Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) uzdevumu izpildi 2013.gada 1.ceturksnī

(01.01.2013. – 31.03.2013.)

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.

Kopsavilkums

Pateicoties CERT.LV aktivitātēm un iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs", kā arī tam, ka globālajā tīmeklī tika pārtraukta vairāku lielu robotu tīklu darbība, pārskata periodā gandrīz par 50% samazinājās reģistrēto zemas prioritātes incidentu daudzums, salīdzinot ar iepriekšējo ceturksni, un turpinājās vienlaicīgi inficēto IP adrešu skaita samazināšanās. Iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs" februārī pievienojās un saprašanās memorandu parakstīja arī nozares tirgus līderis SIA Lattelecom. Augstas prioritātes incidentu skaita samazinājums pret iepriekšējo ceturksni ir neliels, tikai 8%.

Janvāra sākumā pastiprināta uzmanība tika pievērsta Indonēzijas hakeru grupējuma aktivitātēm. Parasti mēnesī tiek izķēmotas vidēji 50 mājas lapas, bet 2013.gada sākumā uzlauzto un izķēmoto lapu skaits pārsniedza 200 lapas mēnesī. Par grupējuma upuriem krita lapas, kurās izmantota neatjaunināta *Joomla!* satura vadības sistēma (CMS), tāpēc par nepieciešamību nekavējoties veikt attiecīgos atjauninājumus tika informēta sabiedrība.

Marta beigās notika apjomīgs izkliedētais pakalpojumu atteices uzbrukums (DDoS) globālā mēstuļu melnā saraksta uzturētājam Spamhaus. Šī uzbrukuma ietvaros arī pret resursiem Latvijā, kas veic mēstuļu plūsmas ierobežošanu, tika raidīts vairāk kā 6.00 Gb/s datu kanāla pārslodzes uzbrukums. Uzbrukums tika veiksmīgi ierobežots.

Pārskata periodā CERT.LV informēja virkni valsts un pašvaldību iestādes par atklātām ievainojamībām šo iestāžu tīmekļa vietnēs un sniedza ieteikumus, kā šīs ievainojamības novērst, bet vairumā gadījumu saņēma atbildi, ka novēršana nav iespējama, jo iestādei nav nepieciešamo resursu un kompetences.

Janvārī CERT.LV organizēja otrās tehniskās IT drošības mācības, kurās sniedza iespēju IT profesionāļiem uzlabot savas zināšanas infrastruktūras aizsardzībā un uzbrukumu atklāšanā un novēršanā. Pārskata periodā kopumā CERT.LV noorganizēja 17 seminārus un apmācīja 722 cilvēkus, publicēja 9 jaunus rakstus portālā www.esidross.lv, 37 jaunas ziņas portālā www.cert.lv, piedalījās 5 radio pārraidēs un 5 televīzijas sižetos. Informācija, kas ieguva plašāko popularitāti interneta mediju vidū, bija ziņa par Indonēzijas hakeru uzbrukumu un 2012.gada pārskatā iekļautie statistiskie rādītāji.

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

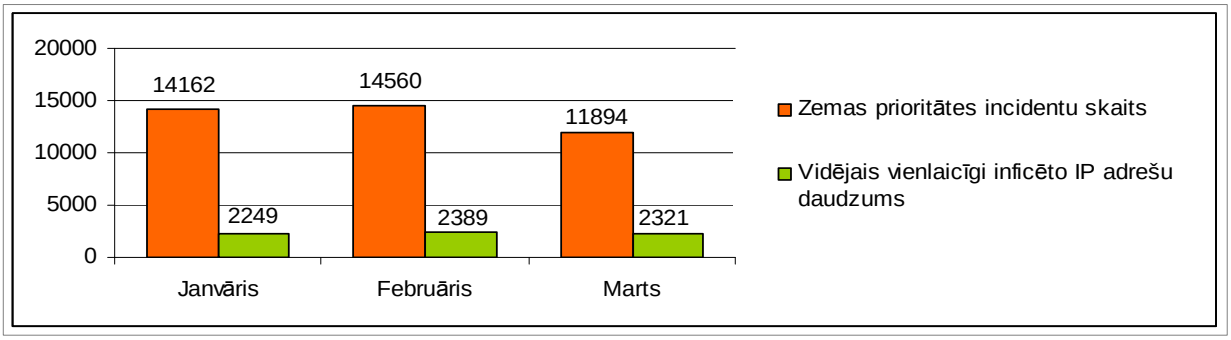
2013.gada pirmajā ceturksnī CERT.LV apstrādāja gan dažādus augstas bīstamības incidentus, gan arī lielu skaitu zemas prioritātes incidentu, kur datori bija inficēti ar dažādiem vīrusiem un bija kļuvuši par robotu tīklu (*botnet*) sastāvdaļām.

Pārskata periodā reģistrēti 926 augstas prioritātes incidenti, kas ir par 260 incidentiem jeb 22% mazāk nekā iepriekšējā gada pēdējā ceturksnī reģistrēto augstas prioritātes incidentu daudzums. Salīdzinot ar 2012.gada 1.ceturksni, pārskata periodā reģistrēto augstas prioritātes incidentu daudzums ir samazinājies par nepilniem 8%.

Zemas prioritātes incidentu jomā ir vērojams būtisks samazinājums. Salīdzinot pārskata periodu ar iepriekšējā gada pēdējo ceturksni, reģistrēto zemas prioritātes incidentu skaits ir samazinājies par 51%, bet, salīdzinot ar iepriekšējā gada pirmo ceturksni, reģistrēto zemas prioritātes incidentu skaits ir samazinājies par 45%. Tas skaidrojams gan ar CERT.LV un Atbildīgo interneta pakalpojumu sniedzēju aktivitātēm, gan ar globālajām tendencēm pasaulē un vairāku lielu robotu tīklu aizvēršanu.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Janvārī šis skaits ir bijis 2249, februārī – 2389, martā - 2321. Pārskata perioda ietvaros šī rādītāja izmaiņas bija nelielas, bet, raugoties uz tendenci kopumā, jau no pagājušā gada sākuma vērojama stabila vienlaicīgi inficēto IP adrešu skaita un ik mēnesi inficēto IP adrešu daudzuma samazināšanās. 2012.gada pirmajos trīs mēnešos vienlaicīgi inficēto IP adrešu skaits nenokrita zem 3000, bet 2012.gada pēdējā ceturksnī tas bija ap 2500, pārskata periodā turpinot samazināties.

