Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) paveikto 2012.gada 1.ceturksnī

(2012.gada 1.janvāris – 2012.gada 31.marts)

Pārskatam ir tikai informatīva nozīme
Pārskatā iekļauta tikai vispārpieejama informācija un tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju.

1. Uzdevums: **Uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu.**

2012.gada pirmajā darbības ceturksnī CERT.LV novēroja gan dažādus augstas bīstamības incidentus, gan arī lielu skaitu zemas prioritātes incidentu, kur datori bija inficēti ar dažādiem vīrusiem un bija kļuvuši par robotu tīklu (*botnet*) sastāvdaļām. Robotu tīkli joprojām ir visizplatītākā problēma ne tikai Latvijā, bet arī visā pasaulē. No augstas bīstamības incidentiem šajā ceturksnī īpaši jāatzīmē dažādu Latvijas serveru uzlaušana, servisu darbības traucēšana un pikšķerēšanas lapu izvietošana, kā arī uzbrukumi valsts un pašvaldību resursiem saistībā ar politiskām un sabiedriskām norisēm Latvijā, tajā skaitā politiski motivēti uzbrukumi, un ļaundabīgas programmatūras klātesamība dažādos tīklos.

2012.gadā CERT.LV ir sācis lietot jaunu incidentu uzskaites sistēmu un klasifikāciju. Ar klasifikāciju iespējams iepazīties CERT.LV mājas lapā:
http://www.cert.lv/section/show/90

Augstas prioritātes incidenti (pirmās sešas incidentu grupas, kā arī jebkurš incidents, kas skar augstas prioritātes institūcijas), tiek apstrādāti incidentu uzskaites un vadības sistēmā AIRT, pārējie incidenti tiek reģistrēti „AbuseHelper" sistēmā. Statistika šajā pārskatā tiek piedāvāta šīm abām incidentu grupām atsevišķi.

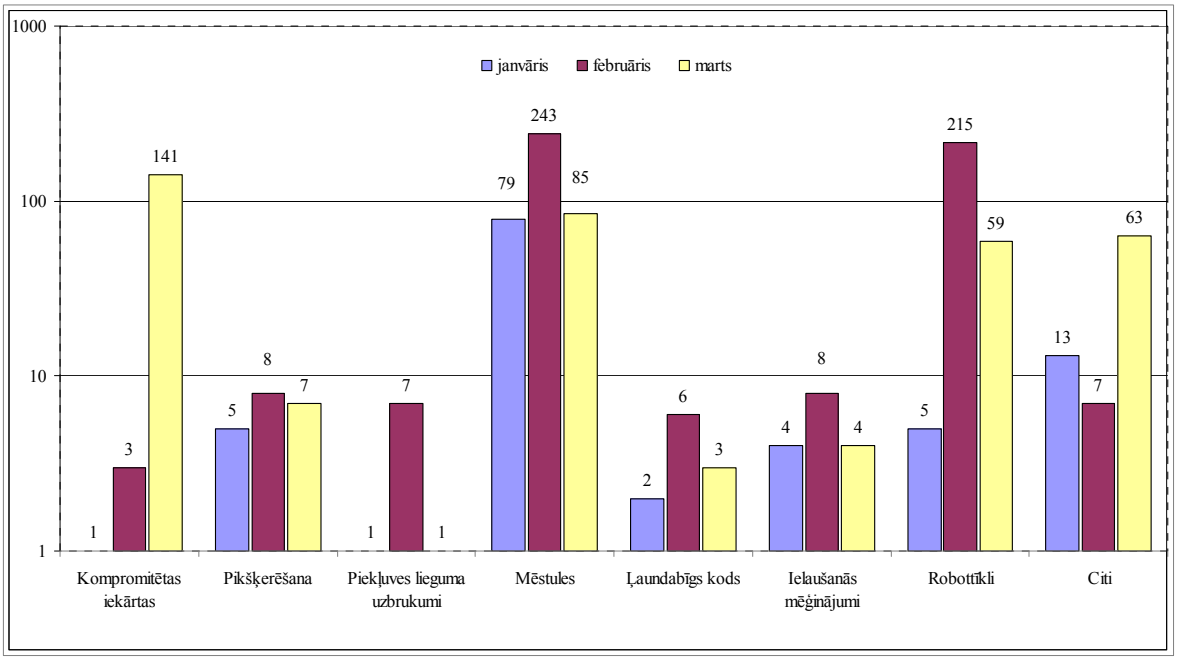
Katru mēnesi CERT.LV apkopo pēc rīcībā esošās informācijas vidējo inficēto IP adrešu skaitu Latvijā. Janvārī šis skaits ir bijis 3520, februārī – 3258, martā – 3072. Liela daļa no šiem datoriem ir dažādu robotu tīklu sastāvdaļas.

