2013.gada publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) darbību

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.

Kas ir CERT.LV?

CERT.LV misija ir veicināt informācijas tehnoloģiju (IT) drošību Latvijā. Pārskata periodā CERT.LV darbojās Latvijas Republikas Aizsardzības ministrijas pakļautībā Informācijas tehnoloģiju drošības likuma ietvaros.

CERT.LV galvenās darbības jomas[1]:

- Vienotu elektroniskās informācijas telpā notiekošo darbību atainojuma uzturēšana.
- Sniegt atbalstu informācijas tehnoloģiju drošības incidentu novēršanā vai koordinēt to novēršanu.
- Uzturēt sabiedrībai pieejamā veidā atbilstoši aktuālajiem apdraudējumiem izstrādātas rekomendācijas par aktuālo informācijas tehnoloģiju risku novēršanu.
- Veikt pētniecisko darbu, organizēt izglītojošus pasākumus, apmācību un mācības informācijas tehnoloģiju drošības jomā.
- 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.
- Uzraudzīt, kā valsts un pašvaldību institūcijas un elektronisko sakaru komersanti izpilda Informācijas tehnoloģiju drošības likumā noteiktos pienākumus.
- Sadarboties ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām (vienībām).
- Veikt citus normatīvajos aktos noteiktos pienākumus.

Šajā pārskatā apskatīts paveiktais katrā no darbības jomām, uzsverot svarīgākos incidentus, pasākumus un sabiedrības izglītošanas aktivitātes.

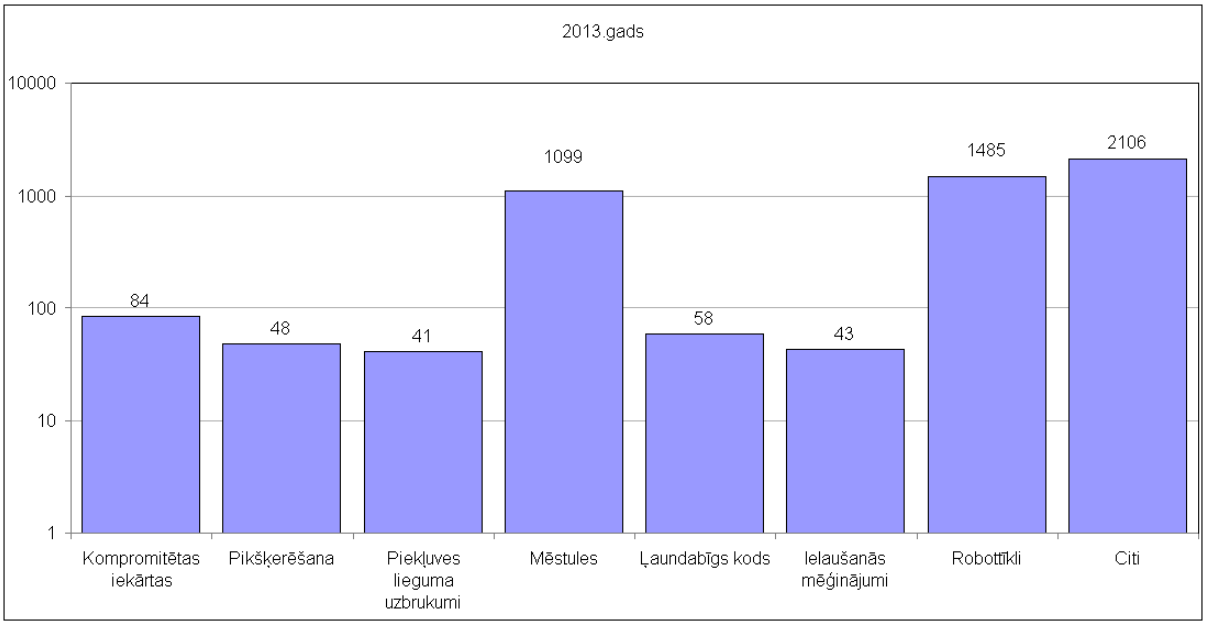
1. Vienota elektroniskās informācijas telpā notiekošo darbību atainojuma uzturēšana.

CERT.LV veic incidentu uzskaiti, dalot incidentus divās grupās: augstas prioritātes incidentos un zemas prioritātes incidentos. Par augstas prioritātes incidentiem tiek uzskatīti visi iekārtu kompromitēšanas gadījumi, pikšķerēšana, piekļuves lieguma uzbrukumi (DoS un DDoS), ielaušanās mēģinājumi, kā arī jebkurš cits incidents, kas skar tieši augstas prioritātes institūcijas (valsts un pašvaldības iestādes, kritisko infrastruktūru) vai ko ir paziņojis cilvēks, nevis automātisks ziņotājs. Katrs augstas prioritātes incidents tiek atsevišķi caurskatīts un manuāli apstrādāts.

Zemas prioritātes incidenti ir galvenokārt inficētas galalietotāju iekārtas, kas kļuvušas par robotu tīklu sastāvdaļām un/vai izsūtītas mēstules.

