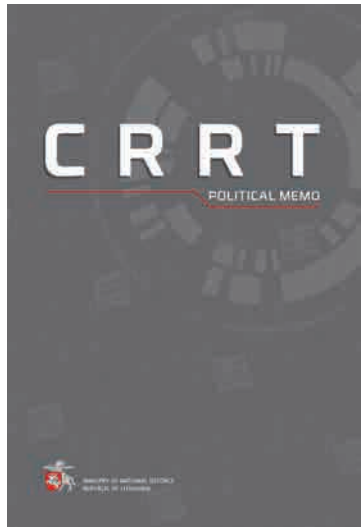
Kibernetiniai incidentai vis dažniau pažeidžia ne tik viešąjį ir privatų sektorius, bet ir žiniasklaidos priemones, kurios vaidina svarbų vaidmenį kuriant saugią kibernetinę erdvę ir objektyviai informuojant Lietuvos gyventojus. 2018 m. rugpjūčio 28 d. Krašto apsaugos ministerija kartu su NKSC ir didžiausiais Lietuvos naujienų portalais bei agentūromis pasirašė bendradarbiavimo susitarimą, kurio pagrindinis tikslas – efektyvinti bendradarbiavimą kibernetinio saugumo srityje, stiprinti visuomenės informavimo priemonių kibernetinį saugumą ir atsparumą kibernetinėms grėsmėms. Įgyvendinant bendradarbiavimo susitarimo nuostatas, 2018 m. spalio 23 d. Lietuvos kariuomenės Gedimino štabo batalione buvo surengti kibernetinio saugumo mokymai žurnalistams, kurie mokėsi, kaip kritiškai vertinti kibernetinę erdvę, atpažinti kibernetines grėsmes ir spręsti kibernetinius incidentus.

Nuo 2018 m. Krašto apsaugos ministerijos iniciatyva pradėti vykdyti Regioninio kibernetinio saugumo centro steigimo darbai. Šio būsimo centro tikslas – didinti Lietuvos kibernetinį atsparumą, dirbant su partneriais stiprinti Lietuvos kibernetinės gynybos specialistų gebėjimą laiku atpažinti ir užkirsti kelią mūsų regione vykstantiems kibernetiniams incidentams.

Žiniasklaidos atstovų mokymai. Ievos Budzeikaitės nuotrauka

Siekiant sustiprinti Europos Sąjungos kibernetinio saugumo ir gynybos pajėgumus bei efektyviau suvaldyti kibernetinius incidentus, peržengiančius valstybių sienas, būtina bendradarbiauti su kitomis Europos Sąjungos šalimis. Lietuvos Respublikos krašto apsaugos ministerija 2017 m. inicijavo (vadovavo krašto apsaugos viceministras Edvinas Kerza) Europos Sąjungos nuolatinio struktūrizuoto bendradarbiavimo projektą „Kibernetinės greitojo reagavimo pajėgos ir tarpusavio pagalba kibernetinio saugumo srityje“ (toliau – PESCO Projektas), kuris buvo pradėtas įgyvendinti 2018 m. vasario mėnesį. Projekto tikslas – sujungti ir panaudoti valstybių narių kibernetinės gynybos pajėgumus, žinias ir kompetencijas. PESCO projekte dalyvauja trylika valstybių, devynios yra šio projekto narės (Estija, Ispanija, Kroatija, Lietuva, Lenkija, Nyderlandai, Prancūzija, Rumunija, Suomija), keturios – stebėtojos (Belgija, Graikija, Slovėnija, Vokietija). Šešios šalys narės 2018 m. birželio 25 dieną, Europos Sąjungos užsienio reikalų tarybos susitikime Liuksemburge, pasirašė „Kibernetinio greitojo reagavimo pajėgų ir tarpusavio pagalbos kibernetinio saugumo srityje susitarimo memorandumą“. Prie pasirašiusiųjų – Lietuvos, Estijos, Ispanijos, Kroatijos, Olandijos ir Rumunijos – 2018 m. lapkričio 24 d. prisijungė ir Lenkija. Memorandumu šalys išreiškė politinę valią siekti glaudesnio bendradarbiavimo pagal projektą. Kibernetinio greitojo reagavimo komandos (toliau – komandos) padės viena kitai užtikrinti aukštesnį kibernetinio atsparumo lygį ir bendrai reaguos į kibernetinius incidentus. Iš skirtingų Europos Sąjungos šalių kibernetinių ekspertų sudarytos komandos keisis, budės kas pusmetį. Komandos taip pat galės padėti kitoms valstybėms narėms ir Europos Sąjungos institucijoms, bendroms saugumo ir gynybos politikos operacijoms ir šalims partnerėms. Šalys narės taip pat bendradarbiauja siekdamos sukurti bendrą kibernetinių įrankių rinkinį, kurį naudotų budinčios komandos. Šio projekto vadovai Tadas Šakūnas ir Eglė Vasiliauskaitė taip pat parengė teisinę ir politinę kibernetinių greitojo reagavimo pajėgų atmintinę, kuria gali naudotis projekto dalyviai ir kitos šalys, kurios norėtų prisijungti prie projekto ateityje.



