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 4. ceturksnis (01.10.2014. – 31.12.2014.)

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 Gmail pikšķerēšanas kampaņa, no kuras cieta vairāki simti e-pasta lietotāju Latvijā. Uzbrucēji uzdevās par Gmail servisu, lai izkrāptu e-pasta lietotāju datus.

Decembrī krasi pieauga krāpnieciskas aktivitātes internetā, pārsvarā ar mērķi izkrāpt naudas līdzekļus. Aktivizējās pikšķerēšana ar mērķi izvilināt banku datus, parādījās pagājušajā gadā aktuālais policijas vīruss, tāpat pieauga izsūtīto mēstuļu daudzums. Parādījās tipiskās gada nogales mēstules, piemēram, viltus rēķini un viltus loteriju laimestu paziņojumi.

Kā viens no lietotājiem nepatīkamākajiem uzbrukuma veidiem jāmin novembra beigās parādījies failu šifrēšanas datorvīruss CTB Locker, kas sašifrē visus lietotāja datorā esošos dokumentus, par atšifrēšanu prasot izpirkuma maksu. Datora inficēšanās ar ļaunatūru notika, apmeklējot leģitīmas interneta vietnes. Lai inficētos, interneta lietotājam nebija jāveic nekādas papildu darbības. Dators tika inficēts automātiski, ļaunatūrai atrodot izmantojamas Java, Adobe Flash spraudņu, kā arī citas interneta pārlūka ievainojamības.

Lai veicinātu sabiedrības izpratni par kiberdrošības jautājumiem, 2014.gada oktobris tika pasludināts par Eiropas kiberdrošības mēnesi. CERT.LV kiberdrošības mēneša ietvaros rīkoja pasākumus gan sabiedrībai, gan IT drošības profesionāļiem, gan valsts un pašvaldību iestāžu darbiniekiem. Lielākais kiberdrošības mēneša pasākums bija IT drošības konference „Apmācīts un atbildīgs IT/IS lietotājs - mūsu visu drošības pamats", kas notika 16. oktobrī. Konferenci apmeklēja 395 dalībnieki.

Pārskata periodā CERT.LV reģistrēja un apstrādāja **894** augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēts un apstrādāts 651 augstas prioritātes incidents, bet 2013.gada 4.ceturksnī - 1213 augstas prioritātes incidenti.

2014.gada tendence augstas prioritātes incidentu skaita samazinājumā neturpinājās. Incidentu skaita pieaugums skaidrojams ar interneta krāpnieku pirms svētku aktivitāti, izsūtot vairāk mēstules un radot pikšķerēšanas kampaņas, lai izvilinātu naudu no neuzmanīgiem lietotājiem.

2014.gada 4.ceturksnī CERT.LV reģistrēja **145 890** zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti 157 293 zemas prioritātes incidenti, bet 2013.gada 4.ceturksnī – 80 230 zemas prioritātes incidenti.

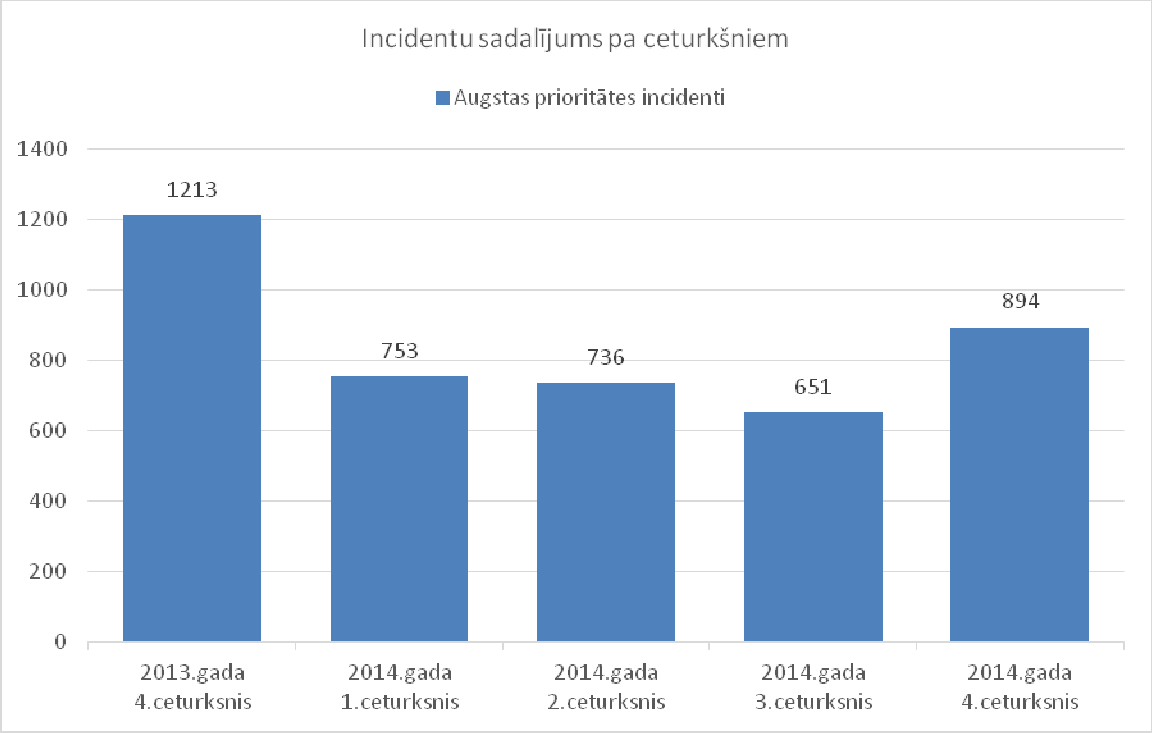
Lielāko sabiedrības un mediju uzmanību pārskata periodā izpelnījās Gmail pikšķerēšanas kampaņa. No mēstulēm ar lūgumu pārskaitīt naudu draugam, kas ārzemēs it kā nonācis finansu grūtībās, cieta vairāki simti cilvēku, tostarp arī sabiedrībā zināmas personas, kas veicināja notikušā publicitāti.

Kopā pārskata periodā CERT.LV piedalījās 37 pasākumos, apmācot 2605 cilvēkus, publicēja 57 jaunas ziņas portālā www.cert.lv, 3 jaunus rakstus portālā www.esidross.lv, piedalījās 5 radio pārraidēs un 11 televīzijas sižetos.

