# 2016 METŲ III 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. III ketvirčio veiklos rezultatus. **Per minėtą ketvirtį CERT-LT apdorojo 12 563 incidentus pagal iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, atliekančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus.** Pažymėtina, kad 16 proc. visų incidentų buvo detaliai tiriami CERT-LT specialistų, įskaitant paskirstyto paslaugos trikdymo (angl. *Distributed Denial of Service*, *DDoS*) 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. III ketv. (9 708 incidentai), incidentų padaugėjo 29,4 procento. Palyginti su 2016 m. II ketvirčiu (10 991 incidentai), incidentų padaugėjo 14,3 procento.

Du pagrindiniai incidentų tipai kartu sudaro 2 trečdalius visų incidentų. 42 procentai visų incidentų buvo susiję su kompiuterių naudotojų tinklo įrenginiais, turinčiais pavojingų saugumo spragų – 5 309. 22 procentus visų incidentų sudarė kenkimo programinė įranga (virusai, Trojos arkliai ir pan.) – 2 805 atvejai. Informacinių sistemų užvaldymų (2 383) ir elektroninių duomenų klastojimų (153) skaičius auga ne pirmą ketvirtį: užvaldymų buvo 41 proc. daugiau, klastojimų – 48 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 ramesnis nei ankstesnis – užfiksuota 11 atvejų. Kiti gauti ir tirti pranešimai: apie vientisumo pažeidimą – 3, įvairaus pobūdžio – 1 899. Ketvirčio įvykiai ir tendencijos (plačiau – https://www.cert.lt/naujienos.html):

1) Visus metus tęsiasi brukalo su kenkimo kodu (paprastai – „JavaScript“) plitimas; šį ketvirtį tokio brukalo buvo itin daug. 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) ZIP formato priedas, angliškos laiškų antraštės.

2) Aptiktos pavojingos saugumo spragos šiose programose: turinio valdymo sistemoje „Drupal“, duomenų bazių valdymo sistemose „MySQL“ ir „MariaDB“.

3) Aptiktos saugumo spragos tinklų įrangos gamintojos „Cisco“ įrenginiuose.

Paminėtina, kad padalinys CERT-LT ketina pakeisti incidentų klasifikavimą (taksonomiją), atsižvelgdamas į gerąją kitų CERT padalinių patirtį.

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. III ketv., 2016 m. II ir III ketv. apdorotų incidentų skaičiaus palyginimas

| Incidentų tipas | Incidentų skaičius | | | Pokytis, proc. | |
|---|---|---|---|---|---|
| | 2015 III | 2016 II | 2016 III | 2016 III / 2015 III | 2016 III / 2016 II |
| Kenkimo programinė įranga | 2 612 | 2 531 | 2 805 | 7,4 | 10,8 |
| Informacinių sistemų užvaldymas | 1 686 | 2 290 | 2 383 | 41,3 | 4,1 |
| El. paslaugų trikdymas | 11 | 36 | 11 | 0 | –69,4 |
| El. duomenų klastojimas | 103 | 147 | 153 | 48,5 | 4,1 |
| Vientisumo pažeidimai | 2 | 11 | 3 | 50 | –72,7 |
| Įrenginių saugumo spragos | 4 490 | 4 417 | 5 309 | 18,2 | 20,2 |
| Neteisėtas elektroninių duomenų naudojimas | 8 | 0 | 0 | –100 | n/d |
| Įvairaus pobūdžio | 796 | 1 559 | 1 899 | 138,6 | 21.8 |
| Iš viso | 9 708 | 10 991 | 12 563 | 29,4 | 14,3 |

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