Lai samazinātu kopējo inficēto IP adrešu skaitu, CERT.LV turpina sarunas par sadarbību ar elektronisko sakaru komersantiem (ESK). Tikai ar ESK aktīvu līdzdalību ir iespējams mērķtiecīgi cīnīties ar inficētajiem datoriem un pakāpeniski samazināt to skaitu. 2011.gadā CERT.LV ir izveidojis sistēmu, kurā ESK var regulāri un automātiski saņemt informāciju par visām inficētajām IP adresēm no viņu rīcībā nodotajiem IP adrešu apgabaliem, 2012.gadā CERT.LV strādā pie šīs sistēmas pilnveidošanas. Pārskata perioda beigās regulārus ziņojumus par incidentiem saņem pieci ESK. Tuvākajā laikā CERT.LV plāno uzsākt aktīvu sadarbību arī ar citiem ESK.

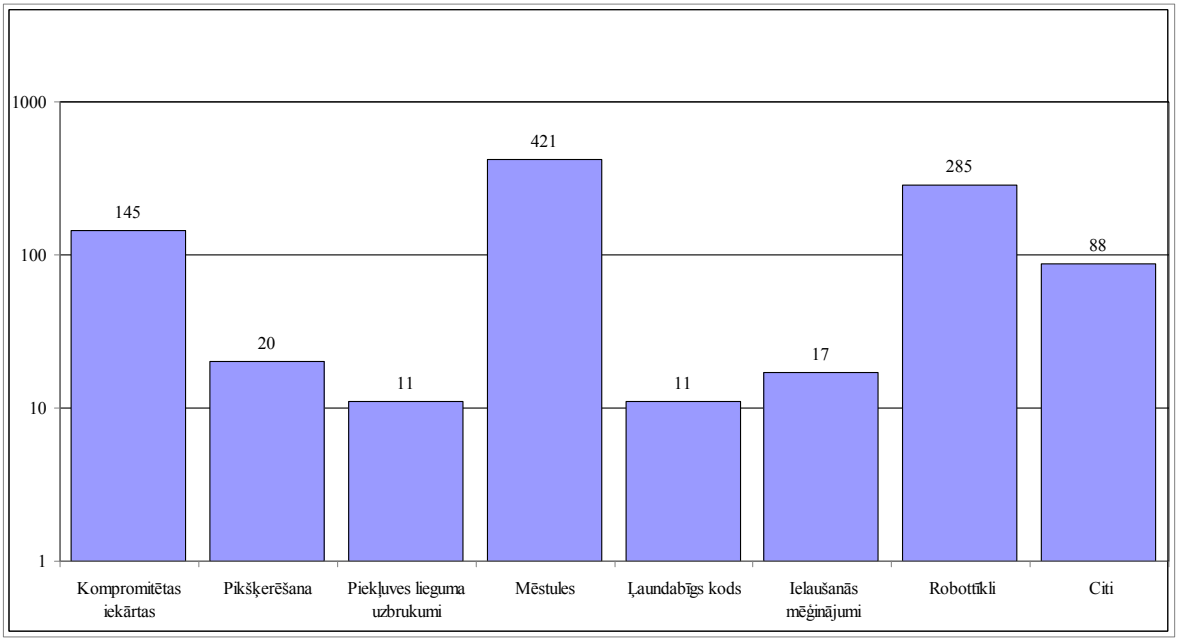
2. Uzdevums: **Sniegt atbalstu informācijas tehnoloģiju drošības incidenta novēršanā vai koordinēt to novēršanu.**

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis **998** augstas prioritātes incidentus un reģistrējis **48841** zemas prioritātes incidentus, par daļu no kuriem ESK ir informējis savus gala lietotājus.

