



NACIONALINIS  
KIBERNETINIO  
SAUGUMO  
CENTRAS  
PRIE KRAŠTO  
APSAUGOS  
MINISTERIJOS

# 2017 METŲ NACIONALINIO KIBERNETINIO SAUGUMO BŪKLĖS ATASKAITA

# TURINYS

**TURINYS | 3**

**IVADAS | 4**

**SANTRAUKA | 6**

**1. LIETUVOS KIBERNETINIŲ GRĖSMIŲ ŽEMĖLAPIS | 8**

- 1.1. Programinės įrangos paplitimas Lietuvoje | 9
- 1.2. NKSC stebimų VII ir YSII tinklų kibernetinių incidentų metinė statistika | 10
- 1.3. Elektroninių paslaugų trikdymas | 11
- 1.4. Kibernetinių incidentų grėsmės lygis | 12
- 1.5. Kibernetinių incidentų kituose sektoriuose statistika | 13

**2. ELEKTRONINIŲ RYŠIŲ TINKLŲ ŽVALGYBA | 15**

**3. PAŽEIDŽIAMOS INTERNETO SVETAINĖS | 18**

**4. KIBERNETINIAI INCIDENTAI TURINTYS**

**SOCIALINĖS INŽINERIJOS POŽYMIŲ | 22**

- 4.1. Valstybinių institucijų interneto svetainių klastojimas | 24
- 4.2. Valstybinės institucijos darbuotojų slaptažodžių grobimas | 26
- 4.3. Bankų paslaugų klastojimas | 27
- 4.4. Kibernetinės atakos prieš išmaniųjų telefonų naudotojus | 29
- 4.5. Sukčiavimas imituojant vadovo laišką | 30

**5. ŽALINGOS PROGRAMINĖS ĮRANGOS PAPLITIMAS | 32**

**6. ORGANIZACINIŲ IR TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ ĮGYVENDINIMAS | 33**

**7. REZONANSINIAI KIBERNETINIAI INCIDENTAI | 39**

**8. PRATYBOS | 41**

**IŠVADOS, REKOMENDACIJOS IR PROGNOZĖS | 43**

Išvados | 43

Rekomendacijos | 45

Prognozės | 48

## IVADAS

Nacionalinis kibernetinio saugumo centras (toliau – NKSC) savo veiklą pradėjo 2015 m. sausio 1 d., įsigaliojus Lietuvos Respublikos kibernetinio saugumo įstatymui (2014 m. gruodžio 11 d. Nr. XII-1428). NKSC, pagal kompetenciją įgyvendindamas kibernetinio saugumo politiką ir vykdydamas valstybės informacinių išteklių (toliau – VII) ir ypatingos svarbos informacinių infrastruktūrų (toliau – YSII<sup>1</sup>) kibernetinių incidentų valdymo padalinio veiklą, rengia ir teikia pasiūlymus krašto apsaugos ministrui dėl organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų VII ir YSII, atlieka šių subjektų atitikties organizaciniais ir techniniais kibernetinio saugumo reikalavimams stebėseną. NKSC turi pareigą teikti konsultacijas ir rekomendacijas VII ir YSII valdytojams kibernetinio saugumo klausimais, analizuoti nacionalinę kibernetinio saugumo situaciją ir rengti nacionalinio kibernetinio saugumo būklės ataskaitas. Vienas NKSC uždavinių – rūpintis, kad YSII valdytojai turėtų kibernetinės gynybos planus ir gebėtų juos vykdyti.

Oksfordo universiteto Pasaulinis kibernetinio saugumo kompetencijos centras vadovaudamasis sukurtu kibernetinio brandumo modeliu (angl. Cybersecurity Maturity Model), 2017 m. atliko Lietuvos kibernetinio saugumo brandos vertinimą. Išanalizavęs kiekvienos iš modelio sudedamųjų dalių – kibernetinio saugumo strategijos rengimo stadijos bei politikos, kultūros ir visuomenės – teisinį reguliavimą, verslo modelį bei technologijų integralumą, Lietuvos kibernetinio saugumo brandą įvertino „vidutiniškai“. Efektyvinant šalies kibernetinio saugumo pajėgumus ir užtikrinant įstatymu reglamentuotų funkcijų vykdymą nacionaliniu mastu, 2018 m. sausio 1 d. įgyvendintas kibernetinio saugumo ir elektroninių ryšių tinklų saugos padalinių ir funkcijų konsolidavimas. NKSC pradėjo veikti kaip atskiras juridinis asmuo prie Krašto apsaugos ministerijos (toliau – KAM), sujungęs Kibernetinio saugumo ir telekomunikacijų tarnybos prie KAM (nuo 2018 m. sausio 1 d. – Informacinių technologijų tarnyba prie KAM), Vyriausybinių ryšių centro prie KAM ir Ryšių reguliavimo tarnybos Saugumo incidentų tyrimų padalinio (toliau – CERT-LT) kibernetinio saugumo specialistus. Nuo 2018 m. sausio 1 d. Kibernetinio saugumo įstatymu sujungus NKSC ir Ryšių reguliavimo tarnybos Saugumo incidentų tyrimų padalinio

funkcijas ir įgaliojimus, suponuojama kryptinga ir nuosekli kibernetinio saugumo ir elektroninių ryšių tinklų apsauga šalies mastu.

2017 m. NKSC, užtikrindamas kibernetinio saugumo būklės stebėseną, diegė technines priemones YSII ir VII valdytojų ir tvarkytojų valdomose infrastruktūrose. Stebimos erdvės plėtra davė akivaizdžių rezultatų – buvo rasta ir neutralizuota daugiau nei keturi šimtai standartinėmis saugumo užtikrinimo priemonėmis neaptinkamos žalingos programinės įrangos veikimo atvejų.

<sup>1</sup> Ypatingos svarbos informacinė infrastruktūra (YSII) Kibernetinio saugumo įstatyme apibrėžta kaip privataus ar viešojo administravimo subjekto valdoma informacinė infrastruktūra, kurioje įvykęs kibernetinis incidentas gali padaryti didelę žalą nacionaliniam saugumui, šalies ūkiui, valstybės ir visuomenės interesams.

## SANTRAUKA

2017 m. nacionalinio kibernetinio saugumo būklės ataskaitą NKSC rengia ir teikia krašto apsaugos ministrui, vadovaudamasis Lietuvos Respublikos kibernetinio saugumo įstatymo (toliau – Įstatymas) 10 str. 2 d. 6 p. nuostata. Nacionalinio kibernetinio saugumo būklė yra vertinama atsižvelgiant į dominuojančias kibernetinio saugumo grėsmes ir šalies gebėjimą jas valdyti. Ataskaita parengta remiantis NKSC techninėmis stebėsenos priemonėmis surinktais duomenimis, organizacijų pateikta bei iš kitų šaltinių gauta informacija.

2017 m. buvo fiksuojamas VII ir YSII elektroninių ryšių tinklų žvalgybos intensyvėjimas. Pastebėta, kad dažniau buvo skenuojami ir įrenginiai, kurie veikia technologiniuose procesuose ir turi sąsają su internetu, o prieš šiuos įrenginius nukreiptos kibernetinės atakos<sup>2</sup> gali sukelti fizinės plotmės pasekmes, kai paveikus technologinius ir pramoninius procesus būtų sutrikdyta gyventojų kasdieninė veikla ir ūkio subjektų teikiamos paslaugos.

NKSC fiksavo didėjantį kibernetinių incidentų kiekį – buvo platinama žalingo kodo programinė įranga, dažniausiai naudojant socialinės inžinerijos principais paremtas kibernetines atakas prieš žmogiškąjį faktorių. Žalingos programinės įrangos paplitimas, palyginti su 2016 m., išaugo viešojo saugumo ir teisinės tvarkos, užsienio reikalų ir saugumo politikos sektoriuose. Energetikos sektoriuje žalingos programinės įrangos paplitimas liko didelis.

Didelio masto elektroninių paslaugų trikdymo (DDoS) atvejų valstybiniu mastu, kaip kad 2016 m., užfiksuota nebuvo, tačiau bendra tokio pobūdžio atakų tendencija išliko nepakitusi. Lietuvoje dažniausiai yra vykdomos kibernetinės atakos, kurių grėsmės lygis – vidutinis, t. y. atakų nutaikymo metodai ir technologijos nėra itin pažangios, vis dėlto NKSC periodiškai aptinka techniškai itin sudėtingų kibernetinių atakų. Rezonansinės kibernetinės atakos (WannaCry, NotPetya), vykusios pasauliniu mastu, Lietuvos VII ir YSII nepaveikė.

2017 metais Lietuvos Respublikos ryšių reguliavimo tarnyboje veikęs nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo pada-

linys CERT-LT apdorojo 54 414 incidentus. Palyginti su 2016 metais (49 463 atvejai), kibernetinių incidentų viešuosiuose ryšių tinkluose užregistruota dešimtadaliu daugiau. Didžiausios kibernetinio saugumo problemos privačiame sektoriuje 2017-aisiais buvo kenkimo programinė įranga (kenkimo kodai) ir nesaugios informacinės sistemos, įskaitant interneto svetaines.

Visų kibernetinių incidentų tyrimų padalinių tirtų incidentų skaičius siekė 54 950, tiek viešajame, tiek privačiame sektoriuose bendrai. Tokio masto incidentų statistika signalizuoja didelį kibernetinio saugumo iššūkį, tenkantį Lietuvos elektronei erdvei, piliečiams, viešajam sektoriui ir verslui.

Atlikus Lietuvos viešojo sektoriaus interneto svetainių pažeidžiamumo vertinimą, buvo nustatyta, kad 2017 m. pažeidžiamų interneto svetainių, į kurias įsilaužti pakanka pasinaudoti jau žinomais pažeidžiamumais, skaičius didėjo. Organizacijos ir toliau vengia laiku atnaujinti svetainėse naudojamą programinę įrangą, o įsigydamos svetainių palaikymo ir administravimo paslaugas į pirkimo sutartis neįtraukia prievolės užtikrinti kibernetinio saugumo reikalavimus.

NKSC fiksavo didėjančią valstybės informacinių išteklių valdytojų ir tvarkytojų, ypatingos svarbos informacinės infrastruktūros valdytojų organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimo apimtį (matyti progresas) – dalis organizacijų sukūrė arba atnaujino saugos politiką nustatančius bei ją įgyvendinančius dokumentus, įdiegė technines priemones, susijusias su kibernetinio saugumo stiprinimu organizacijoje. Per 2017 m. VII valdytojų ir tvarkytojų, iš dalies įgyvendinusių Vyriausybės patvirtintus organizacinius reikalavimus, skaičius padidėjo 47 proc., o visus reikalavimus įgyvendinusiųjų skaičius išaugo 11,5 proc. Pastebimas didėjantis organizacijų susirūpinimas kibernetiniu saugumu, o dauguma organizacijų yra susiplanusios reikalavimus atitikti ateityje. Vis dėlto, didžioji dalis subjektų laiku neįvykdė visų Vyriausybės nustatytų organizacinių ir techninių kibernetinio saugumo reikalavimų.

<sup>2</sup> Kibernetinė ataka – tai bet kokio pobūdžio kenkėjiška veikla kibernetinėje erdvėje, nukreipta prieš elektroninių ryšių tinklus, informacines sistemas ar pramoninių procesų valdymo sistemas.

# LIETUVOS KIBERNETINIŲ GRĖSMIŲ ŽEMĖLAPIS

2017 m. NKSC stebėjo potencialiai didžiausią žalą Lietuvos kibernetiniam saugumui keliančias grėsmes ir kibernetinio saugumo būklės tendencijas (1 pav.).

↑ žalingos programinės įrangos plitimas;

↑ pažeidžiamos interneto svetainės;

↑ socialinė inžinerija;

↑ elektroninių ryšių tinklų žvalgyba;

➔ elektroninių paslaugų trikdymas;

↑ organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas VII ir YSII.

1 pav. 2017 m. kibernetiniam saugumui kilusios grėsmės ir jų tendencijos, palyginti su 2016 m.

2017 m. tendencingai plito žalinga programinė įranga, daugėjo pažeidžiamų interneto svetainių, plito socialinės inžinerijos metodų taikymas kibernetinėje erdvėje, elektroninių ryšių tinklų žvalgybos atvejų skaičius taip pat augo. Didelio masto rezonansinių elektroninių paslaugų trikdymo (DDoS) atvejų valstybiniu mastu, kaip kad 2016 m., užfiksuota nebuvo, tačiau bendra tokio pobūdžio atakų tendencija išliko nepakitusi. 2017 m. YSII ir VII organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimo lygis gerėjo. NKSC prielaidas patvirtina CERT-LT 2017 m. duomenys, pagal kuriuos didžiausios Lietuvos kibernetinio saugumo grėsmės – kenkimo programinė įranga ir nesaugios informacinės sistemos, tarp jų ir interneto svetainės. NKSC atkreipia dėmesį, kad šios dvi grėsmės tarpusavyje koreliuoja, t. y. nesaugios interneto svetainės, manipuliuojant jų pažeidžiamumais, yra užvaldomos ir naudojamos tolesnei kenkėjiškai veiklai vykdyti. Į užvaldytas interneto svetaines gali būti dedamas žalingas kodas arba nuorodos į žalingą kodą

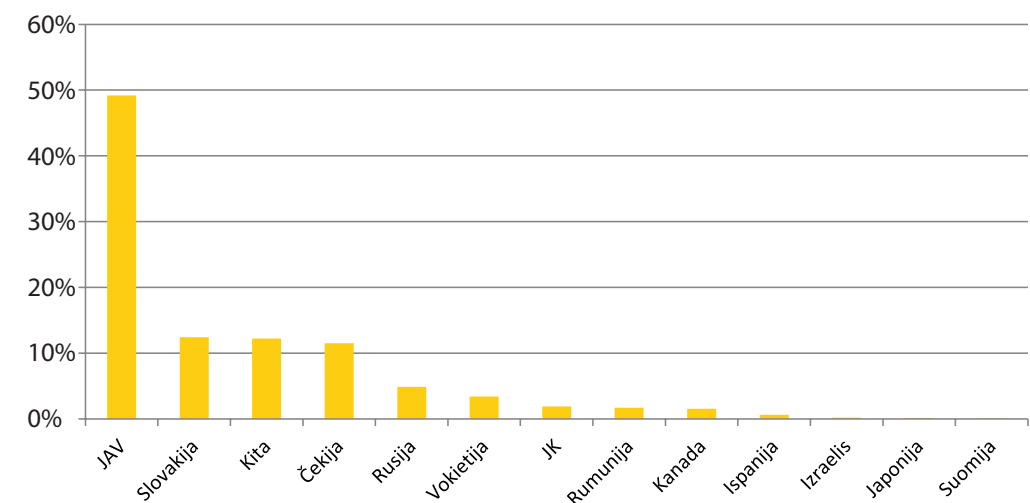
platinančias kitas interneto svetaines, kuriomis siekiama užkrėsti svetainių lankytojų kompiuterius duomenis šifruojančiais virusais, arba priversti užvaldytus kompiuterius „kasti“ kriptovaliutą.

