Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) uzdevumu izpildi 2013.gada 2.ceturksnī

(01.04.2013. – 30.06.2013.)

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

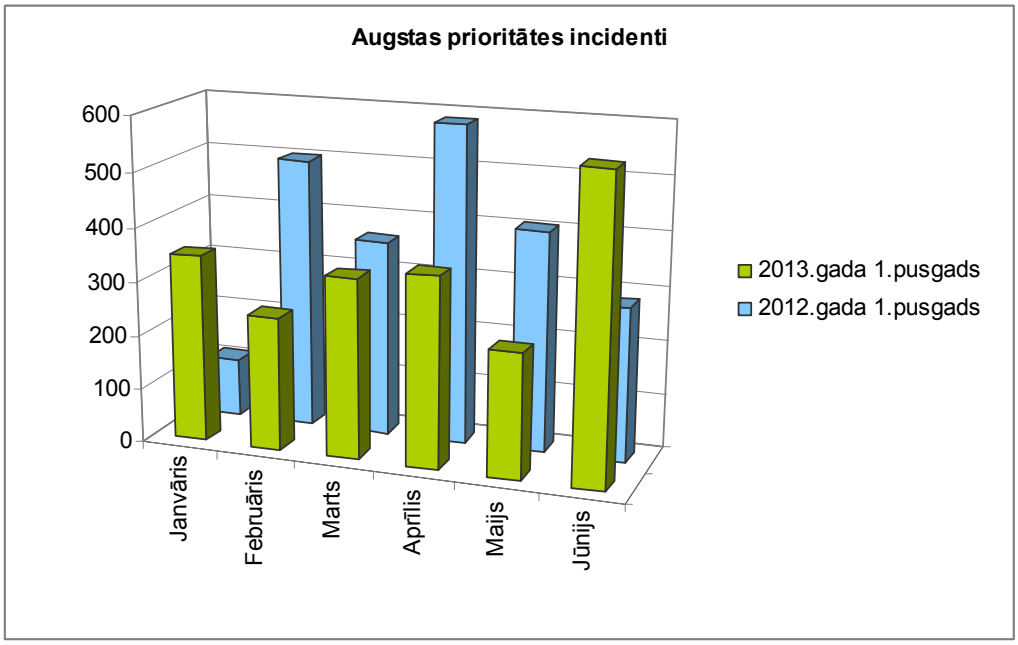
Pārskata periodā CERT.LV ir sācis apstrādāt jaunus ziņojumu avotus, kas nodrošina lielāku no sensoriem saņemto datu apjomu un plašāku informāciju par notikušajiem incidentiem. Papildu ziņojumu avotu izmantošana ir viens no galvenajiem iemesliem, kāpēc ir audzis gan augstas, gan zemas prioritātes incidentu daudzums. Lielākie pasākumi, kas organizēti pārskata periodā, bija „Esi drošs-2" seminārs, kas notika Kara muzejā, un Informācijas aizsardzības seminārs sadarbībā ar NBS Sakaru skolu. Pārskata periodā atrisināti arī daudzi bīstami augstas prioritātes incidenti.

Par augstas prioritātes incidentiem tiek uzskatīti visi iekārtu kompromitēšanas gadījumi, pikšķerēšana, piekļuves lieguma uzbrukumi, 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 izsūta mēstules.

2013.gada 1.ceturksnī tika reģistrēti un apstrādāti 926 augstas prioritātes incidenti, bet 2013.gada 2.ceturksnī 1153 incidenti.

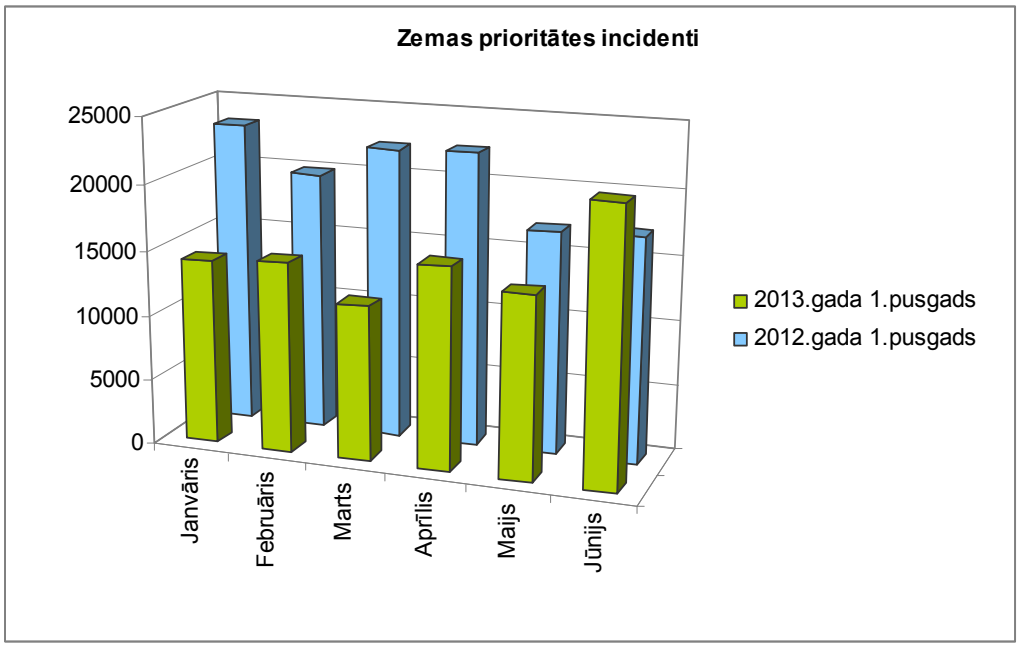
Kā viens no nozīmīgākajiem incidentiem jāuzsver uzbrukums, kas tika vērsts pret mēstuļotāju melno sarakstu uzturētāju "Spamhaus" un bija, iespējams, apjomīgākais servisa atteices (DDoS) uzbrukums interneta vēsturē. No šī uzbrukuma pārskata perioda sākumā cieta arī resursi Latvijā. Pārskata periodā notika arī virkne servisa atteices uzbrukumu Latvijā strādājošām bankām un valsts iestāžu tīmekļa vietnēm. CERT.LV speciālisti veica incidentu analīzi, informācija nodota Valsts policijai. Maija beigās CERT.LV speciālistiem izdevās atklāt unikālu robotu tīklu, kura kontrolei tika izmantota komandu un kontroles programmatūra, kas līdz šim nav tikusi novērota.

Pirmajā attēlā redzams CERT.LV reģistrēto augstas prioritātes incidentu skaits 2013.gada pirmajos sešos mēnešos, salīdzinājumā ar 2012.gada pirmajiem sešiem mēnešiem. Incidentu apjoma straujais kāpums 2013.gada pirmā pusgada beigās skaidrojams ar jaunu ziņojumu avotu izmantošanu un ienākošo ziņojumu apjoma palielināšanos.



