Latvijas Republikas
Aizsardzības ministrija

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

[2014]

Publiskais pārskats par CERT.LV uzdevumu izpildi

2014.gada 1.ceturksnis
(01.01.2014. – 31.03.2014.)

Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) uzdevumu izpildi 2014.gada 1.ceturksnī (01.01.2014. – 31.03.2014.)

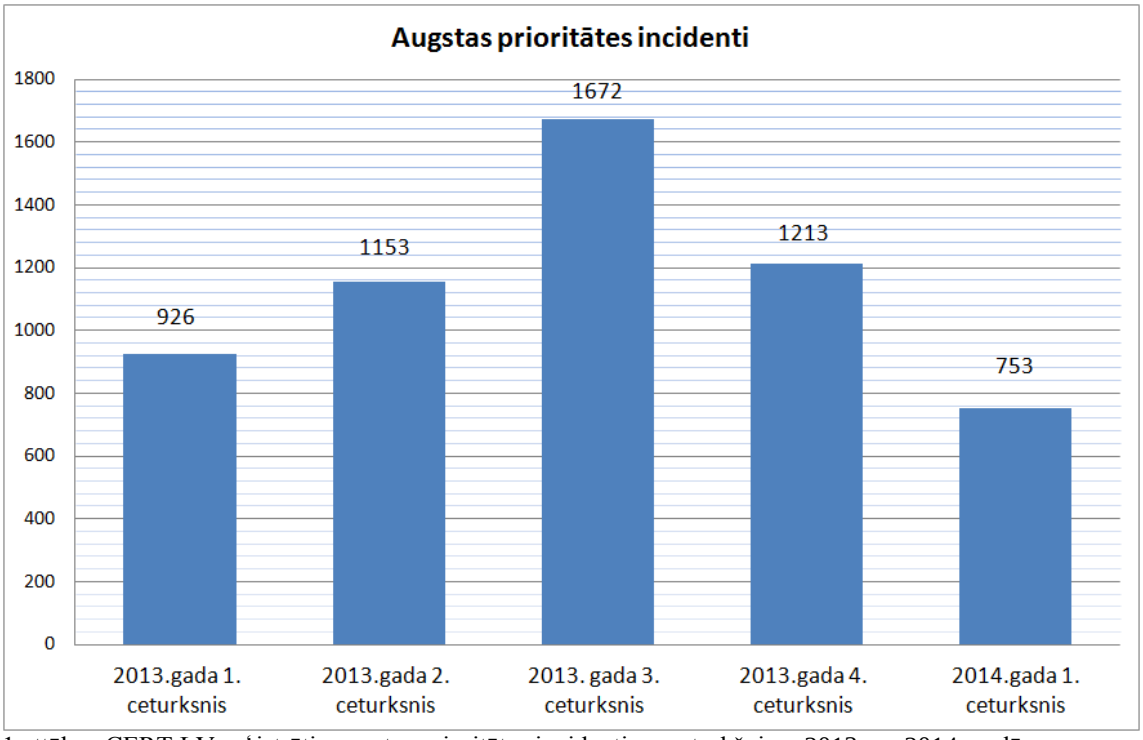
Pārskatam ir tikai informatīva nozīme. Pārskatā iekļauta tikai vispārpieejama informācija, tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju.

SATURS

Kopsavilkums

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.

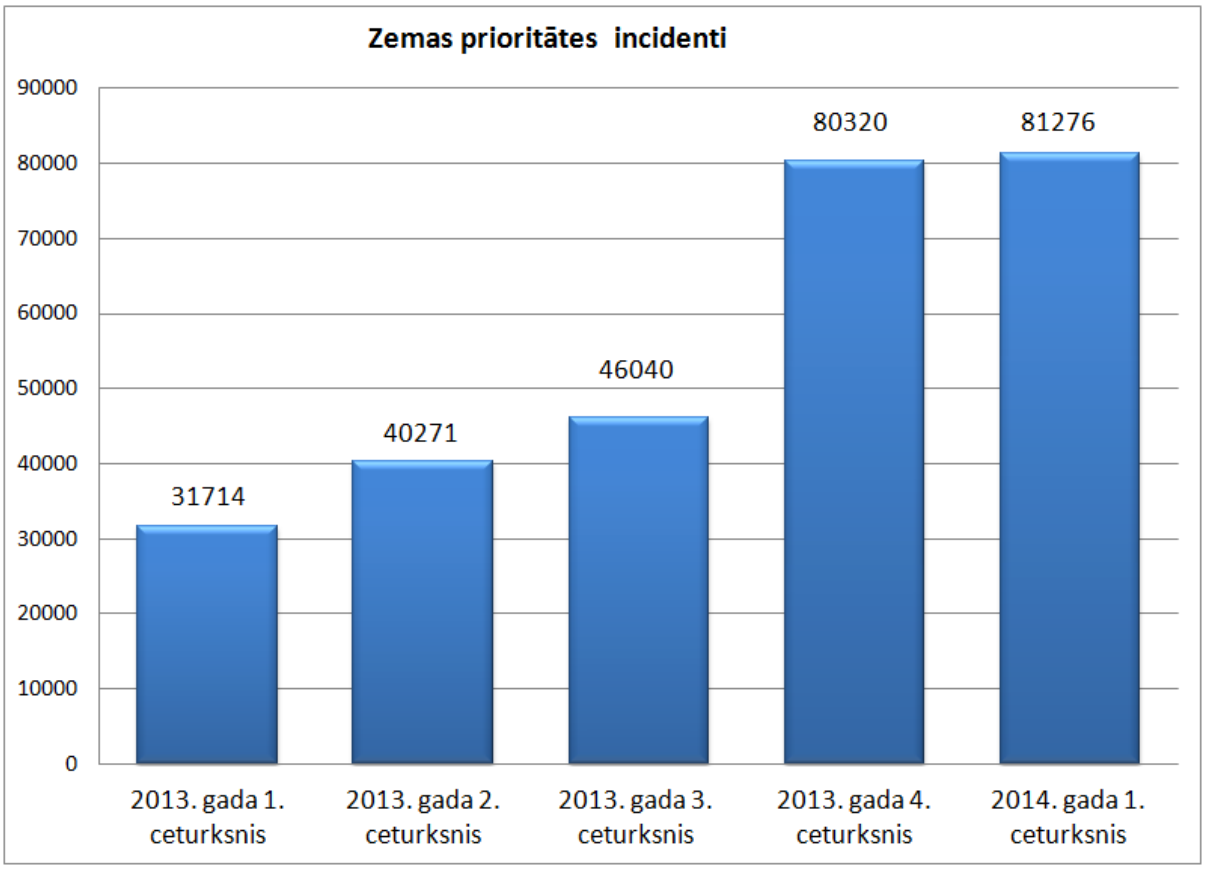
Pārskata periodā CERT.LV reģistrēja un apstrādāja 753 augstas prioritātes incidentus. Iepriekšējā periodā tika reģistrēti un apstrādāti 1213 augstas prioritātes incidenti, bet 2013.gada 1.ceturksnī 926 incidenti.



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

Pārskata periodā, tāpat kā iepriekšējā periodā, vērojams reģistrēto un apstrādāto augstas prioritātes incidentu samazinājums salīdzinot ar iepriekšējo periodu.

