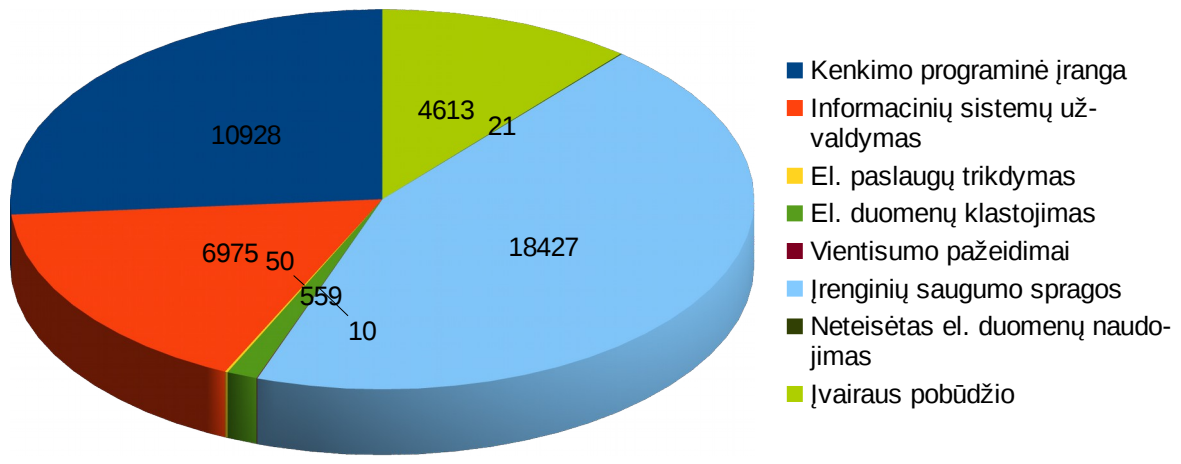
2015 METŲ CERT-LT VEIKLOS ATASKAITA

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2015 metų veiklos rezultatus. 2015 metais CERT-LT ištyrė 41 583 incidentus pagal pranešimus, gautus iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų. Palyginti su 2014 metais (36 136 pranešimai), kibernetinių incidentų užregistruota 15 proc. daugiau. 1-oje lentelėje ir 1-oje diagramoje pateikiamos nagrinėtų pranešimų pagal tipus suvestinės.

1 lentelė. CERT-LT 2015 m. nagrinėti pranešimai pagal jų tipus

Pranešimų pobūdis	**2015 metų laikotarpis**				
	I ketv.	**II ketv.**	**III ketv.**	**IV ketv.**	**iš viso**
Apie kenkimo programinę įrangą	3 051	2 579	2 612	2 686	10 928
Apie informacinių sistemų užvaldymą	1 494	1 278	1 686	2 517	6 975
Apie el. paslaugos trikdymo atakas	18	14	11	7	50
Apie el. duomenų klastojimą	257	83	103	116	559
Apie vientisumo pažeidimus	1	2	2	5	10
Apie įrenginių saugumo spragas	4 856	4 698	4 490	4 383	18 427
Apie neteisėtą el. duomenų naudojimą	5	8	8	0	21
Įvairaus pobūdžio	2025	865	796	927	4 613



1 diagrama. CERT-LT 2015 m. nagrinėtų pranešimų tipai

Pagrindinės kibernetinio saugumo problemos

Didelė Lietuvos kibernetinio saugumo problema (18 427 pranešimai per 2015 m.) buvo ir yra įrenginiai, kurie paprastai priklauso fiziniams asmenims ir turi saugumo spragų. Reikėtų pažymėti, kad dažniausiai 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.

2015 m. užfiksuota daug incidentų, susijusių su kenkimo programine įranga. CERT-LT ištyrė 10 928 kenkimo programinės įrangos panaudojimo atvejus (2014 m. – 11 276). Vienas iš virusų kūrimo ir platinimo tikslų – naudotojų kompiuterių įtraukimas į botnetus. Apie įtraukimą į botų tinklą kompiuterio savininkas ilgą laiką gali nieko nežinoti (kompiuteris veikia įprastai, kartais gali sulėtėti interneto ryšys). Kitas paplitęs tikslas – išgauti pinigus platinant šifruojančius ir išpirkos reikalaujančius virusus (angl. *ransomware*). Antivirusinės programos turi euristinius analizatorius, kurie aptinka žalingą kodą pažeistame kompiuteryje, net jei jo nėra antivirusinės programos duomenų bazėje, analizuodami kodo veikimą. Tačiau pažymėtina, kad naują pavojingą kodą antivirusinės programos paprastai aptinka tik po tam tikro laiko.