1.diagrammā redzams augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem (diagrammas ir logaritmiskā mērogā). 2.diagrammā redzams augstas prioritātes incidentu kopskaits pārskata periodā.

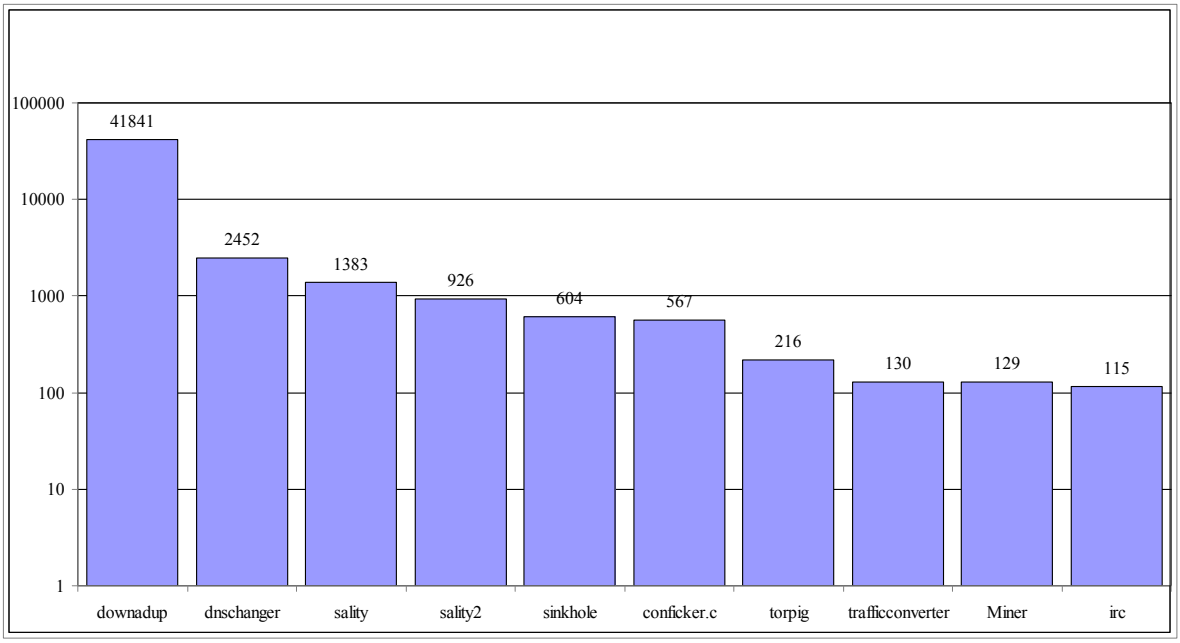


1.diagramma – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.



2.diagramma – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2012.gada 1.janvāra līdz 31.martam.

