Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

LATVIJAS REPUBLIKAS
AIZSARDZĪBAS MINISTRIJA

Publiskais pārskats par CERT.LV uzdevumu izpildi

2014

2014. gada 3. ceturksnis (01.07.2014. – 30.09.2014.)

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

Saturs

Kopsavilkums

Pārskata periodā notika vairāki drošības incidenti, kas skāra Latvijas interneta lietotājus un servisa uzturētājus. Viens no svarīgākajiem incidentiem bija e-pasta datu izkrāpšanas kampaņa ar mēstuļu palīdzību. Uzbrukumu mērķis bija izkrāpt e-pasta lietotāju datus, uzdodoties par pakalpojumu sniedzēju, piemēram, „LATNET serviss" vai latvija.lv. Mēstules saņēma vairāki tūkstoši interneta lietotāji, tostarp arī valsts un pašvaldību iestādēs strādājošie. CERT.LV aicināja interneta lietotājus rūpīgi izvērtēt e-pasta saturu un to pielikumus, lai nekļūtu par krāpnieku upuriem.

Septembra beigās kļuva zināms par Linux un OS X operētājsistēmās atrodamu BASH ievainojamību, kas atsevišķos gadījumos ļauj uzbrucējam attālināti izpildīt patvaļīgu kodu. Ievainojamībai tika pakļauta arī daļa Latvijas WEB serveru. Ievainojamība uzbrucējam ļauj izpildīt papildu komandas, līdzīgi kā tas notiek SQL injekcijas gadījumā. Šobrīd lielākā daļa programmatūras izstrādātāju ir izlaiduši drošības atjauninājumus, kas ievainojamību novērš.

Pārskata periodā CERT.LV reģistrēja un apstrādāja 651 augstas prioritātes incidentu. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 736 augstas prioritātes incidenti, bet 2013.gada 3.ceturksnī 1672 augstas prioritātes incidenti.

Salīdzinot augstas prioritātes incidentus ar to pašu periodu pirms gada, vērojams izteikts samazinājums, jo kopš 2014.gada sākuma incidentu apstrāde notiek automatizēti un daļa incidentu, kas tajā pašā periodā pirms gada tika klasificēti kā augstas prioritātes incidenti, šogad tiek klasificēti kā zemas prioritātes incidenti, jo neprasa papildus manuālu apstrādi.

2014.gada 3.ceturksnī CERT.LV reģistrēja 157 293 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti 102 596 zemas prioritātes incidenti, bet 2013.gada 3.ceturksnī – 46 040 zemas prioritātes incidenti. Salīdzinot zemas prioritātes incidentus ar to pašu periodu pirms gada, vērojams pieaugums, kas saistīts ar sadarbības partneru skaita palielināšanos, kas ziņo par incidentiem un CERT.LV darbību automatizāciju.

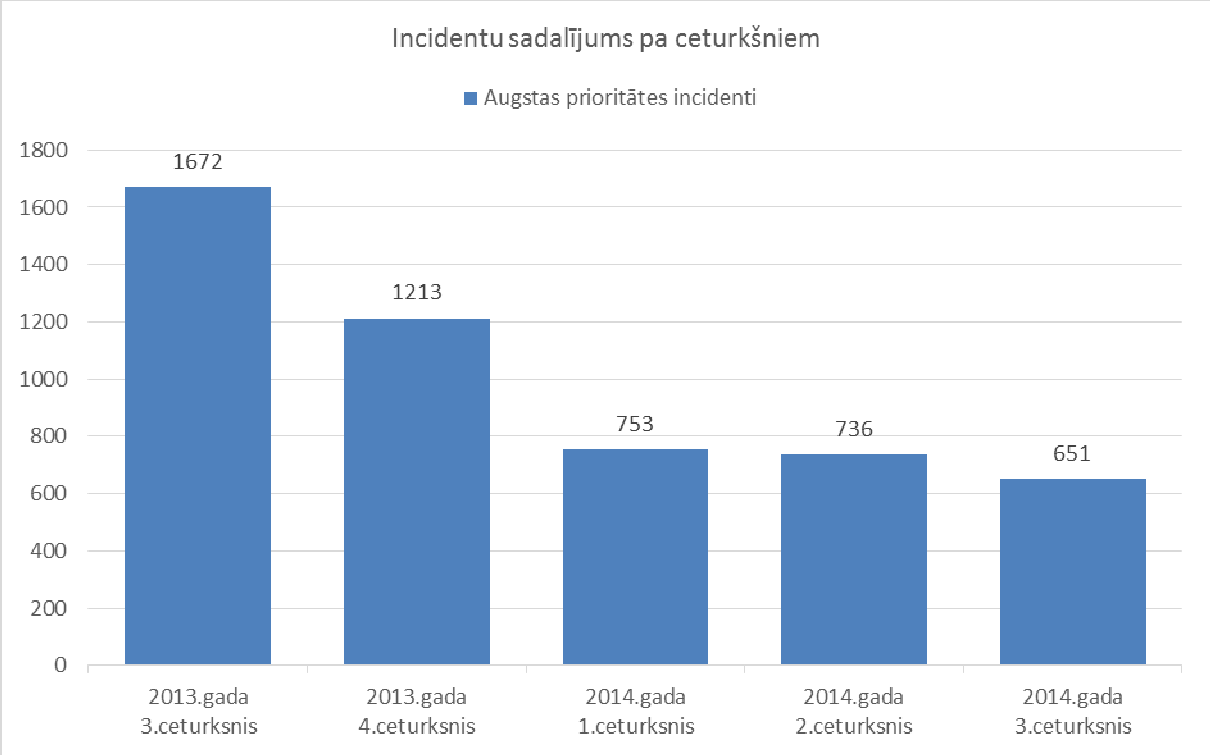
Lielāko sabiedrības un mediju uzmanību pārskata periodā izpelnījās e-pasta datu izkrāpšanas kampaņa ar mēstuļu palīdzību, izmantojot portāla latvija.lv nosaukumu.

Kopā pārskata periodā CERT.LV piedalījās 10 pasākumos, apmācot 324 cilvēkus, publicēja 4 jaunus rakstus portālā www.esidross.lv, 20 jaunas ziņas portālā www.cert.lv, piedalījās 3 radio pārraidēs un 3 televīzijas sižetos.

