Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi 2014.gadā

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 Izplatītākie incidentu veidi bija piķšerēšanas kampaņas, datorvīrusi un ievainojamības populārās lietotnēs, tie skāra Latvijas interneta lietotājus, valsts un pašvaldību iestādes, kā arī interneta pakalpojumu sniedzējus un uzņēmējus.

Pieauga leģitīmo interneta resursu izmantošana ļaunatūras izplatīšanā. Interneta vietnes tika izmantotas banku trojas vīrusa „Zeus" un „Gozi" izplatīšanā, inficējot simtiem lietotāju datorus. Kāds Latvijā nenoskaidrots grupējums realizēja vismaz 3 saistītas uzbrukumu kampaņas no 2013.g oktobra līdz 2014.g martam („Banku vīruss", „Nodokļu vīruss" un „Gozi" banku trojāna izplatīšana caur leģitīmām tīmekļa vietnēm). Aprīlī vairāki Latvijas portāli tika izmantoti vīrusu izplatīšanai caur ievainojamību OpenX baneru apmaiņas sistēmā. Izmantojot šo ievainojamību, tika izplatīts bīstamais „Gozi" banku vīruss.

Aprīļa sākumā tika izziņota OpenSSL ievainojamība, kuru izmantojot, kļuva iespējams attālināti iegūt lietotāju paroles un lietotājvārdus, transakciju datus un citu sensitīvu informāciju, kas glabājas servera atmiņā. Latvijā ievainojamībai tika pakļautas vismaz 1300 vietnes.

Pirmajā gada ceturksnī masveidā tika izplatītas mēstules, kas saturēja datorvīrusu bankas datu izkrāpšanai, jeb tā saukto „VID vīrusu", radot bankas datu izkrāpšanas un naudas līdzekļu nozagšanas risku.

Novembrī Latvijā sāka izplatīties datorvīruss „CTB Locker", kurš šifrē lietotāja datus, par atšifrēšanas atslēgu pieprasot izpirkuma maksu.
Datora inficēšanās ar ļaunatūru notika, lietotājam apmeklējot leģitīmas interneta vietnes. Dators tika inficēts automātiski, ļaunatūrai atrodot Java, Adobe Flash spraudņu, kā arī citas interneta pārlūka ievainojamības.

Gada nogalē e-pasta lietotāji Latvijā cieta no Gmail pikšķerēšanas kampaņas. Vairākiem simtiem lietotāju tika kompromitēts e-pasts, no kura tika izsūtītas mēstules lietotāja adrešu grāmatai. Vēl lielāks e-pasta lietotāju skaits saņēma it kā draugu sūtītas vēstules ar lūgumu pārskaitīt naudu, jo vēstules sūtītājs ārzemēs nonācis grūtībās.

Pārskata periodā CERT.LV reģistrēja un apstrādāja 3034 augstas prioritātes incidentus un reģistrēja 487 055 zemas prioritātes incidentus.

Pārskata periodā CERT.LV piedalījās 95 pasākumos, izglītojot 5664 cilvēkus par IT drošības tēmām.

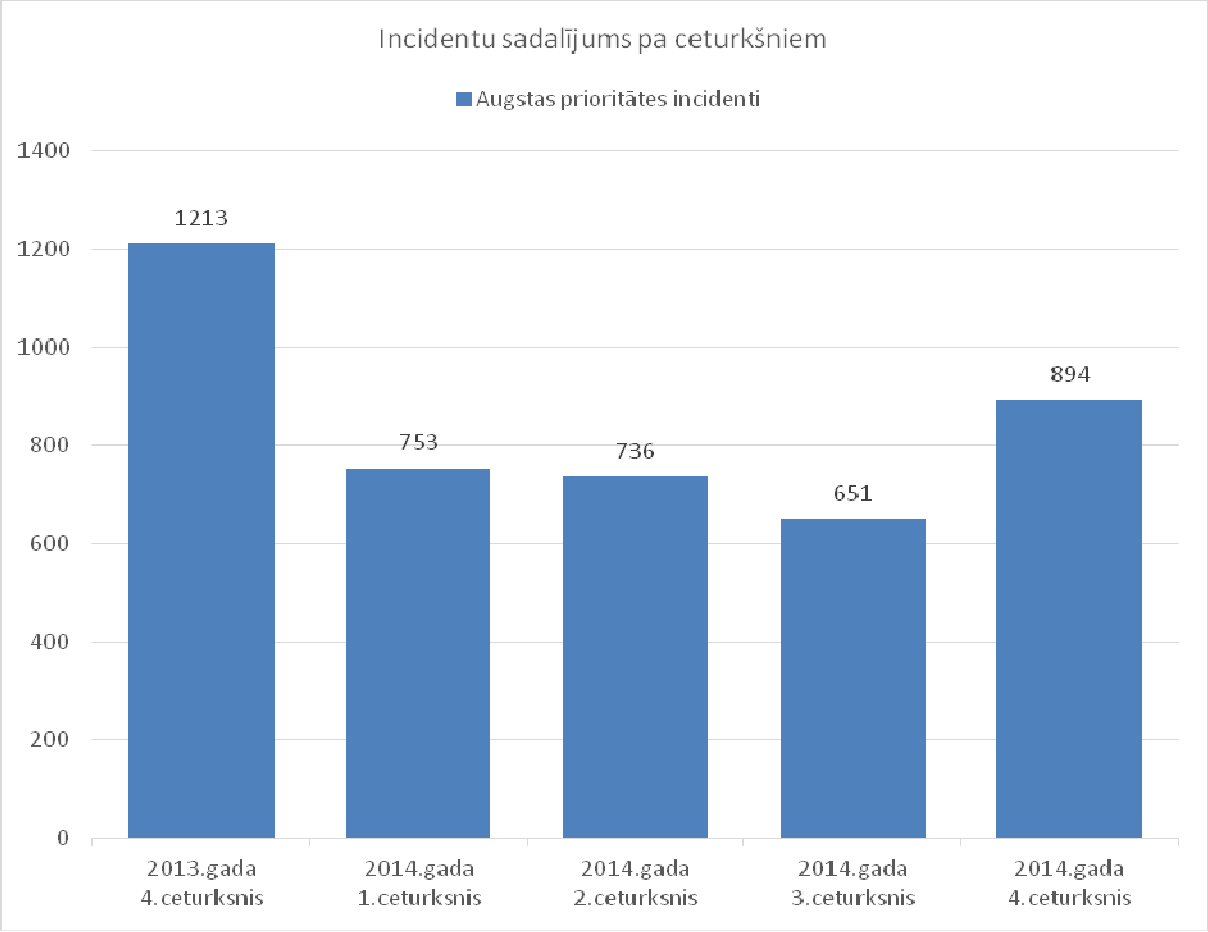
1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

CERT.LV 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.gadā CERT.LV reģistrēja un apstrādāja 3034 augstas prioritātes incidentus. 2013.gadā tika reģistrēti un apstrādāti 4964 augstas prioritātes incidenti, savukārt 2012. gadā - 4794 augstas prioritātes incidenti.

