Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) paveikto 2012.gada 2.ceturksnī

(2012.gada 1.aprīlis – 2012.gada 30.jūnijs)

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 otrajā darbības ceturksnī CERT.LV novēroja un apstrādāja 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 mērķēti uzbrukumi vairākām valsts institūcijām, kā arī robotu tīklu komand un kontrolserveri Latvijas IP adrešu apgabalā.

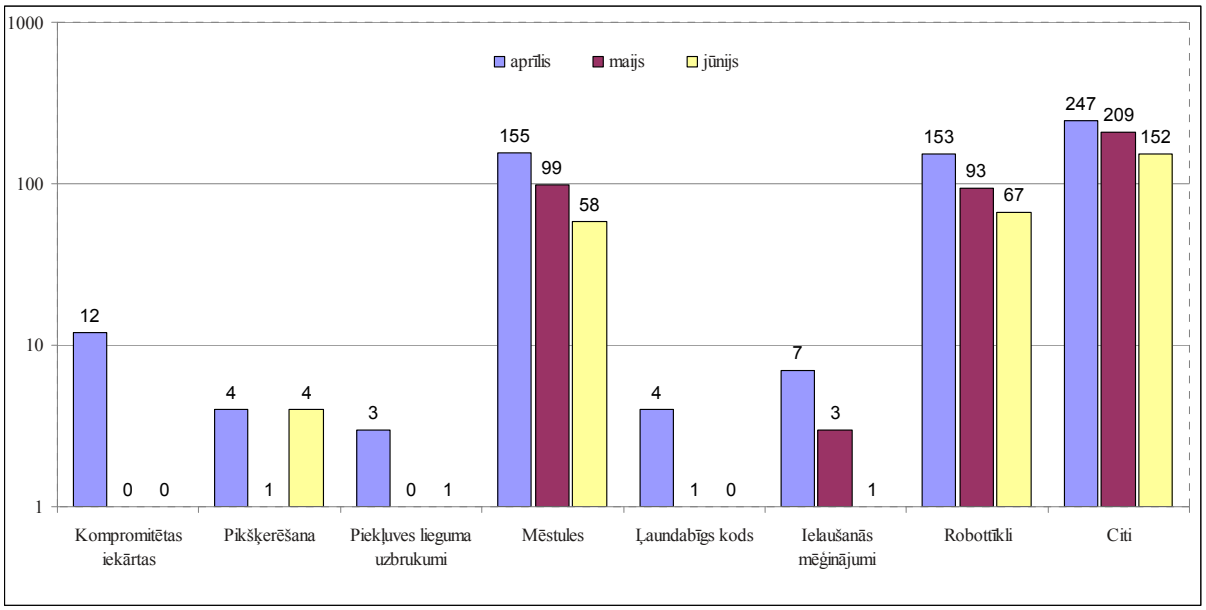
Katru mēnesi CERT.LV rēķina vidējo inficēto IP adrešu skaitu Latvijā. Aprīlī šis skaits ir bijis 3582, maijā – 2943, jūnijā – 2613. Liela daļa no šiem datoriem ir dažādu robotu tīklu sastāvdaļas.

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 un citas organizācijas 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 SIA „Lattelecom", SIA „IZZI", SIA „Telia Latvia", SIA „Ilva", AS "BALTICOM", SIA "Baltcom TV", SIA "Latvijas Mobilais Telefons", SIA „Interneta Pasaule", SIA "DAUTKOM TV", SIA "Stream Networks", SIA „LATNET Serviss" kā arī CSDD, LANET (Latvijas Universitāte) un Rīgas Tehniskā universitāte. Kopā datus saņem 14 IPS/organizācijas, bet ne visas no tām šos datus izmanto, lai informētu gala lietotājus un palīdzētu tiem risināt incidentu. CERT.LV turpina sarunas ar citiem ESK, lai arī tie pieņemtu no CERT.LV un apstrādātu informāciju par inficētajām IP adresēm.

