Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2017

2017. gada 1. ceturksnis (01.01.2017. – 31.03.2017.)

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

2017.gada 1.ceturksnī CERT.LV apkopoja informāciju par 165 889 incidentiem. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, no 2017. gada 1. janvāra incidentu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija). Turpmāk statistikā visi CERT.LV reģistrētie un apstrādātie incidenti tiks uzskaitīt vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa infekciju (piemēram, Confiker, Zeus, Mirai) un ievainojamību (piemēram, Opendns, Openrdp) tipiem.

Pārskata periodā atbildīgas ievainojamību atklāšanas procesa ietvaros CERT.LV saņēma ziņu par XXE ievainojamību programmatūrā eParakstītājs un Java bibliotēkās. Atklātā ievainojamība neapdraudēja eParakstīšanas procesu, taču padarīja iespējamu attālinātu piekļuvi lietotāja failiem, bet, izmantojot Java bibliotēkas, arī servera failiem. CERT.LV sadarbībā ar LVRTC veica ievainojamības novēršanu, un tika izdota atjaunināta eParakstītāja versija 1.3.9.

Marta sākumā, atsaucoties uz Google publiskoto informāciju par kriptogrāfijas algoritma SHA1 ievainojamību, tika mainīts eParaksta radīšanai izmantotais kriptogrāfijas algoritms un izdota eParakstītāja versija 1.4.1.

Pārskata periodā turpinājās biznesa e-pastu kompromitēšana un krāpniecības mēģinājumi, izmantojot rēķinus ar mainītiem konta numuriem. Tika saņemti arī vairāki ziņojumi par uzbrukumiem, kuru realizācijā izmantota inovatīva pieeja, piemēram, piekļuves atteices uzbrukums (DDoS), kas realizēts, izmantojot milzīgu SPAM vēstuļu plūsmu, vai Facebook sociālā tīkla piekļuves datu izkrāpšana, izmantojot pašā sociālajā tīklā izveidotu lapu, kas neuzmanīgus lietotājus pārvirzīja no sociālā tīkla uz krāpniecisku vietni.

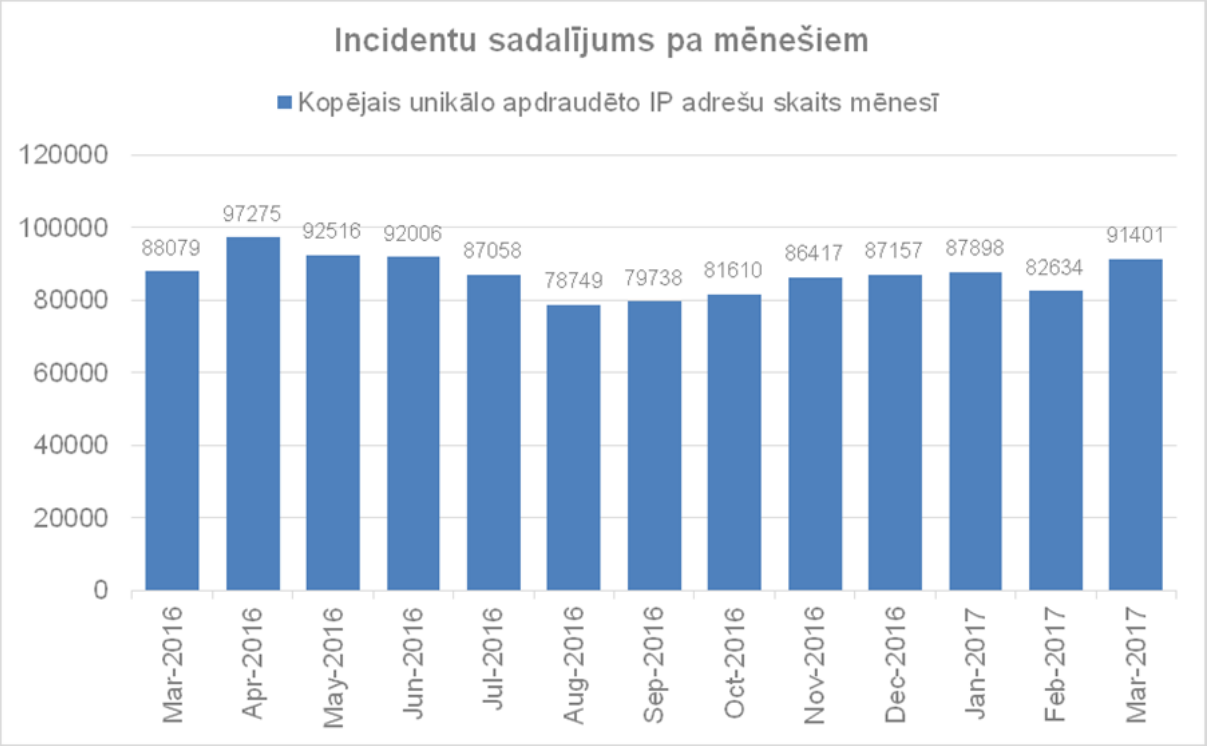
No 27. marta līdz 2. aprīlim Latvijā un Eiropā norisinājās E-prasmju nedēļa. CERT.LV iesaistījās Digitālās drošības dienas pasākumu organizēšanā un 29. martā notika Datorologa akcija.