2014.gada janvārī CERT.LV veica pāreju uz automātisko incidentu uzskaites sistēmu (RTIR), lai uzlabotu incidentu apstrādes efektivitāti. Sistēma vairākus incidentu veidus apstrādāja automātiski, nevis manuāli, veidojot augstas prioritātes incidentu skaita samazinājumu, salīdzinot ar 2013.gadu.

Augstas prioritātes incidentu skaita pieaugums 2014.gada pēdējā ceturksnī skaidrojams ar krāpniecisko aktivitāšu pieaugumu pirmssvētku laikā.

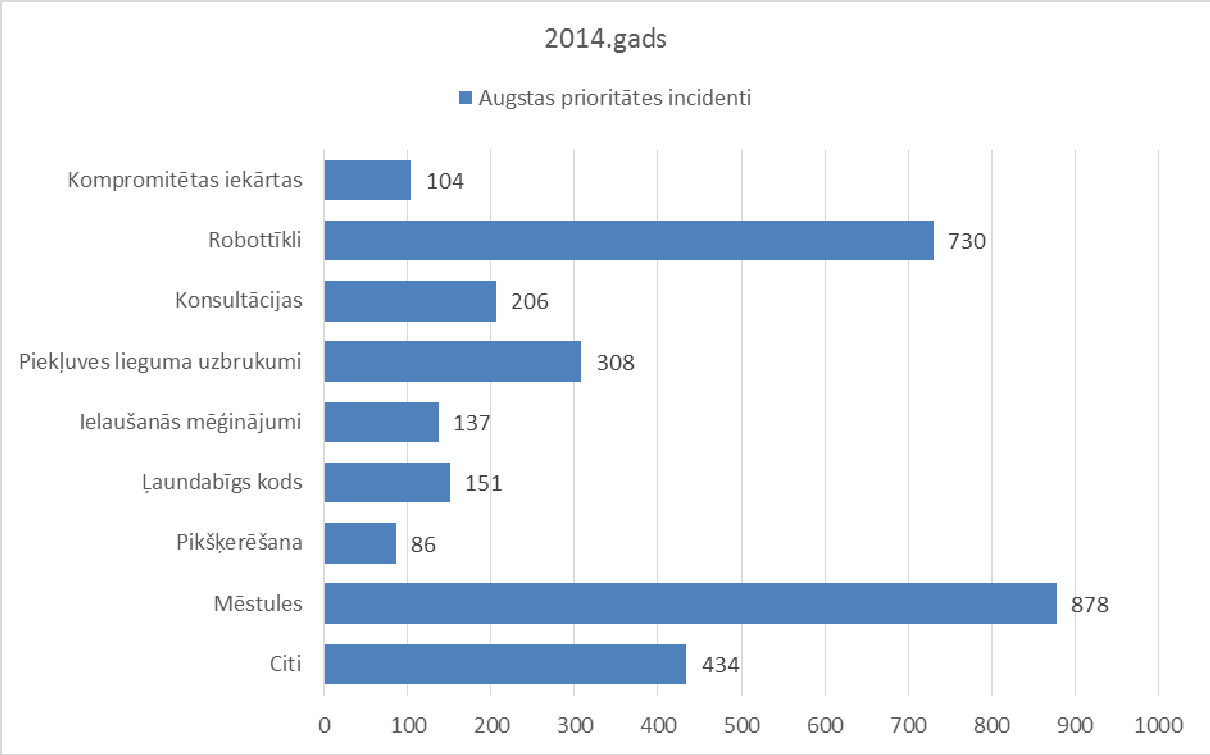


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem.

Izplatītākais augstas prioritātes incidentu veids 2014.gadā bija mēstules. Visbiežāk tieši mēstules ir pamats arī citiem datordrošības apdraudējumiem – pikšķerēšanai, ļaunatūras izplatībai un mērķētiem uzbrukumiem. Attīstoties tehnoloģijām, mēstuļu teksti paliek ticamāki, vizuālais noformējums pikšķerēšanas lapām kļūst kvalitatīvāks, tādēļ lietotājiem jābūt arvien uzmanīgākiem, pat ievadot savus datus it kā zināmās vietnēs.