## Programinės įrangos paplitimas Lietuvoje

Galiniai įrenginiai, turintys prieigą prie interneto, yra labiausiai pažeidžiama organizacijų informacinių sistemų vieta. Kibernetiniam saugumui užtikrinti skirta programinė įranga (toliau – PI) padeda užkardyti grėsmes, tačiau turėdama visas privilegijas, įskaitant išorės subjektų prisijungimo galimybę, pati dažniausiai yra nekontroliuojama.

2017 m. NKSC, atlikdamas kibernetinio saugumo būklės Lietuvos viešojo sektoriaus institucijose vertinimą, taip pat nustatė labiausiai paplitusios saugumo PI, daugiausiai kenksmingą kodą stabdančios, kilmės šalis. Buvo apklausta per 700 respondentų. Tyrimo imtį sudarė YSII valdytojai, Lietuvos valstybės institucijos, įstaigos ir kitos valstybės informacinius išteklius valdančios ir tvarkančios organizacijos.

Respondentų pateiktais duomenimis, daugiausia įstaigų galiniuose įrenginiuose naudoja kibernetinį saugumą užtikrinančią PI, kurios kilmės šalis yra Jungtinės Amerikos Valstijos – tai sudaro 49,18 proc. visos respondentų naudojamos programinės įrangos. PI, kurios kilmės šalis Slovakija – 12,45 proc., Čekija – 11,53 proc. Rusijoje pagamintą kibernetiniam saugumui užtikrinti skirtą programinę naudoja 4,89 proc. respondentų (2 pav.).



2 pav. Bendras PI paplitimas šalies įstaigose pagal PI kilmės šalį

NKSC atkreipia dėmesį, kad kibernetiniam saugumui skirta programinė ir techninė įranga yra tik dalis priemonių, kuriomis yra užtikrinamas kibernetinis saugumas. Itin svarbus organizacijų darbuotojų ir kompiuterių naudotojų švietimas ir sąmoningumo didinimas kibernetinio saugumo klausimais. Be to, papildomos kibernetinės grėsmės organizacijos tinkluose gali atsirasti dėl nekontroliuojamos rangovų ir subrangovų veiklos ir papildomos kontrolės stokos. Dėl šių priežasčių svarbu skatinti organizacijas vertinti ir tobulinti kibernetinio saugumo būklę, atsižvelgiant į jų vidinę organizacinę aplinką; įgyvendinti Vyriausybės nustatytus organizacinius ir techninius kibernetinio saugumo reikalavimus.

### NKSC stebimų VII ir YSII tinklų kibernetinių incidentų metinė statistika

NKSC 2017 m. užfiksavo 8 didelės ir 528 vidutinės reikšmės kibernetinius incidentus. Daugiausiai vidutinės reikšmės incidentų susiję su kenkimo programinės įrangos veikimu. Palyginimui, 2016 m. užfiksuoti 489 didelės bei vidutinės reikšmės incidentai.

Remiantis NKSC fiksuojamais duomenimis galima daryti išvadą, kad užfiksuojamų kibernetinių incidentų kiekis Lietuvoje didėja.

1 lentelė. NKSC užfiksuoti didelės ir vidutinės reikšmės kibernetiniai incidentai 2017 m.

| Grupė                     | Kategorija         | I ketv.    | II ketv.  | III ketv.  | IV ketv.   | Iš viso incidentų: |
|---------------------------|--------------------|------------|-----------|------------|------------|--------------------|
| Kenkimo programinė įranga | Didelės reikšmės   | 1          | 0         | 4          | 1          | <b>6</b>           |
|                           | Vidutinės reikšmės | 97         | 81        | 134        | 180        | <b>492</b>         |
| Įsilaužimas               | Didelės reikšmės   | 0          | 1         | 0          | 1          | <b>2</b>           |
|                           | Vidutinės reikšmės | 0          | 1         | 1          | 0          | <b>2</b>           |
| RIS* trikdymas            | Didelės reikšmės   | 0          | 0         | 0          | 0          | <b>0</b>           |
|                           | Vidutinės reikšmės | 0          | 1         | 0          | 0          | <b>1</b>           |
| Vientisumo pažeidimas     | Vidutinės reikšmės | 28         | 0         | 2          | 3          | <b>33</b>          |
| Iš viso incidentų:        |                    | <b>126</b> | <b>84</b> | <b>141</b> | <b>185</b> | <b>536</b>         |

\*RIS- ryšių ir informacinės sistemos

### Elektroninių paslaugų trikdymas

Viena iš populiariausių kibernetinių atakų, nukreiptų prieš elektronines paslaugas, yra paskirstytas paslaugų trikdymas (angl. Distributed Denial of Service, DDoS), kuriuo siekiama paveikti teikiamų elektroninių paslaugų ir tarnybinių stočių prieinamumą.

NKSC tyrė vykusią plataus masto DDoS ataką prieš vieną iš VII valdytojų: kibernetinė ataka buvo nutaikyta prieš sveikatos sektoriaus interneto svetainę, kartu puolant ir kitus subjektus tame pačiame IP režyje. Į įstaigos svetainę buvo nukreiptas „TCP SYN Flood“ srautas iš daugiau nei 10 000 IP adresų. Incidentas priskirtas vidutinės reikšmės kibernetinių incidentų kategorijai.

NKSC atkreipia dėmesį, kad, įvairių šaltinių duomenimis, daugėja daiktų interneto įrenginių (angl. Internet of Things) užvaldymo ir išnaudojimo DDoS atakoms vykdyti atvejų. 2017 m. CERT-LT užfiksavo 24 612 įrenginius, turinčius saugumo spragų (2016 m. – 20 490 įrenginių)<sup>3</sup>.

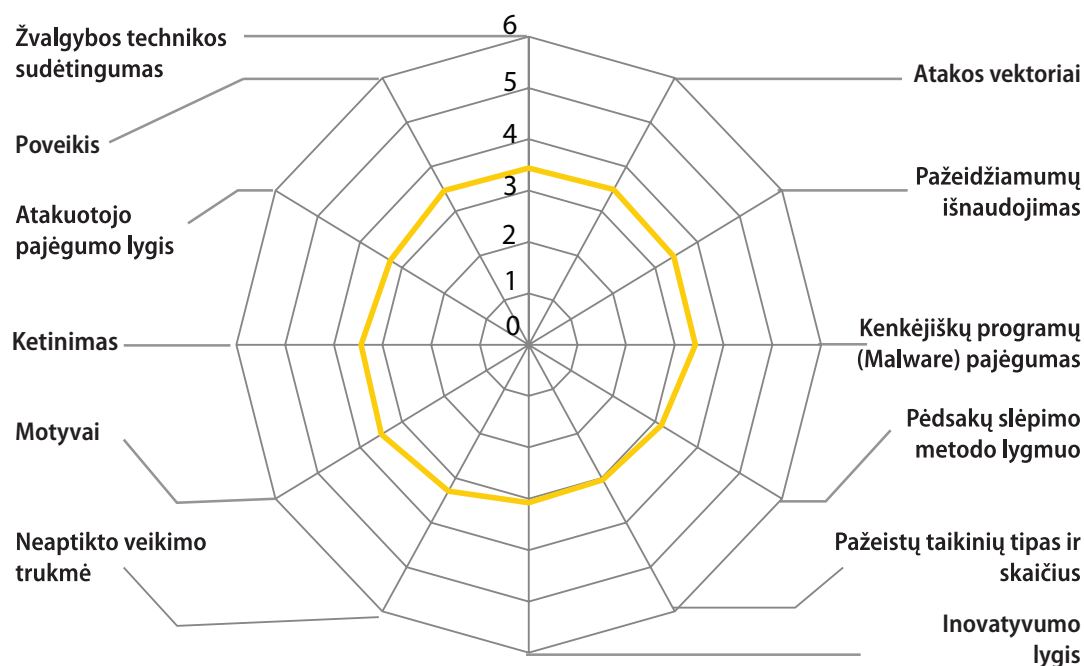
NKSC pažymi, kad apsaugos priemonės turėtų būti suderintos ir diegiamos paslaugos teikėjo infrastruktūroje.

<sup>3</sup> Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio 2017 m. veiklos ataskaita. <https://www.cert.lt/doc/2017.pdf>

## Kibernetinių incidentų grėsmės lygis

Siekdamas nustatyti 2017 m. vykusią kibernetinių atakų grėsmės lygį, NKSC vykdė vidutinės ir didelės reikšmės kibernetinių incidentų analizę, išnagrinėjo ir įvertino atakoms vykdyti naudotas žalingos programinės įrangos pažangumą, tikėtinus jų vykdytojus, motyvus, ketinimus, technologinį atakų modernumą ir kitus grėsmės lygį sąlygojančius rodiklius.

Lietuvoje dažniausiai yra vykdomos kibernetinės atakos, kurių grėsmės lygis – vidutinis, t. y. atakų nutaikymo metodai ir technologijos nėra itin pažangios (3 pav.). Nepaisant to, NKSC periodiškai aptinka techniškai itin sudėtingų, tęstinių ir tikslingai nukreiptų kibernetinių atakų, kurių tikslas yra konkrečių sistemų užvaldymas ir informacijos grobimas.



3 pav. NKSC 2017 m. nagrinėtų kibernetinių incidentų grėsmės įvertinimo vidurkis

## Kibernetinių incidentų kituose sektoriuose statistika

2017 metais Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apdorojo 54 414 incidentų pagal pranešimus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų. Palyginti su 2016 metais (49 463 atvejai), kibernetinių incidentų užregistruota dešimtadaliu daugiau.

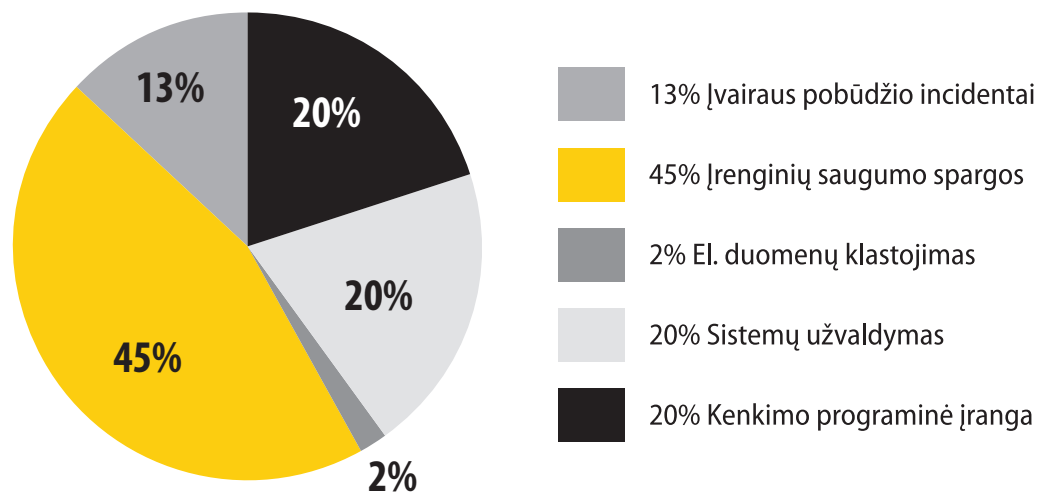
2 lentelė. CERT-LT 2017 m. nagrinėti incidentai pagal jų tipus

| Apdorotų pranešimų tipai            | 2017 metų laikotarpis |          |           |          |          |
|-------------------------------------|-----------------------|----------|-----------|----------|----------|
|                                     | I ketv.               | II ketv. | III ketv. | IV ketv. | Iš viso: |
| Apie kenkimo programinę įrangą      | 2 580                 | 2 755    | 2 898     | 2 606    | 10 839   |
| Apie informacinių sistemų užvaldymą | 2 962                 | 2 775    | 2 704     | 2 510    | 10 951   |
| Apie el. paslaugos trikdymo atakas  | 12                    | 7        | 11        | 20       | 50       |
| Apie el. duomenų klastojimą         | 340                   | 376      | 257       | 264      | 1 237    |
| Apie vientisumo pažeidimus          | 2                     | 7        | 4         | 2        | 15       |
| Apie įrenginių saugumo spragas      | 5 848                 | 5 938    | 6 464     | 6 362    | 24 612   |
| Įvairaus pobūdžio                   | 2 899                 | 1 672    | 943       | 1 196    | 6 710    |

Kaip rodo incidentų statistika, Lietuvoje matomos dvi didžiausios kibernetinio saugumo problemos – kenkimo programinė įranga (kenkimo kodai) ir nesaugios informacinės sistemos, įskaitant interneto svetaines. Minėtos saugumo problemos papildoma viena kita ir didina potencialią interneto naudotojų riziką. CERT-LT duomenimis, 2017 metais Lietuvoje kiekvieną mėnesį buvo užfiksuojama apie 3 000 kompiuterių, kurie, savininkams nežinant, buvo valdomi nuotoliniu būdu.

2017 m. informacinių sistemų užvaldymo incidentų užfiksuota 10 951 (2016 m. užvaldymo atvejų buvo 10 673). Prie šio tipo incidentų priskiriami užvaldyti įrenginiai, kurie naudojami kenkimo veikai, ir pažeistos, užvaldytos interneto svetainės. CERT-LT kiekvieną dieną užfiksuoja vidutiniškai po 10 naujų užvaldytų svetainių atvejų. Nuo rudens matomas didėjantis užvaldytų svetainių naudojimas kriptovaliutoms generuoti.

Populiarėjant kriptovaliutoms, itin aktyviai veikia ir išpirkos reikalaujančių virusų (angl. ransomware) kūrėjai. Nuo šio viruso nukenčia tiek pavieniai naudotojai, tiek ir įmonės. 2017 m. kenkimo programinės įrangos incidentų užfiksuota 10 839 (2016 m. – 11 212).



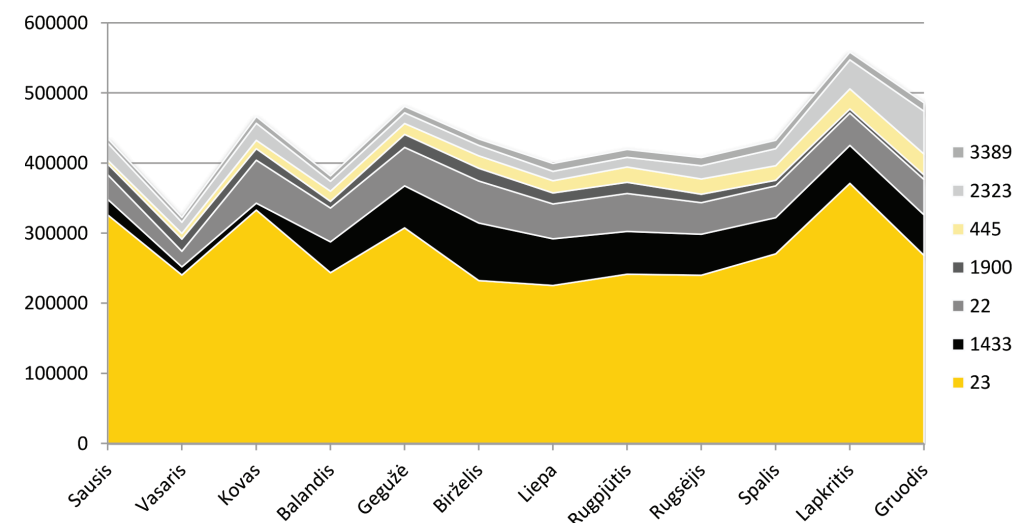
4 pav. 2017 m. pagrindiniai incidentų tipai privačiame sektoriuje

Vis daugiau interneto naudotojų patiria didelių nuostolių dėl kibernetinių sukčiavimų. Apgaulingi el. laiškai iš neva įmonės vadovų, kuriuose pavaldinio prašoma atlikti „skubų pavedimą“ (angliškai tai vadinama „C-level fraud“), ir toliau buvo intensyviai platinami. 2017 m. toliau daugėjo populiarių interneto svetainių klastojimo atvejų – CERT-LT ištyrė 1 237 pranešimus apie svetainių klastojimą (angl. phishing). 2016 m. jų buvo 555. Piktavaliai kuria interneto svetainių klastotes, siekdami iš to pasipelnyti. 2017 m. toliau buvo siuntinėjami el. laiškai, trumposios žinutės (SMS) neva iš banko su nuoroda į banko tinklalapio klastotę.

