2016 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 2016 m. I ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT ištyrė 12 035 incidentus pagal iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus.** Palyginti su 2015 m. I ketv. (11 707 incidentai), tirtų incidentų padaugėjo 2,8 procento. Palyginti su 2015 m. IV ketvirčiu (10 641 incidentas), tirtų incidentų padaugėjo 13,1 procento.

Beveik nesikeitė dviejų pagrindinių incidentų tipų procentinės dalys nuo bendro incidentų skaičiaus. Virš 40 procentų visų incidentų buvo susiję su kompiuterių naudotojų tinklo įrenginiais, turinčiais pavojingų saugumo spragų – 4 963. Ketvirtadalį visų incidentų sudarė kenkimo programinė įranga (virusai, Trojos arkliai ir pan.) – 2 887 atvejai. Pastebime nuolatinę informacinių sistemų užvaldymų skaičiaus augumo tendenciją. Per 2016 m. I ketvirtį tokių buvo net 2 902, beveik dvigubai daugiau nei 2015 m. I ketvirtį. CERT-LT tyrimų duomenys rodo, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis ir susiję su pažeidžiama įranga internete.

Elektroninių duomenų klastojimų skaičius, lyginant su 2015 m. I ketvirčiu, sumažėjo daugiau nei dvigubai: jų buvo 112. Daugiausia buvo klastojami socialinis tinklalapis facebook.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. Minėtas klastotes CERT-LT darbuotojams pavyksta greitai likviduoti.

Kiti gauti ir tirti pranešimai:
1) apie neteisėtą elektroninių duomenų naudojimą – 1;
2) apie elektroninių paslaugų trikdymą – 10 (ženklus padidėjimas lyginant su 2015 IV ketvirčiu, bet kone toks pat procentinis sumažėjimas lyginant su 2015 I ketvirčiu);
3) apie vientisumo pažeidimą – 6;
4) įvairaus pobūdžio – 1 154 (įskaitant 60 konsultacijų).

Pažymėtini ketvirčio įvykiai:
1) Dažnai plito brukalas su pavojingu kenkimo kodu. Pagrindinė naujovė – kodas yra „JavaScript“, o ne EXE failų pavidalu. Laiškų antraštės paprastai yra angliškos, dviejų tipų: apie neva gautą sąskaitą ir apie neva skenuotą dokumentą.
2) Pasaulio IT bendruomenė buvo aptikusi 2 pavojingas plačiai naudojamos programinės įrangos spragas, viena iš kurių egzistavo nuo 2008 m. gegužės mėn. (žr. https://www.cert.lt/naujienos.html). Paminėtina, kad 2015 metais saugumo spragų katalogas, priklausantis kompanijai „Risk Based Security“, turėjo 14 185 įrašų.

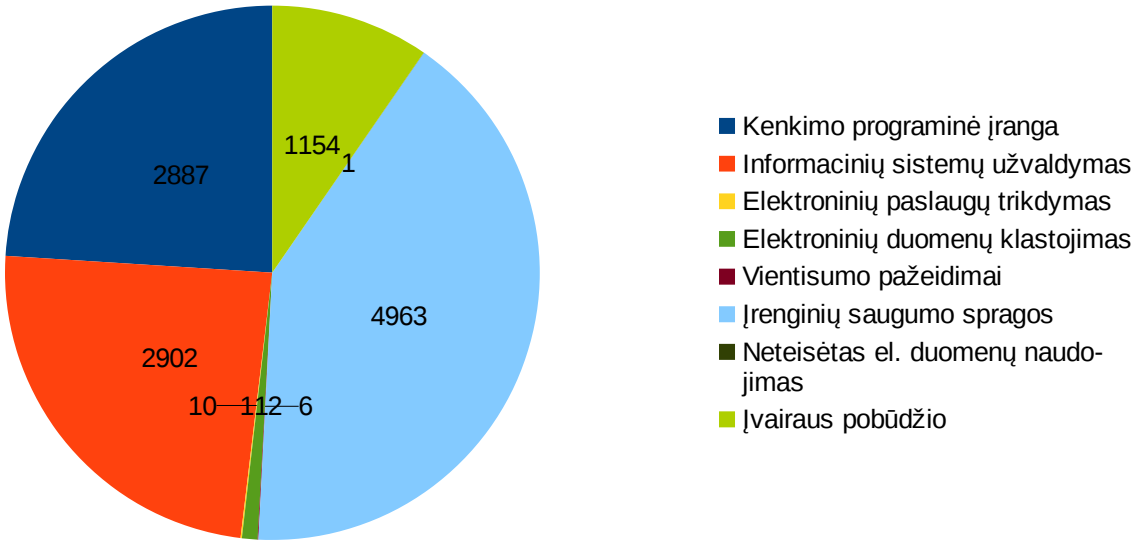
Lentelėse ir diagramoje pateikiame tirtų incidentų suvestines. Visas CERT-LT tirtų incidentų statistikos ataskaitas galite rasti tinklalapyje https://www.cert.lt/statistika.htm. CERT-LT skelbia įspėjimus apie kibernetinius incidentus bei trumpas kibernetinio saugumo naujienas socialiniame tinkle „Twitter“.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

1 lentelė. CERT-LT 2016 m. I ketv. tirtų incidentų suvestinė

Incidentų tipas	Incidentų skaičius	Procentinė dalis nuo 12 035
Kenkimo programinė įranga	2 887	24
Informacinių sistemų užvaldymas	2 902	23,1
Elektroninių paslaugų trikdymas	10	0,1
Elektroninių duomenų klastojimas	112	0,9
Vientisumo pažeidimai	6	0
Įrenginių saugumo spragos	4 963	41,2
Neteisėtas el. duomenų naudojimas	1	0
Įvairaus pobūdžio	1 154	9,6

2 lentelė. CERT-LT 2015 m. I ketv., 2015 m. IV ir 2016 m. I ketv. tirtų incidentų skaičiaus palyginimas

Incidentų tipas	Incidentų skaičius		Pokytis, proc.	
	2015 IV	2015 I	2016 I / 2015 IV	2016 I / 2015 I
Kenkimo programinė įranga	2 686	3 051	7,5	-5,4
Informacinių sistemų užvaldymas	2 517	1 494	15,3	94,2
El. paslaugų trikdymas	7	18	42,9	-44,4
El. duomenų klastojimas	116	257	-3,4	-56,4
Vientisumo pažeidimai	5	1	20	500
Įrenginių saugumo spragos	4 383	4 856	13,2	2,2
Neteisėtas el. duomenų naudojimas	0	5	n/d	-80
Įvairaus pobūdžio	927	2025	24,5	-43



1 pav. 2016 m. I ketvirtį CERT-LT tirtų incidentų statistika