Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

LATVIJAS REPUBLIKAS
AIZSARDZĪBAS MINISTRIJA

Publiskais pārskats par CERT.LV uzdevumu izpildi

2014

2014. gada 2. ceturksnis (01.04.2014. – 30.06.2014.)

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

Saturs

Kopsavilkums

Pārskata periodā notika vairāki pasaules mēroga drošības incidenti, kas skāra arī Latvijas interneta lietotājus un servisa uzturētājus. Kā viens no svarīgākajiem incidentiem bija 7. aprīlī izziņotā OpenSSL ievainojamība jeb „ssl heartbleed". Ievainojamība skāra miljoniem serverus un lietotājus visā pasaulē un CERT.LV aktīvi strādāja pie resursu turētāju apzināšanas un informēšanas Latvijā. Par spīti ievainojamības plašajiem mērogiem, Latvijas pakalpojumu sniedzēju attieksme bija vienaldzīga – gandrīz neviens neizplatīja paziņojumu par to, ka serviss ir bijis skarts un lietotājiem nepieciešams veikt paroles maiņu. Šādi apjomīgi incidenti parāda to, ka informatīvi izglītojošais darbs ir svarīgs ne tikai ar sabiedrību kopumā, bet arī ar medijiem un mitināšanas pakalpojumu sniedzējiem.

16.aprīlī CERT.LV publicēja pārskatu par OpenX baneru apmaiņas sistēmas ievainojamību, izplatot informāciju par ievainojamību un tās profilakses pasākumiem gan valsts un pašvaldību iestādēm, gan elektronisko sakaru komersantiem, gan medijiem un citiem sadarbības partneriem. Latvijā OpenX izmanto tādas plaši apmeklētas tīmekļa vietnes kā e-klase.lv, cv.lv, boot.lv, diena.lv, kasjauns.lv, lursoft.lv, liepajniekiem.lv, hotcars.lv, tiesraides.lv, ventasbalss.lv un citas. Izmantojot šo ievainojamību, caur vairākiem Latvijas portāliem tika izplatīts bīstamais Gozi banku trojāns.
No 20. līdz 22.maijam CERT.LV un Kiberaizsardzības vienība Latvijas-Čehijas apvienotās komandas sastāvā piedalījās NATO Kiberaizsardzības izcilības centra organizētajās „Locked Shields 2014" mācībās un ieguva 2.vietu. Šogad mācībās piedalījās 12 aizsargkomandas no visas Eiropas.

Pārskata periodā CERT.LV reģistrēja un apstrādāja 736 augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 753 augstas prioritātes incidenti, bet 2013.gada 2.ceturksnī 1153 augstas prioritātes incidenti.

Salīdzinot augstas prioritātes incidentus ar to pašu periodu pirms gada, vērojams liels samazinājums, jo kopš 2014.gada sākuma notika pāreja uz automātisko incidentu uzskaites sistēmu, kas vairākus incidentu veidus apstrādā automātiski, nevis manuāli, kā tas bija agrāk, līdz ar to, pateicoties procesu automatizācijai, augstas prioritātes incidentu skaitam ir tendence samazināties. Savukārt, zemas prioritātes incidentu skaits ir palielinājies.

2014.gada 2.ceturksnī CERT.LV reģistrēja 102 596 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti 81 276 zemas prioritātes incidenti, bet 2013.gada 2.ceturksnī - 40 721 zemas prioritātes incidents. Salīdzinot zemas prioritātes incidentus ar to pašu periodu pirms gada, vērojams liels pieaugums, ko var izskaidrot arī ar to, ka CERT.LV ir palielinājies sadarbības partneru skaits, kas ziņo par zemas prioritātes incidentiem.

Lielāko sabiedrības un mediju uzmanību pārskata periodā izpelnījās pārlūka Internet Explorer ievainojamība. CERT.LV aicinājumu atturēties no pārlūka lietošanas, kamēr nav novērsta ievainojamība, tiražēja lielākie mediji gan internetā, gan televīzijā. Lielo mediju interesi var skaidrot ar to, ka arī komercbankas vēlējās brīdināt savu internetbanku lietotājus par

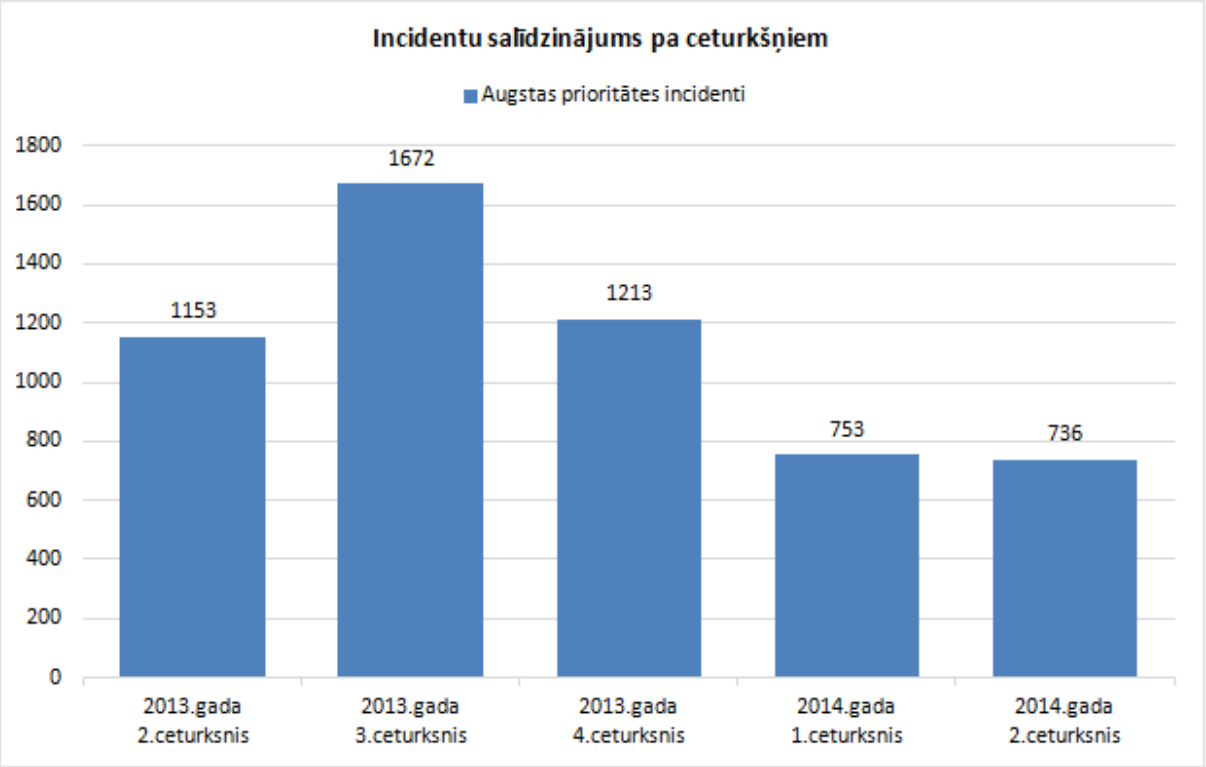
ievainojamības sekām un izplatīja paziņojumu presei vienlaikus ar CERT.LV.

Kopā pārskata periodā CERT.LV piedalījās 24 pasākumos, apmācot 1537 cilvēkus, publicēja 3 jaunus rakstus portālā www.esidross.lv, 46 jaunas ziņas portālā www.cert.lv, piedalījās 5 radio pārraidēs un 4 televīzijas sižetos.

