Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) uzdevumu izpildi 2013.gada 3.ceturksnī

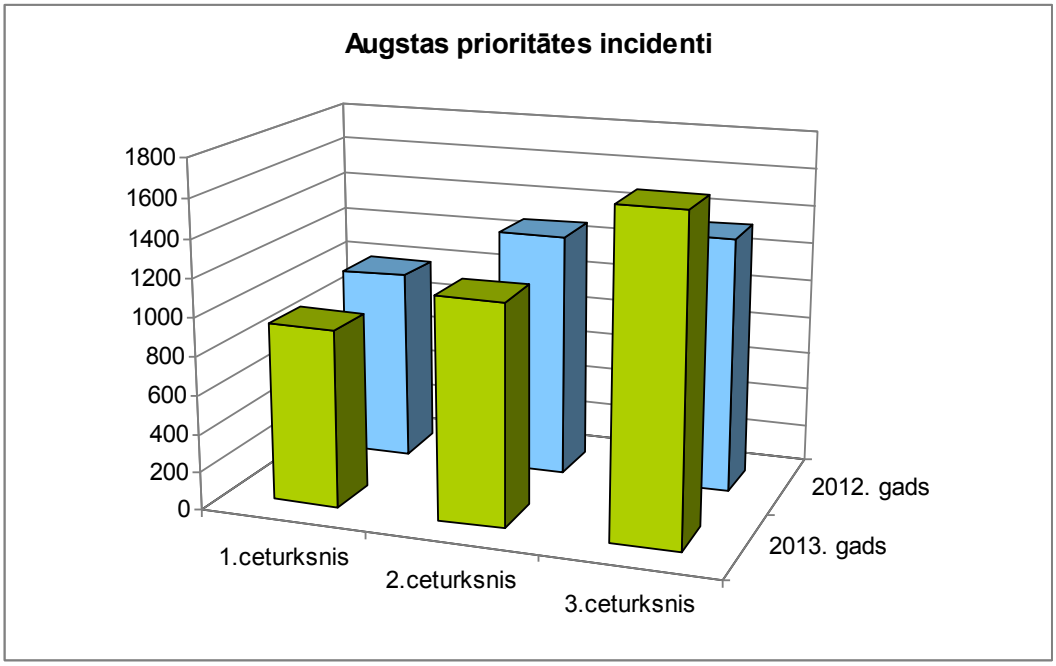
(01.07.2013. – 30.09.2013.)

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

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.

Pārskata periodā CERT.LV reģistrēja un apstrādāja 1672 augstas prioritātes incidentus. Iepriekšējā periodā tika reģistrēti un apstrādāti 1153 augstas prioritātes incidenti, bet 2012.gada jūlija-septembra periodā 1336 incidenti.

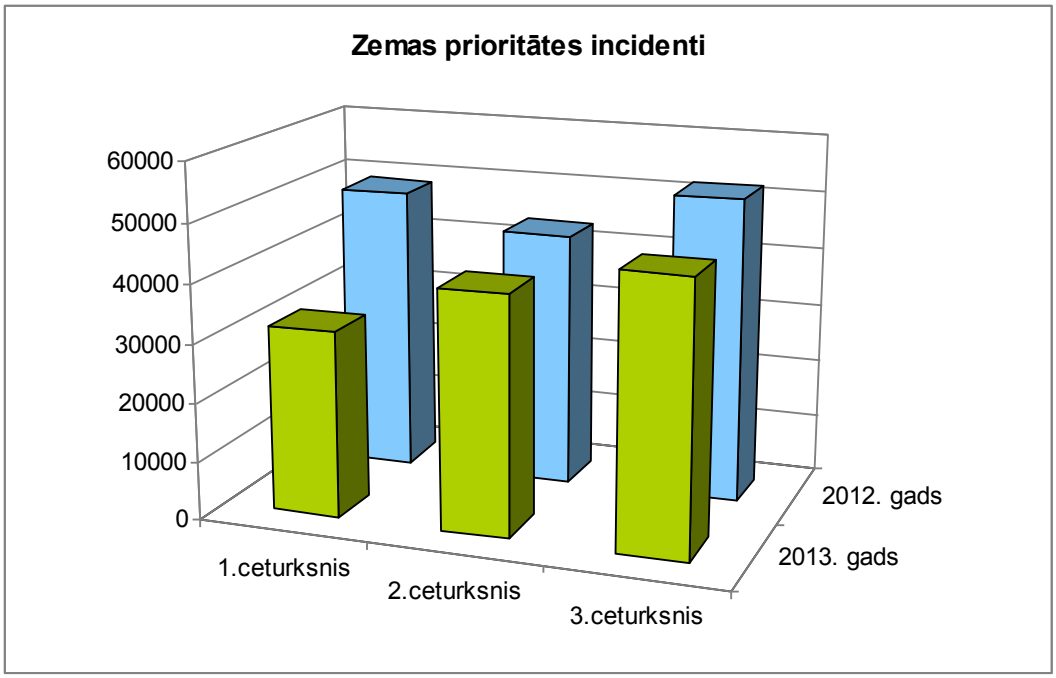


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pārskata gada pirmajos trīs ceturkšņos un iepriekšējā gada pirmajos trīs ceturkšņos.

Lai arī 2013.gadā novērojamo izmaiņu dinamika ir izteiktāka, salīdzinot ar 2012.gadu, kopējā tendence – reģistrēto un apstrādāto augstas prioritātes incidentu apjoma palielināšanās no pirmā uz trešo ceturksni – saglabājas. To var skaidrot ar lietotāju aktivitātes pieaugumu katra gada trešajā ceturksnī, atsākot darbu pēc atvaļinājumiem un uzsākot skolas un studiju gaitas. Tas sekmē gan

infekciju apriti, gan attiecīgajā periodā saņemto ziņojumu skaita pieaugumu.

