Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2015

2015. gada 2. ceturksnis (01.04.2015. – 30.06.2015.)

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

Saturs

Kopsavilkums 3

1. Elektroniskās informācijas telpā notiekošo darbību atainojums. 4

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā. ... 7

3. Rekomendācijas par informācijas tehnoloģiju risku novēršanu (komunikācija ar sabiedrību). 13

4. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā. 15

5. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā. 16

6. Valsts un pašvaldību institūciju un elektronisko sakaru komersantu uzraudzība par Informācijas tehnoloģiju drošības likumā noteikto pienākumu veikšanu. 17

7. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām. 18

8. Citi normatīvajos aktos noteiktie pienākumi. 19

9. Aģentūras papildu pasākumu veikšana. 20

Kopsavilkums

Jūnijā noslēdzās Latvijas prezidentūra Eiropas Savienības Padomē (turpmāk - Prezidentūra). Pirms Prezidentūras un tās laikā tika ieguldīts nozīmīgs darbs, lai nodrošinātu atbilstošu drošības pakāpi dažādiem valsts un pašvaldību iestāžu tiešsaistes resursiem.
Prezidentūras laikā notika dažādi kiberuzbrukumi, taču tiem nebija nopietnas sekas, kas grautu Latvijas reputāciju vai Prezidentūras darbu.

Lai sagatavotos Prezidentūrai, CERT.LV veica ielaušanās un slodzes noturības testus iestāžu resursiem, organizēja ministriju vadītāju apmācības un izglītoja valsts un pašvaldību iestāžu darbiniekus, kā arī interneta pakalpojumu sniedzējus.

No 22. līdz 24.aprīlim CERT.LV kopā ar Zemessardzes Kiberaizsardzības vienību un Lietuvas pārstāvjiem piedalījās lielākajās kiberdrošības mācībās „Locked Shields 2015". Mācības organizēja NATO CCDCoE. Latvijas – Lietuvas apvienotā komanda kopvērtējumā ieguva 4. vietu un juridiskajā komponentē 2. vietu 16 valstu konkurencē.

No 11. līdz 12.maijam CERT.LV kopā ar ENISA organizēja starptautisku semināru "CERTs in Europe", kurā piedalījās dalībnieki no 20 valstīm. Seminārs fokusējās uz dažādu valstu pieredzi, saistītu ar prezidentūru Eiropas Savienības Padomē un Tīklu un informācijas drošības direktīvu.

Pārskata periodā vērienīgākais drošības incidents bija TLS protokola Diffie-Hellman šifrkopas ievainojamība „Logjam". Tā ietekmēja tūkstošiem ar OpenSSL/TLS aizsargātas vietnes (https), pasta serverus un citus plaši izmantotus interneta pakalpojumus, kā arī klientu programmatūru.

Nozīmīga globālā incidentu tendence, kas izpaužas arī Latvijā, ir liels skaits nedroši konfigurēti maršrutētāji un WiFi iekārtas, kas parasti ir mājas un biroja tīkla aprīkojuma sastāvdaļa. Bieži vien šo iekārtu funkcionalitāte tiek nesankcionēti izmantota, lai veiktu pārslodzes uzbrukumus citiem tīkliem. Nedroši konfigurētas iekārtas arvien vairāk tiek izmantotas kā starpniekserveri noziedzīgu darbību slēpšanai.

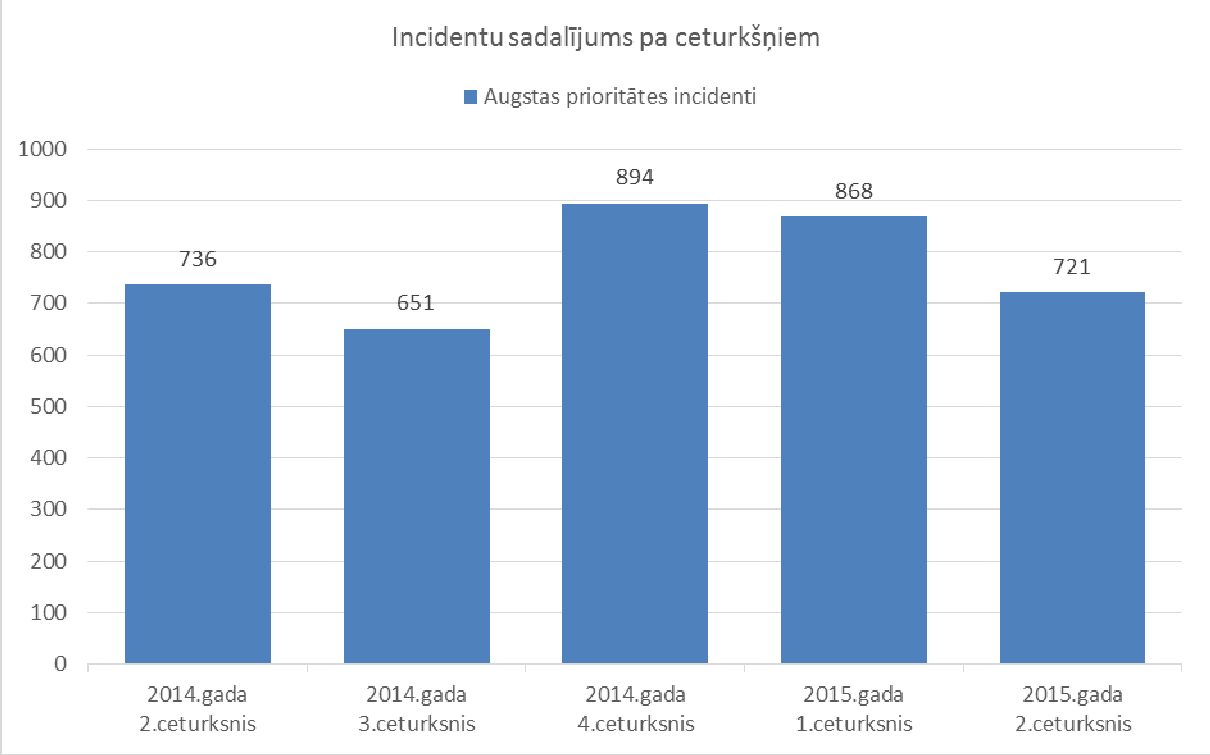
2015.gada 2.ceturksnī CERT.LV reģistrēja un apstrādāja 721 augstas prioritātes incidentu un 173 008 zemas prioritātes incidentus.

Pārskata periodā CERT.LV pārstāvji piedalījās 22 pasākumos, apmācot 1259 cilvēkus, ievietoja 26 jaunas ziņas vietnē www.cert.lv, piedalījās 5 radio pārraidēs un 3 televīzijas sižetos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

CERT.LV ik mēnesi apkopo informāciju par notikušajiem incidentiem, iedalot incidentus augstas prioritātes (visi iekārtu kompromitēšanas gadījumi, pikšķerēšana, piekļuves lieguma uzbrukumi, ielaušanās mēģinājumi, kā arī jebkurš cits incidents, kas skar tieši augstas prioritātes institūcijas vai ko ir paziņojis cilvēks, nevis automātisks ziņotājs) un zemas prioritātes (galvenokārt inficētas galalietotāju iekārtas, kas kļuvušas par robotu tīklu sastāvdaļām un/vai izsūta mēstules) incidentos.