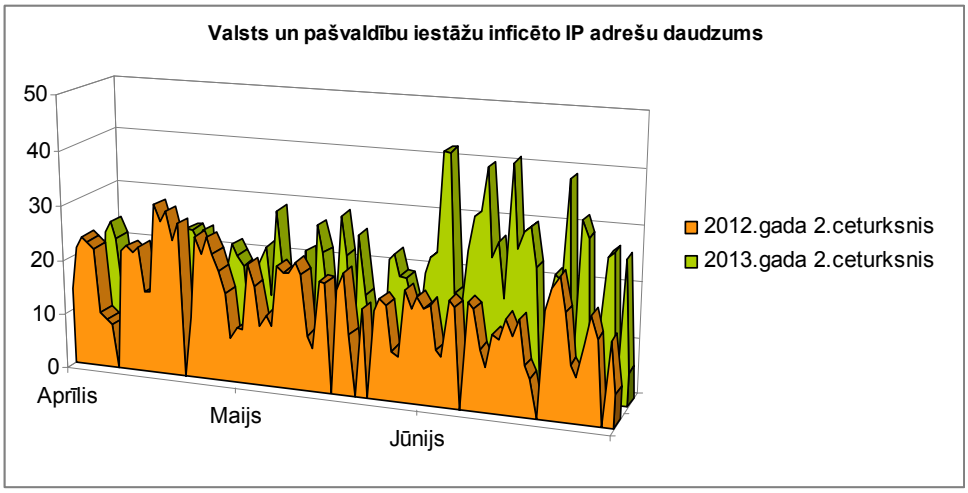
1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pārskata periodā, iepriekšējā periodā un šajā pašā periodā pirms gada.

2013.gada 1.ceturksnī tika reģistrēti 31714 zemas prioritātes incidenti, bet 2013.gada 2.ceturksnī 40721 incidents. Otrajā attēlā redzams CERT.LV reģistrēto zemas prioritātes incidentu skaits 2013.gada pirmajos sešos mēnešos, salīdzinājumā ar 2012.gada pirmajiem sešiem mēnešiem. Arī šeit incidentu apjoma kāpums 2013.gada pirmā ceturkšņa beigās ir saistīts ar jaunu ziņojumu avotu izmantošanu un ziņojumu daudzuma palielināšanos.



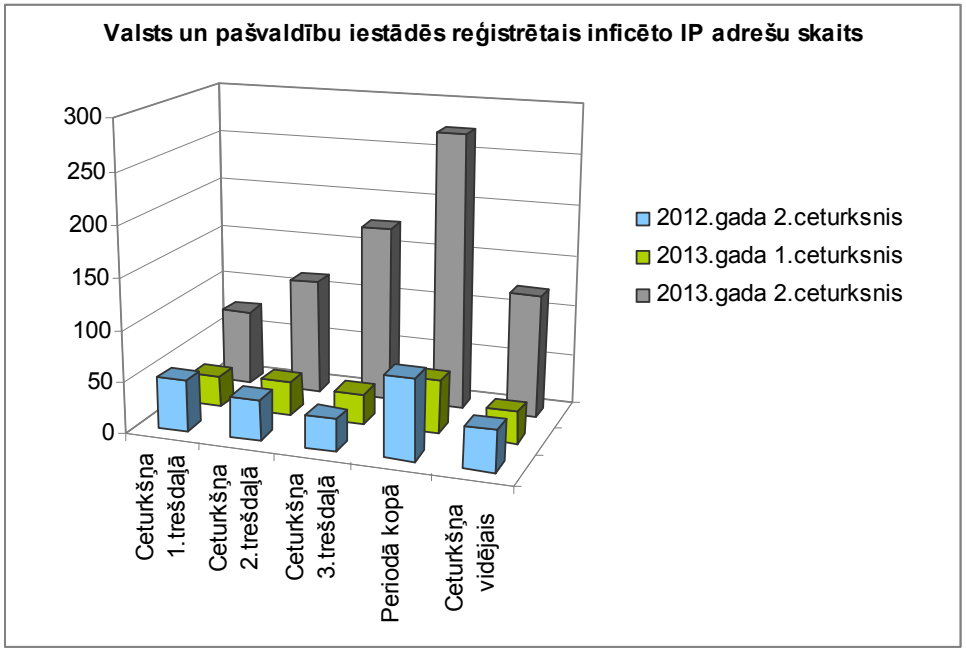
2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā, iepriekšējā periodā un šajā pašā periodā pirms gada.

Palielinājies arī to inficēto IP adrešu daudzums, kas reģistrēts valsts un pašvaldību iestādēs. Arī šis pieaugums saistīts ar papildu ziņojumu avotu izmantošanu un lielāku apstrādājamās informācijas apjomu. Trešajā attēlā redzams valsts un pašvaldību iestādēs reģistrēto inficēto IP adrešu daudzums katras dienas saņemtajos ziņojumos.



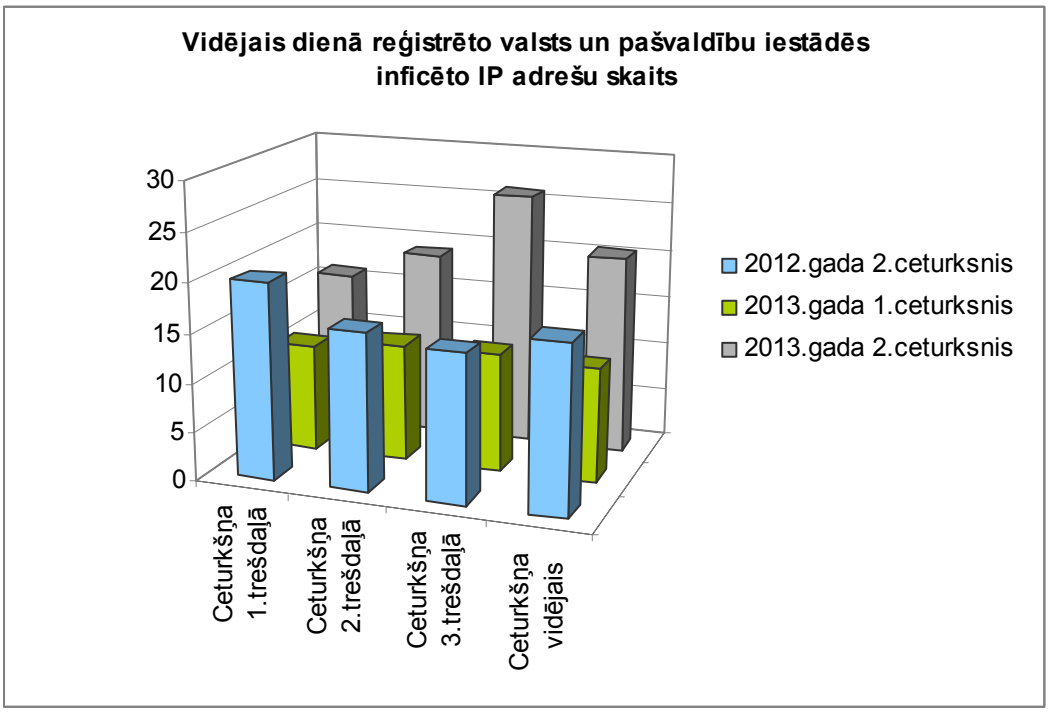
3.attēls – Valsts un pašvaldību iestāžu inficēto IP adrešu daudzums katras dienas saņemtajos ziņojumos pārskata periodā un šajā pašā periodā pirms gada.

2013.gada 1.ceturksnī tika reģistrēti un apstrādāti 53 incidenti, kas saistīti ar valsts un pašvaldību iestādēm, bet 2013.gada 2.ceturksnī šis skaits pieckāršojās, sasniedzot 272 incidentus. Ceturtajā attēlā redzams valsts un pašvaldību iestādēs reģistrēto inficēto IP adrešu skaits pārskata periodā (01.04.2013. – 30.06.2013.), iepriekšējā periodā (01.01.2013. – 31.03.2013.) un šajā pašā periodā pirms gada (01.04.2012. – 30.06.2012.) sadalījumā pa mēnešiem, kopā pa visu periodu, kā arī ir salīdzināms vidējais reģistrēto valsts un pašvaldību inficēto IP adrešu skaits periodā.