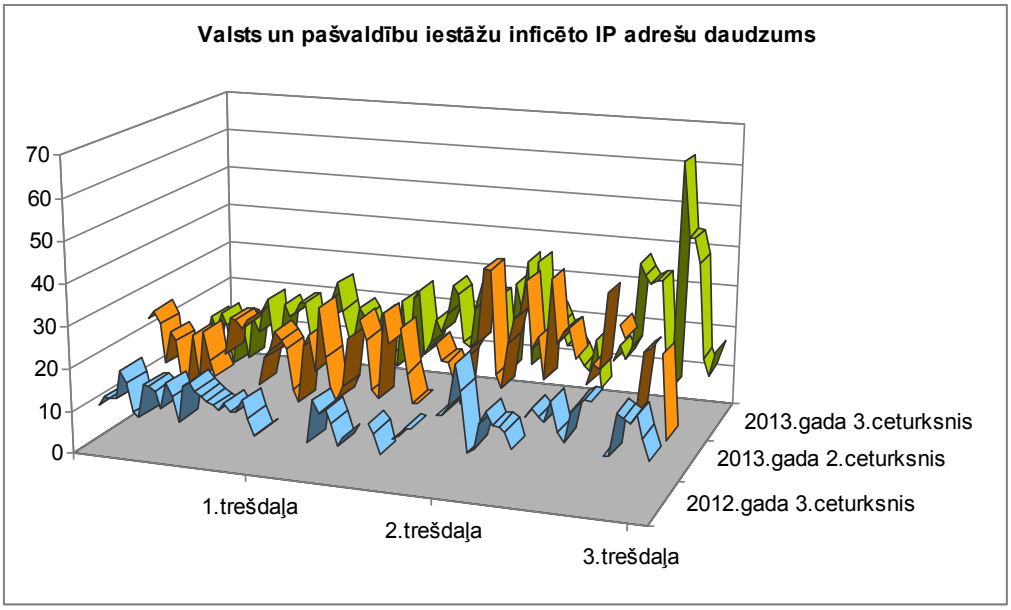
2013.gada trešajā ceturksnī CERT.LV reģistrēja 46 040 zemas prioritātes incidentus. Iepriekšējā periodā tika reģistrēti 40 721 zemas prioritātes incidenti, bet 2012.gada trešajā ceturksnī 52 040 zemas prioritātes incidenti.



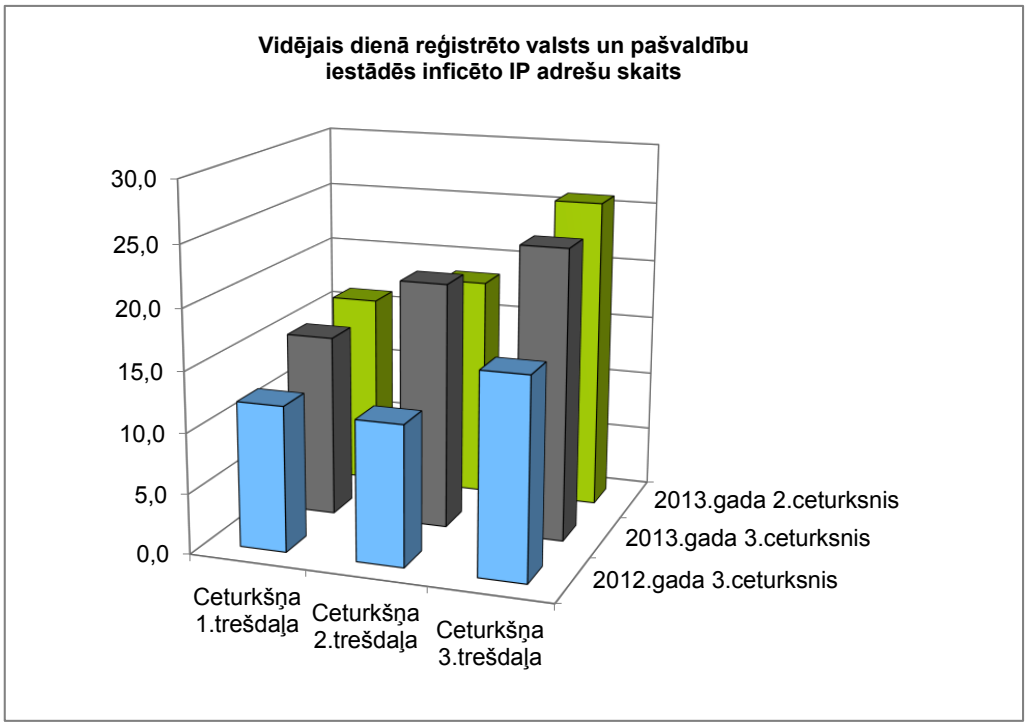
2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pārskata perioda pirmajos trīs ceturkšņos un 2012.gada pirmajos trīs ceturkšņos.

Pārskata periodā reģistrēto zemas prioritātes incidentu skaits ir zemāks, nekā pirms gada, jo globālajā tīmeklī ir tikuši atklāti un aizvērti vairāku robotu tīklu (botnet) komandu un kontroles centri, kas samazināja robotu tīklos esošo datoru apjomu. Reģistrēto zemas prioritātes incidentu pieaugums pārskata periodā pret iepriekšējo pārskata periodu skaidrojams ar papildu ziņojumu avotu izmantošanu, kas tika uzsākta iepriekšējā periodā un kas nodrošina lielāku informācijas apjomu par notikušajiem incidentiem.

2013.gada 3.ceturksnī, salīdzinot ar iepriekšējo pārskata periodu, 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 2013.gada 3.ceturksnī, 2013.gada 2.ceturksnī un 2012.gada3.ceturksnī.



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

Kā nozīmīgākie incidenti pārskata periodā minami mērķētie IT drošības uzbrukumi ministriju darbiniekiem, kuru izpildē tika izmantoti uzbrukumiem īpaši sagatavoti e-pasta sūtījumi, un viltotu, inficētu paziņojumu par multivides ziņapmaiņas (MMS) saņemšanu izplatīšana. Abos gadījumos ievainojamākais posms bija pats lietotājs, kurš neuzmanības vai nezināšanas rezultātā var apdraudēt

savu un kolēģu drošību virtuālajā vidē. Tādēļ svarīgs aspekts kopējā IT drošības līmeņa paaugstināšanā ir datorlietotāju izglītošana ar IT drošību saistītos jautājumos.