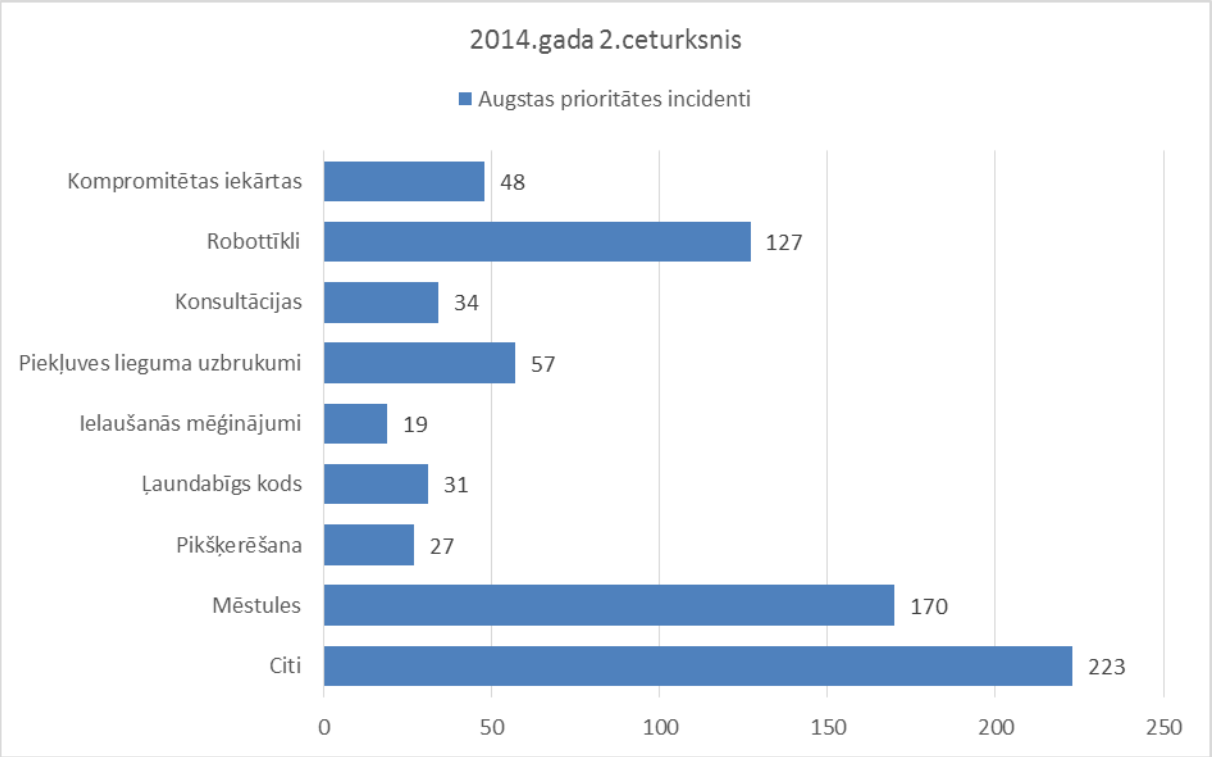
1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

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.

2014.gada otrajā ceturksnī CERT.LV apstrādāja 736 augstas prioritātes incidentus, kas ir par 17 incidentiem jeb 2,25 % mazāk nekā 2014. gada pirmajā ceturksnī un par 417 incidentiem jeb 36,16 % mazāk nekā 2013.gada otrajā ceturksnī.

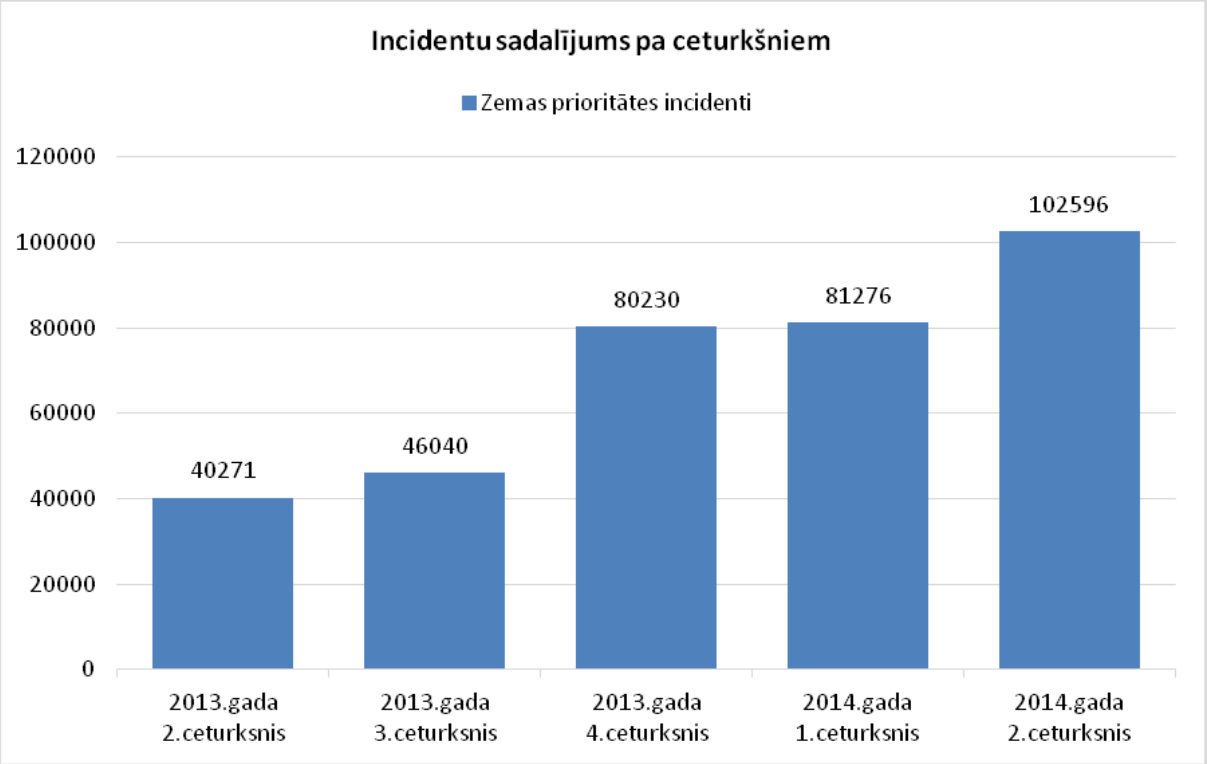


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2013. un 2014. gadā.



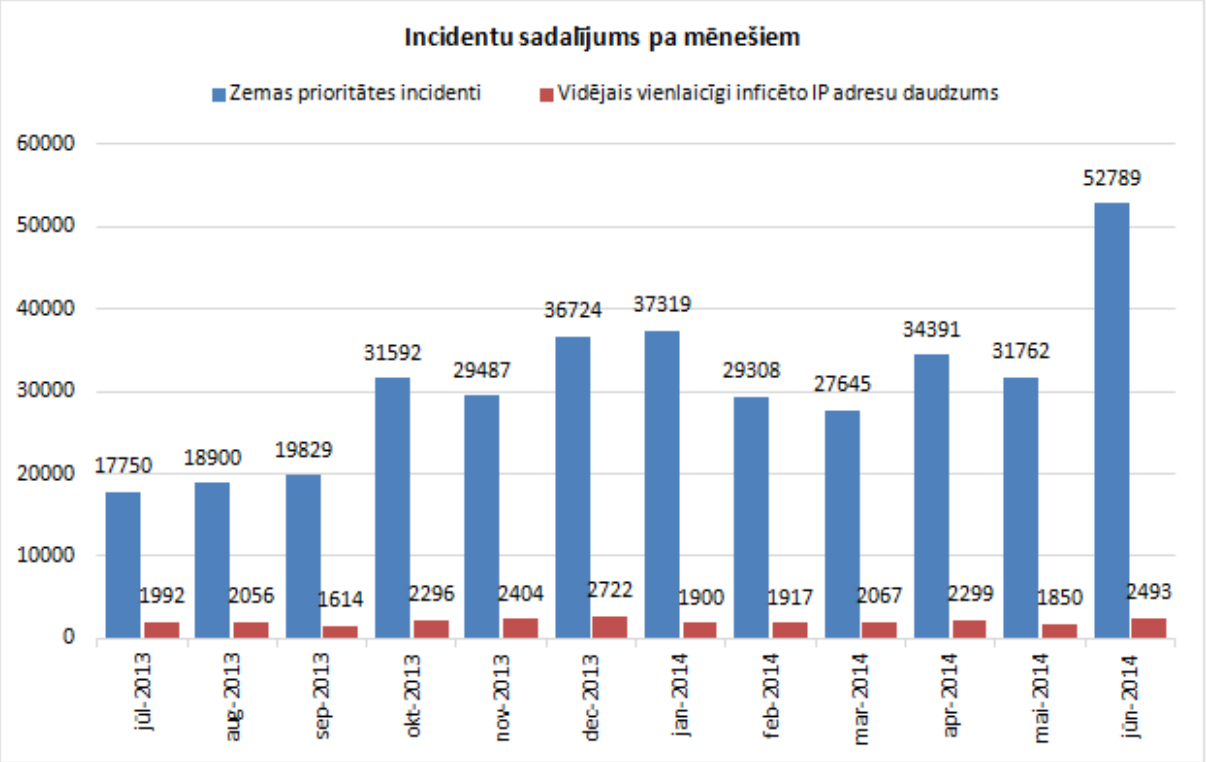
2.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2014.gada 1.aprīļa līdz 30.jūnijam.

