Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2015

2015. gada 4. ceturksnis (01.10.2015. – 31.12.2015.)

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 3

1. Elektroniskās informācijas telpā notiekošo darbību atainojums. 4

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā. 7

3. Rekomendācijas par informācijas tehnoloģiju risku novēršanu (komunikācija ar sabiedrību). 12

4. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā. 15

5. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā. 16

6. Valsts un pašvaldību institūciju un elektronisko sakaru komersantu uzraudzība par Informācijas tehnoloģiju drošības likumā noteikto pienākumu veikšanu. 17

7. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām. 18

8. Citi normatīvajos aktos noteiktie pienākumi. 19

9. Aģentūras papildu pasākumu veikšana. 19

Kopsavilkums

Pārskata periodā vairākas Latvijas bankas piedzīvoja banku trojāna uzbrukumus, CERT.LV veica uzbrukumu kampaņas analīzi. Izpēte atklāja, ka vīruss ir modificēts atvasinājums no Zbot trojan saimes ar WEB injekciju funkcionalitāti, kas nelīdzinās iepriekšējām Zbot variācijām.
Uzbrukumi lietotājiem galvenokārt notika caur inficētiem e-pastu pielikumiem, retāk caur baneru apmaiņas sistēmām leģitīmās vietnēs, kā arī citos veidos.

Visu ceturksni turpinājās apjomīga šifrējošo izspiedējvīrusu izplatība, gan mērķējot mēstules ar pielikumā esošo vīrusu uz atsevišķām lietotāju grupām, piemēram, grāmatvežiem, gan izplatot arvien jaunus vīrusu paveidus, tajā skaitā arī Linux operētājsistēmai.

Oktobrī notika apjomīgi DDoS uzbrukumi Latvijā strādājošām komercbankām, ko organizēja DDoS4bitcoin un Armada kibernoziedznieku grupējumi. CERT.LV sniedza rekomendācijas iespējamo uzbrukumu mērķorganizāciju IKT vides stiprināšanai.

1. oktobrī notika IT drošības konference "Kiberšahs. Stratēģija un taktika virtuālajā vidē", kas pulcēja 500 profesionāļus. Konferencē tika prezentēti CERT.LV pētījuma rezultāti par Krievijas interneta troļļu aktivitātēm Latvijas ziņu portālu komentāru sadaļās, kur ar provokatīviem komentāriem un saitēm tiek veikti mēģinājumi inficēt lietotāju datorus.
Pētījuma rezultāti izpelnījās arī lielu mediju uzmanību.

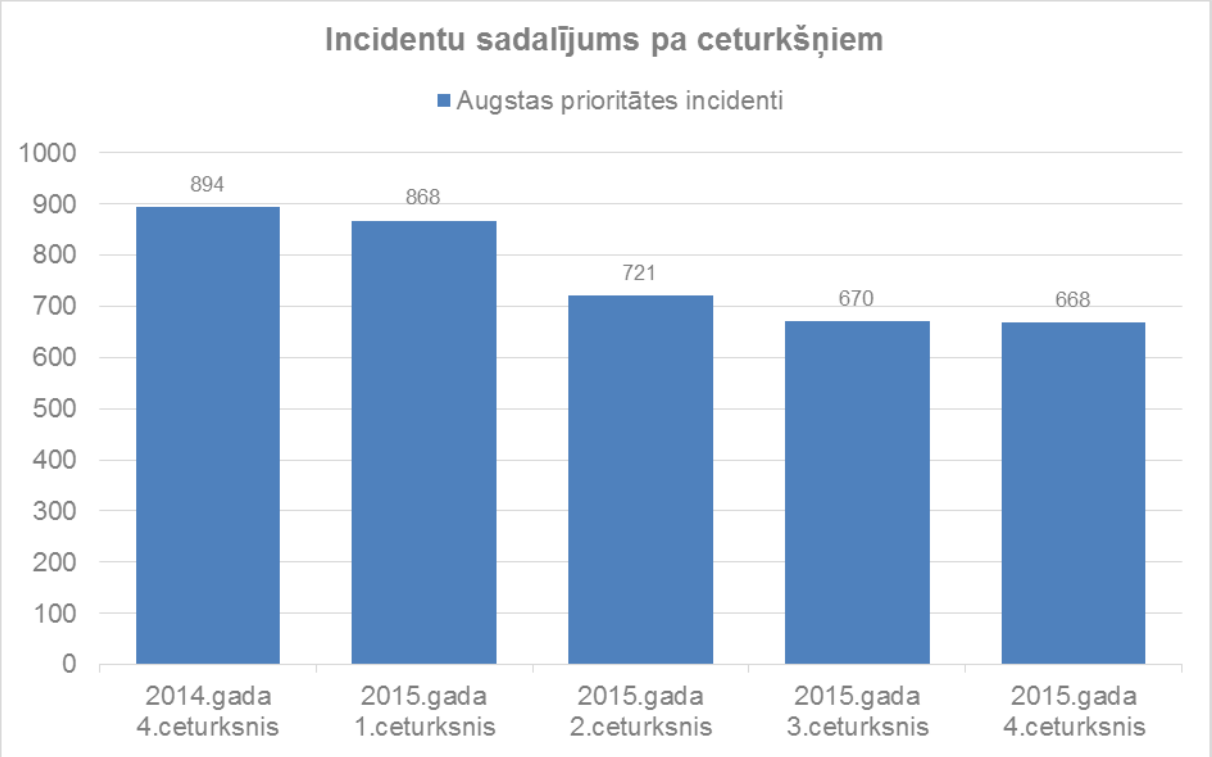
2015. gada 4. ceturksnī CERT.LV reģistrēja un apstrādāja 668 augstas prioritātes incidentus un 135 514 zemas prioritātes incidentus.

Pārskata periodā CERT.LV pārstāvji piedalījās 36 pasākumos, apmācot 2733 cilvēkus, ievietoja 50 jaunas ziņas vietnē www.cert.lv, piedalījās 4 radio pārraidēs un 8 televīzijas sižetos.