Pārskata periodā CERT.LV par IT drošību izglītoja 2494 cilvēkus, iesaistoties 37 izglītojošos pasākumos, ievietoja 33 jaunas ziņas vietnē www.cert.lv, piedalījās 10 radio pārraidēs un 12 televīzijas sižetos.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums.

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, no 2017. gada 1. janvāra incidentu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija). Turpmāk statistikā visi CERT.LV reģistrētie un apstrādātie incidenti tiks uzskaitīt vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa infekciju (piemēram, Confiker, Zeus, Mirai) un ievainojamību (piemēram, Opendns, Openrdp) tipiem.

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 80 000 – 90 000 ievainojamu unikālu IP adrešu.

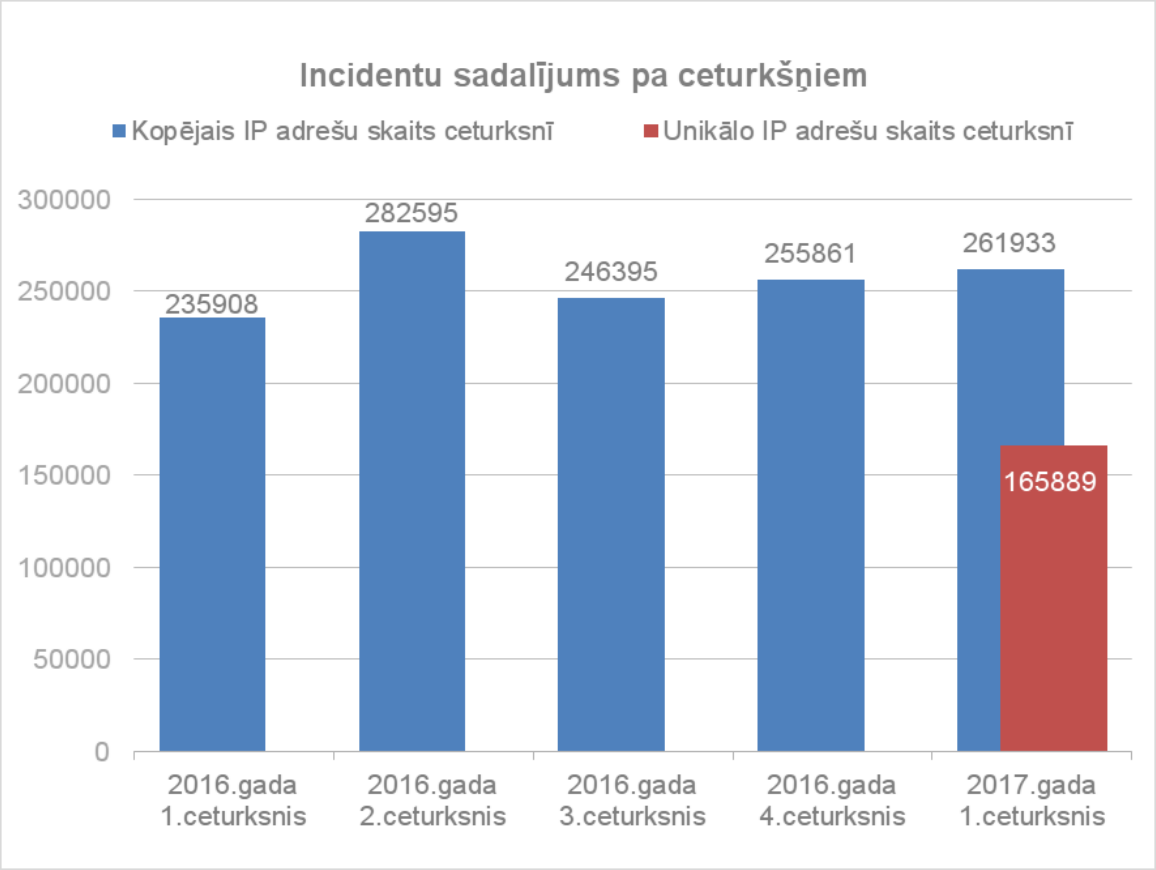


1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

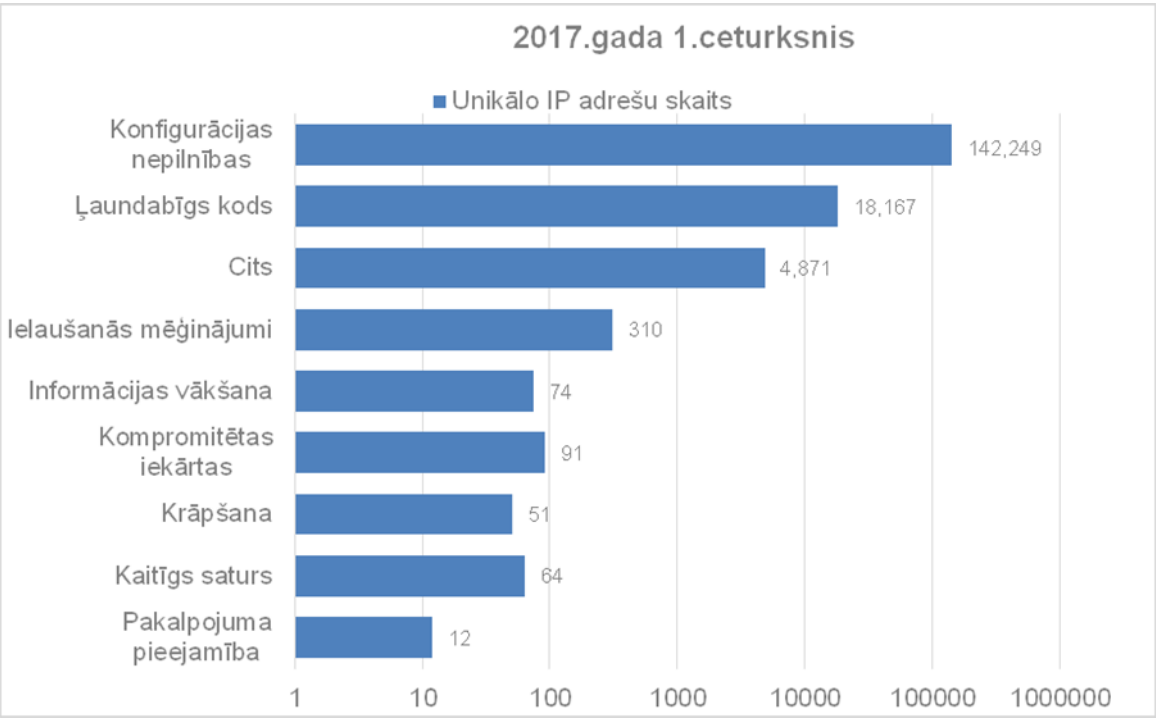
Divpadsmit mēnešu griezumā nav vērojamas būtiskas izmaiņas viena mēneša ietvaros apdraudēto IP adrešu daudzumā.

Līdz šim CERT.LV apkopoja informāciju par ceturksnī apdraudētajām IP adresēm, summējot katrā mēnesī apdraudētās IP adreses (2. attēls – zilie stabiņi). No 2017. gada janvāra CERT.LV veic uzskaiti pa unikālām IP adresēm, kas precīzāk atspoguļo kiberdrošības stāvokli, novēršot to, ka viena un tā pati IP adrese tiek pieskaitīta vairākas reizes (2. attēls – sarkanais stabiņš).