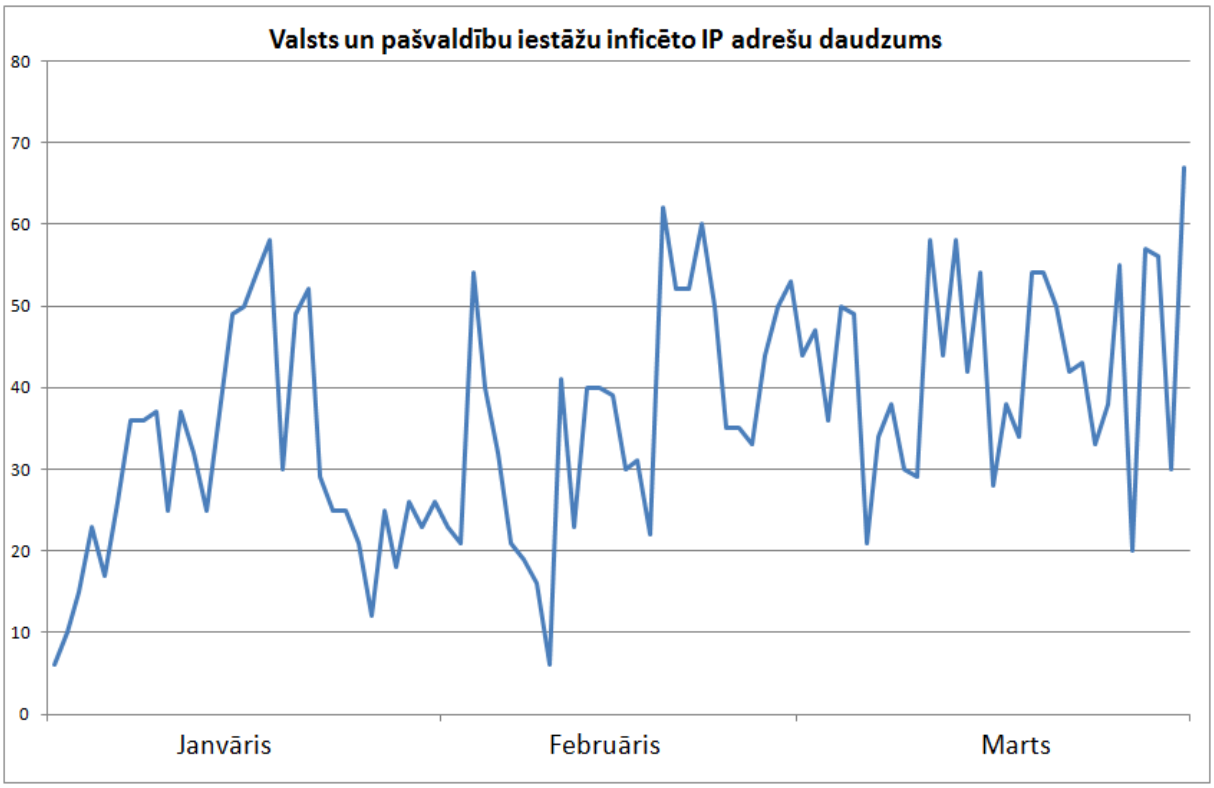
2014.gada 1.ceturksnī CERT.LV reģistrēja 81 276 zemas prioritātes incidentus. Iepriekšējā periodā tika reģistrēti 80 321 zemas prioritātes incidenti, bet 2013.gada 1.ceturksnī 31 714 zemas prioritātes incidenti.



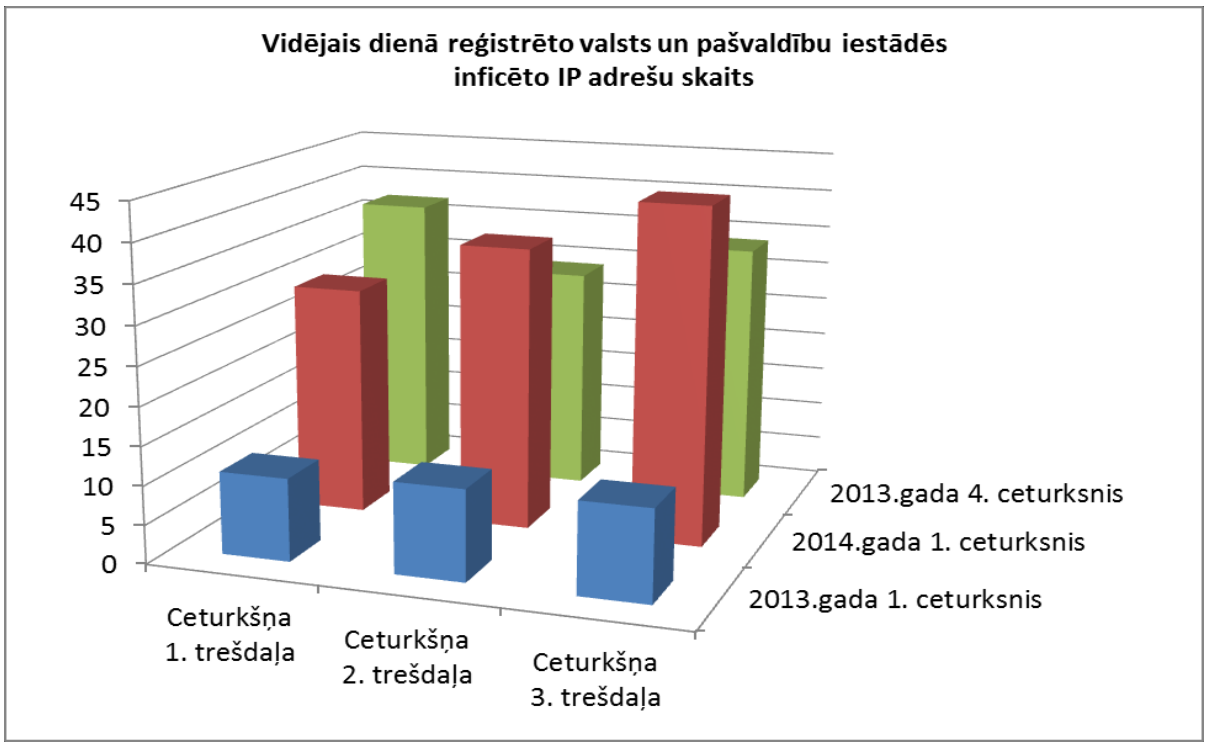
2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem 2013. un 2014.gadā.

Pārskata periodā reģistrēto zemas prioritātes incidentu apjoms būtiski neatšķiras, salīdzinot ar iepriekšējo periodu, tomēr, salīdzinot zemas prioritātes incidentu skaitu ar to pašu periodu pirms gada, vērojams pieaugums vairāk kā uz pusi.

2014.gada 1.ceturksnī, salīdzinot ar iepriekšējo ceturksni, samazinājies inficēto IP adrešu daudzums, kas reģistrēts valsts un pašvaldību iestādēs katras dienas saņemtajos ziņojumos.



3.attēls – Valsts un pašvaldību iestāžu inficēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2014.gada 1.ceturksnī pa mēnešiem.