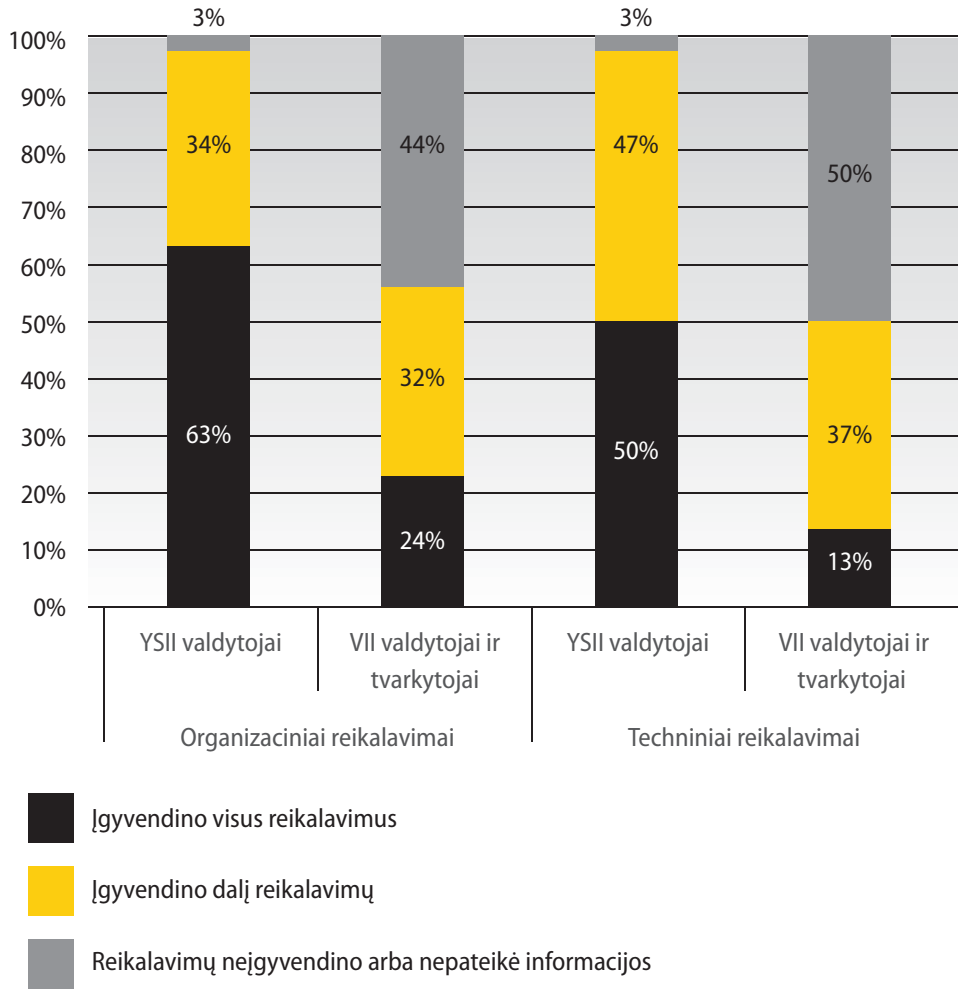


Teisinė ir politinė kibernetinių greitojo reagavimo pajėgų atmintinės, 2019.

