Per 2014 m. III ketvirtį CERT-LT ištyrė 9566 incidentus elektroninėje erdvėje

Lietuvos Respublikos ryšių reguliavimo tarnybos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys (CERT-LT) apibendrina 2014 m. III ketvirčio veiklos rezultatus. CERT-LT 2014 m. III ketvirtį ištyrė 9 566 incidentus pagal iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus apie incidentus elektroninėje erdvėje. Palyginti su tuo pačiu 2013 m. laikotarpiu (5 907 incidentų), incidentų padaugėjo 62 procentais. Šių metų III-ame ketvirtyje CERT-LT atliktų tyrimų metu buvo užregistruoti 3 647 incidentai, susiję su pavojingomis interneto tinkle veikiančių įrenginių saugumo spragomis, kurios gali būti išnaudotos kenkimo veiklai internete.

Daugiausia užregistruota incidentų, susijusių su kompiuterių naudotojų įrenginiais, skirtais prisijungti prie interneto ir turinčiais pavojingų saugumo spragų. Per šį laikotarpį CERT-LT užregistravo 3 647 pavojingas saugumo spragas – 10 proc. daugiau nei 2014 m. II ketvirtį, ir 2 807 kenkimo programinės įrangos panaudojimo atvejų – 16 proc. daugiau nei 2014 m. II ketvirtį, ir 1 222 kompiuterių užvaldymo atvejus – 113 proc. daugiau nei 2014 m. II ketvirtį. CERT-LT atliktų tyrimų duomenys parodė, kad dauguma aptiktų kompiuterių užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis, jie susiję su pažeidžiama įranga internete, o tarp kenkimo programinės įrangos incidentų daugiausia buvo susijusių su botnetų (kompiuterių robotų tinklų) veikla.

2014 m. III ketvirtį padaugėjo klastojimo (angl. phishing) atvejų. CERT-LT ištyrė 220 pranešimus – daugiau nei dviem kartais daugiau nei 2014 m. II ketvirtį. Didžiąją šių pranešimų dalį sudarė pranešimai apie finansinių įmonių, įskaitant Lietuvoje veikiančių finansinių įmonių ir bankų, suklastotas interneto svetaines, kurios veikdavo dažniausiai ne Europos Sąjungos tarnybinėse stotyse. Pasinaudodami nepageidaujamomis elektroninio pašto žinutėmis (angl. spam) ar kitomis apgaulės priemonėmis, piktavaliai siūlydavo aplankyti suklastotas interneto svetaines siekdami išgauti prisijungimo slaptažodžius ir (ar) kitus konfidencialius duomenis. Apie šiuos atvejus CERT-LT informavo Lietuvos ar užsienio interneto paslaugos teikėjus, tarptautinius partnerius ir tarnybinės stoties, iš kurios veikia tokios svetainės, administratorius.

Taip pat šį ketvirti smarkiai išaugo, neva nuo judriojo ryšio operatorių siunčiamų, elektroninių laiškų kiekis, prie kurių pridedama suklastota sąskaita-faktūra ir zip archyvo failas su kompiuteriniu virusu. CERT-LT nustatė kad elektroniniai laiškai platinami iš *cutwail spambot* virusu infekuotų kompiuterių (*spambot* skirti dideliam kiekiui elektroninių laiškų siųsti be vartotojo žinios). Elektroniniame laiške pridėtas zip archyvas „Paslaugu_ataskaita.pdf.zip“ arba „PVM_saskaita.pdf.zip“ ar pan. su failu pavadinimu „Paslaugu_ataskaita.pdf.pif“ arba „PVM_saskaita.pdf.pif“ ar pan. (Windows operacinių sistemų naudotojams failo plėtinio .pif gali nesimatyti), kuris yra infekuotas *Injector* Trojos arklio virusu, skirtu užvaldyti Windows tipo operacines sistemas. CERT-LT apie tai informavo interneto naudotojus ir pateikė rekomendacijas www.cert.lt svetainėje.