2014.gada 2.ceturksnī CERT.LV reģistrēja 102 596 zemas prioritātes incidentus, kas ir par 21320 jeb 26,23 % vairāk nekā 2014. gada 1. ceturksnī un par 61876 incidentiem jeb 154,76 % vairāk, nekā 2013.gada 2.ceturksnī.



3.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem 2013. un 2014.gadā.

Salīdzinot ar 2014.gada pirmo ceturksni, reģistrēto zemas prioritātes incidentu apjoms 2014.gada 2.ceturksnī ir būtiski pieaudzis. Tas skaidrojams ar to, ka 2014.gadā notika pāreja uz jaunu automātisko incidentu uzskaites sistēmu, kas vecinājusi augstas prioritātes incidentu samazinājumu, bet zemas prioritātes incidentu pieaugumu, jo palielinājās automātisko ziņojumu skaits no sadarbības partneriem un apstrādes automatizācija. Turklāt kopš 2013.gada decembra CERT.LV pati ir kā ziņošanas avots par dažādiem incidentiem, piemēram, OpenSSL un OpenX incidentu gadījumos, kad CERT.LV veica iesaistīto resursu apzināšanu. Kā arī CERT.LV veikto pētījumu ietvaros (Nedroši DNS serveri, NTP serveri, un mājas/ofisa maršrutētāji) iegūtā informācija par ievainojamām iekārtām Latvijas tīklos tiek nogādāta līdz gala lietotājam caur iniciatīvu „Atbildīgs IPS" un informācijas avots ir CERT.LV.



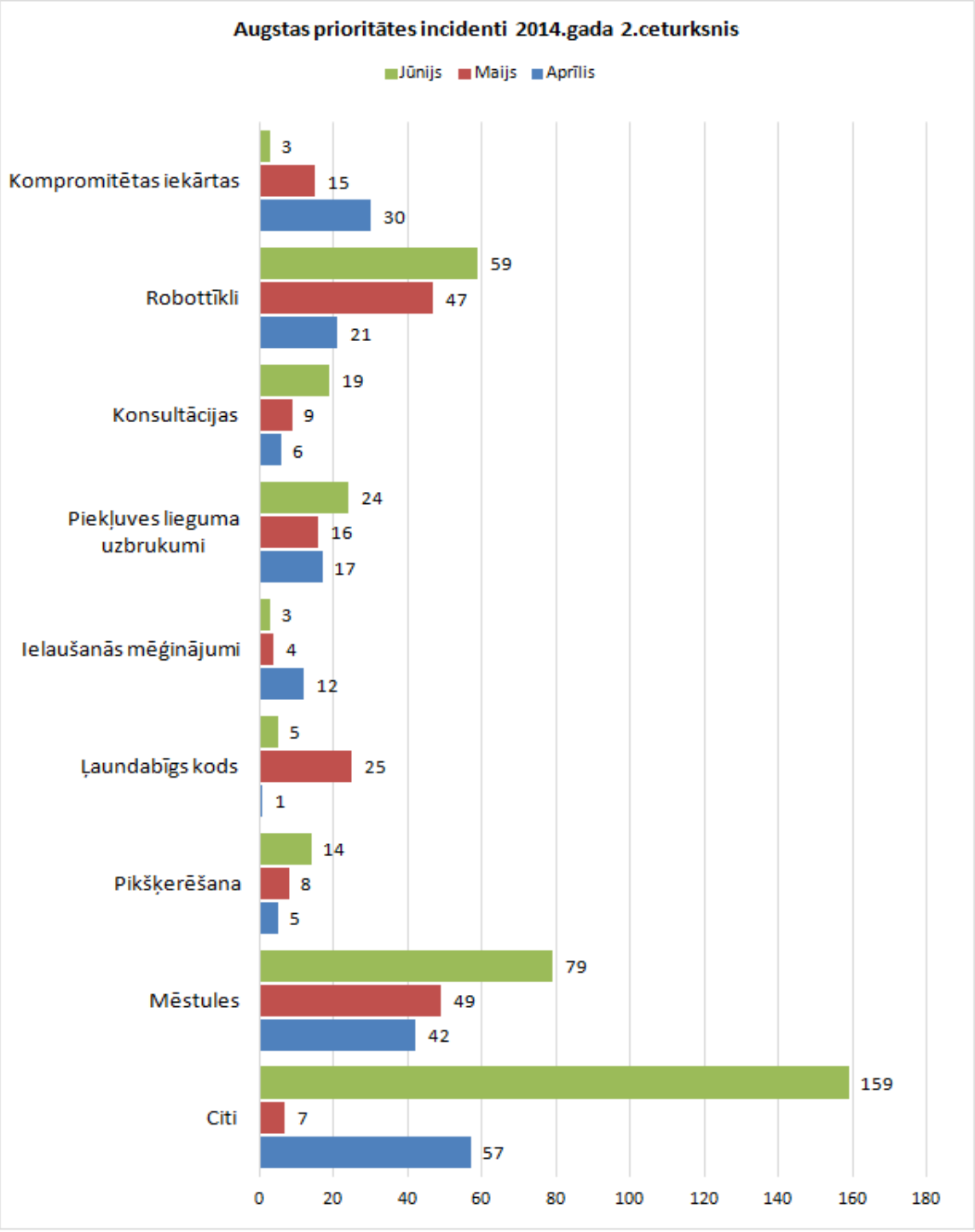
4.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums 12 mēnešu laikā.

2014.gada jūnijā, salīdzinot ar maiju, vērojams zemas prioritātes incidentu palielinājums, jo klāt nāca jauni ziņojumu avoti. 4.attēlā redzams, kā mainījies zemas prioritātes incidentu skaits un vidējais inficēto IP adrešu daudzums pēdējā gada laikā.

Katru mēnesi CERT.LV rēķina arī vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Aprīlī šis skaits bija 2299, maijā – 1850, bet jūnijā – 2493 inficētas IP adreses. 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 interneta pakalpojumu sniedzējiem (IPS), kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". Pārskata perioda beigās atbildīgo IPS kopskaits saglabājās bez izmaiņām – 13

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

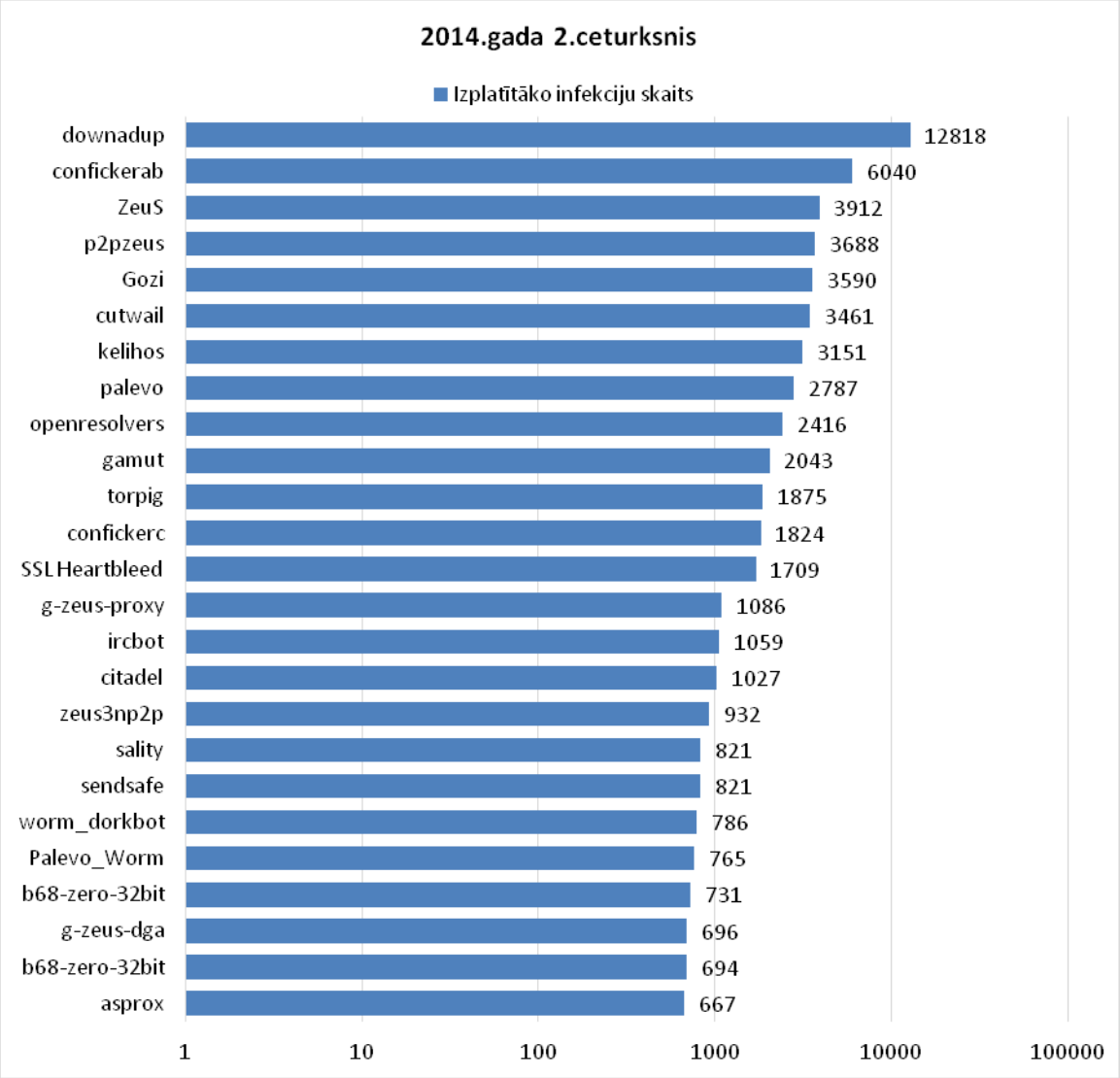
Pārskata periodā CERT.LV ir reģistrējis un apstrādājis 736 augstas prioritātes incidentus. Zemāk redzams augstas prioritātes incidentu sadalījums 2. ceturksnī pa tipiem un pa mēnešiem.