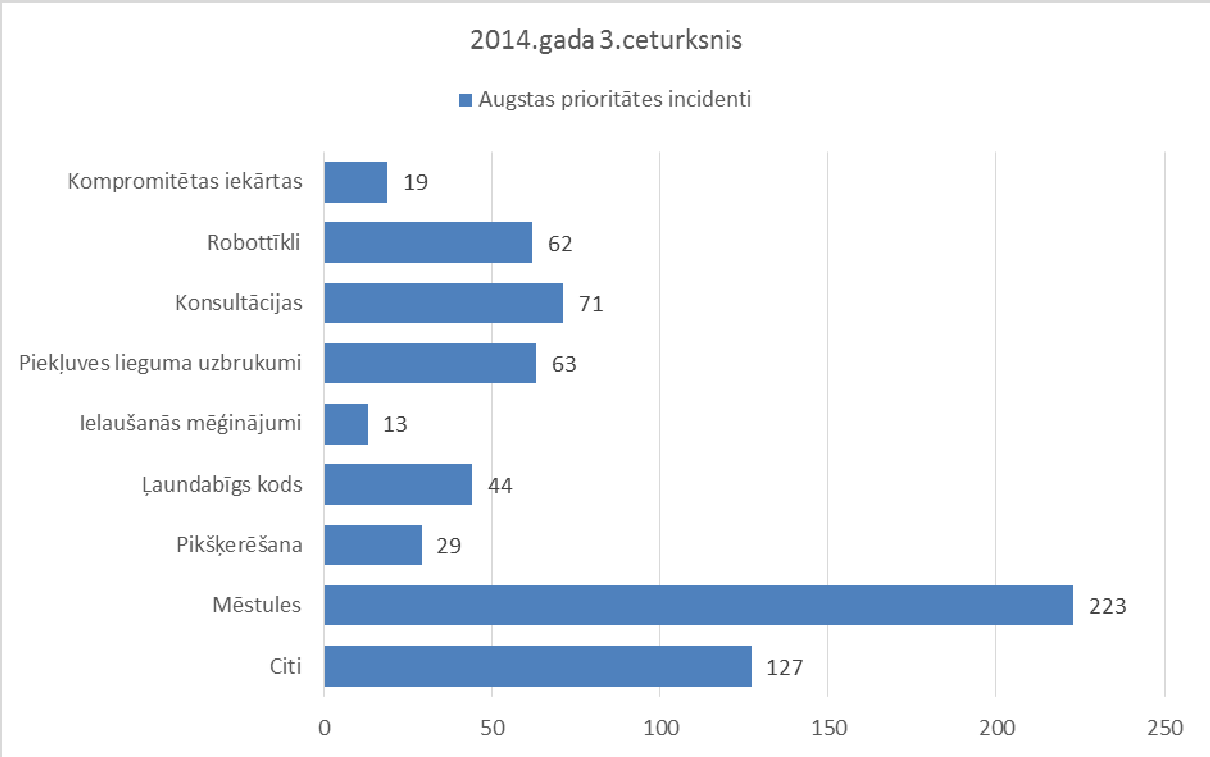
1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

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

2014.gada trešajā ceturksnī CERT.LV apstrādāja 651 augstas prioritātes incidentus, kas ir par 85 incidentiem mazāk nekā 2014.gada otrajā ceturksnī un par 1021 incidentiem mazāk nekā 2013.gada 3.ceturksnī.

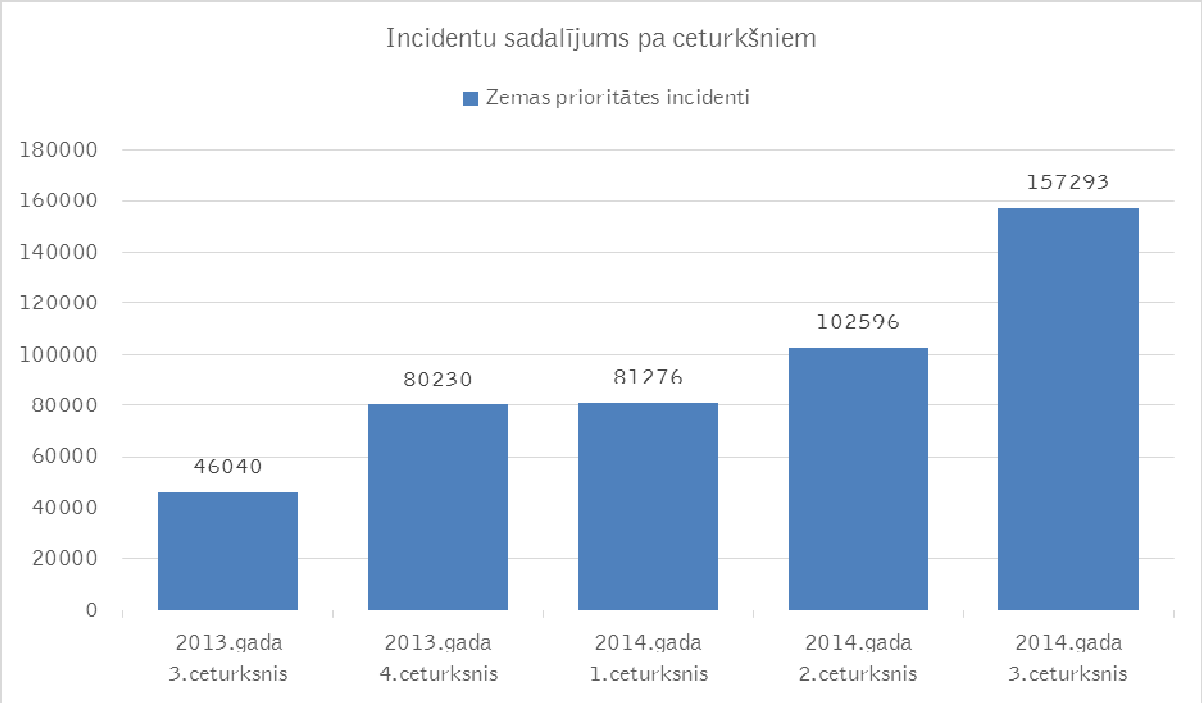


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2013. un 2014. gadā.



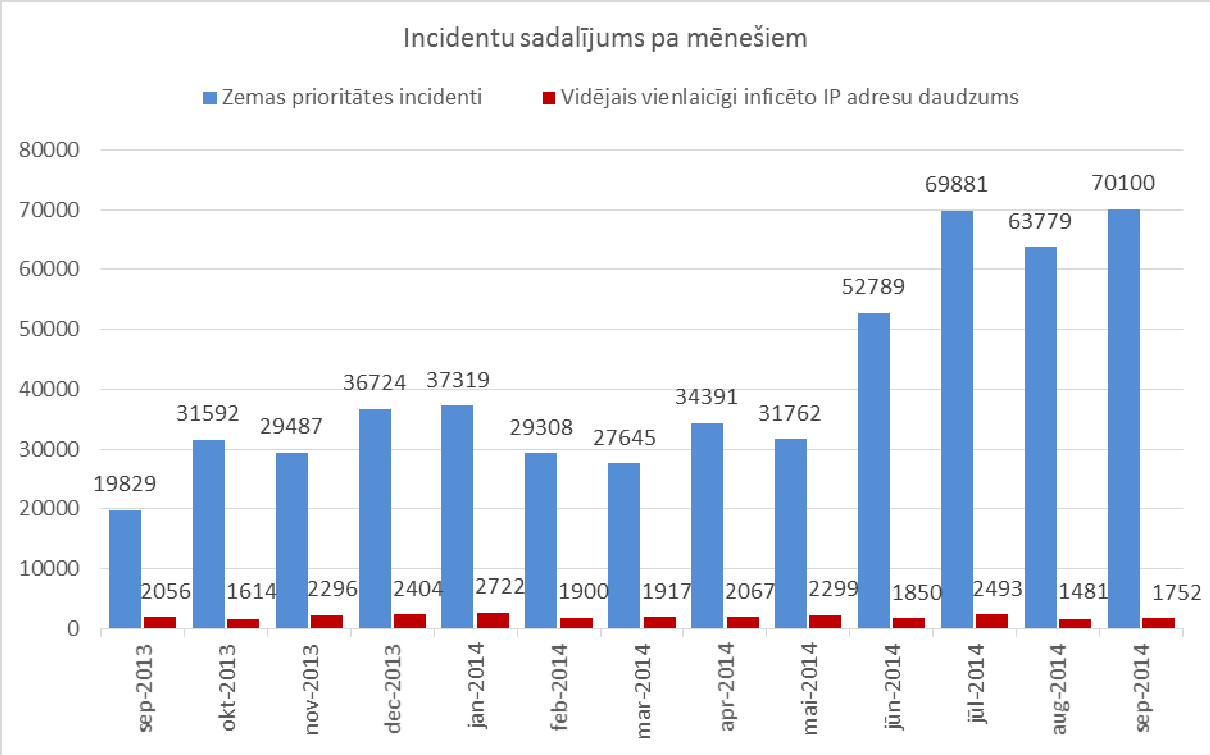
2.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem laika periodā no 2014.gada 1.jūlija līdz 30.septembrim.