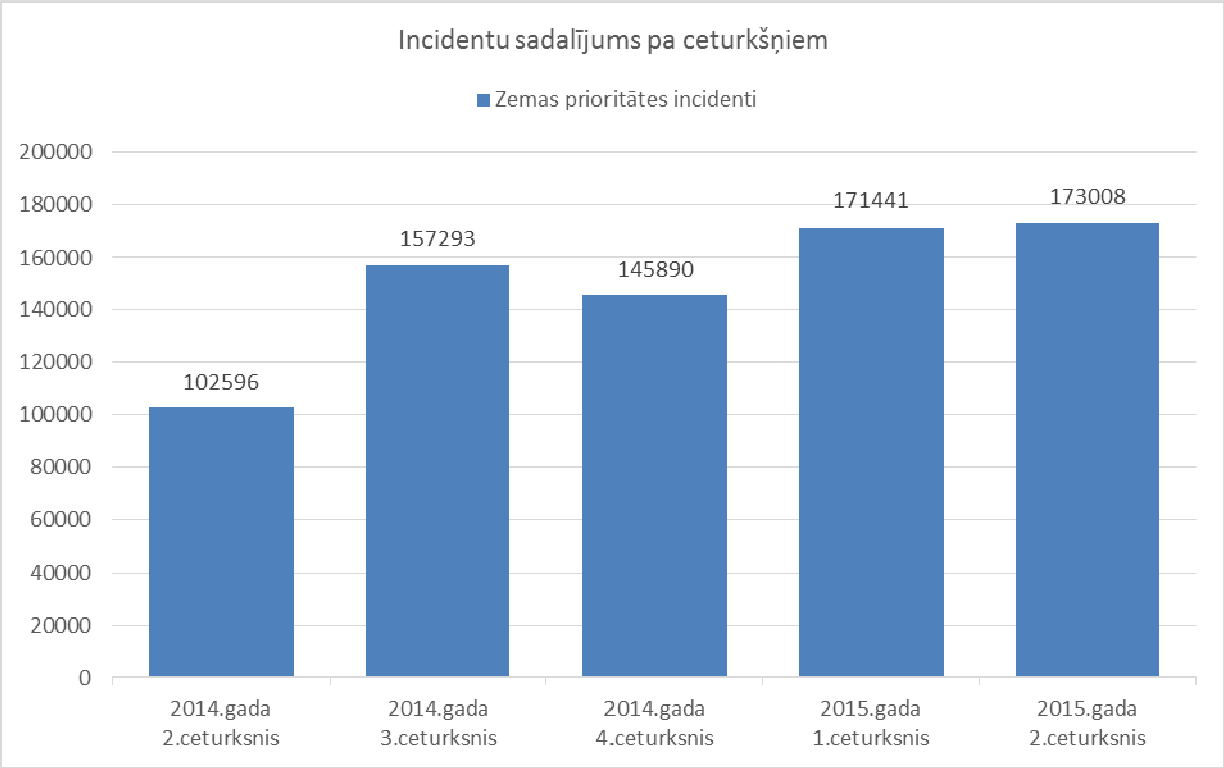
2015.gada 2.ceturksnī CERT.LV apstrādāja 721 augstas prioritātes incidentu. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 868 augstas prioritātes incidenti, bet 2014.gada 2.ceturksnī 736 augstas prioritātes incidenti.



1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2014. un 2015. gadā.

Raksturīgi sezonalitātei, augstas prioritātes incidentu skaits ir samazinājies.

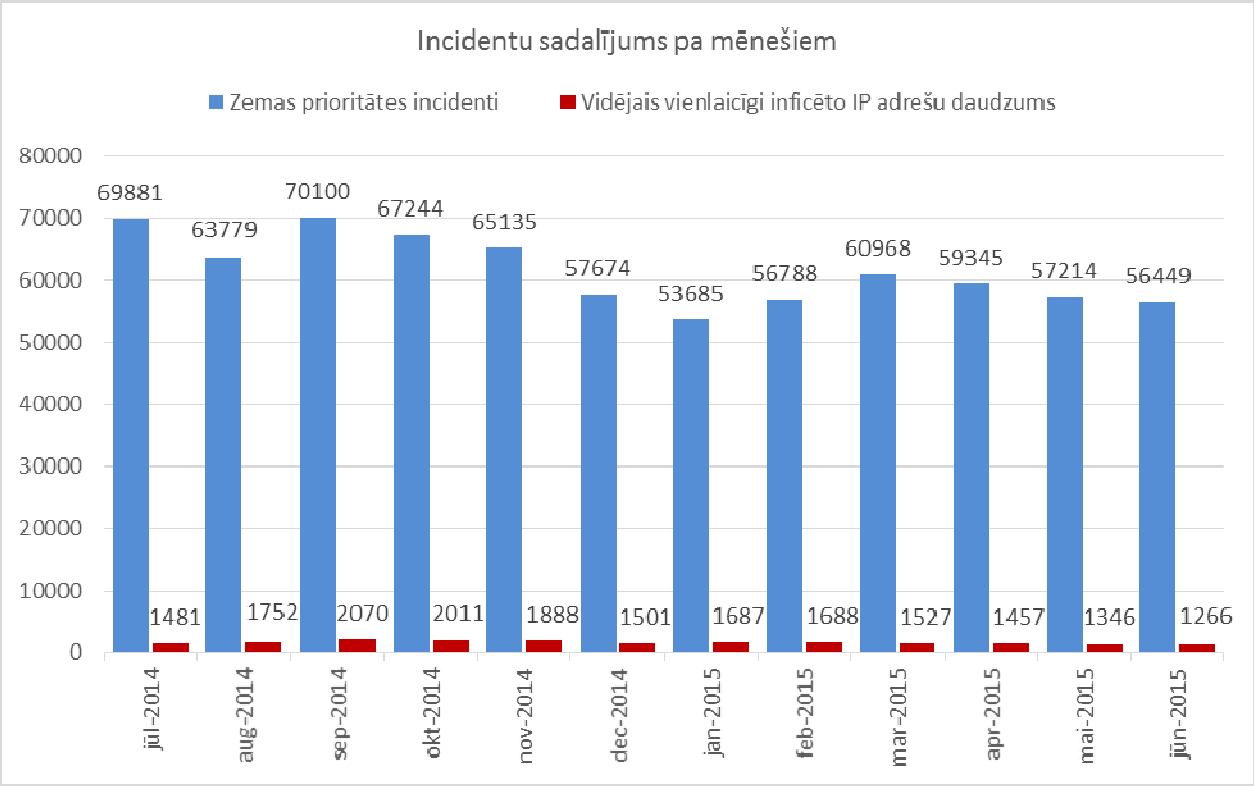
Turpinājās banku vārdā organizētas pikšķerēšanas kampaņas, taču jaunas, plaša mēroga uz Latviju mērķētas uzbrukumu kampaņas šajā periodā netika novērotas.



2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem 2014. un 2015.gadā.

2015.gada 2.ceturksnī CERT.LV reģistrēja 173 008 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēts 171 441 zemas prioritātes incidents, bet 2014.gada 2.ceturksnī – 102596 zemas prioritātes incidenti. Zemas prioritātes incidentu skaits turpina nedaudz pieaugt, jo CERT.LV arvien papildina savu ziņojumu avotu sarakstu.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Otrajā ceturksnī šie rādītāji ir nedaudz samazinājušies, kas nozīmē, ka arvien biežāk inficētā datorā ir sastopami vienlaicīgi dažādi vīrusi.