5.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem un pa mēnešiem.

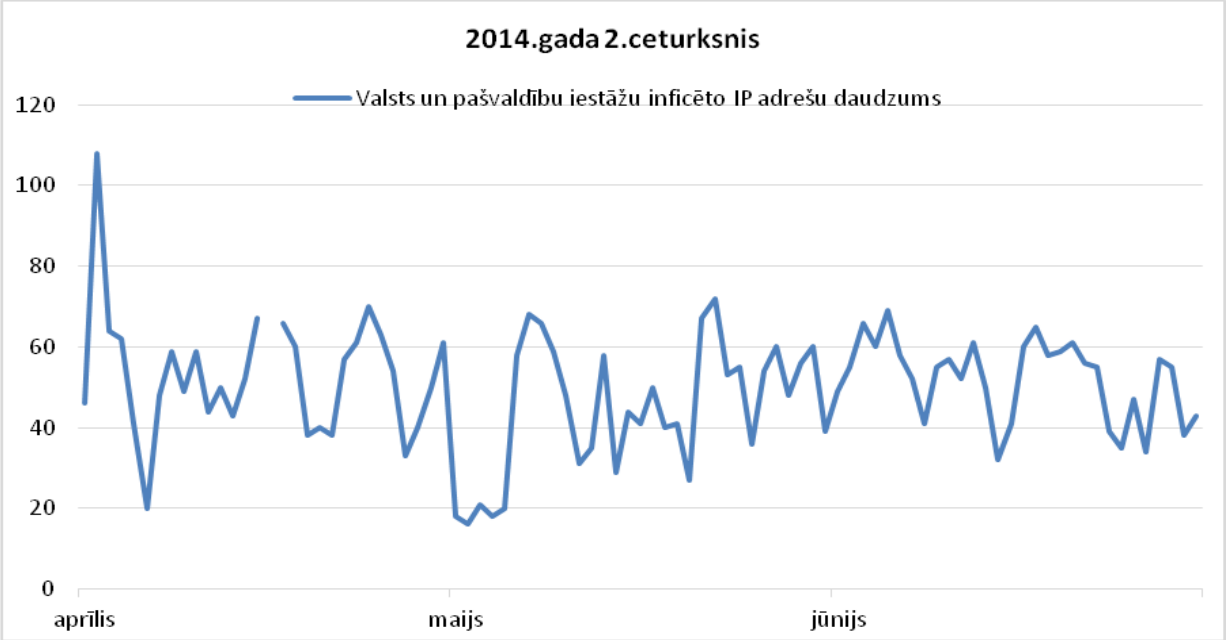
Attiecībā pret iepriekšējo periodu ir pieaudzis kompromitētu iekārtu daudzums, tāpat arī ļaundabīga koda izplatība, kā arī pikšķerēšana. Samazinājums vērojams robotu tīklu izplatībā, piekļuves lieguma uzbrukumu un ielaušanās mēģinājumu izplatībā.

Pārskata periodā CERT.LV reģistrēja 102 596 zemas prioritātes incidentus, zemāk aplūkojams grafiks, kas demonstrē incidentu sadalījumu pa infekciju tipiem.



6.attēls - CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā no 2014.gada 1.aprīļa līdz 30. jūnijam pa infekciju tipiem.

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 regulāri informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā inficētas. Pārskata periodā CERT.LV ir bijusi informācija par 247 inficētām IP adresēm valsts un pašvaldību institūciju tīklos.



7.attēls – Valsts un pašvaldību iestāžu inficēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2014.gada 2.ceturksnī pa mēnešiem.

7.attēlā redzamas izmaiņas katras dienas saņemtajos ziņojumos no valsts un pašvaldību iestādēm.

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

2014. gada 2.ceturksnī notika virkne dažādu uzbrukuma kampaņu, kas bija mērķētas tieši uz Latvijas interneta un internetbanku lietotājiem. Bija vērojama arvien pieaugoša leģitīmo resursu nesankcionēta izmantošana ļaunatūras izplatīšanā. Pamatā notika interneta vietņu izmantošana banku trojāna Zeus un Gozi izplatīšanā, kura sekas ir simtiem inficētu apmeklētāju datori, kurus tālāk izmanto nelikumīgai internetbankas operāciju pārtveršanai un naudas zādzībām no kontiem. Kļuvis zināms, ka Latvijā nenoskaidrots grupējums ir realizējis vismaz 3 saistītas uzbrukumu kampaņas no 2013.g oktobra līdz 2014.g martam. („Banku vīruss", „Nodokļu vīruss" un Gozi banku trojāna izplatīšana caur leģitīmām tīmekļa vietnēm).

No interneta lietotāju puses pieaug tendence tiešsaistē skatīties videomateriālus. Diemžēl šādu servisu nodrošinošie portāli bieži tiek izmantoti apmeklētāju datoru inficēšanai. Visbiežāk uzbrukums apmeklētājam tiek realizēts ar kaitniecisku kodu saturošu reklāmas baneru izvietošanu. Šādu uzbrukumu riska mazināšanai ieteicams lietot specializētu programmatūru, kas bloķē interneta reklāmas, vai nepieļauj klienta puses (client side – javascript/flash) skriptu izpildi.

Zemāk uzskaitīti svarīgākie pārskata periodā risinātie incidenti un to novēršana:

- 01.04. Pēc CERT.LV ziņojuma kādā valsts iestādē tika atklāti divi inficēti datori. Atbildīgā

persona tika informēta.