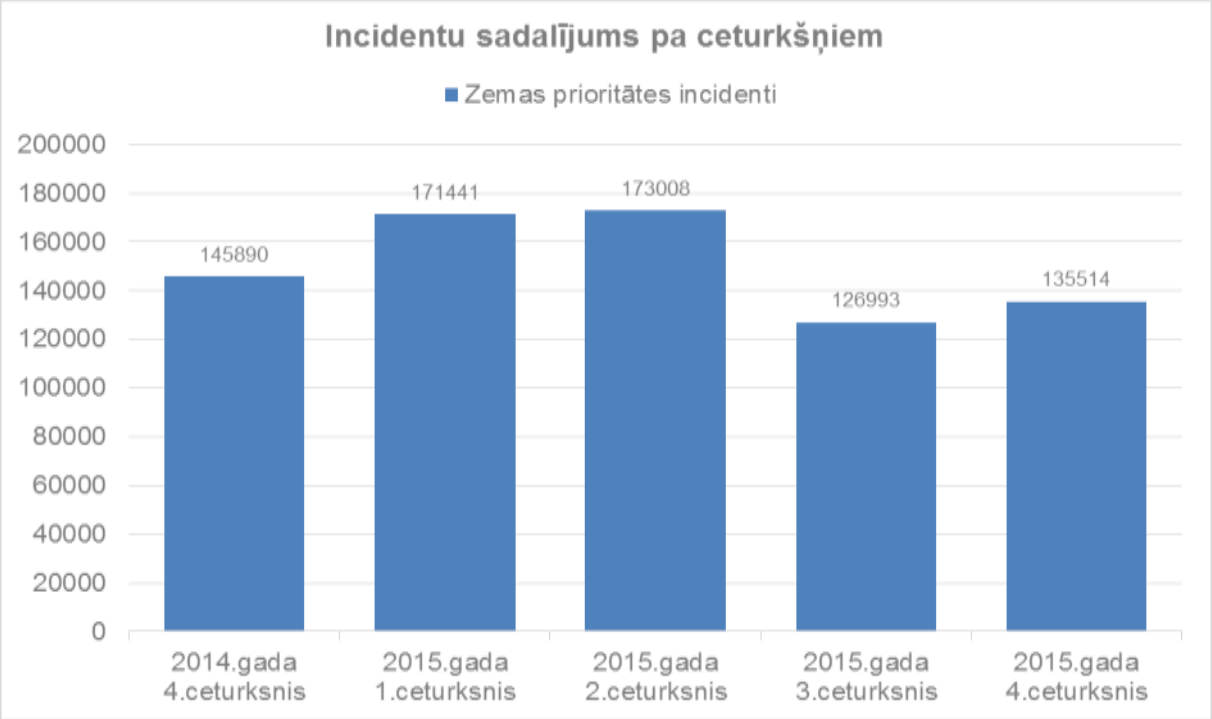
1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

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.

2015. gada 4. ceturksnī CERT.LV apstrādāja 668 augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 670 augstas prioritātes incidenti, bet 2014. gada 4. ceturksnī 894 augstas prioritātes incidenti.

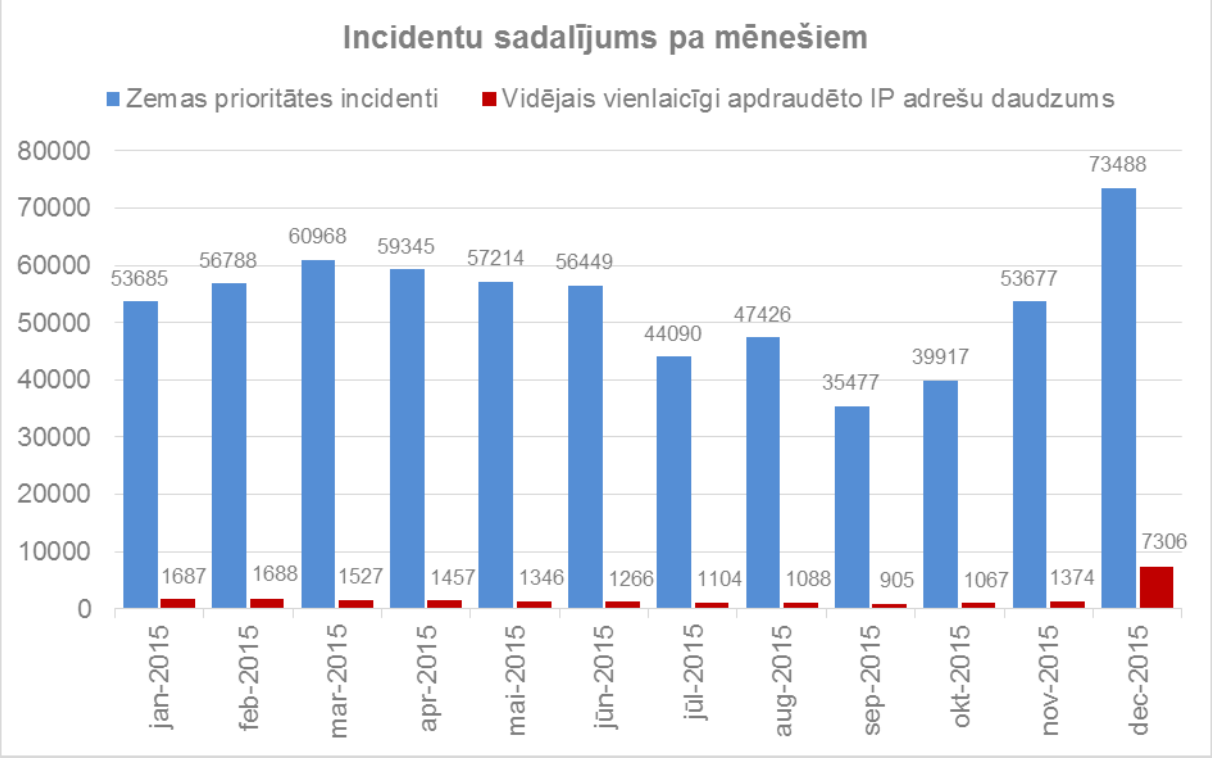


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2014. un 2015. gadā.



2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem 2014. un 2015.gadā.