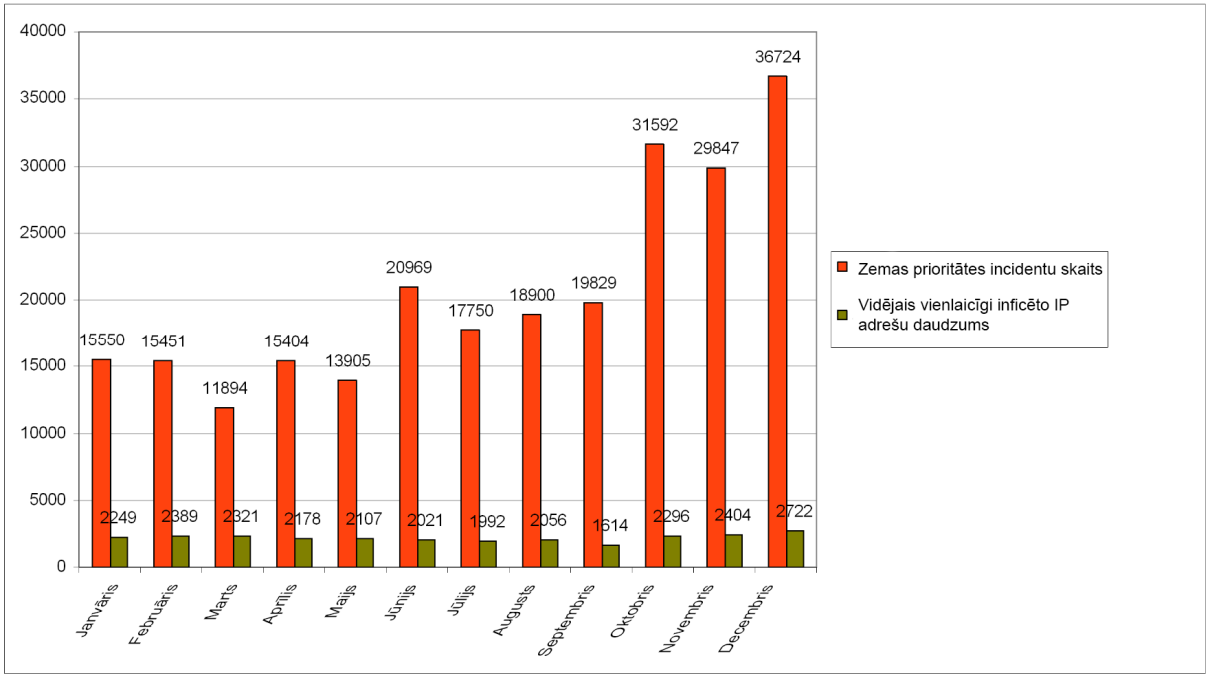
[1] Informācijas tehnoloģiju drošības likums, 5.pants

2013.gadā CERT.LV ir apstrādājis 4964 augstas prioritātes incidentus. Apstrādātie incidenti attēloti pirmajā attēlā, sadalīti pa incidentu tipiem. Biežākie augstas prioritātes incidenti ir kompromitētas iekārtas, kā arī augstas prioritātes institūciju IT iekārtu nonākšana robotu tīklos un iesaiste mēstuļu izsūtīšanā.



1. attēls – CERT.LV reģistrētie augstas prioritātes incidenti 2013.gada griezumā pa incidentu tipiem.

2013.gadā CERT.LV ir fiksējis 247815 zemas prioritātes incidentus. Otrais attēls atspoguļo CERT.LV fiksētos zemas prioritātes incidentus un katra mēneša vidējo vienlaicīgi inficēto iekārtu skaitu – unikālas IP adreses, kas norāda uz inficētām iekārtām.



2. attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem 2013.gadā.

Gada beigās reģistrēto zemas prioritātes incidentu apjoms ir būtiski pieaudzis, salīdzinot gan ar iepriekšējiem ceturkšņiem, gan ar 2012.gada beigām, jo 2013.gada 4.ceturksnī Latvijā tika

izvērstas vairākas kiberuzbrukumu kampaņas, kas tika mērķētas tieši uz Latvijas interneta lietotājiem, kā arī Latvijai nepaslīdēja garām starptautiskas kibernoziedznieku aktivitātes, kuru mērķis bija gūt labumu no pieejamajiem resursiem, neatkarīgi no to atrašanās vietas. Kā piemēru starptautiskām aktivitātēm var minēt ZeroAccess robotu tīkla (botnet) izplešanos virtuālās naudas *bitcoin* ģenerēšanas nolūkos, jo gada pēdējā ceturksnī *bitcoin* piedzīvoja strauju vērtības kāpumu.

CERT.LV turpina iepriekšējā gadā uzsākto izķēmoto mājas lapu uzskaiti. 2013.gada laikā CERT.LV konstatēja 1744 izķēmotu mājas lapu gadījumus.

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". 2013.gada laikā saprašanās memorandu parakstīja SIA Lattelecom, SIA FirstHost un SIA Datnet, pievienojoties 11 jau esošajiem atbildīgajiem IPS.

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

2013.gadā CERT.LV komanda novērsa un koordinēja visdažādāko IT drošības incidentu novēršanu. Pārskata periodā CERT.LV sadarbojās ar dažādām valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām konkrētu, dažādas bīstamības incidentu risināšanā.

CERT.LV ir veikusi arī ievainojamību un ielaušanās testus vairākās iterācijās virknei IT resursu valsts sektorā. Par rezultātiem un atklātajām ievainojamībām katras iestādes atbildīgajam par IT drošību tika nosūtīts oficiāls CERT.LV ziņojums un sniegti ieteikumi, kā šīs ievainojamības novērst. Diemžēl bija sastopami arī gadījumi, kad no attiecīgās iestādes tika saņemta atbilde, ka novēršana nav iespējama, jo iestādei nav nepieciešamo resursu un kompetences.

Lielāko sabiedrības un mediju uzmanību pārskata periodā izpelnījās šādi incidenti:

- ***Hakeru grupas, kas sevi dēvē par "Indonēzijas hakeriem" uzbrukums***
  Gada 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.

- ***Prettiesiskas darbības portālā Draugiem.lv***
  Draugiem.lv portālā krāpnieks, vai krāpnieku grupējums, iespējams, no Lielbritānijas, veica prettiesiskas darbības vairāku mēnešu garumā. Krāpnieku darbības shēma bija šāda: krāpnieki izveido pikšķerēšanas tīmekļa vietnes, ar kuru starpniecību iegūst kontroli pār kāda draugiem.lv portāla lietotāja kontu; no kompromitētā konta tiek izsūtītas vēstules visiem personas draugiem, kurā tiek piedāvāts iegādāties jaunu glāstvirsmas telefonu par ļoti pieņemamu cenu. Nauda jāpārskaita uz it kā drauga kontu. Kad nauda pārskaitīta, upuris, protams, pie kārotās preces netiek.