2014.gada 3.ceturksnī CERT.LV reģistrēja 157 293 zemas prioritātes incidentus, kas ir par 54699 vairāk nekā 2014. gada 2. ceturksnī un par 111253 incidentiem vairāk, nekā 2013.gada 3.ceturksnī.



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

Salīdzinot ar 2014.gada 2. ceturksni, reģistrēto zemas prioritātes incidentu apjoms 2014.gada 3.ceturksnī ir pieaudzis, jo turpināja palielināties sadarbības partneru skaits, kas ziņo par incidentiem, kā arī turpinājās CERT.LV darbības automatizēšana.



4.attēls – Zemas prioritātes incidentu skaits mēnesī un vidējais vienlaicīgi inficēto IP adrešu daudzums.

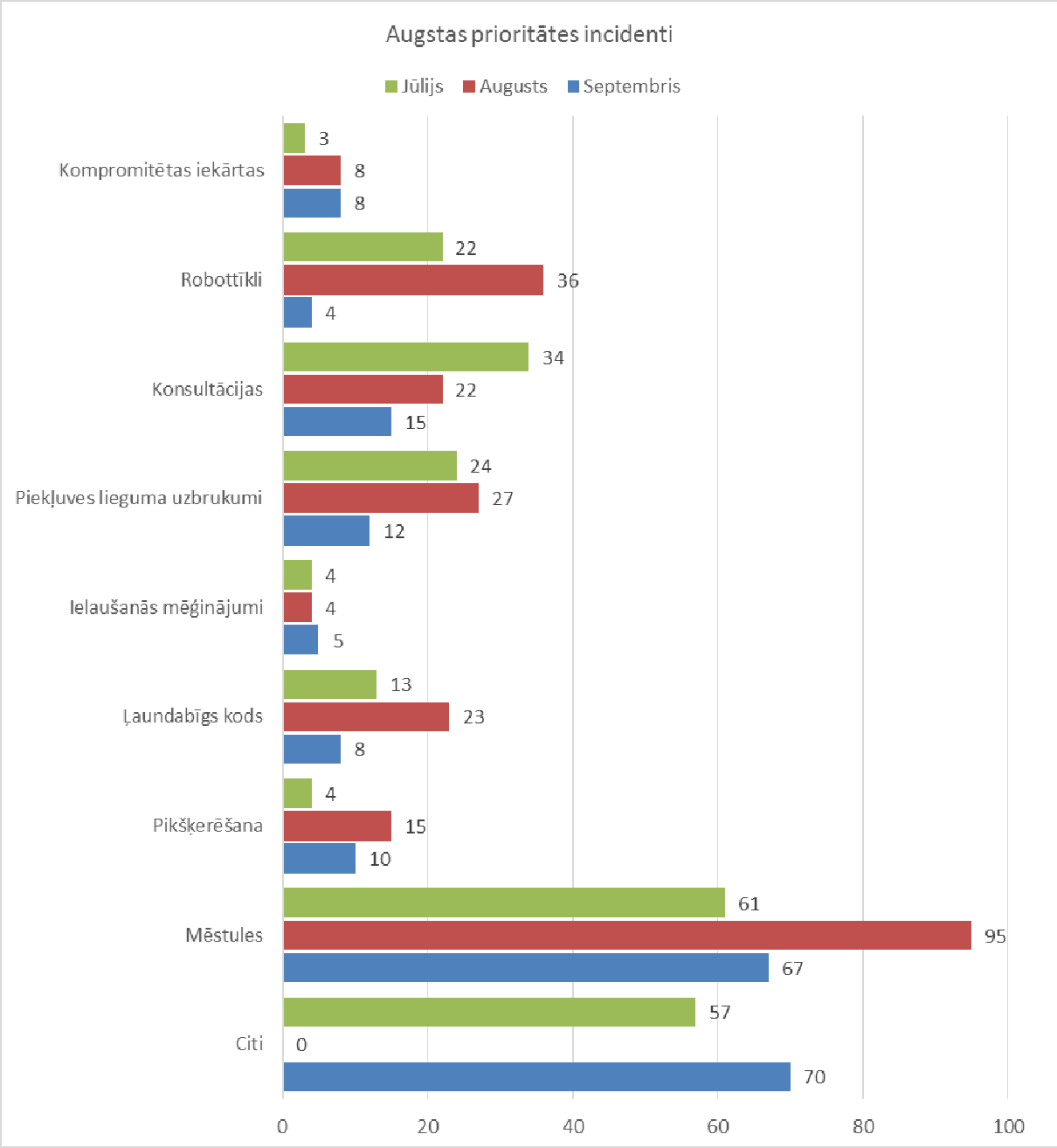
Zemas prioritātes incidentu skaits turpināja pieaugt attiecībā pret vidējo inficēto IP adrešu daudzumu.
No 2014.gada 1.jūlija tika apstrādāti dati no papildu sensoriem, reģistrēto notikumu skaits jūlijā ir dubultojies. Dēļ papildus sensoriem tika ieviesta jauna apdraudējumu kategorija – konfigurācijas kļūda. Jūlijā tādēļ par 10 reizēm palielinājies zemas prioritātes incidentu skaits attiecībā pret iepriekšējiem mēnešiem.

Katru mēnesi CERT.LV rēķina arī vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Jūlijā šis skaits bija 2493, augustā – 1481, savukārt septembrī – 1752 inficētas IP adreses.

CERT.LV apkopo informāciju par interneta pakalpojumu sniedzējiem (turpmāk – IPS) un to izmantotajām autonomajām sistēmām. Lai samazinātu kopējo inficēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar IPS, kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". Pārskata perioda beigās atbildīgo IPS kopskaits saglabājās bez izmaiņām – 13.

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

Pārskata periodā CERT.LV ir reģistrējis un apstrādājis 651 augstas prioritātes incidentu. Augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem redzams 5.attēlā.

