Informatīvais ziņojums
„Par Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas (CERT.LV) darba rezultātiem tās darbības pirmajos trīs mēnešos"

Saskaņā ar Informācijas tehnoloģiju drošības likuma (turpmāka – likums) 4.panta pirmo daļu Informācijas tehnoloģiju drošības incidentu novēršanas institūcija (CERT.LV) (turpmāk – CERT.LV) veicina informācijas tehnoloģiju drošību Latvijas Republikā. CERT.LV darbības uzdevumi un tiesības ir deleģētas Latvijas Universitātes aģentūrai „Latvijas Universitātes Matemātikas un informātikas institūts" (turpmāk tekstā – aģentūra), kas šos uzdevumus izpilda un tiesības īsteno Satiksmes ministrijas pakļautībā atbilstoši piešķirtajiem valsts budžeta līdzekļiem un deleģēšanas līguma noteikumiem. Saskaņā ar likuma 4.panta pirmo daļu Satiksmes ministrija 2011.gada 26.janvārī noslēdza deleģēšanas līgumu ar aģentūru, paredzot CERT.LV darbības nodrošināšanai 2011.gada 11 mēnešos finansējumu 87 991 latu apmērā, kā arī nododot aģentūras lietošanā ministrijas valdījumā esošo kustamo mantu (mēbeles, datortehnika, sakaru līdzekļi un cita veida kustamā manta).

Lai īstenotu likumā CERT.LV noteiktos pienākumus, aģentūrā ir tikusi izveidota jauna laboratorija, kurā pastāvīgi ir nodarbinātas desmit personas (divas uz pilnu darba slodzi, bet astoņas – uz nepilnu darba slodzi), ir izveidota klasificētās informācijas aizsardzības sistēma, izveidota CERT.LV tīmekļa vietne (http://www.cert.lv un http://www.cert.gov.lv), izstrādāts CERT.LV logotips, kā arī veikti citi administratīva rakstura pasākumi veiksmīgai likumā noteikto pienākumu izpildei un tiesību īstenošanai.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums un sniegtais atbalsts informācijas tehnoloģiju drošības incidentu novēršanā

Laika periodā no 2011.gada 1.februāra līdz 30.aprīlim (turpmāk – pārskata periods) CERT.LV ir apkopojusi informāciju par inficētajām interneta protokola (turpmāk – IP) adresēm Latvijas IP adrešu apgabalos, kā arī tos reģistrējusi CERT.LV incidentu apstrādes datu bāzē tālākai risināšanai. Pārskata perioda beigās identificēti ir aptuveni 4500 datoru un lielākā daļa no tiem ir padarīti par dažādu robottīklu sastāvdaļām.

Pārskata periodā CERT.LV ir reģistrējis un apstrādājis 3966 informācijas tehnoloģiju drošības incidentus (turpmāk tekstā – incidenti), kurus kopumā var iedalīt divās kategorijās: (1) bīstami incidenti, kas nenotiek bieži, bet kuru gadījumā ir jāreaģē nekavējoties un incidents pēc iespējas ātrāk ir jānovērš, piemēram, pikšķerēšana, robottīklu komandcentru un kontrolcentru darbība, dalītie pakalpojumu atteices uzbrukumi (turpmāk tekstā

– DDoS) uzbrukumi, neautorizētas piekļuves (ielaušanās) informācijas sistēmām; (2) mazāk bīstami incidenti, kas ir masveidīgi un ar kuriem jācīnās plānveidīgi un pastāvīgi, bet attiecībā uz kuriem nav nepieciešama nekavējoša reakcija, piemēram, kaitniecisku programmatūru inficēti datori, kas ir kļuvuši par robottīklu sastāvdaļu. Lielākā daļa no CERT.LV apstrādātajiem incidentiem pieder otrajai kategorijai un šādu incidentu gadījumos CERT.LV informēja elektronisko sakaru pakalpojumu sniedzēju, kurš nodrošināja attiecīgo elektronisko sakaru pakalpojumu, un nepieciešamības gadījumā sniedza konsultācijas incidentu novēršanai.

Konstatējot pirmās kategorijas incidentus, CERT.LV nekavējoties iesaistījās to novēršanā, sekojot līdzi to novēršanas gaitai un pārliecinoties par to novēršanu. Pārskata periodā CERT.LV sniedza atbalstu valsts institūcijām, pašvaldību institūcijām, kā arī privāto tiesību juridiskajām personām informācijas tehnoloģiju drošības incidentu novēršanā, tajā skaitā sniedzot atbalstu:

- valsts institūcijām un pašvaldības institūcijām, kuru informācijas sistēmās tika izplatīta kaitnieciska programmatūra;
- valsts institūcijai, kuras tīmekļa vietne bija sabojāta un tajā bija ievietota kaitīga informācija;
- pašvaldības institūcijai, kurai piederošai IP adresei notika DDoS uzbrukums, kura rezultātā attiecīgā servera darbība netika traucēta, bet tika pārslogots tā ārzemju sakaru kanāls;
- pašvaldības institūcijai, kuras tīmekļa vietnes saturs tika aizstāts ar tai neparedzētu saturu;
- komersantam, kura informācijas sistēmai notika vairākkārtēji neautorizētas piekļuves mēģinājumi;
- komersantam, no kura informācijas sistēmas tika veikta svešas identitātes zādzība;
- komersantam, kuram piederošam serverim notika neautorizēta piekļūšana, sabojājot aptuveni 300 uz tā izvietotas tīmekļa vietnes;
- komersantam, kura serverim un tīmekļa vietnei notika neautorizēta piekļuve kā rezultātā tīmekļa vietnes saturs tika aizstāts ar tai neparedzētu saturu.