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

Lielāko sabiedrības un mediju uzmanību pārskata periodā izpelnījās datorvīruss bankas datu izkrāpšanai, jeb tā saucamais VID vīruss. Gan janvārī, gan februārī, gan martā masveidā tika izplatītas e-pasta vēstules, kas saturēja ar bīstamu datorvīrusu inficētu pielikumu un radīja bankas datu izkrāpšanas un naudas līdzekļu nozagšanas risku. Ziņa par bīstamā datorvīrusa

izplatību tika publicēta lielākajos interneta medijos, piemēram, portālā Diena.lv

Lai pievērstu mediju un sabiedrības uzmanību drošai rīcībai internetā, CERT.LV sadarbībā ar Swedbank un draugiem.lv 18.martā rīkoja mediju pasākumu „Kā pasargāt sevi internetā un droši lietot tā plašās iespējas", kurā informēja par interneta vidē sastopamajiem aktuālākajiem riskiem un mūsdienu „virtuālās higiēnas" pamatprincipiem.

Organizēto pasākumu ziņā 2014.gada 1.ceturksnis iezīmējas ar augstu sniegto prezentāciju skaitu skolās par IT drošību gan skolēniem, gan skolotājiem. Pārskata periodā šīm izglītojošām aktivitātēm bijis vislielākais īpatsvars skaita ziņā.

IT speciālistiem tika organizēti vairāki semināri - „IT drošība skolā" (divas reizes), kurš bija paredzēts informātikas skolotājiem, kā arī seminārs „IT drošības vizualizācija", kurš bija paredzēts IT speciālistiem un guva lielu atsaucību no interesentu puses, rezultātā tika noorganizēti divi šādi semināri.
Pārskata periodu noslēdza E-prasmju nedēļa, kas norisinājās no 24. līdz 30.martam, kuras laikā notika vairāki izglītojoši pasākumi, ieskaitot Datorologa akciju 26. martā.

Kopā pārskata periodā CERT.LV piedalījās 24 pasākumos, apmācot 1198 cilvēkus, publicēja 4 jaunus rakstus portālā www.esidross.lv, 39 jaunas ziņas portālā www.cert.lv, piedalījās 4 radio pārraidēs un 6 televīzijas sižetos.

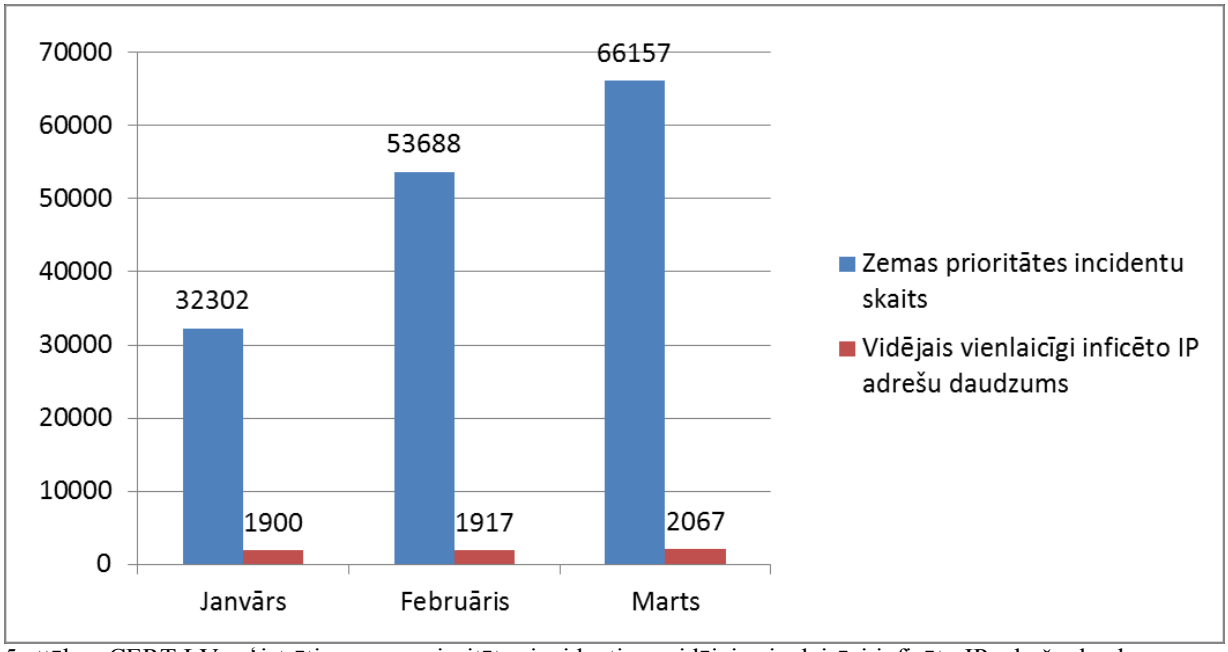
1. Uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu.

2014.gada pirmajā ceturksnī CERT.LV apstrādāja 753 augstas prioritātes incidentus, kas ir par 460 incidentiem jeb 61 % mazāk nekā 2013. gada ceturtajā ceturksnī un par 173 incidentiem jeb 23% mazāk nekā 2013.gada pirmajā ceturksnī.

2014.gada pirmajā ceturksnī CERT.LV reģistrēja 81 276 zemas prioritātes incidentu, kas ir par 995 incidentiem jeb 1.22% vairāk nekā 2013. gada ceturtajā ceturksnī un par 49 562 incidentiem jeb 60.8 % vairāk nekā 2013.gada pirmajā ceturksnī.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Janvārī šis skaits bija 2143, februārī – 1917, bet martā – 2057 inficētas IP adreses.

5.attēlā redzams, kā mainījies zemas prioritātes incidentu skaits un vidējais inficēto IP adrešu daudzums 2014.gada 1.ceturkšņa laikā.



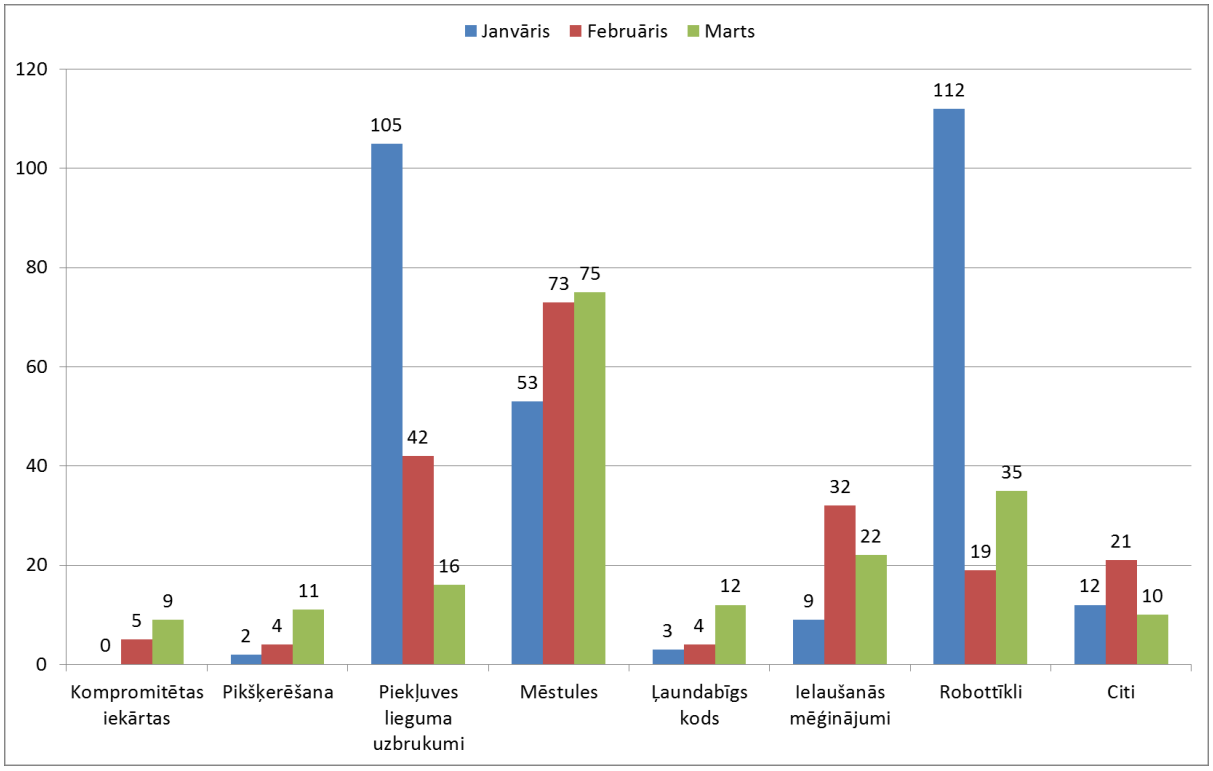
5.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem 2014. gada 1.ceturksnī.

