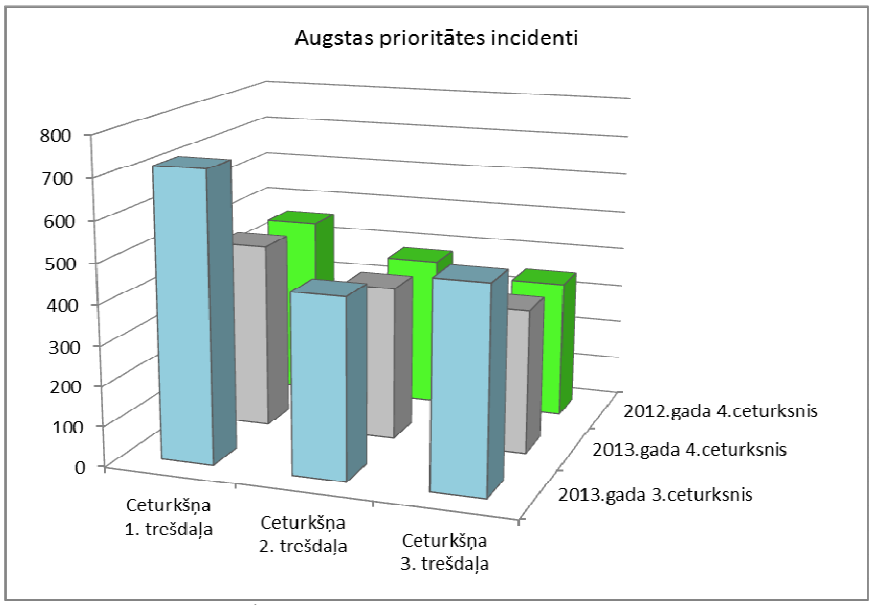
Publiskais pārskats par CERT.LV (Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas) uzdevumu izpildi 2013.gada 4.ceturksnī
(01.10.2013. – 31.12.2013.)

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 1213 augstas prioritātes incidentus. Iepriekšējā periodā tika reģistrēti un apstrādāti 1672 augstas prioritātes incidenti, bet 2012.gada oktobra-decembra periodā 1186 incidenti.

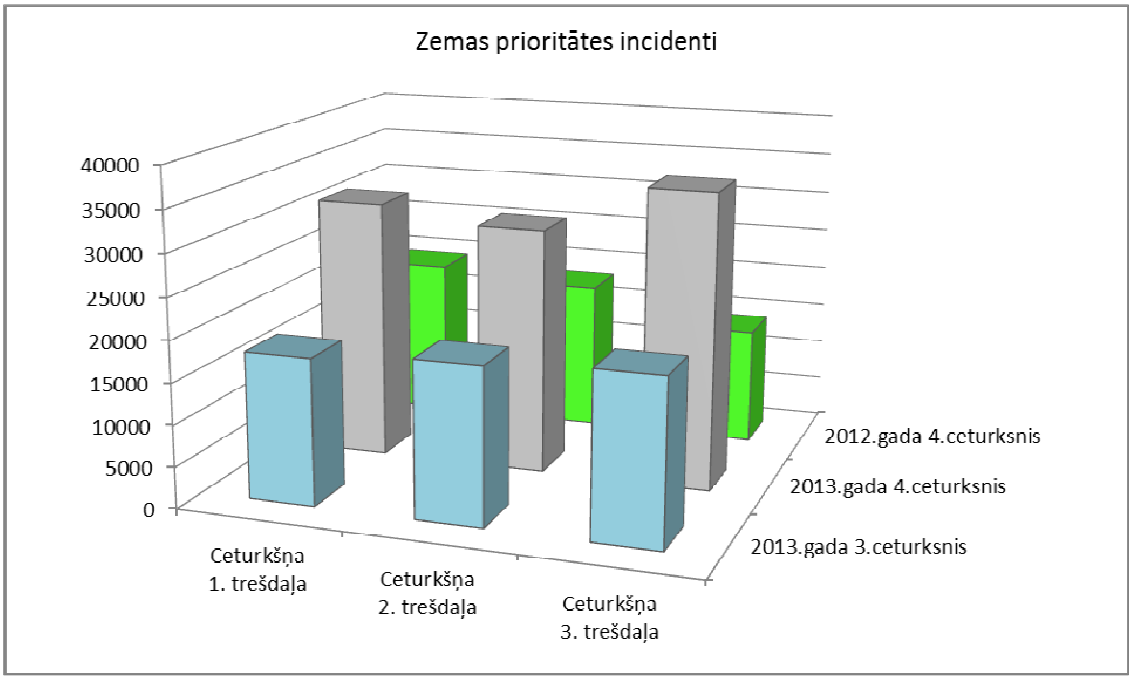


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pārskata gada 4.ceturksnī, kā arī pārskata gada 3.ceturksnī un 2012.gada 4.ceturksnī sadalījumā pa atsevišķiem mēnešiem.

Pārskata periodā, salīdzinājumā ar iepriekšējo periodu, ir vērojams reģistrēto un apstrādāto augstas prioritātes incidentu samazinājums, taču tas skaidrojams ar vispārēju tendenci augstas prioritātes incidentu apjomam katra gada pēdējā ceturksnī kristies. To apliecina arī tas, ka pārskata gada

4.ceturkšņa augstas prioritātes incidentu rādītājs būtiski neatšķiras no reģistrēto un apstrādāto augstas prioritātes incidentu apjoma pirms gada.

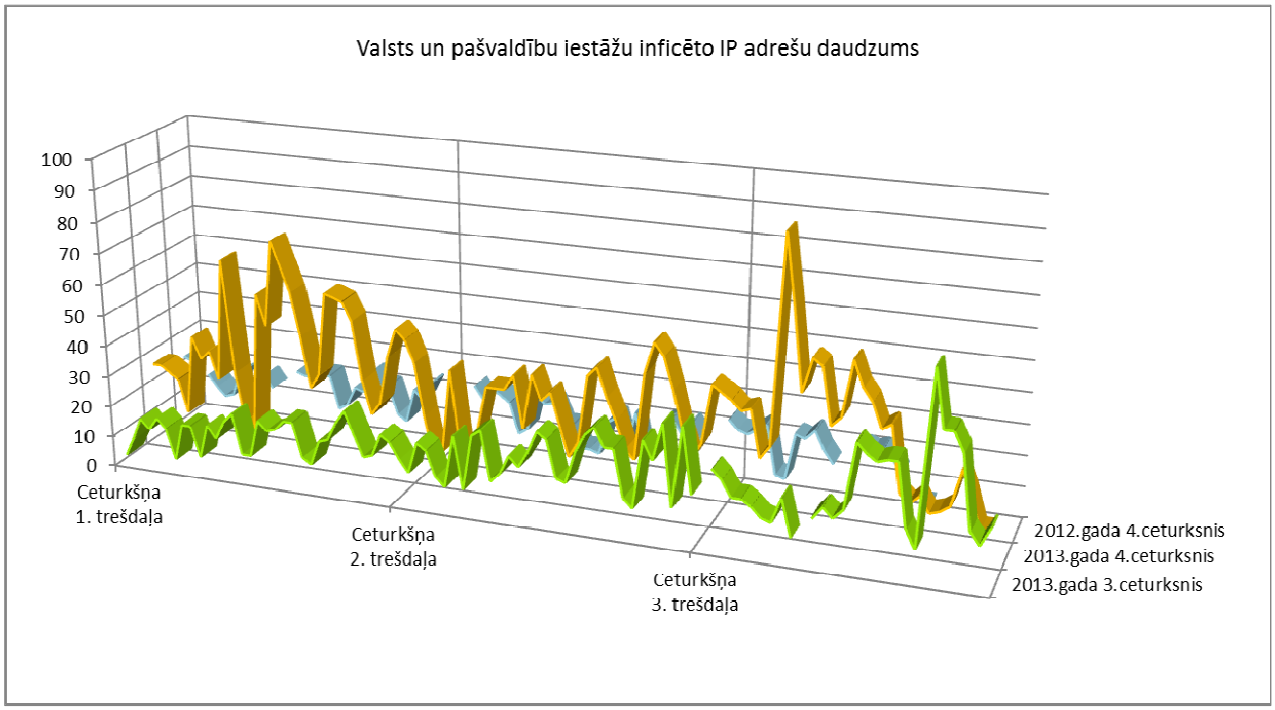
2013.gada 4.ceturksnī CERT.LV reģistrēja 80 321 zemas prioritātes incidentu. Iepriekšējā periodā tika reģistrēti 46 040 zemas prioritātes incidenti, bet 2012.gada 4.ceturksnī 64 944 zemas prioritātes incidenti.