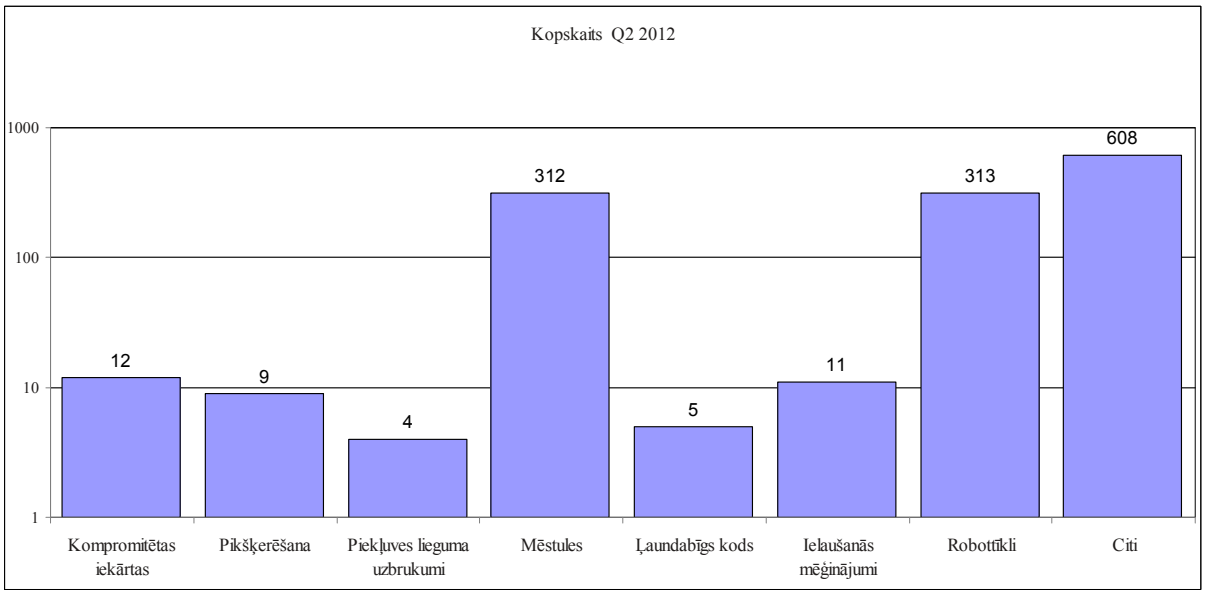
2. Uzdevums: **Sniegt atbalstu informācijas tehnoloģiju drošības incidenta novēršanā vai koordinēt to novēršanu.**

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis **1274** augstas prioritātes incidentus un reģistrējis **43489** 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.



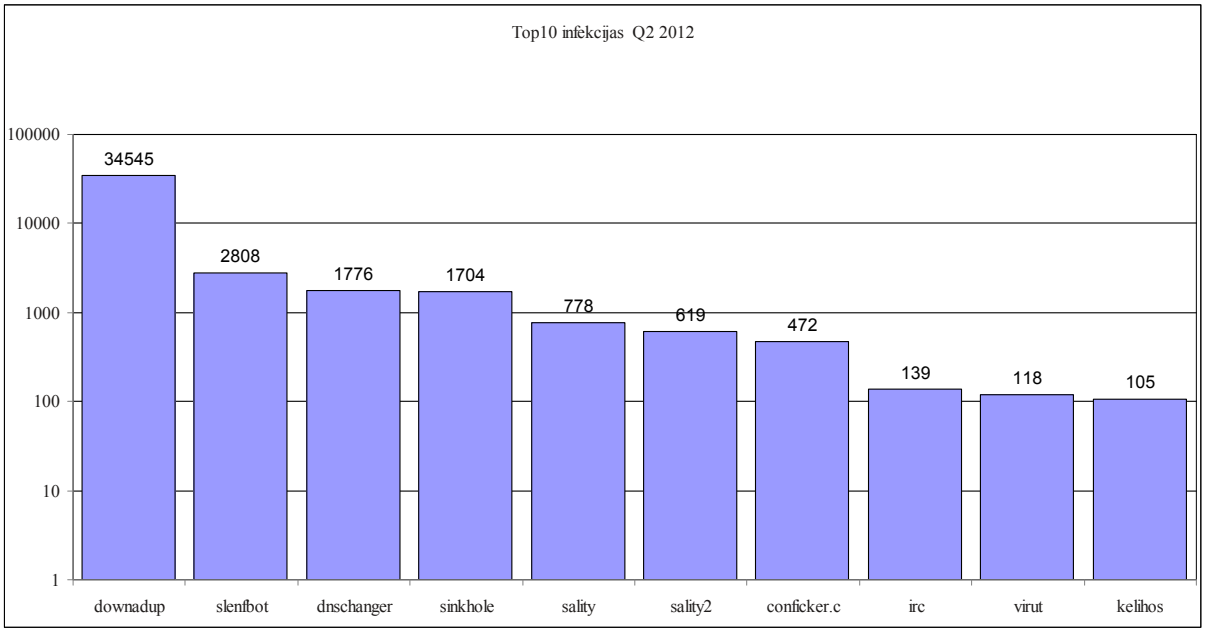
1.diagramma – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.