2014.gada 1.ceturksnī reģistrēto zemas prioritātes incidentu apjoms nav būtiski pieaudzis, salīdzinot ar 2013.gada pēdējo ceturksni.

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, kas vēlas sadarboties ar šīm abām organizācijām un pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". Uz pārskata perioda beigām atbildīgo IPS kopskaits bija 13.

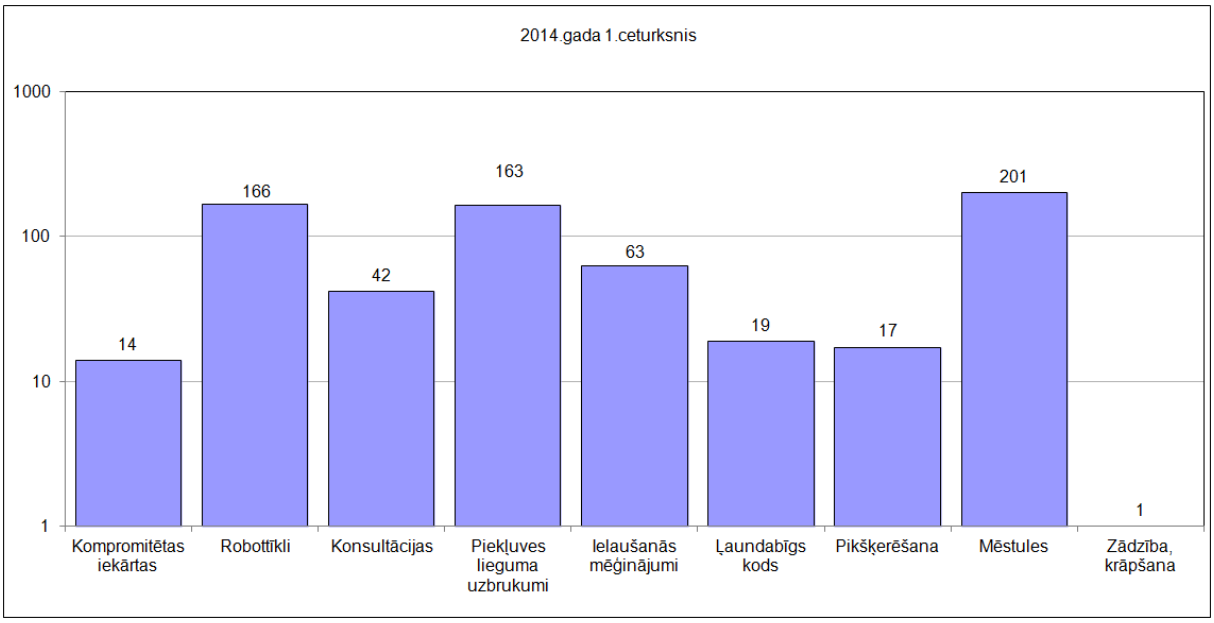
2. Sniegt atbalstu informācijas tehnoloģiju drošības incidenta novēršanā vai koordinēt to novēršanu.

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis 753 augstas prioritātes incidentus. Augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem redzams 6.attēlā.



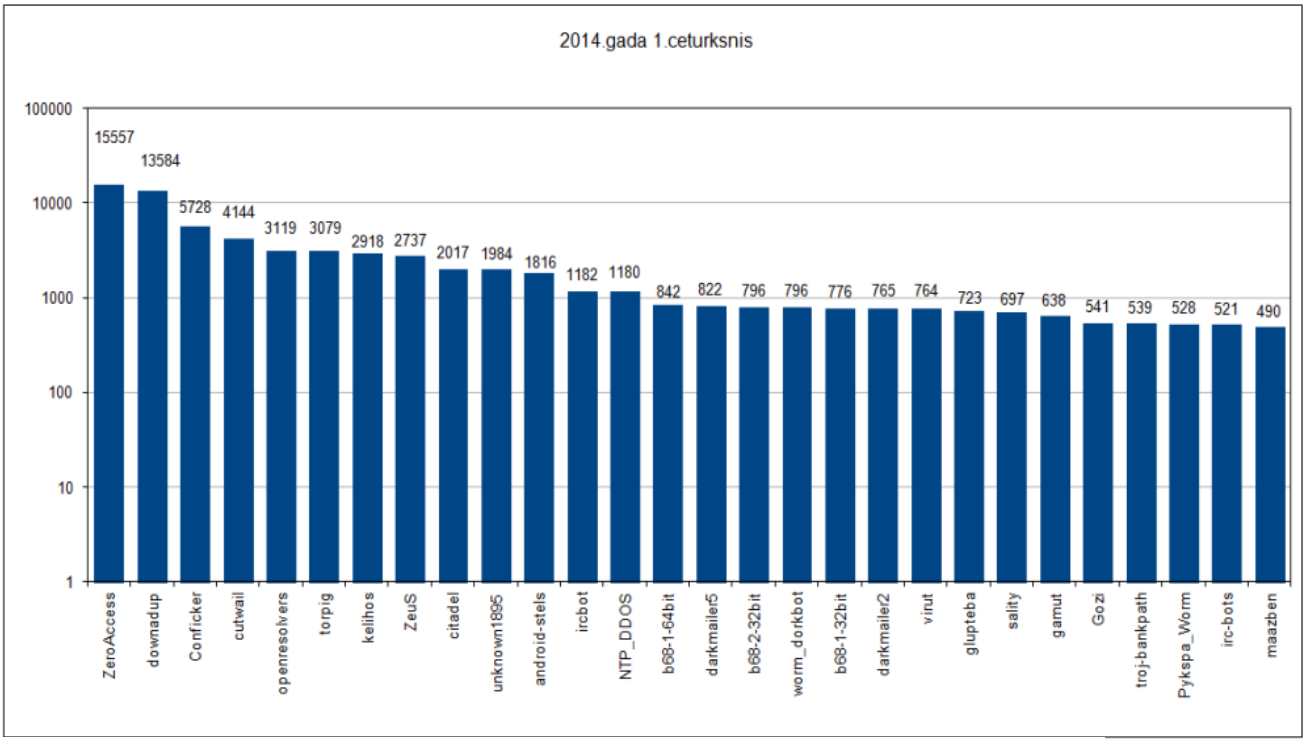
6.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.