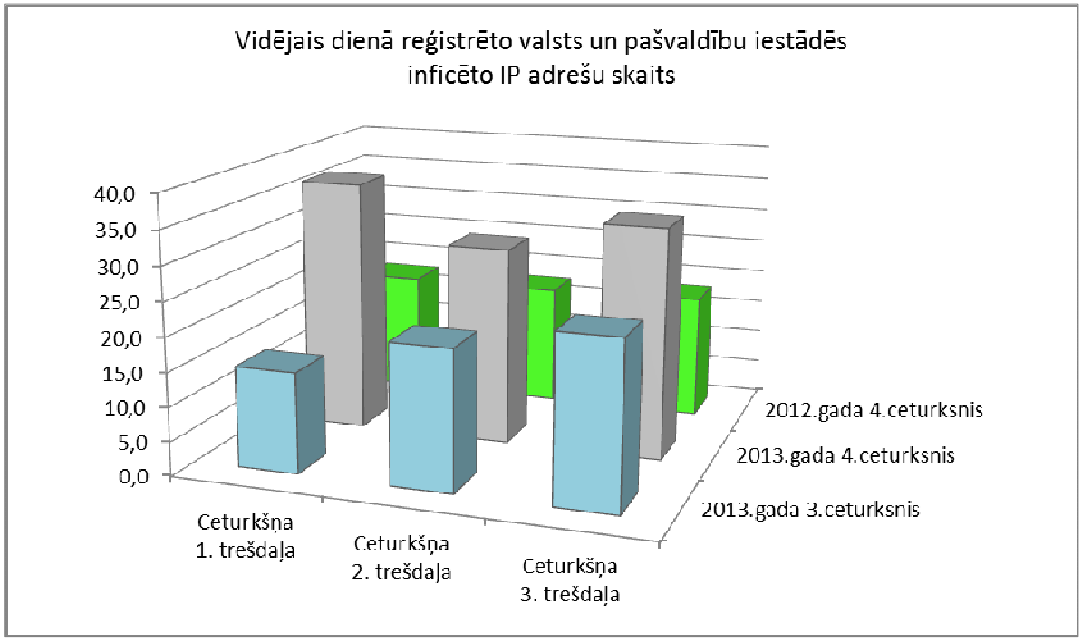
2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pārskata gada 4.ceturksnī, kā arī pārskata gada 3.ceturksnī un 2012.gada 4.ceturksnī sadalījumā pa atsevišķiem mēnešiem.

Pārskata periodā reģistrēto zemas prioritātes incidentu apjoms ir būtiski pieaudzis, salīdzinot gan ar iepriekšējo periodu, gan šo pašu periodu pirms gada, jo 2013.gada 4.ceturksnī Latvijā tika izvērstas vairākas kiberuzbrukumu kampaņas, kas tika mērķētas tieši uz Latvijas interneta lietotājiem, kā arī Latvijai nepaslīdēja garām starptautiskas kibernoziedznieku aktivitātes, kuru mērķis bija gūt labumu no pieejamajiem resursiem, neatkarīgi no to atrašanās vietas. Kā piemēru starptautiskām aktivitātēm var minēt ZeroAccess robotu tīkla (botnet) izplešanos virtuālās naudas *bitcoin* ģenerēšanas nolūkos, jo gada pēdējā ceturksnī *bitcoin* piedzīvoja strauju vērtības kāpumu.

2013.gada 4.ceturksnī, salīdzinot ar iepriekšējo ceturksni un ar šo pašu periodu pirms gada, palielinājies arī to inficēto IP adrešu daudzums, kas reģistrētas valsts un pašvaldību iestādēs. Arī šis pieaugums skaidrojams ar virkni Latvijas kibertelpā izvērsto noziedzīgo kampaņu, kuru mērķis bija inficēt datorus un izgūt lietotāju datus.



3.attēls – Valsts un pašvaldību iestāžu inficēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2013.gada 4.ceturksnī, 2013.gada 3.ceturksnī un 2012.gada 4.ceturksnī.



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

Kā viens no nozīmīgākajiem incidentiem pārskata periodā minamas kiberuzbrukumu kampaņas, kas tika mērķētas uz Latvijas internetbanku lietotājiem ar mērķi izgūt internetbanku piekļuves datus un pārtvert un pārvirzīt internetbankās veicamos maksājumus uz kiberuzbrucēju izvēlētiem kontiem. Oktobrī virknē Latvijas datorlietotāju radīja satraukumu arī tā dēvētā „policijas vīrusa" tīmekļa versija, kuras darbību vairs neierobežoja noteiktas operētājsistēmas lietošana. Kā vēl viens būtisks incidents pārskata periodā minama ielaušanās Nodarbinātības valsts aģentūras (NVA) tīmekļa vietnē un 3000 lietotāju datu izgūšana. Šis incidents ieguva arī starptautisku rezonansi.

Lielāko sabiedrības un mediju uzmanību pārskata periodā izpelnījās NVA incidents, apdraudējums Latvijas internetbanku lietotājiem un NATO mācību „Steadfast Jazz 2013" laikā notikušie

kiberuzbrukumi, izķēmojot dažādas tīmekļa vietnes un izsūtot viltus e-pastus ar mērķi diskreditēt gan NATO, gan „Steadfast Jazz 2013" mācības.

Organizēto pasākumu ziņā 2013.gada 4.ceturksnis iezīmējas ar to, ka oktobris tika pasludināts par Eiropas Kiberdrošības mēnesi, kura laikā tad arī notika lielākā daļa IT drošībai veltītu aktivitāšu. Kā sabiedrībā plašāk atpazīstamā jāmin Datorologa akcija, kas ievadīja šī gada Kiberdrošības mēnesi Latvijā un kuras mērķis ir aktualizēt atbildīgu datora un interneta lietošanu. IT speciālistiem un interesentiem tika organizēta ISACA un CERT.LV rudens konference, bet, lai apmācītu jaunākos datorlietotājus, CERT.LV ar prezentācijām par IT drošību viesojās skolās. Pārskata perioda noslēgumā CERT.LV organizēja IT drošības semināru „Esi drošs-2" valsts un pašvaldību iestāžu par IT drošību atbildīgajiem.

Kopā pārskata periodā CERT.LV piedalījās 19 pasākumos, apmācot gandrīz 2000 cilvēkus, publicēja četrus jaunus rakstus portālā www.esidross.lv, 23 jaunas ziņas portālā www.cert.lv, piedalījās desmit radio pārraidēs un sešos televīzijas sižetos.