2.diagramma – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2012.gada 1.aprīļa līdz 30.jūnijam.

3.diagrammā redzami CERT.LV reģistrētie zemas prioritātes incidenti, to sadalījums pa infekciju tipiem – 10 populārākās infekcijas (kopā tiek apkopota informācija par 32 dažādu infekciju).

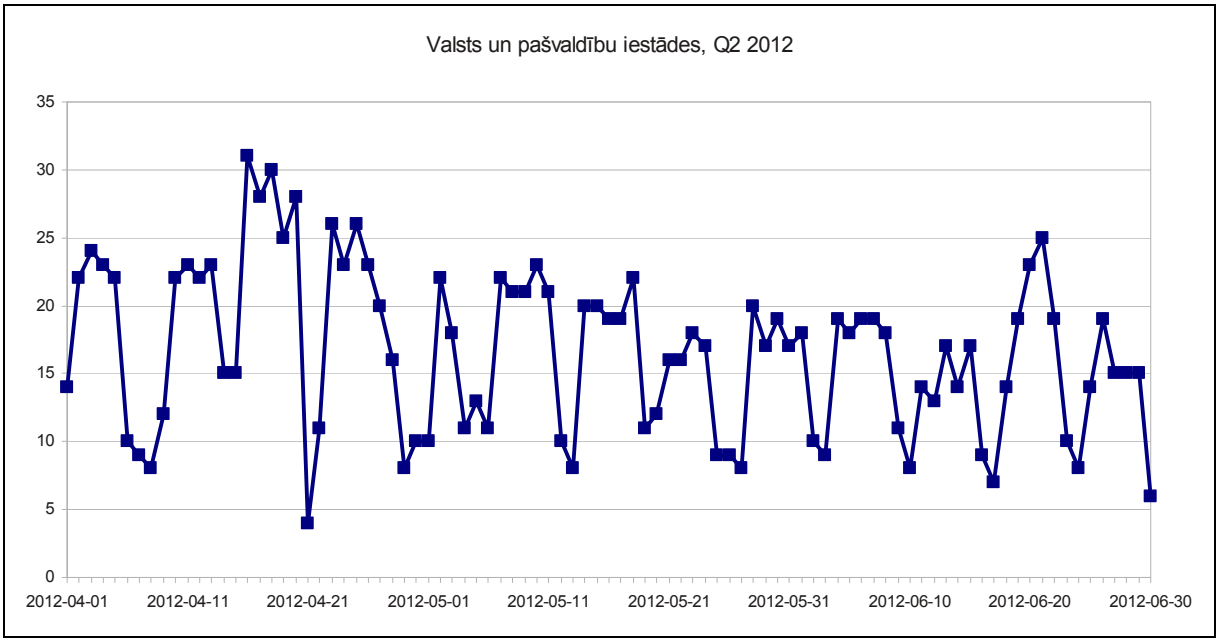
Pārskatam ir tikai informatīva nozīme.
Pārskatā iekļauta tikai vispārpieejama informācija un tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju.



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 iestāžu IT drošības incidentu gadījumos.

5.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.

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.

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.