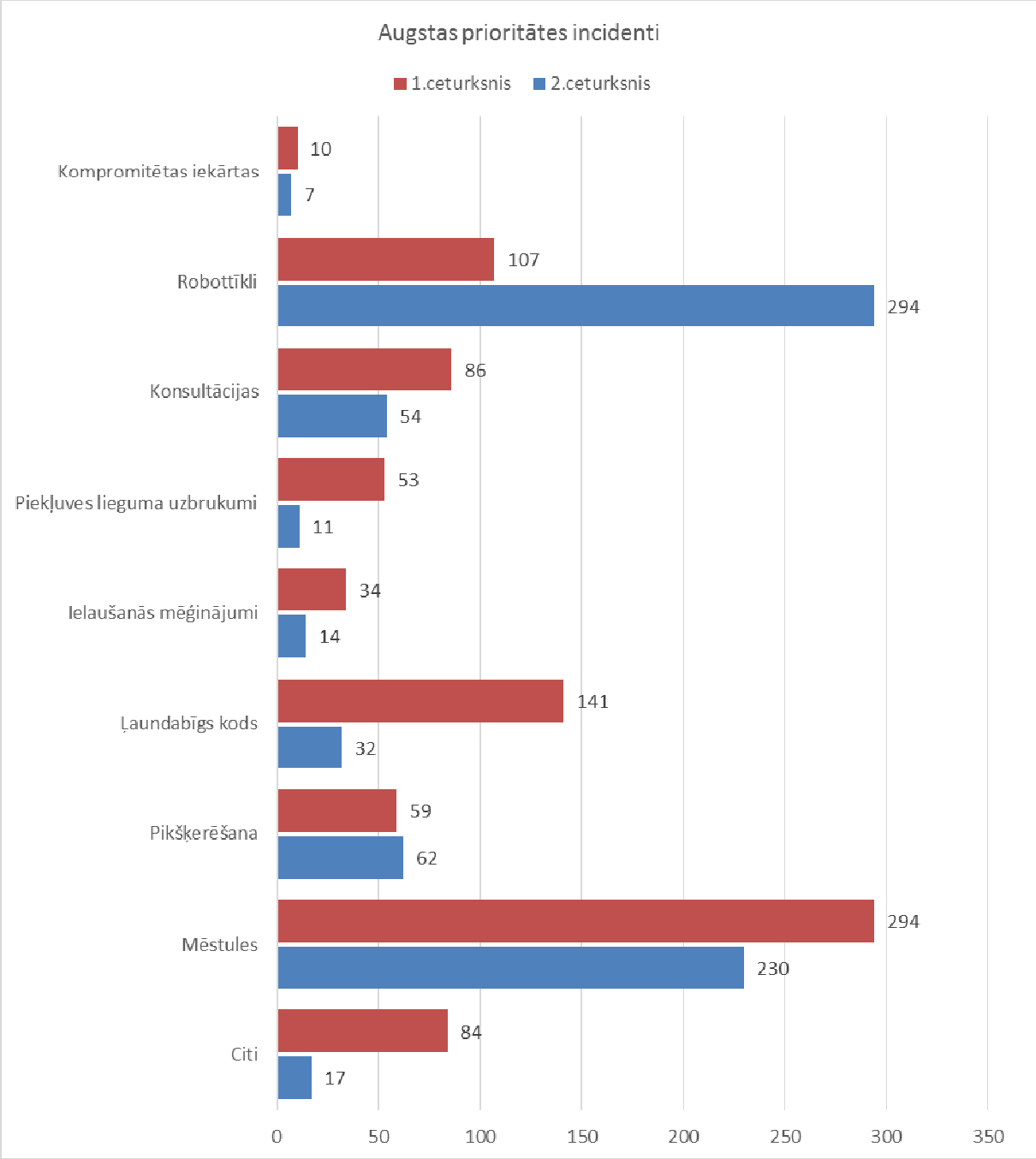


3.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums 2014. un 2015.gadā.

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 IPS, kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". Atbildīgo IPS kopskaits saglabājās bez izmaiņām – 13.

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

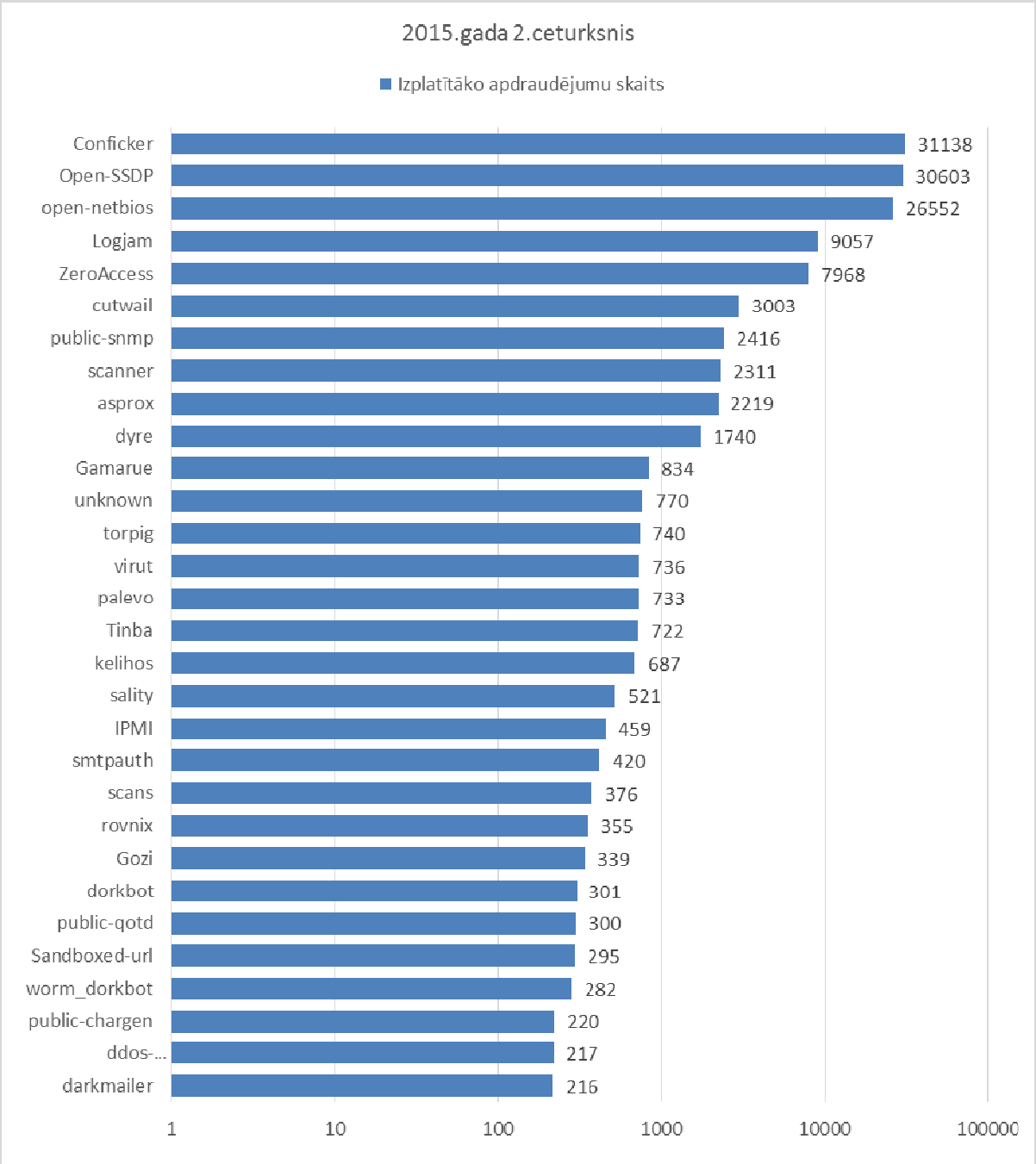
Pārskata periodā CERT.LV reģistrēja un apstrādāja 721 augstas prioritātes incidentu.



4.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2015.gadā.