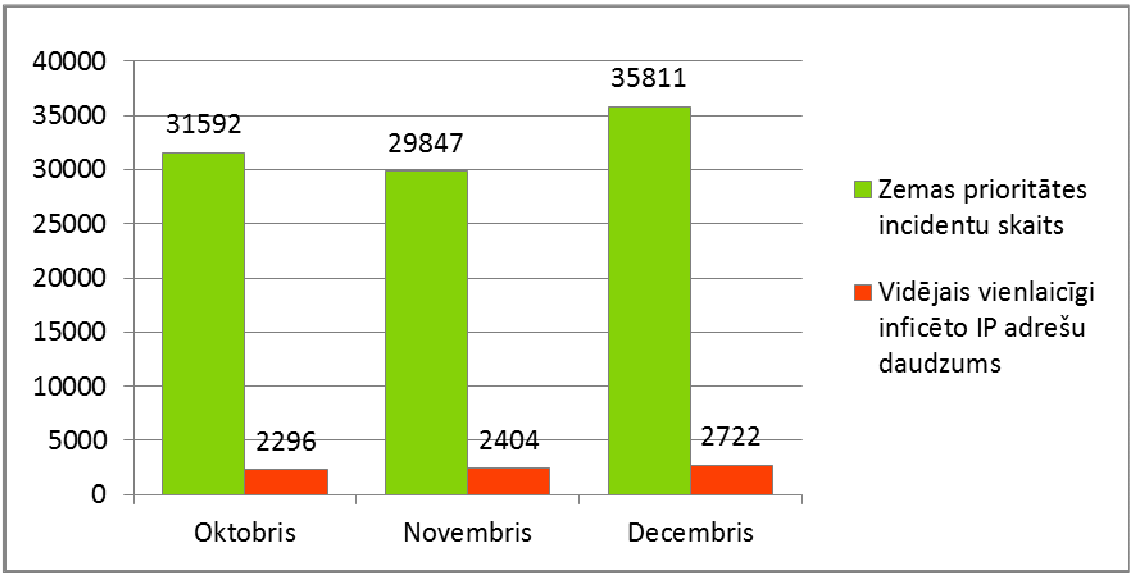
1. Uzturēt vienotu elektroniskās informācijas telpā notiekošo darbību atainojumu.

2013.gada ceturtajā ceturksnī CERT.LV apstrādāja 1213 augstas prioritātes incidentus, kas ir par 459 incidentiem jeb 27,5% mazāk nekā šī gada trešajā ceturksnī un par 27 incidentiem jeb 2% vairāk nekā 2012.gada ceturtajā ceturksnī.

2013.gada ceturtajā ceturksnī CERT.LV reģistrēja 80 321 zemas prioritātes incidentu, kas ir par 34 281 incidentu jeb 74,5% vairāk nekā šī gada trešajā ceturksnī un par 15 377 incidentiem jeb 24% vairāk nekā 2012.gada ceturtajā ceturksnī.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Oktobrī šis skaits bija 2296, novembrī – 2404, bet decembrī – 2722 inficētas IP adreses.

5.attēlā redzams, kā mainījies zemas prioritātes incidentu skaits un vidējais inficēto IP adrešu daudzums 2013.gada 4.ceturkšņa laikā.



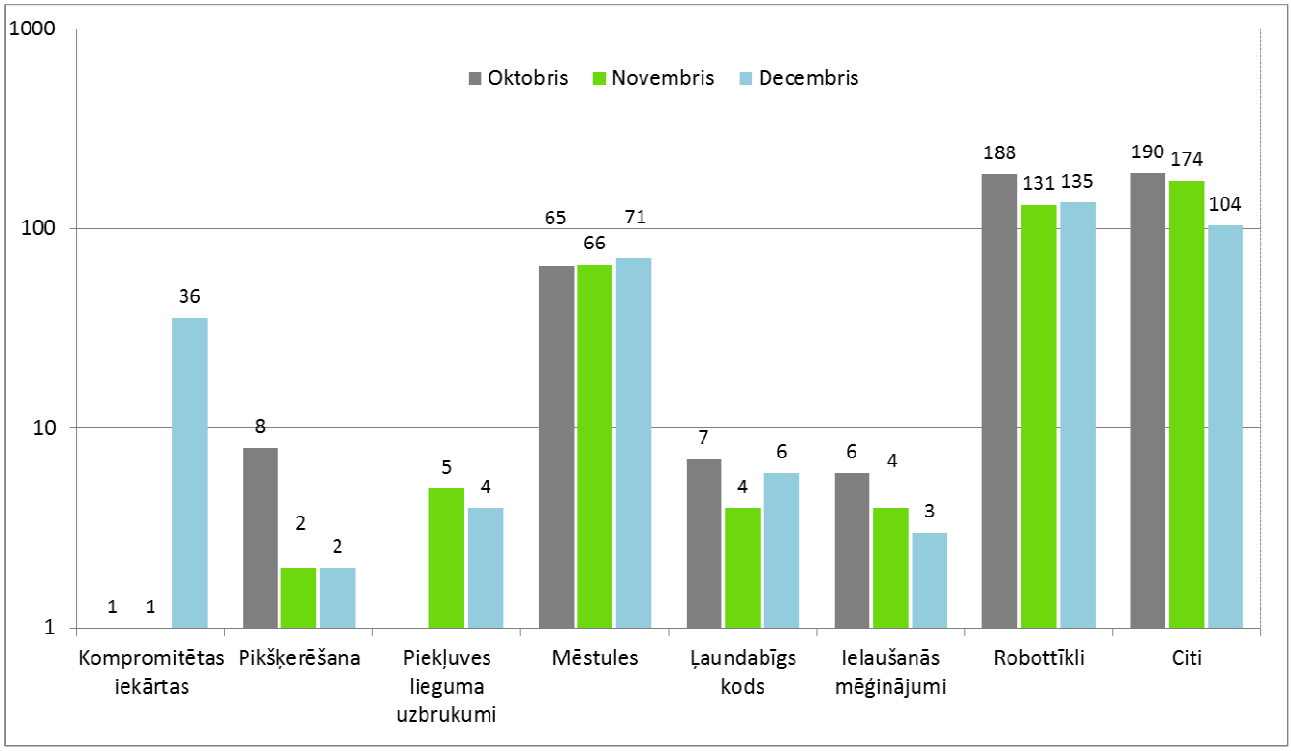
5.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem 2013.gada 4.ceturksnī.

Reģistrēto zemas prioritātes incidentu apjoma pieaugums 2013.gada 4.ceturksnī skaidrojams gan ar vairākām pārskata periodā notikušām pikšķerēšanas kampaņām, kas tika vērstas pret Latvijas internetbanku lietotājiem, gan ar gada nogali, kas saistās ar dāvanu meklēšanu un iepirkšanos internetā, izraisot pastiprinātu mēstuļotāju un kibernoziedznieku aktivitāti. Ļaundari centās izmantot arī gada nogales saspringto situāciju uzņēmumu finanšu un juridiskajos departamentos, izsūtot atslēgvārdus „nodokļi" un „sūdzība" saturošus e-pastus ar inficētiem pielikumiem (pazīstams arī kā „VID vīruss"). Zemas prioritātes incidentu apjoma palielināšanos pārskata periodā sekmēja arī virtuālās naudas *bitcoin* popularitātes un vērtības pieaugums, veicinot datoru inficēšanu ar mērķi iesaistīt tos robotu tīklos, kas paredzēti tieši šīs virtuālās naudas ģenerēšanai (ZeroAccess botnet).

Lai samazinātu kopējo inficēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar tiem interneta pakalpojumu sniedzējiem (IPS), kas vēlas sadarboties ar šīm abām organizācijām un pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". Uz pārskata perioda beigām atbildīgo IPS kopskaits bija 14.

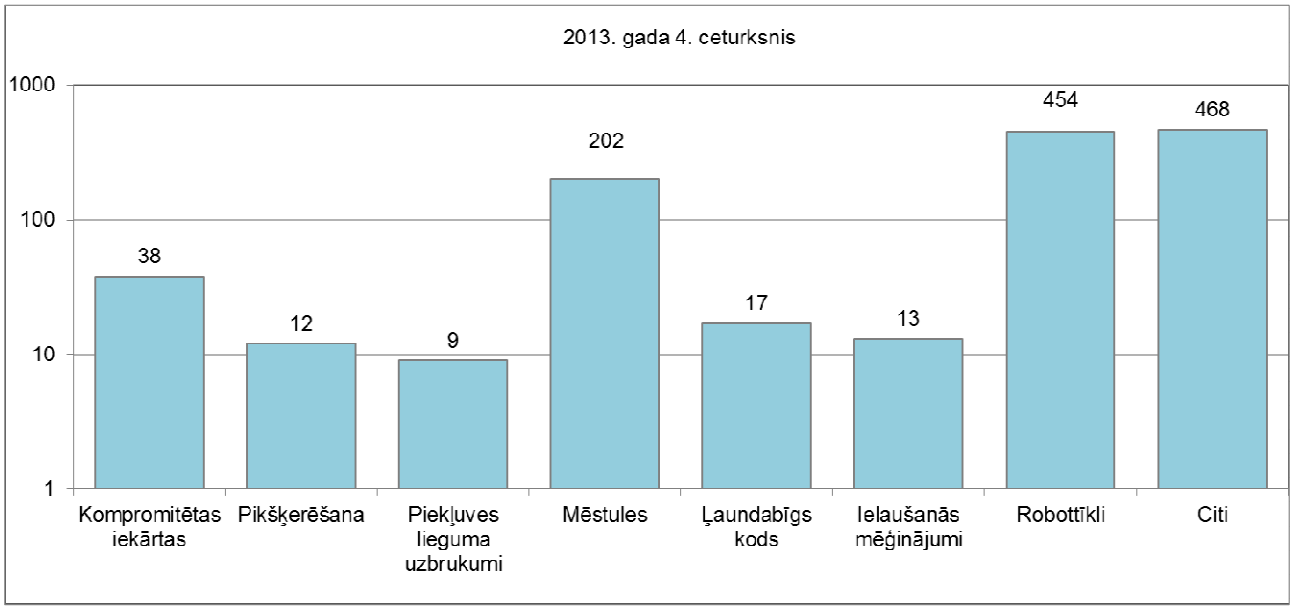
2. Sniegt atbalstu informācijas tehnoloģiju drošības incidenta novēršanā vai koordinēt to novēršanu.