- Tika konstatēts mēģinājums ielauzties vienas Ministrijas datoros, tika meklētas ievainojamas sistēmas šīs ministrijas publisko IP adrešu apgabalā. Uzbrukumi bija nesekmīgi, bet atkārtojas vēl vairākas reizes nākamajās dienās.
- Tika konstatēts datorvīruss kādas valsts iestādes tīklā. Pēc papildus palīdzības un informācijas saņemšanas iestāde atrada savā tīklā inficēto iekārtu - tīkla printeri.
- Lattelecom maršrutizētāju konfigurācijas kļūdas rezultātā LIX tīklā tika nodota pilna Lattelecom iekšējā maršrutizācijas tabula, kas pārpildīja LIX maršrutizētāja atmiņu, radot problēmas LIX darbībā. Tās tika novērstas dažu stundu laikā.
- Tika saņemts ziņojums par draudiem uzlauzt konkrētu mājas lapu. Lapas īpašniekam tika sniegti ieteikumi kā uzlabot servera drošību.
- Notika uzbrukuma mēģinājums kādas Ministrijas resursiem. (Uzbrukuma vektors - *SQL_Injection, HTTP_POST_FileName WinIni)
- Tika konstatēts kaitīga koda izplatīšanas mēģinājumus caur www.delf.lv lapu. Pēc CERT.LV izteiktā brīdinājuma lapas īpašnieks kaitīgo kodu noņēma. Gadījums tika uzskatīts par ļaunprātīgu mēģinājumu izplatīt datorvīrusus. Tuvākajās dienās tika sagatavota un publicēta publiska informācija, kurā datorlietotāji tiek brīdināti par "typosquatteru" aktivitātēm.
- Notika masveida izķēmošanas uzbrukums kādam mājas lapu glabāšanas pakalpojumu sniedzējam. Uzbrukums tika veikts caur CMS Wordpress ievainojamību.
- Pārskata periodā vairākas reizes tika novēroti pikšķerēšanas uzbrukumi, kuru mērķauditorija bija vairāku Latvijas komercbankas klienti.
- CERT.LV ziņoja par kādas bankas tīklā esošu datoru, kurš tika identificēts kā robotu tīkla sastāvdaļa. Visticamāk inficētais dators bija kāda no darbstacijām. Bankas pārstāvji nekavējoties situāciju atrisināja.
- CERT.LV maijā identificēja vairākus masveida mājas lapu izķēmošanu (*mass deface*). Uzbrucēji ieguva kontroli pār pakalpojumu sniedzēja serveri, uz kura tiek uzturētas vairākas mājas lapas. Servera programmatūras nepilnību dēļ uzbrucējiem izdevās iegūt administratora tiesības, tādā veidā radot iespēju izķēmot jebkuru mājas lapu, kas tika uzturēta uz kompromitētā servera.
- CERT.LV saņēma ziņojumu, ka no kompromitēta kādas augstskolas e-pasta konta tiek sūtītas mēstules. Konta piekļuves dati tika nomainīti, mēstuļu izsūtīšana tika veikta no Nigērijas IP adreses.
- CERT.LV saņēma incidenta pieteikumu par iespējamu DNS atbilžu viltošanas uzbrukumu. Identificētais pirmā līmeņa domēna vārds adobe.com atgrieza DNS atbildēs privātā tīkla IP adreses 10.129.34.*. Veicot incidenta analīzi, CERT.LV konstatēja, ka identificētā anomālija nav uzbrukums, bet gan cilvēka izraisīta kļūda adobe.com administrācijā. CERT.LV sazinājās ar adobe.com IT drošības nodaļu, kur guva apstiprinājumu, ka tā ir bijusi cilvēka izraisīta kļūme.
- CERT.LV identificēja inficētu datoru, kas darbojas kā robotu tīkla sastāvdaļa kādā pašvaldībā. CERT.LV sazinājās ar pašvaldību un incidents tika novērsts.
- CERT.LV saņēma incidenta ziņojumu par DDoS uzbrukumu kāda datu centra klientam. Veicot tehnisku analīzi, tika izdarīti secinājumi, ka uzbrukums, kas sākotnēji izskatījās pēc DDoS uzbrukuma, tomēr ir specifiski izveidots, viltojot IP pakešu

saturu, un patiesībā ir veikts no vienas uzbrūkošās mašīnas. Šāds uzbrukuma veids ir identificēts vairāk kārt un ir pamats sākt to uzskatīt par tendenci.