Kompromitētu iekārtu daudzums attiecībā pret iepriekšējo pārskata periodu ir samazinājies, taču ievērojami pieauguši piekļuves lieguma uzbrukumi un ielaušanās mēģinājumi, salīdzinot ar iepriekšējo pārskata periodu.



7.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2014.gada 1.janvāra līdz 31.martam.

Pārskata periodā CERT.LV reģistrēja 81 321 zemas prioritātes incidentus, zemāk aplūkojams grafiks, kas demonstrē incidentu sadalījumu pa infekciju tipiem.

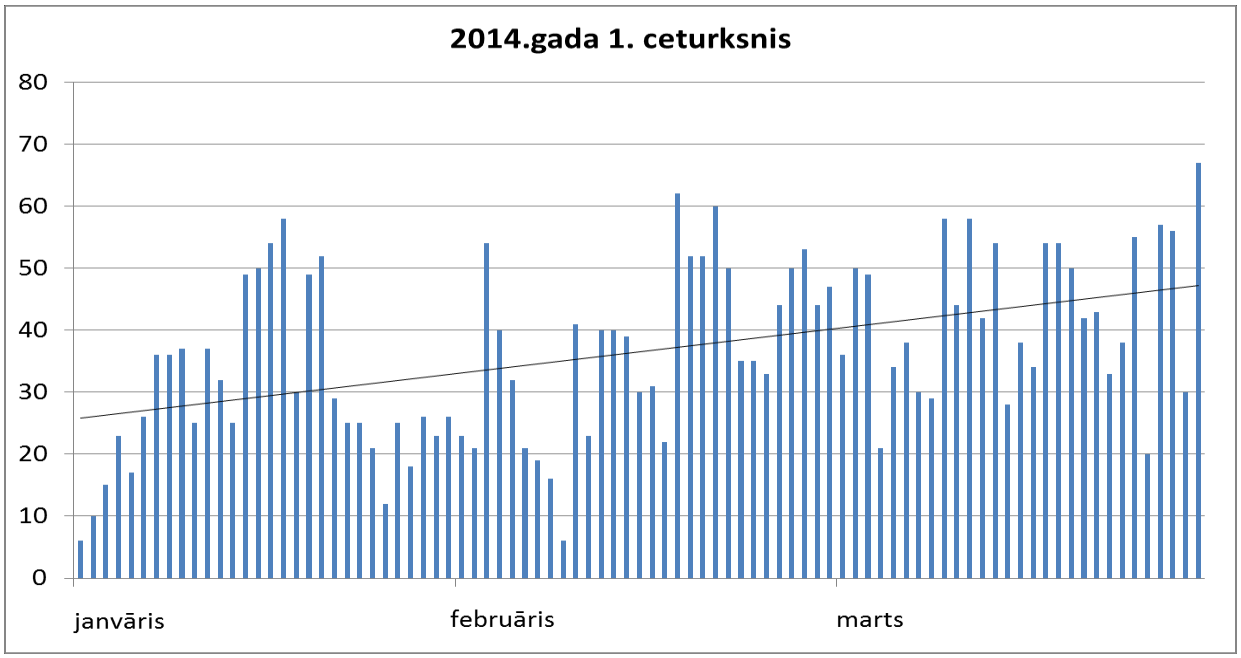


8.attēls - CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā no 2014.gada 1.janvāra līdz 31.martam pa infekciju tipiem.

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 312

inficētām IP adresēm. 9.attēlā 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 un to novēršana:

- 06.01. CERT.LV identificēja vairākus simtus ievainojamu serveru Latvijā, kas piedalījās DDoS uzbrukumā ārvalstu tīmekļa vietnei. Serveru turētāji tika informēti par incidentu, un tiem tika sniegtas instrukcijas problēmas risināšanai.
- 11.01. E-pastos tika masveidā izsūtīts "VID" Zeus saimes datorvīruss, kas satur inficētus failus. Inficētās e-pasta vēstules maldināja lietotājus, liekot domāt, ka saņemtās vēstules saturam ir kāda saistība ar Valsts ieņēmumu dienestu. Inficētās vēstules nosaukuma (subject) varianti bija dažādi, piemēram: *"nodoklu dienestam",*

  "Sudziba nodoklu dienestam", "Re:Sudziba nodoklu dienestam".

  Savukārt, pati vēstule saturēja frāzi (vai līdzīgu):

  "Labdien! Informacija par sudzibu nosutita nodoklu dienestam, nosutu Jums kopiju, skatit pielikuma. Ref id:xz27dns94m",

  Vēstulei tika pievienots pielikums ar inficētu failu, kam izmantots dubultais paplašinājums .DOC.zip, kuru atarhivējot, tiek iegūts .SCR tipa izpildāmais fails ar nosaukumu "nodokludienestam.doc.scr" vai "sudziba.doc.scr". Pielikumos esošais fails saturēja datorvīrusu, kurš domāts tiešsaistes banku maksājumu pārtveršanai un modifikācijai.

- 13.01. Izplatījās paroļu zagšanas vīruss. Inficējot datoru, tas tālāk inficēja arī jebkuru noņemamu disku, kas tiek pieslēgts inficētajam datoram. CERT.LV izpētīja, pie kādiem resursiem vīruss mēģina veikt pieslēgumus, kā arī apzināja potenciāli inficētos lietotājus - Latvijas tīklu diapazonā tie bija 399, pavisam kopā varētu būt inficētas ~460 iekārtas.

  Vīruss izplatījās ar e-pasta vēstuļu palīdzību, kas aicināja atvērt inficētus failus. Vēstules tekstā parādījās aicinājumi atvērt saiti uz files.inbox.lv un citiem failu apmaiņas serveriem. Vēstules nosaukums (subject) saturēja tekstu „Re:par problematisko situāciju", „Re:tikai starp mums" u.c.

  Inficētas vēstules teksta piemērs:

  Cau!

  Nosutu Tev to failu! Kad ielade, pasaki! Lai varu izdzest, jo ja tas nonaks prese vai publika, bus loti lielas nepatiksanas mums visiem! To neviens nedrikst ieraudzit!

  http://files.inbox.lv/ticket/2fcac0ba77b2e03eb33336c54b4cd63de664c9a9/

  Iveta

  Ja norādītā saite tika apmeklēta, fails lejupielādēts un atvērts, dators tika inficēts ar vīrusu. Vīruss ieguva pārlūkprogrammās saglabātās tīmekļa vietņu pieejas paroles, kā arī dažādus citus datus. CERT.LV aktīvi iesaistījās inficēto failu kopiju likvidēšanā uz failu apmaiņas serveriem, kā arī brīdināja inficētos lietotājus.