4.attēls – Valsts un pašvaldību iestāžu inficēto IP adrešu daudzums pārskata periodā, iepriekšējā periodā un šajā pašā periodā pirms gada.

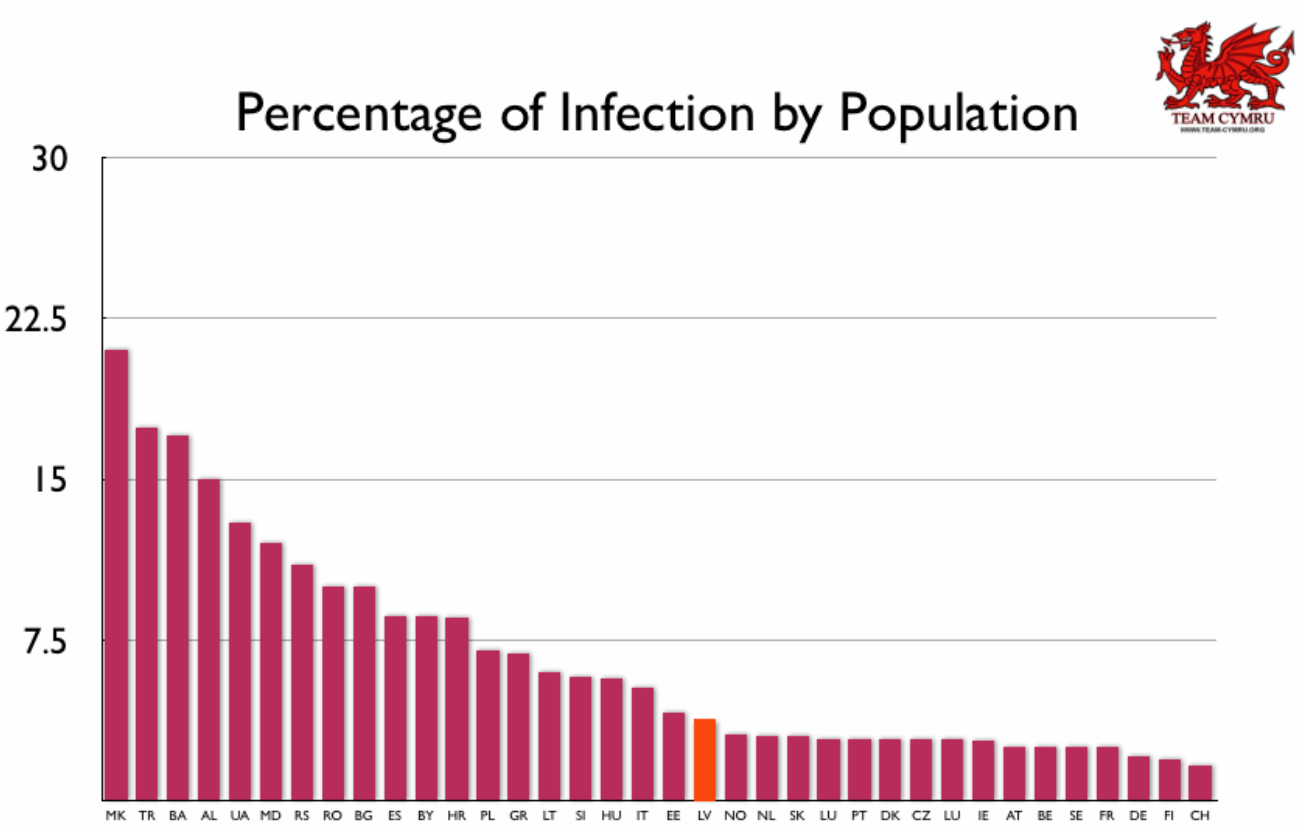
Piektajā attēlā redzams vidējais valsts un pašvaldību iestādēs inficēto IP adrešu skaits, kas parādījās katras dienas saņemtajos ziņojumos, kā arī katra perioda dienas vidējais.



5.attēls – Valsts un pašvaldību iestāžu inficēto IP adrešu skaits, kas parādījās katras dienas saņemtajos ziņojumos pārskata periodā, iepriekšējā periodā un šajā pašā periodā pirms gada.

Gan CERT.LV reģistrēto un apstrādāto augstas, gan zemas prioritātes incidentu skaita pieaugums saistīts ar to, ka veiksmīgas starptautiskas sadarbības rezultātā CERT.LV saviem incidentu ziņojumu avotiem pievienoja vēl divus avotus – Polijas CERT sagatavoto ziņojumu plūsmu un Team Cymru sagatavotos ziņojumus. Tā rezultātā pārskata periodā tika saņemts daudz vairāk informācijas par dažādiem notikušajiem incidentiem, nekā iepriekšējos periodos. Incidentu apjoma pieaugums valsts un pašvaldību iestādēs skaidrojams arī ar to, ka CERT.LV ir ieguvis papildu informāciju par valsts un pašvaldību iestāžu tīkliem un uzturētajām tīmekļa vietnēm, ļaujot efektīvāk identificēt incidentus, kas saistīti ar šiem resursiem.

TF-CSIRT konferencē Bukarestē CERT.LV izpelnījās atzinīgu novērtējumu no Team Cymru par panākto kopējo IT infekciju samazinājumu valstī. Latvija ir ar salīdzinoši zemu infekciju procentuālo sadalījumu uz iedzīvotāju skaitu, ierindojoties 20. vietā, tādā veidā uzrādot no IT drošības viedokļa labākus rādītājus kā kaimiņvalstis Igaunija un Lietuva (6.attēls).



6.attēls – Infekciju procentuālais sadalījums uz iedzīvotāju pa valstīm (Team Cymru dati).

Pārskata periodā lielākie CERT.LV organizētie pasākumi (līdz pat 100 dalībniekiem) bija seminārs „Esi drošs – 2", kas bija paredzēts valsts un pašvaldību iestāžu par IT drošību atbildīgajiem un citiem interesentiem, un Informācijas aizsardzības seminārs, kurā piedalījās tikai valsts un pašvaldību iestāžu darbinieki. 25.aprīlī CERT.LV vadīja video lekciju skolām par mobilo iekārtu drošību, kuru tiešsaistē vēroja 12 skolas (427 skolēni). Pārskata periodā kopumā CERT.LV piedalījās 10 lekcijās un semināros, apmācot 819 cilvēkus, publicēja 9 jaunus rakstus portālā www.esidross.lv, 19 jaunas ziņas portālā www.cert.lv, piedalījās vienā radio pārraidē un trīs televīzijas sižetos.

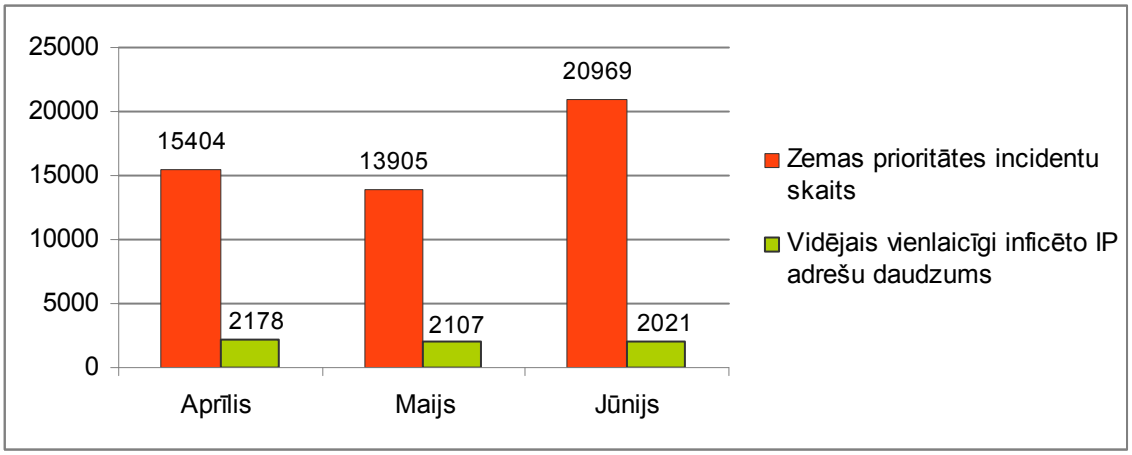
1. Uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu.