1.attēlā redzams, kā mainījies zemas prioritātes incidentu skaits un vidējais inficēto IP adrešu daudzums 2013.gada 1.ceturkšņa laikā.

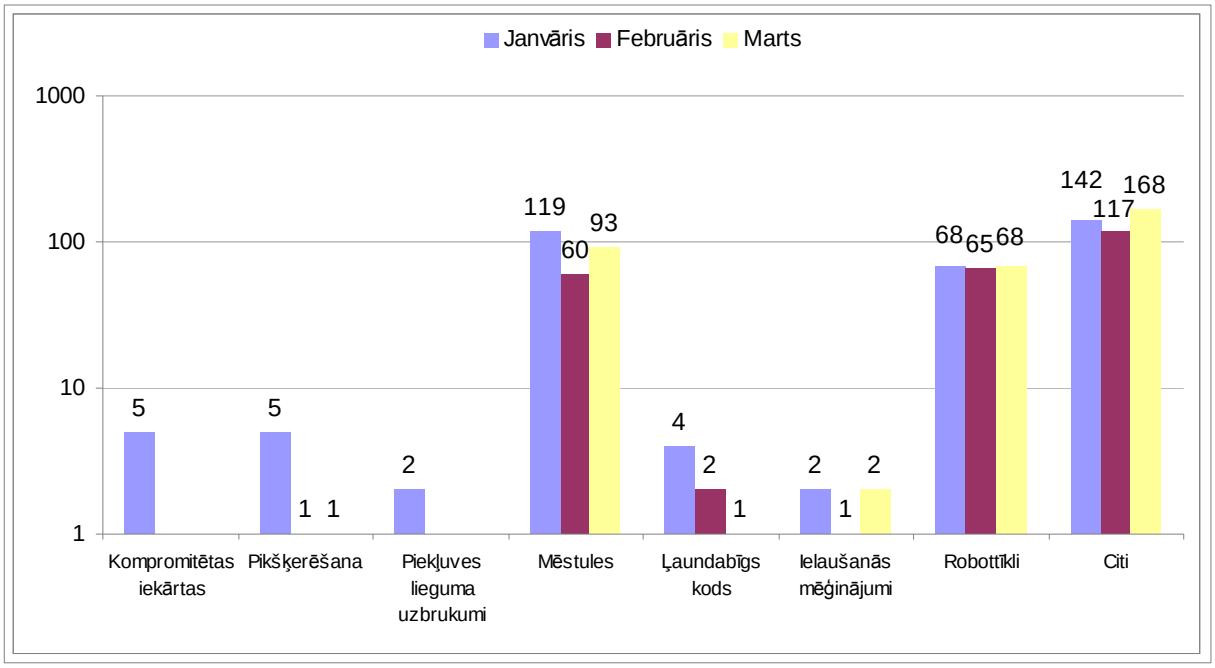


1.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem 2013.gada 1.ceturksnī.

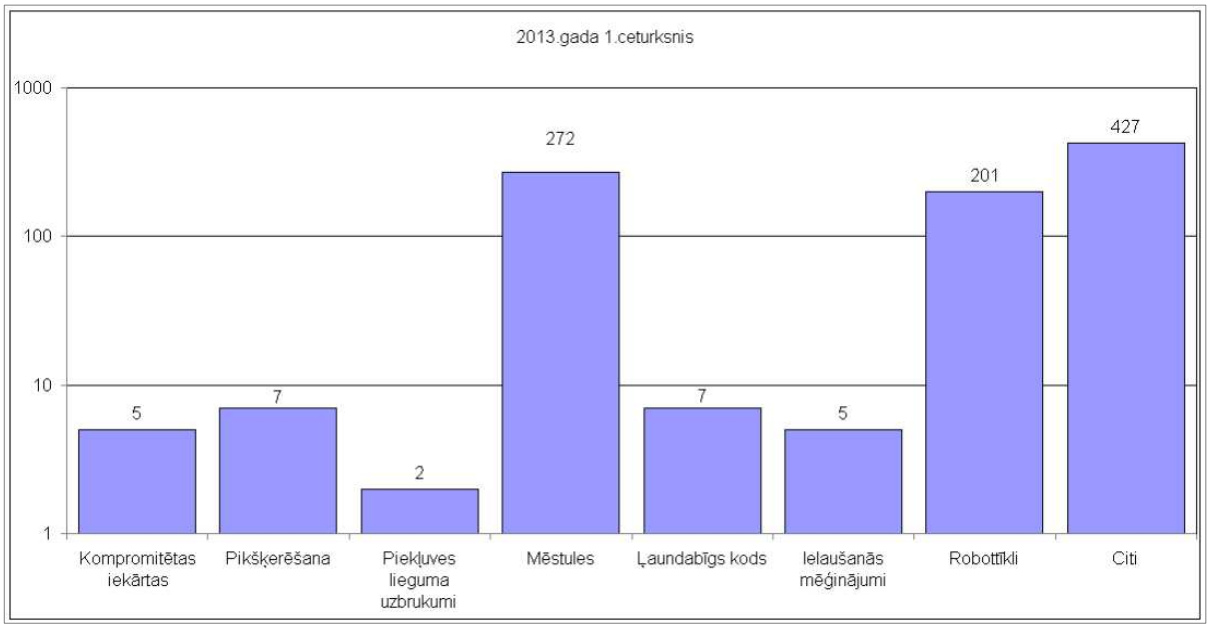
Lai samazinātu kopējo inficēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar tiem interneta pakalpojumu sniedzējiem, kas vēlas sadarboties ar šīm abām organizācijām un pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". Pārskata periodā saprašanās memorandu parakstīja arī SIA Lattelecom un SIA FirstHost, pievienojoties 11 jau esošajiem atbildīgajiem IPS.

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

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis 926 augstas prioritātes incidentus. 2.attēlā redzams augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem (grafiks ir logaritmiskā mērogā).