Lielāko sabiedrības un mediju uzmanību pārskata periodā piesaistīja tādi ar IT drošību saistīti jautājumi, kā Denisa Čalovska izdošana, datu drošība virtuālajā vidē un vēlēšanas internetā. Vairāki mediji izrādīja interesi par CERT.LV uzturētajā portālā esidross.lv publicēto analītisko Bruno Martuzāna rakstu par „Imantas hakera" lietu. Raksts tika vairākkārtēji pārpublicēts.

Laika posmā no 2013.gada 1.jūlija līdz 30.septembrim CERT.LV piedalījās 6 lekcijās un semināros, apmācot 400 cilvēkus, publicēja 3 jaunus rakstus portālā www.esidross.lv, 9 jaunas ziņas portālā www.cert.lv, piedalījās četrās radio pārraidēs un trīs televīzijas sižetos. Lielākā uzmanība pārskata periodā tika veltīta tam, lai sagatavotos Eiropas kiberdrošības mēnesim, par kuru atzīts oktobris, un ISACA Latvijas nodaļas un CERT.LV rudens konferencei.

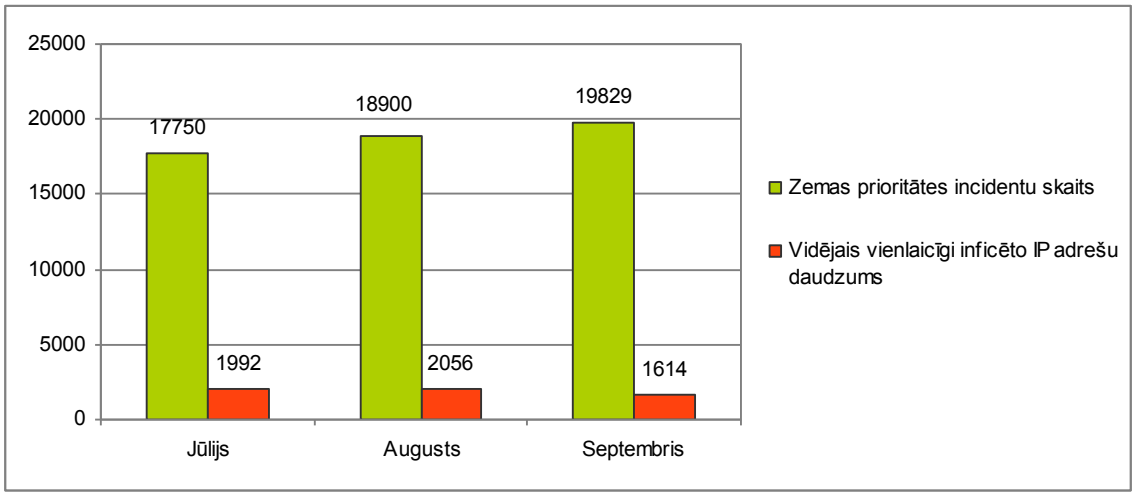
1. Uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu.

2013.gada trešajā ceturksnī CERT.LV apstrādāja 1672 augstas prioritātes incidentus, kas ir par 519 incidentiem jeb 45% vairāk nekā šī gada otrajā ceturksnī un par 336 incidentiem jeb 25% vairāk nekā 2012.gada trešajā ceturksnī.

2013.gada trešajā ceturksnī CERT.LV reģistrēja 46 040 zemas prioritātes incidentus, kas ir par 5319 incidentiem jeb 13% vairāk nekā šī gada otrajā ceturksnī, bet par 6000 incidentiem jeb 11,5% mazāk nekā 2012.gada trešajā ceturksnī.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Jūlijā šis skaits bija 1992, augustā – 2056, bet septembrī - 1614.

5.attēlā redzams, kā mainījies zemas prioritātes incidentu skaits un vidējais inficēto IP adrešu daudzums 2013.gada 3.ceturkšņa laikā.



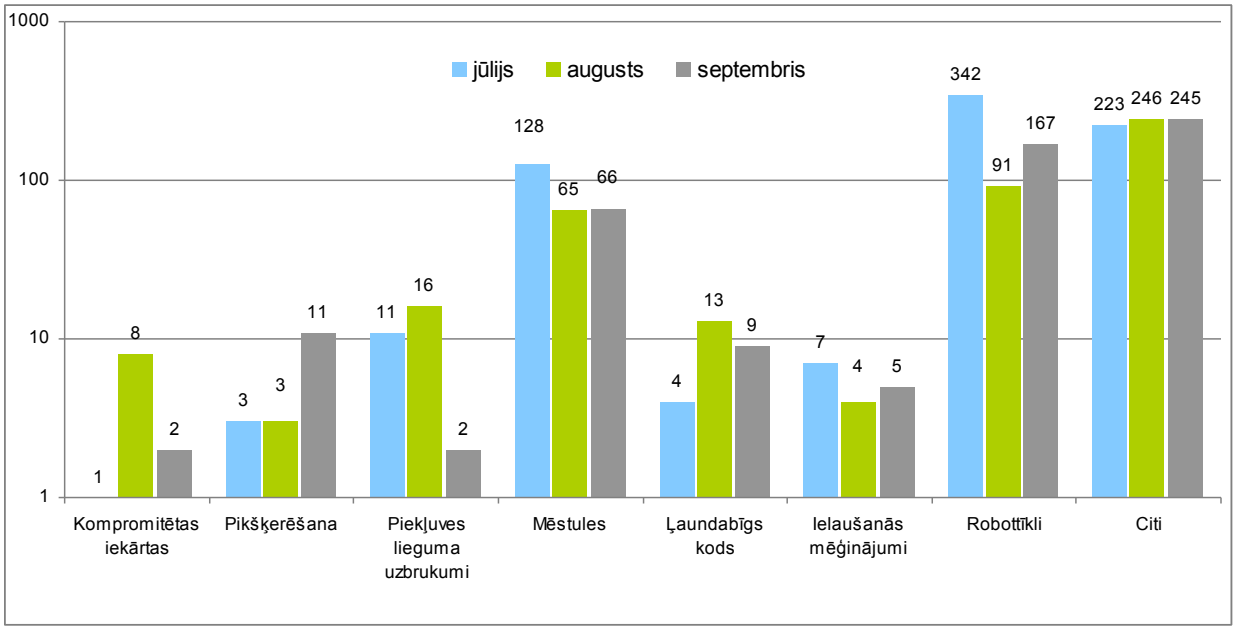
5.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem 2013.gada 3.ceturksnī.