2013.gada 2.ceturksnī CERT.LV apstrādāja 1153 augstas prioritātes incidentus, kas ir par 227 incidentiem jeb 25% vairāk nekā šī gada pirmajā ceturksnī. Salīdzinot ar 2012.gada 2.ceturksni, kurā tika reģistrēti un apstrādāti 1274 augstas prioritātes incidenti, pārskata periodā reģistrēto augstas prioritātes incidentu daudzums ir samazinājies par nepilniem 10%.

Arī zemas prioritātes incidentu jomā ir vērojams pieaugums. 2013.gada otrajā ceturksnī CERT.LV reģistrēja 40 721 augstas prioritātes incidentu, kas ir par 9007 incidentiem jeb 22% vairāk nekā šī gada pirmajā ceturksnī, kurā tika reģistrēti 31 714 incidenti. Salīdzinot ar 2012.gada 1.ceturksni, kurā tika reģistrēti 43 489 augstas prioritātes incidenti, pārskata periodā reģistrēto zemas prioritātes incidentu daudzums ir samazinājies par 6%.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Aprīlī šis skaits bija 2178, maijā – 2107, jūnijā - 2021.

7.attēlā redzams, kā mainījies zemas prioritātes incidentu skaits un vidējais inficēto IP adrešu daudzums 2013.gada 2.ceturkšņa laikā.



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

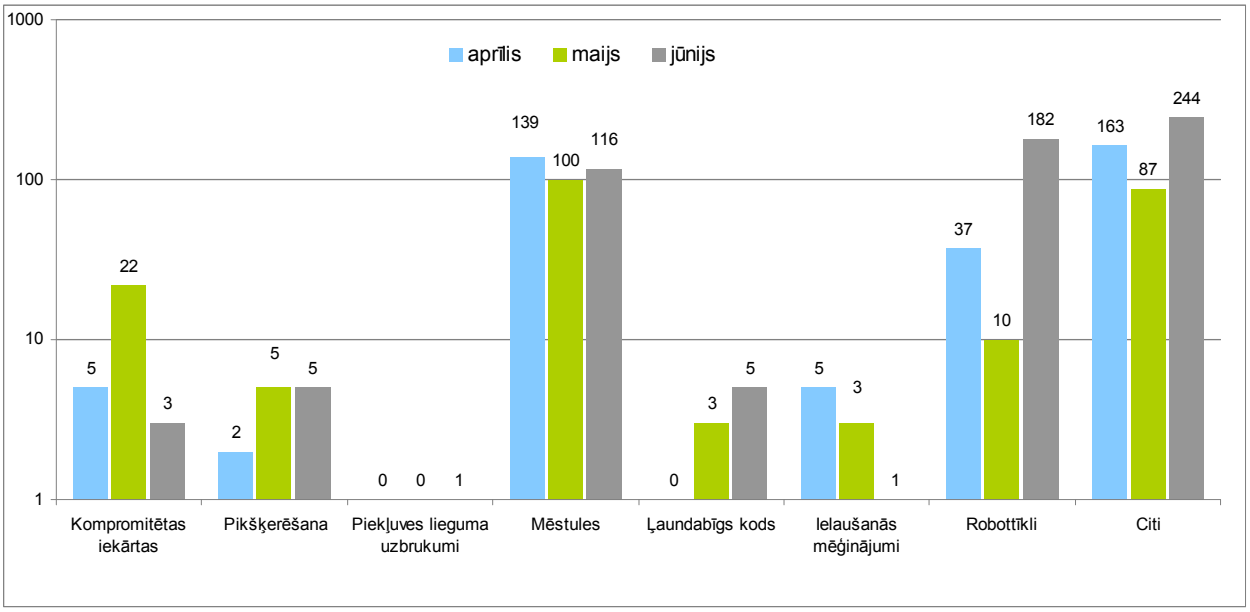
Reģistrēto un apstrādāto incidentu skaita pieaugums pārskata periodā ir skaidrojams ar to, ka veiksmīgas starptautiskas sadarbības rezultātā jau esošajiem informācijas avotiem CERT.LV ir pievienojis vēl divus. Katrs ziņojumu avots sniedz informāciju par savos sensoros fiksētajiem notikumiem, kas CERT.LV datubāzē tiek reģistrēti kā neatkarīgi incidenti.

Neskatoties uz to, ka kopējais reģistrēto incidentu daudzums ir pieaudzis, vidējais mēnesī reģistrēto vienlaicīgi inficēto IP adrešu daudzums pārskata periodā nav palielinājies. Tas norāda uz to, ka daļa CERT.LV datubāzē reģistrēto incidentu, par kuriem informācija ir saņemta no atšķirīgiem ziņošanas avotiem, attiecas uz vienu un to pašu notikumu. CERT.LV strādā pie ziņojumu avotu iesūtītās informācijas apvienošanas iespējām, lai novērstu informācijas dublēšanos un nodrošinātu objektīvākus statistiskos rādītājus un situācijas atainojumu.

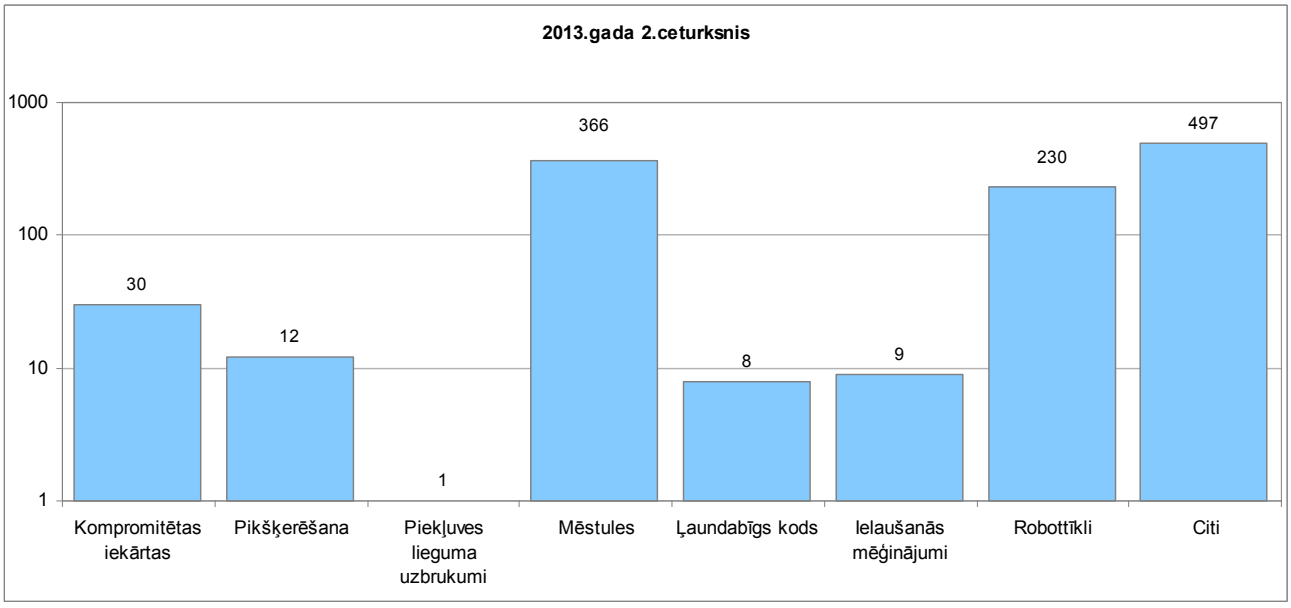
Lai samazinātu kopējo inficēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar tiem interneta pakalpojumu sniedzējiem, kas vēlas sadarboties ar šīm abām organizācijām un pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". Pārskata periodā saprašanās memorandu parakstīja arī SIA Datnet, pievienojoties 13 jau esošajiem atbildīgajiem IPS. Atbildīgo IPS kopskaits perioda beigās ir 14.