- 02.04. CERT.LV veica banneru apmaiņas sistēmas OpenX incidenta analīzi. Tika noskaidrots, ka vairākas Latvijā populāras tīmekļa vietnes ilgstoši tika izmantotas dažādu vīrusu izplatīšanai, izmantojot ievainojamu OpenX versiju. Vienā no pēdējām uzbrukuma kampaņām caur ievainojamu OpenX baneru apmaiņas sistēmu tika izplatīts banku trojāns "Gozi". Vīrusa izplatīšanas kampaņa varētu būt saistīta ar tā dēvētā „VID vīrusa" izplatīšanas kampaņām. Incidenta risināšanā tika iesaistītas arī ārvalstu CERT komandas. Informācija par ievainojamību guva publicitāti arī medijos. Reklāmas baneru apmaiņas sistēmu trūkumus, pēdējo 2 gadu laikā noziedznieki bieži izmanto, lai izplatītu vīrusus caur plaši apmeklētām un populārām tīmekļa vietnēm un ziņu portāliem. Lietotāji sevi var mēģināt pasargāt, izmantojot specializētu programmatūru, kas bloķē interneta reklāmas un klienta puses skriptus (client side scripts – javascript/flash/..)
- 03.04. CERT.LV sniedza konsultāciju kāda uzņēmuma speciālistam par Latvijā izmantotajām datorvīrusu izplatīšanas shēmām un veicamajiem aizsardzības pasākumiem.
- 04.04. Tika sniegta palīdzība vairākiem Facebook lietotājiem kaitīga skripta izvākšanā no viņu profila.
- 08.04. CERT.LV uzsāka OpenSSL jeb tā dēvētās „ssl heartbleed" ievainojamības koordinēšanas un apzināšanas procesu Latvijā. Ievainojamība ļāva nesankcionēti iegūt sensitīvus datus no serveriem, kas izmantoja ievainojamu OpenSSL pakotni. Sākotnēji Latvijā ievainojamībai tika pakļautas vismaz 1300 vietnes. Visu pārskata periodu CERT.LV strādāja pie resursu turētāju informēšanas un problēmas risināšanas.
- 10.04. Pēc CERT.LV ziņojuma kādas iestādes tīklā tika identificēts inficēts dators. Atbildīgā persona tika informēta.
- 15.04. Kādas iestādes tīmekļa resursā tika izmantota OpenSSL ievainojamība un uzbrucējs veica sekmīgu, nesankcionētu piekļuvi valsts informācijas sistēmai.
- 15.04. CERT.LV konstatēja, ka kādas valsts iestādes vajadzībām uzturētā vietne satur OpenSSL ievainojamību. Sazinoties ar resursa turētāju, CERT.LV norādīja uz problēmas nopietnību, jo ievainojamība rada risku, ka tiek izpausti lietotāju e-pasti un izvēlētās sistēmas paroles. Ārpakalpojuma sniedzējs norādīja, ka problēma netiek klasificēta kā kritiska, risinājums tika ieviests tikai pēc vairākām dienām.
- 15.04. Kļuva zināms, ka vairāku Rīgas viesnīcu lapām tika izveidotas viltus kopijas. Uzturētāji tika brīdināti par autortiesību pārkāpumiem un pikšķerēšanas mēģinājumu.
- 16.04. Tika saņemts ziņojums no Bank of America par DDoS uzbrukumu no Latvijas IP adresēm. Tika brīdināti IP adrešu īpašnieki.
- 16.04. CERT.LV sniedza palīdzību datorspēļu izstrādājam novērst viltus pozitīvo detekciju kādā no antivīrusu programmām.
- 17.04. Tika konstatētas nopietnas drošības problēmas kādā tiešsaistes norēķinu sistēmā. Izstrādātājs veica labojumus.
- 21.04. Tika atklāti vairāki liela mēroga nesankcionētas informācijas izgūšanas incidenti

vairākās valsts iestādēs. CERT.LV uzsāka apjomīgu izmeklēšanu, identificēti vairāki desmiti inficētu darbstaciju.

- 23.04. Tika sniegta konsultācija privātpersonai, kurai bija nozagta nauda no bankas konta ar datorvīrusa palīdzību.
- 29.04. Interneta pārlūkprogrammā Internet Explorer tika atklāta kritiska ievainojamība. CERT.LV sagatavoja un izsūtīja brīdinājumus atbildīgajām personām un sabiedrībai izvairīties no Internet Explorer pārlūka lietošanas, kamēr ievainojamība netiks novērsta.
- 08.05. Notika masveidīgs DDoS uzbrukums kādas valsts iestādes e-pasta sistēmai, uzbrukums tika bloķēts filtros.
- 08.05. Tika saņemtas ziņas no ārvalstīm par vīrusa Cryptolocker izplatīšanu uz Android ierīcēm. Pārbaudot situāciju, tika konstatēts, ka Latvijā līdz šim novērotas tikai Windows OS paredzētās versijas.
- 09.05. Haktīvistu organizācija, kas sevi dēvē par Cyber Berkut, organizēja apjomīgu DDoS uzbrukumu par godu 9.maijam. Kā uzbrukuma mērķis tika norādītas visas fašistiskās valstis, neprecizējot, kuras tās, viņuprāt, ir. Ņemot vērā politiskos notikumus, CERT.LV veica potenciāla uzbrukuma analīzi un prevencijas pasākumus.
- 11.05. CERT.LV konsultēja privātpersonu par krāpniecisku bankas maksājuma uzdevumu atpazīšanu.
- 14.05. Monitoringa sistēmā tika pamanīti DDoS uzbrukuma draudi vairākiem Ukrainas valsts iestāžu resursiem. Tika brīdināts Ukrainas CERT.
- 15.05. Tika konstatēts datorvīrusa izplatīšanas mēģinājums ES institūciju vārdā. CERT.LV sniedza konsultācijas viltus vēstuļu saņēmējiem.
- 19.05. Latvijā tika novērota īslaicīga vīrusa izplatīšanas kampaņa ar .docm paplašinājuma failiem e-pasta pielikumos. CERT.LV veica incidenta analīzi, rezultātā tika apzināti Latvijā inficētie datori un gala lietotāji ar "Atbildīgs IPS" programmas starpniecību.
- 19.05. Kādas valsts iestādes darbinieka personas dati tika nesankcionēti nopludināti internetā. Tika uzsākta incidenta izmeklēšana. Datu nopludināšana visticamāk veikta no kurjerpakalpojumu komersanta, taču pagaidām nav izdevies noskaidrot iemeslus.
- 25.05. Tika konsultēta privātpersona par nolaupīta Skype konta atgūšanas kārtību.
- 27.05. Kļuva zināms, ka kādas organizācijas vārdā tika veikta bankas datu izkrāpšanas kampaņa. Kaitīgais resurss pēc brīdinājuma tika slēgts un publicēti brīdinājumi.
- 28.05. Tika veikts DDoS uzbrukums kādas skolas tīklam. CERT.LV sniedza konsultācijas par metodēm tā ierobežošanā.
- 29.05. Tika saņemts brīdinājums par drošības problēmām kādā mājas lapā. Bija iespējama lietotāju datu ieguve. Resursa īpašnieki tika brīdināti.
- 30.05. Tika saņemti vairāki brīdinājumi par pikšķerēšanas mēģinājumiem, izmantojot SMS. Informācija tika nodota mobilo sakaru operatoriem.
- 03.06. Tika konstatēts naudas izkrāpšanas mēģinājums internetā ziedojumu veidā. Pēc

pieprasījuma kaitīgā lapa tika slēgta.

- 06.06. Tika sniegta palīdzība kādas iestādes speciālistiem inficēta datora identificēšanā.
- 09.06. Kādas valsts iestādes mājaslapā tika nesankcionēti ievietota saite uz tiešsaistes spēļu vietnēm. Lapas īpašnieki tika brīdināti, lapa tika salabota.
- 11.06. Tika sniegta palīdzība privātpersonai atgūt kontroli pār kompromitētu Gmail kontu.
- 17.06. Masveidā tika izplatīti datorvīrusi, kas maskēti kā neapmaksāti Vācijas uzņēmumu rēķini. Tika informētas iestāžu atbildīgās personas.

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

CERT.LV uzskaita arī uzlauzto un izķēmoto mājas lapu gadījumus.
Šādu gadījumu skaits:
Aprīlī 46, no tiem 43 - Linux, 2 - Windows, 1 – nezināms;
Maijā – 51, no tiem 45 – Linux, 2 - Windows, 2 - nezināmi, 2 – FreeBSD;
Jūnijā – 12, no tiem 11 - Linux, 1 – FreeBSD.

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

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 sadaļa bija par jaunākajiem vīrusiem, (11 992 apmeklējumi), tai seko „Jaunumi" ar 2 769 apmeklējumiem. Trešā populārākā ziņa pārskata periodā bija CERT.LV sagatavotā informācija par drošības atjauninājumiem Internet Explorer ievainojamībai ar 2 404 skatījumiem pārskata periodā.

Kopā CERT.LV mājas lapai bijuši 20 393 apmeklējumi, kurus veido 13 896 unikāli apmeklējumi no 85 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa - 92,23% apmeklējumu bija no Latvijas.

Pārskata periodā CERT.LV tīmekļa vietnē tika publicētas 46 ziņas, sniegta informācija par CERT.LV organizētiem un starptautiska mēroga pasākumiem, publicētas CERT.LV prezentācijas, mediju ziņas un CERT.LV publiskais darbības pārskats par 2014.gada 1. ceturksni.