## ELEKTRONINIŲ RYŠIŲ TINKLŲ ŽVALGYBA

Viena labiausiai paplitusių, paprasčiausių ir sąlygiškai efektyviausių kibernetinės žvalgybos priemonių 2017 m. tebebuvo tinklo įrenginių prievadų skenavimas. Prievadai skenuojami gali būti vykdomas nebūtinai siekiant įgyvendinti piktavališkus tikslus, tačiau šis žvalgybos būdas tebėra vienas iš pirmųjų žingsnių siekiant surinkti informaciją apie konkrečius įrenginių tipus, įgalintas paslaugas ir protokolus, veikiančią programinę įrangą ir kitus galimus pažeidžiamumus tolesnėms kibernetinėms atakoms vykdyti. 2017 m. prievadų žvalgybos atvejų skaičius augo. Palyginti su 2016 m., ypač padidėjo susidomėjimas 23 prievadu (šiuo prievadu, kaip kad numatyta, įrenginiai gali būti valdomi nešifruotu Telnet protokolu).

Palyginus NKSC surinktą prievadų skenavimo statistiką su CERT-LT teikiama aktualia atakuojamų paslaugų prievadų statistine informacija, galima teigti, kad dažniausiai skenuojami tie patys prievadai tiek viešajame, tiek privačiame sektoriuose – 23, 22, 445, 1433.



5 pav. 2017 m. prievadų skenavimo statistika NKSC stebimoje erdvėje

NKSC 2017 m. ypatingą dėmesį skyrė technologiniuose procesuose naudojamų prievadų žvalgybos stebėsenai: skenavimų skaičius auga ir koreliuoja su kitų prievadų skenavimo statistika.

3 lentelė. Įrenginių, naudojamų technologiniuose procesuose, žvalgybos populiarumo statistika pagal protokolus ir (arba) įrangos gamintojus 2017 m.

| Nr. | PAVADINIMAS                  | Proc. |
|-----|------------------------------|-------|
| 1.  | BACnet                       | 20,7  |
| 2.  | Modbus                       | 15,4  |
| 3.  | Niagara Tridium Fox          | 12,8  |
| 4.  | Siemens S7                   | 9,0   |
| 5.  | EtherNet/IP                  | 8,2   |
| 6.  | DNP3                         | 6,3   |
| 7.  | Mitsubishi Electric MELSEC-Q | 5,0   |
| 8.  | Omron FINS                   | 4,9   |
| 9.  | PCWorx                       | 3,6   |
| 10. | HART-IP                      | 3,2   |
| 11. | ProConOS                     | 2,9   |
| 12. | Red Lion Controls Crimson V3 | 2,8   |
| 13. | Codesys                      | 2,6   |
| 14. | GE Industrial Solutions-SRTP | 2,2   |
| 15. | IEC 60870-5-104              | 0,3   |

Stebimi prievadai susiję su įrenginiais, pvz., programuojamais loginiais valdikliais, kuriais gali būti valdomi konkretūs technologiniai procesai, galintys kurti kinetinius efektus (pvz., tokie įrenginiai gali būti naudojami kontroliuojant vandens valymo įrenginius, valdant elektros energijos tiekimą, paskirstymą, transporto valdymo sistemas ir kt.).

NKSC stebima kibernetinė erdvė yra žvalgoma iš įvairių valstybių teritorijų. Svarbu pabrėžti, kad IP adresai, tiriant skenavimų statistiką, nurodo tik galutinių skenavimų atliekančių įrenginių geografinę vietą. Tikrieji skenavimus vykdančios subjektai prisijungimams prie šių įrenginių gali naudoti tarpinius sujungimus, todėl tikroji jų geografinė buvimo vieta remiantis pirminiais duomenimis negali būti nustatyta.

Dažniausiai Lietuvos erdvė skenuojama (įskaitant ir pramoniniuose tinkluose naudojamų prievadų paiešką) iš šių valstybių teritorijų: Jungtinių Amerikos Valstijų, Rusijos, Kinijos. Pažymėtina, kad daugiau negu pusė ieškomų pramoninių

se tinkluose veikiančių įrenginių naudoja BACnet, ModBus, Niagara Tridium Fox ir Siemens S7 protokolus (3 lentelė). Trečdalis IP adresų, iš kurių buvo skenuojama NKSC stebima kibernetinė erdvė, įvairių šaltinių apibūdinami kaip kenksmingą veiklą vykdančios adresai.

Pramoninius procesus valdantys įrenginiai, kurie veikia specifiniuose tinkluose, dažnai esti prijungti prie galinių įrenginių, turinčių sąsają su internetu, kurie nebūna laiku atnaujinami dėl jų specifikos arba dėl didelės kainos. Dėl šios priežasties išauga kibernetinių atakų, nukreiptų į pramoninius tinklus, grėsmės tikimybė, todėl svarbu užtikrinti, kad informacinės sistemos, kuriomis kontroliuojami pramoniniai procesai, neturėtų sąsajų su internetu arba būtų papildomai apsaugoti komunikacijos šifravimu.

## PAŽEIDŽIAMOS INTERNETO SVETAINĖS

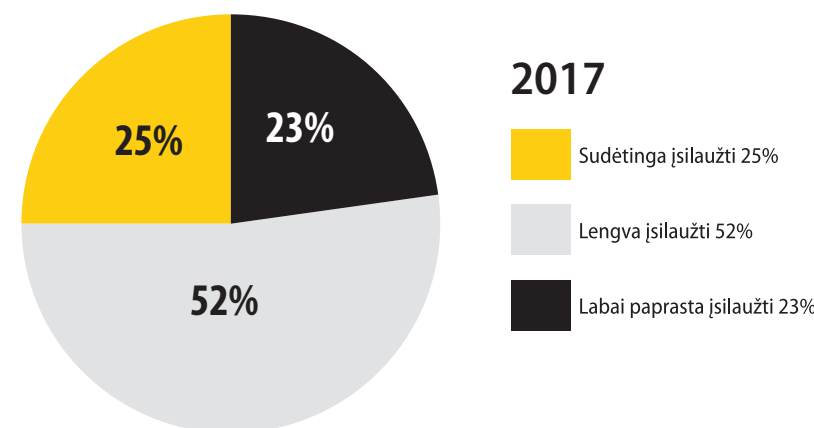
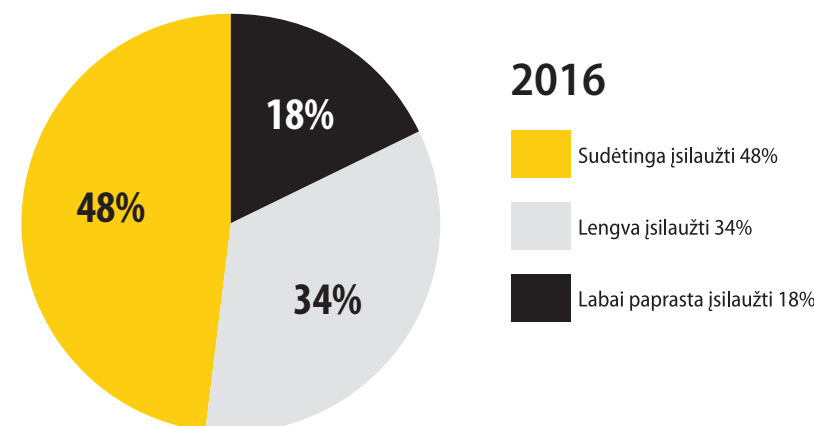
Organizacijos interneto svetainėse skelbia informaciją apie savo vykdomą veiklą ir teikiamas paslaugas. Svarbu pabrėžti, kad organizacijos, priklausomai nuo teikiamų paslaugų spektro, naudojasi skirtingomis įvairaus sudėtingumo informacinių technologijų priemonėmis ir paslaugų įsigijimą ir palaikymą finansuoja skirtingai, o kokybė dažnai nėra vertinama vadovaujantis saugumo kriterijais.

Organizacijų interneto svetainės yra pasiekiamos konkrečiais domeno vardais, kurie interneto vardų registre yra susieti su svetainių prieglobos tarnybinės stoties (toliau – TS) IP adresais. TS esanti programinė įranga apdoroja į svetainę atėjusias užklausas ir perduoda informaciją užklausą pateikusiam subjektui. Kibernetinė ataka šiuo atveju gali būti manipuliavimas ir netipinių darbo sąlygų sukūrimas išprovokuojant TS programinių ir aparatinių komponentų sutrikimus, sukuriant galimybę paveikti svetainės komponentus ir dedamos informacijos vientisumą, konfidencialumą ir prieinamumą.

TS programinė įranga (toliau – PI) susideda iš: operacinės sistemos (toliau – OS), svetainės tinklalapių transliavimo tarnybos, hiperteksto interpretatoriaus, turinio valdymo sistemos (toliau – TVS) ir kitų papildomų tinklo tarnybų, tokių kaip, elektroninio pašto, duomenų mainų ar nuotolinio administravimo programos. Programinėje įrangoje pasitaiko klaidų – pažeidžiamumų, kuriuos išnaudojant, atakos metu gali būti sutrikdomas įprastas programos darbas, atsirasti galimybė įkelti žalingą programinį kodą, gauti prieigą prie duomenų fragmento, keisti šiuos duomenis arba visiškai sutrikdyti programos, o kartu ir interneto svetainės veikimą.

Į pažeistas svetaines įkeliamas kenkėjiškas kodas, siekiant jį toliau platinti, užkrėsti svetainės lankytojus; išnaudoti svetaines kaip tarpines stotis kitų atakų valdymo komunikacijai.

Siekdamas nustatyti interneto svetainių saugos lygį ir pokyčius, 2017 m. NKSC vykdė du interneto svetainių saugos patikrinimus. Pagal pradinį interneto svetainių sąrašą buvo tikrinama apie 1 200 viešojo sektoriaus interneto svetainių adresų. Tyrimas buvo atliktas remiantis statistiniu modeliavimu, analizuojant įprasto svetainės naršymo metu gautą tarnybinės stoties siunčiamą informaciją (GET request



6 pav. Viešojo sektoriaus interneto svetainių kibernetinio saugumo būklė 2016 - 2017 m. \*

HTTP header banner), techninius duomenis, gautus iš viešųjų katalogų duomenų bazių, ir pasyvaus skenavimo priemonėmis gautą informaciją apie prieglobos tarnybinių stočių ir svetainės transliavimo tarnybų programinę įrangą. Buvo vertinamos tinklo tarnybos, veikiančios TCP/IP protokolu 80, 443 prievadais.

Tyrimo metu nustatyta, kad 2017 m. 23 proc. tirtų viešojo sektoriaus svetainių gali būti sutrikdytos žemos kvalifikacijos, 52 proc. vidutinės ir 25 proc. aukštos kvalifikacijos įsibrovėlių. Plg.: 2016 m. beveik į penktadalį svetainių (18 proc.) buvo

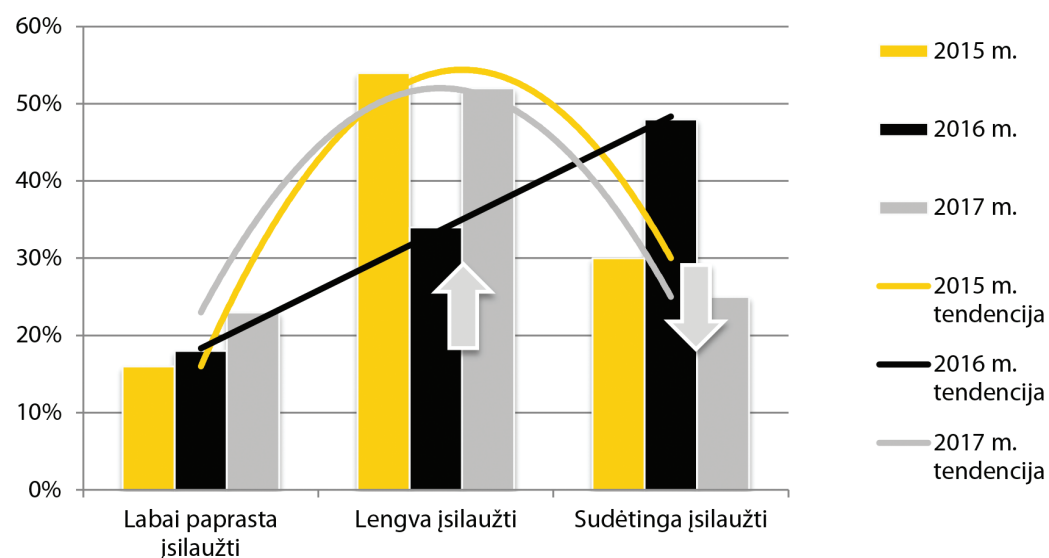
\* Labai paprasta įsilaužti – įsilaužti nereikalingos techninės žinios ar ypatingi programavimo įgūdžiai. Sėkmingai atakai įvykdyti nesudėtingai atkuriami reikiami algoritmai, internete lengvai randamos reikalingų veiksmų instrukcijos.  
Lengva įsilaužti – įsilaužti reikalingi įgūdžiai ir žinios, dažniausiai publikuojamos uždaroje grupėse.  
Sudėtinga įsilaužti – įsilaužti reikalingos kvalifikuotų specialistų, dažnai ne vieno atakuotojo, žinios, nes pažeidžiamumai dar nėra viešai publikuojami.

galima įsilaužti neturint išsamių techninių žinių ar ypatingų programavimo įgūdžių, į 34 proc. svetainių buvo galima įsilaužti, turint įgūdžių ir žinių, o 48 proc. svetainių buvo sąlygiškai saugios, į jas įsilaužti reikėjo kvalifikuotų specialistų žinių (6 pav.).

Dažniausiai interneto svetainėms užvaldyti išnaudojamos TS programinės įrangos, TVS ir jos įskiepių saugumo spragos, nepakankama TS saugumo konfigūracija, piktnaudžiavimas administravimo privilegijomis ir prieiga, nesudėtingi slaptažodžiai.

2017 m. daugėjo atvejų, kai užvaldytos interneto svetainės buvo naudojamos kriptovaliutoms generuoti, interneto svetainių lankytojų kompiuterius panaudojant skaičiavimams atlikti. Lankytojai, atvėrę užkrėstą svetainę, patys to nežinodami, įgalina veikti į ją įkeltą programinį kodą, kuris ima generuoti kriptovaliutą svetainės įsibrovėlių vardu. Pastebima, kad tam tikrais atvejais, kriptovaliutai generuoti skirtas programinis kodas galėjo būti įkeliamas ir pačių interneto svetainių savininkų iniciatyva.