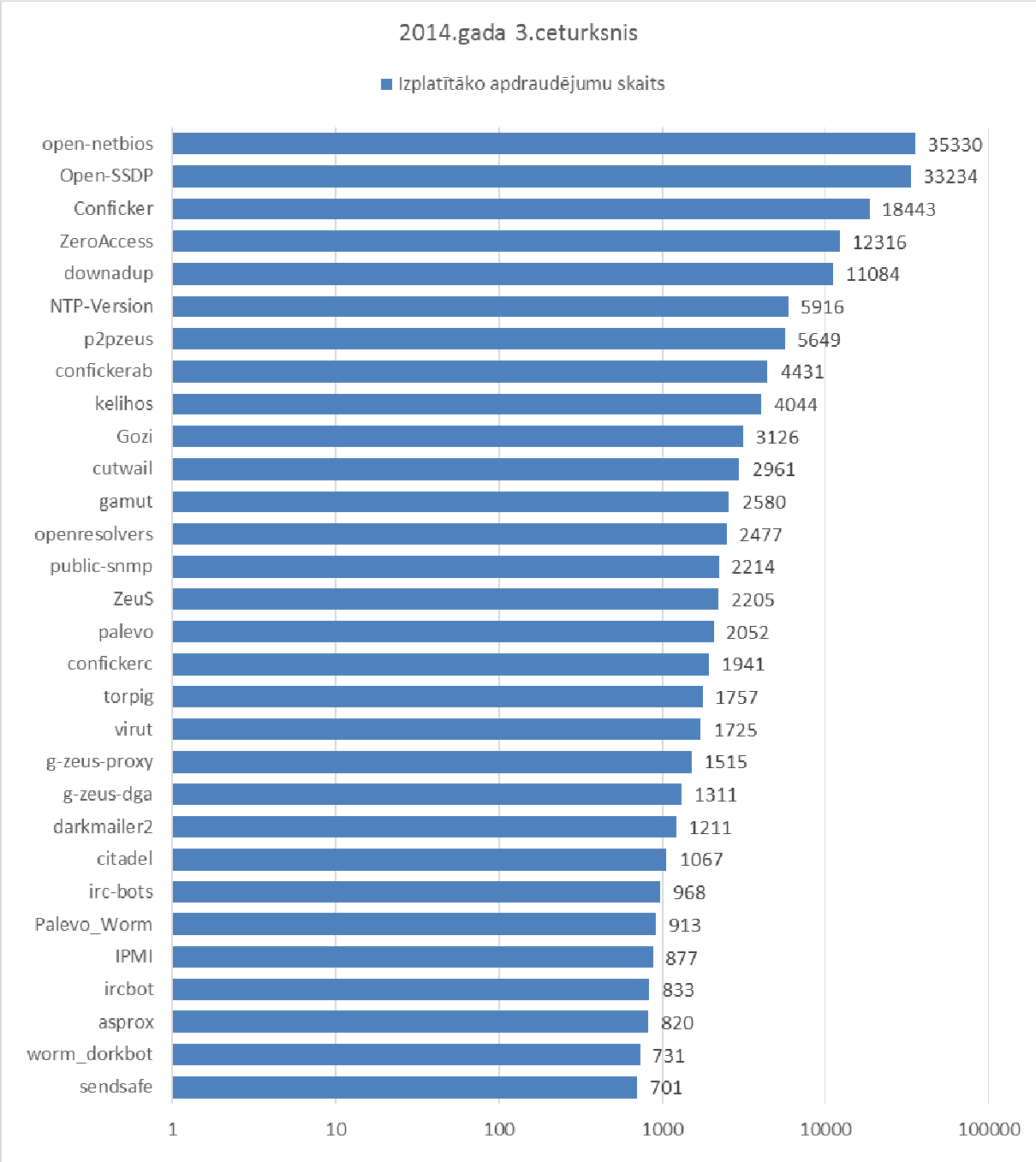


5.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem un pa mēnešiem 2014.gada 3.ceturksnī.

Attiecībā pret iepriekšējo periodu ir pieaudzis CERT.LV sniegto konsultāciju skaits. Izplatīti ir zvani no klientiem, kuri saņēmuši vēstuli no sava interneta pakalpojumu sniedzēja, kurā tiek informēts, ka dators ir inficēts. Tādos gadījumos CERT.LV sniedz konsultācijas, kā novērst

vīrusa infekcijas.

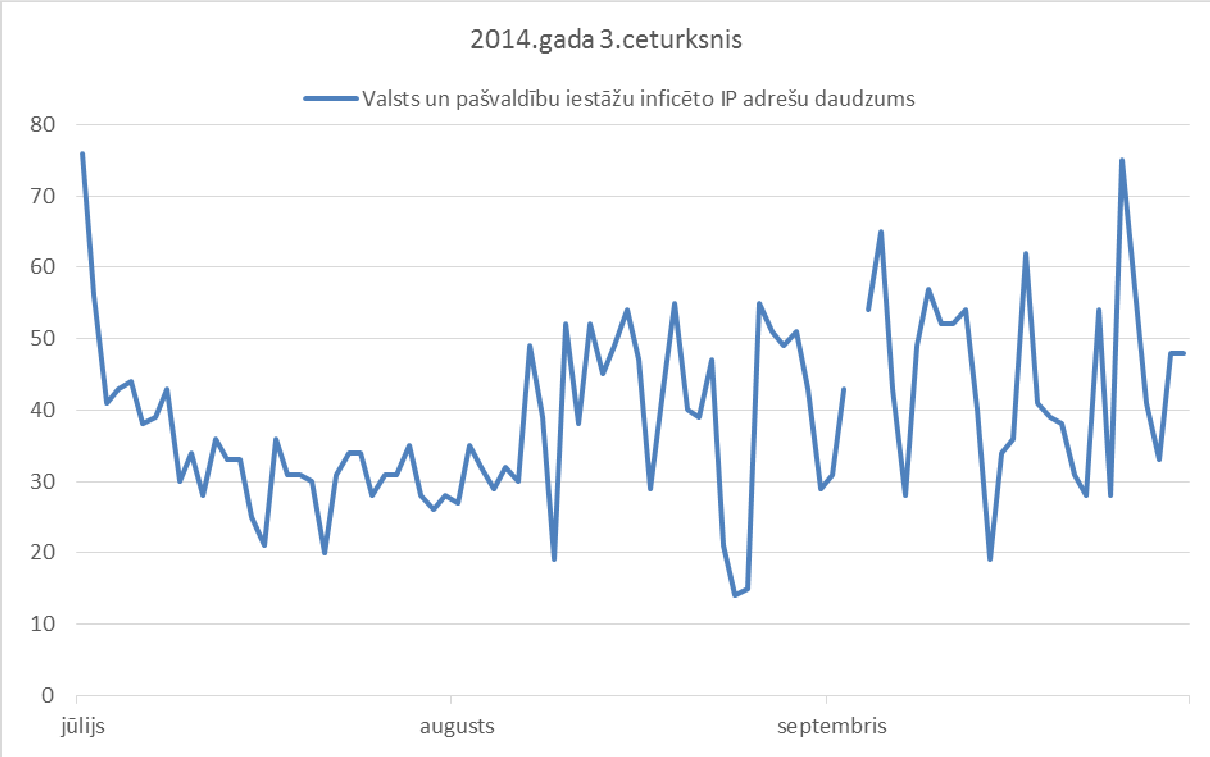
Pārskata periodā CERT.LV reģistrēja 157 293 zemas prioritātes incidentus, attēls demonstrē incidentu sadalījumu pa apdraudējumu tipiem.



6.attēls - CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā no 2014.gada 1.jūlija līdz 30.septembrim.

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 675 inficētām IP adresēm valsts un pašvaldību institūciju tīklos.



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

Pārskata periodā notika virkne dažādu uzbrukuma kampaņu, kas bija mērķētas tieši uz Latvijas interneta un internetbanku lietotājiem.

Augustā tika novēroti vairāki apjomīgi Latvijas e-pasta lietotāju datu izkrāpšanas uzbrukumi. Uzbrucēji izsūtīja mēstules un brīdināja lietotājus par pārpildītu pastkasti, aicinot pieslēgties pasta sistēmai caur webmail. Krāpnieki izvēlējās vairākus Latvijas pakalpojumu sniedzējus, kuru vārdā izsūtīja mēstules, tajā skaitā „LATNET serviss" un latvija.lv.

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

- 01.07. Pēc kādas iestādes lūguma CERT.LV veica pārbaudi viņu IDS konstatētos XSS uzbrukuma mēģinājumus. Pārbaudes rezultātā konstatēts, ka tos ģenerējis interneta meklētājrobots.
- 02.07. CERT.LV konstatēja, ka vietnē tumblr.com ievietota lapa ziedojumu izkrāpšanai. Vietnes īpašnieks tika brīdināts un krāpnieciskā lapa aizvērta.
- 14.07. Pret kādu pakalpojumu sniedzēju sistēmu tika veikts DDoS mēģinājums. To izdevās ierobežot, bloķējot 16 tīkla apgabalus.