Svarbu gerinti kibernetinio saugumo specialistų kompetenciją – nuolat savo gebėjimus išbandyti praktiškai. Dėl šios priežasties kibernetinio saugumo subjektai ir NKSC nuolat dalyvauja tarptautinėse kibernetinio saugumo pratybose, tokiose kaip „Locked Shields 2018", „Cyber Europe 2018" ir „Cyber Coalition 2018". Pažymėtina, kad praėjusiais metais visose iš jų buvo imituojamos kibernetinės atakos prieš ypatingos svarbos infrastruktūrą, akcentuojama tarpusavio priklausomybė, ugdomi eskalavimo, grėsmių valdymo ir kibernetinių atakų priskyrimo gebėjimai. Visi svarbiausios buvo pratybos „Kibernetinis skydas 2018", kurios 2018 m. buvo organizuotos kartu su Lietuvos kariuomenės pratybomis „Gintarinė migla 2018". Šių pratybų metu kibernetinio saugumo subjektai ne tik tobulino gebėjimus atpažinti kibernetinius incidentus ir apie juos informuoti kompetentingas institucijas, tačiau praktiškai buvo išbandytos komandos iškvietimo procedūros, kurių metu projekto dalyviai realiu laiku vertino, kokiu būdu būtų galima suteikti pagalbą Lietuvai. Pratybų metu įgyta patirtis buvo perkelta į greitojo reagavimo pajėgų iškvietimo atmintines.

Kibernetinio saugumo pratybos „Kibernetinis skydas 2018". Giedrės Maksimovicz nuotrauka

Kibernetinio saugumo subjektai taip pat toliau gerino kibernetinio saugumo būklę – įgyvendino Lietuvos Respublikos Vyriausybės nustatytus organizacinius ir techninius kibernetinio saugumo reikalavimus. Pažymėtina, kad YSII valdytojų reikalavimų įgyvendinime įvyko gera pažanga – šie subjektai įgyvendino 63 proc. organizacinių ir 50 proc. techninių kibernetinio saugumo reikalavimų (pernai YSII valdytojai buvo įgyvendinę tik 26 proc. organizacinių ir 6 proc. techninių kibernetinio saugumo reikalavimų) (29 pav.). Dauguma reikalavimų neįgyvendinusių subjektų yra numatę juos įgyvendinti ateityje (vėliausiai – iki 2021 m. sausio 1 d.). Pagrindines priežastis, trukdančias įgyvendinti reikalavimus, kaip ir 2017 m., valdytojai ir tvarkytojai nurodo kompetencijos, finansinių bei žmogiškųjų išteklių stoką, akcentuoja, kad reikalavimų kartelė yra pernelyg iškelta.



29 pav. YSII ir VII valdytojų ir tvarkytojų organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas (2018 m.)

IŠVADOS IR REKOMENDACIJOS

Išvados

1. **Lietuvos Respublikos Vyriausybės sprendimais sistemingai įgyvendinama šalies kibernetinio saugumo politika.** 2018 m. patvirtinta Nacionalinė kibernetinio saugumo strategija, kurioje iki 2023 m. buvo nustatytos svarbiausios nacionalinės kibernetinio saugumo politikos viešajame ir privačiame sektoriuose kryptys. Taip pat buvo užbaigta Lietuvos kibernetinio saugumo konsolidacija bei priimtas sprendimas kurti Saugų valstybinį duomenų perdavimo tinklą, jungiantį gyvybines valstybės funkcijas užtikrinančias institucijas.

2. **Statistiškai kibernetinių incidentų mažėjo, tačiau atakos tapo labiau rafinuotos.** 2018 m. Lietuvoje užregistruoti 53 183 kibernetinio saugumo incidentai, t. y. 3 proc. mažiau nei ankstesniais metais. Tačiau išaugo kibernetinių incidentų sudėtingumas, atakos tampa vis labiau rafinuotos, o jų ištirti automatizuotomis priemonėmis neįmanoma. NKSC ištyrė 914 didelės ir vidutinės reikšmės kibernetinių incidentų, o tai 41 proc. daugiau nei 2017 m.