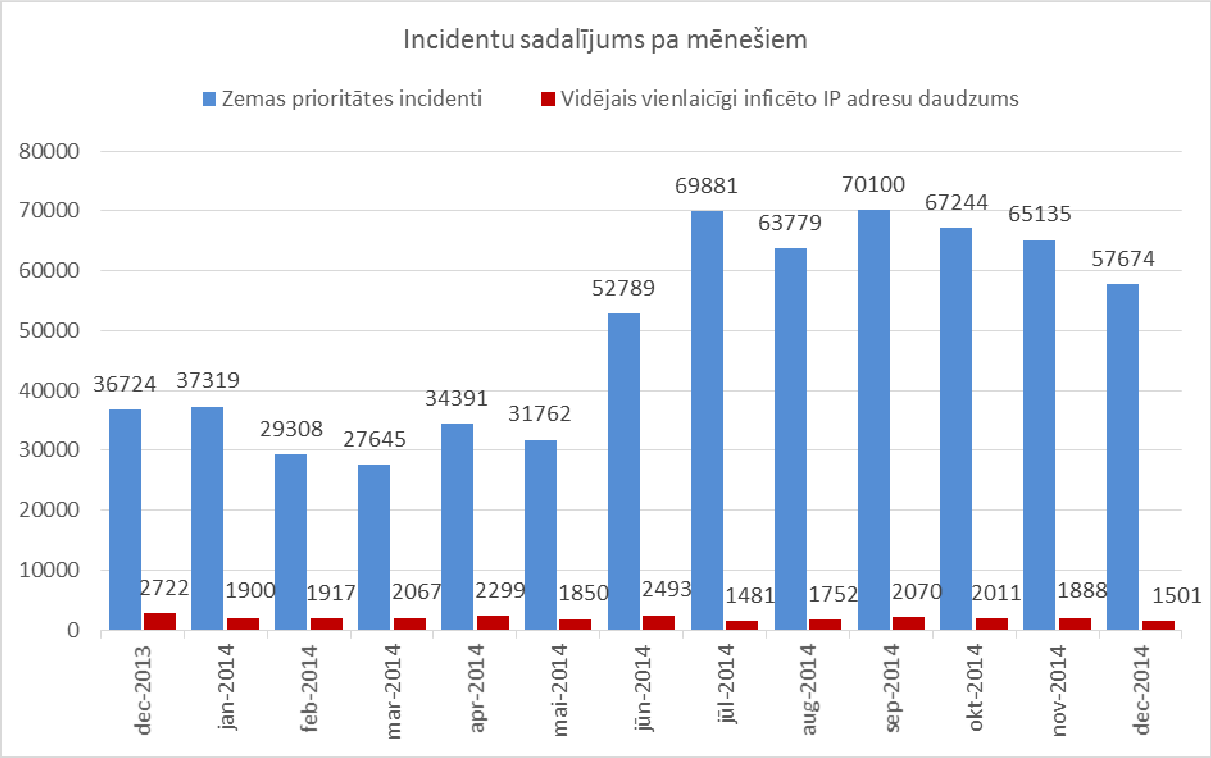
Augsta bijusi robotttīklu izplatība valsts un pašvaldību iestāžu tīklos – pārsvarā tos veido, lai kompromitētos datorus pievienotu „robotu" armijai un tālāk izmantotu dažāda veida drošības apdraudējumu realizēšanai – mēstuļu izplatīšanai, piekļuves lieguma uzbrukumiem vai pat kriptovalūtas ģenerēšanai, kā arī informācijas zagšanai.

CERT.LV visām augstas prioritātes incidentos iesaistītajām pusēm sniedza konsultācijas, kā izvairīties no apdraudējumiem un pasargāt datoru nākotnē.



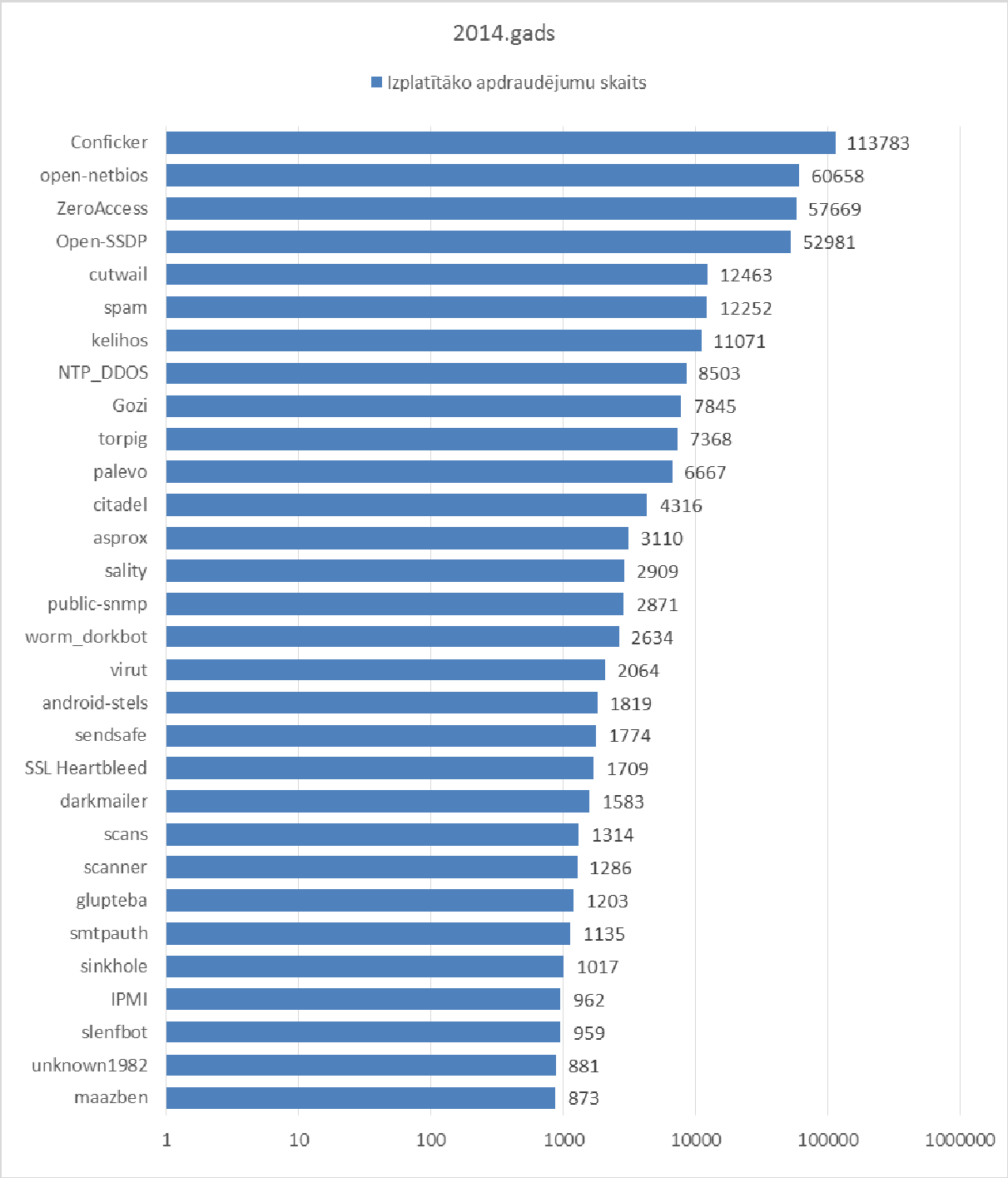
2.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2014.gadā.