- 14.07. Tika sniegta palīdzība lietotājam atgūt kontroli pār pikšķerēšanas rezultātā pārņemtu e-pasta kontu.
- 18.07. CERT.LV veica ievainojamu NTP serveru apzināšanu valstī un informēja par situāciju interneta pakalpojumu sniedzējus, kas piedalās iniciatīvā "Atbildīgs IPS".
- 18.07. CERT.LV uzsāka ļaunatūras kampaņas „Energetic Bear"/ „Black Energy" izmeklēšanu Latvijas IP adrešu apgabalos.
- 21.07. CERT.LV identificēja mēstuļošanas robotu tīklu, kas sastāvēja no vairākiem tūkstošiem inficētu iekārtu. Informācijas apmaiņa par šo incidentu un tā risināšanu tika koordinēta ar starptautisko CERT kopienu un mēstuļotāju melno sarakstu uzturētājiem.
- 22.07. Masveidā tika izplatīti e-pasti, kuros tika mēģināts izkrāpt naudu uzņēmuma Opal Transfer vārdā. Krāpnieciskās vēstules temats bija „Jums ir nosūtīts naudas pārskaitījums Opal Transfer sistēmā". Vēstulē tika aicināts reģistrēt bankas kontu, veicot pārskaitījumu uz Poliju viena eiro apmērā. CERT.LV brīdināja sabiedrību.

  Vēstules paraugs:

```
-------- Original Message --------
Subject: Jums ir nosutiti 479,43 EUR !
From: Opal Transfer <intranet@opaltransfer.com>
To:


Labdien,

Jums ir nosutits naudas parskaitijums Opal Transfer sistema!

Sutitaja valsts: Polija
Summa: 479,43 EUR
Parskaitijuma identifikacijas numurs: RMZ81048

Lai sanemtu parskaitijumu jums jaregistre savs bankas konts Opal Transfer
sistema.
Registret kontu Opal Transfer sistema jus varat nosutot 1.00 EUR uz Opal
Transfer kontu.

Sanemejs: OPAL Transfer
Konta numurs: PL58114000005123010200001663
BIC/SWIFT: BREXPLPW
Valsts: Polija
Summa: 1.00 EUR

Parsakitijuma komentaros OBLIGATI noradiet parskaitijuma identifikacijas
numuru!
Pec registracijas Opal Transfer sistema, naudas parskaitijums tiks
automatiski parskaitits uz registreto bankas kontu!
```

- 24.07. Tika izplatīti e-pasti ar mēģinājumiem izkrāpt naudu kādas bankas vārdā.
- 28.07. CERT.LV identificēja Latvijā uzturētu Zeus robotu tīkla kontrolieri. Datu analīzes rezultātā iegūtā informācija ļāva informēt visus upurus un instruēt par situācijas risināšanu. Upuru skaits bija pavisam neliels, jo kontrolcentra darbība tika pārtraukta tā darbības pirmajās dienās.
- 28.07. CERT.LV panāca vairāku pikšķerēšanas tīmekļa vietņu aizvēršanu Latvijā. Uzbrukuma kampaņas mērķis bija ārvalstu banku klienti. Uzbrucēji izmantoja ievainojamības novecojušā Wordpress programmatūrā.

- 01.08. Tika konstatēta datorvīrusu izplatīšana caur youtube.com, kuru, iespējams, veica Latvijas valsts piederīgais. CERT.LV apkopoja tehnisko informāciju un nodeva policijai.
- 07.08. Tika veikta pikšķerēšanas kampaņas izmeklēšana, kuras mērķi bija dažādi Latvijas e-pasta pakalpojumu sniedzēji.

  Uzbrucēji upurus meklēja, izsūtot mēstules un izliekoties par pakalpojumu sniedzēju, un brīdinot par pārpildītu pastkasti, aicinot pieslēgties pasta sistēmai caur webmail, jo e-pasta konts esot pārpildīts.

  Vēstules paraugs:


From LATNET Webmail Serviss <famuk@latnet.lv>
Subject **Jusu e-pasta driz beigsies**
To undisclosed-recipients:;

Cienijamais lietotaj

Jusu e-pasta driz beigsies

Lai izvairitos no jebkadiem partraukumiem, ludzu noklikskiniet uz saites zemak, un uzlabot savu e-pastu

Klikњkiniet seit <http://www.iepj.com.br/player/Scripts/mail.ls.lv.htm>, lai parietu

Sirsnigi
Klientu Help Desk

  CERT.LV informēja sabiedrību un valsts un pašvaldību iestādes, kā arī veica incidenta monitoringu, lai identificētu un novērstu vairākus datu zādzības gadījumus valsts pārvaldes iestādēs.
- 18.08. CERT.LV veica USB zibatmiņu drošības pārbaudi pēc kādas iestādes saņemtā pieprasījuma.
- 25.08. Pagaidām nenoskaidroti uzbrucēji uzsāka Zeus trojāna izplatīšanas kampaņu ar e-pastu starpniecību. E-pasti tika izsūtīti masveidā ar tekstu “my new photo :)” un photo.zip failu pielikumā, kas satur photo.exe izpildāmo failu, kuram tika nomainīta ikona, lai maldinātu lietotāju, ka tā patiešām ir bilde.
- 25.08. CERT.LV identificēja Zeus vīrusa kontrolcentru, kas tika uzturēts Latvijā.
- 26.08. CERT.LV identificēja ļaunatūras kampaņu, kas bija mērķēta uz Čehijas iedzīvotājiem. Incidenta analīzes rezultātā tika identificēti vairāki simti potenciālo upuru un informācija nodota Čehijas CERT kolēģiem.
- 28.08. CERT.LV organizēja informācijas apmaiņu ar Polijas CERT kolēģiem par uzbrukumiem Polijas valsts pārvaldes tīmekļa vietnēm, par kuriem atbildību uzņēmās grupējums “Cyber-Berkut”.
- 28.08. Incidenta izmeklēšanas laikā tika identificēti nozagti kāda portāla un kāda e-pasta pakalpojumu sniedzēja lietotāju kontu dati. Datus nezināmi uzbrucēji nozaga no pašu lietotāju datoriem ar Zeus Trojan starpniecību.