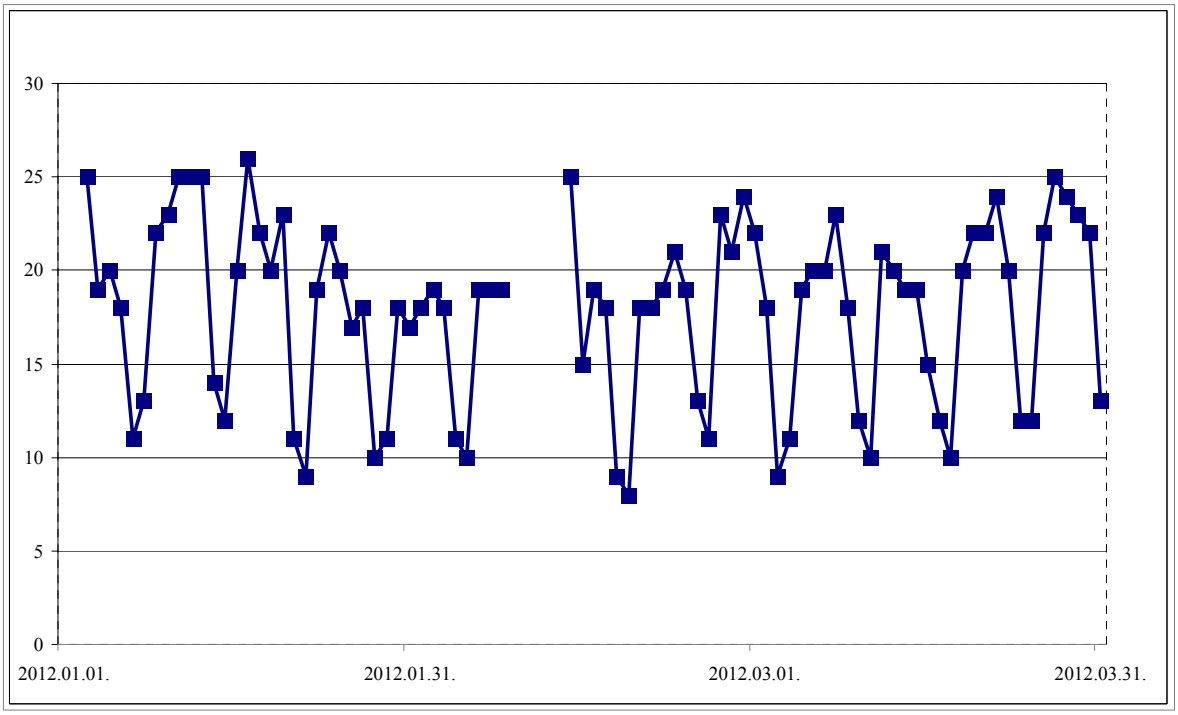
3.diagrammā redzami CERT.LV reģistrētie zemas prioritātes incidenti, to sadalījums pa infekciju tipiem – 10 populārākās infekcijas (kopā tiek apkopota informācija par 31 dažādu infekciju).



3.diagramma – CERT.LV reģistrētie zemas prioritātes incidenti – 10 populārākās infekcijas.

CERT.LV apkopo informāciju no valsts un pašvaldību institūcijām par to izmantotajām IP adresēm un tīmekļa vietnēm, lai CERT.LV varētu operatīvāk reaģēt šo institūciju IT drošības incidentu gadījumos.

4.diagrammā ir redzams, cik inficētu valsts un pašvaldību institūciju IP adreses bijušas katras dienas saņemtajos ziņojumos no dažādiem ziņošanas avotiem.



4.diagramma – Valsts un pašvaldību institūciju IP adrešu skaits, kas reģistrētas pārskata perioda incidentu ziņojumos.

Pārskata perioda laikā CERT.LV ir sadarbojies ar dažādām valsts un pašvaldību iestādēm, bankām, interneta pakalpojumu sniedzējiem, kā arī citām organizācijām konkrētu, dažādas bīstamības incidentu risināšanā. Zemāk aprakstīti daži incidentu piemēri anonimizētā veidā.