CERT.LV Twitter kontā https://twitter.com/certlv regulāri tiek publicētas ziņas par dažādiem jaunumiem. Pārskata periodā tika publicētas 90 ziņas, kontam pievienojušies 32 jauni sekotāji un 61 reizi @certlv ziņa ir tikusi „retvītota" jeb padota tālāk.

CERT.LV ir izveidots profils arī sociālajā tīklā Facebook http://www.facebook.com/certlv (pārskata periodā publicētas 87 ziņas) un profils sociālajā tīklā Google+ https://www.google.com/+CertLv (publicētas 87 ziņas), kā arī lapa draugiem.lv - http://www.draugiem.lv/certlv, kurā publicētas 90 ziņas.

CERT.LV uztur arī pieaugušo izglītošanas portālu https://www.esidross.lv. Pārskata perioda laikā portālā ir publicēti 3 jauni raksti, portāls apmeklēts 15 124 (11 587 unikāli) reizes.

Publicētie raksti:

- „Bieži uzdotie jautājumi par mājas datora Windows XP drošību pēc atbalsta beigām" https://www.esidross.lv/2014/04/22/biezi-uzdotie-jautajumi-par-majas-datora-windows-xp-drosibu-pec-atbalsta-beigam
- „Oi, pazudis dators, un planšete, un vēl arī…" https://www.esidross.lv/2014/04/25/oi-pazudis-dators-un-plansete-un-vel-ari
- 23.05.2014. „Rūpes par datu drošību pēc Heartbleed ievainojamības izziņošanas" https://www.esidross.lv/2014/05/23/rupes-par-datu-drosibu-pec-heartbleed-ievainojamibas-izzinosanas

Pārskata periodā tika sniegti arī komentāri radio un televīzijā, kā arī publicētas ziņas portālos. Sīkāka informācija:

1) Intervijas un ziņas radio:

- 08.04. Saruna par Windows XP operētājsistēmas atbalsta beigām Latvijas radio 4 raidījumā „Doma laukums".
- 15.04. CERT.LV pārstāvis sniedza komentāru par drošību internetā Latvijas radio 1 raidījumā „Pēcpusdiena".
- 24.04. CERT.LV pārstāvis sniedza komentāru par OpenSSL ievainojamību Latvijas radio ziņās.
- 30.04. CERT.LV pārstāvis sniedza komentāru par Internet Explorer pārlūka ievainojamību Latvijas radio 4 ziņās.
- 07.05. Saruna Latvijas radio 1 raidījumā „Zināmais nezināmajā" par SSL Heartbleed ievainojamību.

2) Sižeti televīzijā, tiešraides:

- 07.04. Sniegts komentārs par Windows XP operētājsistēmas oficiālā atbalsta beigām LTV1 raidījumā „Rīta panorāma".
- 08.04. Sniegts komentārs par iespēju aizvērt Latvijas mājaslapas, kurās tirgo nelegālas vielas LTV1 ziņās.
- 30.04. Tika sniegta intervija par Internet Explorer ievainojamību LNT ziņās.
- 15.06. Tika sniegta intervija sižetam par kiberdrošību LNT raidījumā „Top 10".

3) Ziņas portālos:

- 10.04. Rīdzinieks par filmas lejuplādi nonāk zem ASV autortiesību sargu lupas - raksts Latvijas avīze
- 10.04. Būtisks brīdinājums visiem interneta lietotājiem - raksts Apollo.lv
- 10.04. „OpenSSL" ievainojamībai pakļautas vismaz 1300 Latvijas vietnes – raksts Tvnet.lv
- 10.04. Iesaka Gmail un citu pakalpojumu lietotājiem nomainīt paroles - raksts Apollo.lv
- 10.04. CERT.LV iesaka Gmail un citu pakalpojumu lietotājiem nomainīt paroles - raksts Diena.lv
- 10.04. CERT.LV iesaka Gmail un citu pakalpojumu lietotājiem nomainīt paroles – raksts Bauskas dzīve
- 11.04. AM: Pastāv nopietni draudi Latvijas iedzīvotāju informācijas drošībai - raksts Apollo.lv

- 16.04. CERT.LV brīdina par interneta reklāmām, kas inficē datorus - raksts Apollo.lv
- 16.04. Interneta reklāmas inficē datoru ar ļaunatūru, lietotājam nezinot- raksts Diena.lv
- 16.04. CERT.LV brīdina par interneta reklāmām, kas inficē datorus – raksts Tvnet.lv
- 16.04. „E-talonu" apmaksas sistēmā atklāj drošības caurumu – raksts Delfi.lv
- 16.04. Ļaundabīga programmatūra, kas izplatās caur baneru apmaiņas sistēmu OpenX, inficē lietotāju datorus – raksts db.lv
- 28.04. Latvijas pārstāvji piedalās kiberdrošības mācībās „Cyber Europe 2014" – raksts Tvnet.lv
- 30.04. Brīdina neizmantot internetbankām Internet Explorer pārlūku - raksts Apollo.lv
- 30.04. Ejot internetbankā aicina neizmantot Internet Explorer pārlūku – raksts db.lv
- 30.04. Aicina neizmantot internetbankām Internet Explorer - raksts Tvnet.lv
- 30.04. Bankas aicina neizmantot internetbankām Internet Explorer pārlūku - raksts Diena.lv
- 30.04. Interneta lietotājus aicina īslaicīgi izvairīties no pārlūka Internet Explorer lietošanas – raksts valmieraszinas.lv
- 30.04. Bankas aicina neizmantot internetbankām pārlūku Internet Explorer - raksts la.lv
- 30.04. Aicina pagaidām neizmantot internetbankai Internet Explorer – raksts ir.lv
- 04.05. Vējonis: Latvijas atbildīgās institūcijas ir spējīgas atvairīt kiberuzbrukumus - raksts Tvnet.lv
- 04.05. Vējonis: Latvijas atbildīgās institūcijas ir spējīgas atvairīt kiberuzbrukumus - raksts Diena.lv
- 04.06. Bāliņa: Informācija internetā jāaizsargā tāpat, kā armijai jāaizsargā valsts – raksts Diena.lv
- 11.06. Internetā jārēķinās ar legālu spiegošanu – raksts NRA.lv
- 26.06. ENISA Executive Director meets with Latvia's secretary of state – raksts Enisa.europa.eu
- 30.06. Iespējai likt sevi "aizmirst" internetā ir gan priekšrocības, gan trūkumi - raksts mansmedijs.lv

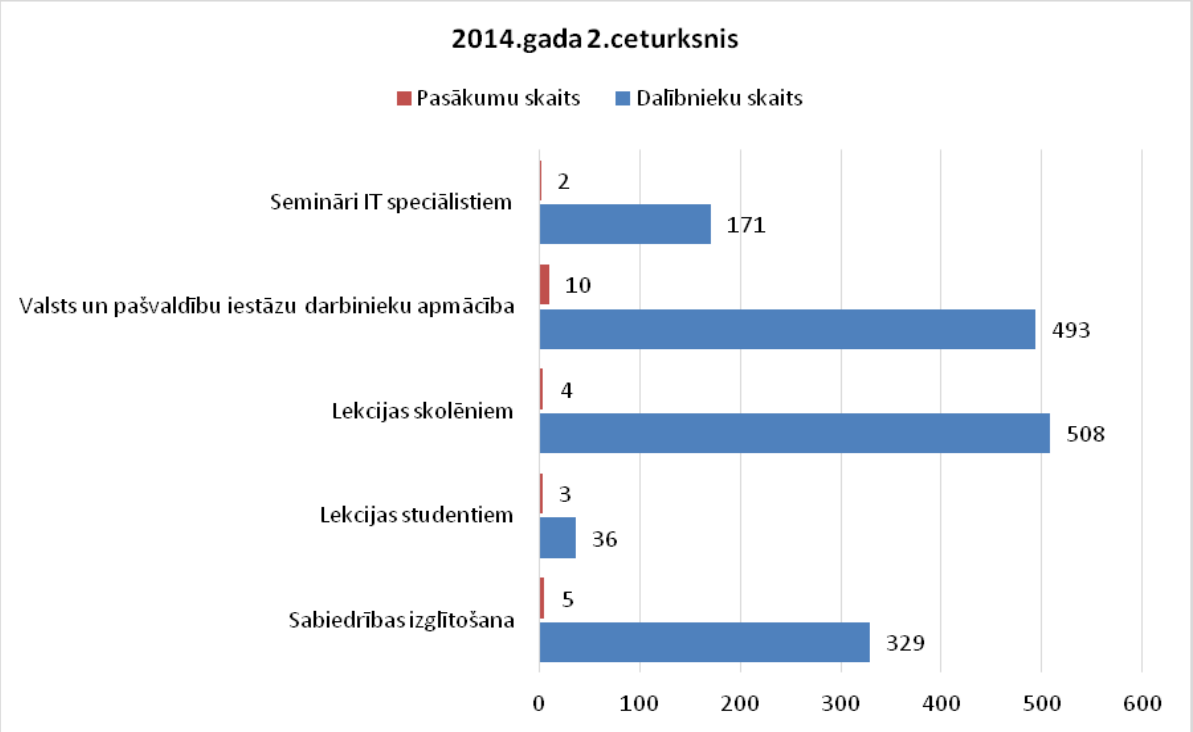
4. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