- 29.08. CERT.LV sniedza konsultācijas par e-pasta filtrāciju kādam uzņēmumam (notika mēģinājums izkrāpt e-pasta pieejas datus vienam no valdes locekļiem).
- 01.09. Autentifikācijas datu zādzības rezultātā tika uzlauzts kādas pašvaldības e-pasta konts. Kļuva zināms, ka tas izmantots masveida mēstuļu izsūtīšanai.
- 02.09. Latvijas akadēmiskais tīkls GEANT piedzīvoja vairākus liela apjoma DDoS uzbrukumus. Tos izdevās atvairīt, koordinējot filtru ieviešanu ar *Upstream* pakalpojumu sniedzējiem. Uzbrukumā bija iesaistīti nedroši konfigurēti DNS un NTP serveri. Par identificētajām iekārtām tika informētas attiecīgo valstu CERT komandas.
- 07.09. Notika masveida e-pasta pieejas datu pikšķerēšanas mēģinājums no e-pasta pakalpojuma lietotājiem. Tika brīdināts pakalpojumu sniedzējs.
- 08.09. Tika izmeklēts FLASH drive-by incidents, kurā ļaunatūras komponentes tika uzturētas uz kāda Latvijas domēna.
- 08.09. CERT.LV sniedza konsultācijas uzņēmumam par DDoS uzbrukumu risināšanas un uzbrukumu analīzes metodēm.
- 17.09. Tika konstatēts pikšķerēšanas mēģinājums pret kādas bankas klientiem. Kaitīgā lapa tika slēgta.
- 23.09. Notika masveida e-pasta pieejas datu pikšķerēšanas mēģinājums. Tika brīdināts pakalpojumu sniedzējs, krāpnieciskais konts tika slēgts.
- 23.09. Igaunijas valsts pārvaldes iestādes piedzīvoja mērķētu uzbrukumu. Informācija par uzbrukumu detaļām tika apkopota arī Latvijā un tika informētas saistītās iestādes. Tiek veikta izmeklēšana.
- 24.09. CERT.LV sniedza konsultācijas kādam uzņēmumam par labākajām metodēm cīņā ar UpNP SSDP DOS tipa uzbrukumiem.
- 24.09. Atklātībā nonāca nopietnas Linux un OS X operētājsistēmās atrodamās BASH ievainojamības detaļas. Ievainojamības izmantošana atsevišķos gadījumos ļauj uzbrucējam attālināti izpildīt patvaļīgu kodu. CERT.LV informēja sabiedrību un uzsāka preventīvo pasākumu ieviešanu.

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

CERT.LV uzskaita arī uzlauzto un izķēmoto mājaslapu gadījumus.

Šādu gadījumu skaits:
Jūlijā - 34, no tiem 29 - Linux, 5 – nezināms;
Augustā – 16, no tiem 15 – Linux, 1 – Windows;
Septembrī – 42, no tiem 35 – Linux, 1 – FreeBSD, 2 – nezināms, 4 – Windows.

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

CERT.LV uztur tīmekļa vietni https://www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs.

Pārskata periodā vispopulārākā sadaļa bija par jaunākajiem vīrusiem, (7 920 lapu skatījumi), tai seko ziņa par krāpniecisku e-pasta vēstuļu izsūtīšanu kompānijas Opal Transfer vārdā ar 1 535 apmeklējumiem. Trešā populārākā ziņa pārskata periodā bija informācija par CERT.LV un ISACA rīkoto IT drošības konferenci „Apmācīts un atbildīgs IT/IS lietotājs - mūsu visu drošības pamats" ar 1 523 lapu skatījumiem pārskata periodā.

Kopā CERT.LV mājaslapai bijuši 36 073 lapu skatījumi, kurus veido 28 479 unikāli lapu skatījumi no 81 valsts. Arī šajā periodā lielākā daļa - 90,82% apmeklējumu bija no Latvijas.

Pārskata periodā CERT.LV tīmekļa vietnē tika publicētas 20 ziņas, sniegta informācija par CERT.LV organizētiem un starptautiska mēroga pasākumiem, publicētas CERT.LV prezentācijas, mediju ziņas un CERT.LV publiskais darbības pārskats par 2014.gada 2. ceturksni.

CERT.LV Twitter kontā https://twitter.com/certlv regulāri tiek publicētas ziņas par dažādiem jaunumiem. Pārskata periodā tika publicētas 48 ziņas, kontam pievienojušies 70 jauni sekotāji un 141 reizes @certlv ziņa ir tikusi „retvītota" jeb padota tālāk.

CERT.LV ir izveidots profils arī sociālajā tīklā Facebook http://www.facebook.com/certlv (pārskata periodā publicētas 40 ziņas) un profils sociālajā tīklā Google+ https://www.google.com/+CertLv (publicētas 40 ziņas), kā arī lapa draugiem.lv - http://www.draugiem.lv/certlv, kurā publicētas 48 ziņas.

CERT.LV uztur arī pieaugušo izglītošanas portālu https://www.esidross.lv. Pārskata perioda laikā portālā ir publicēti 4 jauni raksti, portālam bija 25 571 lapu skatījumi no tiem 20 876 unikāli lapu skatījumi.

Publicētie raksti:

- „Virtuālā izmeklēšana, reāls arests (1. daļa)" https://www.esidross.lv/2014/07/30/virtuala-izmeklesana-reals-arests
- „Virtuālā izmeklēšana, reāls arests (2. daļa)" https://www.esidross.lv/2014/08/28/virtuala-izmeklesana-reals-arests-2-dala
- „LastPass – paroļu pārvaldnieks" https://www.esidross.lv/2014/07/14/lastpass-parolu-parvaldnieks
- „Kādi ir informācijas drošības draudi sociālajos tīklos un kā tos novērst?" https://www.esidross.lv/2014/07/04/kadi-ir-informacijas-drosibas-draudi-socialajos-tiklos-un-ka-tos-noverst

Augustā CERT.LV sadarbībā ar Lattelecom izveidoja rakstu „Pieci lielākie klupšanas akmeņi drošam darbam internetā", kas tika publicēts vairākos medijos.

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

Sīkāka informācija:

1) Intervijas un ziņas radio:

- 09.07. Saruna par IT drošības incidentiem, IT drošību un aizmiršanas tiesībām internetā Latvijas Radio Pieci raidījumā „Domnīca".
- 15.09. Tika sniegta intervija Latvijas radio 1 rīta ziņām par politiķu twitter kontu uzlaušanu.
- 15.08. Tika sniegta intervija Latvijas Radio par IT apdraudējumiem Ukrainas – Krievijas konflikta ietekmē.

2) Sižeti televīzijā, tiešraides:

- 24.07. Tika sniegta intervija LTV7 ziņās par kiberdrošību internetā.
- 28.07. Tika sniegts komentārs LNT raidījumā 900 sekundes par Latvijas iedzīvotāju iesaisti kibernoziegumos Ukrainā.
- 14.09.Tika sniegta intervija TV 3 raidījumam "Nekā personīga" par hakeru iesaisti Ukrainas konfliktā.

3) Ziņas portālos:

- 08.07. Nedari internetā to, ko nedarītu reālajā dzīvē, brīdina speciālisti – raksts la.lv.
- 11.07. Bērnu pornogrāfiju skatās darbā – raksts nra.lv.
- 14.07. Viltus vēstules spēlē uz cilvēku vājībām – raksts nra.lv.
- 12.07. Liela daļa Latvijas iedzīvotāju neievēro drošības pasākumus internetā – raksts delfi.lv.
- 04.08. AM prasīs 40 000 eiro kiberjaunsardzes izveidošanai – raksts tvnet.lv.
- 10.08. Kiberuzbrukumi saasina bažas par cilvēku datu drošību – raksts lsm.lv.
- 15.08. Prognozē drošinātu telefonu nišas plašāku attīstību nākotnē – raksts lsm.lv.
- 15.08. Brīdina par apjomīgu lietotāju e-pasta datu izkrāpšanu – raksts nra.lv.
- 15.08. Novērota apjomīga interneta lietotāju datu izkrāpšanas kampaņa - raksts apollo.lv.
- 15.08. Novērota apjomīga lietotāju e-pasta datu izkrāpšanas kampaņa – raksts valmieraszinas.lv.
- 18.08. Novērota apjomīga lietotāju e-pasta datu izkrāpšanas kampaņa – raksts tvnet.lv.
- 22.08. Aicina neuzķerties uz it kā no «Latvija.lv» sūtītiem e-pastiem – raksts tvnet.lv.
- 22.08. Aicina neuzķerties uz it kā no «Latvija.lv» sūtītiem e-pastiem – raksts delfi.lv.
- 22.08. Aicina neuzķerties uz it kā no «Latvija.lv» sūtītiem e-pastiem – raksts kasjauns.lv.
- 22.08. Aicina uzmanīties no "Latvija.lv" sūtītiem e-pastiem – raksts nra.lv.
- 22.08. TOP 5 подводных камней безопасной работы в интернете – raksts dfakti.lv.
- 22.08. TOP 5 klupšanas akmeņi drošam darbam internetā – raksts ogresnovads.lv.