Reģistrēto zemas prioritātes incidentu apjoma ikmēneša pieaugums skaidrojams ar jaunu papildu ziņojumu avotu izmantošanu, kas nodrošina lielāka apjoma informāciju par notikušajiem incidentiem. Savukārt katra mēneša vidējā vienlaicīgi inficēto IP adrešu daudzuma kritums skaidrojams ar veiksmīgu sadarbību starp CERT.LV un interneta pakalpojumu sniedzējiem, kas saņem informāciju par CERT.LV datubāzē reģistrētajām inficētajām IP adresēm un informē savus gala lietotājus, tādejādi pievēršot viņu uzmanību gan infekcijas faktam, gan nepieciešamībai infekciju datorā novērst. CERT.LV nodrošina instrukcijas, kas palīdz inficēto datoru īpašniekiem atbrīvoties no konkrētā viņu datorā konstatētā vīrusa vai ļaunatūras.

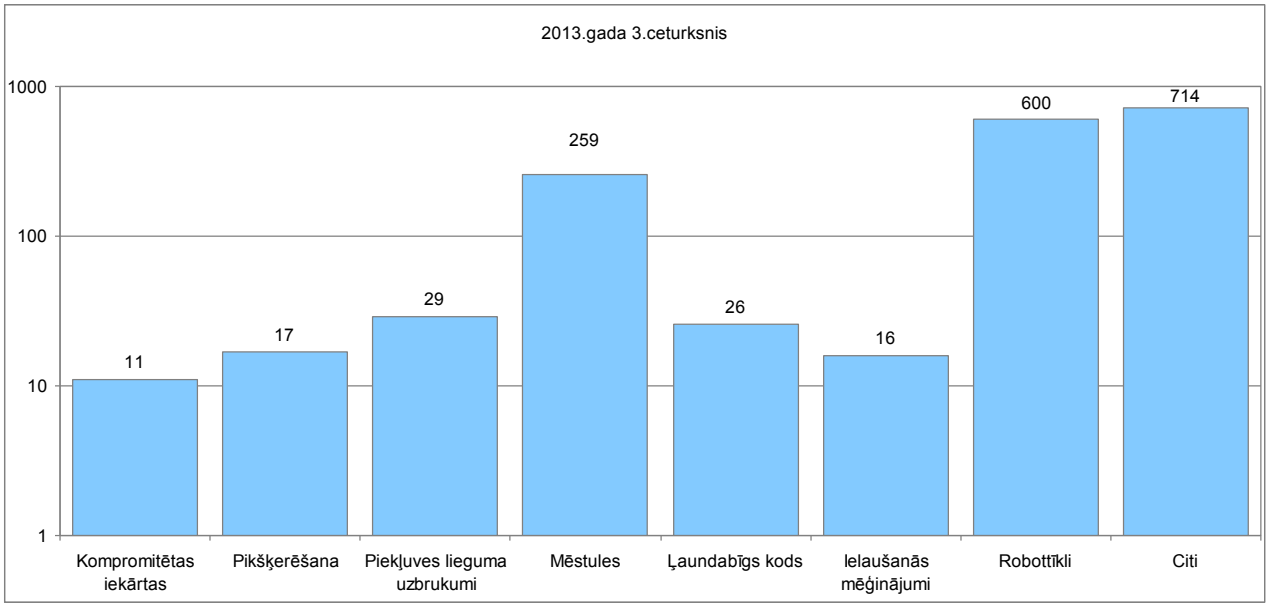
CERT.LV un Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra izveidotajam saprašanās memorandam, kas tiek slēgts ar tiem interneta pakalpojumu sniedzējiem (IPS), kas vēlas sadarboties ar šīm abām organizācijām un pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs", mazinot kaitīga satura izplatību internetā, uz pārskata perioda beigām bija pievienojušies 14 interneta pakalpojumu sniedzēji.

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

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis 1672 augstas prioritātes incidentus. 6.attēlā redzams augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem (grafiks ir logaritmiskā mērogā).

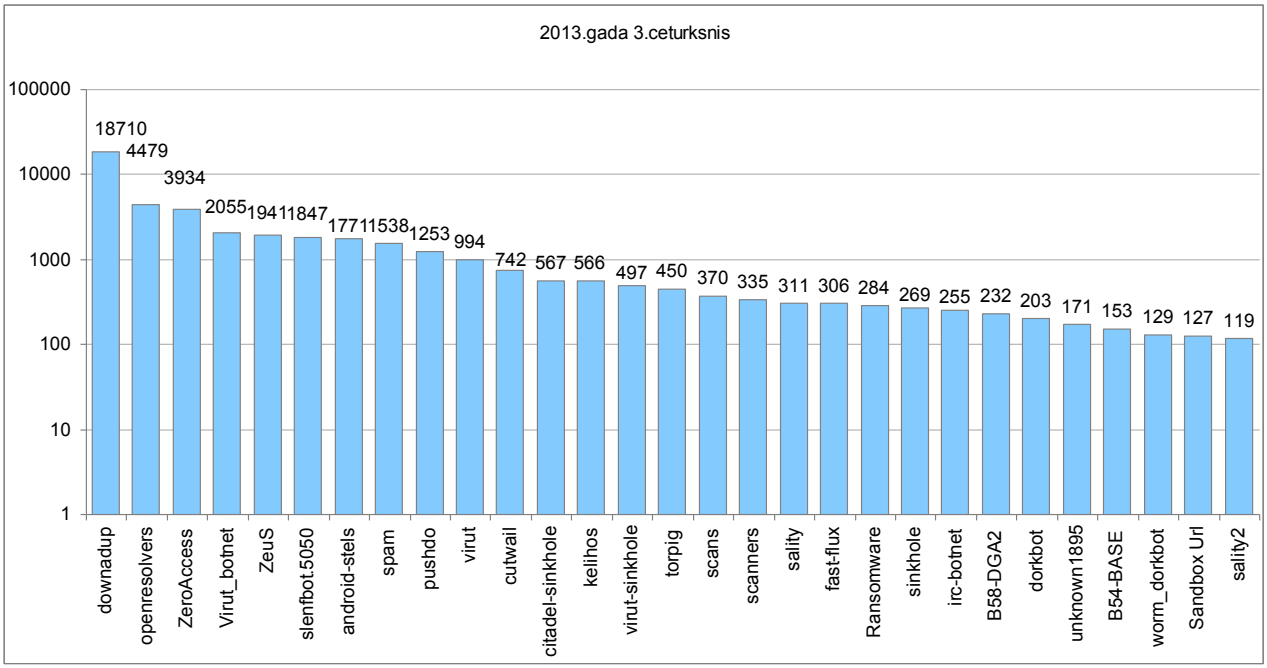


6.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.