2015. gada 4. ceturksnī CERT.LV reģistrēja 135 514 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 126 993 zemas prioritātes incidenti, bet 2014. gada 4. ceturksnī 145 890 zemas prioritātes incidenti. Zemas prioritātes incidentu skaits turpina pieaugt, jo aktuālās uzbrukuma kampaņas un ievainojamības visbiežāk atspoguļojas tieši zemas prioritātes incidentu uzskaites statistikā.



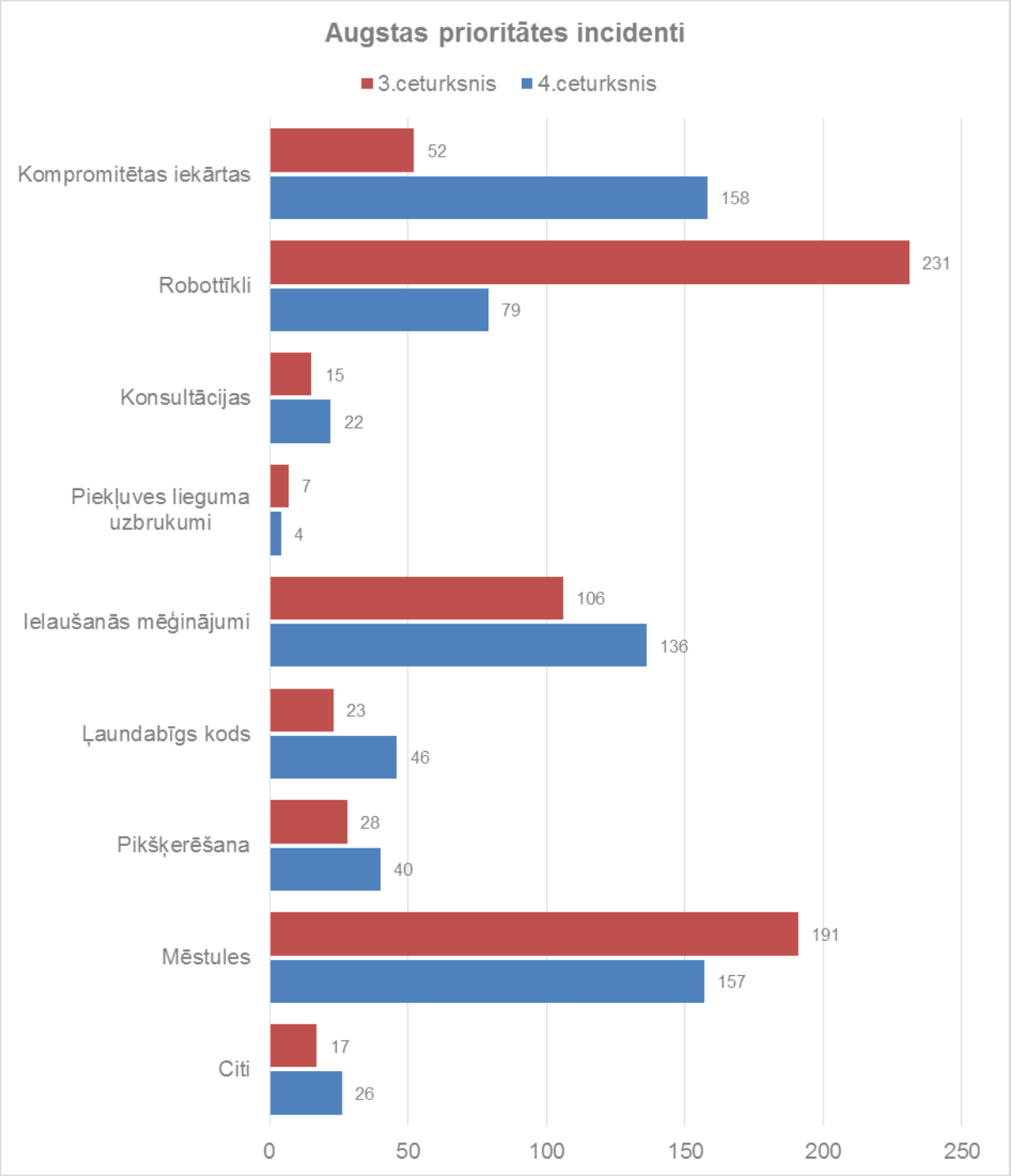
3.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi apdraudēto IP adrešu daudzums 2015. gadā.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi apdraudēto unikālo IP adrešu skaitu Latvijā. Gada pēdējā mēneša inficēto adrešu skaits skaidrojams ar "Poodle SSL" ievainojamības izplatību Latvijā.

Lai samazinātu kopējo apdraudēto 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". Atbildīgo IPS kopskaits saglabājās bez izmaiņām – 13.

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

Pārskata periodā CERT.LV reģistrēja un apstrādāja 668 augstas prioritātes incidentus.