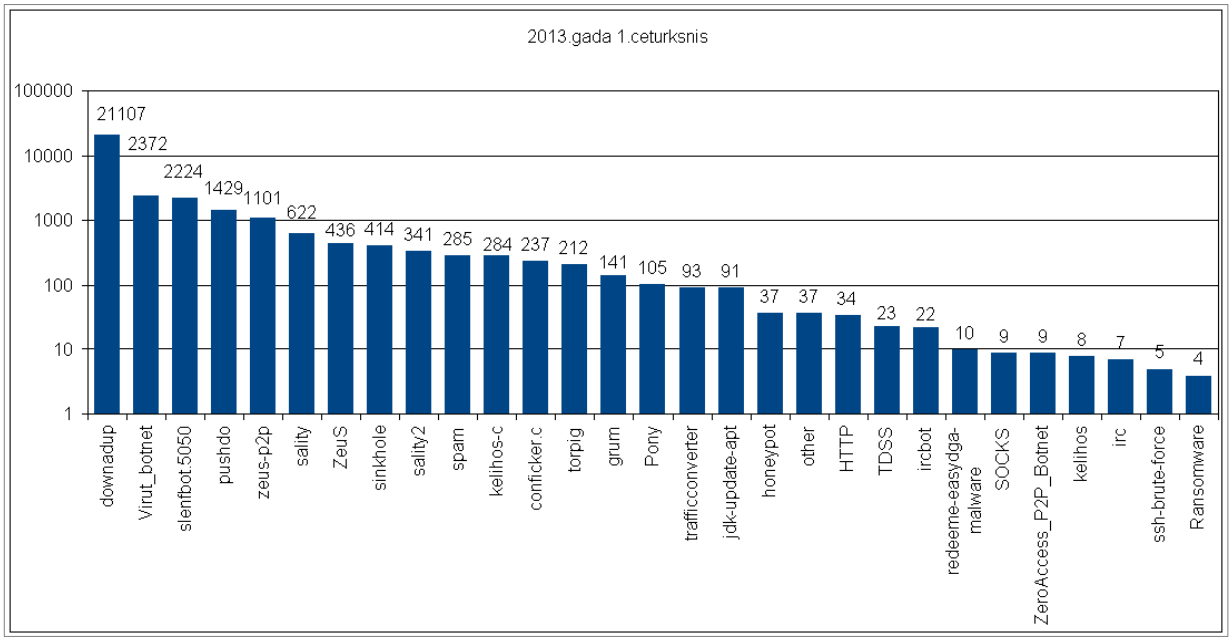


2.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.



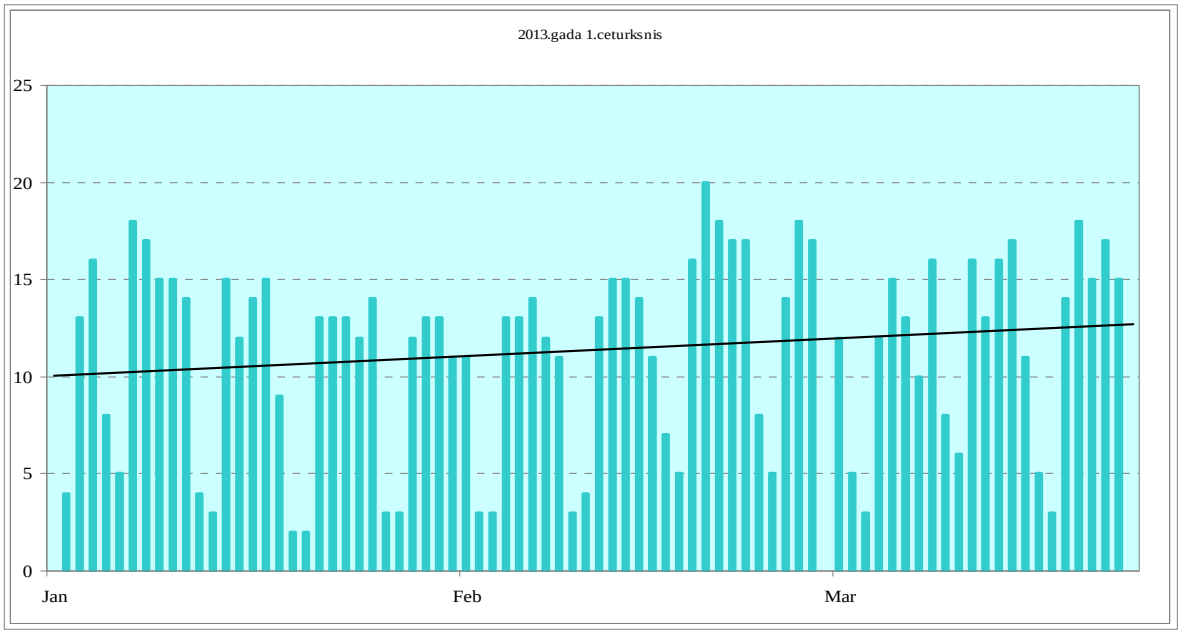
3.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2013.gada 1.janvāra līdz 31.martam (grafikā izmantota logaritmiskā skala).

Pārskata perioda laikā CERT.LV ir reģistrējis 31714 zemas prioritātes incidentus, par 18515 inficētajām IP adresēm jeb 58% IPS ir informējuši savus gala lietotājus.



4.attēls - CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā no 2013.gada 1.janvāra līdz 31.martam pa infekciju tipiem (grafikā izmantota logaritmiskā skala).

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



5.attēls – Valsts un pašvaldību iestāžu inficēto IP adrešu daudzums katras dienas saņemtajos ziņojumos.

Pārskata periodā CERT.LV sadarbojās ar dažādām valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem, un citām organizācijām konkrētu, dažādas bīstamības incidentu risināšanā. Zemāk uzskaitīti svarīgākie un interesantākie gadījumi:

- 02.01. Latvijā tika identificēti vairāki kompromitēti serveri, kas tika izmantoti DDoS uzbrukumu kampaņā Ababil/itsoknoproblembro, kas bija vērsti pret Amerikas finanšu institūcijām. Uzbrukumu datu plūsmas apjoms, kas sasniedza finanšu institūcijas, kulminācijas brīžos sasniedza 70 Gb/s.

  Incidenta analīzes rezultātā tika noskaidrots, ka uzbrucēji savu zombēto datoru armiju veidoja, izmantojot ievainojamības tīmekļa lapās, kas veidotas uz novecojušām *WordPress* un *Joomla!* satura vadības sistēmu versijām. Uz kompromitētā servera tika izvietota uzbrukuma kampaņai sagatavota programmatūra. Uzbrucēji izvēlējās kompromitēt koplietošanas mitināšanas (hosting) serverus, kuriem pieejamā interneta pieslēguma jauda ir vismaz 10 reizes lielāka nekā standarta mājas interneta lietotājam.