Salīdzinot ar iepriekšējo ceturksni, audzis konstatēto robottīklu skaits. Augsts ir arī reģistrēto pikšķerēšanas ziņojumu skaits, jo aktivizējās vairākas banku datu izkrāpšanas kampaņas. Mēstuļu izsūtīšanas apjomi nav būtiski kritušies, taču šajā ceturksnī, salīdzinot ar iepriekšējo, samazinājies reģistrētais piekļuves lieguma jeb DDoS uzbrukumu skaits.

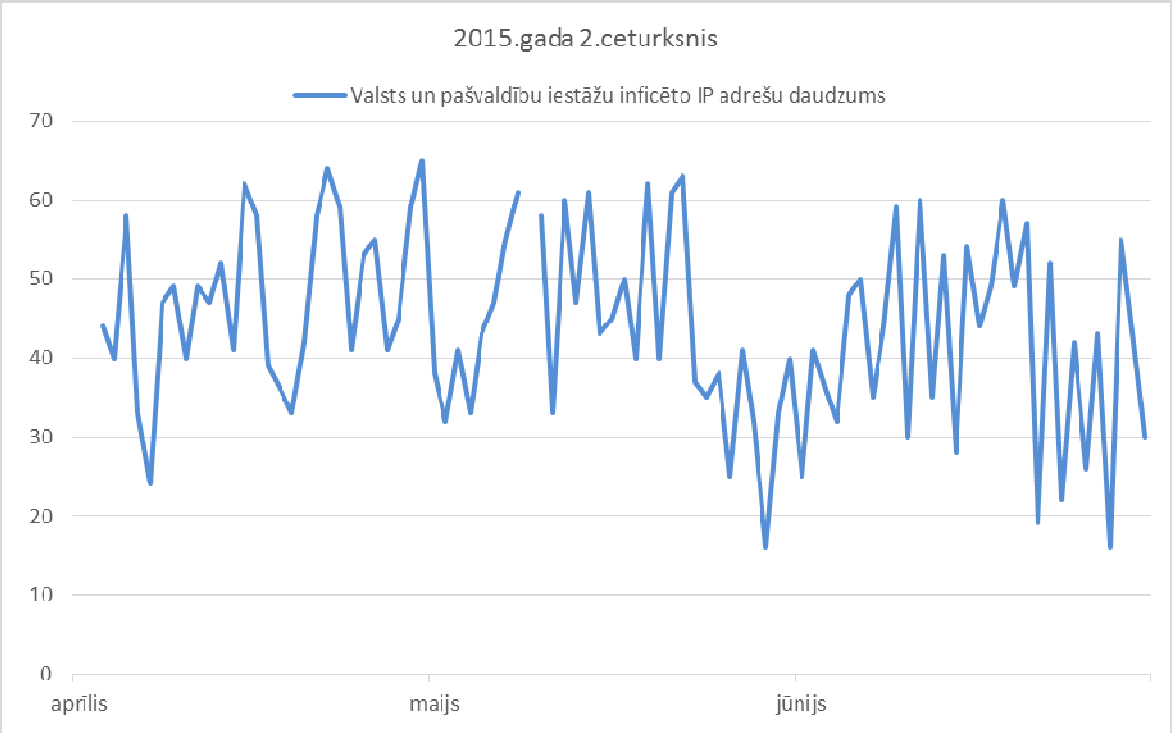
Pārskata periodā CERT.LV reģistrēja 173 008 zemas prioritātes incidentu. Izplatītāko apdraudējumu veidi joprojām saglabājas tie paši, apdraudējumu sarakstā klāt nācis „Logjam", kas arī bijis viens no ievērojamākajiem incidentiem šajā ceturksnī.



5.attēls - CERT.LV reģistrētie zemas prioritātes incidenti no 2015.gada 1.aprīļa līdz 30.jūnijam pa apdraudējumu veidiem.

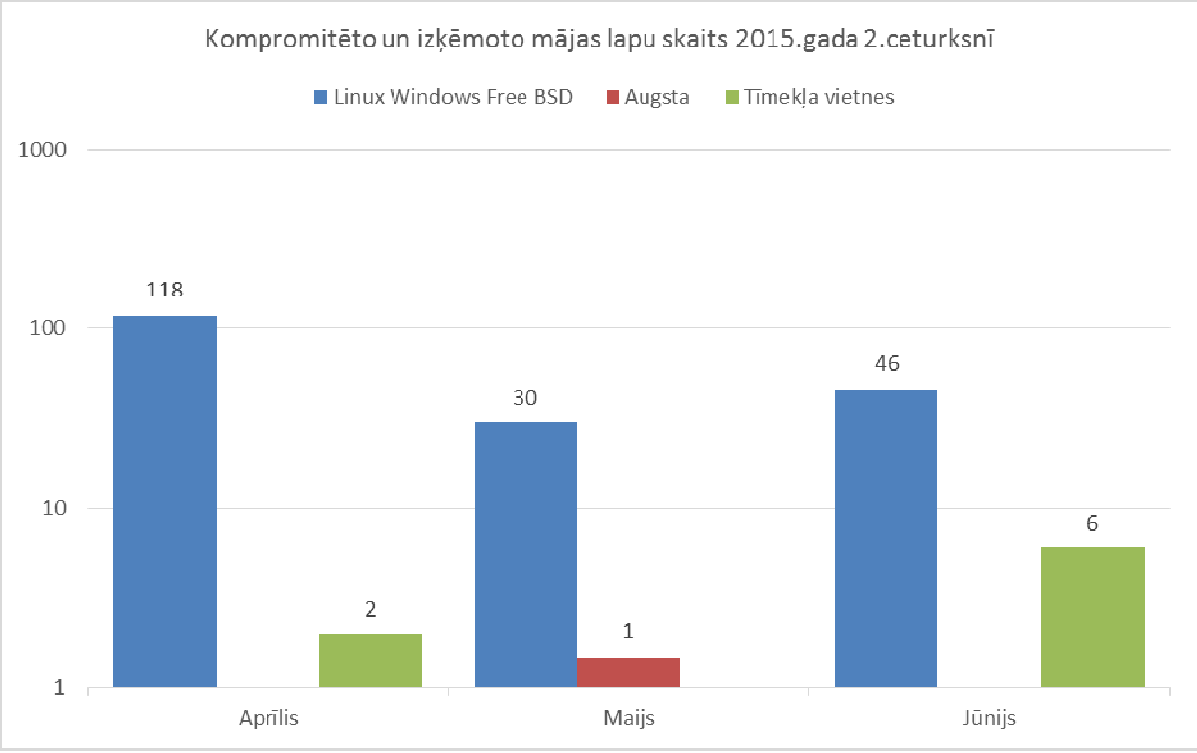
CERT.LV apkopo informāciju no valsts un pašvaldību institūcijām par to izmantotajām IP adresēm un tīmekļa vietnēm, lai CERT.LV varētu operatīvāk reaģēt šo iestāžu IT drošības incidentu gadījumos. CERT.LV informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā inficētas.

Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:



6.attēls – Iestāžu inficēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2015.gada 2.ceturksnī.

CERT.LV uzskaita arī kompromitēto un izķēmoto mājaslapu gadījumus. Šādu gadījumu skaits:



7.attēls – Kompromitēto un izķēmoto mājas lapu skaits pa mēnešiem 2015.gada 2.ceturksnī.

Pārskata periodā notika virkne dažādu uzbrukuma kampaņu, kas bija mērķētas gan uz valsts un pašvaldību iestādēm, gan uzņēmumiem, gan internetbanku lietotājiem.