- 04.09. IT security training by ENISA and Latvia's CERT – raksts ENISA portālā.
- 07.09. Pieci lielākie klupšanas akmeņi drošam darbam internetā – raksts diena.lv.
- 25.09. Atklātā 'Linux' ievainojamība apdraud arī lielu daļu Latvijas sistēmu – raksts delfi.lv.
- 26.09. Atklātā «Linux» ievainojamība apdraud arī lielu daļu Latvijas sistēmu –raksts tvnet.lv.

8.jūlijā CERT.LV pārstāvis uzstājās ar prezentāciju Latvijas Komercbanku asociācijas organizētā pasākumā medijiem par pētījumu „Drošība internetā".

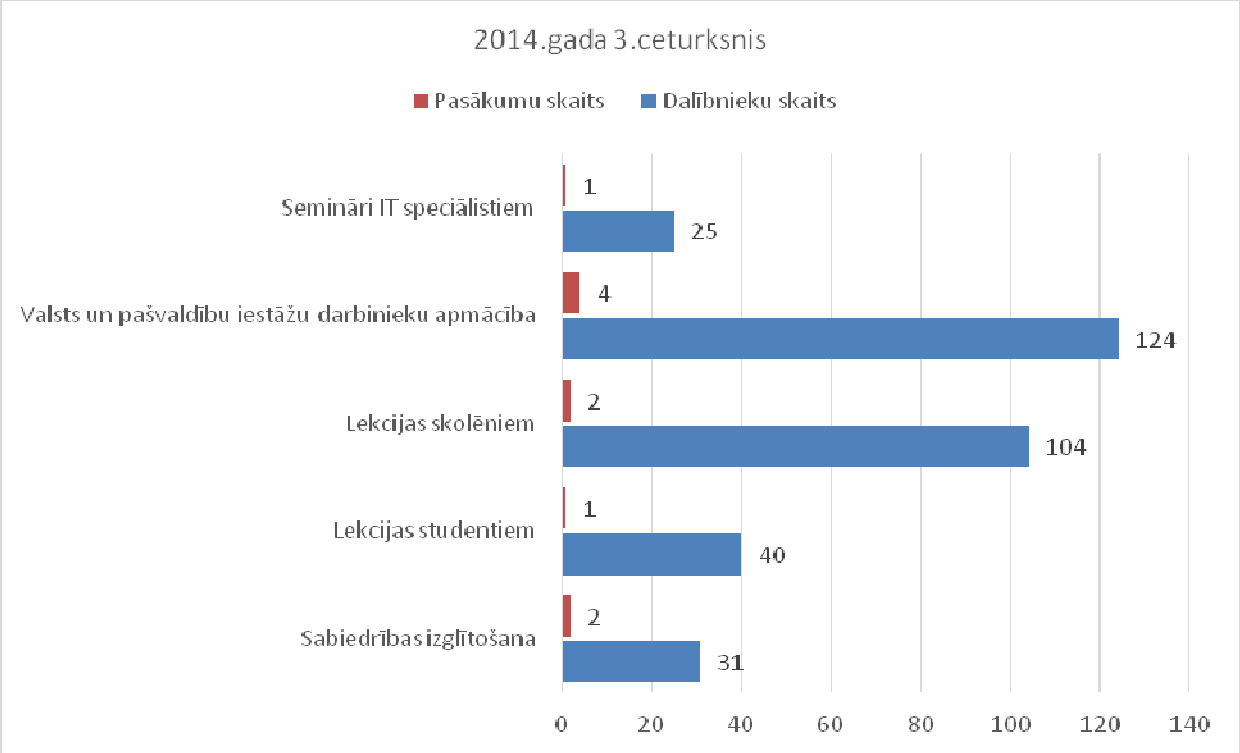
4. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

Pārskata periods sākās ar CERT.LV un ENISA kopīgi organizēto semināru "Elektronisko pierādījumu identificēšana un izmantošana digitālajā ekspertīzē", kurā piedalījās 25 dalībnieki. Semināra tēmas bija pierādījumu vākšana digitālajā vidē un digitālās ekspertīzes pamata principi, kā arī mobilo iekārtu incidenti un to risināšana. Semināra dalībnieku anketēšana uzrādīja, ka dalībnieki semināru novērtēja kā kvalitatīvu un noderīgu.

No jūlija līdz septembrim turpinājās organizatoriskais darbs pie IT drošības konferences "Apmācīts un atbildīgs IS/IT lietotājs – mūsu visu drošības pamats", kas norisināsies 16.oktobrī Latvijas Nacionālajā bibliotēkā. Līdz septembra beigām uz konferenci pieteicās 500 dalībnieki no visas Latvijas.

Pārskata periodā CERT.LV uzsāka sadarbību sabiedrības izglītošanas jomā ar Lattelecom un Netsafe. Sadarbības rezultātā tika izstrādāta prezentācija par drošību internetā ar mērķi palielināt skolēnu un skolotāju zināšanas par droša interneta un WiFi lietošanu. Tāpat CERT.LV atbalstīja arī Latvijas Nebanku kredītdevēju asociācijas veidoto kampaņu kā informatīvais partneris, sniedzot informāciju par droša interneta lietošanas pamatiem, veicot finanšu darījumus.

Kopā pārskata periodā CERT.LV par IT drošību ir izglītojis 324 cilvēkus, piedaloties 10 dažādos pasākumos un lekcijās.



8.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits 2014.gada 3.ceturksnī.

CERT.LV pasākumi pārskata periodā:

1) ***Semināri IT speciālistiem:***

- 09.-10.07. Notika CERT.LV un ENISA organizētais seminārs IT drošības speciālistiem "Elektronisko pierādījumu identificēšana un izmantošana digitālajā ekspertīzē".

2) ***Valsts un pašvaldību iestāžu darbinieku apmācības:***

- 25.09. CERT.LV pārstāvis uzstājās ar divām prezentācijām LR Ārlietu ministrijas konsulāro darbinieku apmācībās Viļņā un stāstīja par IT drošību.
- 29.09. CERT.LV pārstāvis sniedza prezentāciju valsts pārvaldes iestāžu darbiniekiem Ģenerālprokuratūrā par IT drošības jautājumiem.
- 30.09. 29.09. CERT.LV pārstāvis sniedza prezentāciju valsts pārvaldes iestāžu darbiniekiem Ģenerālprokuratūrā par IT drošības jautājumiem.

3) ***Lekcijas skolēniem:***

- 22.08. CERT.LV pārstāvis uzstājās ar prezentāciju jaunāko klašu skolēniem Lattelecom Ģimenes dienā un stāstīja par IT drošību Lattelecom darbinieku bērniem.
- 19.08. CERT.LV pārstāvis uzstājās ar lekciju skolēniem nometnes laikā par IT drošības jautājumiem.

4) ***Lekcijas studentiem:***

- 24.09. CERT.LV pārstāvis uzstājās ar prezentāciju LU Datorikas fakultātes studentu seminārā par tēmu „Atbildīga ievainojamību atklāšana".