  Par *WordPress* un *Joomla!* satura vadības sistēmu ievainojamībām un ar tām saistītiem incidentiem Latvijā CERT.LV ir ziņojis jau agrāk, un tās sastopamas itin bieži. Tas gan nenozīmē, ka šī programmatūra nebūtu jālieto. Incidenti ir skaidrojami ar šo programmatūras izstrādājumu popularitāti un izplatību, kā arī norāda uz programmatūras lietotāju paviršo attieksmi pret atjauninājumu ieviešanu.

  CERT.LV apzināja un brīdināja Latvijas IP adrešu īpašniekus, kuru adreses piedalījās DDoS uzbrukumā Amerikas bankām.

- 02.01. Tika konstatēts, ka 27.decembrī ir tikusi uzlauzta kāda tīmekļa lapa, kas tika uzturēta uz novada pašvaldības servera. Pašvaldības pārstāvji par incidentu uzzināja no CERT.LV sniegtās informācijas. Veicot incidenta analīzi, tika noskaidrots, ka tīmekļa lapa kompromitēta, izmantojot ievainojamību novecojušā *Joomla!* satura vadības sistēmas v.1.5.16 komponentē Password Remind Functionality. Novada pašvaldības atbildīgā persona ziņoja CERT.LV, ka satura vadības sistēma pēc incidenta tika atjaunota uz jaunāku versiju ar drošības ielāpiem.

- 03.01. CERT.LV ziņoja par vairākiem desmitiem uzlauztu un izķēmotu Latvijas tīmekļa lapu. To skaits strauji turpināja augt līdz pat februārim.

  Uzbrucēji sevi dēvēja par Indonēzijas hakeriem. Daļa ļaunprātīgo darbību tika veiktas no Indonēzijas IP adresēm, taču to filtrēšana nebija uzskatāma par risinājumu. CERT.LV aicināja visus *Joomla!* lietotājus atjaunināt lietotās CMS versijas uz jaunāko, kā arī pārliecināties, ka visi papildus *Joomla!* funkcionalitātes moduļi (plugins) arī tiek atjaunināti.

  Līdz šim tika novēroti uzbrukuma pielietojumi uz JCE Joomla Extension versijām 2.0.10 un vecākām, modulim "imgmanager". Uzbrukumi tika veikti automatizēti, un sekmīgas uzbrukuma realizācijas gadījumā uzbrucējs spēja izvietot ļaundabīgus failus uz upura sistēmas.

  CERT.LV brīdināja sabiedrību par masveida izķēmošanas uzbrukumiem lapām ar neatjauninātu *Joomla!* CMS un informēja par nepieciešamību veikt atjauninājumus.

- 11.01. CERT.LV konstatēja aizdomīgu ievades parametru apstrādi kādā valsts institūcijas tīmekļa lapā, kas liecina par iespējamu ievainojamību. Lai pārliecinātos, vai tīmekļa lapai jau nav veikti uzbrukumi, tika pieprasīti žurnālfaili. Tika konstatēti

ievainojamību meklēšanas mēģinājumi, taču tie nav bijuši sekmīgi.

- 11.01. Tika konstatēts uzbrukuma mēģinājums kādas valsts iestādes tīmekļa vietnei. Veicot žurnālfailu un tīkla noslodzes datu analīzi, CERT.LV konstatēja, ka uzbrukums līdzinās testam, lai novērotu iestādes resursa noturību pret servisa atteices jeb pārslodzes uzbrukumiem.

- 14.01. CERT.LV konstatēja, ka kādas finanšu iestādes mājas lapā iespējams izsaukt SQL kļūdas paziņojumus un pastāv iespējamība šo kļūdu izmantot uzbrukumam. Iestādes atbildīgās personas tika informētas un konstatētie trūkumi tika novērsti.

- 15.01. CERT.LV iesaistījās darbā pie inficēto iekārtu identificēšanas Latvijā, kas ir iesaistītas „Sarkanā oktobra" (Red October) kiberspiegošanas kampaņā. Inficētās iekārtas tika apzinātas un atbildīgās personas informētas.

- 23.01. CERT.LV konstatēja ievainojamību kādas valsts iestādes mājas lapā, kas ļāva nesankcionēti izgūt datu bāzes informāciju un, iespējams, operēt ar failu sistēmu. Par konstatēto ievainojamību CERT.LV informēja atbildīgo personu, taču saņēma atbildi, ka iestādē nav resursu un atbilstošas kompetences, lai atklātos trūkumus novērstu.

- 24.01. Kāda novada tīmekļa vietne tika izmantota ļaunatūras izplatīšanai. CERT.LV, izpētot situāciju, secināja, ka tīmekļa lapa nav nedz administrēta, nedz izstrādāta, ievērojot minimālās drošības prasības. CERT.LV sniedza rekomendācijas atbildīgajai personai.

- 24.01. Kompromitēti vairāki kāda IPS maršrutētāji, visi apmeklētāji tika pārvirzīti uz uzlauzēju izvēlētu interneta vietni. Problēma turpinājās apmēram 6 stundas. Uzlaušanas veids - nozagta administratora parole.

- 25.01. CERT.LV identificēja vairākas kritiskas ievainojamības kādas valsts iestādes interneta vietnē. Detalizēts apraksts un rekomendācijas tika nosūtītas atbildīgajai personai. Pēc laika CERT.LV saņēma informāciju, ka identificēto trūkumu novēršanai iestādei trūkst resursu.

- 25.01. CERT.LV sniedza rekomendācijas uzbrukuma risināšanā kādai privātai kompānijai un interneta veikalam. Sākotnēji bija aizdomas par 0-dienas ievainojamību Microtik maršrutētāja programmatūrā, taču žurnālfailu trūkuma dēļ un pēc iegūtā situācijas apraksta tika secināts, ka tika uzminēta maršrutētāja parole. Uzbrucēji veica konfigurācijas izmaiņas, kuru rezultātā visi mājas lapas apmeklētāji tikai pārsūtīti uz uzbrucēju sagatavotu vietni.

- 30.01. CERT.LV saņēma informāciju no Amerikas kolēģiem par jaunas robotu tīkla (botnet) infekcijas izplatību. CERT.LV veica pieejamo datu analīzi, taču Latvijā netika konstatētas ar šo ļaunatūru inficētas iekārtas.