- Notika apjomīgs DDoS uzbrukums kādai Latvijas komercbankas mājas lapai. Uzbrukums tiek veikts no 7460 unikālam IP adresēm, izmantojot rekursīvos DNS serverus. Lielākā daļa no uzbrukumā iesaistītajiem datoriem atrodas ASV (3012), Krievijā (1032), Lielbritānijā (952) un Vācijā (785). CERT.LV sazinājās ar CSIRT vienībām, kuru tīklos atradās uzbrukumos iesaistītas IP adreses, un brīdināja par šo datoru izmantošanu DDoS uzbrukumam.
- CERT.LV no publiski pieejama materiāla uzzināja, ka īsi pirms Baltijas praida it kā tika uzlauztas mājas lapas www.mozaika.lv un www.balticpride.eu. Veicot incidenta izpēti CERT.LV neguva pārliecību, ka incidents tiešām noticis.
- CERT.LV saņēma palīdzības lūgumu no kādas pašvaldības IT administratora, caur kura serveri masveidā tika izsūtītas mēstules. CERT.LV sniedza padomus, kādas izmaiņas servera konfigurācijā nepieciešamas, lai šādus gadījumus nepieļautu, un palīdzēja izņemt serveri no starptautiskajiem "melnajiem sarakstiem", kur tas bija iekļauts par mēstuļu sūtīšanu.
- CERT.LV palīdzēja kādam zinātniskam institūtam atrast un novērst ievainojamības, caur kurām tika izķēmota viņu mājas lapa.
- CERT.LV no publiski pieejama materiāla uzzināja, ka esot uzlauzts portāls manabalss.lv. Veicot incidenta izpēti CERT.LV neguva pārliecību, ka incidents tiešām noticis.
- Tika konstatēts mērķēts uzbrukums kādai ministrijai, izmantojot e-pasta dokumentam pievienotu ļaundabīgu kodu. Sadarbojoties ar ministrijas darbiniekiem tika konstatēts, ka ļaundabīgā programmatūra nav inficējusi datorsistēmas un CERT.LV deva norādījumus par veicamajiem drošības pasākumiem, lai ierobežotu mērķētā uzbrukuma iespējamu izplatīšanos. Papildus CERT.LV veica ļaundabīgā koda statisko un dinamisko analīzi, kā rezultātā identificēja vairākus komandcentrus, kuri pēc CERT.LV pieprasījuma tika atslēgti.
- Jūnijā CERT.LV, ciešā sadarbībā ar „.lv" augstākā līmeņa domēnu reģistru, kas ir apkopojis sarakstu ar 123 ievainojamiem DNS serveriem, uzsāk serveru īpašnieku informēšanu par DNS sistēmas ievainojamību.
- Tika saņemts ziņojums no valsts iestādes par mērķētu mēģinājumu iesūtīt datorvīrusus vairāku darbinieku datoros. CERT.LV saņēma vīrusa paraugu un veica tā analīzi.
- No citas CSIRT vienības tika saņemta informācija par mērķētu datorvīrusu, kas nosūtīts vairāku ministriju darbiniekiem Latvijā. CERT.LV apziņoja iesaistītās iestādes un informēja par IT drošību atbildīgās personas.
- Kādas pašvaldības serverī tika ievietota lapa, kas lietota Paypal lietotāju datu pikšķerēšanai. Lapa tika izvākta un kompromitētā lietotāja konts identificēts un bloķēts.
- CERT.LV saņēma informāciju par serveri, uz kura tika glabāts liels apjoms zagtu paroļu no liela e-pasta pakalpojumu sniedzēja serveriem. CERT.LV uzsāka šo datu analīzi un informēja e-pasta pakalpojumu sniedzēju. TOP biežāk lietotās paroles bija:
    - 123456
    - 1q2w3e4r5t
    - 123456789
    - qwertyuiop
    - 1qaz2wsx

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.

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 5869 apmeklētāji. Kopā CERT.LV mājas lapai bijuši 7941 apmeklējumi, 5640 unikāli apmeklējumi no 65 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa - 92 % apmeklētāju bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicēti 20 jaunumi, publiskais darbības pārskats par 2012.gada 1.ceturksni, kā arī informācija par dažādiem pasākumiem, publikācijām un citiem notikumiem. Pārskata periodā publicētas preses relīzes:

- „Kļūdaini uzrakstīta portāla adrese var inficēt jūsu datoru!", kas vēlāk papildināta arī ar incidenta tehnisko analīzi un video demonstrāciju.
- „Rīgā pārrunā Baltijas valstu IT drošību".