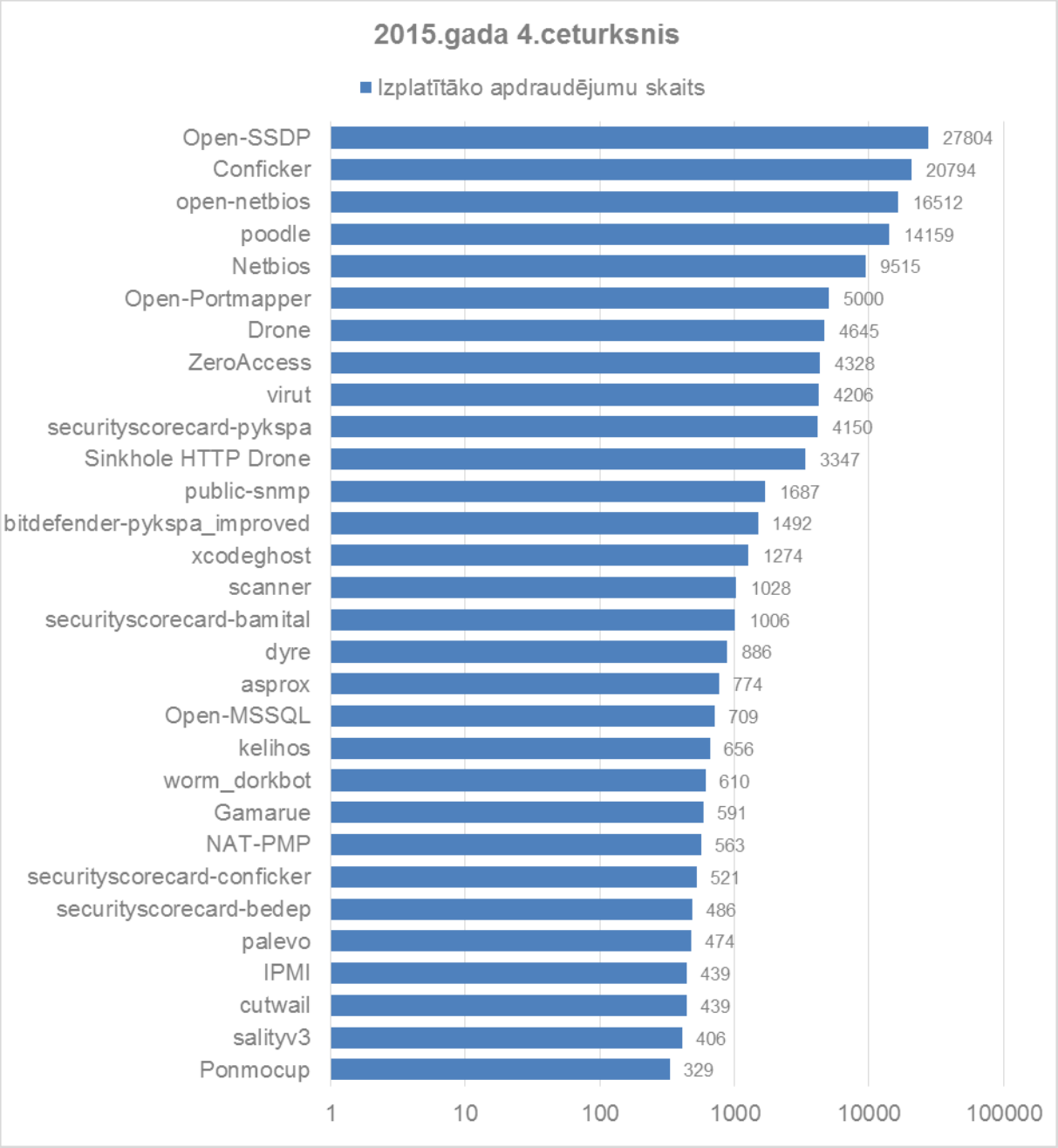


5.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2015. gada 2. un 3. ceturksnī.

Statistika rāda augstu mēstuļu izplatību, salīdzinot ar iepriekšējo pārskata periodu. Tas ir pašsaprotams rādītājs gada nogalē, kad ar mēstuļu kampaņu palīdzību tika gan vākti lietotāju dati, gan izplatīti šifrējošie vīrusi un banku trojāņi.

Kompromitētu iekārtu skaits ir pieaudzis Joomla satura vadības sistēmas ievainojamības izplatības rezultātā.
Apzinot apdraudējuma ietekmi, .lv domēnu zonā tika pārbaudīti apmēram 700 000 domēna vārdi. No tiem 13 000 izmanto Joomla satura vadības sistēmu. Valsts sektorā tika atklāti vairāki desmiti šādu vietņu.

Pārskata periodā CERT.LV reģistrēja 135 514 zemas prioritātes incidentus.

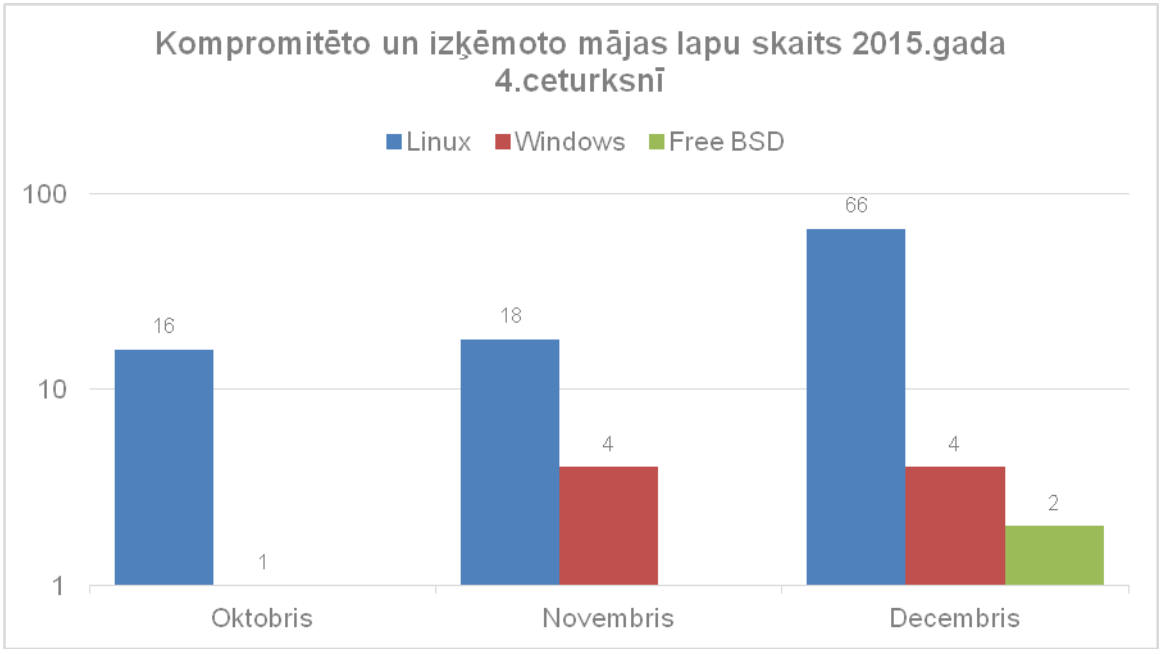


6.attēls - CERT.LV reģistrētie zemas prioritātes incidenti no 2015. gada 1. oktobra līdz 31. decembrim pa apdraudējumu veidiem.

Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

7.attēls –Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2015.gada 3.ceturksnī.

"Poodle SSL" ievainojamības dēļ decembrī tika reģistrēts liels skaits IP adrešu, kuras bija pakļautas šai ievainojamībai. Iekārtu uzturētāji tika aicināti pārbaudīt tajās izmantoto SSL bibliotēku, kuru nepieciešams atjaunināt.
CERT.LV uzskaita arī kompromitēto un izķēmoto mājaslapu gadījumus.



8.attēls – Kompromitēto un izķēmoto mājas lapu skaits pa mēnešiem 2015. gada 4. ceturksnī.

Decembrī kompromitēto mājas lapu skaits ir pieaudzis dēļ atklātās ievainojamības Joomla satura vadības sistēmā. CERT.LV veica arī .lv domēnu zonas pārbaudi, lai noteiktu ievainojamības izplatību.

CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā.

Svarīgākie CERT.LV drošības incidenti pārskata periodā

- 07.10. CERT.LV veica nekorekti konfigurētu Mikrotik maršrutētāju apzināšanu Latvijas IP adrešu apgabalos. Tika noskaidrots, ka atvērts DNS open resolver ir paša lietotāja nekorektu darbību rezultāts, nevis ražotāja Mikrotik kļūme. Latvijā šādas nekorekti konfigurētas iekārtas ir nedaudz vairāk par tūkstoti. Mikrotik ir Latvijas uzņēmums, kas ražo tīkla aparatūru un programmatūru, kas populāra visā pasaulē. Tā kā programmatūras un konfigurācijas iespējas ir ļoti plašas, lietotāji mēdz tās līdz galam neizprast un strādāt ar nesakārtotu konfigurāciju vai nepareizi pieslēgtu iekārtu.
- 09.10. Caur e-pastiem tika izplatīts datorvīrusa instalators "Upatre". Tas, inficētas iekārtas gadījumā, ar Microsoft Outlook programmas palīdzību izplata sevi tālāk visām upura e-pasta kontaktpersonām. Cieta arī vairākas valsts iestādes.
- 12.10. Tika atkārtoti identificētas zagtas kredītkaršu informācijas tirdzniecības vietnes Latvijā. Informācija tika nodota Valsts policijai.
- 12.10. Notika vairāki apjomīgi DDoS uzbrukumi Latvijā strādājošām komercbankām. Uzbrukumus organizēja DDoS4bitcoin un Armada kibernoziedznieku grupējumi. CERT.LV sniedza rekomendācijas iespējamo uzbrukumu mērķorganizāciju IKT vides stiprināšanai.
- 13.10. Vairākās .LV zonas lapās tika konstatētas kļūdas, kas ļauj veikt SQL injekciju uzbrukumu. Lapu īpašnieki tika informēti.
- 14.10. CERT.LV identificēja pirmos Vawtrak/NeverQuest trojāna uzbrukumus pret Latvijas banku lietotājiem. Tika uzsākta izmeklēšana.
- 20.10. Tika atklātas konfigurācijas kļūdas kādas tiesībsargājošās mājaslapā. Iestādes atbildīgās personas tika informētas, lapa tika izlabota. Par atklātiem trūkumiem CERT.LV informēja kāds drošības pētnieks. Trūkumi tika atklāti, ievērojot atbildīgas ievainojamības atklāšanas pamatprincipu, nodarīt mazāko iespējamo kaitējumu. Ievainojamības nebija kritiskas, taču CERT.LV veica to novēršanas koordināciju.
- 22.10. Atkārtoti tika izplatīts liels daudzums surogātpasta, ar pielikumā esošu "Upatre" datorvīrusu instalatoru. Tika inficēti arī vairāku pašvaldību datori. Tādējādi tika mēģināts izplatīt internetbanku apzagšanai domāto "Dyre" datorvīrusu.
- 22.10. CERT.LV identificēja kārtējo šifrēšanas vīrusa izplatīšanas kampaņu, kuras mērķu lokā bija arī vairākas valsts iestādes.
- 28.10. Tika veikts DDoS uzbrukums pret kādu internetveikalu, par uzbrukuma pārtraukšanu pieprasīta izpirkuma maksa. Uzbrukums tika ierobežots, izmainot servera uzturošo infrastruktūru.

- 30.10. Caur kādu sociālo tīklu tika izplatīti krāpnieciski paziņojumi ar saiti, kura domāta apmeklētāju kredītkaršu zādzībai. Krāpnieciskā lapa tika slēgta.
- 02.11. Tika izplatīti e-pasti, kas domāti Apple ID datu izkrāpšanai. Lapa tika slēgta.
- 04.11. Daudziem Latvijas notāriem un zvērinātiem advokātiem tika izsūtīti e-pasti, kas saturēja saiti uz datorvīrusu CTB-Locker saturošu failu. E-pasti bija noformēti kā sūdzības no klientiem, faili izvietoti inbox.lv un dropbox.com serveros. Pēc CERT.LV pieprasījuma kaitīgie faili tika dzēsti.
- 05.11. Pret kādu Rīgas pašvaldības izglītības iestādi tika veikts DDoS uzbrukums. Iestādei tika piešķirta cita IP adrese.
- 16.11. CERT.LV identificēja Latvijā uzturētu serveri, kas tika izmantots t.s. money-mule vervēšanai un pikšķerēšanas kampaņu veikšanai pret ārvalstu banku klientiem. Pikšķerēšanai paredzētā infrastruktūra tika apturēta, tika uzsākta izmeklēšana.
- 27.11. Tika izsūtītas viltotas vēstules, ar kurām mēģināja izkrāpt bankas klientu piekļuves datus. Krāpnieciskais e-pasts pēc CERT.LV pieprasījuma tika slēgts.
- 30.11. Kādas iestādes mājas lapā tika atklāta SQL ievainojamība. CERT.LV informēja lapas uzturētājus.
- 03.12. Pret kādu banku tika veikts pikšķerēšanas uzbrukums. CERT.LV iesaistījās kaitīgās lapas slēgšanā.
- 06.12. Tika mēģināts izkrāpt naudu labdarības mērķiem, izsūtot aicinājumus e-pastos. Krāpnieciskā lapa slēgta.
- 07.12. Notika jaunas šifrēšanas vīrusa uzbrukuma kampaņas, kuru mērķi bija arī valsts iestādes. Vīruss ir Cryptowall 4, kas līdz šim Latvijā nav bijis īpaši izplatīts. Vīrusa versija nebija latviskota.
- 15.12. Tika atklāta kritiska Joomla satura vadības sistēmas ievainojamība, pastiprināti tika informētas valsts un pašvaldību iestādes, kuru mājas lapas izmanto šo CMS. CERT.LV apzināja valsts pārvaldē un citur Latvijā esošos Joomla projektus, lai brīdinātu par apdraudējumu un koordinētu ievainojamību novēršanu.
- 17.12. Tika izplatīti e-pasti ar XLS dokumentā esošu makrovīrusu, kuru iespējojot, notika lietotāja datu šifrēšana. Lai atgūtu šifrētos datus, tika pieprasīta izpirkuma maksa caur QIWI pārskaitījumu sistēmu. Kampaņas mērķis bija krieviski runājoši grāmatveži. CERT.LV brīdināja lietotājus.
- 26.12. Tika izsūtīti krāpnieciski e-pasti kādas bankas vārdā. Tie saturēja saiti uz resursu, kas tika veidots lietotāju pieejas datu izkrāpšanai. Kaitīgo lapu uzturētāji tika informēti, lapas tika slēgtas.
- 28.12. Izmantojot CMS Joomla ievainojamību, tika izķēmota kādas iestādes mājaslapa. Pēc CERT.LV brīdinājuma lapa tika salabota.
- 30.12. Vairāki nelieli Latvijas internetveikali cieta no Linux Encoder šifrēšanas vīrusa. Uzturētājs lapas atjaunoja no rezerves kopijām.