2014.gadā CERT.LV reģistrēja 487 055 zemas prioritātes incidentus. 2013.gadā tika reģistrēti 247 815 zemas prioritātes incidenti, savukārt 2012.gadā – 222 599 incidenti.



3.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem 2014.gadā.

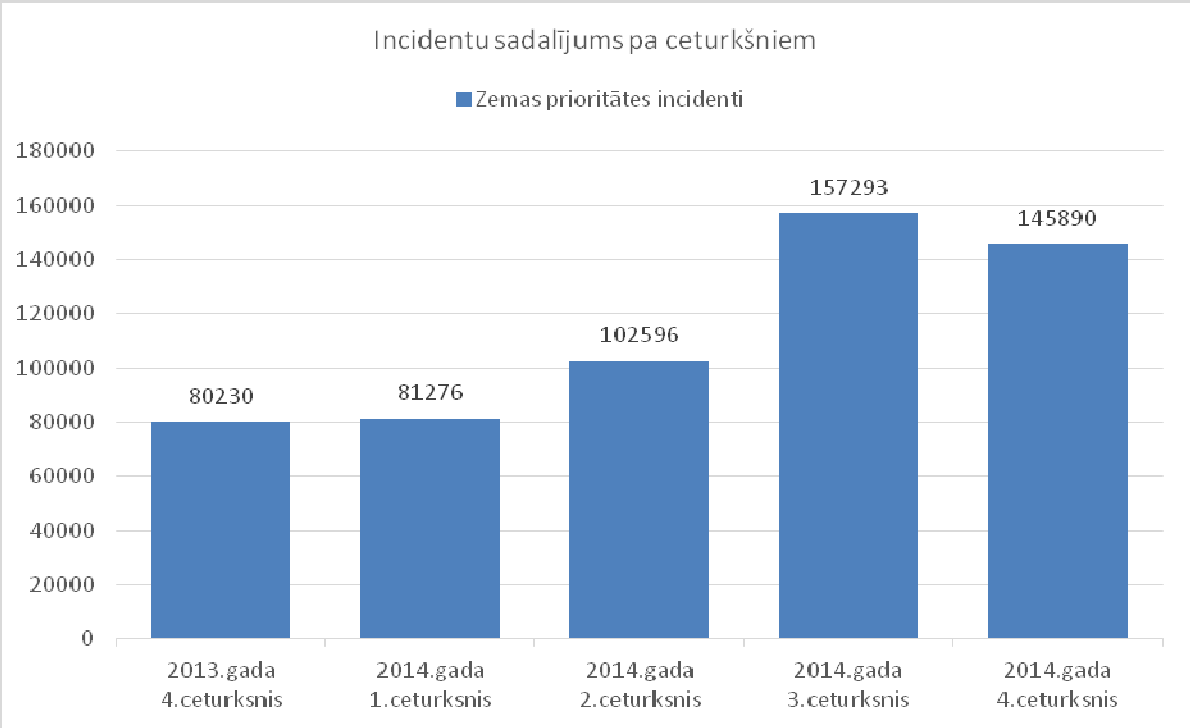
Lai samazinātu kopējo inficēto IP adrešu skaitu, CERT.LV kopā ar „Net-Safe Latvija" ir izveidojuši saprašanās memorandu, kas tiek slēgts ar interneta pakalpojumu sniedzējiem, kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs". 2014.gadā iniciatīvai ir pievienojušies un par incidentiem informē savus gala lietotājus 13 interneta pakalpojumu sniedzēji.



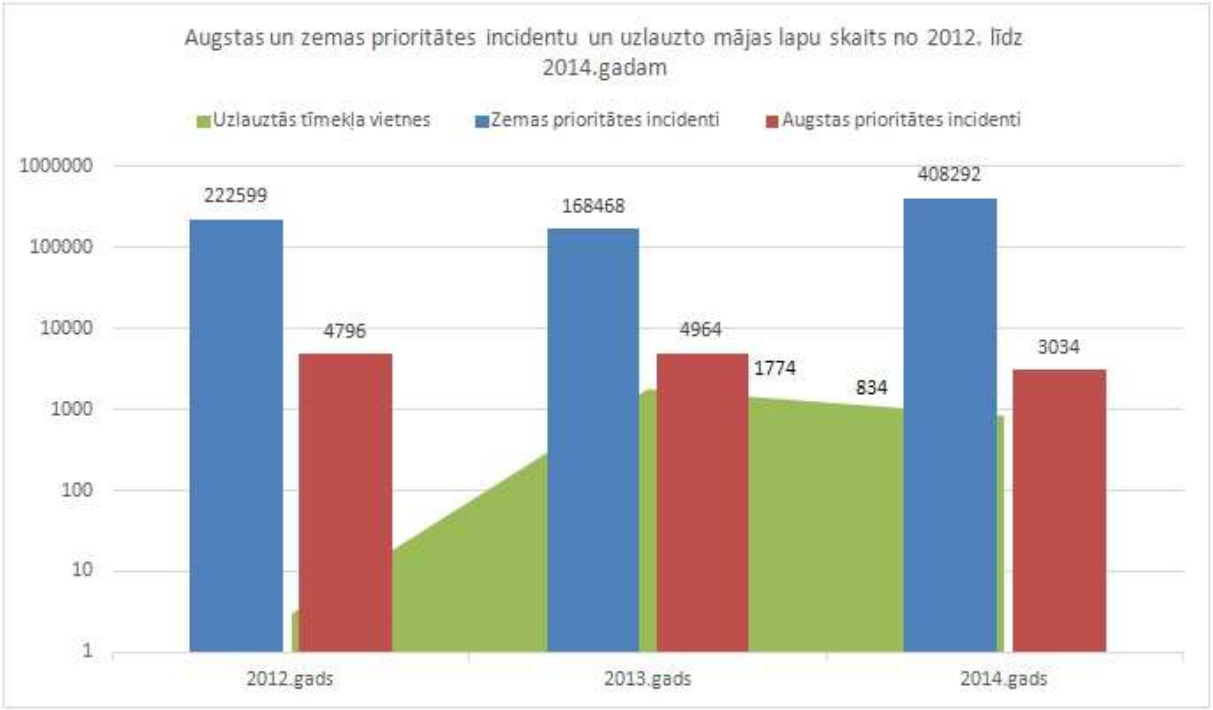
4.attēls - CERT.LV reģistrētie zemas prioritātes incidenti 2014.gadā pa apdraudējumu tipiem.