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

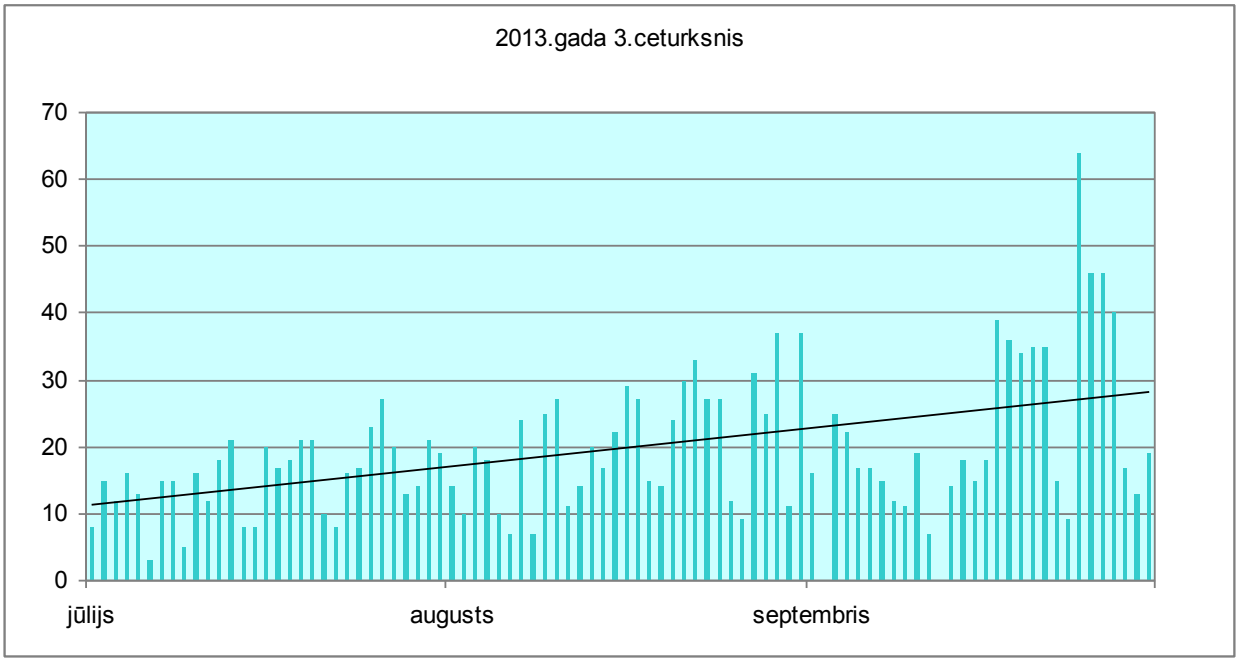
Pārskata perioda laikā CERT.LV ir reģistrējis 46 040 zemas prioritātes incidentus, par 73% jeb 23870 inficētajām IP adresēm IPS, kas sadarbojas ar CERT.LV, ir informējuši savus gala lietotājus.



8.attēls - CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā no 2013.gada 1.jūlija līdz 30.septembrim 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 258 inficētām IP adresēm. 9.attēlā ir redzams, cik inficētu valsts un pašvaldību institūciju IP adreses bijušas katras

dienas saņemtajos ziņojumos no dažādiem ziņošanas avotiem.



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

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

- 12.06. notika tikšanās ar vienu no lielākajiem interneta pakalpojumu sniedzējiem un CERT.LV nodeva sarakstu ar DNS rekursīvo serveru (open resolvers) IP adresēm un atvērto maršrutētāju IP adresēm. IPS darbinieki apstrādāja saņemto informāciju un sazinājās ar "atvērto" maršrutētāju īpašniekiem, paskaidrojot situāciju un aicinot nobloķēt pieeju atvērtajiem maršrutētājiem. IPS darbinieki konstatēja, ka ~70% DNS rekursīvie serveri ir telefonijas adapteri un apņēmās nobloķēt tiem pieeju tuvākajā laikā.

- Jūlijā CERT.LV norādīja uz būtiskiem drošības trūkumiem kādas valsts iestādes sistēmā. CERT.LV sagatavoja sarakstu ar identificētajiem trūkumiem, apdraudējuma aprakstu un rekomendācijām trūkumu novēršanai. Apmēram mēneša laikā iestāde ieviesa SSL šifrēto piekļuvi savai sistēmai, par pārējiem trūkumiem tika informēti izstrādātāji, bet CERT.LV nav guvis apstiprinājumu, ka sistēmā tie būtu novērsti.

- 05.07. Turpinājās neatjauninātu un ievainojamu *Joomla! CMS* un *WordPress* tīmekļa vietņu kompromitēšana. Uzbrucēju mērķis bija izveidot "zombiju" armiju no serveriem, kuri uztur ievainojamās mājas lapas, liekot tiem piedalīties izkliedētā servisa atteices (DDoS) uzbrukumos. CERT.LV strādāja ar interneta pakalpojumu sniedzējiem un mājas lapu īpašniekiem, lai kompromitētās iekārtas apzinātu un "iztīrītu" no ļaundabīgās programmatūras klātbūtnes.

- 10.07. CERT.LV sniedza palīdzību kādas Latvijā strādājošas bankas pikšķerēšanas (phishing) lapas aizvēršanā.