- 02.02. Plaši izplatītajam "Policijas izspiedējvīrusam" tika novērota jauna, daudz bīstamāka versija, kas veic daļēju cietā diska datu šifrēšanu. CERT.LV izdevās no ārzemēm iegūt jaunā vīrusa paraugu analīzei, bet Latvijā šī vīrusa versija līdz šim nav konstatēta.

- 03.02. CERT.LV sniedza konsultāciju "pārņemta" Yahoo e-pasta konta atgūšanā.

- 05.02. Tika konstatēts mērķēts uzbrukums kādas valsts iestādes atvērtā koda e-pasta AntiSpam sistēmai. CERT.LV iesaistījās incidenta risināšanā un koordinēja tā risināšanu ar ārvalstu kolēģiem, kuru tīkli bija iesaistīti uzbrukumā.

- 06.02. Konstatēts mēģinājums pikšķerēt kādas valsts iestādes e-pasta lietotāju paroles. Mēģinājums bija nesekmīgs.

- 06.02. Kādas interneta vietnes administratori lūdza CERT.LV palīdzību IT drošības incidenta risināšanā. Kompānijas serveri bija pakļauti apjomīgam DoS uzbrukumam, kas pārsniedza 4.00 Gb/s, kas uz informācijas saņemšanas brīdi bija jau pārtraukts. Diemžēl kompānija nebija tehniski nodrošinājusi žurnālfailu uzkrāšanu, tādēļ incidenta analīze bija apgrūtināta.

- 11.02 Konstatētas pikšķerēšanas lapas, kas izveidotas vairāku Latvijas komercbanku klientu informācijas izkrāpšanai. Piekļuve tām liegta, pateicoties aktīvai banku darbībai, informējot lapas uzturētāju.

- 13.02. Kāds Latvijai piederīgais uzsāka servisa atteices uzbrukumu kampaņu pret vairākām Latvijā strādājošu banku tīmekļa lapām un internetbanku vietnēm no TOR tīkla IP adresēm. CERT.LV ir nodevis incidenta analīzes rezultātus Valsts policijai.

- 20.02. No Amerikas kolēģiem tika saņemta informācija par jauna spiegošanas tīkla aktivitātēm pasaulē un Latvijā. 25.02. CERT.LV izsūtīja brīdinājuma vēstules vairākām valsts iestādēm par spiegu tīkla aktivitātēm un lūdza veikt žurnālfailu pārbaudes, lai konstatētu aizdomīgas aktivitātes. Atbilžu apkopošana un rezultātu izpēte turpinās.

- 25.02. Lietuvas IP adresē bija izvietota lapa kādas Latvijas komercbankas lietotāju datu izkrāpšanai. CERT.LV informēja lapas uzturētājus un Lietuvas CERT vienību un panāca šī resursa slēgšanu.

- 27.02. Tika konstatēta IP adrese Latvijā, kas bija inficēta ar spiegošanas vīrusu MiniDuke. Infekcija šajā uzbrukumu kampaņā tika izplatīta, izmantojot Adobe PDF lasītāja, Java un MS Office ievainojamības. CERT.LV piedalījās incidenta risināšanā.

- 01.03. Latviju un vairākas citas valstis pāršalca mēstuļu vilnis, kuru ziņojums noformēts kā PayPal paziņojums lietotājam ar lūgumu drošības apsvērumu dēļ nomainīt paroli. Ziņa saturēja saiti uz uzbrucēju sagatavotu tīmekļa vietni. CERT.LV iesaistīja PayPal drošības incidentu risināšanas nodaļu šī incidenta risināšanā.

- 05.03. Tika konstatēts ievainojamību meklēšanas mēģinājums pret kādu portālu. CERT.LV brīdināja IP adreses lietotāju par šādu darbību kaitīgumu un iespējamo atbildību.

- 14.03. CERT.LV sniedza konsultāciju par seku novēršanu veiksmīgam lietotāju privāto datu izkrāpšanas uzbrukumam, kas bija ticis vērsts pret kādu valsts institūciju. Kaitīgu seku uzbrukumam nav.

- 14.03. Konstatēts neveiksmīgs kādas valsts iestādes darbinieka paroles izkrāpšanas mēģinājums. Labi apmācītais darbinieks pats ir pamanījis krāpšanu.

- 15.03. CERT.LV sniedza konsultācijas privātpersonām, izvērtējot vairākus krāpnieciskus e-pastus.

- 20.03. CERT.LV konstatēja, ka kāda valsts iestādes mājas lapa ir uzlauzta. Par incidentu tika informēta atbildīgā persona. Incidents ir bijis uzbrucējiem sekmīgs, jo tīmekļa vietne uzturēta uz novecojušas *Joomla!* CMS, kurai netika veikti drošības atjauninājumi.

- 21.03. Tiek saņemta informācija no Polijas par krāpnieciskiem darījumiem, izmantojot publisko telekomunikāciju tīklu, kurā iesaistīti Latvijas numerācijas grupā ietilpstoši paaugstinātas maksas tālruņu numuri. Par šo gadījumu CERT.LV informē policiju un SPRK.

- 25.03. Tika saņemts incidenta ziņojums par kompromitētu kādas mācību iestādes vietni, kuru apmeklējot, notiek apmeklētāja pārsūtīšana uz uzbrucēja sagatavotu interneta vietni.

- 29.03. Latvijā uzturētais mēstuļotāju melnais saraksts, kas ir CERT.LV un inbox.lv kopīgi realizēts projekts, cieta no apjomīga uzbrukuma, kas bija daļa no vispasaules uzbrukumu kampaņas Spamhaus serveriem (par incidentu ziņoja arī vairāki pasaulē pazīstami mediji: http://nyti.ms/14mVCPd). Pret Latvijas serveri, kas atrodas SigmaNet akadēmiskā tīkla datu centrā, tika raidīts vairāk kā 6.00 Gb/s datu kanāla pārslodzes uzbrukums. Tas tika veiksmīgi ierobežots sadarbībā ar ienākošās datu plūsmas apkalpojošajiem IPS.

Cita veida sadarbība ar dažādām iestādēm ir norādīta pie 8.punkta.

CERT.LV uzskaita arī uzlauzto un izķēmoto mājas lapu gadījumus. Šādu gadījumu skaits janvārī bija 238, februārī – 225, martā – 63. Augstais uzlauzto un izķēmoto lapu skaits pārskata perioda sākumā skaidrojams ar Indonēzijas hakeru uzbrukuma vilni mājas lapām, kas izmantoja neatjauninātu *Joomla!* CMS versiju.