Pārskata periods sākās ar prezentācijām skolēniem par IT drošību. Aprīlī redzamākais pasākums bija CERT.LV organizētais seminārs „Esi drošs 2" IT speciālistiem, kuru apmeklēja 157 personas. Maijā noslēdzās LU IT drošības specseminārs, kurā ar lekcijām Latvijas Universitātes Datorikas fakultātes studentiem piedalījās arī CERT.LV speciālisti. Pārskata periodu noslēdza apmācības Valsts Kases un Centrālās statistikas pārvaldes darbiniekiem par IT drošību.

Lielu dalībnieku atsaucību guva arī mācības IT speciālistiem „Ievads datora atmiņas ļaunprātīgā izmantošanā", uz kurām pieteicās vairāk dalībnieku, nekā bija iespējas uzņemt. Lai apmierinātu IT speciālistu interesi, CERT.LV šogad plāno organizēt vēl vienas šādas apmācības.

Pārskata periodā tika uzsākts darbs pie gatavošanās IT drošības konferencei rudenī. Konferencei izvēlēta tēma "Apmācīts un atbildīgs IS/IT lietotājs – mūsu visu drošības pamats".

Kopā pārskata periodā CERT.LV par IT drošību ir izglītojis 1537 cilvēkus, piedaloties 24 dažādos pasākumos un lekcijās.



8.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits 2014.gada 2.ceturksnī.

CERT.LV pasākumi pārskata periodā:

1) *Semināri IT speciālistiem:*

- 16.04. Notika CERT.LV organizētais seminārs IT drošības speciālistiem „Ievads datora atmiņas ļaunprātīgā izmantošanā".
- 24.04. Notika CERT.LV organizētais seminārs IT drošības speciālistiem „Esi drošs-2" Kara muzejā.

2) *Valsts un pašvaldību iestāžu darbinieku apmācības:*

- 03.04. CERT.LV pārstāvis sniedza prezentāciju valsts pārvaldes iestāžu darbiniekiem Valsts administrācijas skolā par IT drošības jautājumiem.
- 08.04. CERT.LV pārstāvis sniedza prezentāciju Satiksmes ministrijā par IT drošību.
- 10.04. CERT.LV pārstāvis sniedza prezentāciju Centrālās finanšu līgumu aģentūras darbiniekiem par IT drošību.
- 07.05. CERT.LV pārstāvis sniedza prezentāciju pašvaldības darbiniekiem Jēkabpils novada domē par IT drošības jautājumiem.
- 08.05. CERT.LV pārstāvis sniedza prezentāciju darbiniekiem Valsts kasē par IT drošības jautājumiem.
- 22.05. CERT.LV pārstāvis sniedza prezentāciju darbiniekiem Centrālajā statistikas pārvaldē par IT drošības jautājumiem.
- 28.05. CERT.LV pārstāvis sniedza prezentāciju darbiniekiem Centrālajā statistikas pārvaldē par IT drošības jautājumiem.
- 29.05. CERT.LV pārstāvis sniedza prezentāciju darbiniekiem Valsts kasē par IT drošības jautājumiem.
- 06.06. CERT.LV pārstāvis sniedza prezentāciju darbiniekiem Valsts kasē par IT drošības jautājumiem.
- 10.06. CERT.LV pārstāvis sniedza prezentāciju darbiniekiem Centrālajā statistikas pārvaldē par IT drošības jautājumiem.

3) *Lekcijas skolēniem:*

- 02.04. CERT.LV pārstāvis sniedza prezentāciju skolēniem Madonas pilsētas 1.vidusskolā par IT drošību.
- 15.04. CERT.LV pārstāvis sniedza prezentāciju skolēniem Draudzīgā aicinājuma Liepājas pilsētas 5.vidusskolā par IT drošību.
- 07.05. CERT.LV pārstāvis sniedza prezentāciju skolēniem Jēkabpils Agrobiznesa koledžā par IT drošības jautājumiem.
- 15.05. CERT.LV pārstāvis sniedza prezentāciju skolēniem Rīgas Juglas vidusskolā par IT drošību.

4) *Lekcijas studentiem:*

- 08.04. CERT.LV pārstāvis uzstājās ar prezentāciju LU IT drošības specseminārā studentiem par tēmu „DNS".
- 13.05. CERT.LV pārstāvis novadīja lekciju studentiem Latvijas Universitātes Ekonomikas fakultātē par CERT.LV darbību un IT drošību Latvijā.

- 27.05. CERT.LV pārstāvis uzstājās ar prezentāciju LU IT drošības specseminārā studentiem par tēmu „Sandbox”.

5) *Sabiedrības izglītošana:*

- 07.04. CERT.LV pārstāvis uzstājās ar prezentāciju Latvijas sertificēto personas datu aizsardzības speciālistu asociācijas un „Data Security Solutions” organizētajā seminārā "Digitālā Ēra 2014".
- 11.04. CERT.LV pārstāvis uzstājās ar prezentāciju Swedbank Business Network klientiem par IT drošību.
- 15.04. CERT.LV pārstāvis sniedza prezentāciju Latvijas Tirdzniecības un rūpniecības kameras Liepājas filiāles pārstāvjiem par IT drošību.
- 30.04. CERT.LV pārstāvis uzstājās ar prezentāciju „Dienas Bizness” organizētajā konferencē „Biznesa datu drošība” par IT drošības riskiem.
- 03.06. CERT.LV pārstāvis uzstājās ar prezentāciju SIA „Komerccentrs DATI grupa” rīkotajā konferencē “No drošības līdz…” ar prezentāciju „Kritiskas datorsistēmu ievainojamības un to seku apzināšana”.

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

2014.gadā CERT.LV uzsāka veidot agrās brīdināšanas sistēmu jeb sensoru tīkla projektu, kas nodrošinātu pieslēgto iestāžu informācijas tehnoloģiju resursu augstāku drošības līmeni un savlaicīgi atklātu bīstamus un mērķētus informācijas tehnoloģiju uzbrukumus, uzlabotu iestāžu preventīvās spējas, paātrinot un veicinot bīstamu incidentu novēršanu un laicīgu atrisināšanu.

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

- Aprīlī CERT.LV turpināja sadarbību ar Latvijas prezidentūras Eiropas Savienības Padomē sekretariātu. Katru mēnesi notika vairākas tikšanās ar iesaistītajām pusēm, lai apspriestu infrastruktūras aizsardzības plānu.
- 04.04. CERT.LV tikās ar Aizsardzības ministrijas valsts sekretāru J. Sārtu.
- 10.04. 08.05. un 12.06. notika DEG grupas sanāksmes.
- 17.04. CERT.LV tikās ar Ārlietu ministrijas un LVRTC pārstāvjiem par aizsardzības perimetra plānošanu.
- 25.04. CERT.LV tikās ar Aizsardzības ministrijas valsts sekretāru J. Sārtu.
- 28.04. CERT.LV kopā ar Aizsardzības ministriju sagatavoja atzinumu VARAM par Ministru kabineta noteikumu projektu „Parakstu vākšanas sistēmu drošības un tehniskās prasības".
- 29.04. Notika sadarbības tikšanās ar Ģenerālprokuratūru.
- Maijā notika vairākas tikšanās ar Kiberaizsardzības vienības pārstāvjiem, lai sagatavotos „Locked Shields 2014" mācībām.
- 09.05. Notika tikšanās ar Kiberaizsardzības vienību par „Cyber Europe 2014" mācībām.
- 13.05. Notika sadarbības tikšanās ar Ārlietu ministriju.
- 16.05. Notika Nacionālās IT drošības padomes sēde.
- 20.05. Notika sadarbības tikšanās ar Aizsardzības ministriju.
- 06.06. CERT.LV tikās ar Aizsardzības ministrijas valsts sekretāru J.Sārtu.
- 10.06. CERT.LV pārstāvis tikās ar Aizsardzības ministrijas pārstāvjiem.
- 13.06. CERT.LV sadarbībā ar Kiberaizsardzības vienības pārstāvjiem veica incidentu analīzi, lai trenētu abu komandu sadarbību.
- 17.06. CERT.LV tikās ar Latvijas Komercbanku asociācijas biedriem, lai pārrunātu sadarbības iespējas ar finansu sektorā strādājošām iestādēm. CERT.LV piedāvās sadarbības līgumu, kas ļaus uzlabot un stiprināt sadarbību cīņā ar IT drošības

incidentiem, kas skar elektroniskos maksājumus.

