CERT-LT apibendrina I ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2009 m. I ketvirčio veiklos rezultatus.

CERT-LT per 2009 metų I ketvirtį ištyrė 1029 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. I ketvirčiu (105 pranešimai), incidentų skaičius išaugo 880 proc. – beveik dešimt kartų.

Daugiausia pranešimų (921 pranešimas) užregistruota apie kenkėjišką programinę įrangą. Šį didelį skaičių įtakojo visame pasaulyje išplitęs kirminas *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. Glaudžiai bendradarbiaujant su tarptautiniais partneriais, gaunama vis daugiau pranešimų apie Lietuvoje plintančius kompiuterinius zombius, dalyvaujančius *botnet* tinklo veikloje. CERT-LT ir toliau registruoja ir skelbia informaciją apie *botnet*“ tinkluose aptiktų kompiuterių aktyvumą.

Dalyvaudamas projekte „Draugiškas internetas” (www.draugiškasinternetas.lt), CERT-LT per 2009 metų I ketvirtį priėmė ir išnagrinėjo 143 pranešimus apie neteisėtą turinį internete. 20 atvejų CERT-LT identifikavo, kad buvo pažeisti Lietuvos įstatymai dėl nelegalaus turinio internete (pornografijos, pedofilijos, rasizmo), o visa surinkta medžiaga buvo perduota atsakingoms institucijoms tolimesniam tyrimui.

Kitų incidentų skaičius šį ketvirtį išaugo daugiau nei dvigubai: *Spam* – 24 incidentai (2008 m. IV ketvirtį – 9); *DoS* atakos – 20 (2008 m. IV ketvirtį – 11); užvaldymas – 17 (2008 m. IV ketvirtį – 5); klastojimas – 12 (2008 m. IV ketvirtį – 1); manipuliacija – 4 incidentai. Gautus pranešimus apie incidentus iš naudotojų ir teikėjų CERT-LT ištyrė ir pateikė rekomendacijas, kaip pašalinti incidentų pasekmes ar sustabdyti jų plitimą.

Pastebimas elektroninių ryšių tinklų ir informacijos saugumo incidentų padidėjęs aktyvumas, todėl CERT-LT nori atkreipti į tai jūsų dėmesį ir rekomenduoja įsidiegti apsaugos programas ir 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. I ketv.
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 (įskaitant perimti valdymą) informacinės sistemos ar elektroninių ryšių tinklo veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninius duomenis, panaikinti ar apriboti galimybę naudotis elektroniniais	**921**

	duomenimis, sudaryti sąlygas neteisėtai pasisavinti ar kitaip panaudoti 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.	**24**
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.	**20**
Neteisėtas turinys	**Neteisėtas turinys** – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus.	**20**
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.	**17**
Klastojimas	**Elektroninių duomenų klastojimas** (angl. *Phishing*) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.	**12**
Manipuliacija	**Manipuliacija elektroniniais duomenimis** (angl. *Spyware*) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.	**4**
Kita		**12**