2015-iais internete plito apgaulingas brukalas (angl. *spam*), kuriame buvo siūloma atverti PDF failą, kuris neva yra sąskaita. Dažniausiai po nuoroda slėpėsi ZIP failas su viruso EXE failu. CERT-LT primena, kad gavus bet kokį laišką, su priedais reikia elgtis atsargiai (pvz., juos galima prieš atveriant patikrinti www.virustotal.com). Nereikėtų atverti el. laiško priedų, jei siuntėjas jums nežinomas.

Su kenkimo programine įranga betarpiškai susiję užvaldytų kompiuterių (botų) tinklai, kuriais vykdomos kibernetinės atakos: kenkimo kodo ir brukalo platinimas, paslaugos trikdymo atakos ir pan. CERT-LT duomenimis, 2015 metais Lietuvoje kasdien buvo fiksuojama vidutiniškai 2 500 kompiuterių, kurie, savininkams nežinant, buvo valdomi nuotoliniu būdu. Tinklalapyje https://www.cert.lt/botnet registruojama ir skelbiama informacija apie botnetuose aptiktų kompiuterių aktyvumą.

Naudotojai, norėdami sumažinti kompiuterio užkrėtimo virusu tikimybę, turi laikytis elementarios naudojimosi kompiuteriu ir internetu „higienos“, nes tai ženkliai sumažina saugumo riziką. Pavyzdžiui: nespausti ant įtartinų nuorodų, neatverti failų, gautų el. paštu, per „Skype“ ir pan. Būtina turėti antivirusinę programą, daryti atsargines kopijas ir naudoti sudėtingus prisijungimo slaptažodžius.

Grėsmės, susijusios su interneto svetainėmis

Visus 2015 m. aktyviai veikė kenkimo kodas „Stealrat“. Tokie kenkimo kodai ieško nesaugių interneto svetainių ir saugumo spragų, esančių turinio valdymo sistemose, ir bando jas išnaudoti. Vėliau kuriami botnetai ir iš užvaldytų tarnybinių stočių siunčiamas brukalas, kuriuo stengiamasi įtraukti kitus kompiuterius į botnetą, taip pat platinamas kenkimo kodas iš šių svetainių. Išaiškintais atvejais CERT-LT teikė šio kodo šalinimo rekomendacijas svetainių savininkams ar elektroninės informacijos prieglobos paslaugas teikiančioms įmonėms.

Be „Stealrat“, buvo kitų kenkimo kodų, užvaldančių nesaugias interneto svetaines (pvz., „Angler“). Iš viso 2015 m. informacinių sistemų užvaldymo incidentų buvo 6 975 (2014 m. užvaldymų buvo 4 853). Atliktų tyrimų duomenys parodė, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, pasitelkiant botų tinklus, įterpiant kenkimo kodą į prastai apsaugotas interneto svetaines, dažniausiai išnaudojant pasenusių turinio valdymo sistemų saugumo spragas.

2015 m. CERT-LT ištyrė 559 pranešimus apie svetainių klastojimą (angl. *phishing*) (2014 m. – 630 pranešimų). Piktavaliai kuria interneto svetainių klastotes siekdami arba išgauti internetinių paskyrų duomenis, arba iš to pasipelnyti. Dažniausiai gaunama pranešimų apie suklastotus elektroninių mokėjimo sistemų svetaines: daugiausia – „Paypal“, taip pat „Facebook“, „Gmail“,

