LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS
TINKLŲ IR INFORMACIJOS SAUGUMO DEPARTAMENTO
SAUGUMO INCIDENTŲ TYRIMŲ SKYRIUS (CERT-LT)

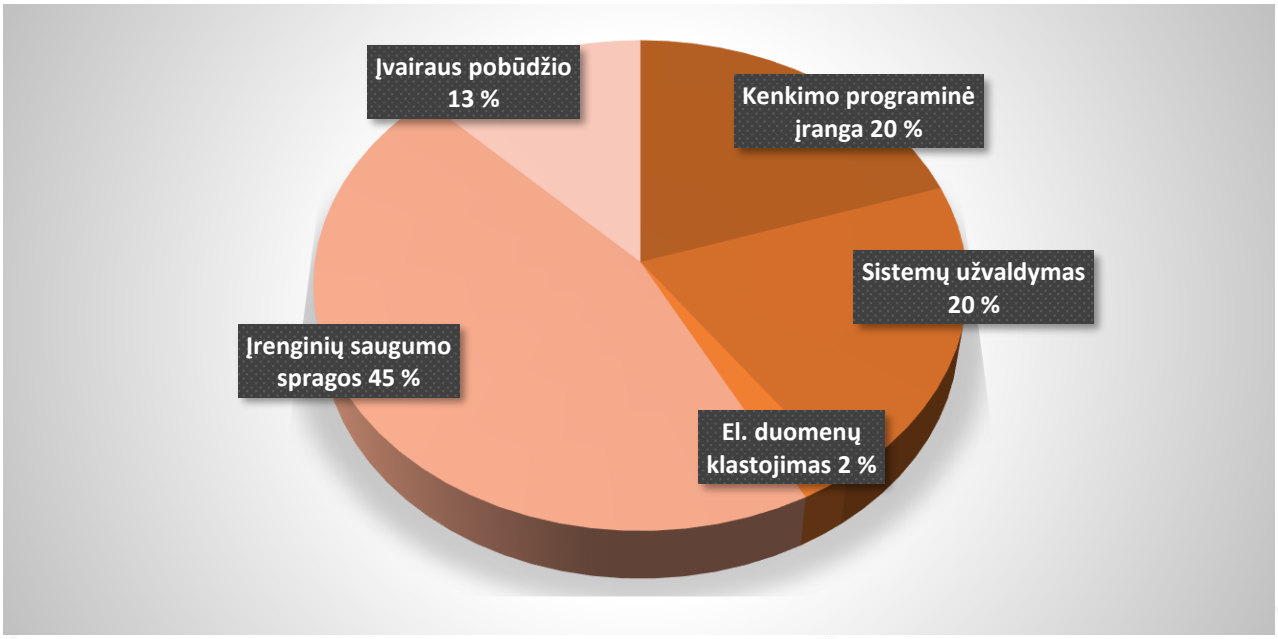
# 2017 METŲ VEIKLOS ATASKAITA

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2017 metų veiklos rezultatus. 2017 metais CERT-LT ištyrė 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. 1-oje lentelėje ir 1-oje diagramoje pateikiamos nagrinėtų pranešimų suvestinės pagal tipus. Tolesniuose skyriuose aptariame kiekvieną incidentų tipą ir ypatingas 2017 m. tendencijas.

1 lentelė. CERT-LT 2017 m. apdoroti pranešimai apie incidentus 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 | 5938 | 6 464 | 6 362 | 24 612 |
| Įvairaus pobūdžio | 2 899 | 1 672 | 943 | 1 196 | 6 710 |

1 diagrama. CERT-LT 2017 m. apdoroti pranešimai apie incidentus pagal tipus, procentinės dalys