- Saņemta informācija par lietotāju piekļuves datu nozagšanu no kāda ārzemju interneta portāla, tajā skaitā arī informācija par vairākiem lietotājiem no Latvijas. Iesaistītie lietotāji tika brīdināti.
- Saņemta informācija par kļūdām valsts iestādes mājas lapā. Lapas uzturētājs brīdināts, kļūdas novērstas.
- Konstatēta pikšķerēšanas lapa, kas cenšas izkrāpt kādas interneta bankas lietotāju piekļuves datus. Krāpnieciskā lapa tika bloķēta. Perioda laikā tika risināti arī vairāki citi pikšķerēšanas incidenti.
- Saņemtas sūdzības par ļaundabīgās programmatūras glabāšanu vairākos komersantu serveros. Komersanti tika informēti un panākta kaitīgā satura izvākšana.
- Konstatēts DDoS uzbrukums pret viena komersanta serveri, CERT.LV konsultēja komersantu par iespējamajiem pretpasākumiem.
- Konstatēti uzbrukumi no robotu tīkliem, izmantojot „IP fragmentation attack". Visas iesaistītās robotu tīkla IP adreses tika identificētas un atbildīgās personas apziņotas.
- Tika saņemts lūgums novērst Dirt Jumper DDoS robotu tīkla kontroles centra darbību no Latvijā esošās IP adreses. CERT.LV sazinājās ar IP adreses lietotājiem, kaitīgās darbības tiek izbeigtas.
- CERT.LV konsultēja pašvaldības pārstāvi uzlauzta mājas lapu servera incidentā.
- Notika DOS uzbrukumi, kas bija vērsti pret vairāku valsts institūciju mājas lapām. Sadarbībā ar IPS un iestāžu atbildīgajam personām CERT.LV koordinēja šo uzbrukumu novēršanu, CERT.LV speciālisti palīdzēja atjaunot serveru darbību. Līdzīgi uzbrukumi notika arī pret citu sektoru mājas lapām.
- Tika konstatēti vairāki mājas lapu izķēmošanas gadījumi gan valsts iestādēm, gan komersantiem. CERT.LV sazinājās ar mājās lapu īpašniekiem un kopīgiem spēkiem risināja incidentus.
- Valsts iestāde pamanīja pret to veikto SQL injekciju uzbrukumu, CERT.LV iesaistījās incidenta novēršanā.
- CERT.LV saņēma incidenta pieteikumu no privātpersonas, kurā bija iesaistīti divi nelieli konkurējoši uzņēmēji. Viens no konflikta dalībniekiem ar IT uzbrukumu un spiegošanas programmatūras starpniecību mēģināja izrēķināties ar otru īpašnieku. CERT.LV iesaistījās incidenta izmeklēšanā.

3. Uzdevums: **Uzturēt sabiedrībai pieejamā veidā atbilstoši aktuālajiem apdraudējumiem izstrādātas rekomendācijas par aktuālo informācijas tehnoloģiju risku novēršanu.**

CERT.LV tīmekļa vietnē redzamā vietā regulāri tiek publicēta informācija par jaunākajām ievainojamībām un vīrusiem. Šī www.cert.lv lapas daļa joprojām ir visapmeklētākā. Pārskata perioda laikā tai ir bijuši kopā 5701 apmeklētāji. Kopā CERT.LV mājas lapai bijuši 7813 apmeklējumi, 5506 unikāli apmeklējumi no 66 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā aptuveni 90 % apmeklētāju bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicēts 21 jaunums, kā arī informācija par dažādiem pasākumiem, publikācijām un citiem notikumiem. Pārskata periodā CERT.LV mājas lapā publicēts dokuments ar incidentu kategorijām un prioritātēm, kā arī satura rādītāja

piemērs elektronisko sakaru komersantu rīcības plāna sagatavošanai. Pārskata periodā publicētas preses relīzes:

- „CERT.LV ieteikumi e-pasta drošībai";
- „CERT.LV aprit viens gads";
- „Pārbaudi sava datora veselību pie Datorologa!"
- „Kāda vīrieša datorā Datorologs uzgājis 110 vīrusus!"

CERT.LV ir „Twitter" konts un tajā tiek regulāri publicētas ziņas par dažādiem jaunumiem: http://twitter.com/certlv. Pārskata perioda laikā tajā ir publicētas 22 ziņas.