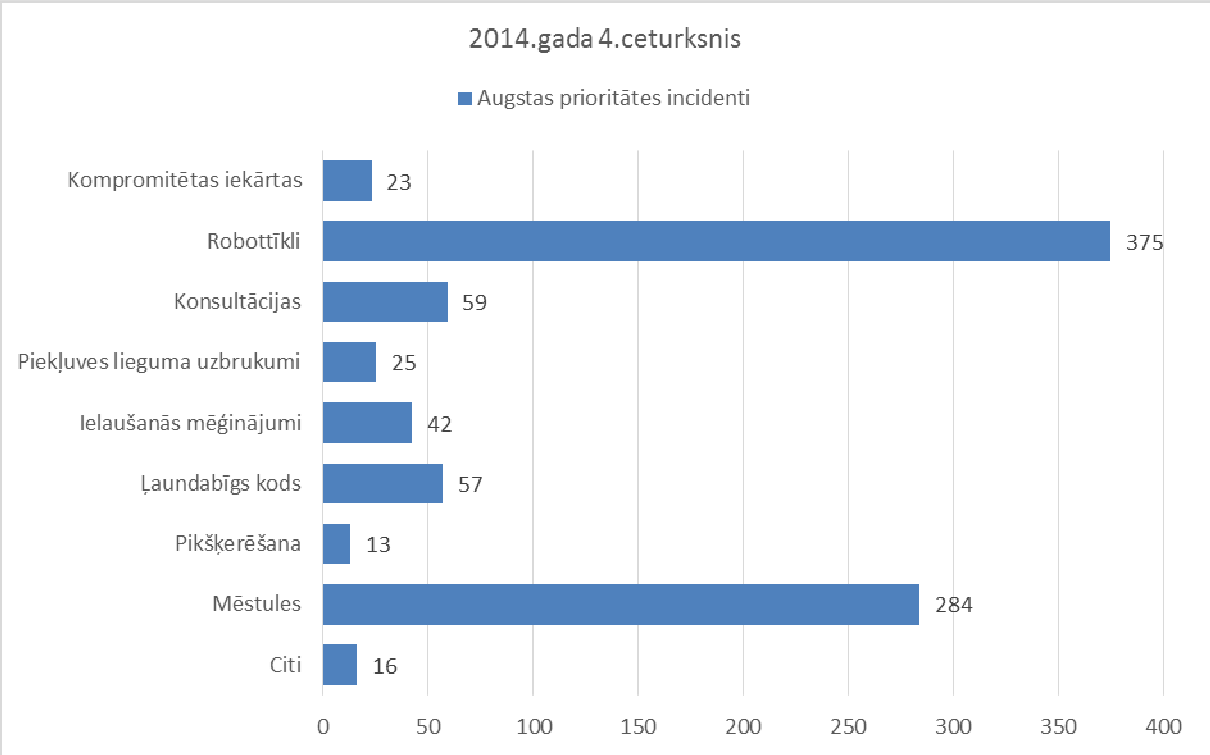
1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

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 ceturtajā ceturksnī CERT.LV apstrādāja 894 augstas prioritātes incidentus, kas ir par 243 incidentiem vairāk nekā 2014.gada trešajā ceturksnī un par 319 incidentiem mazāk nekā 2013.gada 4.ceturksnī.

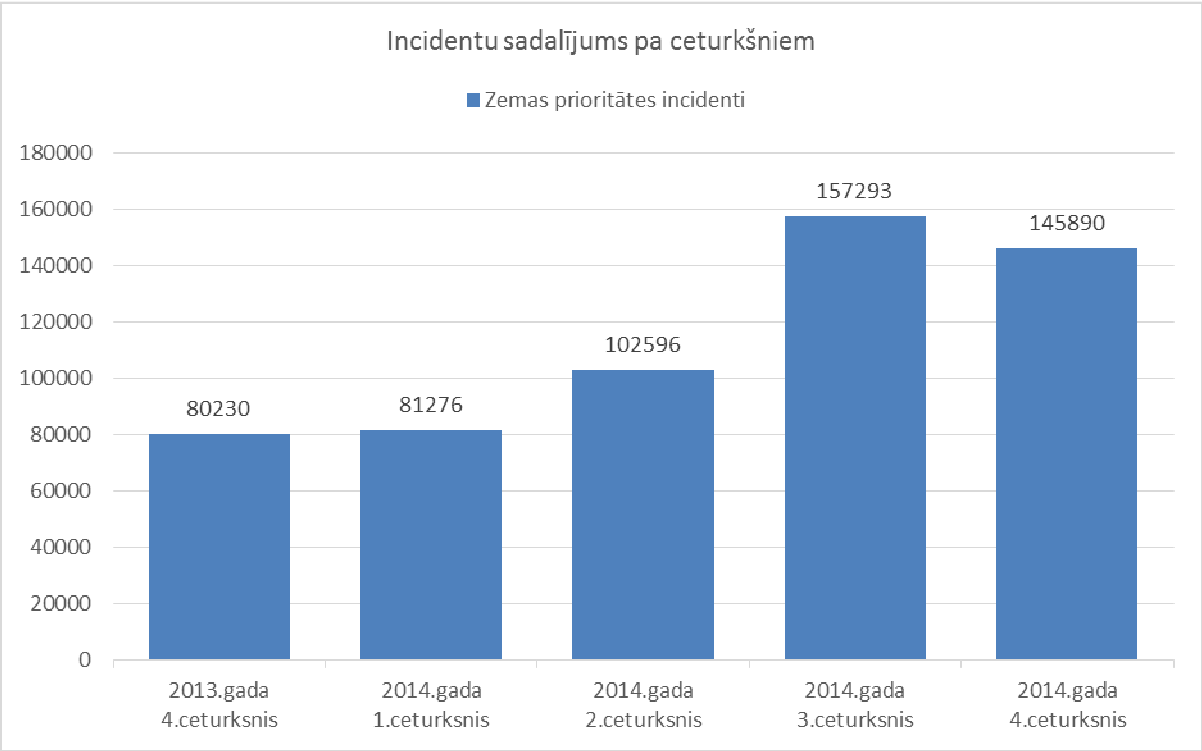


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2013. un 2014. gadā.

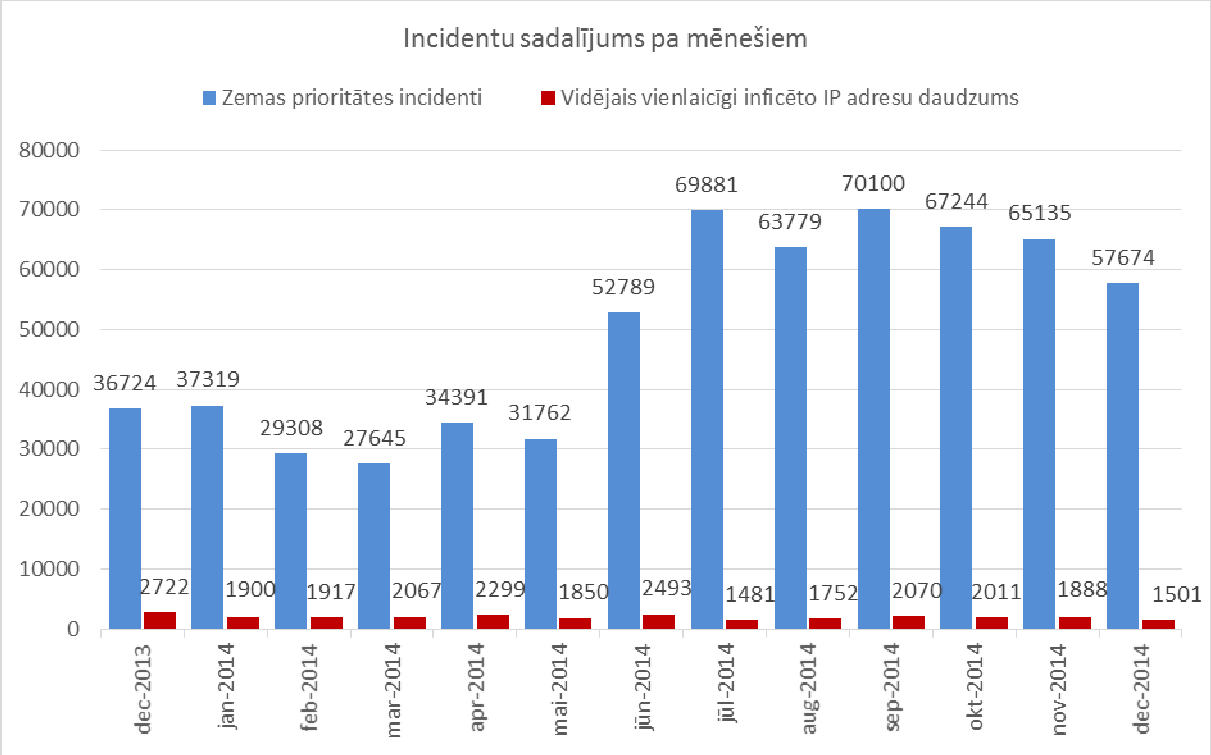


2.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem no 2014.gada 1.oktobra līdz 31.decembrim.