Izplatītāko apdraudējumu vidū līderpozīcijas saglabā Conficker vīruss. Aktuālas ir arī dažādas lietotāju datoru konfigurācijas kļūdas, trešais izplatītākais infekciju veids ir robotu tīkli (gala lietotāju iekārtās, kas nav augstas prioritātes incidenti).

Reģistrēto zemas prioritātes incidentu skaits 2014.gadā palielinājies, jo incidentu uzskaites sistēmas maiņas dēļ vairāki incidentu veidi tiek apstrādāti automātiski. Zemas prioritātes incidentu skaits sākot ar jūniju pieauga arī dēļ sadarbības partneru skaita pieauguma, kas regulāri sūta informāciju par inficētām iekārtām un notikušajiem incidentiem.



5.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem.



6. attēls – Augstas un zemas prioritātes incidentu un uzlauzto mājas lapu skaits no 2012*.gada līdz 2014.gadam.

CERT.LV uzskaita uzlauzto un izķēmoto mājaslapu gadījumus. 2014.gadā tika uzlauztas un izķēmotas 834 mājaslapas. 2013.gadā CERT.LV konstatēja 1744 izķēmotas mājas lapas.

*2012.gadā uzlauztās mājas lapas netika uzskaitītas.

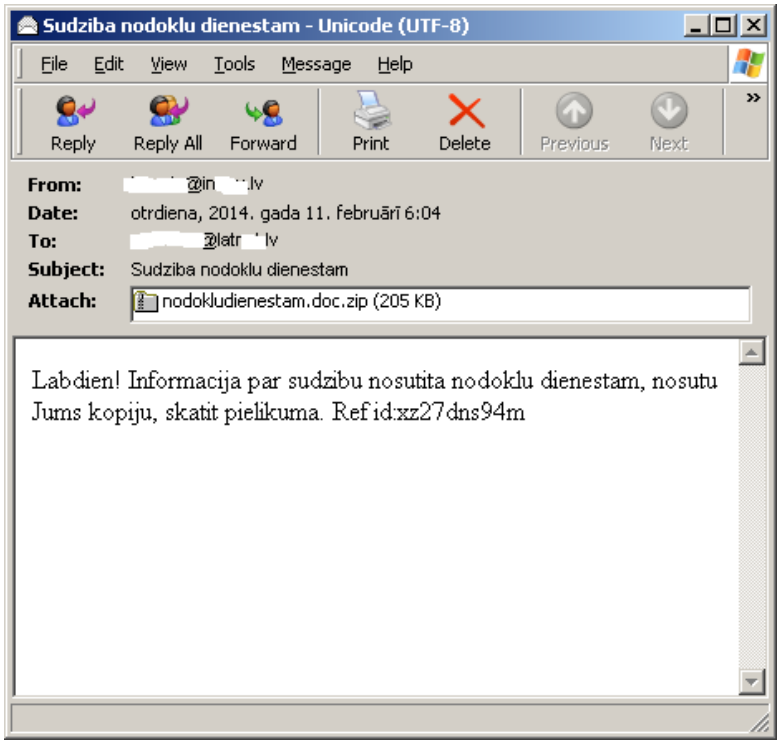
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

Pārskata periodā CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā. Uzbrukuma kampaņas pārsvarā bija mērķētas uz e-pasta un internetbanku lietotājiem, kā arī valsts un pašvaldību iestādēm.

Zemāk uzskaitīti 2014.gada svarīgākie incidenti:

- Latvijas kompromitētie resursi tika iesaistīti dažādās haktīvistu kustības kampaņās. Haktīvistu aktivitātes bija vērojamas gan prokrieviskā, gan Ukrainas krīzes kontekstā. Kā piemērs jāmin grupējums Kiberberkut, kas uzbruka arī NATO tīmekļa resursiem.
- Nezināmi aktīvisti jeb tā dēvētie „interneta troļļi" periodiski veica aktīvu komentāru ievietošanu ziņu portālos, ar mērķi kurināt naidu starp latviski runājošo un krieviski runājošo sabiedrības daļu. Visdrīzāk šādu komentāru aprite tiek veidota automatizēti. Līdzīgi gadījumi par organizētu sabiedriskā viedokļa kropļošanu prokrieviskā virzienā konstatēti arī Lietuvā.
- Gada pirmajos mēnešos e-pastos tika masveidā izsūtīts Zeus saimes datorvīruss jeb tā dēvētais „VID vīruss". Vēstules tematā tika norādīta saistība ar Valsts ieņēmumu dienestu. Vēstule saturēja ar datorvīrusu inficētus failus, kurš domāts tiešsaistes banku maksājumu pārtveršanai un modifikācijai.

  Vēstules paraugs:



- Janvārī Latvijā izplatījās paroļu zagšanas vīruss. Inficējot datoru, tas tālāk inficēja jebkuru noņemamu disku, kas tika pieslēgts inficētajam datoram, inficējot apmēram 500 iekārtu. Vīruss izplatījās ar e-pasta vēstuļu palīdzību, kas saturēja 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.
- Aprīļa sākumā tika izziņota OpenSSL ievainojamība jeb tā dēvētā „Heartbleed" ievainojamība, kura padarīja iespējamu piekļuvi informācijai servera atmiņāIzmantojot šo ievainojamību, bija iespējams attālināti no servera iegūt lietotāju paroles un lietotājvārdus, transakciju datus, konfigurācijas detaļas, e-pasta sistēmu lietotāju datus un citu sensitīvu informāciju. Ievainojamība skāra miljoniem serverus visā pasaulē. CERT.LV aktīvi strādāja pie Latvijas resursu turētāju apzināšanas un informēšanas. Sākotnēji ievainojamībai Latvijā tika pakļautas vismaz 1300 vietnes.
- Aprīlī CERT.LV publicēja pārskatu par ievainojamību OpenX baneru apmaiņas sistēmā. Izmantojot šo ievainojamību, caur vairākiem Latvijas portāliem tika izplatīts bīstamais „Gozi" banku trojāns.
- 3. ceturksnī notika e-pasta datu izkrāpšanas kampaņa ar mēstuļu palīdzību, uzdodoties par pakalpojumu sniedzēju „LATNET serviss" vai portālu latvija.lv. Uzbrukumu mērķis bija izkrāpt e-pasta lietotāju datus. Mēstules saņēma vairāki tūkstoši interneta lietotāji, tostarp arī valsts un pašvaldību iestādēs strādājošie. CERT.LV informēja sabiedrību un valsts un pašvaldību iestādes, kā arī veica incidenta monitoringu, lai identificētu un novērstu datu zādzības iespējas valsts pārvaldes iestādēs.