Šī metode tika izmantota gan lietotāju kontu kompromitēšanai, gan finansiāla labuma gūšanai. Tā NAV ievainojamība, vai drošības trūkums draugiem.lv portālā, bet gan sociālās inženierijas izmantošana uzbrukuma veikšanai. CERT.LV sadarbībā ar ārvalstu iestādēm periodiski panāca kaitīgo resursu atslēgšanu, kā arī sadarbojās incidenta risināšanā ar Valsts policiju.

- ***Ielaušanās Nodarbinātības valsts aģentūras tīmekļa vietnē www.nva.gov.lv***
  7.oktobrī tika konstatēta ielaušanās Nodarbinātības valsts aģentūras tīmekļa vietnē www.nva.gov.lv, kad hakeru uzbrukuma rezultātā tika nopludināti aptuveni 3000 portālā reģistrēto lietotāju dati (lietotājvārds, e-pasts, parole), kā arī portāla administratoru lietotājvārdi un paroles. Uzbrukumā tika izmantoti starpniekserveri, lai nodrošinātu uzbrucēja identitātes slēpšanu. CERT.LV sniedza detalizētas rekomendācijas Nodarbinātības valsts aģentūrai, kā uzlabot savu resursu drošību.

- ***Apdraudējums Latvijas internetbanku lietotājiem jeb tā saucamais „banku vīrus"***
  Oktobrī aktivizējās internetbanku lietotājus apdraudošs datorvīruss (tā saucamais „banku vīruss"). Vīruss pārstāvēja Zeus saimi un bija pielāgots vairāku Latvijā strādājošu banku klientiem. Kaitīgais saturs tika izplatīts ar mēstuļu starpniecību. Vīrusa faili lejuplādei tika izvietoti dažādos bezmaksas failu izvietošanas servisos (files.inbox.lv, dropbox.com, failiem.lv), kā arī uz uzlauztiem serveriem. Uzbrukuma teksta piemēri:

From: Liene <liene.lapina@tesco.com>
Subject: Re:fails

Čau!
Lūdzu steidzami apskaties failu un izsaki savas domas! Gaidīšu atbildi!
http://files.inbox.lv/ticket/<unikāla_simbolu_virkne>/

Liene

3. attēls –„banku vīrusa" uzbrukuma teksta piemērs

vai

FROM: janis.berzins@dell.com
Subject: Re:dokuments

Čau,
Steidzami apskaties failu un dod ziņu! ...mums jārisina tā lieta steidzami! 8 - 17

http://files.inbox.lv/ticket/<unikāla_simbolu_virkne>/

Jānis

4. attēls –„banku vīrusa" uzbrukuma teksta piemērs

Šajā uzbrukumu kampaņā uzbrucēji izmantoja lielu skaitu IT servisu un resursu gan Latvijā, gan ārvalstīs. Uzbrukums vērtējams kā rūpīgi gatavots. Ļaunatūras analīzes rezultāti liecināja, ka konkrētā uzbrukumu kampaņa visdrīzāk tika nopirkta kā serviss. Incidenta risināšanā CERT.LV sekmīgi sadarbojās ar vairākām bankām, inbox.lv,

failiem.lv un dropbox.com pārstāvjiem, kā arī daudziem citiem, kuru resursi nesankcionēti izmantoti kā uzbrukuma sastāvdaļa. Informācija par kampaņu tika nodota policijai.

- ***„Policījas vīrusa" tīmekļa versijas pikšķerēšanas kampaņa***
  Oktobrī tika plaši izvērsta "policijas vīrusa" tīmekļa versijas pikšķerēšanas kampaņa. Ekrānšāviņš:

5. attēls –„Policījas vīrusa" tīmekļa versijas ekrāna momentuzņēmums.

Kaitīgā satura piegādei tika izmantota apmeklētāja pārvirzīšanas funkcionalitāte, pielietojot javascript. Lietotāji uz pikšķerēšanas vietni tika novirzīti, izmantojot baneru servisus apšaubāmos portālos, kas piedāvā filmu skatīšanos tiešsaistē. Veicot incidenta analīzi, CERT.LV atklāja, kā bez specifiskām tehniskām zināšanām novērst ļaundabīgā koda izraisītās sekas, atgūstot kontroli pār inficēto iekārtu. Lai arī veicamās darbības ļauj atsākt datora lietošanu, tās nav uzskatāmas par garantiju, ka dators ir drošs. Analīzes procesā tika noskaidroti visi iespējamie domēnu vārdi, kurus uzbrucēji var izmantot. Sadarbībā ar ārvalstu kolēģiem un spamhaus.org projektu liela daļa kaitīgo domēnu tika atslēgti. Par incidentu tika demonstrēts arī sižets TV3 raidījumā „Bez Tabu".

- ***NATO mācību „Steadfast Jazz 2013" laikā notikušie kiberuzbrukumi***
  Novembrī NATO mācību „Steadfast Jazz 2013" laikā notika virkne kiberuzbrukumu, kuru mērķis bija paust neapmierinātību ar NATO, ES, un to dalībvalstu politiku. Uzbrucēji sevi dēvēja par Anonymous Ukraine, taču uzbrucēju saistība ar šo valsti nav pierādāma. Uzbrukumu kampaņā tika kompromitēta un izķēmota kāda Latvijas medija tīmekļa vietne. Uzbrucēji uzlauztajās tīmekļa vietnēs atstāja paziņojumu NATO vārdā,

tādejādi cenšoties diskreditēt gan pašu organizāciju, gan tobrīd notiekošās mācības „Steadfast Jazz 2013".

WEBSITE HAS BEEN SUSPENDED

Security policy of the website does not meet the requirements of NATO Cooperative Cyber Defence Centre of Excellence

Steadfast Jazz 2013

If you are a visitor to this website, please access this page later

6. attēls – „Steadfast Jazz 2013" kiberuzbrukumu kampaņas laikā kompromitētas vietnes momentuzņēmums.