CERT.LV uztur arī pieaugušo izglītošanas portālu http://www.esidross.lv. Pārskata perioda laikā šajā portālā ir publicēti 12 jauni raksti, portālu apmeklējuši 9046 apmeklētāji. Publicētie raksti:

- Publicēti IT drošības materiāli institūcijām un uzņēmumiem;
- Drošības programmatūras mobilajām ierīcēm;
- Izveidota interaktīvi izglītojoša spēle par drošību internetā;
- Viltus drošības programmatūra;
- VIDEO: ENISA mudina sargāt savus datus;
- Kā atpazīt pikšķerēšanu?
- Kas jāzina, lai droši lietotu „draugiem.lv"?
- Kā pareizi lietot USB zibatmiņas disku?
- Organizē akciju par drošu interneta lietošanu datorā un telefonā;
- Latvijā jau gadu darbojas IT drošības sargi;
- Pārbaudi sava datora veselību pie Datorologa!
- Kāda vīrieša datorā Datorologs uzgājis 110 vīrusus!

4. Uzdevums: **Veikt pētniecisko darbu, organizēt izglītojošus pasākumus, apmācību un mācības informācijas tehnoloģiju drošības jomā.**

Pārskata perioda laikā CERT.LV organizēja divus „Netflow" tehniskos seminārus, piedalījās dažādās konferencēs un semināros, organizēja LV-CSIRT grupas sanāksmi, piedalījās „E-prasmju nedēļā" ar „Datorologa" akciju, kā arī sadarbojās ar dažādiem medijiem.

Sīkāka informācija par paveikto:

- „Informācijas drošības izpratnes programma" prezentēta Jēkabpilī, seminārā piedalījās 116 Jēkabpils pašvaldības administrācijas un institūciju darbinieki.
- „Informācijas drošības izpratnes programma" prezentēta Līvānos, seminārā piedalījās 237 Līvānu pašvaldības administrācijas un institūciju darbinieki.
- „Informācijas drošības izpratnes programma" prezentēta Lauku atbalsta dienesta struktūrvienībās Talsos un Saldū (Talsos piedalījās 56 dalībnieki, Saldū – 53).
- 3. un 10.februārī CERT.LV telpās notika „NetFlow" tehniskie semināri, kuros katrā piedalījās pa 26 dalībniekiem. Semināra ietvaros bija gan teorētiskā daļa par „NetFlow" un „NfSen" rīkiem, gan arī praktiskās nodarbības.
- 22.februārī CERT.LV piedalījās ar divām prezentācijām seminārā informātikas skolotājiem, kas notika Jelgavā un kur piedalījās skolotāji no Jelgavas un Dobeles novadiem. Seminārā piedalījās 37 dalībnieki.
- CERT.LV prezentēts Latvijas Universitātes konferencē, prezentācija „CERT.LV izaugsme un sasniegumi pirmajā darbības gadā".
- 6.februārī un 7.februārī CERT.LV pārstāvji piedalījās Latvijas Radio raidījumā „Kā labāk dzīvot", stāstīja par dažādiem IT drošības aspektiem, it īpaši krāpniecības mēģinājumiem.

- CERT.LV pārstāvja intervija 12.februāra raidījumam „De Facto" par kopējo IT drošības situāciju valstī.
- CERT.LV intervijā avīzei „Bizness & Baltija" par IT drošības jautājumiem.
- 14.martā CERT.LV pārstāvis uzstājās LETA organizētajā konferencē „Datu mākoņi".
- 13.martā CERT.LV organizēja LV-CSIRT grupas sanāksmi, kuras laikā notika tikšanās ar atzītu IT drošības speciālistu un Zemessardzes pārstāvjiem.
- 27.martā CERT.LV pārstāvis piedalījās "Eiropas kustība Latvijā„ organizētajā seminārā par Pilsoņu iniciatīvu un izklāstīja CERT.LV kompetenci šajā jomā.
- „E-prasmju nedēļas" ietvaros CERT.LV:
  - Uzstājās ar prezentāciju konferencē „e-Iespējas iedzīvotājiem";
  - Uzstājās ar prezentāciju konferencē „E-prasmes uzņēmējiem";
  - Piedāvāja „datorologa" akciju, kuras laikā jebkurš interesents varēja bezmaksas atnest savu datoru uz CERT.LV telpām, kur tika pārbaudīts, vai tas nav inficēts ar kādu vīrusu un, ja iespējams, „izārstēts". Akcijas laikā CERT.LV speciālisti pārbaudīja un „izārstēja" aptuveni 50 datorus.
  - „Datorologa" akcija tika reklamēta dažādos medijos – tika radīts kariķēts „Datorologa" tēls, kas kā vizuāls un informatīvs materiāls nonāca visos zemāk minētajos preses izdevumos. Tēla būtība ir „labsirdīgs, izpalīdzīgs speciālists, kurš „izārstēs" vīrusus jūsu datorā". Datorologa tēlā labi redzama arī CERT.LV identitāte.