2014.gada 4.ceturksnī CERT.LV reģistrēja 145 890 zemas prioritātes incidentus, kas ir par 11 405 mazāk nekā 2014. gada 3. ceturksnī un par 65 660 incidentiem vairāk, nekā 2013.gada 4.ceturksnī.



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



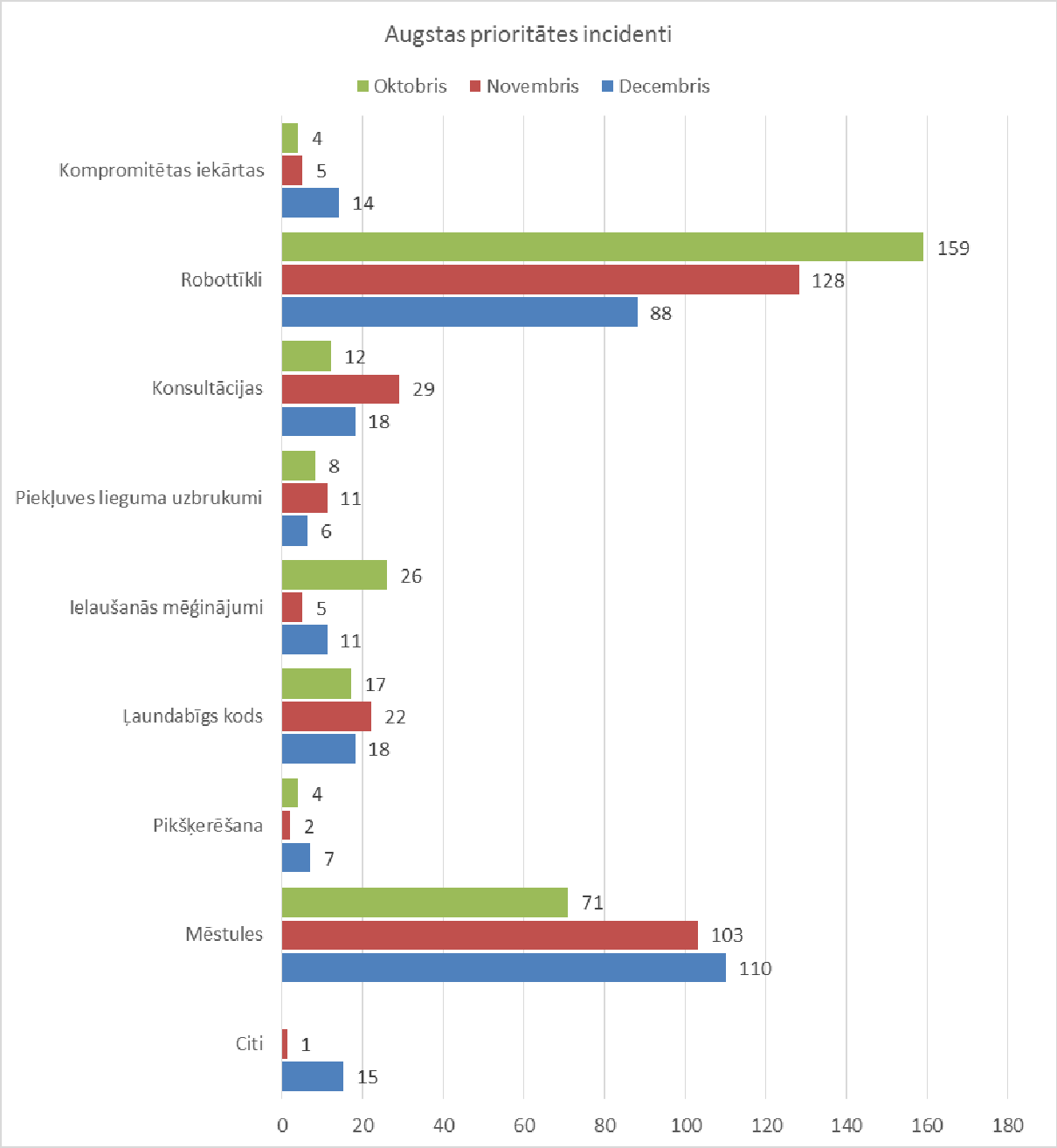
4.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi inficēto IP adrešu daudzums pa mēnešiem.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi inficēto unikālo IP adrešu skaitu Latvijā. Oktobrī šis skaits bija 2011, novembrī – 1888, savukārt decembrī – 1501 inficētas IP adreses.

Lai samazinātu kopējo inficēto IP adrešu skaitu, CERT.LV kopā ar „Net-Safe Latvija" 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.

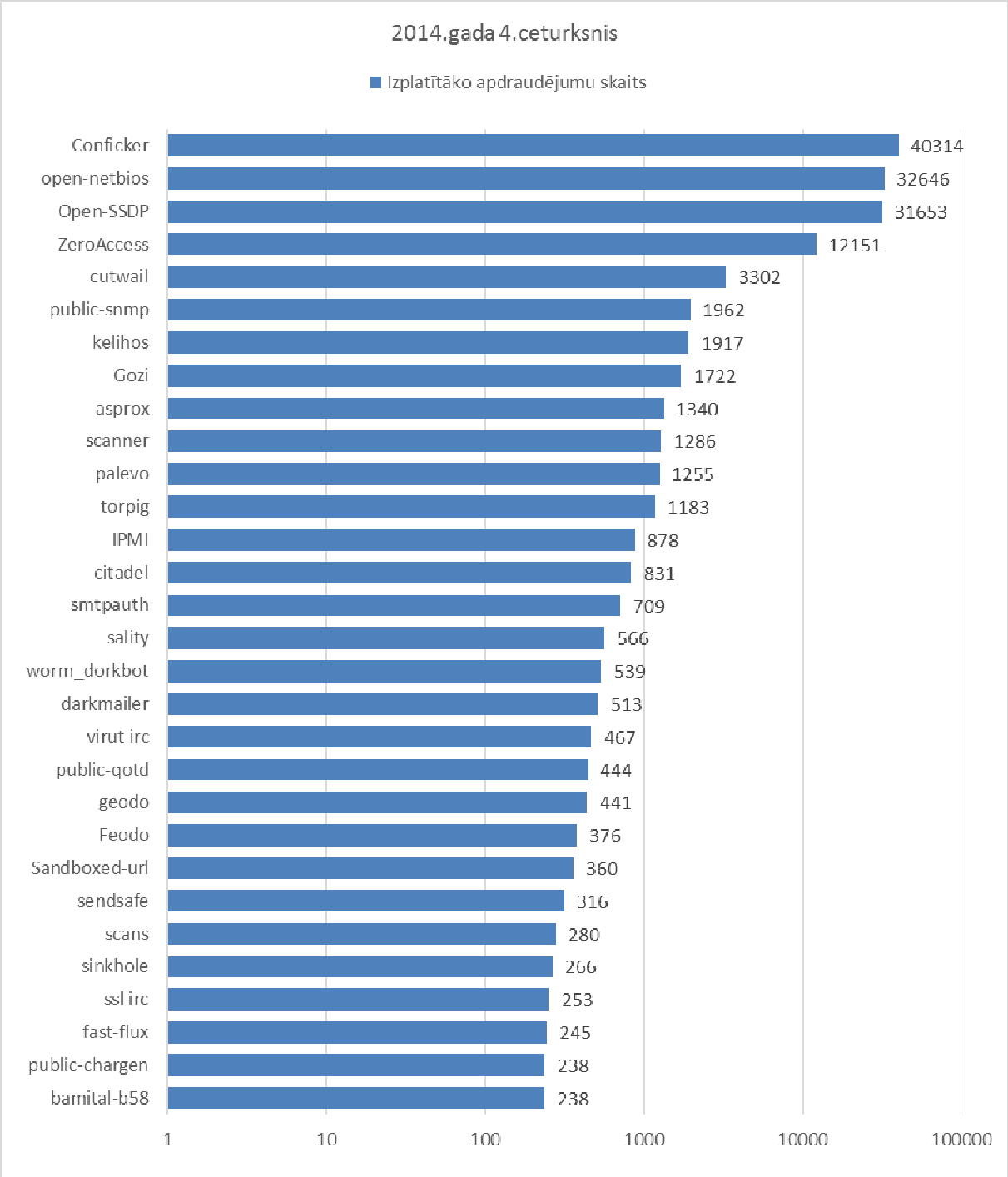
Pārskata periodā CERT.LV ir reģistrējis un apstrādājis 894 augstas prioritātes incidentus. Augstas prioritātes incidentu sadalījums pa tipiem un pa mēnešiem redzams 6.attēlā.