- 18.07. Kādas valsts institūcijas sistēmai radās veiktspējas traucējumi, DDoS uzbrukums netika konstatēts. Vainīga izrādījās tīmekļa indeksēšanas programma (web crawler), tās īpašnieks brīdināts.

- 02.08. Pret kādas bankas klientiem tika izvērsta pikšķerēsanas kapmaņa, izsūtot masveida e-pasta vēstules, it kā bankas vārdā, aicinot apmeklēt bankas mājas saiti, aiz kuras patiesībā nomaskēta saite uz pikšķerēšanas lapu. CERT.LV izdevās vairākas pikšķerēšanas lapas padarīt nepieejamas dažu stundu laikā, pateicoties sadarbībai ar ārvalstu kolēģiem. Incidenta izpētes laikā tika iegūts žurnālfails no pikšķerēšans resursa, kas liecināja par salīdzinoši nelielu klientu skaitu (daži desmiti), kuri savus datus ir nodevuši krāpniekiem.

- 07.08. CERT.LV izskatīja kāda netlog.com portāla lietotāja sūdzību par aizdomīgām portāla aktivitātēm. Apskatot situāciju, tika konstatēts, ka šis portāls konkrētajā gadījumā ir mēģinājis piekļūt reģistrētā lietotāja gmail.com kontam. CERT.LV ieteica šo portālu nelietot, taču detalizēta nosacījumu izpēte, kurai piekristu portāla lietotājs, netika veikta.

- 07.08. Vairākas valsts iestādes un uzņēmumi savos e-pastos saņēma viltus MMS paziņojumus LMT un TELE2 vārdā, kuri saturēja pielikumu ar ļaunatūru. Daži šajos ziņojumos norādītie sūtītāju abonentu numuru piemēri:
  26340918@mms.lmt.lv
  26322995@mms.lmt.lv
  26352647@mms.lmt.lv

  Viltus e-pasti nesaturēja nekādu tekstu, tikai arhīva failu pielikumā (piem., mms52439929.zip), kuru atverot lietotāja dators tika inficēts ar vīrusu.

  Par incidentu tika informēti pakalpojumu sniedzēji. Veicot incidenta analīzi sadarbībā ar LMT drošības dienestu, tika konstatēts, ka e-pastu sūtītāja lauki ir viltoti un šie lietotāji šādas ziņas nav sūtījuši. Krāpnieciskie e-pasti tikuši izsūtīti no IP adreses Nīderlandē. CERT.LV veica nepieciešamos soļus incidenta risināšanā, sazinājās ar ārvalstu CERT komandām un informēja sabiedrību.

- 12.08. CERT.LV konsultēja vairākus portāla esidross.lv lietotājus par kredītkaršu datu izmantošanu internetā.

- 13.08. Kāda portāla uzturētāji informēja par DDoS uzbrukumu, kas, veicot papildus pārbaudi, nepastiprinājās. Uzbrukums tika veikts no portāla iekštīkla, kurā tika konstatēts ar DDoS botu inficēts serveris, kurš uzbrūk citiem datoriem. Serveris tika salabots un iztīrīts.

- 20.08. Kāda novada tīmekļa vietnē tika konstatētas vairākas ievainojamības, tika informēta un konsultēta atbildīgā persona.

- 02.09. CERT.LV saņēma informāciju par klientu datu zādzību no kāda TV pakalpojumu sniedzēja. Par šo gadījumu tika informēta Datu valsts inspekciju, tika ierosināta pārbaudes lieta.

- 03.09. Kādas valsts iestādes ielaušanās atklāšanas sistēma (IDS) konstatēja datorvīrusa aktivitātes no darbinieka datora. Padziļināta šī datora cietā diska un operatīvās atmiņas (RAM) pārbaude vīrusu neuzrādīja, viltus trauksmes iemesls varētu būt primitīvs IDS sistēmas attiecīgā vīrusa paraksts (signature).

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

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

- 05.09. Tika kompromitēta kādas ģimnāzijas tīmekļa vietne. Uzbrucēji uz servera izvietoja vairākus ļaunatūras failus, lai nodrošinātu turpmāku piekļuvi kompromitētajam resursam. Incidents tika novērsts sadarbībā ar attiecīgo pašvaldību.

- 10.09. Tika identificēti mērķēti (*spear phishing*) uzbrukumi vairāku ministriju darbiniekiem. Tika identificēts ļaunatūras kontrolcentrs. Ministriju pasta serveru antivīrusu programmatūra spēja identificēt šo uzbrukumu un līdz gala lietotājam kaitīgais saturs netika nogādāts. Šis pats uzbrukums tika novērots arī vairākās citās ES dalībvalstīs.

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

- 17.09. Kādā tīmekļa vietnē tika izvietoti pikšķerēšanai paredzēti resursi. Tika iegūta šīs vietnes kopija, brīdināti pikšķerēšanas shēmā izmantoto e-pasta adrešu turētāji.

- 24.09. CERT.LV konstatēja Zeus robotu tīkla kontroles centra izvietošanu kādā Latvijas serverī. Failu kopijas iegūtas tālākai analīzei, kaitīgais saturs no servera dzēsts un salabota ievainojamība, kas ļāvusi kaitīgo saturu tur izvietot.

- 29.09. Kāda Latvijas banka cieta no DDoS uzbrukuma, kurā tika iesaistīti vairāki desmiti Ukrainas, Krievijas, Baltkrievijas un Kazahstānas IP adrešu, kuras bija robotu tīkla sastāvā. Uzbrukuma ietekmes mazināšanas pasākumus veica bankas pakalpojumu sniedzējs.

- 30.09. CERT.LV saņēma ziņas par datorvīrusu, kas apdraud internetbankas, un brīdināja kaitīgā satura uzturēšanā iesaistītā resursa turētāju, kaitīgā satura izplatīšana tika novērsta.

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

CERT.LV uzskaita arī uzlauzto un izķēmoto tīmekļa vietņu gadījumus. Šādu gadījumu skaits jūlijā bija 46, augustā – 59, septembrī – 26. Izķēmoto lapu sadalījums pa serveru operētājsistēmām: jūlijā - 28 GNU/Linux, 10 MS Windows, 8 nezināmas, augustā - 57 GNU/Linux, 2 nezināmas, septembrī – 18 GNU/Linux, 8 nezināmas.