Kampaņas ietvaros tika izsūtītas arī dezinformējošas e-pasta vēstules NATO Cooperative Cyber Defence Centre of Excellence vārdā virknei valsts iestāžu, kā arī veikti vairāki nesekmīgi uzbrukumu mēģinājumi valsts iestāžu mājas lapām.
CERT.LV incidenta risināšanu koordinēja ar kolēģiem Lietuvā un Igaunijā. Tika konstatēts, ka uzbrukumi veikti no vairākām IP adresēm Krievijā, taču tas vēl nav uzskatāms par pamatu secinājumam, ka uzbrukumu organizatori atrodas tieši Krievijā. CERT.LV no Krievijas CERT vienībām atbildes netika saņēmusi.

- ***Datorvīruss banku datu izkrāpšanai jeb tā saucamais „VID vīruss"***
  Decembrī tika konstatēta jauna Citadel saimes datorvīrusa izplatīšanas kampaņa, kas domāta atsevišķu Latvijā strādājošu banku pieejas datu zādzībai. Konkrētais datorvīruss zināms arī kā „nodokļu vīruss" vai „VID vīruss", jo krāpnieciskajās vēstulēs tika izmantoti sociālās inženierijas paņēmieni ar atsauci uz Valsts ieņēmumu dienestu (VID). „VID vīrusa" aktivitātes turpinās arī 2014.gada pirmajā ceturksnī. Uzbrukuma teksta piemērs:

Subject: Sudziba nodoklu dienestam

Labdien! Informacija par sudzibu nosutita nodoklu dienestam, nosutu Jums kopiju, skatit pielikuma. Ref id: 1494et4b95

1 attachment: nodokludienestam.doc.zip

7. attēls –„VID vīrusa" uzbrukuma teksta piemērs

Papildus minētajiem, kā būtiski pārskata periodā minami arī šādi incidenti:

- Aprīļa sākumā pasaule piedzīvoja, iespējams, apjomīgāko servisa atteices (DDoS) uzbrukumu interneta vēsturē. Uzbrukuma laikā uzģenerētās datu plūsmas apjoms pārsniedza 300.00 Gb sekundē. Uzbrukumu kampaņu ar nosaukumu "Stophaus" organizēja mitinātājkompānija (hosting company) „Cyber bunker", kuras uzņēmējdarbība bija balstīta uz prettiesisku rīcību Nīderlandē. Uzbrukumu kampaņa primāri tika vērsta pret mēstuļotāju melno sarakstu uzturētāju "Spamhaus", kas centās

ierobežot "Cyber bunker" nelikumīgo rīcību, taču infrastruktūras īpatnību dēļ uzbrukumā cieta vairākas valstis, kuras uztur „Spamhaus" spoguļserverus, un interneta sabiedrība kopumā. Arī Latvija piedzīvoja uzbrukumu, mērķētu uz Spamhous spoguļserveri, kura apjoms pārsniedza 6.00 Gb sekundē. CERT.LV veica šī incidenta koordinētu risināšanu un uzbrukuma datu analīzi, kuras rezultātā tika identificēti 20 000 nedroši konfigurēti DNS serveri, kas izmantoti uzbrukumā. Apkopotā informācija tika izsūtīta pasaules CERT kopienai, kurā ir uzsāktas vairākas iniciatīvas globālā riska samazināšanai.

- Aprīļa sākumā vairākkārtīgi notika servisa atteices (DoS) uzbrukumi pret vairākām Latvijā strādājošām bankām. CERT.LV piedalījās incidenta risināšanā un analīzē, kā arī veica incidenta risināšanas koordinēšanu ar interneta pakalpojumu sniedzējiem.
- Maija beigās CERT.LV, veicot kāda incidenta analīzi, atklāja unikālu robotu tīklu, kas sastāvēja no ~1500 iekārtām un kurā izmantotā komandu un kontroles programmatūra līdz šim nav tikusi citur novērota.
- Augusta sākumā vairākas valsts iestādes un uzņēmumi savos e-pastos saņēma viltus MMS paziņojumus LMT un TELE2 vārdā, kuri saturēja pielikumu ar ļaunatūru. Viltus e-pasti nesaturēja nekādu tekstu, tikai arhīva failu pielikumā (piem., mms52439929.zip), kuru atverot lietotāja dators tika inficēts ar vīrusu. Par incidentu tika informēti pakalpojumu sniedzēji. Veicot incidenta analīzi sadarbībā ar LMT drošības dienestu, tika konstatēts, ka e-pastu sūtītāja lauki ir viltoti, un šie lietotāji šādas ziņas nav sūtījuši. Krāpnieciskie e-pasti tikuši izsūtīti no IP adreses Nīderlandē. CERT.LV veica nepieciešamos soļus incidenta risināšanā, sazinājās ar ārvalstu CERT komandām un informēja sabiedrību.

Augustā un septembrī notika vairāki mērķēti IT drošības uzbrukumi Latvijas valsts iestāžu darbiniekiem. Kaitīgais saturs tika nogādāts ar e-pasta starpniecību, kas noformēts ar Sīrijas konflikta tematiku vai citām starptautiskām aktivitātēm, kurām sabiedrība pievērš pastiprinātu uzmanību. Uzbrukumu mērķi tika identificēti sadarbībā ar atbilstošo valsts iestāžu IT drošības darbiniekiem. Uzbrukuma ietekme un iespējamais kaitējums tika apzināti un veikti preventīvi pasākumi to novēršanai. CERT.LV uzsvēra lietotāju izglītošanas nozīmi šādu incidentu sekmīgai apkarošanai.

Tendences un nākotnes plāni

IT drošības līmeņa uzlabošanai valstī ir jāturpina darbs pie sabiedrības izglītošanas IT drošības jomā, uzsverot, ka par savu drošību IT vidē ir jārūpējas ikvienam. 2013.gada nogalē par sabiedrības izglītošanu IT drošības jomā iniciatīvu un interesi izrādījušas arī vairākas nevalstiskās organizācijas un asociācijas. CERT.LV plāno 2014.gada laikā uzsākt īpašu sadarbības programmu ar tām iestādēm vai privātpersonām, kas vēlas piedalīties sabiedrības informēšanā.