3. **Didžiausios kibernetinio saugumo grėsmės kyla dėl didelio skaičiaus prie interneto prijungtų nesaugių įrenginių, pažeidžiamų interneto svetainių ir piktavališkų socialinės inžinerijos metodų naudojimo.** 2018 m. NKSC užregistravo 21 proc. daugiau įrenginių, kurie turi saugumo spragų. Pusė iš 52 000 interneto svetainių, turinčių TVS, Lietuvoje yra pažeidžiamos, subjektai vis dar nevertina IT teikiamų paslaugų ir RIS saugomos informacijos kaip turto. Socialinės inžinerijos metodais pagrįstų bandymų įsiskverbti į ryšių ir informacines sistemas NKSC 2018 m. užfiksavo 25 proc. daugiau negu 2017 m.

4. **Ypatingos svarbos informacinė infrastruktūra yra aktyvios kibernetinės veiklos objektas.** 2018 m. daugiausiai kenkimo PĮ aptikta valstybės valdymo (iš viso 39 proc.), energetikos (20 proc.) ir užsienio reikalų ir saugumo politikos (19 proc.) sektoriuose. Pernai 18 proc. išaugo elektroninių ryšių tinklų žvalgymo (skenavimo) veikla, kuomet ypač buvo domimasi energetikos, valstybės valdymo ir krašto apsaugos sektoriais.

5. **Informacinės atakos dažniausiai susijusios su gynybos sektoriumi.** 2018 m. neigiama informacinė veikla buvo nutaikyta į svarbiausias Lietuvos nacionalinio saugumo sritis. Lyginant su 2017 m., bendras neigiamos informacijos srautas, stebėtas Lietuvos informacinėje erdvėje, išliko stabilus ir didelis. Nustatyti 2 456 informacinių atakų atvejai, iš jų 29 proc. gynybos srityje.

Rekomendacijos

Socialinės inžinerijos metodais pagrįstų kibernetinių incidentų grėsmių valdymo rekomendacijos

1. Užvesti pelės žymeklį ant nuorodos ir patikrinti, ar atvaizduojamas interneto svetainės adresas yra tikras; įsitikinti, kad adrese nėra gramatinių klaidų, adreso pavadinimas logiškas ir lengvai perskaitomas.
2. Įsitikinti, kad sesija su interneto svetaine yra šifruojama, t. y. yra naudojamas SSL sertifikatas (interneto svetainės adresas turi prasidėti „https“ žyma), naudoti kelių faktorių autentifikavimo įrankius (pavyzdžiui, slaptažodis, mobilusis įrenginys, piršto antspaudas).
3. Saugoti savo prisijungimo slaptažodžius, jokiu būdu nelaikyti jų atviru tekstu darbo vietoje, kompiuteryje ar mobiliajame telefone.
4. 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. Neatidarinėti dokumentų turinio, siunčiamų failų ir PĮ, kurie yra atsiųsti ar parsisiųsti iš nepatikimo šaltinio (pavyzdžiui, iš nelegalios PĮ platinimo šaltinių).
6. Neatlikti skubotų veiksmų, nepasiduoti emocijoms, iki galo išsiaiškinti veiksmų, kuriuos prašoma atlikti, būtinumą.

Kenkimo PĮ kibernetinių incidentų grėsmių valdymo rekomendacijos

1. Naudoti legalią OS ir PĮ, antivirusinę PĮ, ja profilaktiškai skenuoti duomenis įrenginyje, nedelsiant įdiegti gamintojo PĮ atnaujinimus jiems pasirodžius.
2. Nesisiųsti failų iš nepatikimų šaltinių, naršyklėje įdiegti įskiepius kenkėjiškoms interneto svetainėms atpažinti, parsisiųstus įtartinus failus skenuoti antivirusine PĮ, tikrinti juos NKSC priemonėmis[11] .
3. Nesinaudoti nepatikimomis, nepatikrintomis atminties laikmenomis. Nuolat jas formatuoti, išjungti automatinį failų paleidimą.
4. Periodiškai daryti atsarginės duomenų kopijas, jas saugoti atskirai ir kitoje vietoje, nei jos buvo padarytos. Svarbią informaciją laikyti atskiroje laikmenoje ar laikmenose, neturinčiose tiesioginės sąsajos su internetu (pavyzdžiui, išorinėje laikmenoje).

[11] https://www.nksc.lt/irankiai.html

5. Šifruoti konfidencialią informaciją, jeigu būtina, apsaugoti ją saugiu slaptažodžiu. Informacijai perduoti naudoti kriptografines priemones, pavyzdžiui, elektroninių laiškų šifravimą.