Pārskata perioda laikā CERT.LV ir reģistrējis un apstrādājis 1213 augstas prioritātes incidentus. 6.attēlā redzams augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem (grafiks ir logaritmiskā mērogā).



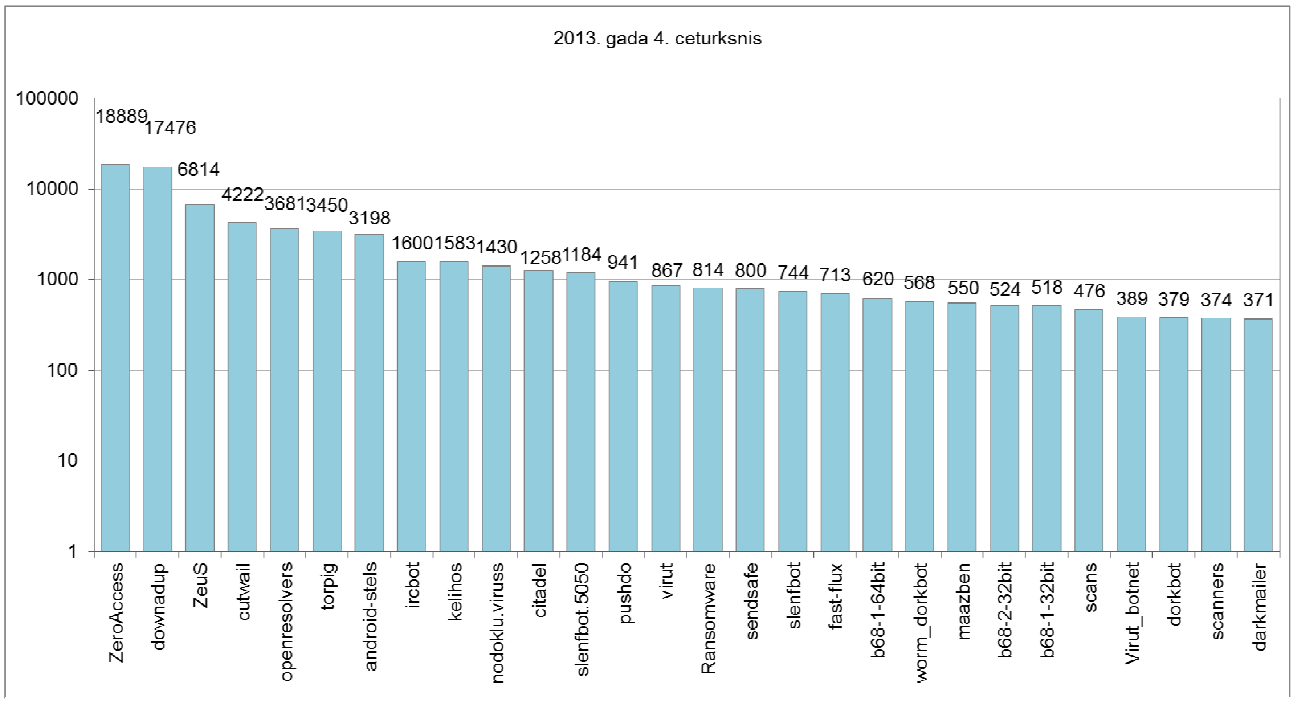
6.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pārskata periodā pa tipiem un pa mēnešiem.

Kompromitētu iekārtu daudzuma pieaugums decembrī skaidrojams ar „VID" jeb „nodokļu" vīrusa kampaņu, kas tika izvērsta gada nogalē. Kampaņas ietvaros uzņēmumiem tika izsūtīti e-pasti ar atslēgvārdiem „nodokļu dienests" un „sūdzība", kas pielikumā saturēja kaitīgu kodu saturošu arhīvu, kura atvēršana nodrošināja datora inficēšanu un kompromitēšanu.



7.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2013.gada 1.oktobra līdz 31.decembrim (grafikā izmantota logaritmiskā skala).

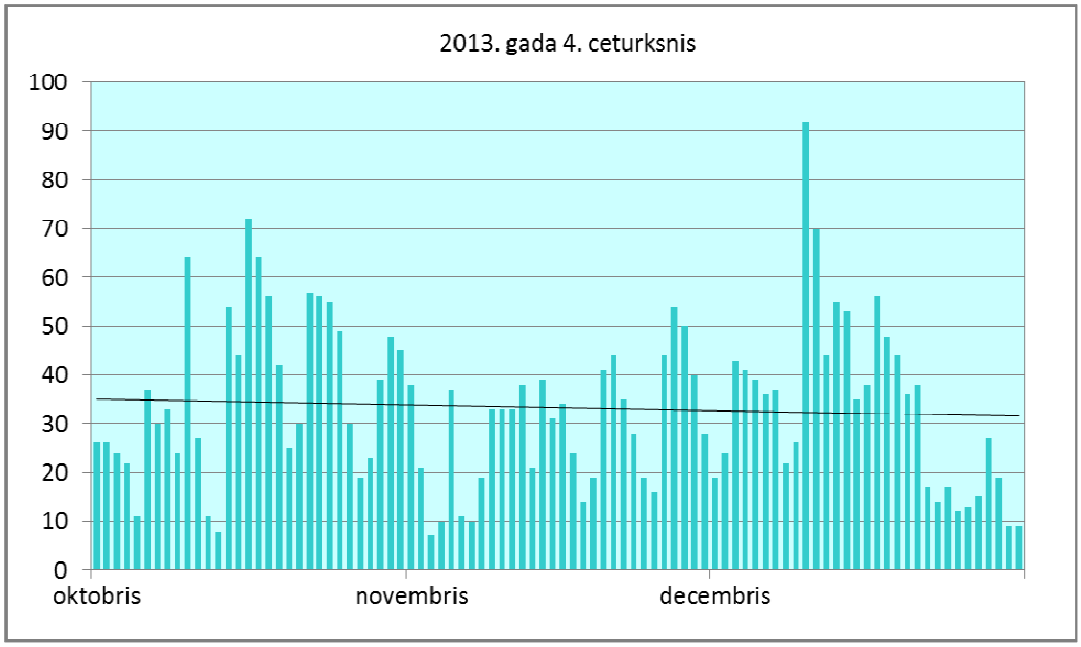
Pārskata perioda laikā CERT.LV ir reģistrējis 80 321 zemas prioritātes incidentus, par 77% gadījumu jeb 25 040 inficētajām IP adresēm IPS, kas sadarbojas ar CERT.LV, ir informējuši savus gala lietotājus.



8.attēls - CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā no 2013.gada 1.oktobra līdz 31.decembrim pa infekciju tipiem (grafikā izmantota logaritmiskā skala).

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 503 inficētām IP adresēm. 10.attēlā ir redzams, cik inficētu valsts un pašvaldību institūciju IP adreses bijušas katras dienas saņemtajos ziņojumos no dažādiem ziņošanas avotiem.