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

Attiecībā pret iepriekšējo periodu ir pieaudzis robotu tīklu skaits. Tas skaidrojams ar CERT.LV veikto robotu tīklu komandu un kontroles centru analīzi un iegūto datu apstrādi. Pieaug lietotāju skaits, kuru datoriem ir labas kvalitātes interneta pieslēgumi, taču nav adekvāta aizsardzība.

Pārskata periodā CERT.LV reģistrēja 145 890 zemas prioritātes incidentus. Izplatītākā infekcija joprojām ir Conficker, par kuru CERT.LV speciālisti regulāri sniedz konsultācijas, kā no tā atbrīvoties, jo antivīrusa risinājumi ne vienmēr palīdz vai arī darbojas tikai īslaicīgi.



6.attēls - CERT.LV reģistrētie zemas prioritātes incidenti pārskata periodā no 2014.gada 1.oktobra līdz 31.decembrim pa apdraudējumu tipiem.

Pārskata periodā notika vairākas uzbrukuma kampaņas, kas bija mērķētas uz e-pasta un internetbanku lietotājiem, kā arī valsts un pašvaldību iestādēm.

Vairākiem simtiem e-pasta lietotāju tika kompromitēts Gmail e-pasta konts, no kura tika izsūtītas mēstules draugiem ar aicinājumu pārskaitīt naudu, jo lietotājam ārzemēs nozagti dokumenti un bankas kartes.

Visbiežāk pēc konta kompromitēšanas lietotājs nevarēja atgūt piekļuvi savam e-pastam, jo uzbrucēji bija kontu izdzēsuši. Sākotnēji lietotājiem tika izsūtīta mēstule ar aicinājumu nospiest uz saites.

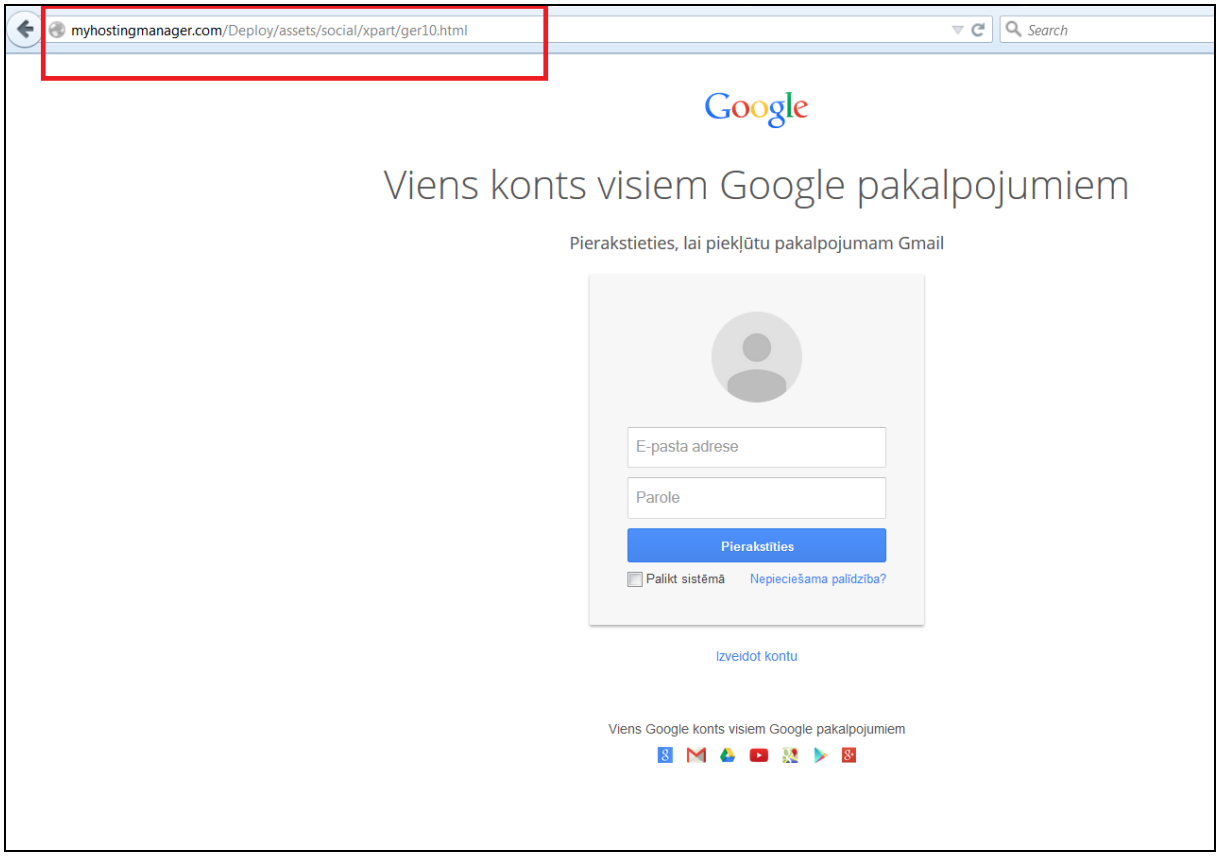
Vēstules paraugs:

---------- Pārsūtītais ziņojums ----------
No: <noreply@account.user.com>
Datums: 2014. gada 9. decembris 21:14
Temats: Noreply
Kam:

Dārgie lietotājs

Divi saņemtās ziņas tiek saglabātas līdz dēļ nesen atjauninātо mūsu datu bāzē, lai saņemtu ziņas no klikšķiniet šeit <http://way.to/ggpt445
Piereģistrēties un gaidīt atbildi. Mēs atvainojamies par sagādātajām neērtībām un pateicamies par jūsu sapratni.

Nospiežot uz saites, lietotājs nonāk viltotā Gmail lapā. Ievadot lapā paroles, tās nonāk krāpnieku rīcībā.



CERT.LV aicināja lietotājus pārbaudīt vietnes adresi, pirms ievadīt tajā e-pasta paroli, kā arī izveidoja rekomendācijas, kā rīkoties, lai atgūtu nozagtu Google kontu.