Maijā CERT.LV saņēma informāciju par organizētām DDoS uzbrukumu kampaņām ar mērķi izspiest naudu. Uzbrucēji izsūtīja e-pastu organizācijai, draudot veikt DDoS uzbrukumu, ja netiks samaksāts no 20 līdz pat 100 Bitcoin. Uzbrucēji apgalvoja, ka viņu rīcībā ir resursi, lai organizētu līdz pat 400 Gbps apjomīgu uzbrukuma datu plūsmu. Vairākos gadījumos noziedzīgais grupējums patiešām ir veicis uzbrukumus, kas ir sasnieguši 50 Gbps, bet pārsvarā, ja upuris nesāk komunicēt un neatbild uz iesūtītajiem draudiem, uzbrukums netiek uzsākts.
CERT.LV informēja valsts iestādes un lūdza ziņot par šādiem gadījumiem un aicināja nekomunicēt ar izspiedējiem.

Pēc tādiem drošības apdraudējumiem kā Heartbleed, POODLE un FREAK, internetā parādījās jauns uzbrukumu veids „Logjam", kas uzbrucējam deva iespēju nolasīt un pārveidot sensitīvus datus, kompromitējot šifrētus savienojumus. „Logjam" ļauj veikt man-in-the-middle (saziņas pārtveršanas/noklausīšanās) uzbrukumu, lai pavājinātu šifrētus savienojumus starp lietotāju un serveri, radot iespēju tos atšifrēt.

CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā.

Zemāk uzskaitīti svarīgākie pārskata periodā risinātie incidenti un to novēršana:

- 01.04.2015. CERT.LV konsultēja kāda uzņēmuma pārstāvjus par iespējām veikt ielaušanās testus.
- 03.04.2015. DNB bankas vārdā tika izsūtīti e-pasti, kas saturēja saiti uz pikšķerēšanas vietni. CERT.LV informēja iesaistīto resursu turētājus. Atklājās, ka kaitīgās lapas izvietotas, izmantojot novecojušu Wordpress satura vadības sistēmu versiju ievainojamības.

  Vēstules paraugs:


From: DNB [mailto:lv@dnblv-security.lv]
Sent: Friday, April 10, 2015 12:16 PM
To: info@antivirus.lv
Subject: Sanemta zina

DNB

Cienījamais klient.

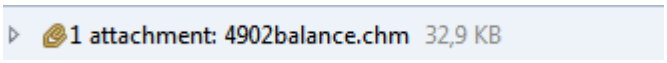
Jūs esat saņēmis paziņojumu.
Piekļūt savam kontam

- 07.04.2015. CERT.LV konstatēja pirmos „Dyre Wolf trojan" infekcijas gadījumus

Latvijā. Upuri tiek apzināti un turpinās incidentu risināšana.

- 10.04.2015. Atkārtoti tika izsūtīti e-pasti ar DNB pikšķerēšanas lapas saiti. CERT.LV sazinājās ar lapas uzturētājiem, lapa tika slēgta.
- 15.04.2015. Tika atklāts, ka kāda portāla servera reklāmas izplatīšanas sistēmā ievietots kaitīgs baneris, kas apmeklētāju datoros automātiski mēģina izplatīt datorvīrusu. Servera īpašnieki tika brīdināti, reklāmu izplatīšanas sistēma tika atslēgta līdz atjaunināšanai.
- 23.04.2015. Atkārtoti tika izsūtīti e-pasti ar DNB pikšķerēšanas lapas saiti. CERT.LV sazinājās ar lapas uzturētājiem, lapa tika slēgta.
- 24.04.2015. Kādas valsts iestādes darbiniekiem tika iesūtīts datorvīruss, izmantojot inficētus Microsoft Word dokumentus, kas saturēja kaitīgus *macro* skriptus. Darbinieki tika brīdināti, mēģinājums inficēt datorus neizdevās.
- 12.05.2015. CERT.LV sadarbojās ar ārvalstu CERT vienību „DDoS 4 Bitcoining" incidentu izmeklēšanā un veica informācijas apmaiņu. Latvijā līdz tam nebija zināms neviens grupējuma upuris nedz valsts sektorā, nedz banku sektorā.
- 12.05.2015. CERT.LV sadarbojās ar ārvalstu kolēģiem kāda banku vīrusa izplatīšanas kontrolcentra izmeklēšanā, kas tika uzturēts Latvijā.
- 21.05.2015. Tika atklāta TLS protokola Diffie-Hellman šifrkopas ievainojamība "Logjam". CERT.LV veica ievainojamības apzināšanu Latvijas IP adrešu tīklos un informēja tīklu turētājus, kuriem konstatēti drošības trūkumi. Kritiski apdraudēti bija līdz 100 resursiem, kuriem DH atslēgas izmērs bija 512 vai mazāk baitu, savukārt >1024 baitu atslēgas, kuras ieteicams mainīt uz drošākām, tika konstatētas vairākiem tūkstošiem resursu. Informatīvā kampaņa tika veikta iniciatīvas "Atbildīgs interneta pakalpojumu sniedzējs" ietvaros.
- 02.06.2015. Latvijā tika izplatīti inficēti e-pasti, kurus uzbrucēji izsūtīja it kā Latvijas mobilo sakaru operatora vārdā. Pielikumā izsūtīti "Microsoft Compiled HTML Help" (.CHM) faili, kurus atverot tiek izpildīta *powershell* palaišanas komanda, kas lejupielādē kaitniecisku putty.exe failu, kurš satur funkcionalitāti, kas uzbrucējam ļauj pārņemt kontroli pār upura datoru. CERT.LV veica infekcijas izplatības apzināšanu valsts sektorā un informēja sabiedrību.

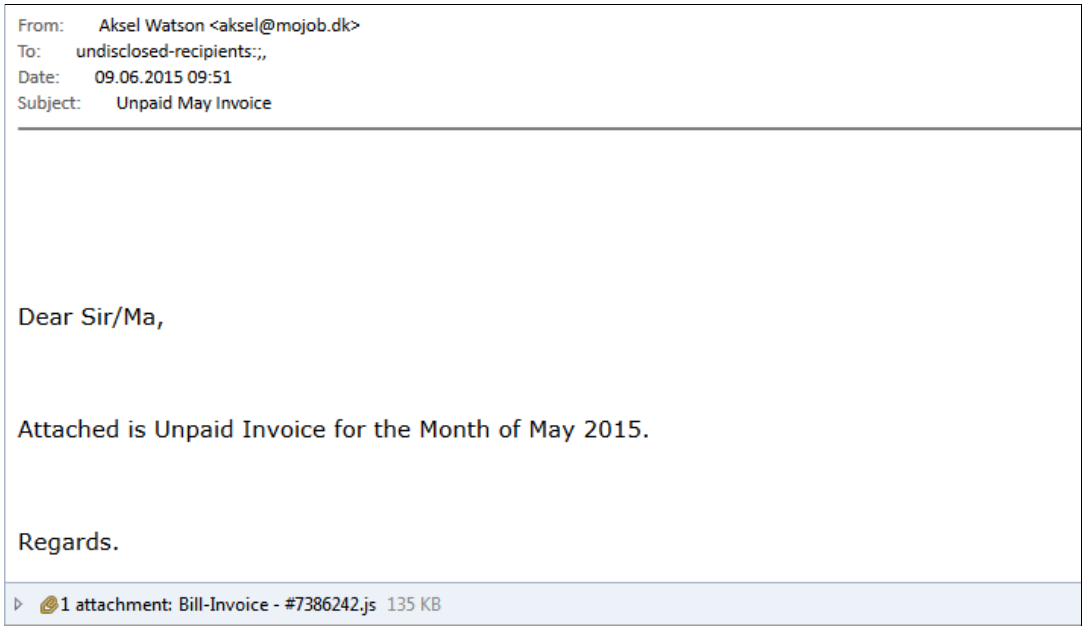
  Inficētā pielikuma attēls:

- 02.06.2015. CERT.LV konstatēja „money mule" jeb naudas pārvedēja vervēšanas mēģinājumus sociālajā tīklā Draugiem.lv. Par šo faktu un identificēto lietotāju tika informēta Valsts policija.

