CERT-LT apibendrina III ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2009 m. III ketvirčio veiklos rezultatus. CERT-LT per 2009 metų III ketvirtį tyrė 4 383 iš Lietuvos elektroninių ryšių paslaugų teikėjų, užsienio CERT tarnybų, vykdančių tarptautinius incidentų tyrimus, ir iš Lietuvos interneto naudotojų gautus pranešimus apie incidentus elektroninėje erdvėje. Palyginti su 2008 m. III ketvirčiu (105 pranešimai), incidentų skaičius išaugo 4 080 proc. – beveik keturiasdešimt dviem kartais. Palyginti su 2009 m. II ketvirčiu, incidentų skaičius išaugo 13 proc.

Daugiausia pranešimų (4 276 pranešimai) užregistruota apie kenkėjišką programinę įrangą. Didžiąją dalį pranešimų sudarė pranešimai apie kirminą *Win32/Conflicker/Downadup*, kuris veikdamas gali perimti kompiuterio valdymą ir įtraukti jį į *botnet* tinklą, t. y., pasitelkus kenkėjišką programinę įrangą, valdomų kompiuterių tinklas dažnai panaudojamas kaip priemonė kitoms saugumo atakoms vykdyti. CERT-LT registruoja ir tinklalapyje www.esaugumas.lt skelbia informaciją apie *botnet* tinkluose aptiktų kompiuterių aktyvumą.

Dalyvaudamas projekte „Draugiškas internetas" (www.draugiskasinternetas.lt), CERT-LT per 2009 metų III ketvirtį gavo ir išnagrinėjo 76 pranešimus apie neteisėtą turinį internete. CERT-LT nustatė 18 atvejų, kuomet buvo pažeisti Lietuvos įstatymai dėl nelegalaus turinio internete (pornografijos, pedofilijos, rasizmo), o visa surinkta medžiaga buvo perduota atsakingoms institucijoms tolimesniam tyrimui.

Šį ketvirtį išaugo užvaldymo incidentų skaičius. CERT-LT užregistravo 15 incidentų – tai 200 proc. daugiau nei 2009 metų II ketvirtį (5 incidentai). Piktavaliai, „nulaužę" internetinę svetainę ar kitaip gavę prieigą prie jos su administratoriaus teisėmis (dažniausiai pavogę administratoriaus prisijungimo duomenis), įterpdavo kenkėjišką programinį kodą joje. Interneto naudotojas, aplankęs tokią internetinę svetainę, būdavo bandomas apkrėsti kenkėjišku programiniu kodu, pasinaudojant vartotojo naudojamų programų saugumo spragomis. CERT- LT ir toliau pastebi šių incidentų augimo tendencijas.

Kitų incidentų skaičius šį ketvirtį: *Spam* – 16 incidentų (2009 m. II ketvirtį – 11); *DoS* atakų – 7 (2009 m. II ketvirtį – 7); klastojimo – 4 (2009 m. II ketvirtį – 15); manipuliacijos – 5 (2009 m. II ketvirtį – 1). Gautus pranešimus apie incidentus iš naudotojų ir teikėjų CERT-LT ištyrė ir pateikė rekomendacijas, kaip pašalinti incidentų pasekmes ar sustabdyti jų plitimą.

CERT-LT 16 kartų konsultavo fizinius ir juridinius asmenis tinklų ir informacijos saugumo klausimais.

Pastebimas didėjantis elektroninių ryšių tinklų ir informacijos saugumo incidentų aktyvumas, todėl CERT-LT nori atkreipti į tai visų dėmesį ir rekomenduoja įsidiegti apsaugos programas, reguliariai atnaujinti jas, taip pat atnaujinti operacines sistemas bei kitas naudojamas programas, atsisiunčiant naujausius programų atnaujinimus iš oficialaus gamintojo tinklalapio.

Užfiksuotų incidentų pasiskirstymas pagal tipus:

Incidentų tipas (sutrumpinimas)	Incidentų tipo paaiškinimas	Incidentų skaičius 2009 m. III ketv.	Incidentų Skaičius 2009 m. III ketv. (proc.)
Virusai	**Kenkėjiška programinė įranga** (angl. *Virus, Worm)* – programinė įranga ar jos dalis, specialiai sukurta neteisėtai prisijungti ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos ar elektroninių ryšių tinklo, sutrikdyti ar pakeisti (taip pat perimti valdymą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip panaudoti	**4 276**	**97,43**

	neviešus elektroninius duomenis tokios teisės neturintiems asmenims.		
Spam	**Nepageidaujamas elektroninis paštas** (angl. *spam*) – elektroninio pašto laiškų tiesioginės rinkodaros tikslais siuntimas be elektroninio pašto naudotojo ir (ar) abonento išankstinio sutikimo, galintis turėti neigiamos įtakos elektroninio pašto informacinių sistemų funkcionalumui Lietuvos Respublikoje.	**16**	**0,36**
DoS	**Elektroninės paslaugos trikdymo ataka** (angl. *DoS*) – tai veiksmas, kuriuo siekiama sutrikdyti elektroninių ryšių tinklo ir (ar) informacinės sistemos darbą arba elektroninių ryšių tinklu teikiamas paslaugas.	**7**	**0,16**
Neteisėtas turinys	**Neteisėtas turinys** – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus.	**18**	**0,41**
Užvaldymas	**Neleidžiamasis naudojimasis informacinės sistemos ištekliais** (angl. *Web Site Defacement*) – neteisėtas informacinės sistemos išteklių naudojimas. ir **Neleidžiamasis prisijungimas** (angl. *System Compromise/Intrusion*) – neteisėtas prisijungimas prie informacinės sistemos ar elektroninių ryšių tinklo.	**15**	**0,34**
Klastojimas	**Elektroninių duomenų klastojimas** (angl. *Phishing*) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.	**4**	**0,09**

Manipuliacija	**Manipuliacija elektroniniais duomenimis** (angl. *Spyware*) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.	**5**	**0,11**
Kiti		**48 (16 konsultacijų)**	**1.09**