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

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

27.10. CERT.LV rīkoja kiberdrošības brokastis mediju pārstāvjiem par aktualitātēm IT drošības jomā. Mediju pārstāvji tika informēti par aktuālākajiem apdraudējumiem, kas skar interneta lietotājus un iespējām, kā pasargāties no jaunākajiem vīrusiem un krāpšanas shēmām interneta vidē.
Pasākums pulcēja 16 dažādu mediju pārstāvjus, pasākuma rezultātā notika vairākas intervijas radio un TV, kā arī tika publicēti raksti presē un ziņu portālos. Pasākums notika Eiropas Kiberdrošības mēneša ietvaros.

Informācija par CERT.LV sadarbību ar medijiem

1) Intervijas un ziņas radio:

- 22.10. CERT pārstāvis sniedza interviju LR1 programmā "Pēcpusdiena", par situāciju kiberdrošības telpā.
- 30.10. CERT.LV pārstāvis sniedza komentāru radio Baltcom ziņās par valsts iestādes mājas lapas uzlaušanu.
- 02.11. CERT.LV pārstāvis sniedza interviju radio Baltcom par kiberdrošības situāciju.
- 06.11. CERT.LV pārstāvis piedalījās LR4 raidījumā "Jūsu tiesības" par datora drošību.
- 04.12. CERT.LV pārstāvis sniedza interviju LR 1 par paroļu drošību.

2) Sižeti televīzijā, tiešraides:

- 27.10. CERT pārstāvis sniedza interviju LNT ziņām par IT drošības situāciju (mediju brokastu ietvaros).
- 27.10. CERT pārstāvis sniedza interviju LTV dienas ziņām (mediju brokastu ietvaros).
- 27.10. CERT pārstāvis sniedza interviju TV3 ziņām (mediju brokastu ietvaros).
- 27.10. CERT pārstāvis sniedza interviju LTV7 ziņām krievu valodā (mediju brokastu ietvaros).
- 27.10. CERT pārstāvis sniedza interviju LNT raidījumam 900 sekundes par aktuālākajiem IT drošības apdraudējumiem (mediju brokastu ietvaros).
- 28.10. CERT pārstāvis sniedza interviju LNT ziņām par Datorologa akciju.
- 22.11. CERT pārstāvis sniedza interviju raidījumam "Nekā personīga" par aktuālajiem kiberdraudiem.
- 06.12. CERT.LV pārstāvis sniedza komentāru TV3 raidījumam "Bez Tabu" par karšu krāpniecības gadījumu.

3) Ziņas portālos:

- 01.10. Ar IT drošības konferenci atklās Eiropas kiberdrošības mēnesi - tvnet.lv
- 22.10. UZMANIES: Brīdina par inficētiem ZIP failiem, kurus pārsūta no uzlauztiem e-pastiem - nra.lv
- 27.10. Eksperte: Kiberincidentu skaits sarūk, bet tie kļūst sarežģītāki diena.lv
- 27.10. CERT.LV pārstāvji informēs par aktualitātēm drošības jomā -BNS

- 27.10. 'Cert.lv': Pastāv aizdomas, ka 'mēstules' tulko vietējie iedzīvotāji - DELFI.LV
- 27.10. Kibernoziegumi kļūst sarežģītāki - lsm.lv
- 27.10. Kiberincidentu skaits sarūk, bet tie kļūst sarežģītāki - LETA
- 29.10. Noticis sekmīgs uzbrukums valsts iestādes mājaslapai - lsm.lv, la.lv, diena.lv
- 28.10. Šodien iespējams bez maksas pārbaudīt datoru - tvnet.lv
- 29.10. Uzlauzta kādas valsts iestādes mājaslapa - tvnet.lv
- 29.10. Cert.lv: взломана страница государственного учреждения - rus.delfi.lv
- 11.11. ES prezidentūras laikā pret Latviju vērsti vairāki kiberuzbrukumi - nra.lv
- 11.11. Cyber-attacks getting more sophisticated - lsm.lv
- 11.12. Eksperti: Bankas Latvijā labi sagatavotas pret kibernoziegumiem, bet iedzīvotāji - ne vienmēr- lsm.lv
- 12.11. Cert.lv: kāds neuzmanīgs valsts iestādes darbinieks inficējis darba datoru ar trojāni - diena.lv, tvnet.lv
- 22.11. Krievijas specdienesti radījuši datorvīrusu, ar kuru inficē datorus Latvijā - skaties.lv
- 04.12. Viltvārdis bankas vārdā cenšas izvilināt klientu datus - diena.lv
- 04.12. Eksperiments: Cik tālu var aiziet sarakste ar mēstules autoru - diena.lv
- 22.12. Palielinājusies izplatība inficētiem e-pastiem, kas orientēti uz grāmatvežiem - tvnet.lv
- 27.12. Kibernoziegumu un kiberuzbrukumu tendences ar katru gadu paliek arvien satraucošākas - tvnet.lv
- 26.12. Lielākos kiberuzbrukumus valsts sektoram Latvijā veikuši ar Krieviju saistīti grupējumi - delfi.lv
- 28.12. Svētku brīvdienās «Swedbank» vārdā mēģināts izkrāpt naudas līdzekļus - tvnet.lv