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 par jaunākajiem vīrusiem un apdraudējumiem (6473 apmeklējumi), bet otrajā vietā ierindojās lapa ar CERT.LV sagatavoto informāciju par „Policijas vīrusa" apkarošanas praksi un mehānismiem (5023 apmeklējumi). Kopā CERT.LV mājas lapai bijuši 11 264 apmeklējumi, kurus veido 8037 unikāli apmeklētāji no 60 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa – 91,61% apmeklētāju - bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicētas 9 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 2.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 24 ziņas, kontam pievienojušies 44 jauni sekotāji un 80 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 10 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 3 jauni raksti, kā arī papildināts raksts par „policijas izspiedējvīrusu", portālu apmeklējuši 20 201 (15 467 unikāli) apmeklētāji. Publicētie raksti:

- Bērna izglītošana datora lietošanā.
- Kā atklāja Imantas hakeri un kas viņam draud ASV (raksts izpelnījās arī plašāku mediju uzmanību).
- Kas jāzina, lai "ask.fm" lietošana kļūtu jums drošāka.

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

Sīkāka informācija:

1) Publikācijas presē:
   - 24.07. – sniegts komentārs izdevumam Telegraf par datu drošību, datu centriem un mākoņdatošanu
   - 06.08. – izdevums „Kas jauns?" pārpublicēja portālā Esidross.lv publicēto Bruno Martuzāna rakstu, kas veltīts D.Čalovska lietas analīzei
   - 13.08. – sniegti komentāri par datu drošību „Bauskas Dzīve"
2) Intervijas un ziņas radio:
   - 25.07. – saruna par datu drošību internetā Latvijas radio raidījumā „Kā labāk dzīvot"
   - 06.08. – diskusija par datu drošību un personiskās dzīves neaizskaramību Latvijas radio raidījumā „Krustpunktā"
   - 07.08. – saruna par globālo kiberkaru Latvijas radio raidījumā „Zināmais nezināmajā"
   - 13.09. – komentārs par e-pastiem Latvijas radio raidījumā „Zināmais nezināmajā"
3) Sižeti televīzijā, tiešraides:
   - 02.07. – sniegts komentārs 1. Baltijas kanālam par kiberdrošību un projektu PRISM
   - 07.08. – komentārs LTV raidījumā „Panorāma" par ar IT drošības incidentiem saistītu lietu izskatīšanu
   - 05.09. – sniegts komentārs LNT raidījumam „Degpunktā" par apdraudējumiem, lietojot internetbanku, sociālos tīklus, kā arī ieteikumi drošai interneta un datora lietošanai
   - 23.09. – dalība LNT rīta raidījumā „900 sekundes", sniedzot CERT.LV viedokli par interneta vēlēšanu sistēmas izveidi
4) Ziņas portālos:
   - 22.07. - Pieaudzis ar iestādēm saistīto drošības incidentu skaits – raksts TVnet
   - 02.08. - Eiropā plāno stingrākus sodus kibernoziedzniekiem– raksts Aprinkis.lv
   - 04.08. - Версия: как хакер Майями (Чаловский) продавал инъекцию для Gozi агентам ФБР - raksts Kriminal.lv (raksts balstīts uz portālā Esidross.lv publicēto Bruno Martuzāna rakstu)
   - 05.08. - Norāda uz LV tiesībsargājošo iestāžu kapacitātes trūkumu kibernoziegumu lietās – raksts Puaro.lv
   - 06.08. - Čalovski FIB varētu būt atklājis ar izmeklētāju kontrolēta pirkuma palīdzību – raksts Delfi.lv (raksts balstīts uz portālā Esidross.lv publicēto Bruno Martuzāna rakstu)
   - 09.08. – Cilvēki ļoti bezrūpīgi izturas pret saviem datiem elektroniskajā vidē – raksts TVnet
   - 09.08. - Cilvēki bezrūpīgi izturas pret saviem datiem elektroniskajā vidē – raksts Apollo
   - 09.08. - Eksperti diskutēs par datu drošību un kibernoziegumiem – raksts Puaro.lv
   - 09.08. - CERT: jebkurām darbībām, kas notiek kibervidē, ir vistiešākā saite ar reālo dzīvi – raksts Focus.lv
   - 12.08. - Aizdomas par apjomīgu krāpšanu; iespējams, cietuši tūkstošiem interneta lietotāju – raksts Apollo
   - 13.08. - CERT.LV: No krāpšanas varētu būt cietuši vairāki desmiti tūkstošu interneta lietotāju - raksts TVnet
   - 13.08. - Atklāta liela apjoma kiberkrāpšana; iespējams, iesaistīts arī Latvijas valstspiederīgais – raksts Diena.lv
   - 16.08. - Eksperti: datu drošības lielākais drauds nereti ir paši uzņēmuma darbinieki – raksts db.lv
   - 03.09. - Inbox.lv блокирует до 97% спама на e-mail – raksts rus.apollo.lv

- 05.09. - E-pasta dati jāsargā rūpīgāk - mēstules abonē paši lietotāji – raksts LA.lv
- 11.09. – ES plāno stingrākus sodus kibernoziedzniekiem – raksts LVportals.lv
- 23.09. - Выборы в интернете — угроза государственности – raksts Telegraf.lv
- 23.09. - IT nozare: Interneta vēlēšanas apdraud valsts pastāvēšanu – raksts TVnet
- 23.09. - Декан ЛУ: выборы в интернете угрожают существованию государства – raksts baltic-course.com

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

Pārskata periodam aptverot jūliju un augustu, kas ir populārs atvaļinājumu laiks, CERT.LV dalība dažādās apmācībās un semināros bija minimāla, bet noritēja aktīvs darbs pie ISACA un CERT.LV rudens konferences plānošanas un organizēšanas, kā arī gatavošanās oktobrim kā Eiropas Kiberdrošības mēnesim.