Plg. 2015 – 2017 m. duomenis (2016 m. fiksuota teigiama svetainių saugumo tendencija), 2017 m. svetainių, į kurias buvo labai paprasta įsilaužti, nežymiai daugėjo (23 proc.), svetainių, į kurias lengva įsilaužti, skaičius augo labiausiai (nuo 34 proc. iki 52 proc.), ir svetainių, į kurias sudėtinga įsilaužti, palyginti su 2016 m. – skaičius mažėjo (iki 25 proc.) (7 pav.).



7 pav. Interneto svetainių pažeidžiamumo kitimo tendencija pagal įsilaužimo sudėtingumą 2015 – 2017 m.

Apibendrinant reikia pasakyti, kad 2017 m. stebėtų viešojo sektoriaus interneto svetainių saugumo būklė blogėjo. Šią išvadą patvirtina 2017 m. CERT-LT atlikto tyrimo duomenys, pagal kuriuos apie 70 proc. svetainių TVS yra pasenusios.

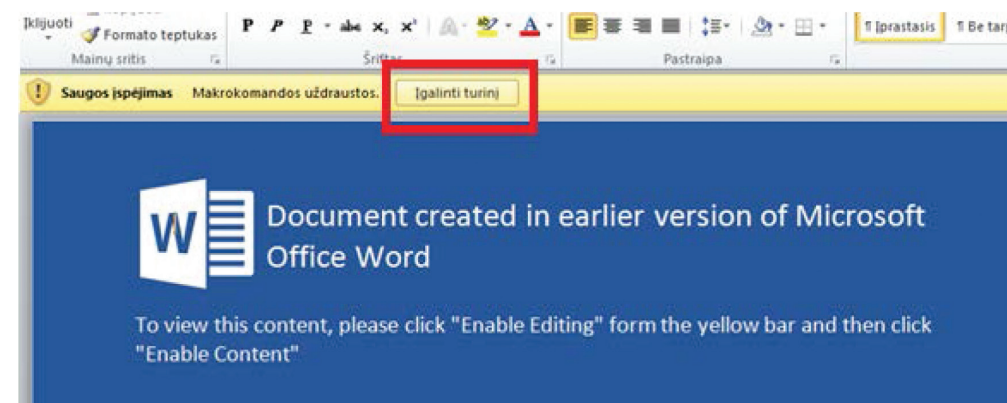
Siekiant apsaugoti viešai prieinamas sistemas arba internetines svetaines nuo užvaldymo, būtina reguliariai atnaujinti tarnybinėse stotyse naudojamą programinę įrangą, apriboti prieigą prie administravimo sąsajos (pvz., prieigos kontrolės sąrašais), naudoti papildomas apsaugos priemones (pvz., tinklo programų užkardą), griežtai kontroliuoti administravimo teises turinčias paskyras, naudoti sudėtingus ir reguliariai keičiamus prieigos slaptažodžius, reguliariai atlikti prisijungimų žurnalo įrašų (angl. Logs) auditą.

# KIBERNETINIAI INCIDENTAI TURINTYS SOCIALINĖS INŽINERIJOS POŽYMIŲ

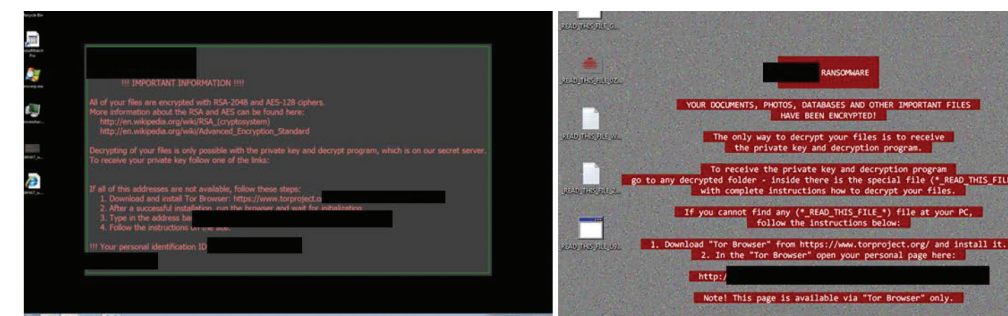
Socialinės inžinerijos metodai naudojami siekiant manipuluoti žmonių emocijomis ir naudojant psichologinį poveikį priversti naudotojus atlikti potencialiai žalingus veiksmus (paspausti nuorodas, atverti svetaines, parsisiųsti bylas, įgalinti veikti žalingą kodą, pateikti asmens ar prisijungimo duomenis). Populiariausi metodai („slaptažodžių žvejyba“ (angl. Phishing), „viliojimas“ (angl. Baiting)) naudojami siekiant gauti informaciją tolimesnėms kibernetinėms atakoms vykdyti, kenkimo programinei įrangai organizacijų tinkluose platinti, pvz., atsidarius į elektroninį paštą atsiųstą dokumentą ir jame įgalinus macro komandas (8 pav.), į darbo stotį atsiunčiamas žalingas kodas, kuris užšifruoja naudotojo saugomus duomenis ir prašo išpirkos (9 pav.). Dažniausiai siunčiami .docx, .xlsx ar .pdf dokumentai. Siekiant išvengti saugumo programų patikrinimo, šie failai neretai archyvuojami, o slaptažodis naudotojui pateikiamas siunčiamo laiško tekste (10 pav.).

2017 m. laiškų, sukurtų naudojantis socialinės inžinerijos principais, skaičius išaugo pusantro karto. NKSC, vienoje iš stebimų institucijų, per metus užfiksavo daugiau kaip 188 500 socialinės inžinerijos požymių turinčių elektroninių laiškų. Plg.: 2016 m. užfiksuota 106 000, 2015 m. – daugiau nei 37 000 gaunamų socialinės inžinerijos pobūdžio el. laiškų.

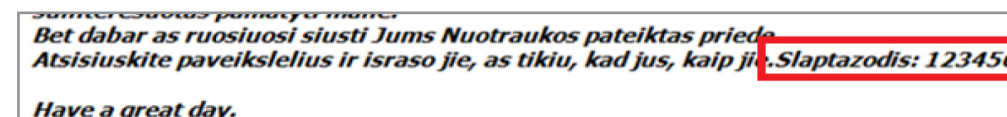
NKSC 2017 m. užfiksavo elektroninių laiškų, sukurtų remiantis socialinės inžinerijos principais, tikslinį platinimą. Norime pabrėžti, kad tikrosios institucijų ir organizacijų interneto svetainės ir informacinės sistemos (žr. žemiau pateiktus pavyzdžius) nebuvo pažeistos, tačiau matomos jų suklastotos versijos, kuriose naudojami organizacijų interneto svetainių dizaino elementai, spalvos, logotipai ir vardai.



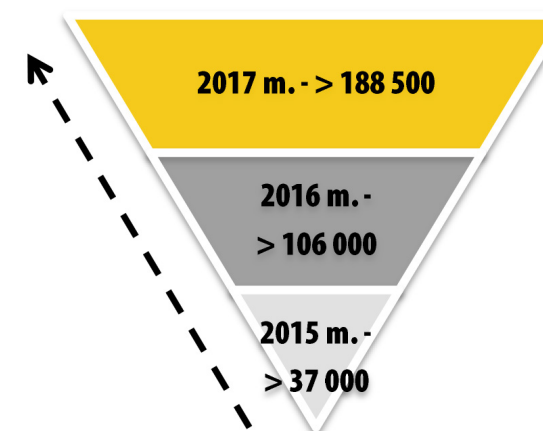
8 pav. Macro komandų įgalinimas gautame dokumente



9 pav. Užšifruotų duomenų pavyzdys



10 pav. Pateiktas slaptažodis laiško tekste

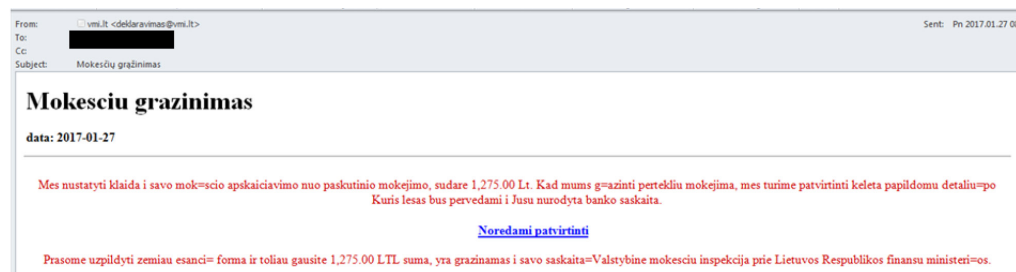


11 pav. Socialinės inžinerijos tendencijos 2015-2017 m.

## Valstybinių institucijų interneto svetainių klastojimas

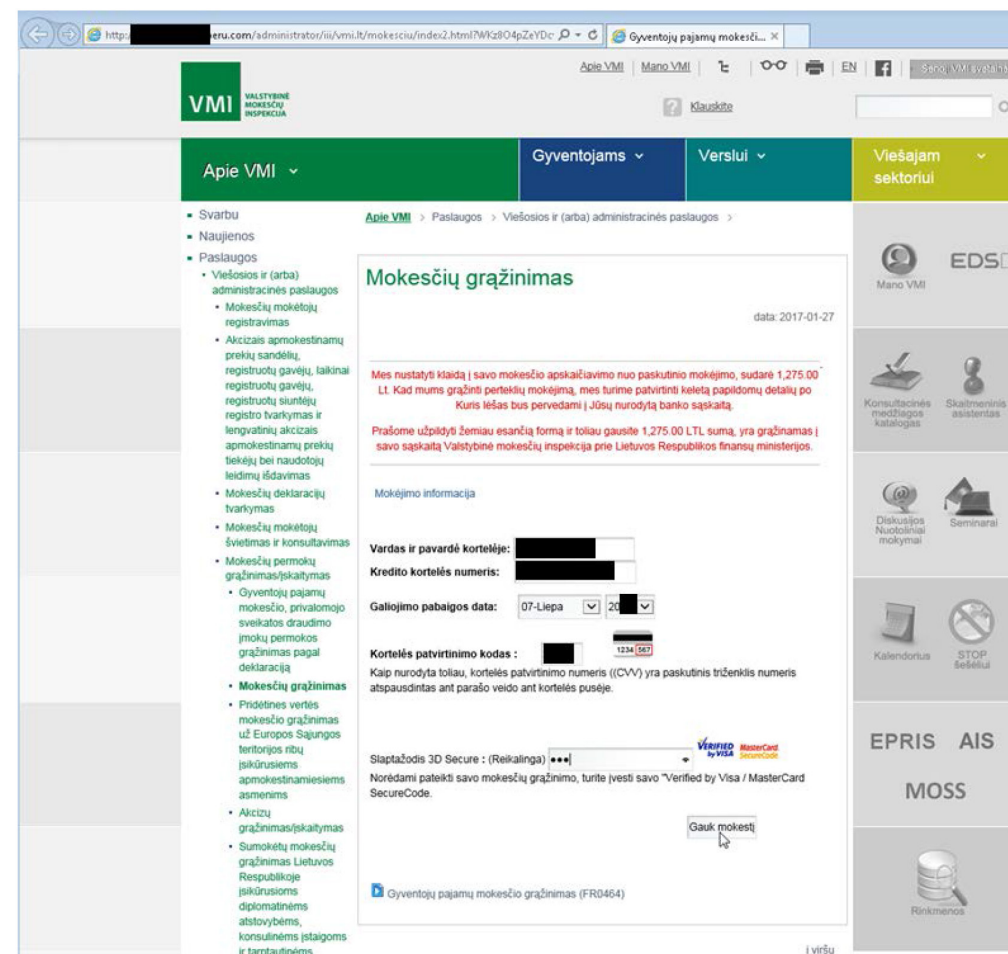
2017 m. NKSC tyrė keletą socialinės inžinerijos metodais pagrįstų ir inicijuotų kibernetinių atakų, kurių metu buvo siunčiami laiškai su nuorodomis į suklastotas Lietuvos valstybinių institucijų internetinės svetainės. Vienas iš pavyzdžių – Valstybinė mokesčių inspekcija (toliau – VMI). Šiuo atveju buvo stengiamasi pasinaudoti VMI vardu ir išvilioti kreditinių banko kortelių duomenis, prisidengiant galimybe susigrąžinti mokesčių permoką.

Platinamame elektroniniame laiške buvo nurodoma, kad VMI skaičiavimuose neva įsivėlė klaida, o gavėjas yra raginamas pateikti savo kreditinės kortelės duomenis permokai susigrąžinti. Grąžintina pinigų suma pateikta litais, taip pat laiško tekste esančios akivaizdžios gramatinės klaidos leidžia spėti, kad turinys buvo išverstas automatizuota kalbos vertimo programa (12 pav.).



12 pav. Suklastotas Valstybinės mokesčių inspekcijos el. laiškas

Laiške buvo pateikta nuoroda į suklastotą interneto tinklalapį, išoriškai panašų į tikrąjį VMI tinklalapį (13 pav.).

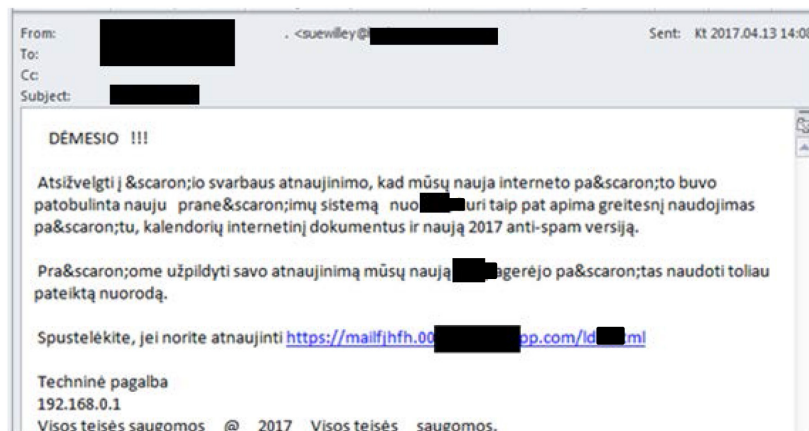


13 pav. Valstybinės mokesčių inspekcijos suklastota interneto svetainė

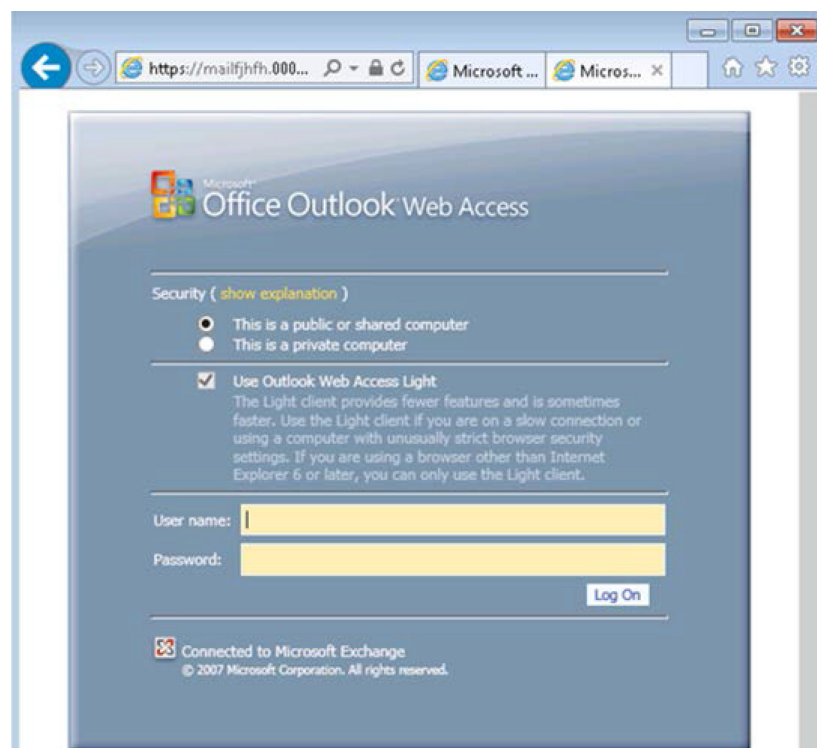
Naudotojui pateikus kreditinės kortelės duomenis, jie atitenka atakos rengėjams.