  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

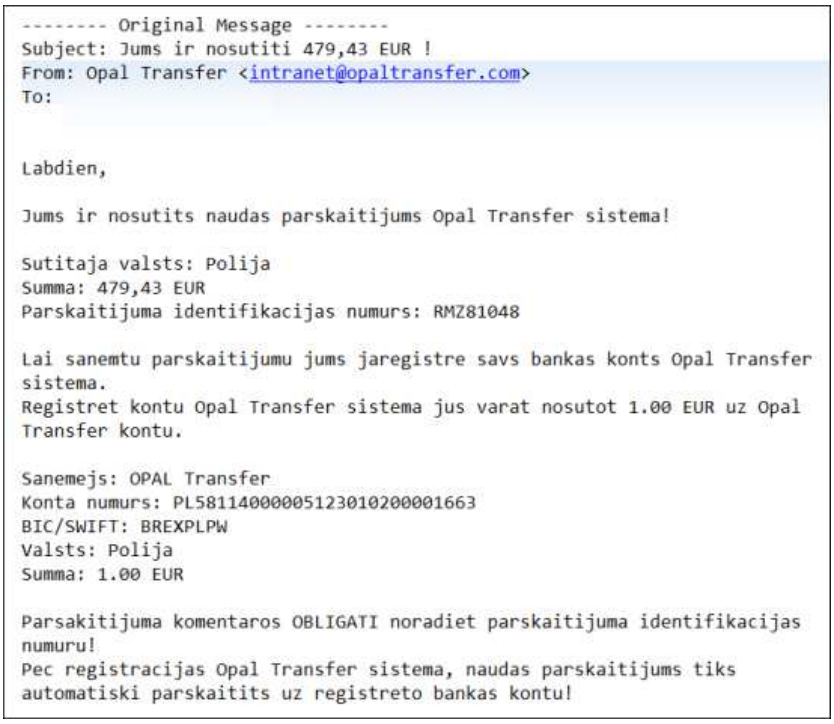
Lai izvairitos no jebkadiem partraukumiem, ludzu noklikskiniet uz saites zemak, un uzlabot savu e-pastu

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

Sirsnigi
Klientu Help Desk

- Augustā notika „Zeus" trojāna izplatīšanas kampaņa - lietotāji masveidā saņēma e-pastu ar tekstu "my new photo :)" un photo.zip failu pielikumā, kas saturēja photo.exe izpildāmo failu, kuram tika nomainīta ikona, lai maldinātu lietotāju domāt, ka pielikumā pievienota bilde.
- Augusta beigās masveidā tika izplatīti e-pasti ar mēģinājumu izkrāpt naudu uzņēmuma Opal Transfer vārdā. Vēstulē tika aicināts reģistrēt bankas kontu, veicot pārskaitījumu uz Poliju viena eiro apmērā.