10.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:

- 01.10. arī oktobrī turpinājās internetbanku lietotājus apdraudoša datorvīrusa izplatīšanās (tā saucamais „banku vīruss"). Vīruss pārstāvēja Zeus saimi un bija pielāgots vairāku Latvijā strādājošu banku klientiem.

  Kaitīgais saturs tika izplatīts ar mēstuļu starpniecību. Vīrusa faili lejuplādei tika izvietoti dažādos bezmaksas failu izvietošanas servisos (files.inbox.lv, dropbox.com, failiem.lv), kā arī uz uzlauztiem serveriem. Uzbrukuma teksta piemēri:

  From: Liene <liene.lapina@tesco.com>
  Subject: Re:fails

  Čau!
  Lūdzu steidzami apskaties failu un izsaki savas domas! Gaidīšu atbildi!
  http://files.inbox.lv/ticket/<unikāla_simbolu_virkne>/

  Liene

  vai

  FROM: janis.berzins@dell.com
  Subject: Re:dokuments

  Čau,
  Steidzami apskaties failu un dod ziņu! ...mums jārisina tā lieta steidzami!

http://files.inbox.lv/ticket/<unikāla_simbolu_virkne>/

Jānis

Informācija par šī incidenta risināšanu sniegta šīs atskaites tālākajos punktos.

- 02.10. Tika saņemta informācija par kādas valsts iestādes pārraudzībā esošās tīmekļa vietnes izķēmošanu. Izķēmošana tika novērsta un vietne tika atjaunota. Kompromitēšana bija iespējama, jo tīmekļa vietnes uzturēšanai tika izmantota novecojusi, neatjaunināta Joomla! satura vadības sistēma.

- 02.10. Notika uzbrukums atsevišķu valsts institūciju darbinieku e-pastu kontiem ar mērķi ievilināt lietotājus uzbrucēja sagatavotā tīmekļa vietnē un iegūt e-pastu paroles.

  Uzbrukums nebija vērtējams kā mērķēts kādai konkrētai iestādei. Incidentā iesaistīto valsts iestāžu atbildīgās personas reaģēja operatīvi un tika veiktas preventīvas darbības lietotāju pasargāšanai. Uzbrukuma teksts:

  "Jūsu pastkaste ir pārsniegusi krātuves robežu 2.GB

  Izveidota administrators pašlaik 2.30GB, nevar nosūtīt vai saņemt jaunas ziņas, kamēr jūs atkārtoti apstiprināt savu e-pastu

  Noklikšķiniet uz saites zemāk, lai apstiprinātu savu e-pastu
  http://e-pasts-service.webs.com/

  paldies
  sistēmas administrators"

- 04.10. Notika virkne datu un naudas līdzekļu izkrāpšanas mēģinājumu portālā draugiem.lv. Par notikumiem tika informēta arī Valsts policija.

- 07.10. CERT.LV publicēja pārskatu par „banku vīrusa" izplatīšanas kampaņu, izplatot informāciju par vīrusu un profilakses pasākumiem arī medijos un savā tīmekļa vietnē.

  Šajā uzbrukumu kampaņā uzbrucēji izmantoja lielu skaitu IT servisu un resursu gan Latvijā, gan ārvalstīs. Uzbrukums vērtējams kā rūpīgi gatavots. Ļaunatūras analīzes rezultāti liecināja, ka konkrētā uzbrukumu kampaņa visdrīzāk tika nopirkta kā serviss. Analīze pieejama cert.lv mājas lapā: https://cert.lv/resource/show/395

  Incidenta risināšanā CERT.LV sekmīgi sadarbojās ar vairākām bankām, inbox.lv, failiem.lv un dropbox.com pārstāvjiem, kā arī daudziem citiem, kuru resursi nesankcionēti izmantoti kā uzbrukuma sastāvdaļa.

  Informācija par kampaņu tika nodota policijai. Uzbrukumu kampaņa turpinājās līdz 23.oktobrim.
- 07.10. tika konstatēta ielaušanās Nodarbinātības valsts aģentūras tīmekļa vietnē www.nva.gov.lv. Hakeru uzbrukuma rezultātā tika nopludināti aptuveni 3000 portālā reģistrēto lietotāju dati (lietotājvārds, e-pasts, parole), kā arī portāla administratoru lietotājvārdi un paroles.

  Šim notikumam uzmanību pievērsa arī ārvalstu portāli un prese: http://news.softpedia.com/news/Anonymous-Hacker-Breaches-Systems-of-Latvia-s-State-Employment-Agency-388813.shtml?utm_source=twitterfeed&utm_medium=twitter&utm_campaign=information_security

  Uzbrukumā tika izmantoti starpniekserveri, lai nodrošinātu uzbrucēja identitātes slēpšanu. CERT.LV sniedza detalizētas rekomendācijas Nodarbinātības valsts aģentūrai, kā

uzlabot savu resursu drošību.

- 07.10. tika plaši izvērsta "policijas vīrusa" tīmekļa versijas pikšķerēšanas kampaņa. Vīrusa paraugs:

Kaitīgā satura piegādei tika izmantota apmeklētāja pārvirzīšanas funkcionalitāte, pielietojot javascript. Lietotāji uz pikšķerēšanas vietni tika novirzīti, izmantojot baneru servisus apšaubāmos portālos, kas piedāvā filmu skatīšanos tiešsaistē.

Veicot incidenta analīzi, CERT.LV atklāja, kā bez specifiskām tehniskām zināšanām novērst ļaundabīgā koda izraisītās sekas, atgūstot kontroli pār inficēto iekārtu. Lai arī veicamās darbības ļauj atsākt datora lietošanu, tās nav uzskatāmas par garantiju, ka dators ir drošs.

Analīzes procesā tika noskaidroti visi iespējamie domēnu vārdi, kurus uzbrucēji var izmantot. Sadarbībā ar ārvalstu kolēģiem un spamhaus.org projektu liela daļa kaitīgo domēnu tika atslēgti.

Par incidentu tika demonstrēts arī sižets TV3 raidījumā „Bez Tabu".

- 23.10. tika atklātas zemas prioritātes informācijas izgūšanas ievainojamības Swedbank mobilajā aplikācijā. Par konstatētajiem trūkumiem informāciju saņēma gan CERT.LV, gan Swedbank pārstāvji. Banka atklāto aplikācijas funkcionalitāti neuzskatīja par drošības risku. Novembrī, izmantojot konkrēto Swedbank mobilās aplikācijas ievainojamību, kiberuzbrukuma rezultātā tika izgūti vairāki tūkstoši Swedbank internetbankas lietotāju dati. Nekāds finansiāls kaitējums netika nodarīts.

- 25.10. CERT.LV identificēja publiski pieejamus kādas valsts iestādes datu bāzes failus, kas saturēja lietotāju e-pastus un citu sensitīvu informāciju, kurai nevajadzētu būt publiski

pieejamai. Par šo faktu tika informēta atbildīgā persona un konstatētie apdraudējumi tika novērsti 3 dienu laikā.

- Oktobrī un novembrī notika vairākas mērķētu uzbrukumu kampaņas valsts iestādēm. Uzbrucēji izsūtīja speciāli sagatavotus e-pastus, kuriem tika pievienots vīrusu saturošs arhīvs.

  Vairumā gadījumu iestādēs esošās aizsardzības sistēmas spēja identificēt ļaundabīgo failu e-pasta pielikumā un apturēt uzbrukumu pirms tas nonāca līdz lietotāja pasta kontam. Tas norāda, ka uzbrukums nav gatavots rūpīgi, un varētu būt kāda indivīda ļaunprātīgas aktivitātes, kas veiktas testēšanas nolūkos.

- 03.11. CERT.LV saņēma informāciju par kādas privātas kompānijas uzlauztu telefoncentrāli. Incidenta sekas – nesankcionēti veiktu zvanu rezultātā radīti zaudējumi gandrīz 80.00 LVL apmērā.

- 04.11. NATO mācību „Steadfast Jazz 2013" laikā notika virkne kiberuzbrukumu, kuru mērķis bija paust neapmierinātību ar NATO, ES, un to dalībvalstu politiku. Uzbrucēji sevi dēvēja par Anonymous Ukraine, taču uzbrucēju saistība ar šo valsti nav pierādāma.