- 15.06.2015. CERT.LV informēja par jaunu mēstuļu kampaņu. Izsūtītie e-pasti pielikumā saturēja kaitīgu JavaScript dokumentu.

  Attēls:



- 15.06.2015. Atkārtoti tika izsūtīti e-pasti ar DNB pikšķerēšanas lapas saiti. CERT.LV sazinājās ar uzturētājiem un lapa tika slēgta.
- 26.06.2015. Ar CERT.LV sazinājās Lattelecom un informēja, ka internetā tika izplatīta krāpnieciska aptauja Lattelecom vārdā.

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 5. un 8.punktā.

3. Rekomendācijas par informācijas tehnoloģiju risku novēršanu (komunikācija ar sabiedrību).

Pārskata periodā CERT.LV pārstāvji sniedza komentārus radio un televīzijā, informēja ziņu portālus par jaunākajām aktualitātēm un ievietoja informāciju par CERT.LV pasākumiem, un aktuālākajiem drošības apdraudējumiem arī CERT.LV sociālo tīklu kontos un mājas lapā.

1) Intervijas un ziņas radio:

- 10.04. CERT.LV pārstāvis piedalījās LKR raidījumā "Atklāti par patiesību" par tēmu „Bērnu un pusaudžu drošība internetā.
- 22.04. CERT.LV pārstāvis sniedza komentāru Latvijas Radio ziņām par kiberdrošības situāciju Latvijā.
- 23.04. CERT.LV pārstāvis piedalījās Latvijas Radio raidījumā "Kā labāk dzīvot" par tēmu „Kā pasargāt naudu, lai to no bankomāta neizņem zaglis? Ko darīt, ja esam apzagti?"
- 15.05. CERT.LV pārstāvis sniedza interviju Latvijas Radio 1 raidījumā "7 dienas Eiropā".
- 02.06. CERT.LV pārstāvis sniedza interviju LR4 ziņās par Trojas vīrusiem.

2) Sižeti televīzijā, tiešraides:

- 01.04. CERT.LV pārstāvis sniedza komentāru TV3 raidījumam par telefonu uzlaušanas iespējām.
- 13.05. Tika sniegta intervija Rīga TV 24 raidījumā „Brokastis ar ekspertu".
- 30.06. Tika sniegta intervija LTV7 ziņām par prezidentūras norisi no kiberdrošības viedokļa.

3) Ziņas portālos:

- 07.04. Bankas neatklāj, cik bieži tiek nozagti mūsu karšu dati - kasjauns.lv
- 13.04. Uzvedība internetā jāapgūst tāpat kā noteikumi uz ceļa - IR.LV
- 22.04. Norisinās lielākās tehniskās kiberdrošības mācības - lvportals.lv
- 03.05. Lielākā IT drošības problēma ir izglītība, uzsver Kiberaizsardzības vienības komandieris - delfi.lv
- 07.05. LIKTA: prezidentūras laikā īpaši pieaudzis kiberuzbrukumu skaits Latvijai - la.lv
- 11.05. Aprīlī „Cert.lv" reģistrējusi 187 augstas prioritātes IT drošības incidentus - tvnet.lv
- 15.05. Aizsardzības ministrijas valsts sekretārs Japānā diskutēs par kiberdrošības jautājumiem – Leta.lv
- 02.06. Telekomunikāciju pakalpojumu rēķinu izskatā izplatās inficēti e-pasti - diena.lv
- 02.06. UZMANĪBU: Brīdina par inficētu e-pastu izplatīšanos - NRA.lv
- 15.06. Aicina būt uzmanīgiem – ļaundari uzsāk jaunu mēstuļu kampaņu - delfi.lv
- 16.06. „Cert.lv": Izplatās e-pasti ar kaitīgu «JavaScript» pielikumu - tvnet.lv
- 16.06. Brīdinājums e-pasta lietotājiem: ļaundari uzsākuši jaunu „kampaņu" - apollo.lv
- 16.06. Brīdina par e-pastiem ar kaitīgu "JavaScript" pielikumu - la.lv

4) **CERT.LV tīmekļa vietnes:**

Pārskata periodā vietnē https://www.cert.lv publicētas 26 ziņas, sniegta informācija par CERT.LV organizētiem un starptautiska mēroga pasākumiem, publicēta IT drošības incidentu statistika un CERT.LV prezentācijas.
Populārākā sadaļa bija par jaunākajiem vīrusiem, kas tika apskatīta 8 930 reizes. Nākamā populārākā sadaļa bija ziņa par semināru „Esi Drošs 2" ar 1 552 apmeklējumiem un ziņa *„Izplatās inficēti e-pasti, kas pielikumā satur kaitīgu .CHM dokumentu."* ar 1 316 apmeklējumiem.

Kopā CERT.LV mājaslapai bijuši 15 861 skatījumi, kurus veido 11 088 unikāli lapu skatījumi no 109 valstīm. Arī šajā periodā lielākā daļa – 81,63 % apmeklējumu bija no Latvijas.

CERT.LV uzturētajai vietnei https://www.esidross.lv pārskata periodā bija 12 725 lapu skatījumi, no tiem 10 071 unikāli lapu skatījumi.

Esidross.lv publicētie raksti:

- „Kā radīt tiešsaistes servisu narkotiku tirdzniecībai un nokļūt cietumā uz atlikušo mūžu".
- „Zelta likumi tavu datu drošībai internetā".

Lai uzlabotu portāla esidross.lv rakstu publicēšanas biežumu un publicētu aktuālu informāciju, sākta sadarbība ar SANS institūtu par OUCH! ikmēneša ziņu lapas tulkošanu un publicēšanu latviešu valodā.

5) **CERT.LV sociālo tīklu konti:**

Twitter kontā https://twitter.com/certlv publicētas 42 ziņas. Pārskata perioda beigās konta sekotāju skaits bija 1253. Kopumā 154 reizes @certlv ziņas tikušas „retvītotas" jeb pārpublicētas.

CERT.LV Facebook profilā http://www.facebook.com/certlv pārskata periodā publicētas 30 ziņas. Pārskata perioda beigās lapas sekotāju skaits bija 199.
Iesaistītie unikālie lietotāji (dalīšanās ar saturu, „like" spiešana vai klikšķis uz ziņas vai saites) pārskata periodā bija 650.

CERT.LV draugiem.lv lapā http://www.draugiem.lv/certlv publicētas 42 ziņas. Pārskata perioda beigās lapas sekotāju skaits bija 63.

Sociālajā tīklā Google+ https://www.google.com/+CertLv publicētas 28 ziņas. Kontam ir 25 sekotāji.