- 20.06. Notika sadarbības tikšanās ar Centrālo vēlēšanu komisiju par IT drošības testu veikšanu 2014. gada vēlēšanu sistēmām.

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 2014.gada 30.jūnijam CERT.LV ir apkopojis informāciju par 622 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 (turpmāk – ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai. Līdz 30.jūnijam plānus ir iesnieguši 58 ESK. Mazajiem ESK ir pieejams CERT.LV izstrādāts Rīcības plāna paraugs, lai palīdzētu tiem izveidot savu plānu.

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

Visa pārskata 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, gan arī kopīgi uzlabojot incidentu risināšanas metodoloģiju, rīkus un procedūras.

Pārskata periodā notika aktīva sadarbība kiberdrošības mācību jomā. No 28.līdz 30.aprīlim notika ENISA organizēto mācību „Cyber Europe 2014" pirmais, tehniskais posms. No Latvijas piedalījās aptuveni 30 dalībnieki. Tika atrisināti visi piedāvātie incidenti un divas no Latvijas komandām pašu komandu pašvērtējumā iekļuva Top 20 rezultātu sarakstā.

No 20. līdz 22.maijam Latvijas pārstāvji (CERT.LV un Kiberaizsardzības vienība) ieguva 2.vietu NATO Kiberaizsardzības izcilības centra (NATO Cooperative Cyber Defence Centre of Excellence) organizētajās „Locked Shields 2014" mācībās. Šogad mācībās piedalījās 12 aizsargkomandas no visas Eiropas.

Sadarbība konkrētu incidentu gadījumos aprakstīta šī pārskata 2.punktā.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 06.04. - 9.04. CERT.LV pārstāvis piedalījās TERENA organizētajos TRANSITS-I kursos, kas notika Nantē, Francijā.

- 07.04. - 08.04. CERT.LV pārstāvis piedalījās FIRST Technical Coloquium, kas notika Amsterdamā.
- 15.04. CERT.LV pārstāvis piedalījās Eiropas ekonomisko un sociālo lietu komitejas organizētajā seminārā „European Citizens' Initiative Day 2014", kas notika Briselē.
- 22.04. CERT.LV pārstāvis tikās ar Somijas Ārlietu ministriju un Somijas CERT pārstāvjiem, lai apspriestu sadarbības iespējas IT drošības jomā.
- 23.04. Notika pieredzes apmaiņas tikšanās par ES prezidentūras jautājumiem ar Lietuvas delegāciju Aizsardzības ministrijā.
- 28.04. - 30.04. CERT.LV pārstāvji piedalījās ENISA organizētajās mācībās „Cyber Europe 2014".
- 29.04. CERT.LV uzsāka dalību starptautiskā IT drošības projektā NISHA.
- 12.05. - 15.05. CERT.LV pārstāvis piedalījās „2014 Honeynet Project Workshop", kas notika Varšavā, Polijā.
- 21.05. - 22.05. Latvijas pārstāvji no CERT.LV un Kiberzemessardzes vienības piedalījās NATO organizētajās divu dienu mācībās „Locked Shields 2014", kurās izcīnīja 2. vietu.
- 22.05. - 23.05. CERT.LV pārstāvis piedalījās Ārlietu ministrijas organizētā seminārā „Enhancing Electricity sector Cyber Security in The Baltics" , kas notika Tallinā, Igaunijā.
- 27.05. - 28.05. CERT.LV pārstāvis piedalījās ENISA organizētā seminārā „CERTs in Europe" Krētā, Grieķijā.
- 29.05. - 30.05. CERT.LV pārstāvji piedalījās FIRST/TF-CSIRT seminārā Krētā, Grieķijā.
- 03.06. - 04.06. CERT.LV pārstāvji piedalījās NCSC (Nīderlandes kiberdrošības centra) organizētajā konferencē "One conference 2014", kas notika Hāgā, Nīderlandē.
- 03.06. - 06.06. CERT.LV pārstāvji piedalījās CCDCoE organizētajā „International Conference on Cyber Conflict" jeb „CyCon" konferencē Tallinā, Igaunijā, kā arī piedalījās pētījuma sagatavošanā. Tika sniegta arī prezentācija par pētījumu "Low-Cost Active Cyber Defence", kura līdzautori ir CERT.LV darbinieki.
- 09.06. - 10.06. CERT.LV pārstāvis piedalījās NATO seminārā par kritiskās infrastruktūras aizsardzību, kas notika Tallinā, Igaunijā.
- 16.06. CERT.LV pārstāvji Aizsardzības ministrijā tikās ar CERT-EU vadītāju, lai pārrunātu sadarbības iespējas.
- 16.06. - 18.06. CERT.LV pārstāvis piedalījās CCDCoE kursos "Joint Monitoring and Forensics Workshop", kas notika Tallinā, Igaunijā.
- 18.06. CERT.LV pārstāvis tikās ar CERT-EE pārstāvjiem par Baltijas sadarbības memorandu Tallinā, Igaunijā.
- 18.06. - 19.06. CERT.LV pārstāvji piedalījās kritiskās infrastruktūras aizsardzības konferencē "0ct0b3rf3st 2014" Tallinā, Igaunijā.
- 22.06. - 29.06. CERT.LV pārstāvji piedalījās ikgadējā FIRST (Forum of Incident Response and Security Teams) konferencē, kas notika Bostonā, ASV, kā arī piedalījās CERT/CC

organizētajā vispasaules nacionālo CERTu sanāksmē un uzstājās ar prezentāciju "Cyberguards Rising" par Kiberaizsardzības vienības izveidi Latvijā.

- 25.06. CERT.LV pārstāvji Rīgā tikās ar ENISA direktoru, lai pārrunātu sadarbības iespējas, kā arī uzstājās ar prezentāciju par situāciju drošības jomā Latvijā

8. Citi normatīvajos aktos noteiktie pienākumi.

- 02.04. CERT.LV pārstāvis piedalījās Lattelecom senioru datorapmācību iniciatīvas „Pieslēdzies, Latvija!" 2014.gada atklāšanas pasākumā.
- 14.04. Notika sadarbības tikšanās ar Kaspersky Lab pārstāvjiem.
- 14.04. CERT.LV pārstāvis sniedza interviju studenta bakalaura darbam.
- 25.04. CERT.LV pārstāvis sniedza interviju maģistra darbam par haktīvismu.
- 16.05. CERT.LV pārstāvis piedalījās Lattelecom organizētājā „Pieslēdzies, Latvija!" skolotāju apmācībā.
- 19.05. Notika sadarbības tikšanās ar SIA Analytica.
- 21.05. Notika sadarbības tikšanās ar Latvijas Nacionālās bibliotēkas pārstāvjiem par IT drošības konferences organizēšanu.
- 27.05. Notika tikšanās ar sociālā tīkla ask.fm pārstāvjiem.
- 29.05. Notika tikšanās ar ISACA Latvija un LIKTA pārstāvjiem par IT drošības konferences organizēšanu.
- 11.06. Notika sadarbības tikšanās ar Lattelecom par incidentu risināšanas jautājumiem.
- 16.06. CERT.LV pārstāvis piedalījās žurnāla „Latvijas intereses Eiropas savienībā" atvēršanas pasākumā par tēmu „Digitālā programma Eiropai".
- 17.06. Notika tikšanās ar komercbanku pārstāvjiem Latvijas Komercbanku asociācijā par sadarbības iespējām ar CERT.LV.
- Pārskata periodā CERT.LV iesaistījās IT drošības datu vizualizācijas rīku izstrādes projektā, kas paredzēts incidentu atklāšanai.

2014.gada 25.jūlijā

Sagatavotājs – Svetlana Amberga
Tālrunis: 67085851
E-pasts: svetlana.amberga@cert.lv