CERT.LV ir Twitter konts un tajā tiek regulāri publicētas ziņas par dažādiem jaunumiem: http://twitter.com/certlv. Pārskata perioda laikā tajā ir publicētas 41 ziņa.

CERT.LV uztur arī pieaugušo izglītošanas portālu http://www.esidross.lv. Pārskata perioda laikā šajā portālā ir publicēti 5 jauni raksti, portālu apmeklējuši 10865 apmeklētāji. Publicētie raksti:

- Populārākie krāpšanas veidi internetā
- Kā lietot bezvadu internetu mājās?
- Kā lietot bezvadu internetu publiskās vietās?
- Datorologs aicina uz E-veselības dienu!
- Kā droši iepirkties tiešsaistē?

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

Pārskata perioda laikā CERT.LV organizēja seminārus „Esi drošs-1" un „Esi drošs-2", kā arī semināru informātikas skolotājiem. CERT.LV piedalījās dažādās konferencēs un semināros, organizēja LV-CSIRT grupas tikšanos, piedalījās ES Dārza svētku pasākumā ar „datorologa" akciju, kā arī sadarbojās ar dažādiem medijiem.

Sīkāka informācija par paveikto:

- 4.aprīlī notika sanāksme/seminārs par Pilsoņu iniciatīvas jautājumiem, tajā piedalījās pārstāvji no procesā iesaistītajām organizācijām.
- Aprīlī BNS žurnāliste intervēja CERT.LV žurnālam „IR".
- 13.aprīlī notika CERT.LV telpās notika seminārs ar Ventspils vakarskolas skolniekiem, seminārā bija prezentācijas par IT drošību kopumā un par mobilo telefonu un citu ierīču drošības aspektiem.
- 17.aprīlī CERT.LV pārstāvji piedalījās ISACA organizētajā sanāksmē par IT drošību.
- 18.aprīlī CERT.LV pārstāvis uzstājās ar prezentāciju Tiesu priekšsēdētājiem „realITāte – IT drošība darbā un ikdienā".

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.

- 19.aprīlī CERT.LV pārstāvis uzstājās ar prezentāciju Latvijas Interneta Asociācijas gada sapulcē.
- 23.aprīlī CERT.LV pārstāvji tikās ar Valsts prezidentu.
- 24.aprīlī CERT.LV pārstāvji piedalījās Latvijas Radio raidījumā "Zināmais Nezināmajā".
- 24.aprīlī CERT.LV pārstāvis piedalījās NBS Sakaru skolas kursā "INFOSEC II" ar inscenētu IT drošības uzlaušanas scenāriju izpildi un prezentāciju.
- 25.aprīlī notika „Esi drošs-1" seminārs, tajā piedalījās 95 dalībnieki no visas Latvijas. Semināra programma un prezentācijas pieejamas CERT.LV mājas lapā: http://www.cert.lv/section/show/98
- 25.aprīlī CERT.LV pārstāvis piedalījās CVK un Spānijas kompānijas "Scytl" rīkotajā prezentācijā par Internet balsošanas risinājumu.
- 27.-28.aprīlī CERT.LV pārstāvis piedalījās DPA un Microsoft konferencē ar prezentāciju "Kā novērst IT drošības incidentus".
- 10.maijā CERT.LV pārstāvis sniedza interviju TV3 raidījumam "Bez tabu" par CERT.LV veikto Typosquatting incidenta analīzi un risināšanu.
- 12.maijā CERT.LV piedalījās ES Dārza svētkos, digitālajā teltī notika Datorologu pieņemšanas. Pasākuma laikā tika apskatīti un izārstēti 30 datori. Notika arī Intervija LTV7 tiešraidei un ziņām par CERT.LV aktivitātēm ES dārza svētkos.
- 15.maijā CERT.LV pārstāvji uzstājās ar lekcijām Ventspils augstskolā - "Realitāte virtuālajā vidē" un "IT drošības aktualitātes", piedalījās 45 studenti.
- 15.maijā notika LV-CSIRT grupas sanāksme, kurā uzstājās CERT-EE pārstāvis, kā arī tika spriests par grupas nākotni.
- 16.maijā CERT.LV pārstāvis uzstājās ISACA sanāksmē ar prezentāciju par novērotājām IT drošības aktualitātēm Latvijas interneta telpā.
- 17.maijā notika „Esi drošs-2" seminārs, tajā piedalījās 110 dalībnieki no visas Latvijas. Pasākuma programma un prezentācijas pieejamas CERT.LV mājas lapā: http://www.cert.lv/section/show/99
- 23. Maijā CERT.LV pārstāvis sniedz interviju LNT raidījumam "Tehnovīzija" par Typosquatting incidentu.
- 24.maijā notika Informācijas drošības izglītības programmas prezentācija Rīgas Stradiņa Universitātē, piedalījās 90 dalībnieki.
- Maijā un jūnijā notika gatavošanās dalībai NATO kiberdrošības mācībās Cyber Coallition 2012 un ENISA mācībās „Cyber Europe 2012".
- 27.-31.maijā CERT.LV pārstāvis piedalījās Baltijas akadēmiskās informācijas tehnoloģiju drošības apmaiņas (BAITSE) projektā, Zviedrijā, Karlskronā, Blekingas Tehniskajā universitātē. Tika veikts:
  - a) dubultā diploma maģistru apmācības programmas kursa "Information system penetration testing and vulnerability management" apraksta, prasību un satura izstrāde.
  - b) vienošanās par Eiropas līmeņa zinātnisko un akadēmisko sadarbību Informācijas Tehnoloģiju un mākoņskaitļošanas drošības virzienā.
- 29.maijā CERT.LV pārstāvis piedalījās Microsoft organizētajā darbnīcā par mākoņskaitļošanas ieviešanu.
- 13.jūnijā CERT.LV telpās notika seminārs „IT drošība skolā", kurā piedalījās 37 informātikas skolotāji no dažādām skolām. Pasākuma programma un prezentācijas pieejamas CERT.LV mājas lapā: http://www.cert.lv/resource/show/199 Pasākumā piedalījās arī Datu Valsts inspekcijas pārstāvis.