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

CERT.LV uztur tīmekļa vietni http://www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. Pārskata periodā vispopulārākā bija lapa par jaunākajām ievainojamībām un vīrusiem (9814 apmeklētāji), tai seko CERT.LV sagatavota informācija par „Policijas vīrusa" apkarošanas praksi un mehānismiem (8603 apmeklētāji). Kopā CERT.LV mājas lapai bijuši 17647 apmeklējumi, kurus veido 12844 unikāli apmeklētāji no 65 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa – 92,96 % apmeklētāju bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicētas 37 ziņas un preses relīzes, publiskais darbības pārskats par 2012.gada 4.ceturksni un par 2012.gadu kopumā, publicēta informācija par publikācijām, dažādiem pasākumiem un citiem notikumiem, kā arī izveidota jauna sadaļa, kas veltīta Kiberaizsardzības vienības jautājumiem.

CERT.LV ir divi Twitter konti un tajos tiek regulāri publicētas ziņas par dažādiem jaunumiem: http://twitter.com/certlv un http://twitter.com/datorologs. Pārskata perioda laikā certlv kontā tika

publicētas 56 ziņas, kontam pievienojušies 73 jauni sekotāji un 77 reizes certlv ziņa ir tikusi „retvītota" jeb padota tālāk. Datorologs kontā pārskata periodā tika publicētas 3 ziņas. CERT.LV ir izveidots arī Facebook profils http://www.facebook.com/certlv (pārskata periodā publicētas 52 ziņas) un draugiem.lv profils http://www.draugiem.lv/certlv.

CERT.LV uztur arī pieaugušo izglītošanas portālu http://www.esidross.lv. Pārskata perioda laikā šajā portālā ir publicēti 9 jauni raksti, portālu apmeklējuši 21561 (15428 unikāli) apmeklētāji. Publicētie raksti:

- Typosquatting – kas tas ir?
- ZoneAlarm – ugunsmūris
- CMS platformas un to drošība
- Planšetdatori un to drošības apdraudējumi
- Divpakāpju autentifikācija
- Bezmaksas aizsardzība no sekotājiem
- Adblock Plus – bezmaksas rīks reklāmu bloķēšanai
- Pajautā Datorologam
- NoScript

Pārskata periodā bijušas arī uzstāšanās televīzijā un radio, dažādas publikācijas presē un portālos. Sīkāka informācija:

1) Publikācijas presē:
- 2013.gada janvārī „CERT.LV - jauns instruments Latvijas kiberdrošībai" – raksts Aizsardzības ministrijas izdevumā „Tēvijas sargs"
- 03.01. – CERT.LV pārstāvis sniedza komentāru laikrakstam Diena par „Policijas izspiedējvīrusu"

2) Intervijas un ziņas radio:
- 08.01. – CERT.LV pārstāvis Latvijas radio 1 raidījumā „Krustpunktā" piedalījās diskusijā par to, kā novērst kibernoziegumus
- 30.01. – CERT.LV sniedza komentāru Latvijas radio 1 ziņu dienestam par Latvijas Nacionālo drošības ziņojumu
- 31.01. – CERT.LV pārstāvis sniedza komentāru Latvijas radio ziņu dienestam par IT jomas darbaspēka atrašanas grūtībām
- 19.02. – CERT.LV pārstāvis piedalījās Latvijas radio 4 raidījumā „Diena pēc dienas", kur studijā diskutēja par to, kā pasargāt sevi internetā
- 07.03. – CERT.LV pārstāvis sniedza komentāru Latvijas radio 1 par e-paraksta drošību un lietošanu.

3) Sižeti televīzijā, tiešraides:
- 08.01. – CERT.LV pārstāvis viesojās 1.Baltijas kanāla studijā un sniedza komentārus par Indonēzijas hakeru uzbrukumu, *Joomla!* ievainojamībām un IT drošības jautājumiem
- 08.02. – CERT.LV pārstāvis piedalījās LNT raidjumā „900 sekundes" sarunā par IT drošības tendencēm un CERT.LV pārnākšanu Aizsardzības ministrijas pakļautībā
- 26.02. – sižets studentu televīzijā KIVI TV par „Policijas izspiedējvīrusu" un IT drošību Latvijā
- 06.03. – LNT raidījumā „900 sekundes" īss sižets par IT drošību un situāciju Latvijā
- 20.03. – pasākuma tiešraide no Datorologa akcijas „E-prasmju nedēļas" ietvaros

4) Ziņas portālos:

- 07.01. - Latvijas lapas piedzīvo masveida hakeru uzbrukumu – raksts TVnet, Diena un Delfi
- 07.01. - Latvijas interneta vietnēm masveidā uzbrūk «Indonēzijas hakeri» - raksts Apollo
- 07.01. - Vairākas mājas lapas Latvijā cietušas no Indonēzijas hakeru rokas – Dienas bizness
- 07.01. - Latvijas mājas lapas saskaras ar masveida hakeru uzbrukumiem – Latvijas Avīze
- 07.01. - Latvijas mājas lapām masveidā uzbrūk «Indonēzijas hakeri» - ziņa BNN
- 07.01. - Hakeri no Indonēzijas uzbrukuši vairākām mājas lapām Latvijā – ziņa LTV mājas lapā
- 07.01. - "Indonēzijas hakeri" uzbrukuši un izķēmojuši vairākus desmitus mājaslapu Latvijā – ziņa portālā LETA un puaro.lv
- 07.01. - Latvijas mājas lapas piedzīvo masveida "Indonēzijas hakeru" uzbrukumu – ziņa portālā Dobele24.lv
- 07.01. - "Indonēzijas hakeri" uzbrukuši un izķēmojuši vairākus desmitus mājas lapu Latvijā – NRA ziņa
- 08.02 - CERT.LV: ar datoru drošību saistītu incidentu skaits samazinājās – ziņa portālā TVnet
- 25.02. - "Lattelecom" pievienojas iniciatīvai par drošāku interneta vidi Latvijā – raksts LA.lv
- 11.03 - Valsts apmaksāta iespēja pārbaudīt sava datora veselību – raksts Delfi par Datorologa akciju
- 15.03. - CERT.LV: Pērn Latvijā konstatēti 4794 augstas prioritātes datu drošības incidenti – ziņa FOCUS.lv
- 16.03. - Latvijā hakeri vidēji mēnesī izķēmo gandrīz 50 mājas lapu – ziņa TVnet
- 16.03. - Latvijā trīs reizes biežāk "uzķeras" uz viltus policijas "izspiedējprogrammu" – ziņa NRA un Delfi
- 17.03. - CERT.LV atklātie trūkumi valsts IT sistēmās tiek laboti ļoti lēni – ziņa Tvnet

18.februārī CERT.LV piedalījās Aizsardzības ministrijas rīkotajā preses konferencē par Kiberaizsardzības vienības izveidošanu.