2013.gads spilgti iezīmējās ar vairākām lielām kiberuzbrukumu kampaņām, kas tēmētas tieši uz Latvijas interneta sabiedrību un atbilstoši pielāgotas. Līdzīgas kampaņas, iespējams pat vēl lielākā skaitā, sagaidāmas arī 2014.gadā.

Arvien biežāk, izmeklējot IT drošības incidentus, CERT.LV ir nonākusi pie secinājuma, ka iestādēm nav pieejama pagātnes informācija, kas ļautu identificēt konkrētās uzbrukumā iesaistītās iekārtas vai apstiprināt inficēšanās faktus. 2014.gadā CERT.LV strādās pie agrās brīdināšanas sistēmas izveides, kas nodrošinās reāla laika valsts iestāžu tīkla datu plūsmas apkopošanu, arhivēšanu un analīzi, kā arī tiešsaistes brīdinājumus par iespējamiem informācijas tehnoloģiju incidentiem. Tādējādi tiks būtiski uzlabota valsts preventīvā spēja, paātrinot un veicinot bīstamu incidentu identificēšanu, novēršanu un laicīgu atrisināšanu.

2014.gadā CERT.LV plāno arī pastiprināti testēt valsts un pašvaldību IT resursus, lai varētu labāk sagatavoties 2015.gada ES Prezidentūrai. Tāpat kā līdz šim CERT.LV saskata problēmas un būtiskas aiztures atklāto ievainojamību novēršanas procesā, kas visbiežāk saistītas ar nepietiekamu finansējumu.

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

CERT.LV uztur tīmekļa vietni https://cert.lv, kurā publicē informāciju par aktuālām ievainojamībām un apdraudējumiem, padomus, kā izvairīties no incidentiem, kā tos atklāt un kā novērst sekas, ja incidents radies. Pārskata periodā CERT.LV tīmekļa vietnē publicētas 88 jaunas ziņas, kā arī izveidota jauna sadaļa, kas veltīta Kiberaizsardzības vienības jautājumiem. Vietnē tiek publicēts arī IT drošības semināru un pasākumu grafiks un aktuālāko notikumu apskats.

Iegūt operatīvu informāciju par jauniem vīrusiem un ievainojamībām, kā arī iesaistīties sarunās par dažādām ar IT drošību saistītām tēmām var CERT.LV Twitter plūsmā https://twitter.com/certlv un https://twitter.com/datorologs, Facebook lapā http://www.facebook.com/certlv un draugiem.lv lapā http://www.draugiem.lv/certlv/.

Portālā https://www.esidross.lv/ CERT.LV eksperti un DEG (Drošības ekspertu grupas) biedri gatavo informāciju par aktuālām tēmām un ievainojamībām IT ne-speciālistiem, kā arī atbild uz rakstu komentāros uzdotajiem lasītāju jautājumiem. 2013.gadā portālā publicēti 25 raksti.

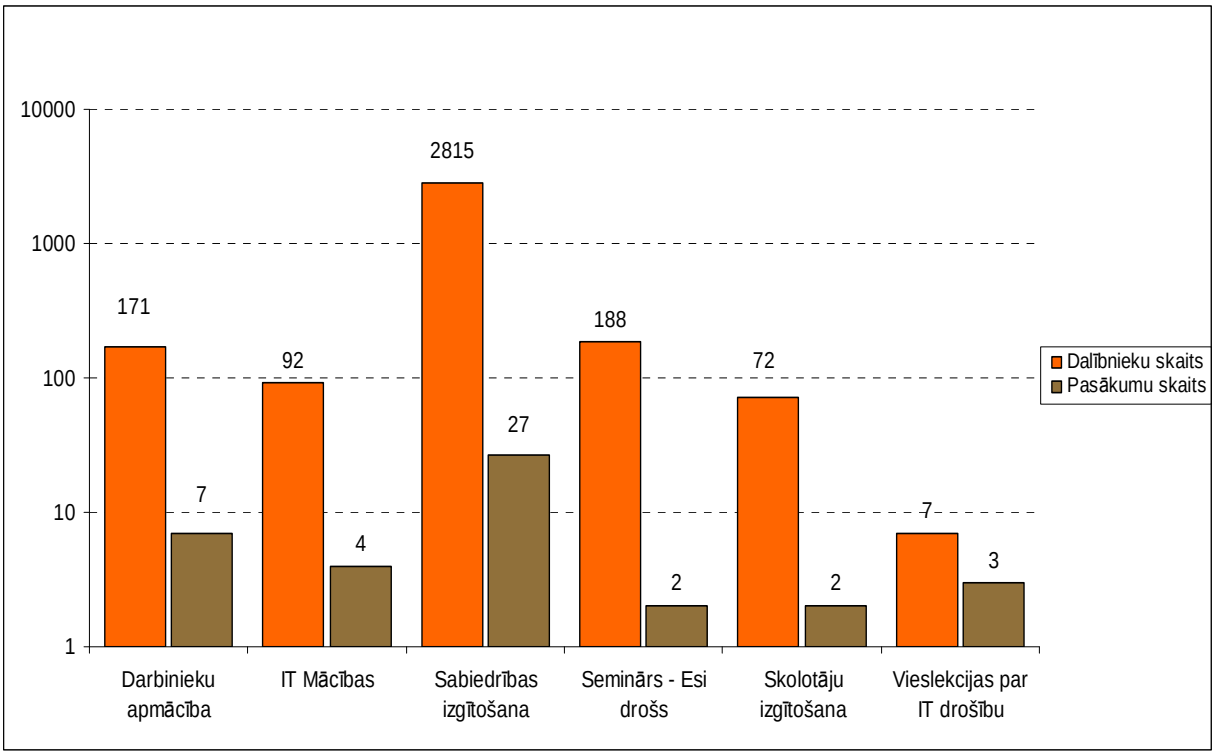
Portāls arī 2013.gadā piedāvāja iespēju pārbaudīt, vai lietotāja IP adrese, ar kuru tas ienācis portālā, ir iekļauta to IP adrešu sarakstā, kas norāda uz inficētām iekārtām. Ja attiecīgā IP adrese ir CERT.LV reģistrēto inficēto iekārtu IP adrešu sarakstā, ekrāna augšmalā parādās paziņojums par infekciju un saite uz ieteikumiem par to, kā no infekcijas atbrīvoties (8.attēls).