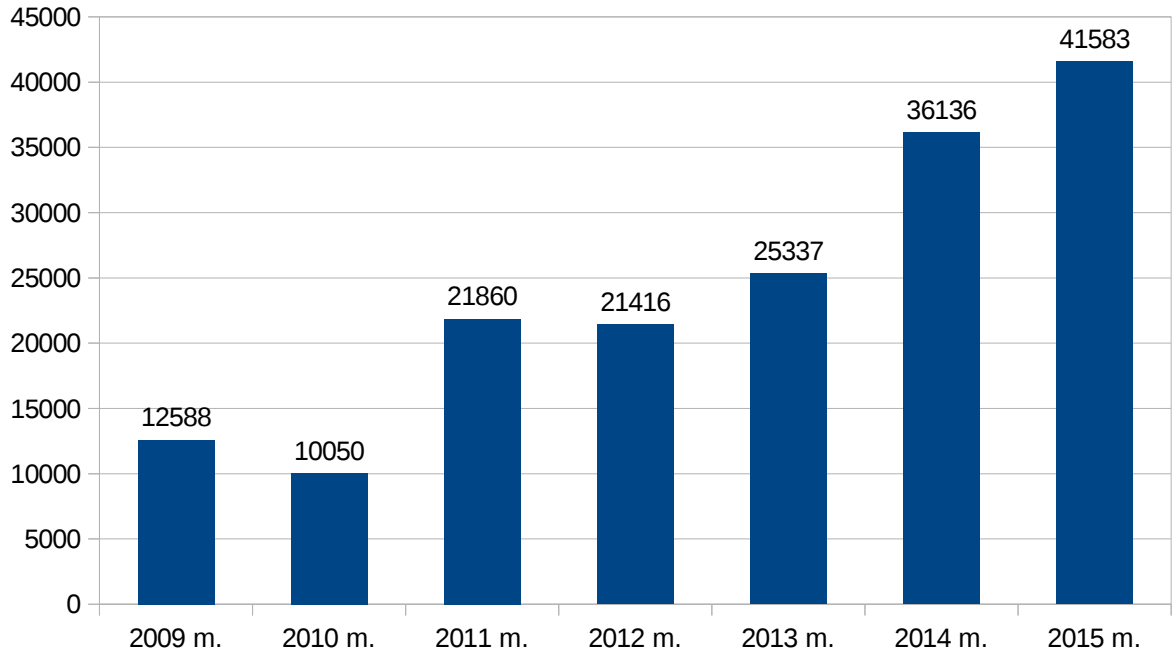
„Yahoo“, „VK.com“. Apie klastotes CERT-LT informuoja Lietuvos ar užsienio interneto paslaugos teikėjus, tarptautinius partnerius ir tarnybinės stoties, iš kurios veikia tokios svetainės, administratorius. Visos žinomos klastotės buvo pašalintos. CERT-LT tinklalapyje pateikiamos atitinkamos rekomendacijos (https://www.cert.lt/naujienos/cert-lt_ispeja_suaktyvejo_elektroniniu_pranesimu_k.html).

Siekdami sumažinti užvaldymo grėsmę, svetainių savininkai turi rūpintis jų saugumu: apsaugoti svetainės valdymo skydą, naudoti sudėtingą prisijungimo slaptažodį ir nuolat jį keisti, diegti turinio valdymo sistemos ir papildinių (angl. *plugins*) atnaujinimus. Be ypatingo poreikio papildinių nereikėtų naudoti. Svetainių kūrėjai, kurie diegia populiarias turinio valdymo sistemas („Wordpress“, „Joomla“ ir pan.), taip pat turi rūpintis tinkamu jų konfigūravimu.

Kitų tipų incidentai

2015 metais CERT-LT ištyrė 50 pranešimų apie paslaugos trikdymo atakas. 2014 m. buvo ištirti 165 tokie pranešimai. Paprastai šios atakos vykdomos automatizuotomis priemonėms, pasitelkiant botų tinklus, arba išnaudojant nesaugius įrenginius (pvz., SSDP saugumo spragą maršruto parinktuve). Siekdamas nutraukti vykdomas DoS atakas, CERT-LT teikė rekomendacijas svetainių savininkams ar elektroninės informacijos prieglobos paslaugas teikiančioms įmonėms, kaip stabdyti šias atakas, koordinavo veiksmus su interneto paslaugų teikėjais ir kitų valstybių CERT tarnybomis.

Taip pat buvo užregistruota 10 ryšių tinklų vientisumo pažeidimų (iš jų 2 atvejai buvo pakankamai rimti, apie kuriuos buvo pranešta Europos tinklų ir informacijos apsaugos agentūrai ENISA), 21 neteisėtas el. duomenų naudojimo atvejis ir įvairaus pobūdžio incidentų – 4 613. Apibendrindami pateikiame CERT-LT registruotų kibernetinių incidentų nuo 2009 m. iki 2015 m. suvestinę.