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

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis 1153 augstas prioritātes incidentus. 8.attēlā redzams augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem (grafiks ir logaritmiskā mērogā).



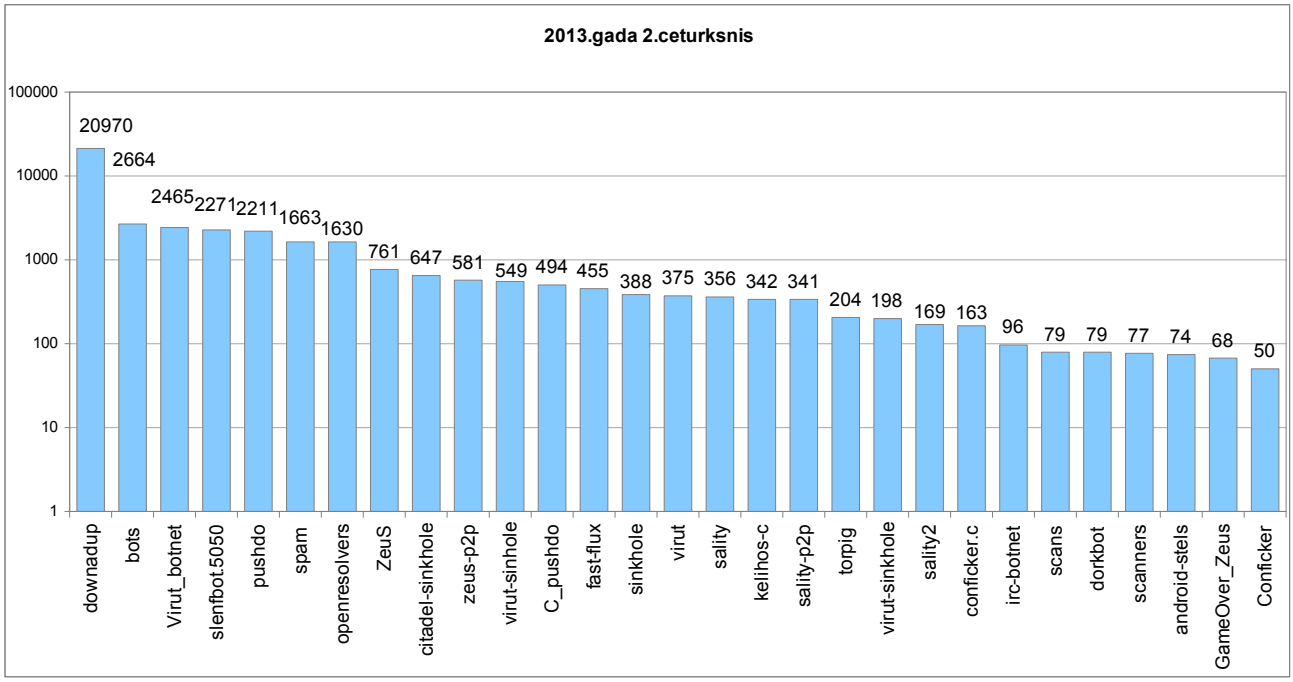
8.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.



9.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2013.gada 1.aprīļa līdz 30.jūnijam (grafikā izmantota logaritmiskā skala).

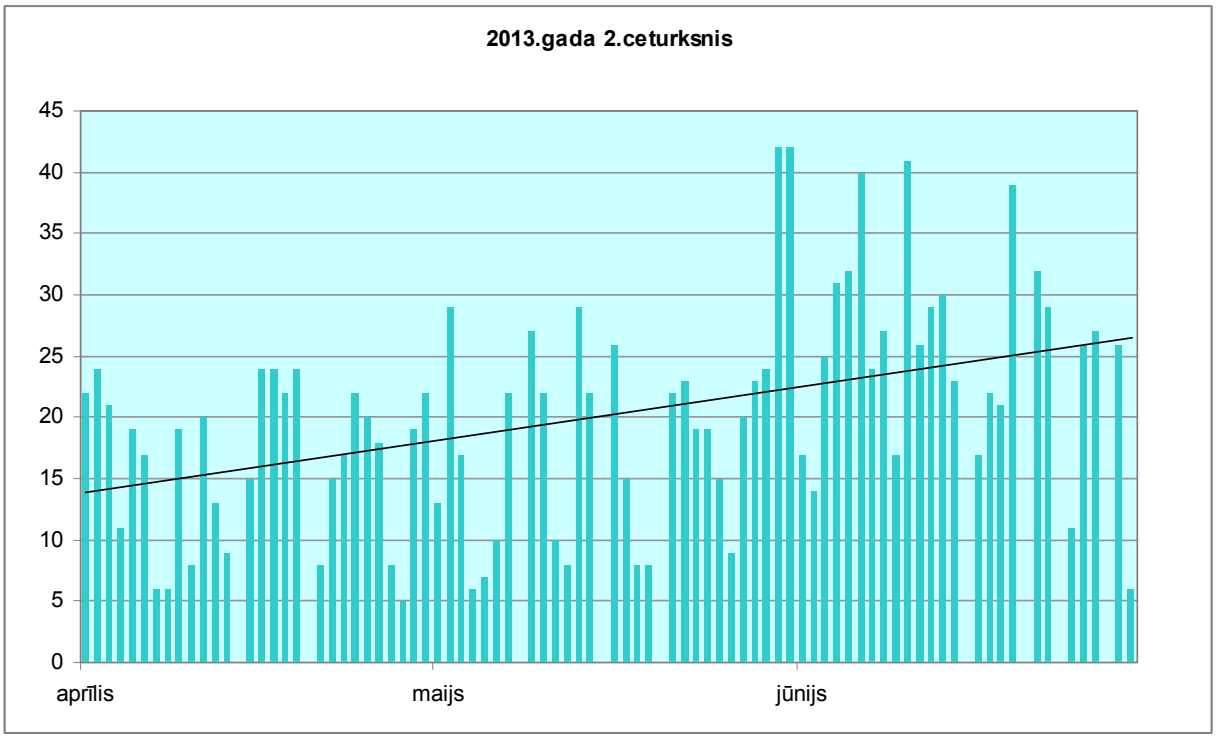
Pārskata perioda laikā CERT.LV ir reģistrējis 40 721 zemas prioritātes incidentu, par 54% jeb 21 953 inficētajām IP adresēm interneta pakalpojumu sniedzēji (IPS), kas sadarbojas ar CERT.LV, ir informējuši savus gala lietotājus.

Nākamajā attēlā aplūkojami zemas prioritātes incidenti sadalījumā pa infekciju tipiem.



10.attēls - CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā no 2013.gada 1.aprīļa līdz 30.jūnijam pa infekciju tipiem (grafikā izmantota logaritmiskā skala).