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

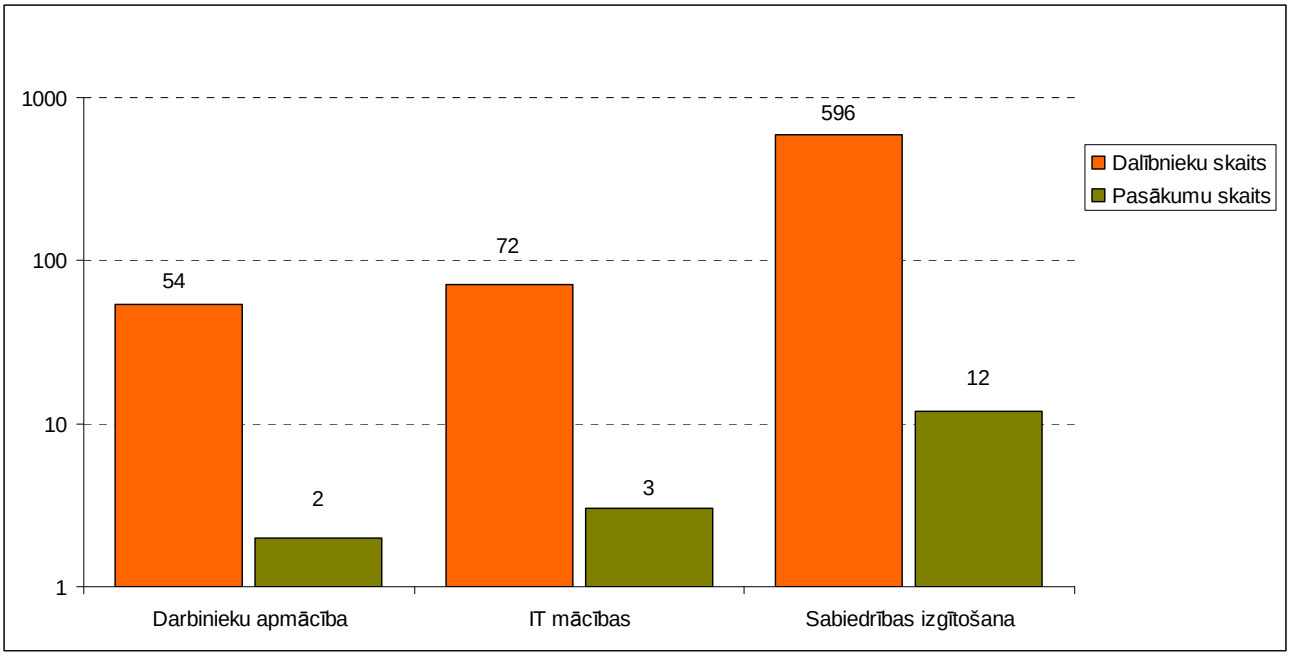
Janvāra beigās CERT.LV komanda organizēja otrās tehniskās IT drošības mācības „Sniega vētra 2013", kurās piedalījās divas Zilā karoga komandas (8 dalībnieki katrā) un viena Sarkanā karoga komanda (6 dalībnieku sastāvā), ar mērķi pilnveidot dalībnieku prasmes un zināšanas IT infrastruktūras aizsardzībā, IT drošības uzbrukumu atklāšanā un novēršanā, kā arī sniegt iespēju dalībniekiem apmainīties ar pieredzi un iepazīt nozarē strādājošos kolēģus.

Drošāka interneta dienas ietvaros 2013.gada 5.februārī CERT.LV apmeklēja vairākas skolas un vadīja IT drošības lekcijas skolēniem. E-prasmju nedēļā laika posmā no 18. līdz 22.martam CERT.LV aktualizēja IT drošības jautājumu, organizējot Datorologa akciju, kas sniedza katram interesentam iespēju atnest pārbaudīt savu datoru pie speciālista – Datorologa, lai bez maksas noteiktu, vai datorā nav vīrusu vai ļaunatūras, un saņemtu konsultācijas par drošāku datora un interneta lietošanu.

Pārskats par CERT.LV pasākumiem pārskata periodā:

- 16.01. CERT.LV pārstāvis uzstājās ar prezentāciju ISACA Latvija sanāksmē.
- 30.-31.01. Notika CERT.LV organizētās 2. tehniskās IT drošības mācības "Sniega vētra 2013"
- 05.02. Lekcijas par IT drošību Baložu skolā un Torņakalna bibliotēkā.
- 08.02. un 26.02. CERT.LV organizēja semināru par infrastruktūras uzraudzības iespējām, izmantojot atvērtā koda risinājumu OSSIM. Semināru vadīja DEG (Drošības ekspertu grupas) dalībnieks Didzis Āboliņš un CERT.LV vadītājas vietnieks Varis Teivāns. Semināros piedalījās 50 valsts un pašvaldību iestāžu, kā arī citu organizāciju IT drošības speciālisti un informācijas sistēmu un tīkla administratori.
- 14.02. CERT.LV uzsāka darbu pie NATO Cyber Coalition 2013 mācību plānošanas sadarbībā ar Nacionālo bruņoto spēku pārstāvjiem.
- 20.02. Lekcija Rīgas Doma kora skolā.
- 25.02. Divi semināri Daugavpilī – viens domes institūciju un kapitālsabiedrību vadītājiem, otrs atbildīgajiem par IT drošību.
- 27.02. Lekcija par IT drošību Rīgas 3.ģimnāzijā.
- 06.03. Dalība NBS Sakaru skolas kursā "INFOSEC 2", mācību vidē, izpildot tēmētus uzbrukuma scenārijus, analizējot iegūtos rezultātus un identificējot aizsardzības pasākumus.
- 11.-15.03. Vieslekcijas Blekingas tehniskajā universitātē (BTH, Zviedrijā), iepazīstinot maģistru programmas studentus ar ievadu tīkla infrastruktūras drošības testēšanā. Lekcijas notiek sadarbības projekta BAITSE ietvaros.
- 12.03. Semināri skolniekiem J.Endzelīna Kauguru pamatskolā un Trikātas pamatskolā, un IT drošības seminārs Beverīnas pašvaldības darbiniekiem.
- 20.03. Lekcija LU Datorikas institūta 4.kursa bakalaura programmas studentiem par aplikāciju ievainojamību un drošību, demonstrējot arī dažus iespējamos uzbrukumu veidus, tādus kā SQL injekcijas, starpvietņu skriptošana (XSS) un bufera pārpilde.
- 20.03. Datorologa akcija Rīgā E-prasmju nedēļas ietvaros.
- 22.03. Datorologa akcija Rēzeknē E-prasmju nedēļas ietvaros.
- 22.03. Seminārs uzņēmējiem Rēzeknes pašvaldībā par IT drošību.
- 23.03. Lekcija LU Datorikas institūta doktorantiem par zinātnisko metožu izmantošanu ar IT drošību saistītu pētniecisko darbu izstrādē, pārrunājot informācijas sistēmu drošības aspektus un diskutējot par zinātnisko metožu pielietošanu pētnieciskajā darbībā.