# Pagrindinės 2017 m. kibernetinio saugumo problemos

Kaip rodo incidentų statistika, Lietuvoje dvi didžiausios kibernetinio saugumo problemos yra kenkimo programinė įranga (kenkimo kodai) ir nesaugios informacinės sistemos, tarp jų ir interneto svetainės. Minėtos saugumo problemos papildo viena kitą ir didina potencialią riziką interneto naudotojams. Vienais atvejais užvaldomos nesaugios interneto svetainės (turinio valdymo sistemos) ir į jas įkeliamas kenkimo kodas, skirtas kenkėjiškai programinei įrangai platinti. Kitais atvejais į užvaldytą svetainę įkeliama speciali valdymo konsolė (*angl*. shell), kuri leidžia piktavaliui vykdyti įvairesnę kenkėjišką veiklą – be jau minėto kenkėjiškos programinės įrangos platinimo, taip pat galima skenuoti ir atakuoti tinklus bei informacines sistemas, rinkti informaciją, valdyti kitus užvaldytus įrenginius ir pan.

## Kenkimo programinė įranga

Populiarėjant kriptovaliutoms, itin aktyviai veikia išpirkos reikalaujančių virusų (*angl*. ransomware) kūrėjai. Antrus metus iš eilės fiksuojamas augantis interneto naudotojų, nukentėjusių nuo šio tipo kenkimo programinės įrangos, skaičius. Nuo šio viruso nukenčia tiek pavieniai naudotojai, tiek įmonės. Išpirkos reikalaujantys virusai nuo kitų skiriasi savo „agresyvumu“ − užvaldytoje sistemoje nesistengiama užmaskuoti jų veikimo pėdsakų, svarbiausia tokių virusų paskirtis yra užšifruoti sistemos savininkui svarbias bylas (pvz., DOC, DOCX, XLS, XLSX) ar net visą failų sistemą, tikintis, kad savininkas bus pasiryžęs sumokėti išpirką, kad jas atgautų. Šiems tikslams naudojami sudėtingi šifravimo algoritmai, todėl atstatyti paveiktas bylas neturint šifravimo rakto yra neįmanoma. Tam tikrais atvejais (pvz., užšifruota įmonės buhalterijos duomenų bazė ir nėra atsarginės kopijos) nuostoliai gali būti itin dideli. Kai kuriems virusams yra sukurti nemokami bylų iššifravimo įrankiai (pvz., „The No More Ransom Project“ projektas), tačiau virusų dinamika tokia didelė, o šifravimo algoritmai tokie sudėtingi, kad labai retai failus galima iššifruoti, pasitelkiant minėtus įrankius.

2017 m. gegužės 12 d. (penktadienį – kaip ir dauguma didžiųjų atakų) buvo užfiksuotas itin spartus vieno išpirkos reikalaujančio viruso, pavadinto „WannaCry“, plitimas. Tai – viena didžiausių tokio pobūdžio atakų per visą skaitmeninio amžiaus istoriją. Ši kenkimo programa turėjo ir kirmino (*angl*. worm) funkcionalumą, kuris leido jam plisti tinkle, išnaudojant „Windows“ operacinės sistemos SMB protokolo saugumo spragą. Šios spragos pataisa buvo išleista dar pora mėnesių iki pačios atakos, todėl didelis užkrėstų kompiuterinių sistemų skaičius dar kartą parodė, kaip atsainiai vartotojai žiūri į savo

įrenginių saugumą ir nesuvokia rizikos, kuri kyla naudojant neatnaujintą programinę įrangą. Per vieną parą paveiktų kompiuterių kiekis perkopė 230 tūkst. ir palietė daugiau nei 150 šalių visame pasaulyje. Tarp nukentėjusių Europos Sąjungoje buvo akademinės institucijos, ligoninės, telekomunikacijų, transporto įmonės ir kitos svarbios informacinės infrastruktūros. Lietuvoje buvo nustatyta apie 180 IP adresų, paveiktų šio viruso. Apie pasitvirtinusius atvejus (t. y. apie užšifruotas kompiuterines sistemas Lietuvoje) CERT-LT informacijos negavo. Plačiau „WannaCry“ aprašytas CERT-LT interneto svetainėje.