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 272 inficētām IP adresēm. 11.attēlā ir redzams, cik inficētu valsts un pašvaldību institūciju IP adreses bijušas katras dienas saņemtajos ziņojumos no dažādiem ziņošanas avotiem.



11.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 interesantākie pārskata periodā risinātie incidenti:

- 01.04. 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, 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.

- 02.04. 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.

- 02.04. Aprīļa sākumā vairākkārtēji tika veikti uzbrukumi Latvijas valsts iestāžu tīmekļa vietnēm. Veicot šo incidentu analīzi, CERT.LV speciālisti izdarīja secinājumus, ka šie uzbrukumi varētu būt saistīti ar uzbrukumiem bankām.

- 02.04. CERT.LV sniedza konsultāciju tīmekļa vietnes īpašniekam vietnes izķēmošanas novēršanai, informējot uzbrukumā izmantoto IP adrešu turētāju par viņu klientu darbībām.

- 03.04. CERT.LV veica ļaunatūras analīzi, kuras izplatīšanā piedalījās Latvijas valsts piederīgais. Analīzes rezultāti tika nodoti Valsts policijai.

- 09.04. Tika panākta vairāku Redkit exploit kit landing page resursu aizvēršana Latvijā.

- 09.04. CERT.LV saņēma ziņojumu par uzbrukumu, kas veikts no Latvijas IP, pret privātu, Polijā esošu sistēmu. Kompromitētā servera īpašnieks tika brīdināts un uzbrukums pārtraukts.

- 11.04. Tika panākta vairāku kompromitētu resursu aizvēršana Latvijā, kuri tika izmantoti uzbrukumiem pret ASV finanšu sektoru.

- 11.04. CERT.LV tika lūgts pārbaudīt aizdomīgu kredītkartes izmantošanas gadījumu. CERT.LV konstatēja krāpniecības pazīmes, informācija nodota Valsts policijai.

- 16.04. Tika saņemta informācija par vairākiem kompromitētiem resursiem Latvijā, kas tiek izmantoti uzbrukumiem ASV. CERT.LV veica šo resursu apzināšanu un koordinēja incidentu risināšanu.

- 18.04. Sadarbībā ar Vācijas CERT-BUND kolēģiem tika konstatēta mērķētu uzbrukumu

izdarīšana kādas valsts iestādes darbiniekiem. Tika konstatēts, ka vairākām valsts iestādēm tika izsūtīti e-pasti, kas noformēti saņēmējam interesējošā formā ar pielikumu, kas satur spiegošanas programmatūru. CERT.LV veica ļaunatūras analīzi, kā arī koordinēja incidenta risināšanu, apzinot radīto ietekmi.

- 08.05. Naktī no 8. uz 9. maiju tika veikti vairāki uzbrukuma mēģinājumi kādai valsts iestādes tīmekļa vietnei ar mērķi to padarīt nepieejamu. Uzbrukumi tika veikti no IP adreses Krievijas federācijā. Uz minētās iekārtas tika uzturēta tīmekļa vietne, kas, visticamāk, tika uzlauzta un serveris tika izmantots uzbrukuma veikšanai. Sadarbībā ar mitinātājkompāniju ļaunprātīgās aktivitātes tika apturētas.

- 13.05. Tika panākta vairāku kompromitētu resursu aizvēršana Latvijā, kuri tika izmantoti uzbrukumiem pret ASV finansu sektoru.

- 14.05. CERT.LV uzsāka apjomīga IT krāpniecības incidenta izmeklēšanu sadarbībā ar Valsts policiju. Cietušie varētu būt vairāki desmiti tūkstošu interneta lietotāju, kas veikuši elektroniskus naudas pārskaitījumus.

- 28.05. CERT.LV ievēroja, ka kādas valsts iestādes tīmekļa vietnē ir ikvienam pieejami kļūdu un atkļūdošanas žurnāli. Tā kā šis tiešsaistes resurss satur pietiekami sensitīvu informāciju, piekļuvi pie tā bija nepieciešams ierobežot. Atbildīgās personas tika informētas un konstatētie trūkumi tika novērsti.

- 29.05 No kādas valsts iestādes tika saņemts ziņojums par aizdomīgu datora darbību, kas sākusies pēc e-pasta pielikuma atvēršanas. Pārbaudot tika konstatēts, ka e-pasts tiešām satur datorvīrusu, kuru nav pārtvērusi izmantotā antivīrusa programma. CERT.LV sniedza rekomendācijas infekcijas seku likvidēšanā.

- 30.05. CERT.LV, veicot kāda incidenta analīzi, atklāja unikālu robotu tīklu, kas sastāvēja no ~1500 iekārtām un tā izmantotā komandu un kontroles programmatūra līdz šim netika novērota. Izmeklēšana turpinās.

- 10.06. Tika identificēti vairāki Citadel ļaunatūras robotu tīkla komand- un vadības centri, kas atrodas Latvijā. CERT.LV veica šo resursu apzināšanu un tika panākta to atslēgšana. Incidenta risināšanas gaitā izdevās iegūt pietiekami lielu apjomu lietderīgas informācijas, kas ļauj identificēt vairāk kā 10 000 inficētu iekārtu internetā. Dati tiek apkopoti un tiks izsūtīti pēc piederības atbilstošo valstu CERT komandām.

- 14.06 Tika konstatētas kļūmes vairāku interneta pakalpojumu sniedzēju DNS serveru konfigurācijās, no tiem iespējams veikt pilnu zonas datu iegūšanu. CERT.LV brīdināja serveru uzturētājus par šo kļūdu.

- 20.06 Tika konstatēts mēģinājums izkrāpt e-pasta kontu paroles, izmantojot tiešsaistes formu. Sistēmas uzturētājs tika informēts, kaitīgā forma slēgta.

- 26.06. Tika uzlauzta kādas Latvijā strādājošas bankas tīmekļa vietne. CERT.LV informēja atbildīgos darbiniekus un problēma tika novērsta, zaudējumi netika radīti.

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

CERT.LV uzskaita arī uzlauzto un izķēmoto tīmekļa vietņu gadījumus. Šādu gadījumu skaits aprīlī bija 135, maijā – 136, jūnijā – 634. Izķēmoto lapu sadalījums pa serveru operētājsistēmām: 788 – GNU/Linux, 10 – MS Windows, 3 – FreeBSD un 33 nezināmi. Augstais uzlauzto un izķēmoto lapu skaits skaidrojams ar to, ka daļa lapu īpašnieku, kas izmanto tādas satura vadības sistēmas kā *Joomla!* un *WordPress*, joprojām nebija veikuši nepieciešamos atjauninājumus un krita par upuri hakeriem, kas to izmantoja. Uzlauzto un izķēmoto tīmekļa vietņu daudzuma palielināšanās jūnijā saistīta ar vienas interneta resursu mitinātājkompānijas (*hosting company*) uzlaušanu, kas noveda pie liela apjoma izķēmošanas.

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

CERT.LV uztur tīmekļa vietni https://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 ar CERT.LV sagatavoto informāciju par „Policijas vīrusa" apkarošanas praksi un mehānismiem (7600 apmeklējumi), bet otrajā vietā ierindojās informācija par jaunākajiem vīrusiem un apdraudējumiem (6716 apmeklējumi). Kopā CERT.LV mājas lapai bijuši 13 915 apmeklējumi, kurus veido 9392 unikāli apmeklētāji no 59 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa – 90,64% apmeklētāju bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicētas 19 ziņas, sniegta informācija par CERT.LV organizētiem un starptautiska mēroga pasākumiem, publicētas CERT.LV prezentācijas, mediju ziņas un CERT.LV publiskais darbības pārskats par 2013.gada 1.ceturksni.