Sīkāka informācija par „Datorologa" akciju:

- Paplašināts raksts par datoru drošību Eiropas Savienībā un Latvijā „Latvijas Avīzē" pielikumā „Tepat Eiropā" 23.martā., kā arī video sižets par „Datorologa" akciju www.la.lv;
- Sižets Latvijas Televīzijas ziņu raidījumā „Panorāma" 26.martā par iespēju atnāk pie „Datorologa";
- TV3 programmā „Bez Tabu" 22.martā sižets par datorvīrusu izplatību un uzaicinājums pie datorologa;
- Sižets LNT raidījumā „Tehnovīzija" 25.martā par vīrusu izplatību un iespēju pārbaudīt savu datoru pie „Datorologa" un www.esidross.lv;
- Sižets LTV7 ziņās 27.martā par „laimīgajiem „Datorologa" „izārstētajiem" datoriem un to īpašniekiem";
- Latvijas Radio 1 programmā „Pēcpusdiena" intervija ar Baibu Kaškinu par „Datorologa" kampaņu un e-prasmju nedēļu;
- Latvijas Radio 4 rīta ziņās intervija par „Datorologa pieņemšanu";
- www.diena.lv, www.tvnet.lv, www.next.lv, www.nozare.lv, www.leta.lv, www.bns.lv, www.pilseta24.lv, kā arī reģionālajos portālos raksti gan pirms, gan pēc „Datorologa" akcijas;
- Uzaicinājums uz „Datorologa" pasākumu tika izsūtīts arī sociālajos tīklos „Facebook" un „Twitter";
- Vairākas pārpublikācijas arī citos interneta portālos un pašvaldību mājas lapās;
- Publikācijas par Datorologu ārī www.esidross.lv, www.cert.lv un www.e-prasmes.lv lapās;
- Preses relīzes pirms un pēc pasākuma tika nosūtīta Latvijas nacionālā un reģionālā līmeņa televīzijām, radio, preses un interneta mediju redakcijām.

5. Uzdevums: **Sniegt atbalstu valsts institūcijām valsts drošības sargāšanā, kā arī noziedzīgu nodarījumu un citu likumpārkāpumu atklāšanā (izmeklēšanā) informācijas tehnoloģiju jomā, ievērojot normatīvajos aktos noteiktos datu apstrādes ierobežojumus.**

CERT.LV strādā pie sadarbības līguma saskaņošanas ar Valsts policiju. Pārskata periodā CERT.LV ir nodevis Valsts policijai informāciju par vairākiem IT drošības incidentiem, kā arī atbildējis uz vairākiem pieprasījumiem.

Pārskata perioda laikā CERT.LV ir ticies ar vairākām institūcijām, lai apspriestu sadarbības iespējas un dalītos pieredzē.

CERT.LV pārstāvis piedalās darba grupā „Informācijas sistēmas drošības pārvaldnieka profesijas standarts" izstrāde, grupu vada Vides un reģionālās attīstības ministrija.

CERT.LV pārstāvis piedalījās Nacionālās IT drošības padomes sēdē.

CERT.LV tikās ar Latvijas Informātikas skolotāju asociācijas pārstāvjiem un vienojās par vairākiem potenciālajiem sadarbības virzieniem, piemēram, specializēts seminārs, dalība Informātikas skolotāju konferencē, aicinājums skolām uzsākt tiešu sadarbību ar CERT.LV, u.c.