Publicitātes saraksts dots izlases veidā, jo CERT.LV neveic pilnu mediju monitoringu.

4) Informācija par CERT.LV tīmekļa vietnēm:
Pārskata periodā vietnē https://www.cert.lv publicētas 50 ziņas.

Kopā CERT.LV mājaslapai bijuši 27,017 lapu skatījumi, kurus veido 19,000 unikāli lapu skatījumi.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 14,095 apmeklējumi, no tiem 11,246 unikāli apmeklējumi. Portāla apmeklējums ir pieaudzis, salīdzinot ar iepriekšējo pārskata periodu. Tas visdrīzāk saistīts, ar to, ka pieaudzis rakstu skaits, kas tiek ievietots portālā.
CERT.LV turpina tulkot un publicēt portālā Esi drošs OUCH! ikmēneša izdevumus

Portālā publicētie raksti:

- Pikšķerēšana
- Izdot hakerus, vai varbūt nē?
- Droša iepirkšanās tiešsaistē

- Paroļu pārvaldnieki
- Aicina uz bezmaksas datora pārbaudi pie datorologa

5) CERT.LV sociālo tīklu konti:

- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1430.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 268.
- CERT.LV draugiem.lv lapā http://www.draugiem.lv/certlv. Pārskata perioda beigās lapas sekotāju skaits bija 64.
- Sociālajā tīklā Google+ https://www.google.com/+CertLv ir 25 sekotāji.

Pēdējos divos ceturkšņos stabili pieaug sekotāju skaits populārajās sociālo tīklu platformās Twitter un Facebook, taču draugiem.lv un Google+ tas saglabājas teju nemainīgs.

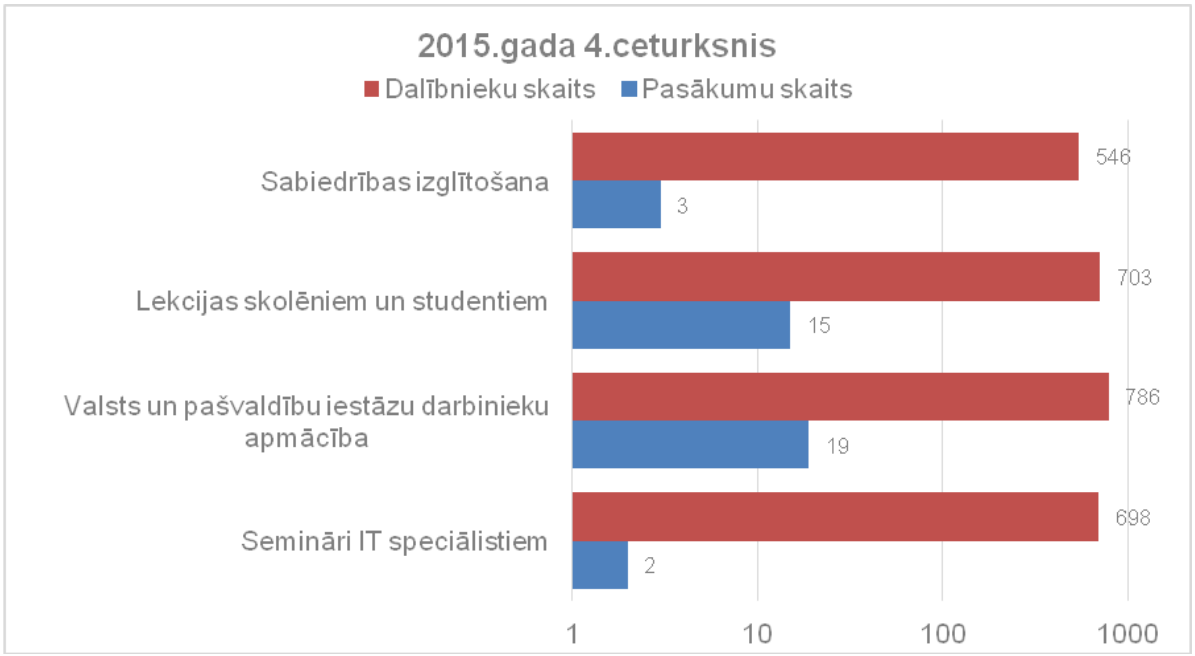
4. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

01.10. Latvijas Nacionālajā bibliotēkā notika ikgadējā IT drošības konference „Kiberšahs. Stratēģija un taktika virtuālajā vidē". Konferenci klātienē apmeklēja 499 dalībnieki, savukārt interneta tiešraidei vietnē straume.lmt bija 2000 unikālie skatījumi.
Konferences programmā tika iekļautas ārvalstu un vietējo IT nozares ekspertu prezentācijas par kiberterorismu, mobilo ierīču drošības izaicinājumiem, komunikācijas stratēģijām kiberkrīžu situācijās, drošas programmatūras izstrādes principiem u.c.
CERT.LV organizēja konferenci sadarbībā ar ISACA Latvijas nodaļu. Pasākumu atbalstīja Eiropas datu centru operators DEAC, SIA „Latvijas Mobilais Telefons" un augstākā līmeņa domēna .lv uzturētājs NIC.