CERT.LV ir divi Twitter konti un tajos tiek regulāri publicētas ziņas par dažādiem jaunumiem: http://twitter.com/certlv un https://twitter.com/datorologs. Pārskata perioda laikā certlv kontā tika publicētas 52 ziņas, kontam pievienojušies 33 jauni sekotāji un 26 reizes certlv ziņa ir tikusi „retvītota" jeb padota tālāk. CERT.LV ir izveidots profils arī starptautiskajā sociālajā tīklā Facebook http://www.facebook.com/certlv (pārskata periodā publicētas 24 ziņas) un profils portālā draugiem.lv http://www.draugiem.lv/certlv.

CERT.LV uztur arī pieaugušo izglītošanas portālu https://www.esidross.lv. Pārskata perioda laikā šajā portālā ir publicēti 9 jauni raksti, portālu apmeklējuši 14 550 (10 548 unikāli) apmeklētāji. Publicētie raksti:

- Kāpēc sociālā inženierija ir efektīva?
- ZoneAlarm – ugunsmūris 2013
- Mobilo iekārtu drošība (video lekcija un pēcāk arī lekcijas materiāls)
- Java un tās drošība
- Eiropas balva "Labākais interneta saturs bērniem"
- Rūpēs par bērnu drošību – viedtālruņu un spēļu konsoļu ierobežojumi
- Ko no Imantas hakera lietas var mācīties katrs interneta lietotājs
- ZoneAlarm – antivīruss un ugunsmūris

- QR kods un tā izmantošana un drošība

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

1) Publikācijas presē:
   - 04.04. – CERT.LV pārstāvis sniedza komentāru laikrakstam IR saistībā ar Imantas hakera lietu
   - 19.06. – CERT.LV pārstāvis sniedz komentāru laikrakstam Diena par maksājumu karšu datu zādzību
2) Intervijas un ziņas radio:
   - 10.05. – CERT.LV pārstāvis sniedza komentāru Latvijas radio 4 ziņu izlaidumā par *Joomla!* un *WordPress* satura vadības sistēmu ievainojamībām un Ababil uzbrukumu kampaņu
3) Sižeti televīzijā, tiešraides:
   - 03.04. – CERT.LV pārstāvis piedalījās diskusijā LTV1 raidījumā „Sastrēgumstunda" par iespējamo D.Čalovska izdošanu ASV
   - 30.04. – CERT.LV pārstāvis piedalījās LTV1 raidījumā „Aculiecinieks", kurā skaidroja kiberdrošības principus un stāstīja par IT drošību Latvijā, raidījums veltīts Kiberaizsardzības vienības tapšanai
   - 27.06. – CERT.LV pārstāvis sniedz komentāru TV5 par krāpniecību internetā
4) Ziņas portālos:
   - 27.05. - Kibernoziegums nav tas pats, kā uzlauzta un apzagta automašīna – raksts TVnet
   - 27.05. - Охота за хакерами: что делать, если вас обокрали – raksts Kriminal.lv
   - 29.05. - Latvijā 10% iedzīvotāju tic viltus ziņojumiem datorā - raksts NRA
   - 29.05. - «Полицейский вирус» атаковал компьютеры латвийцев – raksts Telegraf
   - 30.05. - Осторожно, мошенники: 10% латвийцев стали жертвами «полицейского вируса» – raksts Ves.lv
   - 07.06. - Visizplatītākā valsts IT sistēmu nelaime - tās netiek atjauninātas – BNS ziņa
   - 10.06. - Valsts un pašvaldību interneta lapas ir ļoti dažādā stāvoklī – BNS ziņa
   - 12.06. - Latvija kiberuzbrukumiem ir daudz gatavāka nekā pirms pāris gadiem – BNS ziņa
   - 19.06. - Latvijā izglītību IT drošībā nevar iegūt; brauc uz Igauniju – BNS ziņa

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

17.aprīlī CERT.LV organizēja semināru „Esi drošs-2", kas paredzēts valsts un pašvaldību iestāžu par IT drošību atbildīgajām personām, kā arī citiem interesentiem, kas darbojas IT drošības jomā. 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. Seminārs notika Kara muzejā un tajā piedalījās 98 dalībnieki.

25.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.

CERT.LV ir iesaistīta BAITSE (Baltic Academic Information Technology Security Exchange) projektā, kura mērķis ir izstrādāt maģistru dubultā diploma apmācību kursus "Information Technology penetration testing" un "Malware analysis". Pārskata periodā CERT.LV pārstāvis piedalījās projekta sanāksmē Polijā, Vroclavas tehniskajā universitātē.

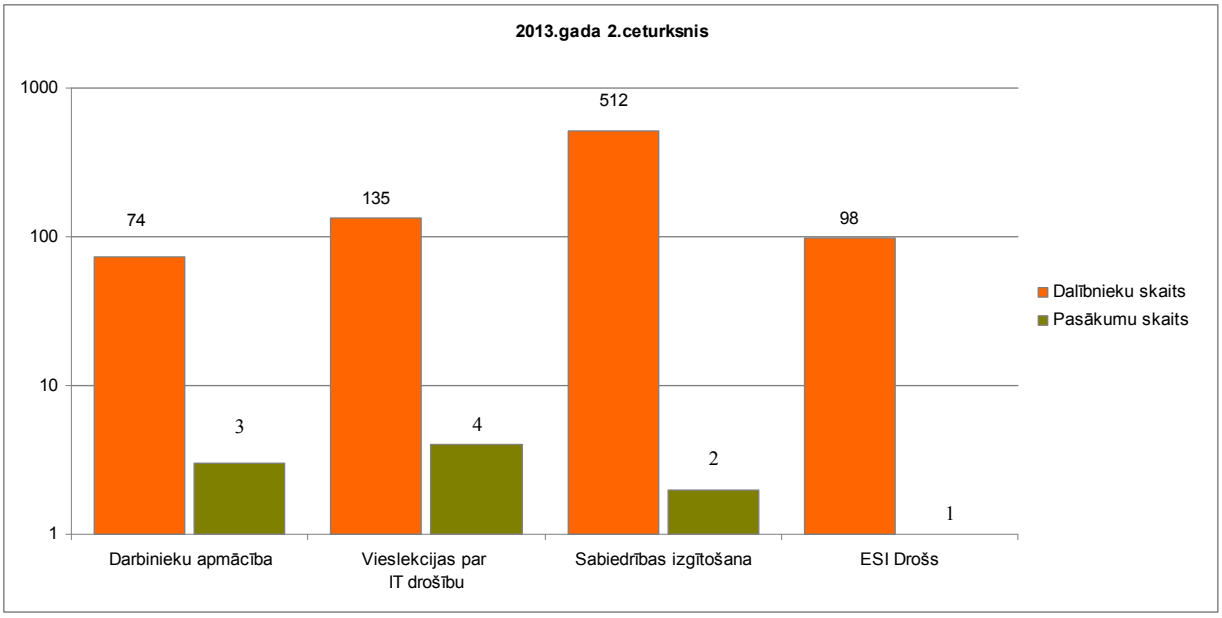
Pārskata periodā CERT.LV sniedza 4 intervijas studentiem, kuri izvēlējušies savu akadēmisko darbu izstrādāt par kādu ar IT drošību saistītu tēmu un vēlējās iegūt CERT.LV pārstāvju viedokli.