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!
```

- Septembra beigās kļuva zināma Linux un OS X operētājsistēmās atrodamā *bash* ievainojamība „shellshock", kas atsevišķos gadījumos ļāva uzbrucējam attālināti izpildīt patvaļīgu kodu. Ievainojamībai tika pakļauta arī daļa Latvijas tīmekļa serveru.
- Novembra beigās un decembra sākumā vairākiem simtiem e-pasta lietotāju Latvijā tika kompromitēts Gmail e-pasta konts. No kompromitētā e-pasta tika izsūtītas mēstules lietotāja adrešu grāmatai ar aicinājumu pārskaitīt naudu, jo lietotājam ārzemēs nozagti dokumenti un bankas kartes. Kontu kompromitēšana notika, lietotājam nospiežot uz saites, kura ieveda lietotāju viltus Gmail lapā, lai izkrāptu Gmail paroles. CERT.LV aicināja sabiedrību pārbaudīt vietnes adresi, pirms ievadīt tajā e-pasta paroli, kā arī izveidoja rekomendācijas, kā rīkoties, lai atgūtu nozagtu Google kontu.
- Novembrī Latvijā parādījās failu šifrēšanas datorvīruss „CTB Locker", kas sašifrē lietotāja datorā esošos dokumentus, par atšifrēšanu prasot izpirkumu. Gada beigās vīruss izplatījās caur leģitīmām interneta vietnēm, lietotāja dators tika inficēts automātiski, ļaunatūrai atrodot izmantojamas Java, Adobe Flash spraudņu, kā arī citas interneta pārlūka ievainojamības.
- Decembrī pieauga krāpnieciskas aktivitātes internetā, pārsvarā ar mērķi izkrāpt naudas līdzekļus. Aktivizējās pikšķerēšana ar mērķi izvilināt banku datus, parādījās pagājušajā gadā aktuālais policijas vīruss un parādījās mēstules ar viltus rēķiniem un viltus loteriju laimestu paziņojumiem.

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. Kopā CERT.LV lapai bijuši 119416 unikāli apmeklējumi.

Pārskata periodā CERT.LV tīmekļa vietnē tika publicētas 152 ziņas, tika sniegta informācija par CERT.LV organizētiem un starptautiska mēroga pasākumiem, publicētas CERT.LV prezentācijas, mediju ziņas un CERT.LV publiskie darbības pārskati.

Gada laikā būtiski pieaudzis gan CERT.LV mājas lapas apmeklējumu skaits, gan sekotāju skaits sociālajos tīklos twitter, Facebook un Draugiem.lv. Aktivitāti var izskaidrot gan ar lielo pasākumu skaitu, gan mediju pieaugošo interesi par kiberdrošības tematu.

CERT.LV uztur arī pieaugušo izglītošanas portālu https://www.esidross.lv. Pārskata perioda laikā portālā publicēti 14 jauni raksti.

Martā CERT.LV 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

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

Gada nogalē CERT.LV sadarbībā ar Latvijas Nebanku kredītdevēju asociāciju CERT.LV iesaistījās izglītojošā kampaņā „Datu drošība internetā", par iedzīvotāju droša interneta lietošanas pamatiem, veicot finanšu darījumus.

Pārskata periodā CERT.LV pārstāvji piedalījās 17 radio pārraidēs un 24 televīzijas sižetos, lai informētu sabiedrību par aktuālākajiem apdraudējumiem, sniegtu rekomendācijas kā no tiem izvairīties un popularizētu CERT.LV organizētos pasākumus.

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

2014.gadā CERT.LV turpināja dažādu mērķa grupu izglītošanu par drošības jautājumiem. IT speciālistiem tika organizēti vairāki semināri - „IT drošība skolā" (divas reizes, informātikas skolotājiem), kā arī seminārs „IT drošības vizualizācija" IT drošības speciālistiem. Pavasarī lielākais pasākums bija CERT.LV organizētais seminārs „Esi drošs 2" IT drošības speciālistiem, kuru apmeklēja 157 personas.

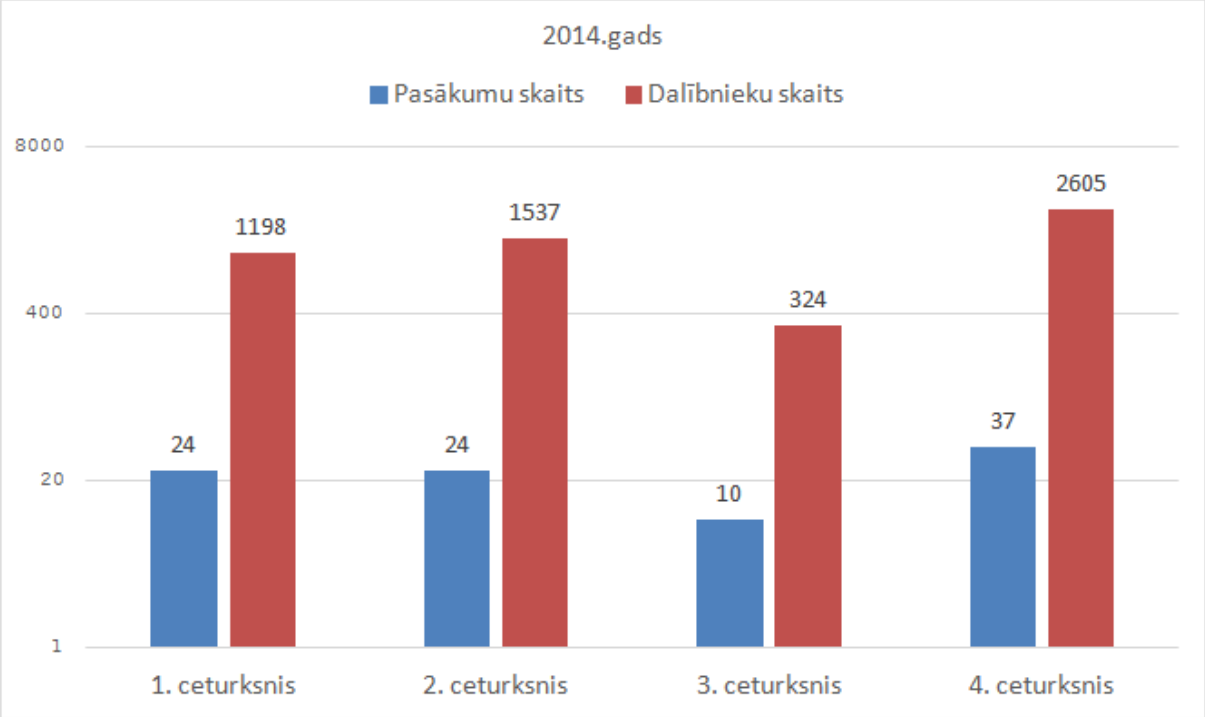
Lielu dalībnieku atsaucību guva arī mācības IT drošības speciālistiem „Ievads datora atmiņas ļaunprātīgā izmantošanā", kuras dalībnieku intereses dēļ tika rīkotas divas reizes, aprīlī un novembrī. No 9. līdz 10.jūlijam notika CERT.LV un ENISA organizētais seminārs IT drošības speciālistiem "Elektronisko pierādījumu identificēšana un izmantošana digitālajā ekspertīzē".

No 24. līdz 30.martam CERT.LV iesaistījās E-prasmju nedēļas kampaņā, kuras laikā notika vairāki izglītojoši pasākumi, ieskaitot Datorologa akciju 26. martā.
Otra lielākā izglītojošā kampaņa bija Eiropas kiberdrošības mēnesis, kura ietvaros notika IT drošības konference, seminārs valsts un pašvaldību darbiniekiem "IT drošības risku mazināšana ES prezidentūras laikā" un datorologa akcija.

CERT.LV izglītoja arī valsts un pašvaldības iestāžu darbiniekus par IT drošības jautājumiem, vadot lekcijas un prezentācijas, kā arī sniedza prezentācijas skolēniem un studentiem par IT drošību. 2014.gadā CERT.LV uzstājās ar lekcijām studentiem Latvijas Universitātē, Vidzemes augstskolā un Rīgas Tehniskajā universitātē.
CERT.LV piedalījās ar prezentācijām un lekcijām dažādos sadarbības partneru pasākumos – konferencēs, semināros un publiskajās diskusijās.

Gada lielākais pasākums bija IT drošības konference "Apmācīts un atbildīgs IS/IT lietotājs – mūsu visu drošības pamats", kas notika 16.oktobrī Latvijas Nacionālajā bibliotēkā. Konferencē uzstājās Latvijas IT nozares eksperti un ārvalstu lektori par tādām tēmām kā interneta atvērtības riski, informācijas drošības riski un izaicinājumi, web aplikāciju drošības uzlabošanas iespējas, kiberdrošības kompetenču pilnveide, domēnu vārdu sistēmas problēmas un risinājumi, ievainojamību atklāšana u.c. Konferenci noslēdza valsts un privātā sektora ekspertu paneļdiskusija par to, kā vislabāk paaugstināt galalietotāju informācijas drošības prasmes. Konferencē piedalījās 395 dalībnieki.