6. Uzdevums: **Uzraudzīt, kā valsts un pašvaldību institūcijas un elektronisko sakaru komersanti izpilda Informācijas tehnoloģiju drošības likumā noteiktos pienākumus.**

IT drošības likumā noteikts, ka valsts un pašvaldību institūcijām jāinformē CERT.LV par nozīmēto atbildīgo personu, kura iestādē īsteno informācijas tehnoloģiju drošības pārvaldību. Līdz 2012.gada 31.martam CERT.LV ir apkopojis informāciju par 484 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību, kā arī par institūciju tīkliem un mājas lapām.

CERT.LV regulāri informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā inficētas. Pārskata periodā CERT.LV ir bijusi informācija par 66 inficētām IP adresēm.

Pārskata periodā CERT.LV ir apziņojis ar vēstulēm organizācijas, lai gan pārbaudītu, kā notiek IT drošības likuma piemērošana, gan lai atgādinātu neizpildītos pienākumus.

IT drošības likums un ar to saistītie MK noteikumi 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" nosaka kārtību kādā Elektronisko sakaru komersantiem (ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai. CERT.LV ir izskatījusi visus saņemtos plānus un nosūtījusi atbildes elektronisko sakaru komersantiem.

7. Uzdevums: **Sadarboties ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām (vienībām).**

Visa perioda laikā ir notikusi aktīva sadarbība ar citu valstu informācijas tehnoloģiju drošības incidentu novēršanas vienībām, gan lūdzot palīdzību un informāciju par incidentiem, kas notiek Latvijā, gan palīdzot ar citās valstīs notikušu incidentu risināšanu.

CERT.LV pārstāvji pārskata periodā piedalījušies sekojošās konferencēs un semināros:

- 30.janvārī CERT.LV pārstāvis piedalās TF-CSIRT un FIRST sanāksmē un uzstājas ar prezentāciju „Spamhaus issues";

- 31.janvārī CERT.LV pārstāvis piedalās TF-CSIRT/FIRST simpozijā ar prezentāciju „Dealing with the whole country: creating a National CSIRT";
- 23-24.februārī CERT.LV pārstāvis piedalījās NATO organizētajā pasākumā – IT drošības mācību organizēšanas pirmajā konferencē, kā arī turpmāk aktīvi iesaistījās NATO mācību „Cyber Coalition 2012" organizēšanā;
- CERT.LV pārstāvis 12.martā piedalījās Eiropas pilsoņu iniciatīvas Ekspertu grupas sanāksmē, Eiropas Komisijā, Briselē;
- 5-6.martā CERT.LV pārstāvis piedalījās „AbuseHelper" seminārā Helsinkos, Somijā, kur uzstājās ar prezentāciju par „AbuseHelper" ieviešanu Latvijā;
- 26-28.martā CERT.LV pārstāvji piedalījās „sarkanajā komandā" NATO IT aizsardzības izcilības centra (CCDCoE) organizētajās tehniskajās IT drošības mācībās Igaunijā.

Starptautiskās sadarbības tēmas:
- CERT.LV pārstāvis piedalās FIRST konferences programkomitejā un iesniegto referātu izvērtēšanā.

8. Uzdevums: **Veikt citus normatīvajos aktos noteiktos pienākumus.**

- CERT.LV ir izstrādāta instrukcija "Kārtība, kādā tiek sertificēta ES Regulai Nr. 211/2011 "par pilsoņu iniciatīvu" atbilstoša vākšanas tiešsaistes sistēma" un formalizēta sistēma, kā veikt sertificēšanu, pēc grozījumu pieņemšanas un spēkā stāšanās likumā „Par tautas nobalsošanu un likumu ierosināšanu", ar kuru tiek ieviestas Eiropas Parlamenta un Padomes 2011.gada 16.februāra Regulas (ES) Nr.211/2011 par pilsoņu iniciatīvu (turpmāk – Regula) 6.panta, 8.panta un 15.panta prasības.
- CERT.LV ir uzsācis vairākus publiskos iepirkumus, lai varētu iegādāties aparatūru, kas nepieciešama turpmākajai darbībai.

Sagatavotājs – Baiba Kaškina
e-pasts: baiba.kaskina@cert.lv