## Valstybinės institucijos darbuotojų slaptažodžių grobimas

NKSC tyrė incidentus, kurių metu valstybės institucijų darbuotojams buvo siunčiami laiškai, imituojantys kompiuterio tinklo administratorių pranešimus, informuojančius apie pašto sistemų atnaujinimus (14 pav.). Pateiktos nuorodos vedė į svetainę, imituojančią institucijos elektroninio pašto paslaugos tinklapį (15 pav.). Naudotojų pateikti slaptažodžiai perimami atakos iniciatorių.



14 pav. Suklastotas administratoriaus el. laiškas



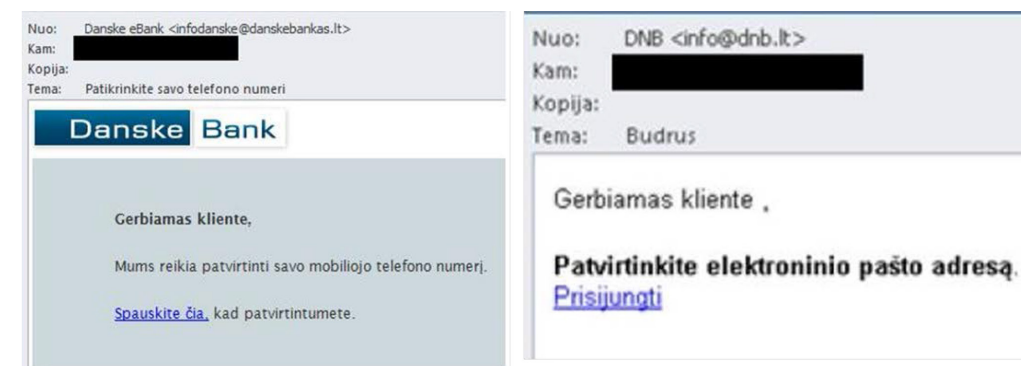
15 pav. Suklastotas elektroninio pašto paslaugos tinklapis

## Bankų paslaugų klastojimas

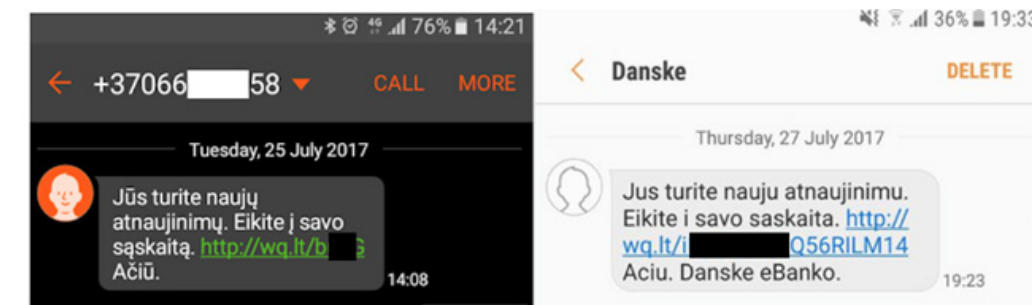
NKSC 2017 m. tyrė socialinės inžinerijos metodais pagrįstas kibernetines atakas, buvo siunčiami el. laiškai su nuorodomis į suklastotas interneto svetaines, imituojančias Lietuvoje veikiančių bankų tinklalapius (16 pav.).

Nusikaltėliai mėgina naudotojus pasiekti ne tik el. laiškais, bet ir trumpomis (SMS) žinutėmis (17 pav.), kuriose pateikiamas suklastotas banko informacinis pranešimas ir nuoroda į suklastotą banko svetainę.

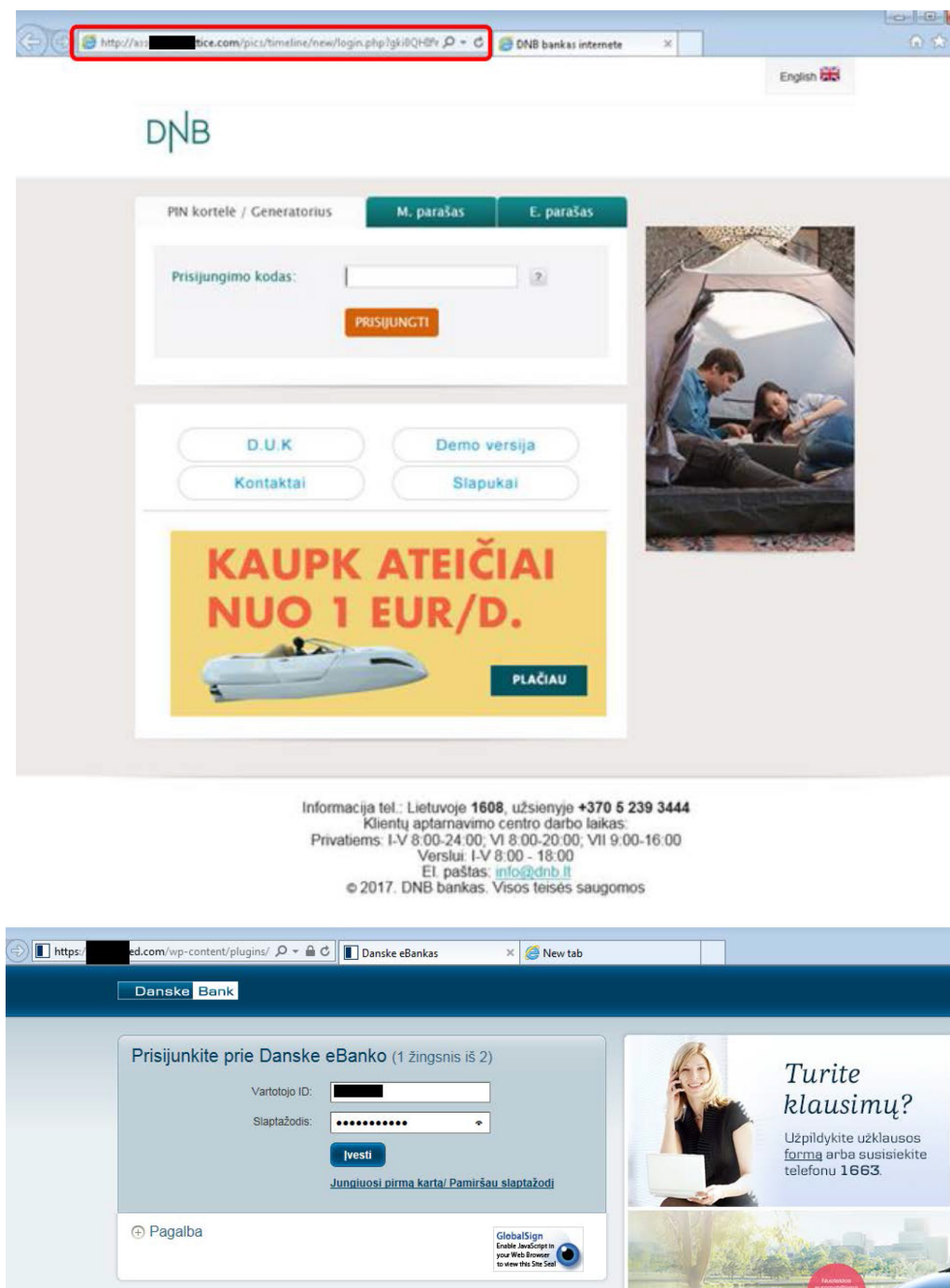
Naudotojui paspaudus laiške pateiktas nuorodas, atidaromos svetainės, kuriose naudojami gerai žinomų organizacijų interneto svetainių dizaino elementai, logotipai ir spalvos. Lankytoją stengiamasi įtikinti, kad tai yra tikras tinklapis, išvilioti elektroninės bankininkystės prisijungimo duomenis (18 pav.). Jeigu lankytojas pateikia savo prisijungimo duomenis (atsidariusi papildoma lentelė klausia antrojo autentifikavimo faktoriaus duomenų), jie perduodami į atakos rengėjo tarnybinių stotį nešifruotu komunikacijos protokolu (http). Pagrobti naudotojų prisijungimo duomenys gali būti panaudoti piniginiams lėšoms pasisavinti.



16 pav. Socialinės inžinerijos pavyzdys – suklastotas banko el. laiškas



17 pav. Suklastotos trumposios žinutės

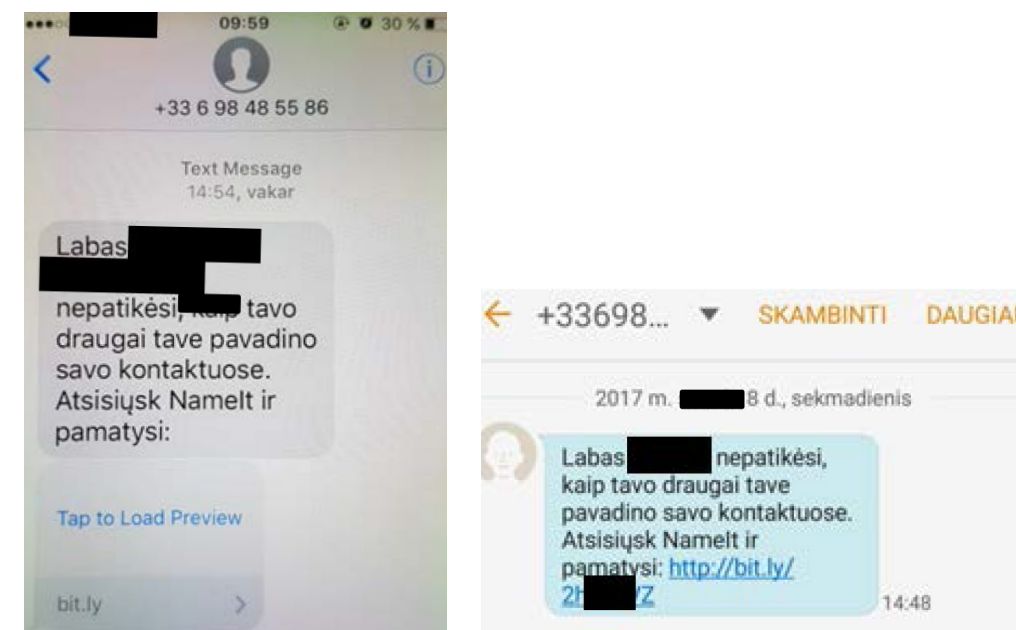


18 pav. Suklastoti internetinės bankininkystės puslapiai

Atkreiptinas dėmesys, kad, siekiant gauti prisijungimo prie el. bankininkystės duomenis, nuorodos į suklastotas svetaines gali būti siunčiamos ne tik el. laiškais, bet ir trumpaisiomis tekstinėmis žinutėmis.

## Kibernetinės atakos prieš išmaniųjų telefonų naudotojus

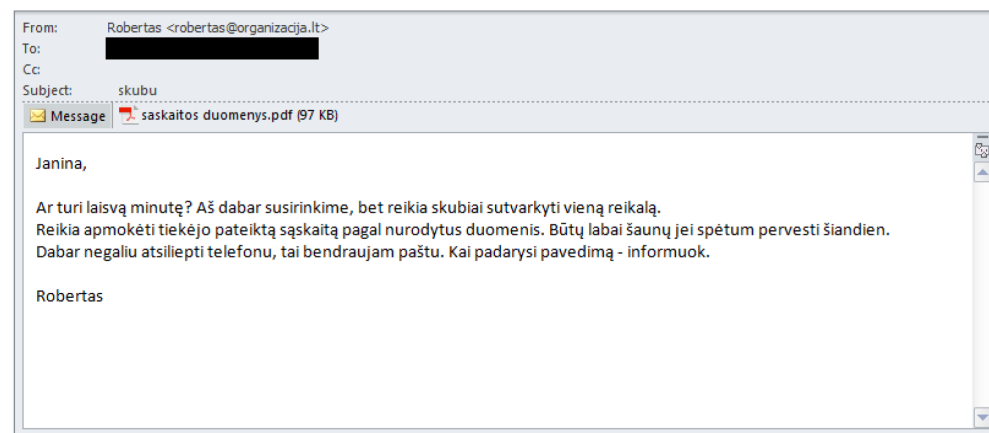
Socialinės inžinerijos metodais pagrįstų kibernetinių atakų spektras neapsiriboja tik el. laiškų siuntimu. Nuorodos į užkrėstus tinklalapius arba pavojingą programinę įrangą gali būti siunčiamos ir trumpaisiomis tekstinėmis žinutėmis (19 pav.). Tokiu būdu gali būti siekiama užkrėsti išmaniuosius telefonus, kuriuose apdorojama daug svarbios asmeninės informacijos (asmens duomenys, slaptažodžiai, geografinės vietos nustatymas, finansinių operacijų informacija, be įrenginio savininko sutikimo padaryti garso ir vaizdo įrašai).