Kitas sparčiai plitęs kenkimo kodas „NotPetya“ buvo sukurtas 2016 m. plitusio išpirkos reikalaujančio viruso „Petya“ pagrindu ir masiškai išplito Europoje 2017 m. birželio pabaigoje. Šis virusas labiausiai paveikė Rytų Europos šalių kompiuterines sistemas. Lietuvoje buvo patvirtinti 5 informacinių sistemų pažeidimo atvejai (kai kur – iki keleto šimtų kompiuterių), dėl ko sutriko įmonių veikla ir patirta nuostolių. Verta paminėti, kad duomenys buvo ne šifruojami, o tiesiog ištrinami, be galimybės juos susigrąžinti. Virusui plisti buvo naudojami keli metodai, vienas iš jų, kaip ir „WannaCry“ viruso atveju, išnaudojant „Samba“ (SMB) protokolo spragas.

*Dažnai viruso aktyvinimo metu iššoka UAC (*angl*. User Account Control) langas. Jeigu naudotojas spaudžia „Ne“ arba „No“, virusui nesuteikiamos papildomos teisės ir jis negali pakenkti.*

*Minėtų virusų plitimas buvo susijęs su programinės įrangos, įskaitant „Samba“, saugumo spragomis. Tai parodo, kaip svarbu nuolat rūpintis turimos programinės įrangos atnaujinimu.*

Dažniausiai kenkimo programinė įranga platinama kartu su brukalu (*angl*. spam). Pasinaudojant socialine inžinerija, bandoma įtikinti naudotojus atsidaryti laiške prisegtą bylą, iš pirmo žvilgsnio nekeliančią jokios grėsmės aukos kompiuteriui. Dažniausiai 2017 m. tai būdavo „Microsoft Office“ ar PDF dokumentai bei ZIP archyvai, kurių viduje slypėdavo kenkimo kodas, sukurtas „Visual Basic“ arba „JavaScript“ programavimo kalba. Atvėrus tokias bylas, minėtas kenkimo programinis kodas aktyvuojamas ir jis

atsiunčia bei paleidžia kitą kenkimo kodą (t. y. veikia kaip kenkimo veikos iniciatorius), dažniausiai išpirkos reikalaujantį virusą.

*CERT-LT primena, kad, gavus įtartiną laišką su priedais, reikia elgtis atsargiai – įsitikinti, kad siuntėjas iš tiesų Jums tokį laišką siuntė, patikrinti priedus turima antivirusine programine įranga arba nemokamu interneto įrankiu www.virustotal.com. Nereikėtų atverti el. laiško priedų, jeigu siuntėjas jums nežinomas.*

## Informacinių sistemų užvaldymas

2017 m. užfiksuotas 10 951 (2016 m. užvaldymų buvo 10 673) informacinių sistemų užvaldymo incidentas. Prie šio tipo incidentų priskiriami užvaldyti įrenginiai, kurie naudojami kenkimo veikai vykdyti, ir pažeistos, užvaldytos interneto svetainės.

*CERT-LT kiekvieną dieną užfiksuoja vidutiniškai po 10 naujų užvaldytų svetainių atvejų.*

Nuo 2017 m. rudens stebime didėjantį užvaldytų svetainių panaudojimą kriptovaliutoms generuoti. Vietoje to, kad lankytojų įrenginius užkrėstų kenkimo kodu, kaip tai buvo daroma anksčiau, dabar svetainių lankytojų kompiuteriai (arba išmanieji įrenginiai) vis dažniau išnaudojami intensyviems skaičiavimams.

