CERT-LT apibendrina I ketvirčio veiklą

Lietuvos Respublikos nacionalinis elektroninių ryšių tinklų ir informacijos saugumo incidentų tyrimo padalinys CERT-LT apibendrina 2010 m. I ketvirčio veiklos rezultatus. CERT-LT per 2010 metų I ketvirtį tyrė 2 313 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 2009 m. I ketvirčiu (1 029 pranešimai), tirtų pranešimų skaičius išaugo daugiau nei dviem kartais. Palyginti su 2009 m. IV ketvirčiu, tirtų pranešimų apie incidentus skaičius sumažėjo 29 proc.

Daugiausia ištirta pranešimų (1 982 pranešimai) apie kenkėjišką programinę įrangą. Didžiąją dalį šių pranešimų sudarė incidentai dėl „kirmino“ *Win32/Conflicker/Downadup*, kuris ypač sparčiai plito 2009 metų pradžioje. „Kirminas“ 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 nuolat registruoja ir tinklalapyje www.esaugumas.lt skelbia informaciją apie *botnet* tinkluose aptiktų kompiuterių aktyvumą.

Dalyvaudamas projekte „Draugiškas internetas“ (www.draugiskasinternetas.lt) CERT-LT 2010 metų I ketvirtį priėmė ir išnagrinėjo 126 pranešimus apie nelegalų ir žalingą turinį internete. CERT-LT pagal suderintus kriterijus identifikavo 11 (21 proc. mažiau nei 2009 m. IV ketvirtį) atvejų, kuriais galbūt buvo pažeisti Lietuvos įstatymai dėl nelegalaus turinio internete. Su šiais atvejais susijusi sukaupta medžiaga ir duomenys buvo perduoti atsakingoms institucijoms tolimesniam tyrimui.

Šį ketvirtį, kaip ir praėjusių metų ketvirčiais, itin padidėjo pranešimų apie kompiuterių užvaldymo incidentus skaičius: CERT-LT ištyrė 261 pranešimą – tai 45 proc. daugiau nei per visus 2009 metus (180 pranešimų). Didžiąją šių tirtų pranešimų dalį sudarė pranešimai apie neteisėtus prisijungimus prie internetinių svetainių naudojant vogtus arba specialiomis programomis parinktus administratoriaus slaptažodžius. Dauguma aptiktų užvaldymo atvejų buvo atlikti automatizuotomis priemonėms, pasitelkiant *botnet* resursus. CERT-LT ir toliau stebi šių incidentų augimo tendencijas.

CERT-LT šį ketvirtį gavo 185 pranešimus apie nepageidaujamus elektroninio pašto pranešimus (angl. *spam*). Šių pranešimų išsamesnis tyrimas buvo perduotas *spam* atvejus nagrinėjančioms kompetentingoms institucijoms, nes juose nebuvo aptikta saugumo pažeidimų, kurie galėtų turėti neigiamos įtakos elektroninio pašto informacinių sistemų funkcionalumui Lietuvos Respublikoje.

Be aukščiau minėtų, buvo tirti pranešimai apie šiuos incidentų tipus: dėl *DoS* atakų – 7 (2009 m. IV ketvirtį – 7); dėl klastojimo – 8 (2009 m. IV ketvirtį – 6); dėl manipuliacijos – 9 (2009 m. IV ketvirtį – 6). CERT-LT ištyrė visus iš naudotojų ir teikėjų gautus pranešimus apie incidentus bei pateikė rekomendacijas, kaip pašalinti incidentų pasekmes ar sustabdyti jų plitimą.

CERT-LT 20 kartų konsultavo fizinius ir juridinius asmenis tinklų ir informacijos saugumo klausimais.

Tirtų pranešimų apie incidentus pasiskirstymas pagal tipus:

Incidentų tipas (sutrumpinimas)	Incidentų tipo paaiškinimas	Incidentų skaičius 2010 m. I ketv.	Incidentų Skaičius 2010 m. I 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	**1 982**	**86,4**

	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.	**0** (gauta185 pranešimai apie pavienį nepageidaujamą elektroninį paštą)	**0**
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**	**0,3**
Neteisėtas turinys	**Neteisėtas turinys** – elektroniniai duomenys, kurių skelbimas ir (ar) platinimas yra draudžiamas pagal Lietuvos Respublikos įstatymus.	**11**	**0,5**
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.	**261**	**11,4**
Klastojimas	**Elektroninių duomenų klastojimas** (angl. *Phishing*) – sąmoningas elektroninių duomenų iškraipymas ar pakeitimas netikrais elektroniniais duomenimis.	**8**	**0,3**
Manipuliacija	**Manipuliacija elektroniniais**	**9**	**0,4**

	duomenimis (angl. *Spyware*) – elektroninių duomenų pasisavinimas, platinimas, paskelbimas ar kitoks neteisėtas jų panaudojimas.		
Kiti		**15**	**0,7**