2015 METŲ I KETVIRČIO CERT-LT VEIKLOS ATASKAITA

Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2015 m. I ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT ištyrė 11 707 incidentus pagal iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus.** Palyginti su 2014 m. I ketv. (7 375 incidentai), incidentų padaugėjo 59 procentais. Palyginti su 2014 m. IV ketvirčiu (11 822 incidentai), incidentų sumažėjo 1 procentu.

Pagal vyraujančių incidentų skaičių šis ketvirtis panašus į 2014 m. paskutinį ketvirtį. Daugiausia užregistruota incidentų, susijusių su kompiuterių naudotojų tinklo įrenginiais, turinčiais pavojingų saugumo spragų – 4 856. 2-oje vietoje pagal incidentų skaičių yra kenkimo programinė įranga (virusai, Trojos arkliai ir pan.) – 3 051 atvejai. Šių dviejų incidentų tipų skaičiaus augimo tendencija pasikeitė ir dabar jų užfiksuota kiek mažiau (atitinkamai 6,5 proc. ir 5,7 proc. mažiau nei praeitą ketvirtį). Taip pat per nurodytą laikotarpį buvo užfiksuoti 1 494 informacinių sistemų užvaldymai. CERT-LT tyrimų duomenys rodo, kad dauguma aptiktų kompiuterių užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis ir susiję su pažeidžiama įranga internete.

El. duomenų klastojimo atvejų buvo 257. Daugiausia buvo klastojami socialiniai tinklalapiai (facebook.com, vk.com), el. pašto sistemos (gmail.com, yahoo.com), el. atsiskaitymų svetainė paypal.com. Taip pat buvo klastojami Lietuvoje veikiančių bankų tinklalapiai. Pasinaudodami brukalu (angl. *spam*) ar kitomis apgaulės priemonėmis, piktavaliai siūlydavo aplankyti suklastotas interneto svetaines siekdami išgauti prisijungimo slaptažodžius ar kitus konfidencialius duomenis. Šios klastotės, CERT-LT operatyviai veikiant, buvo santykinai greitai likviduojamos.

Kiti gauti ir tirti pranešimai:
1) apie manipuliaciją elektroniniais duomenimis – 5;
2) apie elektronines paslaugos trikdymo atakas – 18;
3) apie vientisumo pažeidimą – 1;
4) įvairaus pobūdžio – 2025.

CERT-LT nuolat informuoja interneto naudotojus apie kibernetinius pavojus ir teikia rekomendacijas tinklalapyje www.cert.lt. Pažymėtini 2015 m. I ketv. įvykiai:
1) Pavojingo programinio kodo „CTB Locker“ plitimas. Jis priklauso „*ransomware*“ (išpirkos reikalaujančių) kodų šeimai. Aktyvuotas kompiuteryje, turinčiame „Windows“ OS atmainą, kodas užšifruoja failus ir parodo pranešimą, kuriuo siūloma sumokėti išpirką (paprastai – bitkoinais). CERT-LT pataria nuolat daryti atsargines kopijas (kurių bent viena turi būti saugoma kitoje vietoje).
2) Socialiniame tinklalapyje „Facebook“ plito pavojingas „Chrome“ naršyklės papildinys (angl. *add-on*). Įdiegta į kompiuterį kaip papildinys, programa „Facebook“ draugams siuntė nuorodą į neva vaizdo klipą. Paspaudęs ant nuorodos, kitas asmuo taip pat galėjo užkrėsti savo kompiuterį. Atlikęs analizę, CERT-LT kreipėsi į užsienyje esančius paslaugų teikėjus su prašymu pašalinti minėtos žalingos veiklos komponentus.
3) Kovo 17 dieną dėl VĮ „Infostruktūra“ įrangos gedimo buvo paveikta nemaža Lietuvos interneto erdvės dalis, įskaitant ir valstybės institucijų tinklalapius. CERT-LT darbuotojai stebėjo gedimo atsiradimą ir jo pasekmes naudodami Lietuvos interneto stebėjimo sistemą LITIS. Apie gedimą buvo pranešta Europos tinklų ir informacijos apsaugos agentūrai (angl. *ENISA*). Gedimo pasekmės buvo pašalintos per maždaug 3 val.
4) Nemažėjantis piktybinio programinio kodo „Stealrat“, kuriančio botnetus, aktyvumas. Kiekvieną dieną CERT-LT fiksuoja tiek naujus, tiek jau žinomus užkrėstus tinklalapius. Visais atvejais informacijos prieglobos paslaugas teikiančios bendrovės ir tinklalapių savininkai raginami imtis priemonių piktybinio kodo šalinimui ir tinklalapio apsaugojimui.