8. attēls – Portāla esidross.lv ekrāna momentuzņēmums ar paziņojumu par inficētu IP adresi.

Par aktuālākajiem notikumiem Latvijas virtuālajā telpā aktīvi tika informēti arī masu mediji – tika sniegti komentāri par IT drošības incidentiem, izplatīti brīdinājumi par datorvīrusiem un sniegti padomi par privāto datu aizsardzību un IT drošību.

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

2013.gadā CERT.LV organizēja 45 informatīvi-izglītojošus pasākumus, kurus apmeklēja 3345 dalībnieki (9. attēls).



9. attēls – Informatīvi-izglītojošie pasākumi 2013.gadā, kurus organizēja CERT.LV.

Gada sākumā 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 CERT.LV apmeklēja vairākas skolas un vadīja IT drošības lekcijas skolēniem, bet E-prasmju nedēļā laika 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.

Aprīlī un decembrī CERT.LV organizēja semināru „Esi drošs-2", kas bija paredzēts valsts un pašvaldību iestāžu par IT drošību atbildīgajām personām, kā arī citiem interesentiem, kas darbojas IT drošības jomā. Aprīļa seminārā tika aplūkotas problēmsituācijas un ieteikumi IT iepirkumu jomā, fizisko personu elektroniskās identifikācijas likuma nianses, sociālās inženierijas izmantošana IT vidē, sniegts ievads urķuslazdos un diskutēts par profesiju standartu. Savukārt decembra seminārā tā dalībnieki tika iepazīstināti ar IT drošības aktualitātēm Latvijā, sīkdatņu izmantošanas un privātās informācijas aizsardzības principiem, atvērto datu būtību, dažādiem ārpakalpojumu izmantošanas aspektiem un citiem aktuāliem tematiem gan CERT.LV speciālistu, gan vieslektoru prezentācijās.

Aprīlī CERT.LV organizēja video lekciju skolām par mobilo iekārtu drošību. Šī bija pirmā šāda veida lekcija, kurā dalībnieki varēja vērot lekciju tiešsaistē un lekcijas laikā nosūtīt lektoriem jautājumus, uz kuriem lektori sniedz atbildes lekcijas beigās. Tiešraidei pieslēdzās 12 skolas un lekciju noskatījās 427 skolēni.

Oktobris tika aizvadīts Eiropas Kiberdrošības mēneša zīmē, kura ietvaros norisinājās Datorologa akcija, notika ISACA Latvijas nodaļas un CERT.LV organizētā IT drošības konference "Mūsu informācijas drošība - nākotnes panākumu atslēga" (kuru apmeklēja vairāk kā 400 dalībnieki), kā arī CERT.LV organizētais seminārs IT drošības speciālistiem par sociālo tīklu izmantošanu mērķētu uzbrukumu veikšanai, kuru vadīja vieslektori no ENISA (European Network and Information Security Agency).

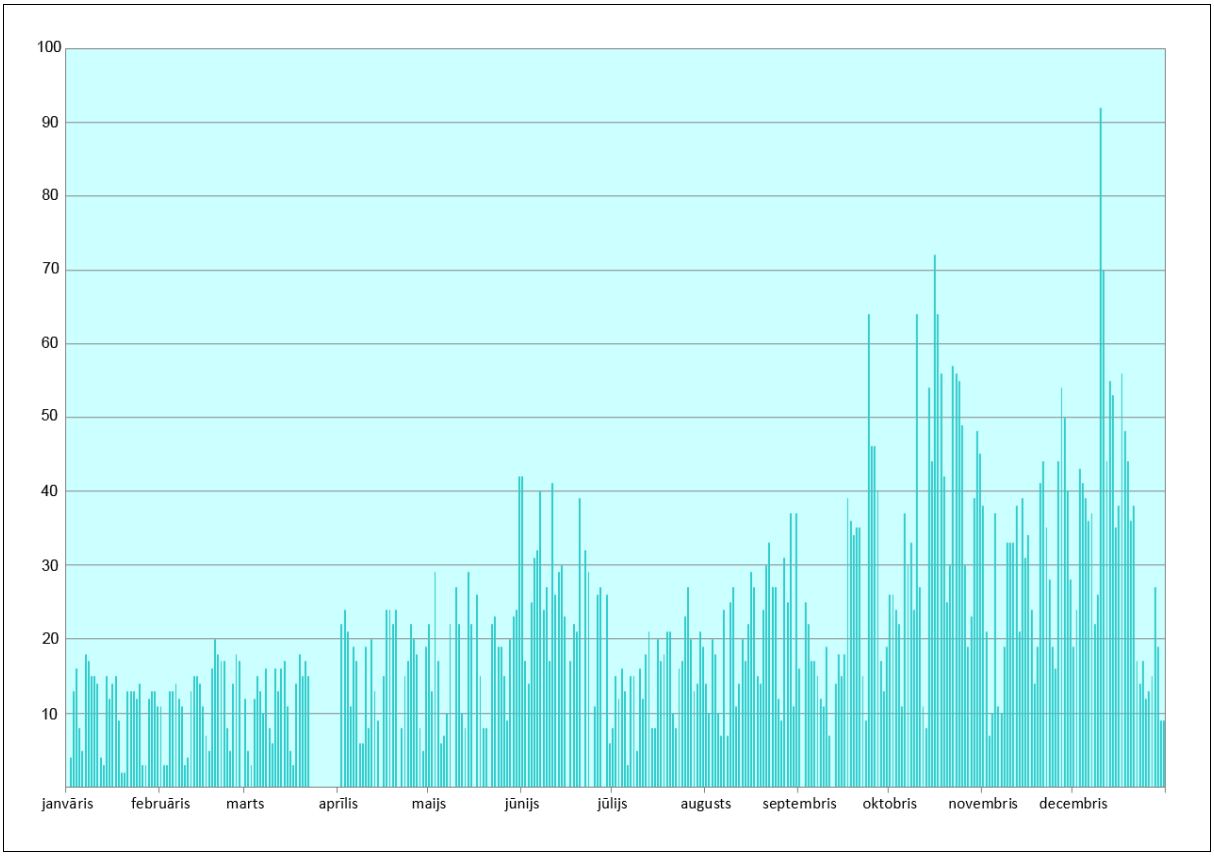
Kiberdrošības mēneša ietvaros CERT.LV speciālisti apmeklēja arī vairākas skolas un iepazīstināja skolēnus ar IT drošības pamatprincipiem, kas jāievēro, lietojot datorus un viedtālruņus gan komunikācijai sociālajos tīklos, gan veicot citas darbības internetā.