Tai nauja kenkimo tendencija, atsiradusi tik šiais metais. Asmeniui užėjus į interneto svetainę (pvz., www.pavyzdys.lt), kurioje yra nuoroda į kriptovaliutos generavimui skirtą programinį kodą, esantį toje pačioje arba kitoje interneto svetainėje (pvz., www.pavyzdys.lt/skriptas.js arba www.kriptogeneravimas.com/skriptas.js), interneto naršyklė pradeda vykdyti intensyvius skaičiavimus. Atvejai, kai interneto svetainėje gali atsirasti kriptovaliutą generuojantis programinis kodas:

- Kibernetiniai nusikaltėliai užvaldo nesaugią svetainę (pvz., naudojančią pasenusią turinio valdymo sistemą) ir įterpia minėtą scenarijų (*angl.* script).
- Programinį kodą svetainėje įterpia svetainės kūrėjas (programuotojas) arba administratorius, ir tą padaro be svetainės savininko žinios.

- Scenarijų svetainėje sąmoningai įterpia pats svetainės savininkas, siekdamas sau finansinės naudos.

*Atvejus, kai interneto svetainės savininkas sąmoningai įdeda kriptovaliutos generavimo scenarijų ir apie tai neinformuoja svetainės lankytojų, RRT vertina kaip neetišką veiką, kadangi procesas vyksta be lankytojo, kurio kompiuteriniai resursai yra išnaudojami, žinios.*

Interneto svetainėse, kuriose naudojama neatnaujinta ir dėl to pažeidžiama turinio valdymo sistema (TVS), svetainės įskiepiai (*angl*. plugins) ir (ar) papildiniai (*angl*. extensions), vis dažniau pastebimi svetainės užvaldymo požymiai – piktavalių parašai, tokie kaip „Hacked by ...“ ir pan. Tokie užrašai dažniausiai slepiami ir jokios kenkimo veiklos nevykdo, tačiau tai yra požymis, kad svetainė yra pažeista ir joje gali būti įkeltas kenkimo kodas.

2017 m. IV ketv. CERT-LT atlikto tyrimo duomenimis, apie 70 proc. svetainių turinio valdymo sistemų (TVS) yra pasenusios (skaičiuotos .LT adresų srities svetainės ir tik tos TVS, kurių versijas pavyko nustatyti).

*Siekdami sumažinti užvaldymo grėsmę, svetainių savininkai turi rūpintis jų saugumu: apsaugoti svetainės valdymo skydą (*angl*. admin panel), naudoti sudėtingą prisijungimo slaptažodį ir reguliariai jį keisti, diegti turinio valdymo sistemos ir jos papildinių naujinius. Papildinių be ypatingo poreikio naudoti nereikėtų apskritai. Svetainių kūrėjai, kurie diegia populiarias turinio valdymo sistemas („Wordpress“, „Joomla“ ir pan.), taip pat turi rūpintis tinkamu jų konfigūravimu. Plačiau apie tai – mūsų rekomendacijoje.*

## Botnetai

Užvaldytų kompiuterių tinklai (botnetai) – jau minėtų pagrindinių saugumo problemų (nesaugios informacinės sistemos ir kenkimo programinė įranga) rezultatas. Jais vykdomos kibernetinės atakos: žalingų programų ir brukalo platinimas, paslaugos trikdymo atakos ir pan. Ši problema itin aktuali, kadangi nuolat daugėja „IoT“ (*angl*.

Internet of Things) įrenginių – bet kokių prietaisų, prijungtų prie interneto: namų elektronikos, jutiklių, vaizdo kamerų ir kt. Tokie įrenginiai dažnai kelia saugumo problemų (pvz., naudojami nepakeisti gamykliniai slaptažodžiai, neatnaujinama programinė įranga, turinti saugumo spragų, ir pan.) ir gali suformuoti didžiulius botnetus. Pagal „Gartner“ duomenis, 2017 m. pasaulyje „IoT“ įrenginių buvo daugiau nei visų planetos gyventojų – apie 8–8,4 mlrd. vienetų.

Apie įtraukimą į botnetą įrenginio savininkas ilgą laiką gali nieko nežinoti. CERT-LT duomenimis, 2017 metais Lietuvoje kiekvieną mėnesį buvo fiksuojama apie 3 000–3 200 kompiuterių, kurie, savininkams nežinant, buvo valdomi nuotoliniu būdu. Informacija apie botnetuose aptiktų kompiuterių aktyvumą skelbiama mūsų interneto svetainėje.

