CERT-LT apibendrina IV ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2009 m. IV ketvirčio veiklos rezultatus. CERT-LT per 2009 metų IV ketvirtį tyrė 3276 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. IV ketvirčiu (41 pranešimas), užregistruotų panešimų apie incidentus skaičius išaugo 7 890 proc. – aštuoniasdešimt kartų. Palyginti su 2009 m. III ketvirčiu, pranešimų apie incidentus skaičius sumažėjo 25 proc.

Daugiausia pranešimų (2 975 pranešimų) 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 skelbia informaciją apie *botnet* tinkluose aptiktų kompiuterių aktyvumą tinklalapyje www.esaugumas.lt.

Dalyvaujant projekte „Draugiškas internetas” (www.draugiškasinternetas.lt) CERT-LT per 2009 metų IV ketvirtį priėmė ir išnagrinėjo 96 pranešimus apie nelegalų turinį internete. 14 atveju CERT-LT pagal suderintus kriterijus identifikavo, kad galimai buvo pažeisti Lietuvos įstatymai dėl nelegalaus turinio internete. Visa surinkta medžiaga buvo perduota atsakingom institucijom tolimesniam tyrimui.

Šį ketvirtį taip pat augo pranešimų apie užvaldymo incidentus skaičius. CERT-LT užregistravo 141 pranešimą – tai 840 proc. daugiau nei 2009 metų III ketvirtį (15 pranešimų). Didžiąją šių pranešimų dalį sudarė neteisėtas prisijungimas prie internetinių svetainių naudojant vogtus arba specialiomis programomis parinktus administratoriaus slaptažodžius. Dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėms, pasitelkiant botnet resursus. Kitaip, nei ankstesniais metais, dauguma atveju užvaldytos svetainės vizualiai nebuvo keičiamos, o įterpiamas į ją kenkėjiškas kodas.. CERT- LT ir toliau stebi šių incidentų augimo tendencijas.

Kitų pranešimų apie incidentų skaičius šį ketvirtį : *Spam* – 78 pranešimai (2009 m. III ketvirtį – 16); *DoS* atakų – 7 (2009 m. III ketvirtį – 7); klastojimo – 6 (2009 m. III ketvirtį – 4); manipuliacijos – 6 (2009 m. III ketvirtį – 5). Gautus pranešimus apie incidentus iš naudotojų ir teikėjų CERT-LT ištyrė ir pateikė rekomendacijas, kaip pašalinti incidentų pasekmes ar sustabdyti jų plitimą.

CERT-LT 32 kartų konsultavo fizinius ir juridinius asmenis, tinklų ir informacijos saugumo klausimais.

Gautų pranešimų apie incidentus 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 neviešus elektroninius duomenis tokios teisės neturintiems asmenims.	**2 975**	**90,08**
Spam	**Nepageidaujamas elektroninis paštas** (angl. *spam*) – elektroninio pašto laiškų tiesioginės rinkodaros	**78**	**2,4**

	tikslais siuntimas be elektroninio pašto naudotojo ir (ar) abonento išankstinio sutikimo, galintis turėti neigiamos įtakos elektroninio pašto informacinių sistemų funkcionalumui Lietuvos Respublikoje.		
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**	**0,2**
Neteisėtas turinys	**Neteisėtas turinys** – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus.	**14**	**0,4**
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.	**141**	**4,3**
Klastojimas	**Elektroninių duomenų klastojimas** (angl. *Phishing*) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.	**6**	**0,2**
Manipuliacija	**Manipuliacija elektroniniais duomenimis** (angl. *Spyware*) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.	**6**	**0,2**

Kiti		**49 (32 konsultacijų)**	**1.5**