2014 METŲ IV KETVIRČIO CERT-LT VEIKLOS ATASKAITA

Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2014 m. IV ketvirčio veiklos rezultatus. Per minėtą ketvirtį CERT-LT ištyrė 11 822 incidentus pagal iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus. Palyginti su 2013 m. IV ketv. (7 576 incidentai), incidentų padaugėjo 56 procentais.

Daugiausia užregistruota incidentų, susijusių su kompiuterių naudotojų tinklo įrenginiais, turinčiais pavojingų saugumo spragų. Per šį laikotarpį CERT-LT užregistravo 5 197 saugumo spragas. 2-oje vietoje pagal incidentų skaičių yra kenkimo programinė įranga (virusai, Trojos arkliai ir pan.) – 3 237 atvejai. Tiek pirmojo, tiek antrojo tipo incidentų skaičius pastebimai augo (atitinkamai 42,5 proc. ir 15,3 proc.)

Per nurodytą laikotarpį buvo užfiksuoti 1 369 informacinių sistemų užvaldymai. CERT-LT tyrimų duomenys rodo, kad dauguma aptiktų kompiuterių užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, jie susiję su pažeidžiama įranga internete. Metų pabaigoje CERT-LT pradėjo taikyti naujas kovos su informacinių sistemų užvaldymu metodikas, kurios iškart davė rezultatų.

Per nurodytą laikotarpį buvo nustatyti 208 el. duomenų klastojimo atvejai. Daugiausia buvo klastojami socialiniai tinklalapiai (facebook.com, vk.com), žinomi interneto portalai (google.com, yahoo.com) ir el. atsiskaitymų svetainė paypal.com. Pasinaudodami brukalu (angl. *spam*) ar kitomis apgaulės priemonėmis, piktavaliai siūlydavo aplankyti suklastotas interneto svetaines siekdami išgauti prisijungimo slaptažodžius ar kitus konfidencialius duomenis. Apie tai CERT-LT informavo Lietuvos ar užsienio interneto paslaugos teikėjus, tarptautinius partnerius ir tarnybinės stoties, iš kurios veikia apgaulingos svetainės, administratorius.

Kiti gauti ir tirti pranešimai:
1) apie manipuliaciją elektroniniais duomenimis – 6;
2) apie elektronines paslaugos trikdymo atakas – 42;
3) įvairaus pobūdžio – 1 763.

CERT-LT nuolat informuoja interneto naudotojus apie kibernetinius pavojus ir teikia rekomendacijas www.cert.lt svetainėje. Pažymėtini 2014 m. IV ketv. įvykiai:
1) Buvo užfiksuota dar viena „banga“ pavojingų tinklalapių, kurie apsimetė policijos ar interpolo tinklalapiais ir reikalavo išpirkos. Tinklalapiai atrodė įtikinamai ir piktavalių buvo suprogramuoti taip, kad neleido uždaryti interneto naršyklės. Pažymėtina, kad šios klastotės, CERT-LT operatyviai veikiant, buvo greitai likviduojamos.
2) Plito brukalas su klastingu „Geodo“ kompiuterių virusu. Antivirusinės programos viruso neatpažindavo, todėl, jei kompiuterio su „Windows“ šeimos operacine sistema naudotojas paleisdavo vykdomąjį failą, kompiuteris būdavo užkrečiamas. CERT-LT persiunčia įtartinus failus antivirusinių programų gamintojams, kurie po analizės atnaujina virusų duomenų bazes.
3) Atrasta pavojinga SSL v3.0 saugumo spraga. Pagal CERT-LT duomenis, lapkričio 24 d. Lietuvoje buvo daugiau kaip 14 000 įrenginių su minėta spraga. CERT-LT parengė išsamias rekomendacijas, kaip apsaugoti savo asmeninį kompiuterį ar tarnybines stotis.