2017 metais Lietuvoje veikė du „IoT“ botnetai: „Mirai“ ir „Reaper“ („Reaper IoT“, „IoTroop“). „Reaper“ naudojo dalį „Mirai“ programinio kodo, o kita dalis buvo unikali. CERT-LT duomenimis, IV ketv. Lietuvoje buvo 447 „Mirai“ ir „Reaper“ valdomi i□renginiai (unikalūs IP adresai). I, II ir III ketv. atitinkamai buvo 626, 464 ir 369 užvaldyti įrenginiai.

*Labai svarbu yra pasikeisti gamyklinius slaptažodžius ir nustatymus (*angl*. default configuration) naudojamuose „IoT“ įrenginiuose ir užtikrinti jų programinės įrangos naujinimą.*

## Elektroninių duomenų klastojimas

Populiarių interneto svetainių klastojimo atvejų 2017 m. toliau daugėjo. 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. Dažniausiai pasitaikantys klastočių kūrimo būdai:

- Užvaldoma nesaugi atsitiktinė svetainė, į kurią įterpiamas suklastotas turinys (pvz., www.nesaugi-svetaine.lt/klastote).
- Sukuriama nauja suklastota svetainė su panašiu į tikrosios svetainės domeno vardu (pvz., tikroji svetainė – www.pavadinimas.lt, o klastotė – www.payadinimas.lt).

Didžiąją dalį CERT-LT tirtų interneto svetainių klastočių atvejų sudarė pranešimai apie suklastotą elektroninių mokėjimo sistemų svetainę „Paypal“, taip pat „Facebook“, „Gmail“ ir pan. svetaines, kurioms elektroninės informacijos prieglobos paslaugos teiktos Lietuvoje. Pažymėtina, kad šios klastotės nebuvo orientuotos tiesiogiai į Lietuvos interneto naudotojus.

Kur kas rečiau (apie 20 kartų per metus) pasitaiko Lietuvoje veikiančių bankų internetinės bankininkystės platformų klastočių. Dažniausiai naudojamos 2 užvaldytos svetainės, iš kurių viena turi tik nukreipimą (*angl*. redirect), o kita – klastotą turinį (*angl*. landing page). Abi svetainės beveik visada talpinamos skirtingose užsienio tarnybinėse stotyse, todėl jų pašalinimas dažniausiai užtrunka kiek ilgiau dėl laiko juostos skirtumo.

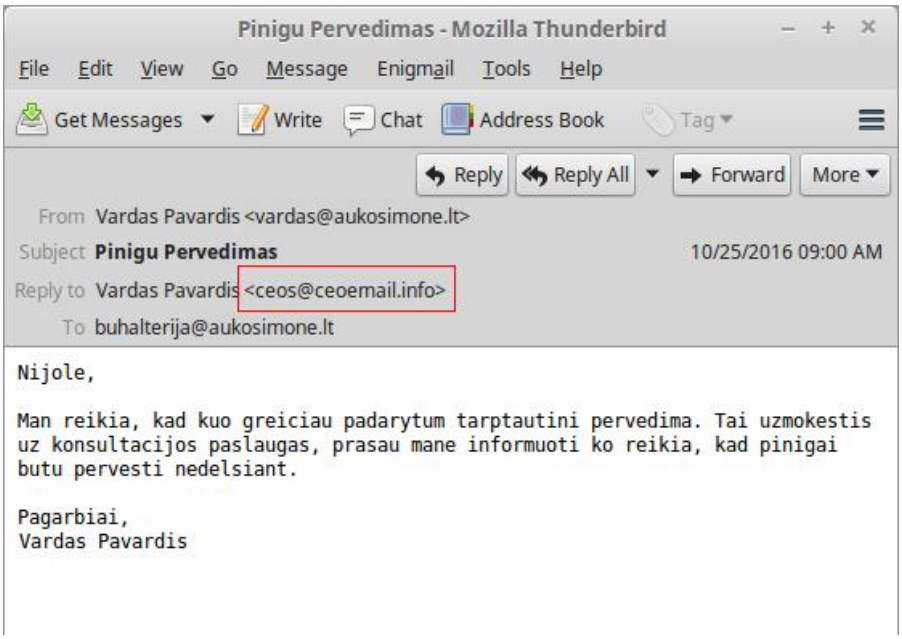
2017 m. piktavaliai platino žinutes, kuriomis siekė išgauti prisijungimo prie el. bankininkystės duomenis ne tik elektroniniais laiškais, bet ir trumposiomis tekstinėmis žinutėmis (SMS). Trumpąsias žinutes siunčiantys asmenys informuodavo apie gautą ar atliktą naują mokėjimą ir apie būtinybę atlikti kokį nors veiksmą paspaudus žinutėje pateiktą interneto nuorodoje.