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:

- 03.10. No Facebook lietotāja tika mēģināts izspiest naudu par viltota privāta video neizplatīšanu. Tika sniegta konsultācija, kā atgūt kontroli pār Facebook un Gmail kontiem.
- 12.10. CERT.LV sagatavoja pētījumu par Latvijas interneta apmaiņas punkta LIX drošības trūkumiem un sekmīgu ielaušanos galvenajos tīkla maršrutētājos. Pētījuma rezultāti tika demonstrēti IT drošības konferencē 16.oktobrī. Informācija par identificētajiem drošības trūkumiem tika nosūtīta LIX dalībniekiem, trūkumi tika novērsti līdz konferencei.
- 13.10. CERT.LV saņēma palīdzības lūgumu no citas valsts CERT, lai mazinātu pret valsti vērsta DDoS uzbrukuma ietekmi. CERT.LV brīdināja uzbrukumā iesaistīto Latvijas IP adrešu īpašniekus.
- 15.10. Tika sniegta palīdzība identificēt kādas iestādes tīklā kļūdaini konfigurētas iekārtas, kas varētu tik izmantotas DDoS uzbrukumiem.
- 24.10. CERT.LV saņēma informāciju, ka uzlauzta kādas biedrības mājaslapa.

- 26.10. Masveidā tika izplatītas krāpnieciskas vēstules ar aicinājumu ziedot kādai fiktīvai privātpersonai. CERT.LV sazinājās ar krāpniecisko lapu uzturošā servera īpašniekiem, lapa tika slēgta.
- 28.10. Tika konstatēts zema riska drošības trūkums kādas valsts iestādes vietnē. Par faktu informēts atbildīgais.
- 2014.gada oktobrī un novembrī tika konstatēti vairāki DNS amplifikācijas uzbrukumi, kuros iesaistīti Latvijas resursi (nedroši konfigurēti DNS serveri - "open resolvers"). Analīze atklāja, ka uzbrukuma mērķi ir bijuši vairāki DNS zonas serveri datorspēļu organizācijām Ķīnā, kā arī Izraēlas valsts resursi. Uzbrukumos iesaistītās adreses tika apzinātas un gala lietotāji tika informēti ar "Atbildīgs IPS" iniciatīvas starpniecību.
- 29.10. CERT.LV identificēja uzbrukumu kampaņu, kuras mērķu vidū bija vairākas valsts iestādes Latvijā.
- 02.11. CERT.LV saņēma informāciju par vairākām inficētām Latvijas uzņēmumu mājaslapām, kuru apmeklētāji tika inficēti ar datorvīrusu. Īpašnieki tika brīdināti, lapas iztīrītas.
- 03.11. Vairākās Latvijas internetbankās atklāta iespēja autentificēties ar e-parakstu, kam beidzies derīguma termiņš. Bankas tika brīdinātas.
- 11.11. Tika saņemta informācija par privātpersonas datu nelikumīgu izvietošanu internetā. Servera turētājs tika brīdināts, dati izdzēsti.
- 12.11. Latvijā tika intensīvi izplatīti datorvīrusu Win32/Kryptik.CQBI saturoši e-pasti. CERT.LV brīdināja atbildīgās personas.
- 14.11. CERT.LV veica kādas iestādes darbinieka iekārtas analīzi, kas inficēta ar „policijas vīrusu". Kaitnieciskais saturs tika likvidēts, sniegtas preventīvo darbību instrukcijas.
- 26.11. Notika apjomīgs DDoS uzbrukums kāda uzņēmuma infrastruktūras serveriem. Uzbrukums tika novērsts sadarbībā ar interneta pakalpojumu sniedzēju.
- 27.11. CERT.LV atklāja vairākus robotu tīklu kontrolserverus Latvijā. Tika uzsākts darbs pie incidentu analīzes un piesaistīta Valsts policija.
- 01.12. Tika izsūtītas viltus vēstules degvielas tirgotāja Lukoil Latvija vārdā, ar mērķi iegūt personu datus.
- 02.12. CERT.LV konsultēja Valsts policijas pārstāvi par identificēto, kaitniecisko darbību no vairākām Latvijas IP adresēm, kas piedalījušās prettiesiskās darbībās ar mērķi gūt finansiālu labumu, izkrāpjot informāciju.
- 02.12. CERT.LV konstatēja, ka dēļ ievainojamības novecojušā WordPress satura vadības sistēmā atkārtoti kompromitēta kāda sabiedrībā pazīstama cilvēka tīmekļa vietne. Tika informēta atbildīgā persona un sniegtas rekomendācijas preventīvo mehānismu ieviešanai.
- 08.12. Daudziem iedzīvotājiem izkrāptas Gmail e-pasta kontu paroles. Izkrāptie konti tika izmantoti mēstuļu sūtīšanai upuru kontaktpersonām, tādējādi mēģinot izkrāpt naudu.

- 10.12. Vairāku iedzīvotāju datori tika inficēti ar bīstamo CTB locker datorvīrusu, kas šifrē datoros pieejamo informāciju un pieprasa izpirkumu par failu atbloķēšanu. Vīruss tiek izplatīts, izmantojot reklāmas banerus inficētās vietnēs.
- 10.12. Kādas iestādes tīkls cieta no DDoS uzbrukuma. Datortīkla administratori tika konsultēti par nepieciešamajām izmaiņām maršrutētājos, kas ļauj ierobežot uzbrukuma ietekmi.
- 10.12. CERT.LV identificēja robotu tīkla darbību, kura kontrolcentrs tiek uzturēts citā valstī. Uzsākta sadarbība ar attiecīgās valsts CERTa kolēģiem incidenta risināšanā.
- 15.12. CERT.LV veica incidenta risināšanas koordināciju, kurā identificēti drošības trūkumi European ATM Security Team (EAST) tīmekļa vietnē.

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

CERT.LV uzskaita arī uzlauzto un izķēmoto mājaslapu gadījumus. Šādu gadījumu skaits:
Oktobris: 32, no tiem Linux – 29, MacOSX – 3.
Novembris: 37, no tiem Linux – 35, FreeBSD – 1, Windows 2008 – 1.
Decembris: 102, no tiem Linux – 95, FreeBSD – 7.

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, 10 358 lapu skatījumi, tai seko ziņa par Windows atjauninājumu instalēšanu dēļ ievainojamības MS Microsoft Schannel ar 7891 apmeklējumiem. Trešā populārākā ziņa pārskata periodā bija informācija par IT drošības konferenci „Apmācīts un atbildīgs IT/IS lietotājs - mūsu visu drošības pamats" ar 2273 lapu skatījumiem pārskata periodā.

Kopā CERT.LV mājaslapai bijuši 70 048 lapu skatījumi, kurus veido 56 344 unikāli lapu skatījumi no 94 valstīm. Lielākā daļa - 93% apmeklējumu bija no Latvijas.

Pārskata periodā CERT.LV tīmekļa vietnē tika publicētas 57 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 3. ceturksni.

CERT.LV Twitter kontā https://twitter.com/certlv pārskata periodā tika publicētas 78 ziņas, kontam pievienojušies 132 jauni sekotāji un 189 reizes @certlv ziņa tikusi „retvītota" jeb padota tālāk.

Būtiski pieaudzis gan CERT.LV mājas lapas apmeklējumu skaits, gan sekotāju skaits sociālajos tīklos. Aktivitāti var izskaidrot gan ar lielo pasākumu skaitu, gan mediju pieaugošo interesi par kiberdrošības tematu.

CERT.LV izveidots profils arī sociālajā tīklā Facebook http://www.facebook.com/certlv (pārskata periodā publicētas 57 ziņas) un profils sociālajā tīklā Google+ https://www.google.com/+CertLv (publicētas 57 ziņas), kā arī lapa draugiem.lv - http://www.draugiem.lv/certlv, kurā publicētas 78 ziņas.