5. **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 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. Ja CERT.LV fiksē inficētas valsts un pašvaldību institūciju IP adreses, tad attiecīgo institūciju par IT drošību atbildīgie tiek par inficēšanās faktu laicīgi brīdināti. 2013.gadā CERT.LV valsts un pašvaldību institūcijās reģistrēja 853 unikālas IP adreses, kas norādīja uz inficētām iekārtām.

Desmitajā attēlā ir redzams, cik daudz valsts un pašvaldību institūcijās esošo inficēto iekārtu IP adreses bijušas katras dienas saņemtajos ziņojumos no dažādiem ziņošanas avotiem. Vidēji dienā tika reģistrētas 22 šādas IP adreses. Maksimālais vienā dienā reģistrētais inficētu valsts un pašvaldību iekārtu IP skaits bija 92 IP adreses.

2013.gada nogalē palielinājies arī to inficēto IP adrešu daudzums, kas reģistrētas valsts un pašvaldību iestādēs. Arī šis pieaugums skaidrojams ar virkni Latvijas kibertelpā izvērsto noziedzīgo kampaņu, kuru mērķis bija inficēt datorus un izgūt lietotāju datus.



10. attēls – Valsts un pašvaldību institūciju IP adrešu skaits, kas reģistrētas 2013.gada incidentu ziņojumos.

Lai veicinātu IT drošību valsts un pašvaldību iestādēs, 2013.gadā CERT.LV konsultēja virkni valsts un pašvaldību iestādes par kļūdām viņu mājas lapās un to satura vadības sistēmās, palīdzēja novērst incidentus, kuros lapas tika uzlauztas un izķēmotas, kā arī sniedza palīdzību dažādu citu incidentu novēršanā. Taču viens no joprojām izplatītākajiem incidentiem ir augstas prioritātes institūciju iekārtu nonākšana robotu tīklos. Pārskata periodā robotu tīklos nonākušas 1485 šādas iekārtas.

CERT.LV 2013.gadā, lai apspriestu sadarbības iespējas un dalītos pieredzē, tikās ar Centrālās Statistikas pārvaldi, Eiropas Savienības prezidentūras biroju, Valsts kontroli un Latvenergo.

CERT.LV veica arī konsultatīvo darbu valsts institūcijās ar IT drošību saistītu normatīvo aktu un citu dokumentu izstrādē. CERT.LV pārstāvji piedalījās Elektronisko sakaru likuma izmaiņu apspriešanā saistībā ar IP adrešu bloķēšanu, kā arī tikās ar VARAM, lai diskutētu par risinājumiem Tautas nobalsošanai. Savukārt ar Aizsardzības ministrijas valsts sekretāru J.Sārtu un nevalstiskajām organizācijām tika pārrunāta IT drošības stratēģija.

Pārskata periodā CERT.LV iesaistījās vairākās Vides un reģionālās attīstības ministrijas (VARAM) vadītajās darba grupās, proti, darba grupās „Par Informācijas sabiedrības attīstības pamatnostādņu 2014.-2020.gadam izstrādi", „Par uzticamu sertifikācijas pakalpojumu sniedzēju (USPS) pārraudzību un kontroli", „Par Uzraudzības iestādes veidošanu". Kā arī CERT.LV piedalījās Satiksmes ministrijas vadītajā darba grupā „Par interneta vēlēšanām".

2013.gada laikā CERT.LV ir piedalījies vairākās sanāksmēs, apspriežot ar IT drošību saistītus būtiskus jautājums. CERT.LV ir piedalījies sanāksmē par iniciatīvu veidot vienotu valsts iestāžu tīmekļa vietņu satura vadības sistēmu, sanāksmē par ES prezidentūras drošības jautājumiem, sanāksmē par NetSafe projekta nākotni, Satiksmes ministrijas organizētajā

sanāksmē „Par kaitīgu saturu elektroniskās informācijas telpā", Aizsardzības ministrijas organizētajā sanāksmē par Kiberjaunsardzes izveidošanu un citās.

CERT.LV ir pārstāvēts Nacionālajā IT drošības padomē un regulāri piedalās padomes sēdēs ar ziņojumiem par IT drošības situāciju valstī. Kā arī CERT.LV piedalījās Nacionālās IT drošības padomes organizētajā tikšanās ar nevalstisko organizāciju pārstāvjiem, lai apspriestu ES IT drošības stratēģiju un topošo direktīvu un citus jautājumus.

6. **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.decembrim CERT.LV apkopoja informāciju par 610 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību.

CERT.LV veic regulāru komunikāciju ar valsts un pašvaldību iestādēm, informējot tās par aktuālajiem draudiem un ievainojamībām, kā arī par iespējām apmeklēt seminārus un citus izglītojošos pasākumus.