*Prieš įvesdami savo asmens duomenis tinklalapyje, pirmiausia įsitikinkite, kad jis nėra suklastotas. Būtina atkreipti dėmesį į domeno vardą bei puslapyje esančias nuorodas. E. bankininkystės sistemos visada naudoja saugų TLS ryšio protokolą, adreso pradžioje būtinai yra „https“ (arba žalia juosta) ir galima patikrinti svetainės sertifikatą. Bankai niekuomet neprašo pateikti ar keisti tik Jums žinomų banko internete ar mokėjimo kortelės slaptažodžių el. laiškais ar telefonu. Kilus įtarimui, kad svetainė gali būti suklastota, patariama į naršyklės adresų juostą patiems įvesti tikrosios svetainės adresą.*

## Kibernetinis sukčiavimas

Kibernetinio sukčiavimo mastas ir dėl to atsirandantys nuostoliai 2017 m. nemažėjo. Sukčiai greitai įsisavina naujas technologijas, taip pat sėkmingai išnaudoja senąsias. Nors asmenų, kuriuos pavyksta apgauti elektroninėje erdvėje, skaičius yra santykinai nedidelis, pasekmės gyventojams ir įmonėmis yra skaudžios.

2016 m. prasidėjusi „C-level fraud“, kur „C“ reiškia „CEO“ (įmonės vadovas), sukčiavimo kampanija ir toliau sėkmingai veikė 2017-aisiais. Šis sukčiavimo modelis nukreiptas prieš įmonių buhalterius arba sprendimus priimančius asmenis. Nusikaltėliai apsimeta įmonės vadovais ir ragina buhalterius atlikti skubų tarptautinį pavedimą. Suklastotas laiškas atrodo taip:




1 pav. Socialinės inžinerijos pavyzdys – suklastotas el. pašto adresas

Kitas dažnas sukčiavimo atvejis – pinigų išviliojimas apsimetant įmonės verslo partneriu. Tai yra sudėtingesnio lygio ataka, kuriai nusikaltėliai gerai pasiruošia rinkdami informaciją apie atakuojamą įmonę, jos verslo sandorius ir pan. Negana to, atakos eigoje kartais yra užvaldomos vienos iš sandoryje dalyvaujančių šalių informacinės sistemos, sekamas jų tarpusavio susirašinėjimas, dėl to reikiamu metu pinigų pervedimus galima nukreipti į nusikaltėlių sąskaitas.

*Įmonių vadovams būtina nustatyti konkrečias procedūras, kurių būtų laikomasi atliekant finansines operacijas. Darbuotojai turėtų būti informuoti apie tokio tipo sukčiavimus. Atidumą itin padidintų reguliariai atliekami darbuotojų atsparumo grėsmėms patikrinimai, kuriuos atliktų pati įmonė ar specialiai tam pasamdyti specialistai.*