19 pav. Trumpaisiomis teksto žinutėmis platinamos žalingos nuorodos

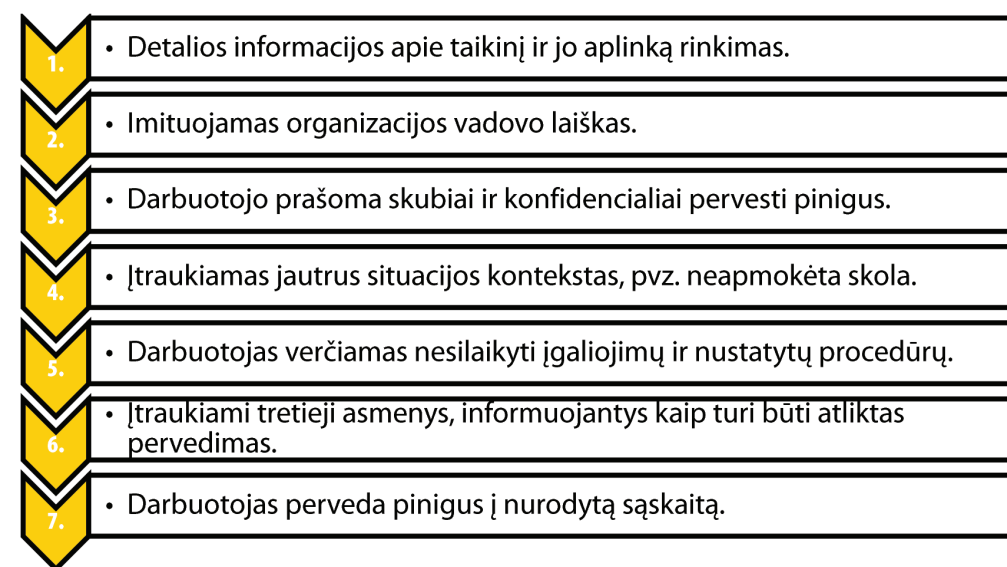
## Sukčiavimas imituojant vadovo laišką

2017 m. NKSC sulaukė daug nusiskundimų iš organizacijų atstovų dėl gaunamų imituojamų vadovų elektroninių laiškų, kuriuose stengiamasi įtikinti už finansines operacijas atsakingą personalą atlikti pinigines perlaidas į atakos iniciatorių sąskaitas (20 pav.). Tokio pobūdžio kibernetinės atakos nėra techniškai sudėtingos, tačiau prieš jas organizuojant yra renkama detali informacija apie taikinį ir jo aplinką rinkimas (organizacijos veiklą, atsakingą personalą, darbotvarkę ir pan.).



20 pav. Socialinės inžinerijos pavyzdys – suklustotas el. pašto adresas

Atakos iniciatoriams svarbu, kad pinigų pervedimas būtų kuo skubesnis ir konfidencialus, nes kitu atveju kiltų grėsmė, kad apie operaciją sužinos kiti organizacijos darbuotojai ir kils įtarimų. Pinigų išviliojimo operacijos metu atakos iniciatoriams svarbu sukurti stresinę situaciją ir priversti darbuotojus veikti neracionaliai, todėl pinigų išviliojimo metu stengiamasi pasinaudoti vadovo autoritetu ir tariamais sunkumais su juo susisiekti. Kartais stengiamasi priversti darbuotoją nesilaikyti nustatytų procedūrų ar įgaliojimų. Paveikus ir įtikinus darbuotoją, dažnu atveju įtraukiami tretieji asmenys, nurodantys, kaip turi būti atlikta pinigų pervedimo operacija, po kurios darbuotojas atlieka pervedimą į vieną ar kelias nekontroliuojamas ir sunkiai susekamas atakos organizatorių sąskaitas.

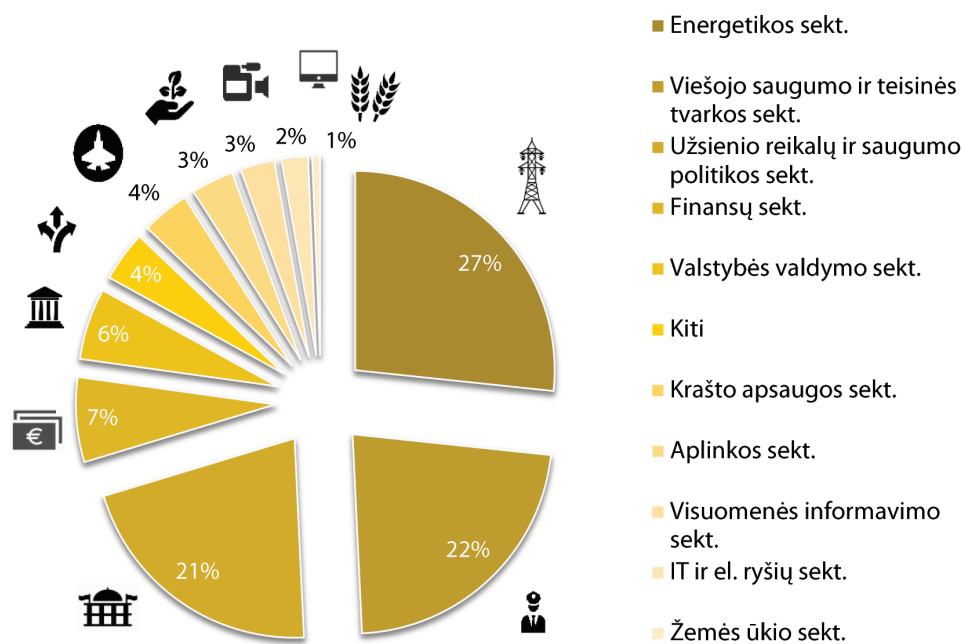


21 pav. Pinigų išviliojimo schema

Svarbu pabrėžti, kad įmonių vadovai dažnai nesilaiko elementarios kibernetinio saugumo higienos, kuri yra privaloma paprastiems organizacijos darbuotojams, todėl svarbu kibernetinio saugumo priemonės taikyti visoje organizacijoje. Darbuotojai, kuriuos gali būti stengiamasi apgauti, taip pat turėtų būti informuoti apie tokio pobūdžio sukčiavimą. Atidumą itin padidintų reguliarūs darbuotojų mokymai ir atsparumo grėsmėms patikrinimai, kuriuos atliktų pati įmonė ar specialiai tam pasamdyti specialistai.

## ŽALINGOS PROGRAMINĖS ĮRANGOS PAPLITIMAS

NKSC 2017 m. stebėjo augančią žalingos programinės įrangos (angl. malware) plitimo tendenciją. 2017 m. NKSC daugiau negu 450 kartų aptiko ir neutralizavo žalingos programinės įrangos veikimą (22 pav.). Buvo tiriama keletas incidentų, kurių metu buvo identifikuota itin pažangi šnipinėjimo programinė įranga, siejama su užsienio valstybių žvalgybos tarnybomis. Tokios programinės įrangos veikimas buvo aptiktas ir užkardytas keliose Lietuvos valstybės įstaigose.



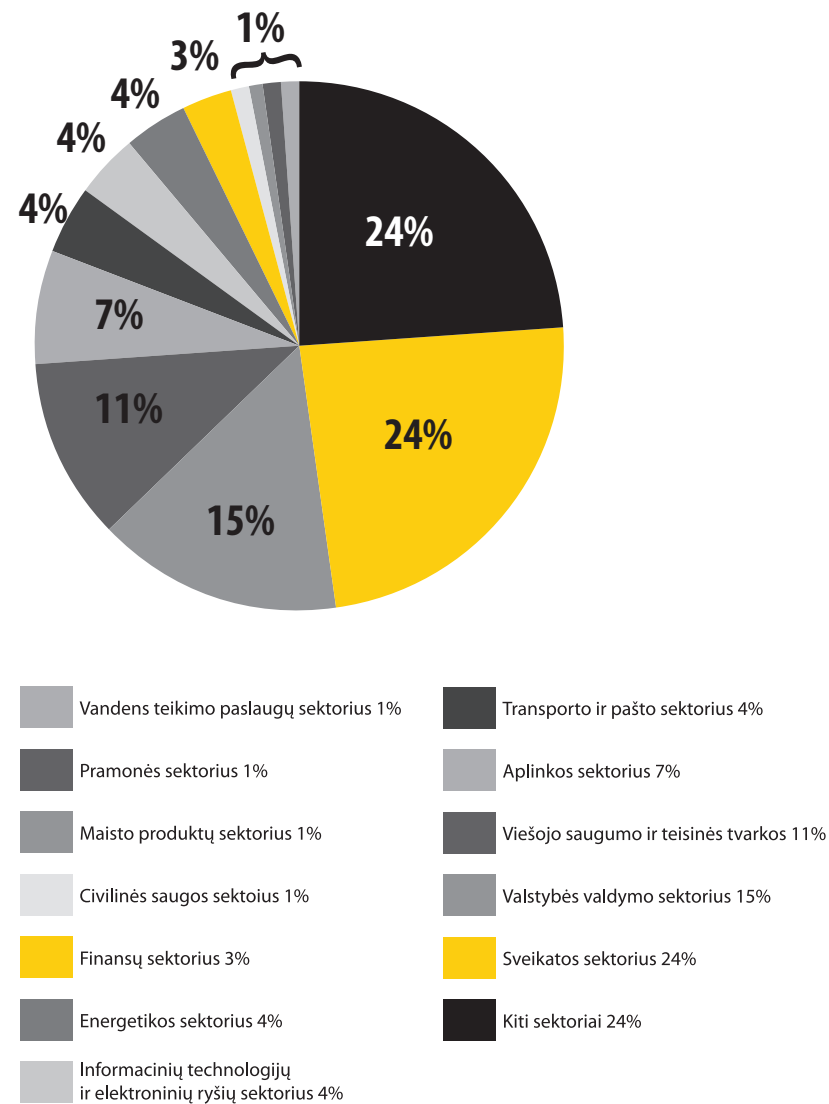
22 pav. NKSC aptiktos žalingos programinės įrangos kiekis pagal sektorius 2017 m.

NKSC, naudodamasis įdiegtomis techninėmis stebėsenos priemonėmis, 2017 m. daugiausia žalingos programinės įrangos veikimo atvejų užfiksavo energetikos (daugiau nei 26 proc.), viešojo saugumo ir teisinės tvarkos (daugiau nei 22 proc. visų atvejų) ir užsienio reikalų ir saugumo politikos sektoriuje (daugiau nei 21 proc. visų užfiksuotų atvejų). Žalingos programinės įrangos paplitimas, palyginti su 2016 m., išaugo viešojo saugumo ir teisinės tvarkos, užsienio reikalų ir saugumo politikos sektoriuose, energetikos sektoriuje taip pat išliko aukštas.

## ORGANIZACINIŲ IR TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ ĮGYVENDINIMAS

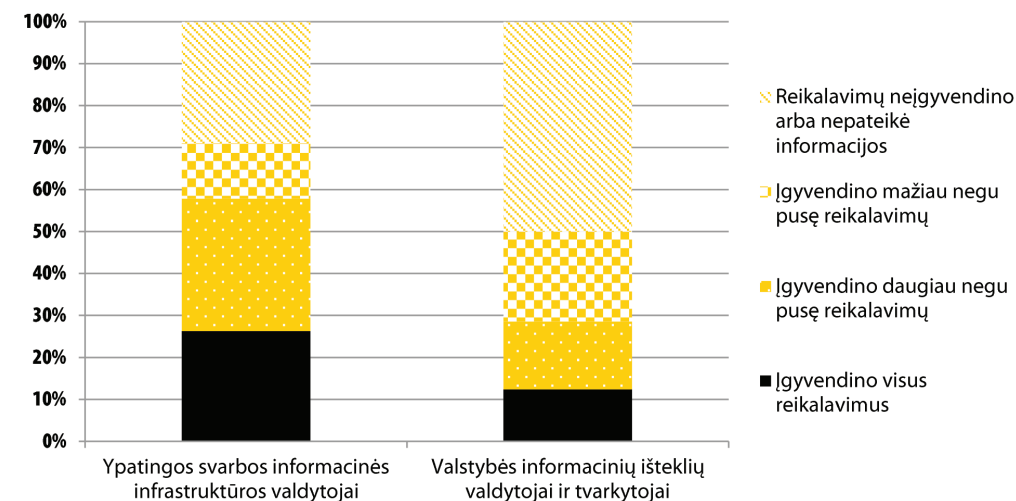
Lietuvos Respublikos Vyriausybė 2016 m. balandžio 20 d. nutarimu Nr. 387 (toliau – Nutarimas) apibrėžė organizacinius ir techninius kibernetinio saugumo reikalavimus, kuriuos turi atitikti YSII valdytojai ir VII valdytojai ir tvarkytojai, užtikrindami valdomos informacinės infrastruktūros ir informacinių išteklių kibernetinio saugumo būklę ir atsparumą kibernetinėms atakoms. Vyriausybės nustatyti reikalavimai de facto įpareigojo organizacijose nusistatyti kibernetinio saugumo politiką, vykdyti rizikos vertinimus, įsilaužimų prevenciją, ugdyti reikalingus gebėjimus, nustatė būtinybę apibrėžti kibernetinių incidentų valdymą ir būti įdiegus konkrečias technines priemones. Svarbu pabrėžti, kad VII valdytojai ir tvarkytojai organizacinius reikalavimus turėjo įgyvendinti per 4 mėnesius nuo Nutarimo įsigaliojimo dienos, t. y. iki 2016 m. rugpjūčio mėnesio, o techninius reikalavimus – per 12 mėnesių, t. y. iki 2017 m. balandžio mėnesio. YSII valdytojai organizacinius kibernetinio saugumo reikalavimus turėjo įgyvendinti per 4 mėnesius nuo Lietuvos Respublikos Vyriausybės patvirtinto sąrašo, t. y. iki 2017 m. liepos, o techninius reikalavimus – per 12 mėnesių, t. y. iki 2018 m. kovo mėnesio.

2018 m. pradžioje NKSC, siekdamas detalai įvertinti VII valdytojų ir tvarkytojų ir YSII valdytojų atitiktį organizaciniams ir techniniams kibernetinio saugumo reikalavimams, vykdė apklausą, kurią sudarė daugiau negu 200 klausimų su prašymais organizacijoms pagrįsti deklaruojamą reikalavimų įgyvendinimą. Didžioji dalis apklausoje dalyvavusių subjektų atstovavo sveikatos ir valstybės valdymo sektoriams (23 pav.), didžioji dalis respondentų nurodė, kad yra susipažinę su Nutarimo reikalavimais, 5 proc. respondentų nurodė kad nėra susipažinę, tuo tarpu, prieš metus NKSC atliktos apklausos duomenys rodo, kad 2016 m. nesusipažinusių su teisės aktu buvo trečdalis respondentų.



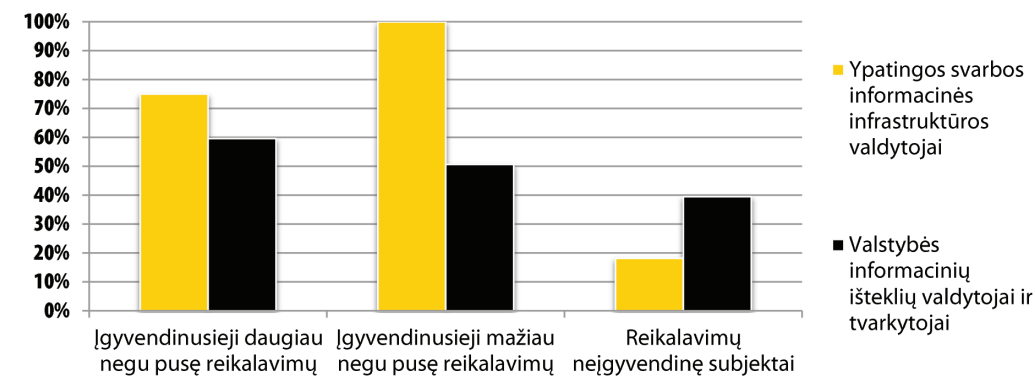
23 pav. Apklausoje dalyvavusių organizacijų pasiskirstymas pagal sektorius

VII valdytojų ir tvarkytojų organizacinių reikalavimų įgyvendinimo apimtis 2017 m. didėjo – visus reikalavimus yra įgyvendinę 13 proc. subjektų, 16 proc. subjektų daugiau nei pusę, 21 proc. mažiau negu pusę, o 50 proc. reikalavimų neįgyvendino arba NKSC nepateikė informacijos. Tuo tarpu, 26 proc. YSII valdytojų nurodė, jog įgyvendino visus nustatytus organizacinius reikalavimus. 32 proc. subjektų įgyvendino daugiau negu pusę reikalavimų, 13 proc. mažiau negu pusę, o 29 proc. reikalavimų neįgyvendino arba nepateikė informacijos (24 pav.).