CERT.LV uztur arī pieaugušo izglītošanas portālu https://www.esidross.lv. Pārskata perioda laikā portālā ir publicēti 3 jauni raksti, portālam bija 18 581 jauni skatījumi, no tiem 13 792 unikāli lapu skatījumi.

Publicētie raksti:

- "Mobilo iekārtu drošība – padomi lietotājiem". https://www.esidross.lv/2014/10/31/mobilo-iekartu-drosiba-padomi-lietotajiem/
  "Virtuālā izmeklēšana, reāls arests" 3.daļa.
- https://www.esidross.lv/2014/10/20/virtuala-izmeklesana-reals-arests-3-dala/
- "Virtuālā izmeklēšana, reāls arests" 4.daļa. https://www.esidross.lv/2014/12/11/virtuala-izmeklesana-reals-arests-4-dala/

Pārskata periodā CERT.LV sniedza komentārus radio un televīzijā, kā arī publicētas ziņas portālos. Sīkāka informācija:

1) Intervijas un ziņas radio:
   - 03.10. Saruna par pikšķerēšanu un banku trojāniem Latvijas radio 1 raidījumā „Zināmais nezināmajā".
   - 09.10. Sniegta intervija Latvijas radio 1 raidījumā "Pēcpusdiena".
   - 27.10. Diskusija par datordrošību un Eiropas kiberdrošības mēnesi Latvijas radio 1 raidījumā "Kā labāk dzīvot".
   - 29.10. Saruna par datoru inficēšanos un robotu tīkliem Latvijas radio 1 raidījumā "Zināmais nezināmajā".
   - 25.11. Sniegts komentārs par aktuālo Gmail pikšķerēšanas kampaņu Latvijas Radio 4 ziņām.

2) Sižeti televīzijā, tiešraides:
   - 06.10. Saruna par mobilo ierīču drošību un bilžu nopludināšanas skandālu TV3 raidījumam „Bez tabu".
   - 24.10. Saruna par datorologa akciju Rīga TV24 raidījumā „Tīkla vīzija".
   - 27.10. Diskusija par datu drošību un kiberdrošības mēnesi Rīga TV24 kopā ar Nebanku kredītu asociācijas pārstāvi.
   - 29.10. CERT.LV viesojās Rīga TV24 raidījumā "Tīkla vīzija" lai pastāstītu par CERT.LV darbību, tā vēsturi, par portālu esidross.lv, kā arī komentēja raidījumā apspriestās ar informācijas tehnoloģijām saistītās tēmas.
   - 29.10. Sniegts komentārs LTV1 raidījumam „Rīta panorāma" par iespēju ļaundariem izmantot lietotāja mobilās ierīces fotokameru.
   - 25.11. Intervija LNT raidījumam „900 sekundes" par iespējamo Latvijas reputācijas graušanu Prezidentūras laikā.
   - 27.11. Sniegts komentārs LTV1 raidījumam „4.studija" par Gmail krāpniecības mēģinājumu ar lūgumu nosūtīt naudu ārzemēs esošam draugam.
   - 02.12. Sniegta intervija LU SZF KiwiTV par personas datu drošību internetā.
   - 09.12. Sniegts komentārs LTV7 ziņām par e-pasta vēstulēm ar aicinājumu aizdot naudu ārzemēs esošam draugam (Gmail pikšķerēšana).
   - 10.12. Sniegts komentārs par Gmail e-pastu uzlaušanas gadījumiem LNT ziņām.
   - 12.12. Sniegts komentārs Rīga TV24 raidījumā par datorkrāpniekiem.

3) Ziņas portālos:
   - 02.10. IT drošības uzņēmums: Kļūdas dēļ e-talonu iespējams atjaunot neierobežoti - raksts diena.lv
   - 02.10. Uzņēmums: «Rīgas satiksmes» e-talonu sistēma ir viegli apkrāpjama - raksts tvnet.lv
   - 02.10. IT speciālisti brīdina: "Rīgas satiksmes" e-talonu sistēma ir viegli apkrāpjama - raksts kasjauns.lv
   - 02.10. IT drošības uzņēmums: "Rīgas satiksmes" e-talonu sistēma ir viegli apkrāpjama - raksts la.lv
   - 10.10. 10 soļi iedzīvotāju personīgo datu drošībai internetā - raksts dzirkstele.lv

- 24.10. 10 soļi datu drošībai internetā - raksts diena.lv
- 27.10. Ar izglītojošu kampaņu aicinās iedzīvotājus pievērst uzmanību personīgo datu drošībai – raksts delfi.lv
- 28.10. Otrdien bez maksas var pārbaudīt savu datoru pie datorologa - skaties.lv
- 28.10. Būs iespēja bez maksas pārbaudīt datoru - raksts tvnet.lv
- 25.11. CERT.LV saņemti vairāki iesniegumi par paziņu vārdā sūtītām krāpnieciskām mēstulēm - raksts tvnet.lv
- 25.11. Krāpnieki izsūta mēstules no it kā pazīstamiem cilvēkiem un prasa naudu - raksts delfi.lv
- 25.11. Latvijā kārtējais mēstuļu jeb spama vilnis. Kā neiekrist krāpnieku nagos? - raksts kasjauns.lv
- 30.11. Hakeri piekļuvuši arī Latvijas tīmekļa kamerām; vai ir pamats uztraukumam? - raksts apollo.lv
- 16.12. Interneta krāpnieki atkal uzdarbojas - raksts liepajniekiem.lv
- 17.12. Aicina uzmanīties – Latvijā izplata bīstamu ļaunatūru - raksts delfi.lv
- 17.12. Brīdina: Latvijā tiek izplatīts bīstams izspiedējvīruss - raksts apollo.lv
- 24.12. Svētku laikā aktivizējas datorkrāpnieki - raksts bauskasdzive.lv
- 28.12. Interneta drošības riski “parastā lietotāja” ikdienā ir augsti - raksts lvportals.lv

CERT.LV atbalstīja Latvijas Nebanku kredītdevēju asociācijas veidoto kampaņu „Datu drošība internetā” kā informatīvais partneris, sniedzot informāciju par droša interneta lietošanas pamatiem, veicot finanšu darījumus. Kampaņas rezultātā pasta nodaļās tika izplatīti kalendāri ar drošas interneta lietošanas ieteikumiem un vairākos televīzijas kanālos tika demonstrēts video klips par datu drošību internetā.

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

Oktobrī norisinājās Eiropas kiberdrošības mēnesis. Kiberdrošības mēneša aktivitātes CERT.LV atklāja ar semināru "IT drošības risku mazināšana ES prezidentūras laikā". Semināra tēmas bija: gatavošanās ES prezidentūrai no IT drošības viedokļa, IT drošības izaicinājumi ES prezidentūras laikā un informācijas sistēmu aizsardzība pret dažādiem uzbrukumu veidiem.

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, *heartbleed* ievainojamības atklāšana u.c. Konferenci noslēdza valsts un privātā sektora ekspertu paneļdiskusija par to, kā vislabāk paaugstināt galalietotāju informācijas drošības prasmes.