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.

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

CERT.LV pārstāvis ir pabeidzis darbu Vides un reģionālās attīstības ministrijas darba grupā „Informācijas sistēmas drošības pārvaldnieka profesijas standarts" izstrādei. Grupu vadīja Vides un reģionālās attīstības ministrija, sanāksmju rezultātā tika sagatavoti divi dokumenti:

- Informācijas drošības vadītāja profesijas standarts. Profesijas kods - 1330 --. (pēdējie divi cipari nav vēl piešķirti)
- Informācijas sistēmas drošības pārvaldnieka/vadītāja profesijas standarts. Profesijas kods: 2529 07.

28.maijā CERT.LV pārstāvis piedalījās Centrālās Vēlēšanu Komisijas rīkotajā sanāksmē par EK sagatavoto aptaujas anketu "ECI automatizētā atbalsta anketu skaitīšanas programmnodrošinājuma izveides pētījumā" - "ISA study for open source software for validation and analysis of statements of support for European Citizen's Initiatives".

16.,22. un 29.maijā, 5. un 12.jūnijā CERT.LV pārstāvji piedalījās kā pieaicinātie eksperti Saeimas Juridiskās komisijas sēdēs par grozījumiem likumā "Par tautas nobalsošanu un likumu ierosināšanu".

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 30.jūnijam CERT.LV ir apkopojis informāciju par 505 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 79 inficētām IP adresēm.

Aprīlī CERT.LV elektroniski izsūtīja 229 vēstules valsts un pašvaldību organizācijām, lai pateiktos par labo sadarbību un uzzinātu, kā tiek pildīts IT drošības likums. Uz lielāko daļu no vēstulēm ir saņemtas atbildes.

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. CERT.LV ir

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.

sācis individuāli pa telefonu sazināties ar ESK un atgādināt viņiem iesniegt rīcības plānus, kā arī piedāvājis palīdzību konsultēt neskaidrību gadījumos.

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.

Atsevišķi jāizceļ gadījums, kad tika saņemts palīdzības lūgums no Azerbaidžānas pret kuras ministrijām tika veikti DDoS uzbrukumi. CERT.LV informēja iesaistīto IP adrešu un tīklu īpašniekus un centās palīdzēt Azerbaidžānas CSIRT komandai. Par sniegto atbalstu CERT.LV ir saņēmis atzinības vēstuli no Azerbaidžānas CERT.