CERT.LV tikās gan ar ISACA Latvija pārstāvjiem, gan potenciālajiem konferences atbalstītājiem Lattelecom, QUALYS un citiem, lai pārrunātu sadarbību un risinātu organizatoriskus jautājumus, tika gatavoti sadarbības līgumi. Tika izsludināta referātu pieteikšana konferencei, veikta pieteikumu atlase un apstiprinājumu izsūtīšana. Tika veikta telpu rezervācija un tehniski organizatorisko aspektu plānošana, sagatavota konferences programma, veikta konferences izziņošana un izsludināta pieteikšanās.

Notika aktīva komunikācija un informācijas apmaiņa ar ENISA pārstāvjiem, lai koordinētu Kiberdrošības mēneša aktivitātes. Tika veikta arī ENISA lektoru piesaiste, kas Kiberdrošības mēneša ietvaros ieradīsies Latvijā, lai novadītu semināru IT speciālistiem par sociālo tīklu izmantošanu mērķētu uzbrukumu veikšanā.

Pārskats par CERT.LV pasākumiem pārskata periodā:

- 21.08. CERT.LV pārstāvis sniedza prezentāciju par IT drošības aktualitātēm ISACA Latvija nodaļas augusta sanāksmē, kas notika CERT.LV telpās.
- 21.08. CERT.LV piedalījās informātikas skolotāju konferencē un sniedza prezentāciju par IT drošības risinājumiem un problēmām skolās.
- 28.08. CERT.LV pārstāvis piedalījās videomateriāla sagatavošanā skolēniem, kas vēlas apgūt programmēšanu, un stāstīja par IT drošību.
- 05.09. CERT.LV pārstāvis piedalījās Augstākās tiesas seminārā par drošību Eiropā un sniedza prezentāciju.
- 07.09. CERT.LV nodrošināja informatīvi – izglītojošos materiālus TC Dole organizētajā Telekomunikāciju dienā.
- 13.09. CERT.LV pārstāvji viesojās TechHub un sniedza prezentāciju, informējot TechHub biedrus par CERT.LV darbību, IT drošības aktualitātēm Latvijas virtuālajā telpā un Kiberaizsardzības vienību.

Pārskata periodā CERT.LV par IT drošības jautājumiem ir informējuši un izglītojuši 400 dažādu pasākumu dalībniekus.

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.

- 11.07. CERT.LV piedalījās sanāksmē par ES prezidentūras drošības jautājumiem.
- 20.08. CERT.LV pārstāvji piedalījās Kiberaizsardzības vienības sanāksmē.
- 21.08. CERT.LV piedalījās AM sanāksmē par NetSafe projekta nākotni.
- Jūlijā, augustā un septembrī CERT.LV piedalījās VARAM darba grupu sanāksmēs par Uzraudzības iestādes veidošanu.
- Augustā CERT.LV piedalījās Satiksmes ministrijas darba grupu sanāksmēs par interneta vēlēšanām.
- 25.09. CERT.LV pārstāvis piedalījās sanāksmē Satiksmes ministrijā "Par kaitīgu saturu elektroniskās informācijas telpā".

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.septembrim CERT.LV apkopoja informāciju par 606 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. Līdz 2013.gada 30.septembrim rīcības plānus bija iesnieguši 55 ESK. Mazajiem ESK ir pieejams CERT.LV izstrādāts Rīcības plāna paraugs, lai palīdzētu tiem izveidot savu plānu.

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

Visa perioda laikā ir notikusi aktīva sadarbība ar citu valstu 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. Konkrēti incidenti uzskaitīti šī pārskata 2.punktā.

CERT.LV pārstāvji pārskata periodā piedalījušies sekojošos starptautiskos pasākumos:

- 1.-3.07. CERT.LV pārstāvis piedalījās ENISA Cyber Europe mācību plānošanas sanāksmē Luksemburgā, prezentējot idejas par mācību scenārija izpildi un mācībās iekļautajām sfērām. Notika diskusijas par iesaistītajiem sektoriem un mācību plānošanas un izpildes kārtību.

- 12.07. ENISA Skype intervija ar CERT.LV pārstāvi par industriālo vadības sistēmu drošības incidentu reaģēšanas vienības izveides nosacījumiem un darbības pamatprincipiem.
- 25.07. CERT.LV pārstāvis piedalījās NATO Cyber Coalition‘13 mācību tehniskā scenārija un specifikāciju izvērtēšanā.
- 17.-19.09. CERT.LV pārstāvis Briselē piedalījās ENISA un CERT-EU organizētajā seminārā, uzstājoties ar prezentāciju par NfSen rīkiem.
- 23.-24.09. CERT.LV pārstāvis piedalās ENISA organizētā konferencē, kas veltīta kiberkrīzes scenāriju risināšanai un valsts mēroga IT drošības mācību organizēšanai.
- 25.-28.09. CERT.LV pārstāvis piedalījās Trusted Introducer un TF-CSIRT sanāksmēs Londonā, uzstājoties ar prezentāciju "CERT.LV update and case study on stolen credit cards", un tika ievēlēts par TF-CSIRT Steering Committee locekli.
- Septembrī CERT.LV papildināja incidentu informācijas apmaiņu ar starptautiskajiem partneriem, šoreiz nodrošinot datu apmaiņu no Latvijā iegūtās informācijas par Citadel banking trojan upuriem. CERT.LV ieguldījums tika atzinīgi novērtēts no The Shadowserver Foundation.

8. Veikt citus normatīvajos aktos noteiktos pienākumus.

- Pārskata periodā notikušas trīs DEG grupas sanāksmes.
- 08.07. CERT.LV kopā ar Aizsardzības ministriju tikās ar LIKTA, lai pārrunātu sadarbību.
- Jūlijā tika izsludināta jauna vakance un notika potenciālo kandidātu atlase.
- Jūlijā notika tikšanās ar Lattelecom, lai pārrunātu iespējamo sadarbību arī sabiedrības izglītošanas jomā un IT drošības jautājumu popularizēšanā.
- 30.08. dalība Nacionālās IT drošības padomes sanāksmē.
- 27.09. dalība VARAM sanāksmē par Profesijas standartu.

Sagatavotājs – Līga Besere
Tālrunis: 67085858
E-pasts: liga.besere@cert.lv