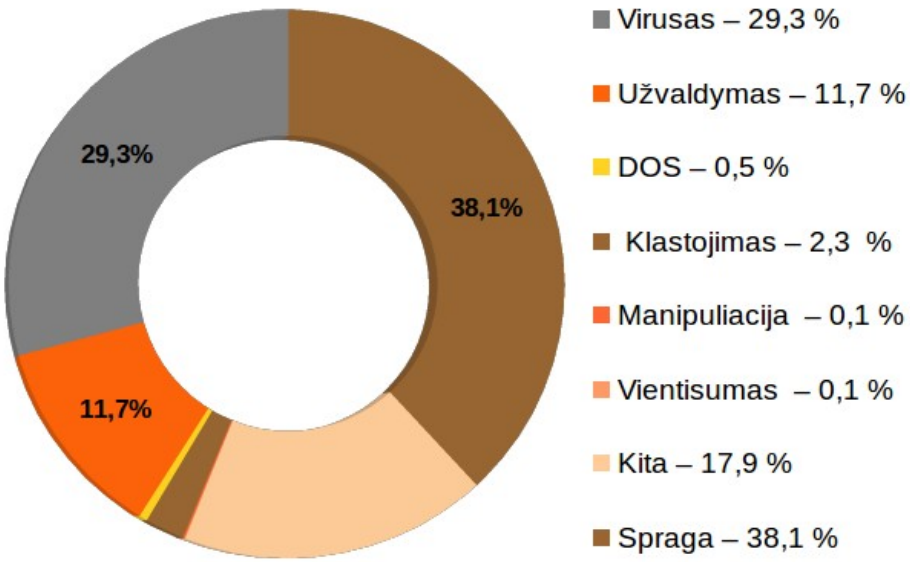
Kiti gauti ir tirti pranešimai: apie manipuliaciją elektroniniais duomenimis – 8 (2014 m. II ketvirtį – 5), vientisumo pažeidimus – 5 (2014 m. II ketvirtį – 11), ir paskirstytosios paslaugos trikdymo atakas (DdoS) - 45 (2014 m. II ketvirtį – 35)

Taip pat CERT-LT 2014 m. rugsėjo 22-24 dienomis organizavo tarptautines tarpinstitucines kibernetines pratybas „X14“. Šios pratybos buvo surengtos atsižvelgiant į šių dienų kibernetinio saugumo realijas, jose dalyvavo 25 valstybinės institucijos, 8 bankų atstovai, 10 Lietuvos ir užsienio valstybių CERT padalinių bei Galimų kibernetinių saugumo incidentų pasekmių valdymo grupės nariai. Kaip ir ankstesnių pratybų, taip ir šių pratybų tikslas buvo stiprinti tarptinsitucinio

bendradarbiavimo sprendžiant sudėtingesnius kibernetinius incidentus efektyvumą, komunikacijos spartą, būtinybę kritinėse situacijose rasti atsakingų institucijų atstovų kontaktus, pasirengimą naudoti lengvai prieinamas šifravimo priemones duomenų perdavimui viešaisiais tinklais ir įgūdžius operatyviai keistis informacija galimų kibernetinių incidentų metu.

Lentelė. 2014 m. III ketv. tirti pranešimai apie incidentus pagal tipus

Incidentų tipas	**Incidentų skaičius 2014m. III ketv. (vnt.)**	**Procentinė visų incidentų dalis (proc.)**
Spraga	3647	38,1
Virusas	2807	29,3
Užvaldymas	1122	11,7
Klastojimas	220	2,3
DOS	45	0,5
Vientisumas	5	0,1
Manipuliacija	8	0,1
Kita	1712	17,9



1 pav. 2014 m. III ketvirtį CERT-LT užfiksuotų incidentų statistika, proc.

Visas CERT-LT incidentų statistikos ataskaitas galite rasti interneto svetainėje https://www.cert.lt/statistika.html