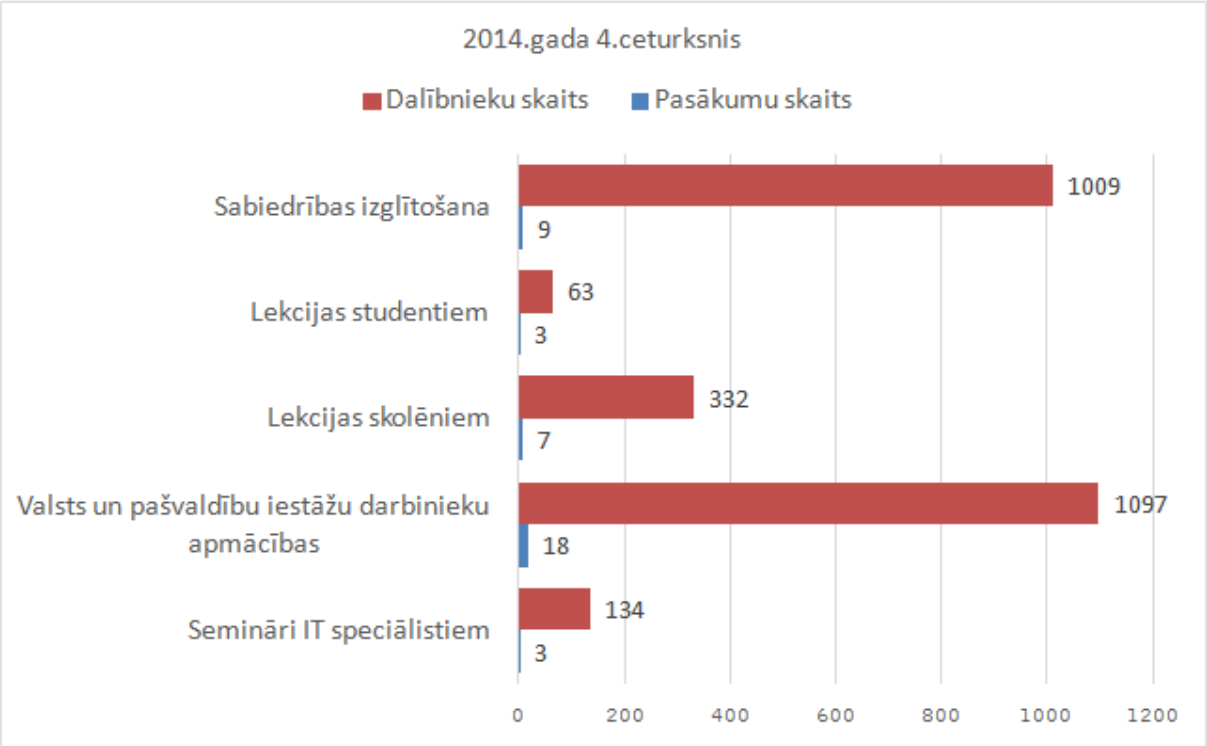
Dalībnieki konferenci novērtēja kā kvalitatīvu un noderīgu, arī kopējais novērtējums bija ļoti augsts. Konferenci tiešraidē noskatījās 945 lietotāji pēc tiesraides.lv datiem, pēc Google analitics datiem tiešraidi bija skatījušies 1 548 apmeklētāji.

17.oktobrī CERT.LV rīkoja interneta pioniera Paul Vixie semināru par DNS drošību. Seminārā tika aplūkotas tādas tēmas kā Passive DNS, DNStap, DNSSEC, tsig, Bind features, DDoS controls un DNS firewalls.

Kiberdrošības mēnesi 28.10. noslēdza datorologa akcija, kurā piedalījās 36 interesenti. Akcija notika sadarbībā ar „Atbildīgs IPS" iniciatīvas pārstāvjiem SIA Lattelecom, SIA Stream Networks, SIA Versija un SIA Latnet Serviss.

CERT.LV turpināja dažādu mērķa grupu izglītošanu par IT drošības tēmām.

Kopā pārskata periodā CERT.LV par IT drošību tika izglītoti 2605 cilvēki, piedaloties 37 dažādos pasākumos. Lielākā auditorija šajā ceturksnī bija valsts un pašvaldību iestāžu darbinieki.



7.attēls – CERT.LV organizēto pasākumu un apmācīto cilvēku skaits 2014.gada 4.ceturksnī.

CERT.LV pasākumi pārskata periodā:

1) Semināri IT speciālistiem:

- 02.10. Notika CERT.LV organizētais seminārs IT drošības speciālistiem "IT drošības risku mazināšana ES prezidentūras laikā".
- 16.10. CERT.LV ISACA konference „Apmācīts un atbildīgs IT/IS lietotājs – mūsu visu drošības pamats".
- 17.10. Paul Vixie seminārs par DNS drošību.
- 06.11. Notika CERT.LV organizētais seminārs „Ievads datora atmiņas ļaunprātīgā izmantošanā".
- 07.11. CERT.LV pārstāvis uzstājās ar lekciju kiberzemessardzes biedriem par IOC (indicators of compromise) dokumentācijas sagatavošanu.

2) Valsts un pašvaldību iestāžu darbinieku apmācības:

- 01.10. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Ģenerālprokuratūrā.
- 05.10.- 08.10. CERT.LV pārstāvis uzstājās ar prezentācijām par IT drošību Latvijas Republikas Pastāvīgā pārstāvniecībā Eiropas Savienībā un Latvijas Republikas Pastāvīgā pārstāvniecība NATO.
- 14.10. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Ārlietu ministrijā.
- 22.10.-25.10. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Ārlietu ministrijas konsulārajiem darbiniekiem Stambulā.
- 28.10. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Ārlietu ministrijā.

- 04.11. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Pārtikas drošības, dzīvnieku veselības un vides zinātniskajā institūtā „BIOR”.
- 06.11. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Ārlietu ministrijā.
- 07.11. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Pārtikas drošības, dzīvnieku veselības un vides zinātniskajā institūtā „BIOR”.
- 10.11. CERT.LV pārstāvis uzstājās ar prezentāciju vēstniekiem Ārlietu ministrijā.
- 12.11. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Pārtikas drošības, dzīvnieku veselības un vides zinātniskajā institūtā „BIOR”.
- 20.11. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Ārlietu ministrijā.
- 21.11. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Liepājas pilsētas pašvaldībā.
- 26.11. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Satiksmes ministrijā.
- 03.12. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Finanšu ministrijā.
- 03.12. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Ārlietu ministrijā.
- 04.12. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Pārtikas drošības, dzīvnieku veselības un vides zinātniskajā institūtā „BIOR”.
- 05.12. CERT.LV pārstāvji piedalījās LVRTC seminārā, kā arī uzstājās ar prezentāciju.
- 05.12. CERT.LV pārstāvis uzstājās ar prezentāciju par IT drošību Finanšu ministrijā.
- 09.12. CERT.LV pārstāvis uzstājās ar lekciju par IT drošību Ārlietu ministrijā.

3) Lekcijas skolēniem:

- 10.10. CERT.LV pārstāvis uzstājās ar lekcijām skolēniem par IT drošību Kalsnavas pamatskolā.
- 10.11. CERT.LV pārstāvis uzstājās ar lekcijām skolēniem par IT drošību Rīgas Mūzikas internātvidusskolā.
- 19.11. CERT.LV pārstāvji piedalījās ar prezentāciju skolēniem par IT drošību Liepājas Raiņa 6. vidusskolā Lattelecom, CERT.LV un Net-Safe Latvija organizētajā IT drošības seminārā “Internets – lieto drošāk un atbildīgāk".
- 25.11. CERT.LV pārstāvji piedalījās ar prezentāciju skolēniem par IT drošību Jelgavas valsts ģimnāzijā Lattelecom, CERT.LV un Net-Safe Latvija organizētajā IT drošības seminārā “Internets – lieto drošāk un atbildīgāk".
- 27.11. CERT.LV pārstāvji piedalījās ar prezentāciju skolēniem par IT drošību Tukuma 2. pamatskolā Lattelecom, CERT.LV un Net-Safe Latvija organizētajā IT drošības seminārā “Internets – lieto drošāk un atbildīgāk".
- 02.12. CERT.LV pārstāvju prezentācija par IT drošību Daugavpils 12. vidusskolā Lattelecom, CERT.LV un Net-Safe Latvija organizētajā IT drošības seminārā “Internets – lieto drošāk un atbildīgāk".