Pārskats par CERT.LV pasākumiem pārskata periodā:

- 8.04. CERT.LV pārstāvis novadīja lekciju par sociālo inženieriju RTU Studentu pašpārvaldes organizētā studentu pasākumā.
- 17.04. Notika seminārs „Esi drošs-2".
- 18.04. CERT.LV pārstāvis piedalījās NBS Sakaru skolas organizētajā seminārā „INFOSEC2", izpildot mērķētus uzbrukumus mācību videi un novadot nodarbību par iekšēja uzbrucēja radītiem draudiem informācijas sistēmai.
- 19.04. Notika NIC.LV konference, kurā CERT.LV pārstāvji piedalījās ar prezentāciju un vadīja vienu no sesijām.
- 25.04. CERT.LV novadīja video lekciju skolām par mobilo iekārtu drošību, kuras beigās lektori sniedza atbildes uz lekcijas laikā iesūtītajiem skolēnu jautājumiem.
- 29.04. CERT.LV pārstāvis tikās ar LU maģistratūras studentiem, lai pārrunātu interneta balsošanas tehniskos un drošības aspektus.
- 02.05. CERT.LV pārstāvis novadīja vieslekciju LU Datorikas institūta pirmā kursa studentiem par tīkla ievainojamību testēšanas principiem.
- 07.05. CERT.LV pārstāvis novadīja lekciju RTU maģistratūras studentiem par IT drošības sistēmu Latvijā.
- 16.05. CERT.LV pārstāvis tikās ar Starptautiskās komerciālās profesionālās un vispārējās izglītības vidusskolas skolēniem un sniedza prezentāciju.
- 16.-17.05. CERT.LV pārstāvji piedalījās SIA „DPA" IT drošības konferencē. Pasākuma ietvaros CERT.LV pārstāvji uzstājās ar prezentāciju par DDoS uzbrukumu anatomiju, kā arī pilnībā nodrošināja CyberChallenge mācību/konkursa tehnisko nodrošinājumu, scenāriju, vadību, izpildi un novērtēšanu. 4 CERT.LV un 2 DPA pārstāvji veidoja uzbrūkošo komandu.
- 21.05. CERT.LV organizēja informācijas aizsardzības semināru valsts un pašvaldību iestāžu atbildīgajiem par IT drošību. Semināru vadīja NBS Sakaru skolas pasniedzēji.
- 28.05. CERT.LV pārstāvis sniedza prezentāciju IBM rīkotajā konferencē „Jūsu IT sistēmu drošība kā ārpakalpojums - iespējas un izaicinājumi".
- 28. un 30.05. CERT.LV organizēja un vadīja semināru „Par tehniskā atbalsta sniegšanu datoru lietotājiem", kas bija paredzēts interneta pakalpojumu sniedzēju tehniskā atbalsta speciālistiem.
- 29.05 CERT.LV sniedza konsultāciju Rīgas Valsts tehnikuma operētājsistēmu skolotājam datorvīrusu apkarošanas vingrinājuma izveidē.
- 11.06. CERT.LV organizēja un vadīja semināru valsts un pašvaldību iestāžu par IT drošību atbildīgajiem darbiniekiem „Ievads tīkla ievainojamību testēšanā".

12.attēlā redzams kopējais pasākumu daudzums un apmācīto cilvēku skaits 2013.gada 2.ceturksnī. Pārskata periodā CERT.LV par IT drošību ir izglītojis 819 cilvēkus, kas ir par 97 apmācāmajiem

vairāk nekā iepriekšējā periodā, piedaloties 10 lekcijās un semināros.



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

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.

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

- 26.06. CERT.LV pārstāvis piedalījās VARAM organizētājā darba grupā par uzticamu sertifikācijas pakalpojumu sniedzēju (USPS) pārraudzību un kontroli.
- 20.06. CERT.LV pārstāvis piedalās Aizsardzības ministrijas organizētā sarunā par Kiberjaunsardzes izveidošanu.
- 27.06. CERT.LV pārstāvis tikās ar Aizsardzības ministriju, lai koordinētu Eiropas kiberdrošības mēneša aktivitāšu organizēšanu.

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 norīkoto atbildīgo personu, kura iestādē īsteno informācijas tehnoloģiju drošības pārvaldību. Līdz 2013.gada 30.jūnijam CERT.LV ir apkopojis informāciju par 603 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 nosaka kārtību, kādā Elektronisko sakaru komersantiem (ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla

nepārtrauktas darbības nodrošināšanai. 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.

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

Visa perioda laikā ir notikusi aktīva sadarbība ar citu valstu IT 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 sekojošos starptautiskos pasākumos:

- 02.-03.04. CERT.LV pārstāvji piedalījās FIRST Technical Coloqioum Amsterdamā, Nīderlandē.
- 12.04. CERT.LV pārstāvis 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.
- 22.-26.04. CERT.LV pārstāvis piedalījās BAITSE projekta sanāksmē Polijā, Vroclavas tehniskajā universitātē, un novadīja vieslekciju par ievainojamību testēšanu.
- 23.-26.04. CERT.LV pārstāvis piedalās NATO organizētajās IT drošības mācībās „Locked Shields" organizatoru (baltajā) komandā.
- 26.04. CERT.LV piedalījās telekonferencē ar EU-CERT par savstarpējo sadarbību.
- 09.05. CERT.LV pārstāvis tikās ar Ungārijas e-pārvaldes valsts sekretariāta delegāciju un sniedza prezentāciju par IT drošības aktualitātēm Latvijā.
- 21.-24.05. CERT.LV pārstāvis piedalījās TF-CSIRT konferencē Bukarestē, Rumānijā. Konferences laikā ir panāktas vairākas vienošanās par incidentu informācijas apmaiņu ar citu valstu CERT komandām. CERT.LV izpelnījās atzinīgu novērtējumu no Team Cymru kā valsts, kurā panākts IT infekciju samazinājums.
- 23.05. CERT.LV pārstāvis piedalījās ENISA rīkotā telekonferencē par Eiropas kiberdrošības mēneša aktivitāšu plānošanu.
- 04.-07.06. CERT.LV pārstāvis piedalījās NATO starptautiskajā konferencē "CyCon 2013".
- 05.06. CERT.LV pārstāvis piedalījās "Israeli Info Security Summit" Rīgā.
- 06.-07.06. CERT.LV pārstāvis piedalījās slēgtā EGC (European Govermental CSIRT) grupas sanāksmē Helsinkos un prezentēja IT drošības situāciju Latvijā. EGC ir ieinteresēti uzņemt Baltijas valstu CERT vienības savā pulkā.
- 13.-14.06. CERT.LV pārstāvji piedalījās kritiskās informācijas aizsardzības seminārā Tallinā.
- 14.-24.06. CERT.LV pārstāvji piedalījās FIRST konferencē un gadskārtējā nacionālo CSIRTu sanāksmē. FIRST konferencē CERT.LV pārstāvis vadīja vienu no "Policy and Management" sesijām, nacionālo CSIRTu sanāksmē CERT.LV pārstāvji sniedza prezentāciju "Responsible ISPs - developing cyber security capabilities in Latvian networks".

8. Veikt citus normatīvajos aktos noteiktos pienākumus.

- Pārskata periodā notikušas trīs DEG grupas sanāksmes.
- Turpinājās zemas mijiedarbes urķuslazda HoneyD ieviešana akadēmiskā mākoņa vidē, konfigurēšana, darbības pārbaude un iegūto datu analīze.
- Turpinājās darbs pie *Taranis* ziņu apkopošanas sistēmas funkcionalitātes apzināšanas un tā iespējamo pielietojumu izpētes, atbilstoši CERT.LV un tā pārziņā esošo iestāžu vajadzībām.
- Pārskata periodā notika CERT.LV tikšanās ar NetSafe, lai pārrunātu sadarbību.
- CERT.LV pārstāvis piedalās žūrijas komisijā NetSafe organizētajā konkursā bērniem par bērniem atbilstošu saturu internetā.

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