CERT.LV pārstāvji pārskata periodā piedalījušies sekojošās konferencēs un semināros, kā arī veikuši citus uzdevumus:

- 18.aprīlī CERT.LV pārstāvis piedalījās ‘European Commision, Directorate-General „Home Affairs” rīkotajā sanāksmē „Identity Theft”.
- Pārskata periodā CERT.LV pārstāvis piedalījās ENISA IT drošības mācībās "Cyber Europe 2012" organizēšanā un plāno dalību tajās.
- 10-11.maijā Amsterdamā, Nīderlandē notika kārtējā TF-CSIRT sanāksme. CERT.LV pārstāvis uzstājās ar prezentāciju par tehnisko IT drošības mācību organizēšanu.
- 14-15.maijā Rīgā notika ceturtā Baltijas valstu informācijas tehnoloģiju drošības politiku koordinācijas sanāksme, kurā tika pārrunāta visu trīs Baltijas valstu drošība IT jomā.
- 5-8.jūnijā CERT.LV pārstāvis piedalījās NATO CCDCoE organizētajā konferencē "International Conference on Cyber Conflict - CyCon 2012". Pārstāvis piedalījās tehniskajā un stratēģiskajā virzienā, debatēs, kā arī apmainījās ar pieredzi un viedokļiem par informācija sistēmu drošību un aizsardzību.
- 18-19.jūnijā CERT.LV pārstāvji piedalījās CERT.EE rīkotajā simpozijā par IT drošības incidentiem un kritiskās infrastruktūras aizsardzību, kur uzstājās ar prezentāciju „Information security education programme”.
- 26.jūnijā CERT.LV pārstāvis piedalījās ENISA "Cyber Europe 2012" mācību plānošanas darba grupas sanāksmē. Sanāksmē tika apspriesti mācību mērķi, svarīgākie datumi un laiki, paredzētā mācību norises gaita, nepieciešamie pasākumi un sagatavošanās darbi.
- Jūnijā CERT.LV pārstāvis piedalījās vairākos IT drošības pasākumos:
  - ENISA organizētajās praktiskajās IT drošības mācībās, kuru materiālus veidoja ENISA ar Team Cymru.
  - FIRST 2012 konferencē, kurā piedalījās vairāk kā 500 dalībnieku no visas pasaules. Šīs konferences laikā vairākās prezentācijās tika pieminēts CERT.LV un Latvija, pateicoties CERT.LV uzsāktajai sadarbībai ar citu valstu CSIRT komandām.
  - CERT.LV pārstāvis uzstājas ar prezentāciju CERT-CC rīkotajā sanāksmē CERT komandām ar nacionālu nozīmi. Prezentācijā klātesošie tika iepazīstināti ar CERT.LV un Latvijas IT drošības sistēmu
- CERT.LV piedalījās ENISA 2012.gada aptaujā par CSIRT un tiesībsargājošo iestāžu sadarbību. Aptaujas rezultāti tiks izmantoti, lai stiprinātu nacionālu/ valdību CSIRT vienību darbu, izstrādājot labās prakses vadlīnijas un apmācību materiālus.

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.

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

- CERT.LV ir uzsācis vairākus publiskos iepirkumus, lai varētu iegādāties aparatūru, kas nepieciešama turpmākajai darbībai, perioda laikā uzsākta aparatūras piegāde.
- LV CSIRT grupas sanāksmes par restrukturizāciju notika 12.aprīlī un 15.maijā, CERT.LV un neliela darba grupa strādā pie jaunās grupas nolikuma un ētikas kodeksa gatavošana.
- CERT.LV ir ticies ar Aizsardzības ministrijas Valsts sekretāru.
- CERT.LV tikās ar „Drošs internets" pārstāvjiem un Latvijas Interneta Asociācijas (LIA) pārstāvjiem, lai apspriestu iespēju veidot kopīgu kvalitātes zīmi ESK, kas izpildīs konkrētus nosacījumus. Ir jau izstrādāts saprašanās memorands, kuru apspriež
- LIA.
- Trīs CERT.LV pārstāvji piedalījās CCDCoE rīkotajos kursos Tallinā, Igaunijā.

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

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.