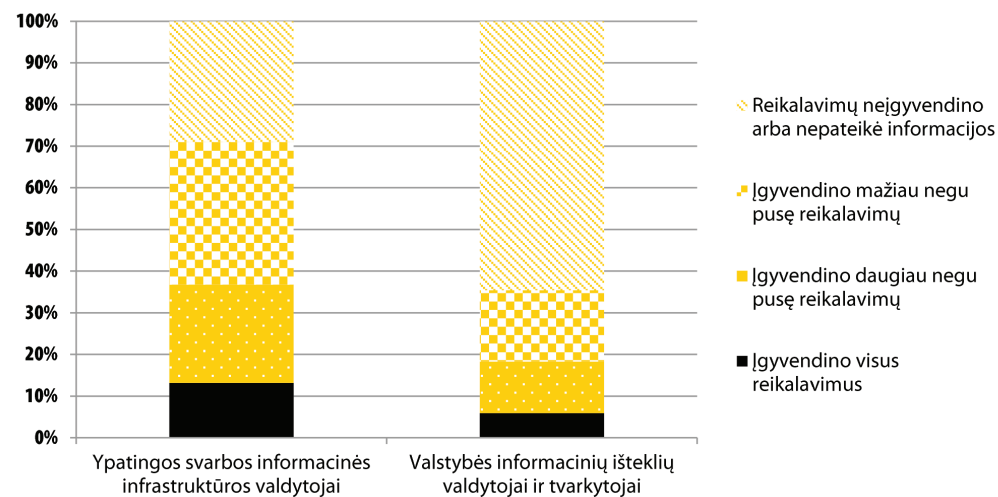
24 pav. YSII ir VII valdytojų ir tvarkytojų organizacinių reikalavimų įgyvendinimas

60 proc. VII valdytojų ir tvarkytojų, kurie įgyvendino daugiau negu pusę reikalavimų, 51 proc. subjektų, įgyvendinusių mažiau negu pusę reikalavimų, ir 40 proc. reikalavimų neįgyvendinusių subjektų nurodė, jog yra suplanavę likusius reikalavimus įgyvendinti ateityje. 75 proc. YSII valdytojų, kurie įgyvendino daugiau negu pusę reikalavimų, 100 proc. subjektų, įgyvendinusių mažiau negu pusę reikalavimų, ir 18 proc. reikalavimų neįgyvendinusių subjektų nurodė, kad yra suplanavę kitus reikalavimus įgyvendinti ateityje (25 pav.). Galima daryti išvadą, kad didžioji dalis subjektų, kurie nėra įgyvendinę reikalavimų, didžiąja dalimi neplanuoja jų įgyvendinti ir ateityje.



25 pav. YSII ir VII valdytojai ir tvarkytojai, kurie teigia, kad yra suplanavę organizacinius reikalavimus įgyvendinti ateityje

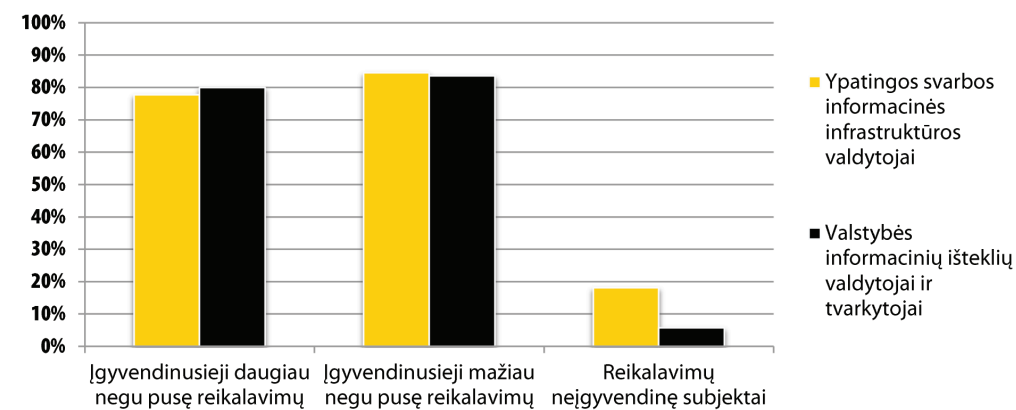
Techninius reikalavimus organizacijos turėjo įdiegti per metus nuo Nutarimo arba YSII sąrašo patvirtinimo dienos, todėl pasibaigus Vyriausybės nustatytiems terminams NKSC vykdė apklausą siekdamas nustatyti, kiek organizacijų atitinka nustatytus reikalavimus arba kaip juos planuoja įgyvendinti ateityje (26 pav.).



26 pav. YSII valdytojų ir VII valdytojų ir tvarkytojų techninių reikalavimų įgyvendinimas

6 proc. VII valdytojų ir tvarkytojų nurodė, kad įgyvendino visus nustatytus techninius reikalavimus. 12 proc. subjektų įgyvendino daugiau negu pusę reikalavimų, 17 proc. mažiau negu pusę, o 65 proc. reikalavimų neįgyvendino arba NKSC nepateikė informacijos. Apklausus YSII valdytojus paaiškėjo, kad 13 proc. įgyvendino visus nustatytus techninius reikalavimus. 24 proc. įgyvendino daugiau negu pusę reikalavimų, 34 proc. – mažiau negu pusę, o 29 proc. – reikalavimų neįgyvendino arba nepateikė informacijos.

YSII ir VII valdytojai ir tvarkytojai, kurie iš dalies yra įgyvendinę techninius reikalavimus, nurodė jog yra suplanavę juos įgyvendinti ateityje, tačiau tik 6 proc. reikalavimų neįgyvendinusių VII valdytojų ir tvarkytojų ir 18 proc. YSII valdytojų, nurodė, kad yra suplanavę kitus reikalavimus įgyvendinti ateityje. Todėl iš žemiau pateikto grafiko galima daryti išvadą, kad didžioji dalis subjektų, kurie nėra įgyvendinę reikalavimų, to nesiruošia daryti ir ateityje. (27 pav.).



27 pav. YSII valdytojų ir VII valdytojai, kurie teigia, kad yra suplanavę techninius reikalavimus įgyvendinti ateityje

2017 m. buvo matyti kylantis organizacinių reikalavimų įgyvendinimo lygis. NKSC atliko išsamų organizacinių reikalavimų įgyvendinimo atitikties vertinimą organizacijose, deklaruojančiose, kad yra įgyvendinusios visus Nutarimu nustatytus organizacinius reikalavimus. Subjektai, kurių reikalavimų įgyvendinimo lygį tikrinu NKSC, valdo valstybės informacinius išteklius ir ypatingos svarbos informacinę infrastruktūrą. Vertinant metu buvo siekiama nustatyti kokybinį organizacijų kibernetinio saugumo politiką formuojančių dokumentų, apibrėžiančių reikalavimų įgyvendinimą, koreliavimą su politiką įgyvendinančiais dokumentais ir procedūromis, jų integravimą į vidinius organizacijos procesus. Taip pat buvo siekiama identifikuoti problemas, su kuriomis organizacijos susiduria praktiškai įgyvendindamos organizacinius reikalavimus.

Konstatuotina, kad įstaigos, formaliai įgyvendinusios visus Nutarime nustatytus reikalavimus, nėra jų integravusios į organizacijos politiką įgyvendinančius dokumentus visa apimtimi, nėra apibrėžtas integruotas reikalavimų įgyvendinimas, perkeliant tiesioginę atsakomybę darbuotojams. Nepaisant to, kad reikalavimai yra vykdomi, procesai ne visada yra valdomi ir vertinami, įgyvendinami iš dalies intuityviai.

Kibernetinių incidentų valdymas organizacijose yra apibrėžtas ir vykdomas, yra paskirti atsakingi asmenys, tačiau de facto Nutarime ir Tipiniame incidentų valdymo plane nustatyta būtinybė informuoti atsakingas organizacijas apie konkrečius požymius turinčius kibernetinius incidentus neintegruota ir formalizuota organizacijos, taip pat ir darbuotojų lygmens, procedūriniuose dokumentuose.

Organizacijos nurodo, jog Nutarimu nustatytus reikalavimus joms yra sudėtinga įgyvendinti dėl kompetencijos, žmogiškųjų ir finansinių išteklių stokos (28 pav.). Subjektai dar nesugeba adekvačiai įvertinti kibernetinio saugumo svarbos jų valdomiems informaciniams ištekliams ir kibernetinio saugumo nevertina kaip prioritetinės srities.



28 pav. Pagrindinių problemų, kylančių įgyvendinant organizacinius ir techninius kibernetinio saugumo reikalavimus, tarpusavio sąveika

NKSC, atlikdamas apklausą dėl organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimo būklės, nustatė, jog dauguma organizacijų yra susipažinusios su joms taikomais reikalavimais, o reikalavimų įgyvendinimo tendencija gerėja. NKSC, atlikęs organizacijų, kurios deklaruoja, kad yra įgyvendinusios visus organizacinius reikalavimus, atitikties vertinimą pastebėjo, kad reikalavimai mutatis mutandis yra įgyvendinti formaliai, o visų be išimties organizacinių reikalavimų įgyvendinimas praktiškai neužtikrinamas. Svarbu pabrėžti, kad dauguma organizacijų, kurios nebuvo ir nėra įgyvendinusios reikalavimų, neplanuoja jų įgyvendinti ir ateityje.

## REZONANSINIAI KIBERNETINIAI INCIDENTAI

2017 m. įvyko keletas kibernetinių išpuolių, kurie sukėlė didelį susidomėjimą nacionaliniu ir tarptautiniu lygiu.

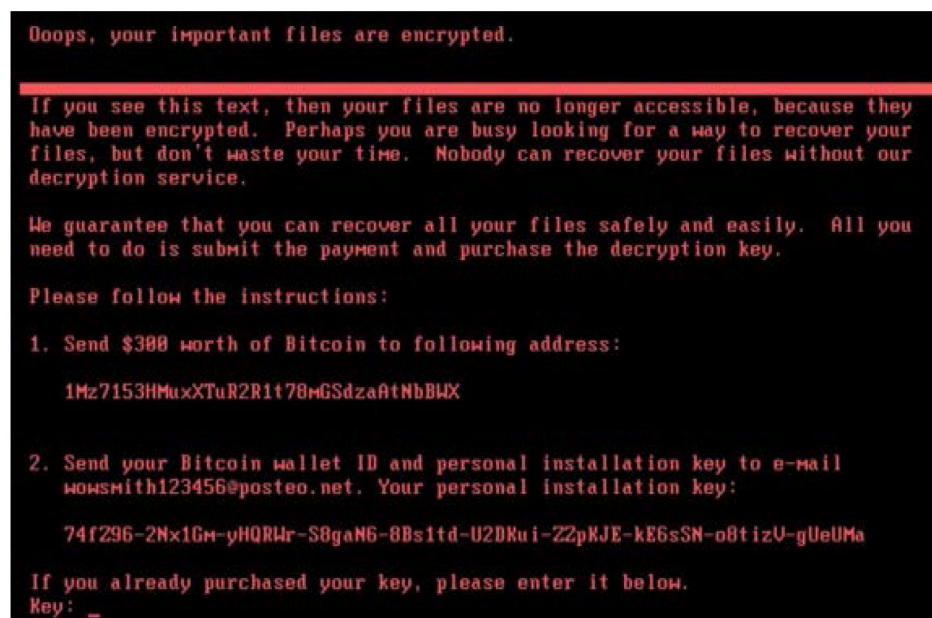
Užfiksuoti prieš žiniasklaidą vykdyti kibernetiniai išpuoliai, kurių metu buvo skelbiama klaidinanti ir paniką kelianti informacija, susijusi su NATO karių misija. Balandžio mėnesį įsilaužta į BNS sistemą – paskelbta melaginga žinia apie JAV karių Latvijoje. Tai buvo padaryta neteisėtai pasinaudojus [www.bns.lt](http://www.bns.lt) turinio valdymo sistemos administratoriaus paskyra, o prisijungimams prie jos buvo panaudota „Tor“ anonimizavimo paslauga.

Gegužę vyko tarptautinio masto kibernetinė ataka, kurios metu buvo puolami taikiniai daugiau nei pusantro šimto šalių taikiniai. „WannaCry“ kompiuterinis virusas, išnaudojantis operacinės sistemos „Windows“ saugumo spragą, plito kompiuterių tinkluose ir šifravo kompiuteriuose saugomus naudotojų duomenis, o už prieigos atkūrimą prašė išpirkos kriptovaliuta (angl. ransomware). Europos Sąjungos šalyse nukentėjo švietimo, sveikatos, susisiekimo sektorių organizacijos ir kitos svarbios informacinės infrastruktūros. NKSC duomenimis, Lietuvoje tarp viruso užkrėstų IP adresų, valstybinės reikšmės ar ypatingos svarbos informacinės infrastruktūros objektų nebuvo.



29 pav. „WannaCry“ viruso užšifruotų duomenų pavyzdys

Birželio mėnesį plito tą pačią operacinės sistemos spragą išnaudojantis ir išpirkos už duomenų iššifravimą reikalaujantis virusas „NotPetya“.



30 pav. „NotPetya“ viruso užšifruotų duomenų pavyzdys

Virusas daugiausia plito Rytų Europos kompiuterinėse sistemose. CERT-LT duomenimis, Lietuvoje buvo užfiksuoti 5 informacinių sistemų pažeidimo atvejai, sutrikdę įmonių veiklą ir padarę nuostolių<sup>4</sup>. NKSC neužfiksavo duomenų apie viruso paveiktus VII ar YSII valdytojus.

NKSC atkreipia dėmesį, kad organizacijų tinkluose naudojamų tarnybinių ir darbo stočių operacinės sistemos turi būti laiku atnaujinamos (vos tik gamintojas išleidžia saugumo spragų pataisas). Jeigu naudojamos sistemos nėra palaikomos gamintojo, jų prieiga prie interneto turi būti apribota, o saugumas sustiprintas papildomomis priemonėmis.

Saugantis nuo tokio tipo atakų, rekomenduojama reguliariai daryti svarbių apdorojamų duomenų atsargines kopijas, kurios būtų saugomos atskirai, nepasiekiamos iš darbuotojų aplinkos.

NKSC atkreipia dėmesį, kad išpirkos sumokėjimas neužtikrina duomenų atgavimo, todėl nerekomenduotina atlikti prašomų pinigų pervedimų.

Užšifruotų duomenų kopija gali būti išsaugoma tikintis, kad ateityje iššifravimo raktai bus prieinami viešai<sup>5</sup>.