6.attēlā redzams kopējais pasākumu daudzums un apmācīto cilvēku skaits 2013.gada 1.ceturksnī. Pārskata periodā CERT.LV par IT drošību ir izglītojis 722 cilvēkus, piedaloties 17 dažādos pasākumos un lekcijās.



6.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits (grafikā izmantota logaritmiskā skala).

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.

Daļēji sadarbība ar valsts iestādēm incidentu risināšanā jau aprakstīta pie šīs atskaites 2.punkta. Šeit uzskaitītas citas sadarbības tikšanās un konsultācijas.

- 9.01., 22.02. un 22.03. Tikšanās ar Aizsardzības ministrijas valsts sekretāru.
- 18.01. Sadarbības tikšanās ar Centrālās Statistikas pārvaldes atbildīgajām personām.
- 29.01. Sadarbības tikšanās ar Latvenergo.
- 30.01. CERT.LV pārstāvis piedalījās sanāksmē par iniciatīvu veidot vienotu valsts iestāžu tīmekļa vietņu satura vadības sistēmu. CERT.LV sagatavoja detalizētu viedokli un argumentāciju, kāpēc būtu jābūt ļoti uzmanīgiem, šādu ideju realizējot, un skaidroja saistītos riskus un iespējamo apdraudējumu.
- 31.01. Latvijas IT drošības padomes sanāksme.
- 01.02. Tikšanās ar VARAM par risinājumiem Tautas nobalsošanai. Dalība VARAM darba grupā par Informācijas sabiedrības attīstības pamatnostādņu 2014-2020 izstrādi.
- 21.02. Sadarbības tikšanās ar Eiropas Savienības prezidentūras biroju.
- 28.02. Latvijas IT drošības padomes tikšanās ar nevalstisko organizāciju pārstāvjiem, lai apspriestu ES IT drošības stratēģiju un topošo direktīvu.
- 2013.gada martā Dalība VARAM darba grupā par Informācijas sabiedrības attīstības pamatnostādņu 2014-2020 izstrādi.

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 2013.gada 31.martam CERT.LV ir apkopojis informāciju par 574 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību.

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 53 inficētām šādām IP adresēm.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 nosaka kārtību, kādā Elektronisko sakaru komersantiem jāizstrādā rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai un tas jāiesniedz CERT.LV. CERT.LV ir izskatījis iesniegtos plānus un nosūtījis atbildes vēstules ar vērtējumu. CERT.LV ir arī izstrādājis Rīcības plāna paraugu, lai palīdzētu mazajiem ESK izveidot savus plānus, un izsūtījis informāciju par šo paraugu tiem ESK, kuri līdz šim nav izstrādājuši un iesnieguši CERT.LV savus rīcības plānus elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai.

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. Konkrēti incidenti uzskaitīti šī pārskata 2.punktā.

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

- 21.-22.01. CERT.LV pārstāvis piedalījās NCSC konferencē Nīderlandē, Hāgā.
- 28.-31.01. CERT.LV pārstāvis piedalījās TF-CSIRT sanāksmē, FIRST tehniskajā seminārā un Trusted Introducer sanāksmē Lisabonā, Portugālē.
- 5-7.02. CERT.LV pārstāvji piedalījās FIB rīkotajos apmācības kursos, kas notika Rīgā.
- 5.-6.02. ENISA 13a.panta sanāksme Rīgā, CERT.LV pārstāvis uzstājās ar prezentāciju.
- Informācijas apmaiņa ar Amerikas kolēģiem un sadarbība DDoS uzbrukumu novēršanā un ar spiegu tīkliem saistītu incidentu risināšanā, kas sīkāk aprakstīta šīs atskaites 2.punktā.
- 18-22.02. CERT.LV pārstāvis piedalījās IT drošības konferencē Digital Crimes Consortium 2013 Barselonā, Spānijā.
- 26.03. CERT.LV piedalījās NATO IT drošības mācību "Cyber Coalition 2013" sākotnējā plānošanas konferencē.
- Starptautiskā projekta BAITSE ietvaros CERT.LV pārstāvis martā vadīja lekcijas Zviedrijā.

8. Uzdevums: Veikt citus normatīvajos aktos noteiktos pienākumus.

- Pārskata periodā notikušas trīs DEG grupas sanāksmes.
- No 04.02. notiek Zemas mijiedarbes urķuslazda HoneyD ieviešana akadēmiskā mākoņa vidē, konfigurēšana, darbības pārbaude un iegūto datu analīze.
- Kopš februāra uzsākts darbs pie dažādos resursos pieejamo nozares ziņu apkopošanas sistēmas *Taranis* funkcionalitātes apzināšanas un tās iespējamo pielietojumu izpētes, atbilstoši CERT.LV un tā pārziņā esošo iestāžu vajadzībām.
- 14.03. Rīgā viesojās Lielbritānijas Ārlietu ministrijas Cyber officer Baltijas valstīs Kaija Kirch no Tallinas. Kaija Kirch tikās ar pārstāvjiem no Satiksmes, Ārlietu un Aizsardzības ministrijām, kā arī notika tikšanās ar CERT.LV pārstāvjiem, lai pārrunātu jomas aktualitātes un uzzinātu vairāk par CERT.LV darbu.

Sagatavotājs – Līga Besere
tālrunis 67085858
e-pasts liga.besere@cert.lv