22.10. SIA DSS ITSEC konferencē CERT.LV pārstāvis prezentēja pētījuma rezultātus par Krievijas interneta troļļu aktivitātēm Latvijas ziņu portālu komentāru sadaļās, kur ar provokatīviem komentāriem un saitēm tiek veikti mēģinājumi inficēt lietotāju datorus.

03.12. CERT.LV rīkoja semināru "Esi drošs". Semināru apmeklēja 199 dalībnieki no valsts un pašvaldību iestādēm. Seminārā tika prezentētas tādas tēmas kā aktualitātes IT drošības jomā, wifi drošības aspekti, SSL/TLS protokolu drošības izaicinājumi, datu drošība mākonī un sociālās inženierijas stresa testi iestādēs.

Pārskata periodā CERT.LV par IT drošību izglītoja 2733 cilvēkus, iesaistoties 36 izglītojošos pasākumos.



9.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2015.gada 4.ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 08.10. un 12.11. Notika DEG sanāksmes.
- 08.10. CERT.LV iesaistās Aizsardzības ministrijas darba grupā par Atbildīgas ievainojamību atklāšanas politikas ieviešanu.
- 09.10. Notika sanāksme Tieslietu ministrijā par mēstuļu uzraudzības iespējām.
- 16.11. CERT.LV pārstāvis piedalījās sanāksmē VARAM par E-prasmju nedēļas 2016. organizēšanu.

Sadarbība ar valsts iestādēm incidentu risināšanā aprakstīta atskaites 2. punktā

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.

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 2015. 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.

No 16. līdz 20. novembrim norisinājās ikgadējās NATO "Cyber Coalition 2015" treniņmācības, kurās piedalījās ap 600 kiberdrošības ekspertu no NATO un tās partneru dalībvalstīm, tai skaitā arī Latvijas pārstāvji no CERT.LV, Zemessardzes Kiberaizsardzības vienības un Nacionālajiem bruņotajiem spēkiem.

Mācību mērķis bija pārbaudīt alianses un partneru spēju pārvarēt sarežģītus drošības izaicinājumus. Izmantojot kontrolētu virtuālo vidi, dalībniekiem tika sniegta informācija ar sižetiem, kas ietvēra tādus draudus kā mobilo ļaunatūru un spiegprogrammatūru vai konkrētu tīklu uzlaušanu. Pateicoties veiksmīgai sadarbībai starp valstīm, dotie uzdevumi tika veiksmīgi atrisināti.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 05.10. Notika video konference par sadarbību ar NCSC-NL.
- 05.- 06.10. CERT.LV pārstāvis piedalījās CERT-RO organizētajā "The New Global Challenges in Cyber Security" un uzstājās ar prezentāciju. Pasākums notika Bukarestē, Rumānijā.
- 05.-06.10. CERT.LV pārstāvis piedalījās "Kaspersky Lab Cybersecurity Forum" konferencē Kijevā, Ukrainā.
- 05.- 09.10. CERT.LV pārstāvis piedalījās CCDCoE kursos "Network and Host Forensics" Tallinā, Igaunijā.
- 07.- 08.10. CERT.LV pārstāvis piedalījās Portugāles kiberdrošības centra konferencē "C-DAYS" Lisabonā, Portugālē.
- 13.-15.10. CERT.LV pārstāvis piedalījās CERT Polska organizētajā seminārā un konferencē "Secure 2015" Varšavā, Polijā.
- 15.-16.10. CERT.LV pārstāvis piedalījās mācību "Locked Shields 2016" plānošanas sanāksmē Tallinā, Igaunijā.
- 22.-23.10. CERT.LV pārstāvis uzstājās ar prezentāciju FI-ISAC sanāksmē Cīrihē, Šveicē.
- 26.-28.10. CERT.LV pārstāvis piedalījās ENISA sanāksmē par mācību "Cyber Europe 2016" plānošanu Atēnās, Grieķijā.
- 16.-20.11. CERT.LV pārstāvji piedalījās NATO mācībās "Cyber Coalition".
- 07.-11.12. CERT.LV pārstāvis piedalījās CCDCoE kursos "Smartphone Security and Forensics" Tallinā, Igaunijā.
- 08.-10.12. CERT.LV pārstāvis piedalījās CCDCoE tehniskā vingrinājuma "Crossed Swords 2016" testa pasākumā Tallinā, Igaunijā.
- Turpinās gatavošanos starptautiskajai *Trusted Intrducer* sertifikācijai.

Sadarbība konkrētu incidentu risināšanā aprakstīta pārskata 2.punktā.

8. Citi normatīvajos aktos noteiktie pienākumi.

- 29.10. Notika sanāksme par 2016. gada IT drošības konferences plānošanu.
- 10.11. Notika tikšanās ar Komunikāciju aģentūru par iespējamo sadarbību Digitālās drošības alianses veidošanā.
- 12.11. Notika tikšanās ar Carnegie Melon universitātes pārstāvjiem par izglītošanas jautājumiem.
- 08.12. Notika tikšanās ar Microsoft par sadarbības iespējām.
- 14.12. Notika Skype intervija ar studentu, studiju pētījuma ietvaros.
- Tika uzsākta CERT.LV darbinieku atlase, izsludinot vakances un vadot darba intervijas.

9. Aģentūras papildu pasākumu veikšana.

Atskaite par Latvijas Interneta asociācijas Net-Safe Latvia Drošāka interneta centra ziņojumu līnijas darbību.

Latvijas interneta asociācijas „Net-Safe Latvia" drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.10.2015. līdz 31.12.2015. ir saņēmusi un izvērtējusi 97 ziņojumus. No tiem 46 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 7 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 11 ziņojumos konstatēta personas goda un cieņas aizskaršana. Par finanšu krāpšanas mēģinājumiem internetā saņemti 5 ziņojumi, 11 ziņojumu saturs nav bijis pretlikumīgs, 17 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 4 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 39 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā sadarbojoties ar Valsts policiju un interneta servisa piegādātājiem ir izdevies dzēst visus bērnu seksuālās izmantošanas materiālus, kas tika uzturēti Latvijā.

2015. gada 26. janvārī

Sagatavotājs – Svetlana Amberga
Tālrunis: 67085888
E-pasts: svetlana.amberga@cert.lv