5) ***Sabiedrības izglītošana:***

- 08. 07. CERT.LV pārstāvji uzstājās ar prezentāciju Latvijas Komercbanku asociācijas un LIKTA rīkotajās mediju brokastīs par pētījuma „Drošība internetā" prezentāciju.
- 29.08. CERT.LV uzstājās ar prezentāciju Finanšu un kapitāla tirgus komisijas organizētajās krīzes komunikācijas mācībās par IT drošību Latvijā.

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

Pārskata periodā CERT.LV turpināja uzsākto darbu pie Agrās brīdināšanas sistēmas izveides un līgumu saskaņošanas ar sadarbības partneriem. Agrās brīdināšanas sistēma jeb sensoru tīkla projekts nodrošinās iestāžu informācijas tehnoloģiju resursu augstāku drošības līmeni un palīdzēs savlaicīgi atklāt bīstamus un mērķētus informācijas tehnoloģiju uzbrukumus.

Septembrī CERT.LV uzsāka gatavošanos seminārам "IT drošības risku mazināšana pirms ES prezidentūras", izstrādājot „Informācijas tehnoloģiju drošības rekomendācijas valsts un pašvaldību iestādēm", gatavojoties ES Prezidentūrai.

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

- 21.07. Notika sadarbības tikšanās par Latvijas prezidentūru Eiropas Savienības Padomē.
- 22.07. CERT.LV pārstāvis tikās ar Ārlietu ministriju, lai pārrunātu sadarbību apmācību jomā.
- 23.07. Notika sadarbības tikšanās ar Aizsardzības ministriju un Ārlietu ministrijas pārstāvjiem.
- 24.07. CERT.LV pārstāvis piedalījās Aizsardzības ministrijas sanāksmē, lai apspriestu kādu likumprojektu.
- 14.08. Notika Drošības ekspertu grupas sanāksme.
- 20.08. Notika sadarbības tikšanās ar Aizsardzības ministrijas Kiberdrošības politikas nodaļas darbiniekiem, lai pārrunātu līdzšinējo sadarbību.
- 03.09. Notika sadarbības tikšanās ar Valsts kases pārstāvi.
- 04.09. CERT.LV pārstāvis uzstājās ar prezentāciju Ārlietu ministrijā, jauno diplomātu apmācībā.
- 10.09. Notika Drošības ekspertu grupas izbraukuma sēde.
- 11.09. Notika darba tikšanās ar Valsts policijas pārstāvi.
- 12.09. Notika tikšanās ar Aizsardzības ministrijas pārstāvjiem par finanšu jautājumiem.
- CERT.LV piedalījās sanāksmēs par kiberdrošības mācību plānošanu.

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

IT drošības likums nosaka, ka Valsts un pašvaldību institūcijām jāinformē CERT.LV par nozīmēto atbildīgo personu, kura iestādē īsteno informācijas tehnoloģiju drošības pārvaldību. Līdz 2014.gada 30.septembrim CERT.LV ir apkopojis informāciju par 1377 kontaktpersonām, kuras ir atbildīgas par IT drošības pārvaldību.
Kontaktpersonu skaits, salīdzinot ar iepriekšējo pārskata periodu, palielinājies, pateicoties sadarbībai ar Kultūras informācijas sistēmu centru, jo septembrī CERT.LV pievienoja savai datu bāzei informāciju par bibliotēkām.

IT drošības likums un ar to saistītie MK noteikumi Nr. 327 nosaka kārtību, kādā Elektronisko sakaru komersantiem (turpmāk – ESK) jāizstrādā un jāiesniedz CERT.LV rīcības plāns elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai. Līdz 30. septembrim plānus ir iesnieguši 58 ESK. Mazajiem ESK ir pieejams CERT.LV izstrādātais Rīcības plāna paraugs, lai palīdzētu tiem izveidot savu plānu.

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

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

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

Pārskata periodā notika aktīva sadarbība ar citu valstu IT drošības incidentu novēršanas vienībām, gan lūdzot palīdzību un informāciju par incidentiem, kas notiek Latvijā, gan palīdzot risināt citās valstīs notikušus incidentus, gan kopīgi uzlabojot incidentu risināšanas metodoloģiju, rīkus un procedūras.

Pārskata periodā tika uzsākta gatavošanās ENISA organizēto kiberdrošības mācību „Cyber Europe 2014" 2.posmam.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 01.07. Notika sadarbības videokonference ar Lietuvas valdības CERT.
- 03.07. CERT.LV pārstāvis piedalījās CCDCOE organizētā „Locked Shields 2014" atskaites pasākumā un uzstājās ar prezentāciju par Latvijas - Čehijas apvienotās komandas dalību mācībās. Tikšanās notika Tallinā, Igaunijā.
- 21-25.07. CERT.LV pārstāvis piedalījās NATO School kursos „Seminar on International law of cyber operations", kas notika Oberammergau, Vācijā.
- 22.07. Vizītē CERT.LV ieradās Regional Cyber Officer for Baltics Kaija Kirch no Lielbritānijas vēstniecības Tallinā. Tika pārrunātas sadarbības iespējas.
- 04.-12.08. CERT.LV pārstāvis piedalījās DEF CON® konferencē, kas notika Lasvegasā, ASV.
- 25.08. CERT.LV organizēja tikšanos ar Lietuvas speciālistiem par DDoS uzbrukumu novēršanu Lietuvas prezidentūras laikā ES padomē.
- 15-19.09. CERT.LV pārstāvis piedalījās CCDCoE kursos „Malware and Exploits Essentials Course", kas notika Tallinā, Igaunijā.
- 18-19.09. CERT.LV pārstāvis piedalījās TF-CSIRT sanāksmē un uzstājās ar prezentāciju „Preparations for the EU presidency in Latvia", kas notika Romā, Itālijā. Sanāksmes laikā CERT.LV vadītāja Baiba Kaškina tika ievēlēta par TF-CSIRT grupas priekšsēdētāju.
- 22.-24.09.CERT.LV pārstāvji piedalījās "Hands-on workshop for penetration testers", kas notika CCDCoE, Tallinā, Igaunijā.
- 23.09. CERT.LV viesojās Lithuanian Cybercrime Center of Excellence for Training pārstāvji.
- 29.09. CERT.LV pārstāvji piedalījās seminārā C4E workshop kopā ar Czech CyberCrime Centre of Excellence un Digital Forensics Institute of Czech republic.

Sadarbība konkrētu incidentu gadījumos aprakstīta šī pārskata 2.punktā.

8. Citi normatīvajos aktos noteiktie pienākumi.

- 07.-11.07. CERT pārstāvji apmeklēja Certified Ethical Hacker kursus.
- 27.07. Tika organizēta sadarbības tikšanās ar Komercbanku asociāciju un banku pārstāvjiem.
- 07.08. CERT.LV pārstāvis piedalījās Nacionālās apvienības „Visu Latvijai!" – „Tēvzemei un Brīvībai/LNNK" organizētajā diskusijā "Interneta vēlēšanas Latvijā: par un pret".
- 04.09. Notika sadarbības tikšanās ar Nebanku kredītu devēju asociāciju par lietotāju izglītošanas kampaņu.
- 04.09. Notika sadarbības tikšanās ar Kaspersky Lab pārstāvjiem.
- 11.09. Notika sadarbības tikšanās ar Netsafe Latvija un Lattelecom pārstāvjiem par Wifi drošības semināriem skolās.
- 24.09. CERT.LV tikās ar Vidzemes augstskolas pārstāvjiem, lai pārrunātu IT drošības mācību organizēšanu un studentu iesaistīšanas iespējas.

2014.gada 7.novembrī

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