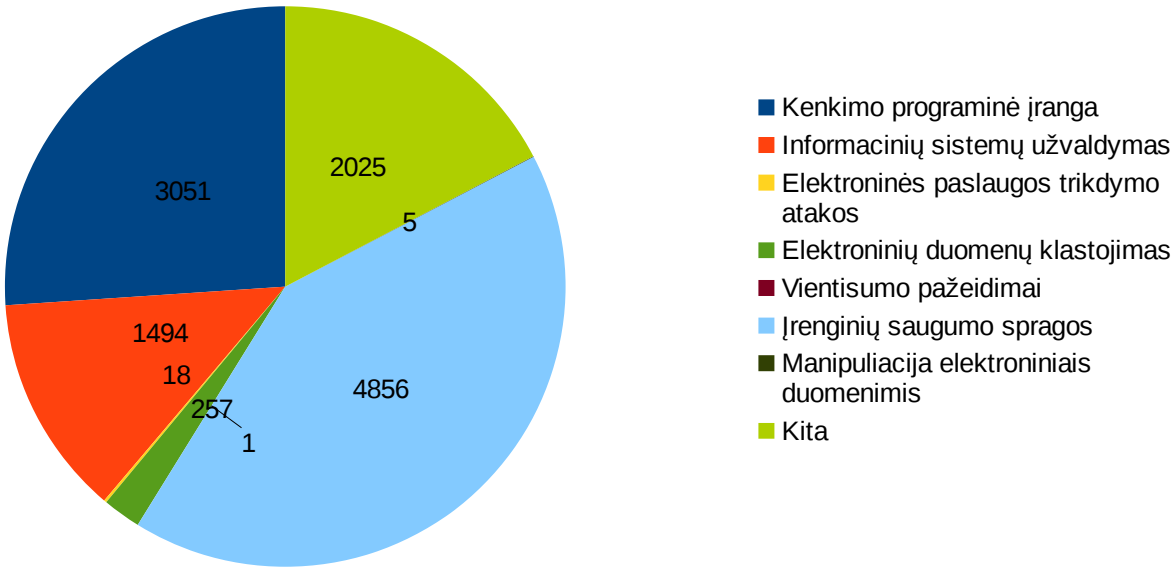
Lentelėse ir diagramoje pateikiame incidentų suvestines. Visas CERT-LT incidentų statistikos ataskaitas galite rasti tinklalapyje https://www.cert.lt/statistika.htm.

Lentelė 1. CERT-LT 2015 m. I ketv. nagrinėtų incidentų suvestinė

Incidentų tipas	Incidentų skaičius	Procentinė dalis (proc.)
Kenkimo programinė įranga	3 051	26
Informacinių sistemų užvaldymas	1 494	12,8
Elektroninės paslaugos trikdymo atakos	18	0,2
Elektroninių duomenų klastojimas	257	2,2
Vientisumo pažeidimai	1	0
Įrenginių saugumo spragos	4 856	41,5
Manipuliacija elektroniniais duomenimis	5	0
Kita	2 025	17,3

Lentelė 2. CERT-LT 2014 m. IV ketv. ir 2015 m. I ketv. nagrinėtų incidentų skaičiaus palyginimas

Incidentų tipas	Incidentų skaičius 2014 m. IV ketv.	Incidentų skaičius 2015 m. I ketv.	Pokytis, proc.
Kenkimo programinė įranga	3 237	3 051	-5,7
Informacinių sistemų užvaldymas	1 369	1 494	9,1
El. paslaugos trikdymo atakos	42	18	-57,1
El. duomenų klastojimas	208	257	23,5
Vientisumo pažeidimai	0	1	n/d
Įrenginių saugumo spragos	5 197	4 856	-6,5
Manipuliacija el. duomenimis	6	5	-16,6
Kita	1 763	2 025	14,8



1 pav. 2015 m. I ketvirtį CERT-LT užfiksuotų incidentų statistika