  Uzbrukumu kampaņā tika kompromitēta un izķēmota kāda Latvijas medija tīmekļa vietne. Uzbrucēji uzlauztajās tīmekļa vietnēs atstāja paziņojumu NATO vārdā, tādejādi cenšoties diskreditēt gan pašu organizāciju, gan tobrīd notiekošās mācības „Steadfast Jazz 2013".

  Kampaņas ietvaros tika izsūtītas arī dezinformējošas e-pasta vēstules NATO Cooperative Cyber Defence Centre of Excellence vārdā virknei valsts iestāžu, kā arī veikti vairāki nesekmīgi uzbrukumu mēģinājumi valsts iestāžu mājas lapām.

  CERT.LV incidenta risināšanu koordinēja ar kolēģiem Lietuvā un Igaunijā. Tika konstatēts, ka uzbrukumi veikti no vairākām IP adresēm Krievijā, taču tas vēl nav uzskatāms par pamatu secinājumam, ka uzbrukumu organizatori atrodas tieši Krievijā. CERT.LV no Krievijas CERT vienībām atbildes nav saņēmis.

- 08.11. CERT.LV konstatēja sensitīvu datu pieejamību no kāda interneta pakalpojumu sniedzēja pārvaldībā esošas IP adreses. Incidenta informācija tika nodota attiecīgā uzņēmuma atbildīgajai personai. CERT.LV saņēma no minētā uzņēmuma papildu tehnisko informāciju un paskaidrojumu, ka 2013.gada 9.novembrī incidents novērsts un sensitīvās informācijas

publiska pieejamība skaidrojama ar cilvēka izdarītu kļūdu rezerves kopēšanas serveros.

- 10.11. tika konstatēta lietotāju datu pikšķerēšanas kampaņa, kas vērsta pret kādu Latvijā strādājošu banku. Iesaistīto resursu turētāji tika brīdināti, kaitīgās lapas slēgtas.

- 14.11. konstatēts mēģinājums iesūtīt datorvīrusu kāda interneta pakalpojumu sniedzēja uzņēmuma darbinieka datorā. Kaitīgo kodu neatpazina antivīrusu programma, bet infekcija tika novērsta, pateicoties darbinieka piesardzībai attiecībā uz nezināmu e-pasta pielikumu atvēršanu.

- 29.11. kādas tīmekļa vietnes esošā attēlā konstatētas kibernoziedznieku pievienotas kaitīga koda rindas. Servera īpašnieks brīdināts, fails iztīrīts.

- 29.11. CERT.LV sniedza konsultāciju kādas valsts iestādes atbildīgajai personai par tīkla noslodzes datu saglabāšanu un labo praksi žurnālfailu uzturēšanā.

- 04.12. tika identificēts IT uzbrukums kādas ministrijas darbiniekiem. Darbinieki saņēma e-pasta vēstules ar kaitīgiem pielikumiem. Atbildīgā persona ministrijā reaģēja nekavējoties.

- 06.12. konstatēta jauna pikšķerēšanas kampaņa pret Latvijā strādājošas bankas klientiem. Kaitīgie resursi tika iztīrīti vai slēgti.

- 06.12. tika konstatēta jauna Citadel saimes datorvīrusa izplatīšanas kampaņa, kas domāta atsevišķu Latvijā strādājošu banku pieejas datu zādzībai. Konkrētais datorvīruss zināms arī kā „nodokļu vīruss" vai „VID vīruss", jo krāpnieciskajās vēstulēs tika izmantoti sociālās inženierijas paņēmieni ar atsauci uz Valsts ieņēmumu dienestu (VID). Uzbrukuma teksts:

  Subject: Sudziba nodoklu dienestam

  Labdien! Informacija par sudzibu nosutita nodoklu dienestam, nosutu Jums kopiju, skatit pielikuma. Ref id: 1494et4b95

  1 attachment: nodokludienestam.doc.zip

- 10.12. CERT.LV sazinājās ar IT drošības kompāniju FireEye, lai pārbaudītu "New York Times" (NYT) izskanējušo apgalvojums par Ķīnas hakeru ielaušanos Latvijas Ārlietu ministrijas datorsistēmā (http://www.nytimes.com/2013/12/10/world/asia/china-is-tied-to-spying-on-european-diplomats.html?_r=1&), jo, veicot Latvijas Republikas Ārlietu ministrijas tīkla pieslēgumu vēsturisko analīzi, sekmīgas ielaušanās un kompromitētu iekārtu pazīmes konstatētas netika. FireEye pētnieki, kas strādāja pie "Ke3Chang" uzbrukumu kampaņas izmeklēšanas, apstiprināja, ka Latvija kampaņā netika iesaistīta un Latvijas pieminēšana NYT rakstā bijusi nepamatota.

- 11.12. tika konstatēts DDoS uzbrukums uz nsz.nic.lv ar apjomu līdz 500 Mb sekundē. Notiekošais bija *Distributed Reflection* CHARGEN uzbrukums, visi iesaistītie avoti bija reāli un atbildēja uz CHARGEN.

- 16.12 CERT.LV sniedza konsultāciju kādas valsts iestādes e-pasta serveru izņemšanai no Microsoft.Live blacklist.

- 18.12. notika DDoS uzbrukums Community DNS serverim. Uzbrukuma apjoms sasniedza līdz 500 Mb sekundē.

- Gadu mijā tika novēroti vairāki DDoS uzbrukumi bankām Latvijā, Igaunijā un Zviedrijā, kas, iespējams, bija saistīti ar eiro ieviešanu.

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

CERT.LV uzskaita arī uzlauzto un izķēmoto tīmekļa vietņu gadījumus. Šādu gadījumu skaits oktobrī bija 39, novembrī – 72, decembrī – 8. Izķēmoto lapu sadalījums pa serveru operētājsistēmām: oktobrī - 15 GNU/Linux, 23 MS Windows 2003, 1 FreeBSD, novembrī - 48 GNU/Linux, 24 MS Windows 2003, decembrī – 7 GNU/Linux, 1 MS Windows 2008.

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

CERT.LV uztur tīmekļa vietni https://www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. Pārskata periodā vispopulārākā bija lapa ar CERT.LV sagatavoto informāciju par „Policijas vīrusa" apkarošanas praksi un mehānismiem (26701 skatījumi), bet otrajā vietā ierindojās lapa par jaunākajiem vīrusiem un apdraudējumiem (16320 skatījumi). Kopā CERT.LV mājas lapai bijuši 43 908 apmeklējumi, kurus veido 32 980 unikāli apmeklētāji no 84 valstīm. Tāpat kā iepriekšējos pārskata periodos, arī šajā periodā lielākā daļa – 92,65% apmeklētāju - bija no Latvijas.

CERT.LV tīmekļa vietnē pārskata periodā publicētas 23 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 3.ceturksni.

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 57 ziņas, kontam pievienojušies 75 jauni sekotāji un 79 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 18 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 4 jauni raksti, kā arī papildināts raksts par „policijas izspiedējvīrusu", portālu apmeklējuši 24 140 (18 838 unikāli) apmeklētāji. Publicētie raksti:

- "VID vīruss" – kā to atpazīt un iztīrīt.
- Informācija glabāšana un sinhronizācija bezmaksas krātuvē mākonī.
- Windows 8 – izmaiņas un drošības jautājumi.
- Banku vīruss – kā no tā atbrīvoties.

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

1) Intervijas un ziņas radio:

- 01.10. – saruna par Datorologa akciju un Eiropas Kiberdrošības mēnesi Latvijas radio

raidījumā „Kā labāk dzīvot”.