- 14.01. Tika identificēti 1185 NTP (Network Time Protocol) serveri, kas bija nedroši nokonfigurēti. Serveri tika identificēti, piedaloties DDoS uzbrukumos. Ir zināms, ka uzbrucēji izmantoja *NTP mode 7* ziņojumus kombinācijā ar avota IP adrešu viltošanu, lai veiktu uzbrukumus. Tika izstrādātas rekomendācijas, kā droši konfigurēt NTP servisu un tika apziņoti serveru īpašnieki.
- 20.01. Latvijā tika identificēti vairāki desmiti kompromitēti augstas veiktspējas Linux serveri. Infekcijas nosaukums bija *Ebury rootkit/backdoor trojan*. Veicot tā analīzi, tika noskaidrots, ka Ebury ir salīdzinoši sarežģīti identificējams un ārkārtīgi bīstams *trojāns*. Iesaistītajiem serveru turētājiem CERT.LV izsūtīja informāciju par incidentu un instrukcijas tā identifikācijai.
- 11.02. Tika aktivizēta jauna "VID" Zeus saimes vīrusa izsūtīšanas kampaņa.
- 11.02. Notika DDoS uzbrukums kāda uzņēmuma DNS serveriem. CERT.LV sniedza konsultācijas tā ietekmes mazināšanai.
- 20.02. Notika atkārtota "VID" Zeus saimes vīrusa izsūtīšanas kampaņa.
- 26.02. Twitter un e-pastos tika veikta kampaņa lietotāju datu izkrāpšanai, izmantojot „Positivus 2014" biļešu izlozes faktu. Izmantotie konti tika bloķēti.
- 27.02. Notika atkārtota "VID" Zeus saimes vīrusa izsūtīšanas kampaņa ar jaunākā vīrusa versiju, masveidā izplatot e-pasta vēstules, kas satur ar bīstamu datorvīrusu inficētu pielikumu, radot bankas datu izkrāpšanas un naudas līdzekļu nozagšanas risku.
- 28.02. Tika atklāti vairāki trūkumi valsts iestāšu tīmekļa vietņu SSL implementācijā. Iesaistīto lapu uzturētāji tika brīdināti.

- 03.03. Notika atkārtota VID "Zeus" saimes datorvīrusa izplatīšana.
- 03.03. Notika zemas intensitātes DDoS uzbrukums pret kādu portālu Latvijā. Uzbrukums īslaicīgi ietekmēja tā darbību. CERT.LV palīdzēja atklāt kļūdas serveru konfigurācijā, kas radīja šādas sekas.
- 11.03. Notika atkārtota VID "Zeus" saimes datorvīrusa izplatīšana.
- 14.03. Tika sniegta konsultācija kādam advokāta birojam par rīcību klienta datu zādzības gadījumā.
- 19.03. Tika sniegta palīdzība un rekomendācijas Skype sarakstes noklausīšanās novēršanai kāda privāta uzņēmuma amatpersonai.
- 21.03. Kādā valsts iestādes e-pastā tika konstatēts mēģinājums iesūtīt kaitīgus PDF pielikumus. Antivīruss tos bloķēja.
- 24.03. Tika konstatēts mēģinājums uzbrukt kādas valsts iestādes mājas lapas CMS sistēmai – tika veiktas izmaiņas konfigurācijā, padarot CMS nepieejamu no ārējām IP adresēm.
- 28.03. Kādā valsts iestādē konstatēti četri, ar „gozi" vīrusu inficēti datori. Datori tika iztīrīti, infekcijas avots tiek noskaidrots.

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 janvārī bija 30, februārī – 99, martā – 102.

Izķēmoto lapu sadalījums pa operētājsistēmām:
janvārī - 29 Linux, 1 FreeBSD,
februārī - 89 Linux, 4 FreeBSD, 6 nezināmas,
martā - 93 Linux, 7 FreeBSD, 2 Windows.

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

CERT.LV uztur tīmekļa vietni https://www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. Pārskata periodā vispopulārākā bija lapa ar CERT.LV sagatavoto informāciju par jaunākajām ievainojamībām un vīrusiem (11833 apmeklējumi), tai seko CERT.LV sagatavota informācija par „Policijas vīrusa" apkarošanas praksi un mehānismiem (9283 apmeklējumi). Trešā populārākā ziņa pārskata periodā bija CERT.LV sagatavotā informācija un brīdinājums par „VID vīrusu" (8639 apmeklējumi).
Kopā CERT.LV mājas lapai bijuši 27805 apmeklējumi, kurus veido 20697 unikāli apmeklējumi no 80 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa – 94,24% apmeklējumu bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicētas 39 ziņas, sniegta informācija par CERT.LV organizētiem un starptautiska mēroga pasākumiem, publicētas CERT.LV prezentācijas, mediju ziņas un CERT.LV publiskie darbības pārskati par 2013.gada 4.ceturksni un 2013.gadu.

CERT.LV ir divi Twitter konti un tajos tiek regulāri publicētas ziņas par dažādiem jaunumiem: https://twitter.com/certlv un https://twitter.com/datorologs. Pārskata perioda laikā certlv kontā tika publicētas 86 ziņas, kontam pievienojušies 77 jauni sekotāji un vismaz 84 reizes CERT.LV ziņa ir tikusi „retvītota" jeb padota tālāk. CERT.LV Facebook profilā http://www.facebook.com/certlv pārskata periodā publicētas 82 ziņas. CERT.LV izveidots profils portālā draugiem.lv www.draugiem.lv/certlv.

CERT.LV uztur arī pieaugušo izglītošanas portālu https://www.esidross.lv. Pārskata perioda laikā portālā ir publicēti 4 jauni raksti, portāls apmeklēts 19 547 (15 119 unikāli) reizes. Publicētie raksti:

- Visa dzīve interneta spogulī.
- Pārbaudi savas zināšanas IKT drošībā ar e-GUARDIAN drošības prasmju barometru.
- Iespēja bez maksas pārbaudīt datoru! – Aicinājums apmeklēt akciju Datorologs.
- Latvijā izstrādāts paroļu aizstājējs – unikāls risinājums CaptureIn.

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

1) Intervijas un ziņas radio:

- 20.01. Komentārs par starptautisko spiegošanu valsts līmenī Latvijas radio 1 raidījumā "Septiņas dienas Eiropā".
- 18.02. Saruna par zibatmiņu drošību Latvijas radio 1 raidījumā "Zināmais Nezināmajā".
- 18.02. Saruna par mobilajām aplikācijām telefonā Latvijas radio 1 raidījumā "Kā labāk dzīvot".
- 24.02. Meet Latvia's cyber guards - CERT.LV vadītājas komentārs vācu raidsabiedrības "Deutsche Welle" radījumam "Spectrum" par Latvijas

kiberzemessardzi.

2) Sižeti televīzijā, tiešraides:

- 22.01. Sniegts komentārs LTV1 raidījumam "Rīta panorāma" par IT drošību.
- 16.02. Sniegts komentārs TV3 raidījumā "Nekā personīga" par kibernoziedzību publiskās informācijas pieejamības kontekstā.
- 11.03. Intervija raidījumā "Bez Tabu par mobilo aplikāciju drošību.
- 24.03. Sniegts komentārs TV3 raidījumā „Bez tabu"saistībā ar interneta vietnē www.avaaz.org rīkoto parakstu vākšanu par Latvijas iestāšanos Krievijas Federācijā.
- 24.03. Sniegts komentārs LNT raidījumā 900 sekundes par kiberdrošību Latvijā Ukrainas notikumu kontekstā.
- 25.03. Sniegts komentārs TV3 raidījumā „Bez tabu" par banku vīrusu.

3) Ziņas portālos:

- 20.01. Prezidentūras laikā Latvijai draud globāli kiberuzbrukumi – raksts portālā "Diena.lv".
- 17.02. Uzņēmumus atkal mulsina bīstamais VID vīruss – raksts portālā "Diena.lv".
- 04.03. Latvia launches Cyber Defence Unit to beef up online security – raksts vācu raidsabiedrības Deutsche Welle portālā www.dw.de.
- 11.03. CERT.LV: Tā dēvētā VID datorvīrusa izplatītājs varētu būt saistīts ar Latviju – raksts portālā "Diena.lv".
- 11.03. CERT.LV: Ar Ukrainu saistīti kiberuzbrukumi nav konstatēti – raksts portālā "Tvnet.lv".
- 11.03. Eksperts: Vecie mobilie telefoni ir drošāki par viedtālruņiem – raksts portālā "Diena.lv".
- 13.03. Hakeriem apnikuši datori, tie tēmē uz mobilām ierīcēm – raksts portālā "Tvnet.lv".
- 19.03. Pilns internets ar ziloņiem trauku veikalā – raksts portālā "Diena.lv".