2 diagrama. CERT-LT 2009–2015 m. apdorotų incidentų suvestinė

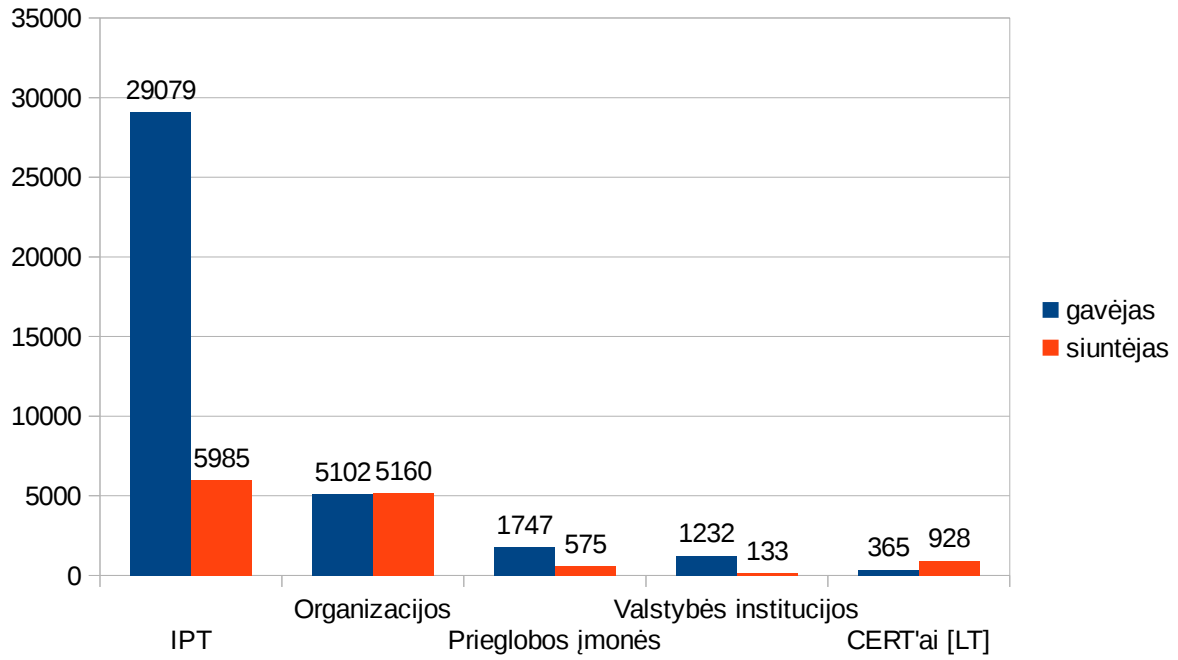
Nauji reikalavimai interneto ir prieglobos paslaugų teikėjams

2015 m. birželio mėn. buvo patvirtinta nauja Viešųjų ryšių tinklų, viešųjų elektroninių ryšių paslaugų ir elektroninės informacijos prieglobos paslaugų saugumo ir vientisumo užtikrinimo taisyklių redakcija. Taisyklės nustato reikalavimus kovai su šiuo metu aktualiausiomis kibernetinio saugumo problemomis tinkluose: IP adresų klastojimu ir elektroninių paslaugų trikdymo atakomis. Esminis taisyklių pakeitimas yra susijęs su Kibernetinio saugumo įstatymo nuostatų įgyvendinimu, kuriuo remiantis pirmą kartą Lietuvoje elektroninės informacijos prieglobos paslaugų teikėjams yra nustatomos teisės ir pareigos užtikrinant jų teikiamų paslaugų saugumą ir vientisumą. Plačiau apie tai – https://www.cert.lt/naujienos/nustatyti_nauji_reikalavimai_interneto_prieglobos_.html.

Bendradarbiavimas, informavimas

2015 m. vasario 27 d. ir birželio 4 d. CERT-LT organizavo susitikimus su interneto paslaugų teikėjais dėl efektyvesnio tinklų saugumo užtikrinimo. Susitikimų metu buvo pristatoma esama padėtis, aptariamos kliūtys kovai su įrenginių saugumo spragomis, nagrinėjami pasiūlymai ir teikėjų patirtis. 2016 m. CERT-LT toliau bendradarbiaus su interneto paslaugų teikėjais, ragins vartotojus pasirūpinti turimų tinklo įrenginių saugumu.

Svarbus CERT-LT veiklos aspektas yra apsikeitimas kibernetinio saugumo informacija.. Tam naudojamos ir kuriamos vis našesnės automatizuoto techninės informacijos apdorojimo ir paskirstymo priemonės. 3-oje diagramoje pateikiami 5 pagrindiniai saugumo pranešimų gavėjai ir siuntėjai, esantys Lietuvoje.



3 diagrama. CERT-LT 2015 m. saugumo pranešimų pagrindiniai siuntėjai ir gavėjai

CERT-LT daug svarbios informacijos skelbia savo svetainėje. Atnaujintoje interneto svetainėje www.cert.lt, kuri yra pritaikyta mobiliesiems įrenginiams ir pasiekiama naudojant IPv6 protokolą, galima:

1) skaityti naujienas, susijusias su IT saugumu;
2) peržiūrėti kaupiamą statistiką (tiek grafikus, tiek ataskaitas);
3) sužinoti pagrindinius CERT-LT veiklos uždavinius;
4) susipažinti su teisės aktais, reglamentuojančiais kibernetinį saugumą;

5) pasinaudoti tikrinimo įrankiais (pvz., patikrinti, ar turimas tinklo įrenginys nenaudoja pažeidžiamo UPnP 1.0 protokolo, ar kompiuteris nėra įtrauktas į botneto veiklą, ar turimas IP adresas nėra užfiksuotas CERT-LT duomenų bazėje kaip dalyvaujantis kenkimo veikloje ir pan.).

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“. Jeigu norite sužinoti IT saugumo aktualijas, prisijunkite (angl. *follow*) prie mūsų adresu https://twitter.com/cert_lt.