Kopā pārskata periodā CERT.LV par IT drošību tika izglītoti 5664 cilvēki, piedaloties 95 dažādos pasākumos. Lielākā auditorija bija valsts un pašvaldību iestāžu darbinieki.



6.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits 2014.gadā.

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

CERT.LV sniedza ieguldījumu gatavojoties Latvijas prezidentūrai ES, piedaloties Latvijas prezidentūras Eiropas Savienības Padomē sekretariāta organizētās sanāksmēs par informācijas sistēmu vides plānošanu un drošības prasību definēšanu, kā arī konsultēja sekretariātu par drošības risinājumiem informācijas sistēmām, kas paredzētas lietošanai ES Prezidentūras laikā.

CERT.LV novadīja semināru "IT drošības risku mazināšana pirms ES prezidentūras", kā arī izstrādāja „Informācijas tehnoloģiju drošības rekomendācijas valsts un pašvaldību iestādēm", gatavojoties ES Prezidentūrai.

2014.gadā CERT.LV uzsāka veidot agrās brīdināšanas sistēmu jeb sensoru tīkla projektu. Valsts iestādēm tika piedāvāts izvietot iekārtu, kura nodrošinātu iestādes IT resursu augstāku drošības līmeni un savlaicīgi atklātu bīstamus un mērķētus informācijas tehnoloģiju uzbrukumus un uzlabotu iestāžu preventīvās spējas, paātrinot un veicinot bīstamu incidentu novēršanu un laicīgu atrisināšanu.

CERT.LV veicināja sadarbību ar Zemessardzes Kiberaizsardzības vienību, gan kopīgi strādājot pie incidentu risināšanas, gan piedaloties mācībās, kā arī nodrošinot virtuālu treniņu vidi drošības incidentu risināšanas pilnveidei.

CERT.LV turpināja atbalstīt Drošības ekspertu grupas (DEG) darbību, kas nodrošina diskusiju forumu IT drošības speciālistiem gan no privātā, gan valsts sektora. DEG sanāksmes notika regulāri reizi mēnesī.

CERT.LV 2014.gadā piedalījās arī dažādu darba grupu darbībā, likumprojektu izstrādē un sniedza konsultācijas IT drošības jautājumos dažādām valsts iestādēm.

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 31.decembrim CERT.LV ir apkopojis informāciju par 1379 kontaktpersonām, kuras atbildīgas par IT drošības pārvaldību.

Pārskata periodā CERT.LV regulāri informēja valsts un pašvaldību iestāžu atbildīgās personas par aktuālajiem drošības apdraudējumiem.

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. CERT.LV ir izstrādājis rīcības plāna paraugu, lai palīdzētu mazajiem ESK izveidot savus plānus, un izsūtījis informāciju par šo paraugu tiem ESK, kuri līdz šim nav izstrādājuši un iesnieguši CERT.LV rīcības plānu elektronisko sakaru tīkla nepārtrauktas darbības nodrošināšanai. Saistībā ar rīcības plāniem saņemtas atbildes no 63 ESK. Līdz 31.decembrim saņemti 58 ESK rīcības plāni, kā arī 5 ESK rakstiski apliecinājuši, ka neuztur publisko elektronisko sakaru tīklu, no kuriem 1 ESK nodevis visu ārpakalpojumā citam ESK.

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 ar citās valstīs notikušu incidentu risināšanu, gan arī kopīgi uzlabojot incidentu risināšanas metodoloģiju, rīkus un procedūras.

CERT.LV aktīvi piedalījās dažādās starptautiskās konferencēs un semināros, sniedzot prezentācijas, kā arī papildināja darbinieku zināšanas un uzlaboja sadarbību ar citu valstu CERT vienībām.

Pārskata periodā notika aktīva sadarbība ar partnerorganzācijām kiberdrošības mācību jomā. No 20. līdz 22.maijam CERT.LV un Kiberaizsardzības vienība Latvijas-Čehijas apvienotās komandas sastāvā piedalījās NATO Kiberaizsardzības izcilības centra organizētajās „Locked Shields 2014" mācībās un ieguva 2.vietu. Mācībās piedalījās 12 aizsargkomandas no visas Eiropas.

No 28. līdz 30.aprīlim notika ENISA organizēto mācību „Cyber Europe 2014" pirmais, tehniskais posms. No Latvijas piedalījās aptuveni 30 dalībnieki no Kiberaizsardzības vienības, CERT.LV, SIA "BITI" un AS "Latvenergo".

No 29. līdz 31.oktobrim notika ENISA organizēto mācību „Cyber Europe 2014" 2. posms. Mācību mērķis bija testēt sadarbību Eiropas ietvaros liela apjoma enerģētikas sektora kiberkrīzes gadījumā. No Latvijas mācībās piedalījās CERT.LV, Kiberaizsardzības vienība un AS „Latvenergo". Mācību noslēdzošais posms notiks 2015.gada februārī.

TF-CSIRT 43. sanāksmes laikā, kas notika 2014.gada 18. un 19.septembrī Romā, par TF-CSIRT grupas priekšsēdētāju tika ievēlēta CERT.LV vadītāja Baiba Kaškina. TF-CSIRT („Task Force Of Computer Security Incident Response Teams") ir darba grupa, kas Eiropas mērogā vieno drošības incidentu risināšanas komandās strādājošos speciālistus. TF-CSIRT darba grupa izstrādā un nodrošina CSIRT komandas ar servisiem, veicina kopīgu standartu un procedūru izmantošanu drošības incidentu apstrādē, kā arī nepieciešamības gadījumā koordinē kopīgas iniciatīvas.

Sīkāka informācija par CERT.LV uzdevumu izpildi pieejama CERT.LV mājaslapā: https://cert.lv/section/show/48

Atskaiti sagatavoja Svetlana Amberga, tālrunis 67085851, e-pasts svetlana.amberga@cert.lv

2015.gada 17.februārī