5.martā CERT.LV pārstāvji piedalījās LETA organizētā mediju diskusijā par kibernoziedzību Latvijā, rezultātā tapa vairāki LETA raksti par IT drošības tēmu, kurus pārpublicēja tādi ziņu portāli kā "Diena.lv" un "Tvnet.lv". Publicitāte parādījās arī medijos ārvalstīs.

18.martā CERT.LV pārstāvis uzstājās e-drošības konferencē medijiem „Kā pasargāt sevi internetā un droši lietot tā plašās iespējas?", kas tika organizēta sadarbībā ar Swedbank un draugiem.lv.

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

Pārskata periods uzsākās ar prezentācijām skolēniem par IT drošību. Janvāris noslēdzās ar CERT.LV rīkoto semināru informātikas skolotājiem "IT drošība skolā". Salīdzinot ar iepriekšējo pārskata periodu, pieaudzis sniegto prezentāciju skaits skolās par IT drošību.

2014. gada 11.februārī tika atzīmēta Drošāka interneta diena, kuru CERT.LV atzīmēja, sniedzot prezentācijas par IT drošību.

Ēnu dienas ietvaros 12.februārī diviem skolēniem bija iespēja iepazīties ar CERT.LV speciālistu darbu, sīkāk uzzināt par informācijas tehnoloģiju drošības incidentiem, to risināšanu, kā arī uzzināt par citiem CERT.LV darbības virzieniem.

Martā redzamākais pasākums bija E-prasmju nedēļa, kas norisinājās no 24.-30.martam. Tās ietvaros 26.martā CERT.LV rīkoja Datorologa akciju, kas sniedza iespēju ikvienam interesentam pārbaudīt sava datora "veselību" pie datorologa – CERT.LV speciālista. Salīdzinot ar iepriekšējiem gadiem, tika atklāts ievērojami mazāks inficēto datoru skaits, kas liecina, ka cilvēki arvien vairāk rūpējas par savu datoru veselību. Galvenās problēmas, ko datorologam nācās risināt, izraisīja aizmirsti programmatūras atjauninājumi, iespējoti spraudņi, kurus lietotājs neizmanto, un neuzmanības pēc lejupielādēti pārlūkprogrammu paplašinājumi. Akcija norisinājās vienas dienas garumā, un tās laikā datorologi veica 58 datoru pārbaudi un "ārstēšanu". CERT.LV datorologiem talkā nāca Lattelecom un Latnet Serviss eksperti.

E-prasmju nedēļas ietvaros CERT.LV drošības speciālisti piedalījās IKT Karjeras dienā, dodot iespēju jauniešiem iepazīties ar savu darbu, kā arī CERT.LV pārstāvis nolasīja lekciju Rīgas Tehniskās universitātes studentiem par IT drošību.

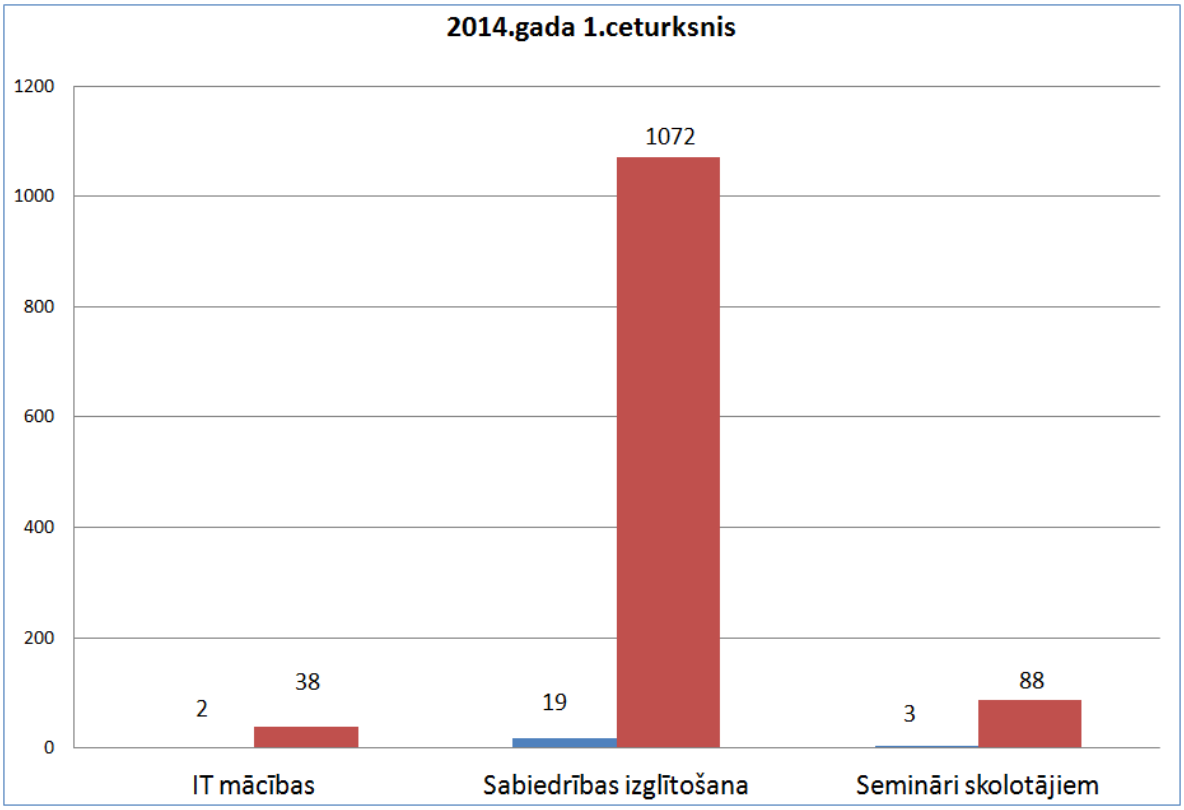
Pārskata periodu noslēdza CERT.LV organizēts seminārs "IT drošība skolā" informātikas skolotājiem CERT.LV telpās. To apmeklēja 26 dalībnieki.