2. Izglītojošie pasākumi, rekomendācijas sabiedrībai par aktuālo informācijas tehnoloģiju riskiem

CERT.LV tīmekļa vietnē (http://www.cert.lv un http://www.cert.gov.lv) regulāri ir tikusi publicēta informācija par aktuālajām informācijas tehnoloģiju ievainojamībām un kaitnieciskām programmatūrām, kā arī pastāvīgi ir tikusi papildināta sadaļa par biežāk uzdotajiem jautājumiem, sniedzot padomus rīcībai konkrētās situācijās. Bet, lai paplašinātu sabiedrībai iespējas saņemt

informāciju, sadarbībā ar Latvijas datoru drošības incidentu risināšanas komandu un ieinteresēto organizāciju sadarbības iniciatīvas grupu „LV-CSIRT" ir izveidots izglītošanas portālu „Esi drošs" (http://www.esidross.lv), kurā tiek publicēti raksti par informācijas tehnoloģiju drošību ikdienā.

2011.gada 5.aprīlī Rīgā CERT.LV organizēja semināru/apmācību personām, kuras saskaņā ar likumu īsteno informācijas tehnoloģiju drošības pārvaldību valsts un pašvaldību institūcijās, „Esi drošs – 1". Tajā piedalījās 108 personas no valsts institūcijām un pašvaldību institūcijām gan no Rīgas, gan no citām apdzīvotām vietām. 2011.gada 11.aprīlī šāds seminārs/apmācība sadarbībā ar Latvijas Pašvaldību savienību tika organizēta arī Kuldīgā un tajā piedalījās 15 pārstāvji no Kurzemes pašvaldību institūcijām.

CERT.LV pārstāvji ir piedalījušies dažādās publiskās diskusijās, kā arī snieguši atbildes uz masu mediju jautājumiem, bet 2011.gada 8.februārī piedalījās Vispasaules drošāka interneta dienas pasākumos. Šī un citu pasākumu laikā CERT.LV ir izplatījusi informācijas tehnoloģiju galalietotājus izglītojošus plakātus „Vai esi interneta profiņš?" un „Virtuālā realitāte".

CERT.LV kopā ar aģentūru un Latvijas Universitāti ir uzsākusi sadarbības projektu ar Visbijas universitāti Zviedrijā par divu informācijas tehnoloģiju drošības kursu izstrādi Latvijas Universitātes maģistratūras programmās.

3. Sadarbība ar valsts institūcijām, pašvaldību institūcijām un starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām (vienībām)

Pārskata periodā ir saņemta informācija par 168 valsts institūcijām un 152 pašvaldību institūcijām par to vadītāju nozīmētajām personām, kuras saskaņā ar likumu īsteno informācijas tehnoloģiju drošības pārvaldību attiecīgajās institūcijās. Saskaņā ar šā ziņojuma 1. un 2.nodaļā sniegto informāciju pastāvīgi ir ticis sniegts atbalsts valsts un pašvaldības institūcijām incidentu novēršanā, kā arī veikta to nodarbināto apmācība.

CERT.LV pārstāvji piedalījušies Ministru kabineta 2011.gada 26.aprīļa noteikumu Nr.327 „Noteikumi par elektronisko sakaru komersantu rīcības plānā ietveramo informāciju, šā plāna izpildes kontroli un kārtību, kādā galalietotājiem tiek īslaicīgi slēgta piekļuve elektronisko sakaru tīklam" izstrādē. Atbildot uz valsts institūciju izteiktajiem jautājumiem par informācijas tehnoloģiju drošības jautājumiem, ir sniegtas atbildes un rekomendācijas, tajā skaitā par informācijas šifrēšanu un drošu bezvadu tīklu izveidošanu un uzturēšanu.

Pārskata periodā ir notikusi aktīva sadarbība ar citu valstu informācijas tehnoloģiju drošības incidentu novēršanas institūcijām (vienībām), tajā skaitā ar citu valstu valdību/nacionālajām informācijas tehnoloģiju drošības

incidentu novēršanas institūcijām (vienībām), gan lūdzot palīdzību un informāciju Latvijā notikušu informācijas tehnoloģiju drošības incidentu novēršanā, kā arī sniedzot palīdzību citās valstīs notikušu incidentu novēršanā.

Satiksmes ministrs U.Augulis

Vīza: Valsts sekretārs A.Matīss

16.05.2011. 13:58
960
M.Andžāns
67028262, maris.andzans@sam.gov.lv