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, ka Elektronisko sakaru komersantiem (ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai, kā arī nosaka kārtību, kādā tas veicams. Līdz 2013.gada 31.decembrim rīcības plānus iesnieguši 55 ESK. Mazajiem ESK ir pieejams CERT.LV izstrādāts Rīcības plāna paraugs, lai palīdzētu tiem izveidot savu plānu.

7. **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.

Lai atvieglotu starptautisko incidentu risināšanu, pārskata periodā notika sadarbības tikšanās ar Ungārijas CERT. Savukārt, sadarbojoties ar ASV kolēģiem, notika informācijas apmaiņa un sadarbība DDoS uzbrukuma novēršanā un ar spiegu tīkliem saistītu incidentu risināšanā.
Būtiski atzīmēt, ka maija beigās CERT.LV pārstāvis piedalījās TF-CSIRT konferencē Bukarestē, Rumānijā. Konferences laikā tika panāktas vairākas vienošanās par incidentu informācijas apmaiņu ar citu valstu CERT komandām. Kā arī CERT.LV izpelnījās atzinīgu novērtējumu no Team Cymru kā valsts, kurā panākts datorinfekciju samazinājums.
Aprīlī CERT.LV piedalījās telefonkoferencē ar EU-CERT par savstarpējo sadarbību, bet septembrī CERT.LV papildināja incidentu informācijas apmaiņu ar starptautiskajiem partneriem, nodrošinot datu apmaiņu no Latvijā iegūtās informācijas par *Citadel banking trojan* upuriem. CERT.LV ieguldījums tika atzinīgi novērtēts no The Shadowserver Foundation.

Virknē starptautisku konferenču un sanāksmju CERT.LV sniedza prezentācijas, piedalījās tehniskajos semināros, debatēs, kā arī apmainījās ar pieredzi un viedokļiem par IT drošību un

aizsardzību. Piemēram, CERT.LV pārstāvji regulāri piedalās TF-CSIRT, FIRST, Trusted Introducer un ENISA rīkotajās sanāksmēs un semināros. CERT.LV piedalījās arī gadskārtējā nacionālo CSIRTu sanāksmē un FIRST konferencē. FIRST konferencē CERT.LV pārstāvis vadīja vienu no "*Policy and Management*" sesijām, bet nacionālo CSIRTu sanāksmē CERT.LV pārstāvji sniedza prezentāciju "*Responsible ISPs - developing cyber security capabilities in Latvian networks*".

Lai sekmētu starptautisko sadarbību un nodrošinātu Latvijas gatavību atvairīt IT drošības uzbrukumus, CERT.LV aktīvi iesaistījās virknē starptautisku IT drošības mācību. Kā nozīmīgākās no tām var minēt NATO līmeņa IT drošības mācības „Cyber Coalition 2013".

Vēl 2013.gadā CERT.LV startēja organizatoru „baltajā komandā" NATO IT drošības mācībās „Locked Shields", kā arī piedalījās ENISA rīkotajā Eiropas līmeņa mācību plānošanas konferencē, lai uzsāktu sagatavošanos IT drošības mācībām "Cyber Europe 2014" un pārrunātu šī gada "EURO SOPEX" mācību izpildi.

CERT.LV piedalās projektā BAITSE (Baltic Academic IT Security Exchange), kura ietvaros CERT.LV pārstāvis vadīja lekcijas Zviedrijā un Polijā.

8. Veikt citus normatīvajos aktos noteiktos pienākumus.

Pārskata periodā regulāri notika Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupu (DEG) sanāksmes. DEG ir brīvprātīga drošības ekspertu grupa, kuras mērķis ir veicināt IT/IS drošību, drošības apziņas kultūru Latvijas Republikā un sniegt atbalstu CERT.LV.

Lai pārrunātu iespējamo sadarbību sabiedrības izglītošanas jomā un IT drošības jautājumu popularizēšanā, pārskata periodā notika CERT.LV tikšanās ar Lattelecom. Savukārt, lai pārrunātu IT drošībai veltīta specsemināra plānošanu, notika tikšanās ar LU Datorikas fakultātes pārstāvjiem. Sadarbības tikšanās notika arī ar NetSafe, LIKTA, LATA un SIA „Latnet Serviss" pārstāvjiem.

Martā 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.

Pārskata periodā CERT.LV pārstāvji piedalījās dažādos ar IT drošību saistītos pasākumos. Piemēram, CERT.LV piedalījās žūrijas komisijā NetSafe organizētajā konkursā bērniem par bērniem atbilstošu saturu internetā un Lattelecom organizētās akcijas „Pieslēdzies, Latvija" noslēguma pasākumā.

CERT.LV pārstāvis piedalījās arī LIKTA gadskārtējā konferencē un VARAM organizētajā sanāksmē par Profesiju standartu.

Apkopojums

2013.gadā tika apstrādāti 4964 augstas prioritātes incidenti, fiksēti gandrīz 200 tūkstoši zemas prioritātes incidentu, uzturēts regulārs kontakts ar 610 kontaktpersonām valsts un pašvaldību iestādēs, publicēti 25 raksti portālā esidross.lv un atklāti un apturēti vairāki Latvijas IP adrešu apgabalā uzturēti robotu tīklu komandu un kontroles centri.

CERT.LV organizēja 45 izglītojošus pasākumus, kurus apmeklēja 3345 dalībnieki, organizēja un piedalījās virknē valsts vai starptautiska līmeņa IT drošības mācībās un semināros. Konsultatīvā kapacitātē CERT.LV piedalījās vairākās darba grupās un vairāku ar IT drošību saistītu dokumentu izstrādē.

CERT.LV pateicas par sadarbību Latvijas Republikas Aizsardzības ministrijai, NetSafe Latvia Drošāka interneta centram, DEG biedriem, kā arī visiem pārējiem, kas sniedza savu atbalstu CERT.LV komandai.

Pārskatu sagatavoja – Vilnis Tukums
e-pasts: vilnis.tukums@cert.lv