2015 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 2015 m. IV ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT ištyrė 10 641 incidentą 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. IV ketv. (11 822 incidentai), tirtų incidentų sumažėjo 10 procentų. Palyginti su 2015 m. III ketvirčiu (9708 incidentai), tirtų incidentų padaugėjo 9,6 procento.

Virš 40 procentų visų incidentų yra susijusi su kompiuterių naudotojų tinklo įrenginiais, turinčiais pavojingų saugumo spragų – 4 383. Ketvirtadalį visų incidentų sudaro kenkimo programinė įranga (virusai, Trojos arkliai ir pan.) – 2 686 atvejai. Taip pat per nurodytą laikotarpį buvo užfiksuoti 2 517 informacinių sistemų užvaldymai. CERT-LT tyrimų duomenys rodo, kad dauguma aptiktų kompiuterių užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis ir susiję su pažeidžiama įranga internete. Pagal skaitinius duomenis aptariamasis ketvirtis ženkliai skiriasi nuo 2014 m. IV ketvirčio. Yra ir tam tikrų pokyčių, palyginti su 2015 m. III ketvirčiu:
1) informacinių sistemų užvaldymo atvejų padaugėjo net 49 proc.;
2) elektroninių paslaugų trikdymo (angl. *DoS* ir *DDoS*) atvejų sumažėjo 36 proc.

Per IV ketvirtį buvo ištirti 116 elektroninių duomenų klastojimo atvejų. 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 ir užsienyje veikiančių bankų tinklalapiai (pastarųjų klastočių buvo daugiau). Pasinaudodami brukalu (angl. *spam*) ar kitomis apgaulės priemonėmis, piktavaliai siūlydavo aplankyti suklastotas interneto svetaines, kad išgautų prisijungimo slaptažodžius ar kitus konfidencialius duomenis. Šios klastotės, CERT-LT operatyviai veikiant, buvo santykinai greitai likviduojamos.

Kiti gauti ir tirti pranešimai:
1) apie neteisėtą elektroninių duomenų naudojimą – 0;
2) apie elektroninių paslaugų trikdymą – 7;
3) apie vientisumo pažeidimą – 5;
4) įvairaus pobūdžio – 927 (įskaitant 95 konsultacijas).

Pažymėtini ketvirčio įvykiai:
1) Dažnai plito brukalas su itin pavojingais failus šifruojančiais ir išpirkos reikalaujančiais virusais (plačiau: https://www.cert.lt/naujienos.html). Nors yra sukurti keli įrankiai, skirti dešifruoti užšifruotus failus (pvz., https://noransom.kaspersky.com), tikimybė atgauti failus yra itin maža. Ne vienas IT ar IT saugumo tinklalapis tokius (angl. *ransomware*) virusus vadina didžiausia kibernetine grėsme atėjusiais 2016 m.
2) 2015 m. gruodžio pabaigoje Lietuvoje kirminu „Pykspa“ buvo užvaldyti keli šimtai kompiuterių (per užvaldymo piką tokių buvo virš 600).

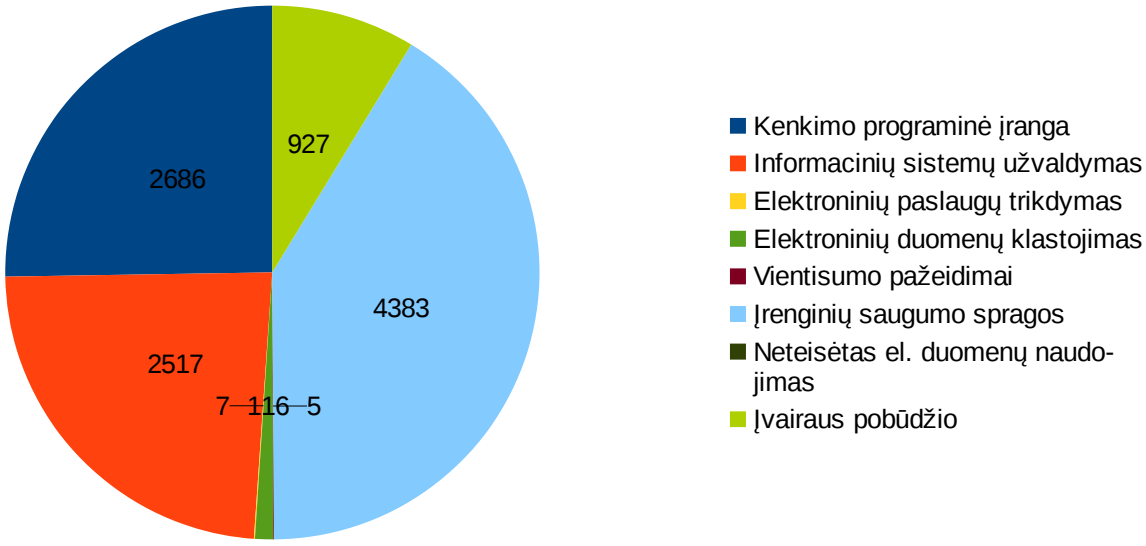
Lentelėse ir diagramoje pateikiame tirtų incidentų suvestines. Visas CERT-LT tirtų incidentų statistikos ataskaitas galite rasti tinklalapyje https://www.cert.lt/statistika.htm. CERT-LT skelbia įspėjimus apie kibernetinius incidentus bei trumpas kibernetinio saugumo naujienas socialiniame tinkle „Twitter“. Jeigu norite sužinoti naujausias IT saugumo aktualijas, prisijunkite (angl. *follow*) prie mūsų adresu https://twitter.com/cert_lt.

1 lentelė. CERT-LT 2015 m. IV ketv. tirtų incidentų suvestinė

Incidentų tipas	Incidentų skaičius	Procentinė dalis nuo 10 641
Kenkimo programinė įranga	2 686	25,2
Informacinių sistemų užvaldymas	2 517	23,7
Elektroninių paslaugų trikdymas	7	0,1
Elektroninių duomenų klastojimas	116	1,1
Vientisumo pažeidimai	5	0
Įrenginių saugumo spragos	4383	41,2
Neteisėtas el. duomenų naudojimas	0	0
Įvairaus pobūdžio	927	8,7

2 lentelė. CERT-LT 2014 m. IV ketv., 2015 m. III ir IV ketv. tirtų incidentų skaičiaus palyginimas

Incidentų tipas	Incidentų skaičius		Pokytis, proc.	
	2015 III	2014 IV	2015 IV / 2015 III	2015 IV / 2014 IV
Kenkimo programinė įranga	2 612	3 237	2,8	-17
Informacinių sistemų užvaldymas	1 686	1 369	49,3	83,9
El. paslaugų trikdymas	11	42	-36,4	-83,3
El. duomenų klastojimas	103	208	12,6	-44,2
Vientisumo pažeidimai	2	0	150	n/d
Įrenginių saugumo spragos	4 490	5 197	-2,4	-15,7
Neteisėtas el. duomenų naudojimas	8	6	-100	-100
Įvairaus pobūdžio	796	1 763	16,5	-47,4



1 pav. 2015 m. IV ketvirtį CERT-LT tirtų incidentų statistika