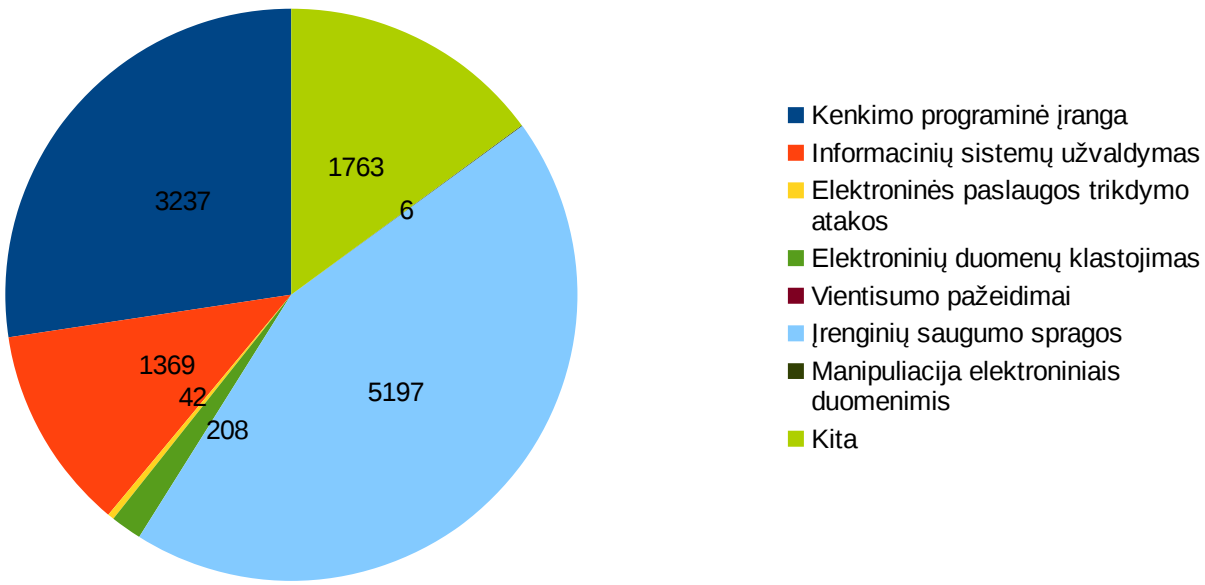
Lentelėse ir grafike pateikiame incidentų suvestines. Visas CERT-LT incidentų statistikos ataskaitas galite rasti tinklalapyje https://www.cert.lt/statistika.htm.

Lentelė 1. CERT-LT 2014 m. IV ketv. nagrinėtų incidentų suvestinė

Incidentų tipas	Incidentų skaičius	Procentinė dalis (proc.)
Kenkimo programinė įranga	3 237	27,3
Informacinių sistemų užvaldymas	1 369	11,5
Elektroninės paslaugos trikdymo atakos	42	0,3
Elektroninių duomenų klastojimas	208	1,7
Vientisumo pažeidimai	0	0
Įrenginių saugumo spragos	5 197	43,9
Manipuliacija elektroniniais duomenimis	6	0,05
Kita	1 763	14,9

Lentelė 2. CERT-LT 2014 m. III ketv. ir IV ketv. nagrinėtų incidentų skaičiaus palyginimas

Incidentų tipas	Incidentų skaičius 2014 m. III ketv.	Incidentų skaičius 2014 m. IV ketv.	Pokytis, proc.
Kenkimo programinė įranga	2 807	3 237	15,3
Informacinių sistemų užvaldymas	1 122	1 369	22,0
El. paslaugos trikdymo atakos	45	42	-6,6
El. duomenų klastojimas	220	208	-5,4
Vientisumo pažeidimai	5	0	-100
Įrenginių saugumo spragos	3 647	5 197	42,5
Manipuliacija el. duomenimis	8	6	-25
Kita	1 712	1 763	2,9



1 pav. 2014 m. IV ketvirtį CERT-LT užfiksuotų incidentų statistika