4) Lekcijas studentiem:

- 21.10. CERT.LV pārstāvji uzstājās ar lekciju Vidzemes augstskolas studentiem par CERT.LV aktivitātēm kursa "Globālo datortīklu projektēšana un administrēšana" ietvaros.
- 05.11. CERT.LV pārstāvis uzstājās ar lekciju LU Datorikas fakultātes specseminārā par tēmu „Atbildīga ievainojamību atklāšana”.

- 24.11. CERT.LV pārstāvji uzstājās ar lekciju Latvijas Universitātes Datorikas fakultātē par IT drošību.

5) Sabiedrības izglītošana:

- 28.10. CERT.LV pārstāvis uzstājās ar prezentāciju eBIZ 2014 konferencē.
- 29.10. CERT.LV pārstāvis uzstājās ar prezentāciju Rīgas izglītības un informatīvi metodiskā centra darba grupā: Informācijas drošība internetā un sociālajos tīklos.
- 30.10. CERT.LV pārstāvis uzstājās ar prezentāciju *„Convenience has messed up the Internet beyond repair*?" DSS konferencē.
- 30.10. CERT.LV pārstāvis piedalījās Latvijas skolu tehnoloģiju ekspozīcijā IT skolotājiem ar Datoloroga konsultācijām.
- 28.12. CERT.LV organizēja Datorologa akciju LU Matemātikas un informātikas institūta telpās.
- 25.11. CERT.LV pārstāvis uzstājās ar prezentāciju bibliotekāru konferencē Latvijas akadēmisko, speciālo un publisko bibliotēku direktoru rudens sanāksmē.
- 11.12. CERT.LV pārstāvis uzstājās ar prezentāciju "Lietošanas ērtums par drošības cenu" Latvijas Informācijas un komunikācijas tehnoloģijas asociācijas (LIKTA) konferencē "Latvijas loma Eiropas „digitālās kartes" veidošanā".

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

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

- 07.10. CERT.LV pārstāvji piedalījās Ministru kabineta sēdē.
- 9.10., 13.11. un 11.12. Notika DEG sanāksmes.
- 22.10. Notika sadarbības tikšanas ar Centrālo statistikas pārvaldi.
- 03.11. CERT.LV pārstāvis piedalījās Aizsardzības ministrijas darba grupas sanāksmē.
- 04.11. Notika sadarbības tikšanās ar ASV vēstniecības pārstāvi.
- 10.11. CERT.LV pārstāvji piedalījās apmācību seminārā par Valsts informācijas sistēmām darbam ar Eiropas Savienības dokumentiem (ESVIS).
- 11.11. Notika sadarbības tikšanās ar Valsts policiju.
- 24.11. Notika tikšanās Aizsardzības ministrijā par Informācijas tehnoloģiju drošības likuma grozījumiem.
- 25.11. CERT.LV pārstāvis piedalījās OECD (Ekonomiskās sadarbības un attīstības organizācija) iestāšanās intervijās.
- 18.12. CERT.LV pārstāvis tikās ar Aizsardzības ministriju, lai pārrunātu DDoS aizsardzības pasākumus.

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.

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 nav izmaiņu attiecībā pret 2014.gada 3.ceturksni - ir 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.

Sadarbība ar citu valstu IT drošības incidentu novēršanas vienībām incidentu risināšanā aprakstīta atskaites 2.punktā.

No 29.-31.oktobrim notika ENISA organizēto mācību „Cyber Europe 2014" 2. fāze. Mācību mērķis bija testēt sadarbību Eiropas ietvaros liela apjoma Enerģētikas sektora kiberkrīzes gadījumā. No Latvijas mācībās piedalījās CERT.LV, Kiberzemessardzes vienība un Latvenergo. Mācību rezultāts ir kopējs visu dalībvalstu ziņojums nākamā līmeņa mācībām, kas notiks 2015.gada februārī.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 01.- 03.10. CERT.LV pārstāvis piedalījās ENISA mācību plānošanas sapulcē Atēnās, Grieķijā.
- 07.- 08.10. CERT.LV pārstāvis piedalījās CERT-EU organizētā seminārā Briselē, Beļģijā.
- 13.-14.10. CERT.LV pārstāvis piedalījās ENISA un Europol organizētajā LEA-CERT konferencē Hāgā, Nīderlandē.
- 20.-24.10. CERT.LV pārstāvis piedalījās CERT Polska ikgadējā konferencē par IT drošību Varšavā, Polijā.
- 28.10. -31.10. Dalība ENISA mācībās „Cyber Europe 2014".
- 29.-31.10. CERT.LV pārstāvis uzstājās ar prezentāciju Itālijas prezidentūras organizētajā seminārā "The role of Cyber Defence to protect and sustain EU economy" Romā, Itālijā.
- 13.11. CERT.LV pārstāvis piedalījās „Tallina Digital Forensics Institute" atkāšanā un uzstājās ar prezentāciju konferencē "CyberCrime 2014"Tallinā, Igaunijā.
- 19.11.- 21.11. CERT.LV pārstāvis piedalījās TRANSITS I kursos Prāgā, Čehijā.
- 18.11. - 20.11. CERT.LV, NBS un Kibersardzes vienības apvienotā komanda piedalījās NATO kiberdrošības mācībās „Cyber Coalition 2014".
- 09.12. Notika sadarbības tikšanās ar Igaunijas kiberzemessardzes pārstāvjiem.
- 10.12. Notika sadarbības videokonference ar CERT-UK par sadarbību, kurā piedalījās Aizsardzības ministrijas un CERT.LV pārstāvji.

Sadarbība konkrētu incidentu gadījumos aprakstīta šī pārskata 2.punktā.

8. Citi normatīvajos aktos noteiktie pienākumi.

- 01.10. Notika tikšanās Nacionālajā bibliotēkā par IT drošības konferences organizēšanu.
- 09.10. CERT.LV pārstāvis piedalījās Samsung „Living business" konferencē.
- 21.10. Notika sadarbības tikšanās ar LIKTA par CERT.LV dalību LIKTA konferencē.
- 27.10. Notika sadarbības tikšanās ar Izložu un azartspēļu uzraudzības inspekciju.
- 03.11. Notika sadarbības tikšanās ar Banku augstskolu.
- 13.11. Notika sadarbības tikšanās ar ISACA Latvija par 2015.gada IT drošības konferences plānošanu.
- 13.11. CERT.LV pārstāvis piedalījās NATO Startcom apaļā galda diskusijā "Social Media in Contemporary Conflicts".
- 28.11. CERT.LV pārstāvis piedalījās DPA un Ernst & Young rīkotajā Latvijas kiberdrošības jautājumiem veltītajā sesijā "Latvijas prezidentūra Eiropas savienības Padomē – Latvijas iespēja IT inovācijām".
- Novembrī trīs CERT darbinieki pēc CEH eksāmena nokārtošanas ieguva CEHv8 (Certified Ethical Hacker) sertifikātu.
- 15.12. Notika izvērtēšanas sanāksme par Lattelecom, CERT.LV un Netsafe projektu skolām „Internets – lieto drošāk un atbildīgāk".
- 16.12. Notika sadarbības tikšanās ar Latvenergo.
- 18.12. Notika tikšanās par Swedbank IT drošības nedēļas projektu.
- 18.12. Notika sadarbības tikšanās ar Latvijas Dzelzceļu.
- 18.12. Notika sadarbības tikšanās ar Lattelecom.

2015.gada 10.februārī

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