CERT.LV pasākumi pārskata periodā:

- 12.01. CERT.LV pārstāvis sniedza prezentāciju skolēniem Dobeles 1.vidusskolā par IT drošību.
- 12.01. CERT.LV pārstāvis sniedza prezentāciju skolēniem Dobeles Valsts ģimnāzijā par IT drošību.
- 12.01. CERT.LV pārstāvis sniedza prezentāciju skolēniem Rīgas Katoļu ģimnāzijā par IT drošību.
- 14.01. CERT.LV pārstāvis sniedza prezentāciju skolēniem Rīgas 69.vidusskolā par IT drošību.
- 16.01. CERT.LV pārstāvis uzstājās ar prezentāciju ISACA Latvija sanāksmē par Steadfast Jazz incidentu.
- 17.01. Notika CERT.LV organizēts seminārs skolotājiem Rīgas 9.vakara maiņu vidusskolā par IT drošību.
- 24.01. Notika CERT.LV organizēts seminārs Rundāles pašvaldībā par informācijas drošības izpratnes veicināšanu.
- 28.01. CERT.LV pārstāvis sniedza prezentāciju skolēniem Rīgas Katoļu ģimnāzijā par tēmu „Prasme pasargāt sevi digitālajā laikmetā".
- 31.01. CERT.LV seminārs informātikas skolotājiem "IT drošība skolā".
- 11.02. Norisinājās Drošāka interneta diena.
- 12.02. CERT.LV piedalās Ēnu dienā.
- 12.02. CERT.LV pārstāvis sniedza prezentāciju skolēniem Rīgas Katoļu ģimnāzijā vecāko klašu skolēniem.
- 13.02. CERT.LV pārstāvis sniedza prezentāciju skolēniem Dobeles 1. vidusskolā par IT drošību.
- 13.02. CERT.LV pārstāvis sniedza prezentāciju skolēniem Dobeles Valsts ģimnāzijā par IT drošību.
- 14.02. CERT.LV pārstāvis sniedza prezentāciju skolēniem Rīgas 69.vidusskolā par IT drošību.
- 17.02. CERT.LV pārstāvis sniedza prezentāciju skolotājiem Rīgas 9. vakara (maiņu) vidusskolā par IT drošību.
- 18.02. CERT.LV pārstāvis sniedza prezentāciju LU IT drošības specseminārā par tēmu "Responsible disclosure policy".

- 27.02. Notika CERT.LV organizētais seminārs "IT drošības vizualizācija" par IT drošības datu vizualizāciju.
- 06.03. Notika CERT.LV organizētais seminārs "IT drošības vizualizācija" par IT drošības vizualizāciju.
- 19.03. CERT.LV pārstāvis uzstājās ar prezentāciju ISACA Latvija sanāksmē IT drošības vizualizācija.
- 25.03 E-prasmju nedēļas ietvaros CERT.LV pārstāvis sniedza prezentāciju RTU studentiem par IT drošību.
- 26.03 E-prasmju nedēļas ietvaros CERT.LV telpās norisinājās Datorologa akcija.
- 26.03. E-prasmju nedēļas ietvaros CERT.LV telpās norisinājās IKT Karjeras diena.
- 28.03. Notika CERT.LV organizētais seminārs informātikas skolotājiem "IT drošība skolā".

Pārskata periodā CERT.LV par IT drošību ir izglītojis 1198 cilvēkus, piedaloties 24 dažādos pasākumos un lekcijās.



10.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits 2014.gada 1.ceturksnī.

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 aprakstīta atskaites 2.punktā. Zemāk uzskaitītas citas sadarbības tikšanās un konsultācijas.

- 10.01. CERT.LV tikās ar LU Datorikas fakultātes pārstāvjiem par IT drošības specsemināru organizēšanu.
- 15.01., 21.01., 27.01. CERT.LV tikās ar Aizsardzības ministriju par IT drošības stratēģijas rīcības plāna izstrādi.
- 29.01. Notika tikšanās ar Aizsardzības ministru R.Vējoni.
- 07.02. CERT.LV piedalījās Latvijas IT drošības padomes sēdē.
- 07.02. CERT.LV tikās ar VARAM un LIKTA pārstāvjiem par E-prasmju nedēļas pasākumiem
- 11.02. CERT.LV pēc Valsts kancelejas lūguma sniedza viedokli par Valsts tiešās pārvaldes un centrālo valsts iestāžu tīmekļa vietņu attīstības koncepciju.
- 18.02. CERT.LV piedalījās VARAM darba grupā par „Par kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un paaugstinātas drošības kvalificētu personas elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību".
- 21.02. Notika sadarbības tikšanās ar VARAM par ES prezidentūras jautājumiem.
- 21.02. un 07.03. CERT.LV piedalījās Tieslietu ministrijas organizētajā sanāksmē par Eiropas Parlamenta un Padomes direktīvas 2013/40/ES par uzbrukumiem informācijas sistēmām.
- 28.02. CERT.LV tikās ar Aizsardzības ministrijas valsts sekretāru J.Sārtu.
- 28.02. CERT.LV uzstājās VARAM organizētajā seminārā par E-prasmju nedēļu reģionālajiem partneriem.
- 13.03. CERT.LV pārstāvis piedalījās Aizsardzības sektora sabiedrisko attiecību speciālistu sanāksmē.
- Pārskata periodā CERT.LV uzsāka darbu pie IT drošības agrās brīdināšanas sistēmas veidošanas. Tika apzināti potenciālie sadarbības partneri, uzsākta vēstuļu sarakste un notika vairākas tikšanās.

6. Uzraudzīt, kā valsts un pašvaldību institūcijas un elektronisko sakaru komersanti izpilda Informācijas tehnoloģiju drošības likumā noteiktos pienākumus.

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 31.martam CERT.LV ir apkopojis informāciju par 617 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 31.martam plānus ir iesnieguši 58 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 šādos starptautiskos pasākumos:

- 27.01. CERT.LV pārstāvis piedalījās „NB8/UK/Poland Cyber Policy Roundtable" sanāksmē.
- 30.01. CERT.LV pārstāvis piedalījās Baltijas valstu sanāksmē, „Latvia-Estonia cyber-cooperation". Rīgā par Latvijas - Igaunijas sadarbības iespējām kiberdrošības un e-pakalpojumu savietojamības jomā.
- 06.02. CERT.LV pārstāvji piedalījās „Baltic Cyber security Policy Coordination Meeting", kas notika Viļņā.
- 10.-12.02. CERT.LV pārstāvji piedalījās TF-CSIRT un Trusted Introducer sanāksmēs un FIRST tehniskajā seminārā Cīrihē, Šveicē.
- 20.02. CERT.LV pārstāvis piedalījās sadarbības videokonferencē ar CERT.EE.
- 28.02. CERT.LV pārstāvis piedalījās Ārlietu ministrijas organizētajā videokonferencē ar Igauniju un Lietuvu par sadarbību kritiskās infrastruktūras aizsardzības un kiberdrošības jautājumos.
- CERT.LV vienojās ar Čehijas pārstāvjiem veidot kopīgu komandu NATO kiberdrošības mācībās „Locked Shields".
- Tika aizpildīta Eiropas Komisijas IT risku novērtēšanas metožu anketa (Survey of Risk Management Methods, Frameworks and Capability Maturity Models for the EU Network Information Security Platform).

8. Veikt citus normatīvajos aktos noteiktos pienākumus.

- 09.01. 13.02 un 13.03. notika DEG grupas sanāksmes.
- 27.01. CERT.LV pārstāvis piedalījās *webinārā* par IBM datu analīzes un vizualizācijas risinājumu.
- 05.02. Notika sadarbības tikšanās ar SIA DPA par CaptureIn risinājumu.
- 13.02. CERT.LV piedalījās IT drošības datu vizualizācijas rīku izstrādes projekta plānošanā sadarbībā ar citām LUMII laboratorijām.
- 24.02. Notika CERT.LV pārstāvja tikšanās ar LLU studentu par maģistra darba izstrādi.
- 06.03. Notika CERT.LV pārstāvju tikšanās ar Lattelecom par projektu "Pieslēdzies, Latvija".

2014. gada 28.aprīlī

Sagatavotājs – Svetlana Amberga,
tālrunis 67085866
e-pasts Svetlana.Amberga@cert.lv