- 02.10. – saruna par kiberdrošību un Eiropas Kiberdrošības mēnesi Latvijas radio raidījumā „Aktuālais temats”.
- 10.10. – sniegts komentārs RadioTev par “banku vīrusu”.
- 23.10. – saruna par kiberdrošību 1. Biznesa radio.
- 07.11. – saruna par krāpšanu internetā un “nigēriešu” mēstulēm Latvijas radio 4 raidījumā “Doma laukums”.
- 07.11. – saruna par kiberuzbrukumiem NATO mācību „Steadfast Jazz 2013” laikā Latvijas radio raidījumā “Aktuālais temats”.
- 12.11. – diskusija par azartspēļu ierobežošanas iespējām internetā Latvijas radio raidījumā “Krustpunkti”.
- 12.11. – komentārs par viedtālruņu drošību Latvijas radio raidījumā “Kā labāk dzīvot”.
- 10.12. – komentārs par “VID vīrusu” Latvijas radio 4 ziņās.
- 12.12. – komentārs Latvijas radio par „mākoņpakalpojumu” drošību.

2) Sižeti televīzijā, tiešraides:

- 02.10. – sižets LNT ziņās par Eiropas Kiberdrošības mēnesi ievadošo Datorologa akciju.
- 09.10. – sniegts komentārs LTV raidījumam „Panorāma” par “banku vīrusu”.
- 14.10. – sniegts komentārs par kiberdrošību RīgaTV raidījumā “Notikumi un viedokļi”.
- 24.10. – sižets TV3 raidījumā „Bez Tabu” par „policijas vīrusu”.
- 09.12. – sniegts komentārs par “VID vīrusu” LNT ziņās.
- 09.12. – sniegts komentārs par “VID vīrusu” Latvijas televīzijas ziņām krievu valodā.

3) Ziņas portālos:

- 07.10. - Izplatās bīstams vīruss, kas apdraud internetbanku lietotājus, brīdina CERT.LV – raksts Delfi.lv
- 09.10. - Atmasko bīstamo vīrusu, kas apdraud internetbanku lietotājus – raksts Apollo.lv
- 09.10. - Nezināmi hakeri uzlauzuši NVA mājas lapu; 'nosūknēti' ap 3000 lietotāju dati – raksts Delfi.lv
- 15.10. - В Латвии обнаружен новый компьютерный вирус – raksts Ves.lv
- 24.10. - Pieaug IT drošības riski un kibernoziedznieku uzbrukumu draudi – raksts TVnet
- 11.11. - Noskaidrots, kas NATO mācību laikā Latvijā veicis kiberuzbrukumus – raksts Apollo.lv
- 11.11. - Hakeru uzbrukumu NATO mācību laikā organizējusi grupa "Anonymous Ukraine" – raksts Puaro.lv
- 11.11. - Latvija Steadfast Jazz laikā atvairījusi kiberuzbrukumus no vairākām IP adresēm 10 valstīs – raksts Diena.lv
- 11.11. - Zināms, kas organizējis hakeru uzbrukumu NATO mācību laikā – raksts TVnet
- 11.11. - Hakeru uzbrukumu NATO mācību laikā organizējusi grupa, kas sevi dēvē par "Anonymous Ukraine" – raksts Focus.lv
- 14.11. - Aktivizējušies krāpnieki pa telefonu. Esiet uzmanīgi! – raksts TVnet
- 10.12. - Latvijā masveidā izplatās datorvīruss: kā atpazīt, ka jūsu dators ir inficēts? – raksts Apollo.lv
- 10.12. - Par bīstamā VID datorvīrusa upuriem jau kļuvuši simtiem datorlietotāju – raksts Delfi.lv
- 13.12. - Datorvīruss pārtver internetbanku maksājumus, inficē ap 1000 datoru – raksts TVnet
- 13.12. - Jāuzmanās: Bankas datu zagšanas vīruss turpina izplatīties – raksts Apollo.lv

23.oktobrī CERT.LV pārstāvis piedalījās arī Microsoft organizētā mediju pasākumā, kas notika Eiropas Kiberdrošības mēneša ietvaros un kurā tika diskutēts par IT drošības riskiem, kibernoziedznieku uzbrukumu mērķiem un izmantotajām metodēm..

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

Pārskata periods uzsākās ar oktobra kā Eiropas Kiberdrošības mēneša aktivitātēm. 2013.gada 2.oktobrī CERT.LV telpās norisinājās Datorologa akcija, kas sniedza iespēju ikvienam interesentam pārbaudīt sava datora "veselību" pie datorologa – CERT.LV speciālista, kurš gan veic datoru pārbaudi un, ja nepieciešams, arī "ārstēšanu", gan atbild uz jautājumiem par drošu datora un interneta lietošanu. Šī Datorologa akcija bija īpaša ne tikai ar to, ka ievadīja šī gada Kiberdrošības mēneša aktivitātes Latvijā, bet arī ar to, ka šajā akcijā pirmo reizi iesaistījās un CERT.LV datorologiem talkā nāca arī atbildīga interneta pakalpojumu sniedzēja memorandu parakstījušā un kvalitātes zīmi ieguvušā *Lattelecom* eksperti, gūstot vērtīgu pieredzi tiešā saskarē ar gala lietotājiem un popularizējot IT drošības ideju sabiedrībā. Akcija norisinājās vienas dienas garumā, un tās laikā datorologi veica 67 datoru pārbaudi un "ārstēšanu".

Eiropas Kiberdrošības mēneša ietvaros 23.oktobrī notika ISACA Latvijas nodaļas un CERT.LV organizētā IT drošības konference "Mūsu informācijas drošība - nākotnes panākumu atslēga". Konferencē ar prezentācijām uzstājās gan Latvijas, gan ārvalstu IT drošības eksperti. To apmeklēja gandrīz 400 dalībnieki. Tiem, kuri kāda iemesla dēļ nevarēja apmeklēt konferenci klātienē, tika dota iespēja vērot to tiešraidē internetā.

Dienu pēc konferences, 24.oktobrī, notika CERT.LV organizētais seminārs IT drošības speciālistiem par sociālo tīklu izmantošanu mērķētu uzbrukumu veikšanai, kuru vadīja vieslektori no ENISA (European Network and Information Security Agency).

Kiberdrošības mēneša ietvaros CERT.LV speciālisti apmeklēja arī vairākas skolas un iepazīstināja skolēnus ar IT drošības pamatprincipiem, kas jāievēro, lietojot datorus un viedtālruņus gan komunikācijai sociālajos tīklos, gan veicot citas darbības internetā.

Kiberdrošības mēneša aktivitāšu popularitāte liecina par IT drošības jautājuma aktualitāti, nepieciešamību veikt skaidrojošo darbu un popularizēt IT drošības principus plašākā sabiedrībā, kā arī sniegt iespēju padziļināt specifiskas zināšanas IT drošības speciālistiem un interesentiem.

Pārskata periodu noslēdza CERT.LV organizēts seminārs "Esi drošs-2", kurā dalībnieki tika iepazīstināti ar IT drošības aktualitātēm Latvijā, sīkdatņu izmantošanas un privātās informācijas aizsardzības principiem, atvērto datu būtību, dažādiem ārpakalpojumu izmantošanas aspektiem un citiem aktuāliem tematiem gan CERT.LV speciālistu, gan vieslektoru prezentācijās.