<sup>4</sup> Lietuvos Respublikos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio 2017 m. veiklos ataskaita. <https://www.cert.lt/doc/2017.pdf>

<sup>5</sup> <https://www.nomoreransom.org/>

## PRATYBOS

Didėjant kibernetinių išpuolių skaičiui, ypač svarbu operatyviai reaguoti į kylančias grėsmes, jas atpažinti ir užkardyti. Kibernetinio saugumo pratybos – viena iš geriausių praktinių priemonių, padedančių išmokyti organizacijų darbuotojus ir saugumo personalą.

2017 m. Lietuvoje vyko NKSC organizuotos antrosios nacionalinės kibernetinio saugumo pratybos „Kibernetinis skydas 2017“. Kibernetinius incidentus atremti ir suvaldyti treniravosi daugiau nei 200 IT padalinių vadovų ir kibernetinio saugumo specialistų iš daugiau nei 50 valstybinių institucijų, informacinių išteklių valdytojų, mokslo įstaigų, energetikos, ryšio operatorių ir įmonių. Pratybų tikslai: plėtoti VII ir YSII valdytojų ir kibernetinius incidentus tiriančių institucijų bendradarbiavimą, ugdyti VII ir YSII valdytojų saugumo personalo incidentų stabdymo gebėjimus, išbandyti Nacionalinio kibernetinių incidentų valdymo plano procedūras, lavinti jų taikymo įgūdžius. Procedūrų mokymų dalyje institucijų ir įmonių vadovai treniravosi valdyti kibernetinius incidentus, aptikti sistemų pažeidžiamumus bei juos pašalinti pagal Lietuvoje sukurtą teisinę kibernetinio saugumo bazę. Techninėje mokymų dalyje specialistai treniravosi suvaldyti kibernetines atakas specialiai pratyboms sukurtoje virtualioje informacinėje infrastruktūroje. Treniruojamos komandos veikė iš mokymų vietų Vilniuje, Kaune ir kituose Lietuvos miestuose. Pratybų metu išbandyta NKSC sukurta kibernetinių incidentų valdymo platforma<sup>6</sup>, skirta VII ir YSII valdytojams.

Lietuva 2017 m. kartu su Latvija, Estija ir JAV dalyvavo tarptautinėse pratybose „Baltic Ghost 2017“. Šių pratybų tikslas – stiprinti bendradarbiavimą tarp trijų Baltijos šalių ir JAV pavojingų kibernetinių incidentų atvejais (ypatingos svarbos infrastruktūros gynyba regione, civilinių ir karinių kibernetikos srities organizacijų, kurios kibernetinės krizės atveju remtų viena kitą, identifikavimas, efektyviausi keitimosi informacija būdai ir priemonės), kuriems suvaldyti būtinos bendros aukšto lygio procedūros.

Lietuvos atstovai dalyvavo NATO organizuotose pratybose „Cyber Coalition

<sup>6</sup> Kibernetinio saugumo informacinis tinklas – tai saugi informacijos mainų platforma, kurios paskirtis yra dalytis informacija apie galimus ir įvykusius kibernetinius incidentus, taip pat rekomendacijomis, nurodymais, techniniais sprendimais ir kitomis priemonėmis, užtikrinančiomis kibernetinį saugumą ir bendradarbiavimą tarp KSIT narių kibernetinio saugumo srityje.

2017“, kurių tikslas – patikrinti NATO valstybių reagavimo ir informacijos keitimosi efektyvumą kibernetinių grėsmių atveju.

2017 m. II ketvirtį Lietuva dalyvavo kasmetinėse tarptautinėse kibernetinio saugumo pratybose „Locked Shields 2017“, kurias organizavo NATO kibernetinės gynybos kompetencijos centras. Pratybose komandos tapo taikiniais, prižiūrinčiais karinių oro pajėgų tinklus, patyrusius atakas elektros energijos skirstymo, vadovavimo ir valdymo sistemose, ypatingos svarbos informacinėse infrastruktūrose. „Locked Shields 2017“ buvo didžiausios pasaulyje tarptautinės kibernetinio saugumo pratybos pagal scenarijų, panaudotas technologijas ir jose dalyvavusių šalių skaičių. Dalyviams buvo parengta per 2500 įvairaus pobūdžio atakų, taip pat panaudota daugiau nei 3000 virtualių sistemų. Pratybos vyko simuliuojamoje kibernetinėje erdvėje realiu laiku, jose dalyvavo daugiau nei 800 specialistų iš 25 šalių<sup>7</sup>.

<sup>7</sup> <https://ccdcoe.org/locked-shields-2017.html>

## IŠVADOS, REKOMENDACIJOS IR PROGNOZĖS

### Išvados

Kibernetinio saugumo būklė 2017 m., palyginti su 2016 m., Lietuvoje nežymiai gerėjo. Tačiau atsižvelgiant į sparčią kibernetinių grėsmių augimo dinamiką, dedamos pastangos užtikrinti kibernetinį saugumą yra nepakankamos. Pagrindinės priežastys, leidžiančios daryti tokią išvadą, yra:

1. Gerėjantis organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimas valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėje infrastruktūroje rodo padidėjusį organizacijų dėmesį kibernetiniam saugumui. Tačiau, NKSC duomenimis, reikalavimai yra įgyvendinami ad hoc, ne visa apimtimi ir formaliai, o didėjantis fiksuojamų incidentų kiekis ir atlikti tyrimai rodo, kad organizacijos laiku netaiko būtinų priemonių, kad užkardytų žinomus pažeidžiamumus ir grėsmes.
2. Didėjantis susidomėjimas ir intensyvėjanti elektroninių ryšių tinklų žvalgyba, įskaitant ir technologiniuose tinkluose veikiančios įrangos paieškas, taip pat aptinkamos žalingos programinės įrangos kiekio didėjimas, rodo nepakankamą organizacijų sugebėjimą apsisaugoti nuo grėsmių ir užtikrinti adekvačią gynybą ir organizacijų atsparumą.
3. Visų kibernetinių incidentų tyrimų padalinių Lietuvoje tirtų incidentų skaičius siekė 54 950, bendrai tiek viešajame tie privačiame sektoriuose ir tai yra dešimtadaliu daugiau incidentų negu buvo fiksuota 2016-ais. Tokio masto incidentų statistika signalizuoja didelį kibernetinio saugumo iššūkį tenkantį Lietuvos elektrinei erdvei, piliečiams, viešajam sektoriui ir verslui.
4. Sėkmingų socialinės inžinerijos principais paremtų kibernetinių atakų kiekio didėjimas rodo, kad naudotojų ir organizacijų darbuotojų patiklumas, žinių ir dėmesio trūkumas tebėra viena pagrindinių kibernetinio saugumo spragų.
5. Stiprinami NKSC pajėgumai, techninėmis kibernetinio saugumo priemonėmis išplėstas stebėjimo laukas, leido užfiksuoti daugiau kitomis priemonėmis

mis neaptinkamos žalingos programinės įrangos. Tačiau organizacijos ir toliau vangiai praneša apie jų tinkluose pastebėtus kibernetinius incidentus, nėra linkusios keisti informacija, grėsmių indikatoriais.

6. Nuolat kintanti Lietuvos viešojo sektoriaus interneto svetainių kibernetinio saugumo būklė rodo, kad laiku neatnaujinama programinė įranga, organizacijos pačios negeba užtikrinti jų interneto svetainių kibernetinio saugumo, o įsigydamos svetainės prieglobos ir administravimo paslaugas, į pirkimo sutartis neįtraukia prievolės paslaugos tiekėjams užtikrinti kibernetinio saugumo reikalavimų.

## Rekomendacijos

- Siekdami užtikrinti didesnę organizacijų brandą sprendžiant su kibernetiniu saugumu susijusius klausimus ir užtikrinant kibernetinių grėsmių užkardymą, rekomenduojame nedelsiant imtis įgyvendinti Vyriausybės nustatytus organizacinius ir techninius kibernetinio saugumo reikalavimus. Kad reikalavimai būtų ne tik formaliai įgyvendinti, bet ir būtų gauta praktinės naudos, rekomenduojame planuoti kibernetiniam saugumui skirtus materialiuosius ir žmogiškuosius išteklius.
- Sklandžiam kibernetinių incidentų valdymui užtikrinti NKSC rekomenduoja pagal Vyriausybės patvirtintus organizacinius ir techninius kibernetinio saugumo reikalavimus pasitvirtinti procedūras, apibrėžiančias kibernetinių incidentų valdymą, informacijos rinkimą ir kompetentingų institucijų informavimą.
- Kuriant organizacijos kompiuterinių tinklų kibernetinio saugumo pagrindus, NKSC rekomenduoja taikyti technines ir organizacines priemones griežtai įrenginių ir programinės įrangos, kuriems leidžiama būti vidiniame organizacijos tinkle, kontrolei (taikyti įrenginių identifikavimą, neleistinos programinės įrangos ribojimą). Organizacijos naudojamų įrenginių ir programinės įrangos kruopštus konfigūravimas ir saugumo nustatymų standartizavimas yra vienas iš tinklo saugumą kuriančių pagrindų. Atsižvelgiant į NKSC stebimų incidentų techninius požymius, svarbu pabrėžti, kad nuolatinė organizacijos naudojamos programinės įrangos priežiūra ir saugumo atnaujinimų diegimas yra ypač svarbus procesas, saugantis nuo vis atsirandančių naujų kibernetinių grėsmių. Esant nuotolinės komunikacijos tarp organizacijos tinklo elementų poreikiui, svarbu užtikrinti, kad komunikacija viešojoje terpėje būtų papildomai apsaugota šifravimo technologijomis. Stengiantis išlaikyti norimą tinklo saugumo lygį, svarbu griežtai kontroliuoti administratoriaus privilegijų suteikimą ir naudojimą, taikyti technines priemones kompiuterių naudotojų potencialiai pavojingiems veiksams riboti. Atsižvelgiant į didėjantį išpirkos reikalaujančių virusų skaičių, siūlome taikyti patikimas ir patikrintas priemones itin svarbių duomenų atsarginėms kopijoms daryti ir saugoti.
- NKSC pabrėžia, kad, stiprinant organizacijų atsparumą kibernetinėms grėsmėms, yra gyvybiškai svarbu gerinti darbuotojų gebėjimus atpažinti sociali-

nės inžinerijos principais paremtas kibernetines atakas. Tą galima pasiekti, reguliariai rengiant darbuotojų mokymus, atsparumo grėsmėms patikrinimus, imituojant piktavalių veiksmus, prireikus ar pritrūkus kompetencijos pasitelkti išorės ekspertų pagalbą.

- Atkreipiamė dėmesį, kad, siekiant gerinti naudotojų supratimą ir gebėjimą atpažinti kibernetines grėsmes, turėtų būti informuojama apie tai, kad gaunamų laiškų siuntėjo adresas gali būti imituotas (todėl nereiktų juo akiai pasitikėti); atkreipti dėmesį į gramatines klaidas ir sakinių rišlumą (į lietuvių kalbą tekstas išverstas automatinėmis priemonėmis); neskubėti atsidaryti prie laiško prisegtų priedų ir pateiktų nuorodų – susimąstyti ar siuntėjas yra žinomas, ar laiško buvo laukiama; nuorodų adreso patikimumą naudotojai gali patikrinti pelytės žymeklį užvedę ir palaikę virš atsiųstos nuorodos, tačiau jos nespausdami – automatiškai parodomas informacinis pranešimas (31 pav.); atkreipti dėmesį į tariamą laiško antraštės sensacingumą, gavėjo veiksmų skubinimą ar viliojimą materialine nauda, slaptažodžių pateikimą laiško tekste; naudotojai turėtų tvirtai žinoti, kad niekas neturi teisės klausti jų slaptažodžių, todėl kiekvienas prašymas (prisidengiant administratoriaus ar teisėtvarcos vardu) turėtų sukelti įtarimų. Norint apsaugoti asmeninius duomenis ir saugomą informaciją, kompiuteriuose turėtų būti naudojama tik legali komercinė arba atvirojo kodo programinė įranga (nelegalioje įrangoje dažnai įterpiamas kenksmingas kodas), korektiškai veikiančios apsaugos priemonės (daugelis saugumo priemonių gamintojų namų naudotojams leidžia naudotis nemokamomis jų programų versijomis).



31 pav. Pateikta nuoroda į žalingą tinklapį.

- Organizacijos, siekdamos apsaugoti savo viešai prieinamas sistemas ar interneto svetaines nuo įsibrovimo ir neteisėto turinio keitimo, privalo reguliariai atnaujinti tarnybinėse stotyse naudojamą programinę įrangą, apriboti prieigą prie administravimo sąsajos (pvz., prieigos kontrolės sąrašais), nuotolinis svetainės administravimas turi būti atliekamas patikimu komunikacijos ka-

nalų (pvz., šifruotuoju loginiu tinklu, naudojančiu dviejų faktorių autentifikavimą, angl. virtual private network), naudoti papildomas apsaugos priemones (pvz., tinklo programų užkardą, angl. web application firewall), griežtai kontroliuoti administravimo teises turinčias paskyras, naudoti sudėtingus ir reguliariai keičiamus prieigos slaptažodžius, reguliariai atlikti prisijungimų žurnalo įrašų (angl. Logs) auditą, prireikus įsigyti elektroninių paslaugų trikdymo atakų (DDoS) užkardymo paslaugas. Išvardytų apsaugos priemonių įgyvendinimą organizacijos gali numatyti prieglobos paslaugų pirkimo sąlygų sutartyje.

## Prognozės

NKSC, atsižvelgdamas į pasaulio ir Lietuvos kibernetinių grėsmių tendencijas, prognozuoja, kad 2018 m. ir toliau bus ieškoma saugumo spragų Lietuvos valstybės informaciniuose ištekliuose ir ypatingos svarbos informacinėse infrastruktūrose, kartu toliau didės susidomėjimas technologiniuose procesuose dalyvaujančiais ir turinčiais sąsają su internetu įrenginiais.

Prognozuojama, kad socialinės inžinerijos metodai modernės, daugės atvejų, kai bus vykdomos tikslingai nukreiptos kibernetinės atakos. Dėl nepakankamo naudotojų sąmoningumo, ateityje daugės sėkmingų tokio pobūdžio kibernetinių atakų.

Atsižvelgiant į tai, kad naudotojų sąmoningumas kibernetinių grėsmių atžvilgiu yra mažas, visos kibernetiniam saugumui užtikrinti būtinos priemonės laiku neįdiegiamos, o duomenis šifruojančių ir išpirkos reikalaujančių virusų daugėja, numatoma, kad ateityje sėkmingų tokio pobūdžio atakų skaičius didės.

Didėjanti užfiksuotos rafinuotos žalingos programinės įrangos tendencija 2017 m. leidžia daryti prielaidą, kad 2018 m. bus vis dažniau išnaudojami dar nežinomi pažeidžiamumai. Prognozuojama, kad užsienio reikalų ir saugumo politikos, energetikos, viešojo saugumo ir teisinės tvarkos sektoriai tebebus didžiausią susidomėjimą keliantys kibernetinių atakų taikiniai.

Remdamasis pastarųjų metų kibernetinių grėsmių tendencijomis, 2018 m. prognozėmis, NKSC pažymi, kad būtina kurti kibernetinio saugumo kompetencijos viešajame sektoriuje pagrindus, kaupti žinias ir ugdyti gebėjimus, adekvačiai planuoti išteklius, siekiant sumažinti kibernetinio saugumo grėsmių riziką.