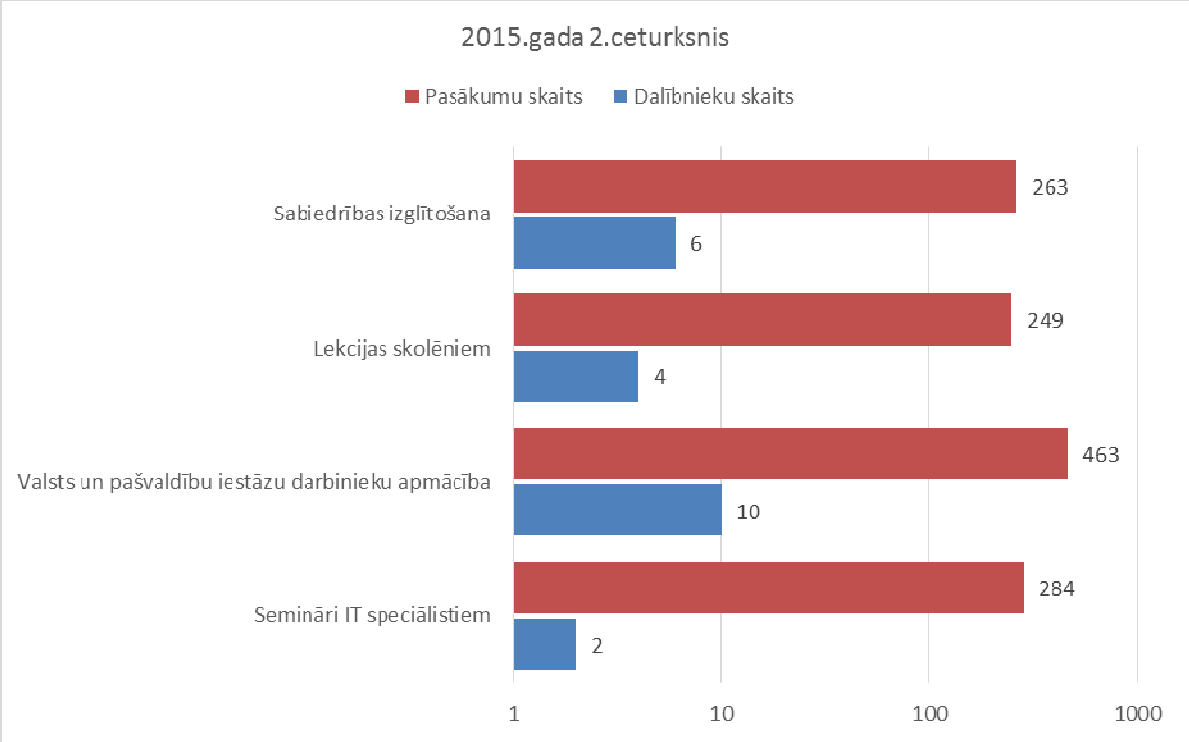
4. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

29.aprīlī CERT.LV rīkoja semināru "Esi drošs - 2". Seminārā tika apskatītas tādas tēmas kā izmaiņas IT drošības likumā, mobilo iekārtu lietošanas riski, „whitelist" saraksta izmantošana aizsardzībai pret vīrusiem un piekļuves lieguma uzbrukumi ES prezidentūras laikā. Semināru atbalstīja SIA DSS un LMT. Pasākumu apmeklēja 254 dalībnieki, savukārt semināra tiešraidi skatījās 249 unikālie apmeklētāji.

No 11. līdz 12.maijam CERT.LV organizēja starptautisku ENISA semināru "CERTs in Europe", kas bija domāts Eiropas valstu nacionālajām un valdības CERT vienībām. Seminārs fokusējās uz dažādu valstu pieredzi saistītu ar prezidentūru Eiropas Savienības Padomē un Tīklu un informācijas drošības direktīvu.

Noslēgusies CERT.LV veiktā aptauja valsts un pašvaldību iestāžu darbiniekiem "Interneta lietotāju paradumi". Aptaujā piedalījās 771 respondents no 20 iestādēm. Rezultāti tiks prezentēti kādā CERT.LV pasākumā.

Pārskata periodā CERT.LV par IT drošību izglītoja 1259 cilvēkus, iesaistoties 22 izglītojošos pasākumos.



8.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2015.gada 2.ceturksnī

5. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā.

Jūnijā noslēdzās Latvijas prezidentūra Eiropas Savienības Padomē. Pirms Prezidentūras un tās laikā tika ieguldīti nozīmīgi resursi, lai nodrošinātu atbilstošu drošības pakāpi dažādiem valsts un pašvaldību iestāžu tiešsaistes resursiem.

Prezidentūras norises laikā īpaša gatavība reaģēt bija Prezidentūras sākumā, 16.martā, 9.maijā, Austrumu partnerības samita un Digitālās asamblejas laikā. Šajos datumos CERT.LV darbojās paaugstinātas gatavības režīmā, pievēršot īpašu uzmanību kibertelpas situācijas un izmaiņu uzraudzībai.

Sadarbība ar valsts iestādēm incidentu risināšanā aprakstīta atskaites 2.punktā. Zemāk uzskaitītas citas sadarbības tikšanās un konsultācijas.

- 13.04. Tikšanās Aizsardzības ministrijā par MK noteikumu projektu „Kārtība, kādā valsts un pašvaldības institūcijas nodrošina informācijas un komunikācijas tehnoloģiju sistēmu atbilstību minimālajām drošības prasībām".
- 15.05. Sadarbības tikšanās Ārlietu ministrijā.
- 15.05. Tikšanās par Ekonomiskās sadarbības un attīstības organizācijas OECD intervijām.
- 20.05. CERT.LV piedalījās pašvaldību savienības organizētā sanāksmē par drošības situāciju Latvijas pašvaldībās un topošajiem Ministru kabineta noteikumiem par minimālajām drošības prasībām informācijas sistēmām.
- 17.06. Dalība starpinstitūciju sanāksmē par MK noteikuma projektu "Grozījumi Ministru kabineta 2014. gada 12. augusta noteikumos Nr. 471 „Parakstu vākšanas tiešsaistes sistēmu drošības un tehniskās prasības".
- 17.-18.06. CERT.LV pārstāvis piedalījās Digitālajā asamblejā.
- 19.06. Notika Eiropas Savienības valstu telekomunikāciju atašeju vizīte CERT.LV, tika prezentēta CERT.LV darbība un sasniegumi.

6. Valsts un pašvaldību institūciju un elektronisko sakaru komersantu uzraudzība par Informācijas tehnoloģiju drošības likumā noteikto pienākumu veikšanu.

IT drošības likums nosaka, ka Valsts un pašvaldību institūcijām jāinformē CERT.LV par nozīmēto atbildīgo personu, kura iestādē īsteno informācijas tehnoloģiju drošības pārvaldību.

Līdz 2015.gada 30.jūnijam CERT.LV ir apkopojis informāciju par 1337 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību vai ar to saistītas.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 nosaka kārtību, kādā Elektronisko sakaru komersantiem (turpmāk – ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai.
Saistībā ar rīcības plāniem nav izmaiņu attiecībā pret 2015.gada 1.ceturksni - ir saņemtas atbildes no 63 ESK. Līdz 30.jūnijam saņemti 58 ESK rīcības plāni, kā arī 5 ESK rakstiski apliecinājuši, ka neuztur publisko elektronisko sakaru tīklu, no kuriem 1 ESK nodevis visu ārpakalpojumā citam ESK.

Pārskata periodā CERT.LV nav saņēmis nevienu ziņojumu no ESK par drošības vai integritātes pārkāpumiem, kas būtiski ietekmējuši elektronisko sakaru tīkla darbību vai pakalpojumu sniegšanu un atbilst Informācijas tehnoloģiju drošības likuma (ITDL) 9.panta pirmās daļas 2.punktam.).

Pārskata periodā CERT.LV nav konstatējis apdraudējumus, kuru atrisināšanai būtu nepieciešams slēgt galalietotājam piekļuvi elektronisko sakaru tīklam (ITDL 9.panta pirmās daļas 5.punkts).

7. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām.