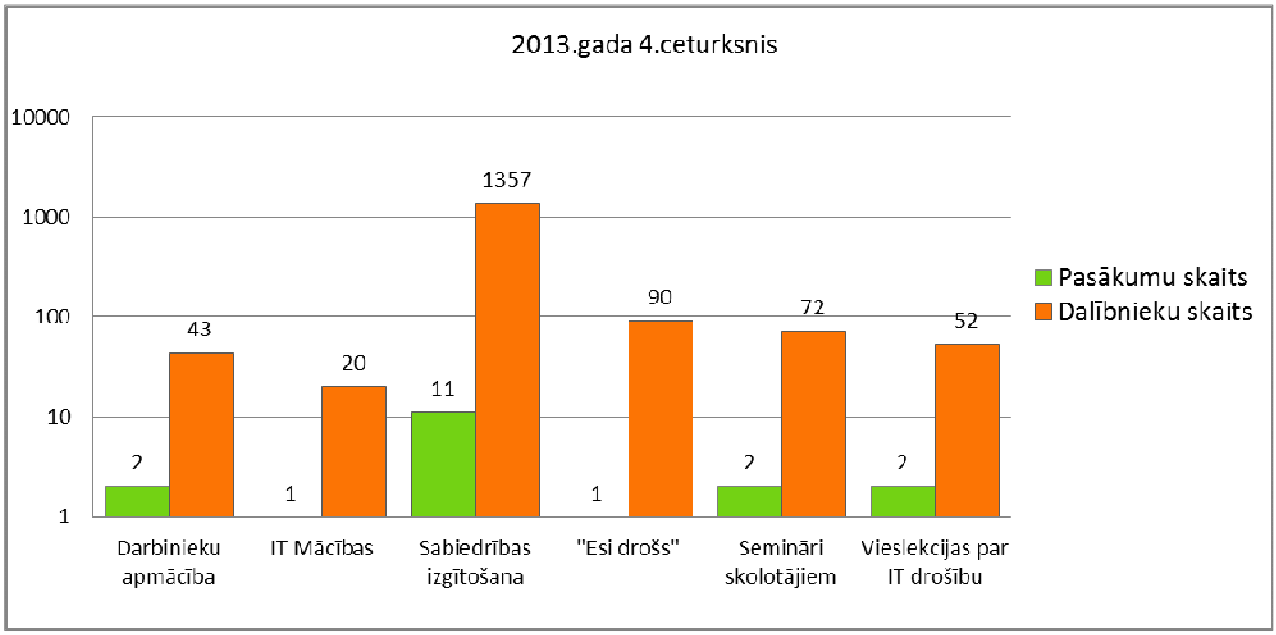
Pārskats par CERT.LV pasākumiem pārskata periodā:

- 01.10. CERT.LV pārstāvis sniedza prezentāciju Jaunsardzes instruktoriem, lai tie varētu efektīvāk izglītot jaunsargus par IT drošības jautājumiem.
- 02.10. CERT.LV telpās norisinājās Datorologa akcija, kas aizsāka šī gada Eiropas Kiberdrošības mēneša aktivitātes Latvijā un sniedza iespēju visiem interesentiem pārbaudīt savu datoru un saņemt speciālistu konsultācijas par drošu datora un interneta lietošanu.
- 23.10. notika ISACA Latvijas nodaļas un CERT.LV rīkotā IT drošības konference "Mūsu informācijas drošība - nākotnes panākumu atslēga".
- 24.10. notika CERT.LV organizētais seminārs par sociālo tīklu izmantošanu mērķētiem uzbrukumiem, kuru vadīja vieslektori no ENISA.
- 30.10. CERT.LV pārstāvis nolasīja lekciju LU Sociālo zinātņu fakultātes studentiem par IT drošību.
- Oktobrī, Eiropas Kiberdrošības mēneša ietvaros, CERT.LV pārstāvji vairākkārt viesojās

skolās un stāstīja skolēniem par drošu datoru, viedtālruņu un interneta lietošanu.

- 04.11. CERT.LV pārstāvji nolasīja lekciju LU Datorikas fakultātes studentiem par IT drošību.
- 04.11. CERT.LV pārstāvis piedalījās CVK organizētajā seminārā un sniedza prezentāciju par IT drošības jautājumiem.
- 07.11. CERT.LV pārstāvji sniedza prezentāciju par pašreizējo situāciju, sasniegumiem un izaicinājumiem IT drošības sfērā Latvijā, kā arī piedalījās paneļdiskusijā par servisa atteices uzbrukumiem un to novēršanu DSS organizētā IT drošības konferencē „IT Security matters and alone is not enough".
- 14.11. CERT.LV pārstāvis sniedza prezentāciju IKT nozares pedagogu un prakses vadītāju praktiskajā seminārā.
- 14.11. CERT.LV pārstāvis sniedza prezentāciju Priekuļu tehnikuma audzēkņiem par prasmi sevi pasargāt digitālajā laikmetā.
- 22.-23.11. Riga COMM 2013 ietvaros notika Datorologa akcija.
- 03.12. Kara muzeja telpās notika CERT.LV organizētais seminārs valsts un pašvaldību iestāžu par IT drošību atbildīgajiem un citiem interesentiem "Esi drošs-2".
- 09. un 11.12. CERT.LV pārstāvji vadīja informācijas drošības seminārus Valsts kontroles darbiniekiem.

Pārskata periodā CERT.LV piedalījās 19 pasākumos, kuros par IT drošības jautājumiem informēja un izglītoja 1634 dalībniekus.



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

5. Sniegt atbalstu valsts institūcijām valsts drošības sargāšanā, kā arī noziedzīgu nodarījumu un citu likumpārkāpumu atklāšanā (izmeklēšanā) informācijas tehnoloģiju jomā, ievērojot normatīvajos aktos noteiktos datu apstrādes ierobežojumus.

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

- 04.10. CERT.LV tikās ar Aizsardzības ministrijas valsts sekretāru J.Sārtu.
- Oktobrī CERT.LV tikās ar Aizsardzības ministriju un VARAM, lai piedalītos diskusijā par

kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un paaugstinātas drošības kvalificētu personas elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību.
- Oktobrī CERT.LV piedalījās Elektronisko sakaru likuma izmaiņu apspriešanā saistībā ar IP adrešu bloķēšanu.
- 15.11. CERT.LV piedalījās IT drošības padomes sanāksmē.
- 21.11. notika sadarbības tikšanās ar Valsts kontroli.
- 22.11. notika tikšanās ar Aizsardzības ministrijas valsts sekretāru J.Sārtu un nevalstiskajām organizācijām par IT drošības stratēģiju.
- 02.12. notika vairākas tikšanās ar kritiskās infrastruktūras iestādēm.

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 31.decembrim CERT.LV apkopoja informāciju par 610 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 31.decembrim rīcības plānus 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:

- 9.-10.10. CERT.LV pārstāvis piedalījās telekomunikāciju un IT drošības konferencē „Secure 2013", kas notika Varšavā, Polijā.
- 21.-25.10. CERT.LV pārstāvis piedalījās NATO CCDCoE organizētajos kursos „Cyber Defence Monitoringc & Security Events Management Course" Tallinā, Igaunijā.
- 05.11. Rīgā notika sadarbības tikšanās ar Ungārijas CERT pārstāvjiem.
- 25.-29.11. CERT.LV kopā ar Latvijas Nacionālo bruņoto spēku pārstāvjiem piedalījās NATO organizētās IT drošības mācībās „Cyber Coalition 2013", kas tika koordinētas no Tartu, Igaunijā.
- 27.-30.11. CERT.LV pārstāvis piedalījās TERENA un ENISA organizētajos „TRANSITS I" kursos Prāgā, Čehijā.
- 02.-05.12. CERT.LV pārstāvis piedalījās IT drošības mācību „Baltic Ghost III" plānošanas sanāksmē, kas notika Viļņā, Lietuvā.
- 09.-13.12. CERT.LV pārstāvji piedalījās „Certified Ethical Hacker" (CEH v8) kursos.

8. Veikt citus normatīvajos aktos noteiktos pienākumus.

- Pārskata periodā notikušas trīs DEG grupas sanāksmes.
- 05.11. CERT.LV pārstāvis piedalījās Lattelecom organizētās akcijas „Pieslēdzies, Latvija!" noslēguma pasākumā.
- 07.11. notika sadarbības tikšanās ar LATA pārstāvjiem.
- 21.11. sadarbības tikšanās ar LU Datorikas fakultātes pārstāvjiem par IT drošībai veltīta specsemināra plānošanu.
- Novembrī CERT.LV pārstāvis piedalījās NetSafe Latvia Drošāka interneta centra rīkotā konkursa bērniem un jauniešiem par labāko saturu internetā žūrijas komisijā, piešķirot arī specbalvas tiem, kas savos projektos pievērsa papildu uzmanību tieši IT drošības jautājumiem.
- 05.12. CERT.LV pārstāvis piedalījās LIKTA gadskārtējā konferencē.
- 06.12. notika NetSafe rīkotā konkursa bērniem uzvarētāju apbalvošanas ceremonija.
- 28.12. notika sadarbības tikšanās ar SIA Latnet Serviss.

Sagatavotājs – Baiba Kaškina
tālrunis 67085858
e-pasts baiba.kaskina@cert.lv