6. Įstaigose taikyti tinklo segmentavimą, naudoti keletą filtravimo priemonių (pavyzdžiui, tinklo ir darbo stoties užkardą), svarbias RIS atskirti fiziškai.

Pažeidžiamų interneto svetainių kibernetinių incidentų grėsmių valdymo rekomendacijos

1. Pakeisti interneto svetainės TVS administratoriaus ir naudotojų prisijungimo adresus, periodiškai keisti slaptažodžius, įgalinti ribotą bandymų prisijungti skaičių.

2. Nuolat atnaujinti TS OS, TVS ir susijusius įskiepius, nenaudoti nereikalingų TVS įskiepių, naudoti taikomųjų programų ugniasienę (angl. *web application firewall*), uždrausti nenaudojamus prievadus, vykdyti interneto svetainės pažeidžiamumų skenavimus ir reguliarius žurnalinių įrašų (angl. logs) patikrinimus, įdiegti „reverse Proxy“ sprendimą, kad piktavalis negalėtų identifikuoti TVS.

3. Sukonfigūruoti ugniasienes taip, kad prie interneto svetainių TVS būtų galima jungtis tik iš patikimų IP adresų (sudaryti taip vadinamąjį „baltąjį“ sąrašą).

4. Perkant svetainės kūrimo, įdiegimo ir priežiūros paslaugas į sutartį įtraukti reikalavimą paslaugų teikėjui, kad šis užtikrintų interneto svetainės kibernetinį saugumą, apsaugą nuo įsilaužimų, užtikrintų jos atitiktį Lietuvos Respublikos Vyriausybės nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams.

5. Į interneto svetainę įdiegti SSL sertifikatą, kas užtikrins šifruotąjį ryšį. Tai viena efektyviausių kibernetinio saugumo priemonių interneto svetainėms.

6. Naudoti taikomųjų programų ugniasienę (angl. *web application firewall*), užsisakyti didesnį pralaidumą, įsigyti papildomas interneto svetainės prieglobos tiekėjo siūlomas prevencines DDoS paslaugas.

Elektroninių ryšių tinklų žvalgybos grėsmių valdymo rekomendacijos

1. Pakeisti įrenginių prievadus į rečiau naudojamus, išjungti nenaudojamus prievadus, įgalinti „reverse Proxy“, kad nebūtų įmanoma iš išorės identifikuoti aktyvių paslaugų ar PĮ.

Rangovų nepatikimumo ir PĮ grėsmių valdymo rekomendacijos

1. Rekomenduojama techninę ir PĮ įsigyti tik iš oficialių šaltinių ir tiekėjų, kurie veikia pagal Bendrojo duomenų apsaugos reglamento nuostatas 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 vaizdo kamerą, o organizacijoje – užkardyti bet kokią technologinio tinklo sąsają su internetu).
2. Rekomenduojama įsigyti techninę ir PĮ iš šaltinių, kurie yra nepriekaištingos reputacijos ir nėra iškilusios rizikos dėl bendradarbiavimo su ne NATO ir ES užsienio žvalgybos tarnybomis.
3. Suteikti ribotą rangovų prieigą prie RIS, vengiant suteikti nuotolinio prisijungimo prie RIS galimybę, stebėti ir audituoti komunikacijų žurnalinius įrašus.

Įrenginių saugumo spragų grėsmių valdymo rekomendacijos

1. Pakeisti IoT, pasiekiamų internetu ar per „bluetooth“ sąsają, prisijungimo slaptažodžius į saugius.
2. Reguliariai atnaujinti IoT įrenginių taikomąją ir PĮ.
3. IoT įrenginiuose išjungti slaptažodžių išsaugojimo galimybę.
4. Įsigyti ir naudoti įrenginius, kurių komunikacijos sesija yra šifruojama.
5. Jeigu yra galimybė, patikrinti, ar įrenginyje nėra perteklinio funkcionalumo (atvirų prievadų).
6. Prieš įsigyjant įrenginį, įsitikinti, ar jo gamintojas atitinka Bendrojo duomenų apsaugos reglamento reikalavimus, ar siunčiami duomenys yra saugomi ES teisės.
7. Vengti nežinomų gamintojų, kurių kilmės šalį ir patikimumą yra sudėtinga patikrinti.