2016 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 2016 m. IV ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT apdorojo 13 874 incidentus pagal iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus.** Pažymėtina, kad 15 proc. visų incidentų buvo detaliai tiriami CERT-LT specialistų, įskaitant paslaugos trikdymo (angl. *Denial of Service*, *DoS*) atakas, informacinių sistemų užvaldymo ir kitokius išskirtinius incidentus, taip pat incidentus, apie kuriuos pranešta CERT-LT interneto svetainėje užpildžius specialią formą (www.cert.lt/pranesti.html) arba elektroniniu paštu. Likusioji incidentų dalis yra apdorojama automatiniu būdu, perduodant informaciją apie incidentą bei rekomendacijas paslaugų teikėjams, kuriems priklauso su incidentu susiję IP adresai. Palyginti su 2015 m. IV ketv. (10 641 incidentai), incidentų padaugėjo 30,4 procento. Palyginti su 2016 m. III ketvirčiu (12 563 incidentai), incidentų padaugėjo 10,4 procento.

Dviejų incidentų tipų procentinės dalys buvo kaip ir praėjusiame ketvirtyje. 42 procentai visų incidentų buvo susiję su kompiuterių naudotojų tinklo įrenginiais, turinčiais saugumo spragų – 5 801. 22 procentus visų incidentų sudarė kenkimo programinė įranga (virusai, Trojos arkliai ir pan.) – 2 989 atvejai. Informacinių sistemų užvaldymų (3 098) skaičius auga kelis ketvirčius iš eilės: jų 23 proc. daugiau nei prieš metus. CERT-LT tyrimų duomenys rodo, kad dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėmis ir susiję su pažeidžiama įranga internete. Kaip ir anksčiau, daugiausia buvo klastojamos socialinio tinklo svetainė *facebook.com*, el. pašto sistemos (*gmail.com*, *yahoo.com*), el. atsiskaitymų svetainė *paypal.com*, kartais – užsienio bankų svetainės ir užsienio el. parduotuvės.

Pagal elektroninių paslaugų trikdymo atvejų skaičių ketvirtis buvo pakankamai ramus – užfiksuoti 4 atvejai. Kiti gauti ir tirti pranešimai: apie vientisumo pažeidimus – 1, apie elektroninių duomenų klastojimą – 143, įvairaus pobūdžio – 1 838.

Kiti ketvirčio įvykiai (taip pat žr. https://www.cert.lt/naujienos.html):

1) Tęsiasi brukalo su kenkimo kodu (paprastai – „JavaScript“) plitimas. Kenkimo kodo paskirtis – užmegzti ryšį su vienu arba keliais nutolusiais kompiuteriais (kontroleriais), iš jų į aukos įrenginį atsiųsti kitą – pagrindinį – kenkimo kodą ir jį paleisti. Pasekmės gali būti itin blogos, jei bus paleistas išpirkos reikalaujantis (angl. *ransomware*) virusas, aukos kompiuteryje užšifruojantis kone visą svarbią informaciją. Tokį brukalą atpažinti nesunku: nedidelis (keli KB) priedas, angliškos laiškų antraštės, nors pasitaiko ir lietuviškų (neretai – gramatiškai netaisyklingų).

2) Veikė didžiulis botnetas (užvaldytų įrenginių tinklas) „Mirai“. Naudojami jį, piktavaliai vykdė itin galingas paslaugos trikdymo atakas, kurių įtaka jautėsi ir Lietuvos paslaugų teikėjų tinkluose. CERT-LT duomenimis, IV ketv. pabaigoje Lietuvoje buvo beveik 150 „Mirai“ užkrėstų įrenginių (unikalių IP adresų).

3) CERT-LT kartu su Lietuvos policija dalyvavo dviejose tarptautinėse švietimo kampanijose: dėl kenkimo programų mobiliuosiuose įrenginiuose ir dėl neatsakingo jaunimo požiūrio į kompiuterinius nusikaltimus ir galimas rizikas. Plačiau apie šias kampanijas: https://www.cert.lt/naujienos/tarptautines_operacijos_taikiniai_-_jauni_ddos_kib.html ir https://www.cert.lt/naujienos/kaip_apsaugoti_nuo_kenkimo_programu_mobiliuosius_i.html.

4) Spalio mėn. CERT-LT kartu su Lietuvos interneto ir debesų kompiuterijos paslaugų teikėjais dalyvavo didelio masto kibernetinio saugumo pratybose „Cyber Europe 2016“, kurias organizavo ENISA. Tai didžiausios ir sudėtingiausios iki šiol vykusios kibernetinio saugumo pratybos Europos Sąjungoje, kuriose dalyvavo kibernetinio saugumo specialistai iš daugiau kaip 300 organizacijų iš 30 Europos Sąjungos ir EFTA šalių. Šių pratybų tikslas buvo patikrinti bendradarbiavo procesus Europos Sąjungos ir nacionaliniu lygiu, didinti kvalifikacinius gebėjimus kibernetinio saugumo srityje.

Lentelėse ir diagramoje pateikiame incidentų suvestines. Visas CERT-LT apdorotų incidentų statistikos ataskaitas galite rasti tinklalapyje https://www.cert.lt/statistika.html. 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., 2016 m. III ir IV ketv. apdorotų incidentų skaičiaus palyginimas

Incidentų tipas	Incidentų skaičius			Pokytis, proc.	
	2015 IV	2016 III	2016 IV	2016 IV / 2015 IV	2016 IV / 2016 III
Kenkimo programinė įranga	2 686	2 805	2 989	11,3	6,6
Informacinių sistemų užvaldymas	2 517	2 383	3 098	23,1	30
El. paslaugų trikdymas	7	11	4	-42,9	-63,6
El. duomenų klastojimas	116	153	143	23,3	-6,5
Vientisumo pažeidimai	5	3	1	-80	-66,7
Įrenginių saugumo spragos	4 383	5 309	5 801	32,4	9,3
Neteisėtas elektroninių duomenų naudojimas	0	0	0	n/d	n/d
Įvairaus pobūdžio	927	1 899	1 838	98,3	-3,2
Iš viso	10 641	12 563	13 874	30,4	10,4

1 pav. 2016 m. IV ketvirtį CERT-LT tirtų incidentų diagrama (proc. nuo 100)