No 22.-24.04.2015. notika lielākās starptautiskās kiberdrošības mācības "Locked Shields 2015", kuras organizēja NATO CCDCoE. Mācībās piedalījās vairāk kā 400 kiberdrošības speciālisti no 16 valstīm.
Latvijas - Lietuvas apvienotā komanda 16 komandu konkurencē ieguva 4. vietu, savukārt juridiskajā komponentē Latvijas - Lietuvas komanda bija otra labākā. Pagājušajā gadā šajās mācībās Latvijas - Čehijas apvienotā komanda ieguva 2. vietu.

Latvijas komandu veidoja CERT.LV, Zemessardzes Kiberaizsardzības vienība, eksperti no privātā sektora un Lietuvas CERT kiberdrošības eksperti.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 13.-14.04. CERT.LV pārstāvji piedalījās „One conference" Nīderlandē.
- 16.-17.04. CERT.LV pārstāvis piedalījās „Global Conference on CyberSpace" Hāgā, Nīderlandē, kā arī piedalījās paneļdiskusijā "Computer Security Incident Response Team Maturity".
- 13.04.-16.04. CERT.LV pārstāvis piedalījās FI-ISAC (European FI-Information Sharing and Analysis Center) sanāksmē Nīderlandē, Amsterdamā.
- No 22.04.-24.04. CERT.LV piedalījās starptautiskajās kiberdrošības mācībās "Locked Shields 2015", kuras organizēja NATO CCDCoE.
- 23.-24.04. CERT.LV pārstāvis piedalījās TERENA organizētajos TRANSITS 1 kursos Prāgā, Čehijā.
- 27.04. CERT.LV pārstāvis piedalījās Baltijas valstu sanāksmē Aizsardzības ministrijā „7th Baltic Cyber security Policy Coordination Meeting".
- 05.05.-07.05. CERT.LV pārstāvji piedalījās FIRST Technical Coloquium Amsterdamā, Nīderlandē.
- 06.05. CERT.LV pārstāvji piedalījās ES-ASV-Kanādas kritiskās infrastruktūras aizsardzības ekspertu sanāksmē „6th EU-US-Canada Expert Meeting on Critical Infrastructure Protection" CERT.LV pārstāvis uzstājās ar prezentāciju, "Strengthening IT critical infrastructure protection with everyday CERT.LV activities".
- 11.-12.05. CERT.LV pārstāvji uzstājās ar prezentācijām par CERT.LV pieredzi Prezidentūras laikā un CERT.LV gatavošanos NIS direktīvas ieviešanai ENISA organizētajā seminārā „CERTs in Europe", kas notika Rīgā.
- 13.05. CERT.LV pārstāvis piedalās paneļdiskusijā un uzstājās ar prezentāciju par Responsible Disclosure ENISA un Aizsardzības ministrijas organizētā konferencē, kas notika Rīgā Latvijas prezidentūras ES padomē pasākumu ietvaros.
- 14.05. Notika sadarbības tikšanās ar NCSC-NL pārstāvi, apspriesti jautājumi par gatavošanos Prezidentūrai un incidentiem tās laikā.
- 18.-19.05. CERT.LV piedalījās un prezentēja par "Current situation in Latvia": 2ND BALTIC – U.S. Seminar on Critical Energy Infrastructure Protection and Cybersecurity.
- 20.-22.05. CERT.LV pārstāvis piedalījās un vadīja Trusted Introducer un TF-CSIRT sanāksmes Poznaņā, Polijā.

- 18.-22.05. CERT.LV pārstāvis piedalījās Aizsardzības ministrijas organizētā vizītē Japānā, ministrijas Valsts sekretāra delegācijas sastāvā.
- 18.-19.05. CERT.LV pārstāvis piedalījās Ārlietu ministrijas organizētajā ASV un Baltijas kritiskās infrastruktūras aizsardzības un kiberdrošības ekspertu seminārā.
- 25.-29.05. CERT.LV pārstāvis piedalījās CCDCoE organizētajā CyCON konferencē Tallinā, Igaunijā.
- 15.-19.06. CERT.LV pārstāvji piedalījās FIRST konferencē, kas notika Berlīnē, Vācijā, CERT.LV pārstāvis vadīja vairākas sesijas.
- 16.06. CERT.LV pārstāvis piedalījās ENISA organizētajā „EU28 Cloud Security Conference: Reaching the Cloud Era in the European Union", kas notika Rīgā.
- 20.-21.06. CERT.LV pārstāvis piedalījās vispasaules Nacionālo CERTu sanāksmē, kas notika Berlīnē, Vācijā, t.sk. piedalījās paneļdiskusijā par CERTu brieduma pakāpes rādītājiem.

Sadarbība konkrētu incidentu gadījumos aprakstīta pārskata 2.punktā.

8. Citi normatīvajos aktos noteiktie pienākumi.

- 09.04. un 07.05. Notika DEG sanāksmes.
- 09.04. Tikšanās ar Briseles universitātes studenti, intervija maģistra darbam.
- 10.04. Sadarbības tikšanās ar LMT par IT drošības konferences organizēšanu.
- 10.04. Tikšanās ar AIM un sadarbības partneriem par projekta „Cyber Hygiene" ieviešanu.
- 28.04. Tikšanās ar Zemessardzes Kiberaizsardzības vienības pārstāvjiem.
- 30.04. Sadarbības tikšanās ar Kaspersky Lab pārstāvjiem.
- 05.05. Tikšanās ar Latvijas Universitātes studenti par maģistra darba rakstīšanu par IT drošības tēmu.
- 13.05. Dalība sanāksmē par Kiberjaunsardzes apmācības iespējām.
- 14.05. Notika telefonintervija ar „Deliotte" par pētījumu par CERTu un tiesībaizsardzības institūciju sadarbību.
- 28.05. CERT.LV pārstāvis piedalījās „Baltijas kiberdrošības forumā 2015".
- 11.06. Notika CERT.LV un ISACA Latvijas nodaļas IT drošības konferences plānošanas sanāksme.

9. Aģentūras papildu pasākumu veikšana.

Atskaite par Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra ziņojumu līnijas darbību.

Latvijas interneta asociācijas „Net-Safe Latvia" drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.04.2015. līdz 30.06.2015. ir saņēmusi un izvērtējusi 140 ziņojumus. No tiem 61 ziņojuma saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 14 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 7 ziņojumos konstatēta personas goda un cieņas aizskaršana. Par finanšu krāpšanas mēģinājumiem internetā saņemti 13 ziņojumi, 29 ziņojumu saturs nav bijis pretlikumīgs, 16 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 9 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 44 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites. 1 ziņojums par naida kurinošu saturu ir nosūtīts ZL sadarbības partnerim Latvijas cilvēktiesību centram izvērtēšanai un turpmāko darbību veikšanai.

Pārskata periodā, sadarbojoties ar Valsts policiju un interneta pakalpojumu sniedzējiem, izdevies dzēst visus bērnu seksuālās izmantošanas materiālus, kas tika uzturēti Latvijā un par kuriem tika saņemti ziņojumi. Vidēji nelegālā satura dzēšanai bija nepieciešamas 14 dienas.

Salīdzinoši ar iepriekšējā pārskata periodu, 2015. gada pirmajiem trim mēnešiem, 2015. gadā no maija līdz jūnijam vērojams kopējo saņemto ziņojumu kritums par aptuveni 50%, kas ir daļēji skaidrojams ar vasaras periodu, kad ir zemāka ziņotāju aktivitāte, par ko liecina arī iepriekšējo gadu ziņojumu uzskaite.

2015.gada 27.jūlijā

Sagatavotājs – Svetlana Amberga
Tālrunis: 67085888
E-pasts: svetlana.amberga@cert.lv