Dar vienas populiarus sukčiavimo būdas – apsimesti kilnojamojo turto pirkėju. Kibernetinis nusikaltėlis susisiekia su pardavėju el. paštu ir klausia, ar pastarasis sutinka gauti pavedimą už parduodamą turtą (pvz., automobilį) per mokėjimų internetu platformą „PayPal“. Jeigu pardavėjas sutinka, tada tariamas pirkėjas nurodo, kad automobilį paims ne jis, o kurjeris, pirkėjas pridės 500 eurų kurjerio paslaugoms apmokėti ir dar 50 eurų „už papildomus rūpesčius“. Kai sandorio šalys galutinai susitaria ir pirkėjas neva „atlieka pavedimą“, pardavėjas gauna suklastotą el. laišką neva iš „PayPal“, kuriame nurodoma, kad pardavėjo sąskaitą pasiekė lėšos, tačiau jos yra „įšaldytos“ (*angl*. We've placed a temporary hold on the funds of this transaction). Norėdamas disponuoti minėtomis lėšomis, asmuo (t. y. automobilio pardavėjas) turi nuvykti į artimiausią „Western Union“ biurą ir pervesti 500 eurų „už kurjerio paslaugas“. Asmeniui atlikus tokį pavedimą, jo lėšos dažniausiai būna prarastos.

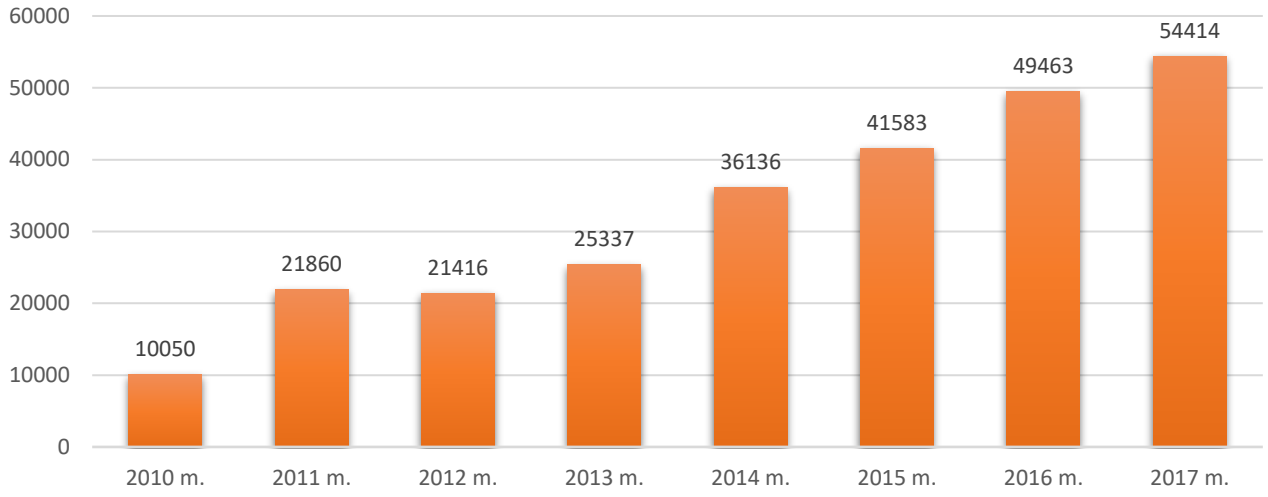
## Kitų tipų incidentai

Nemaža dalis „IoT“ įrenginių (plačiau apie juos – skyrelyje „Botnetai“) turi įvairių saugumo spragų. Paprastai tokios spragos nekelia tiesioginės grėsmės įrenginių savininkų duomenų saugumui, tačiau sudaro sąlygas piktavaliams naudoti įrenginius paskirstytųjų paslaugos trikdymo (*angl*. Distributed Denial of Service, DDoS) atakų metu kaip atakų stiprintuvus. 2017 m. buvo užfiksuota 24 612 įrenginių su saugumo spragomis (2016 m. – 20 490).

2017 metais CERT-LT ištyrė 50 pranešimų apie paslaugos trikdymo (*angl*. Denial of Service, DoS) atakas (2016 m. tokio tipo tyrimų buvo 61). Paprastai šios atakos vykdomos automatizuotomis priemonėms, pasitelkiant botų tinklus arba išnaudojant nesaugius tinklo įrenginius. Siekiant nutraukti vykdomas atakas, CERT-LT teikė rekomendacijas užvaldytų ir nesaugių įrenginių savininkams. Taip pat teiktos rekomendacijos elektroninės informacijos prieglobos (*angl*. hosting) paslaugas teikiančioms įmonėms, kaip stabdyti šias atakas, koordinuoti veiksmai su interneto paslaugų teikėjais ir kitų valstybių CERT tarnybomis.

Per 2017 m. buvo užregistruota 15 ryšių tinklų vientisumo pažeidimų (2016 m. - 21). Įvairaus pobūdžio incidentų buvo 6 710 (įskaitant ir aprašytus skyrelyje „Kibernetinis sukčiavimas“).

Apibendrinimui pateikiama CERT-LT apdorotų kibernetinių incidentų nuo 2010 m. iki 2017 m. suvestinė.




2 diagrama. CERT-LT 2010–2017 m. apdorotų incidentų suvestinė

## Kibernetinio saugumo įstatymo pakeitimas

2017 m. gruodžio 19 d. Lietuvos Respublikos Seimas priėmė Kibernetinio saugumo įstatymo pataisas, kuriomis konsoliduota informacinių išteklių saugumo sritis ir Ryšių reguliavimo tarnybos atliekamos nacionalinio elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinio funkcijos nuo 2018 m. sausio 1 d. perduotos naujai įsteigtam Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos. Atitinkamai buvo pakeistas ir Elektroninių ryšių įstatymas.

Iki minėtų pakeitimų įsigaliojimo informacinių išteklių saugumą užtikrino Nacionalinio kibernetinio saugumo centro funkcijas vykdanti Kibernetinio saugumo ir telekomunikacijų tarnyba prie Krašto apsaugos ministerijos ir Ryšių reguliavimo tarnyba: Nacionalinis kibernetinio saugumo centras rūpinosi valstybės informacinių išteklių ir ypatingos svarbos informacinių infrastruktūrų saugumu, o Ryšių reguliavimo tarnyba – viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų saugumu.

Priimtų įstatymų pataisų pagrindu įgyvendinti pokyčiai padės užtikrinti bendrą ir koordinuotą informacinių išteklių saugumo politikos įgyvendinimą, aiškų ir nuoseklų informacinių išteklių saugumo reglamentavimą.

## Visuomenės informavimas

CERT-LT svarbią ir aktualią informaciją skelbia savo svetainėje www.cert.lt. Joje galite:

- skaityti naujienas, susijusias su IT saugumu;
- peržiūrėti kaupiamą statistiką (tiek grafikus, tiek ataskaitas);
- sužinoti pagrindinius CERT-LT veiklos uždavinius;
- susipažinti su teisės aktais, reglamentuojančiais kibernetinį saugumą;
- pasitikrinti savo kompiuterinę įrangą dėl saugumo spragų ir neleistinos veiklos;
- rasti saugumo rekomendacijas, kenkimo programų aprašymus ir jų pašalinimo instrukcijas;
- pranešti apie vykdomą nusikalstamą kibernetinę veiklą;
- kreiptis pagalbos, įvykus kibernetiniam incidentui.

Naudotojams, susidūrusiems su tinklų ir informacijos saugumo problemomis, patariama nedelsiant kreiptis į savo interneto paslaugų teikėją, o jei šis problemų išspręsti negali, informuoti apie tai CERT-LT užpildant formą tinklalapyje www.cert.lt/pranesti. Daugiau informacijos interneto naudotojams apie saugumą internete prieinama svetainėje www.esaugumas.lt.

Įspėjimus apie kibernetinius incidentus bei trumpas kibernetinio saugumo naujienas CERT-LT skelbia ir socialiniame tinkle „Twitter“ adresu https://twitter.com/cert_lt.