2017. gada 1. ceturksnī tika reģistrētas 165 889 unikālas apdraudētas IP adreses (izmantojot iepriekšējo metodi, tās būtu 261 933 IP adreses). Skaita atšķirība norāda uz to, ka vienas un tās pašas adreses tiek reģistrētas kā apdraudētas vairāku mēnešu garumā, jo apdraudējums netiek ilgstoši novērsts vai atkārtojas.

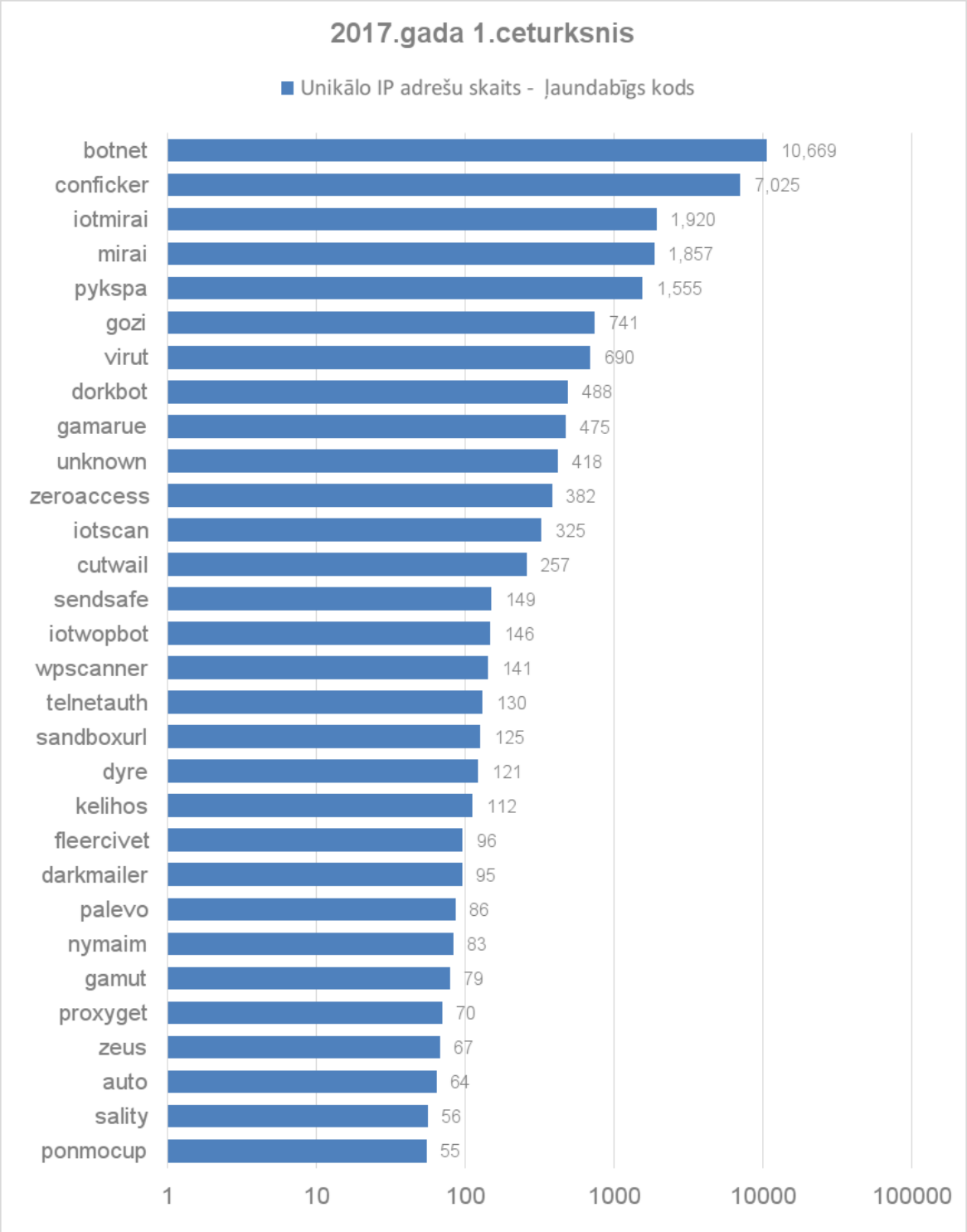


2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2016. un 2017. gadā.



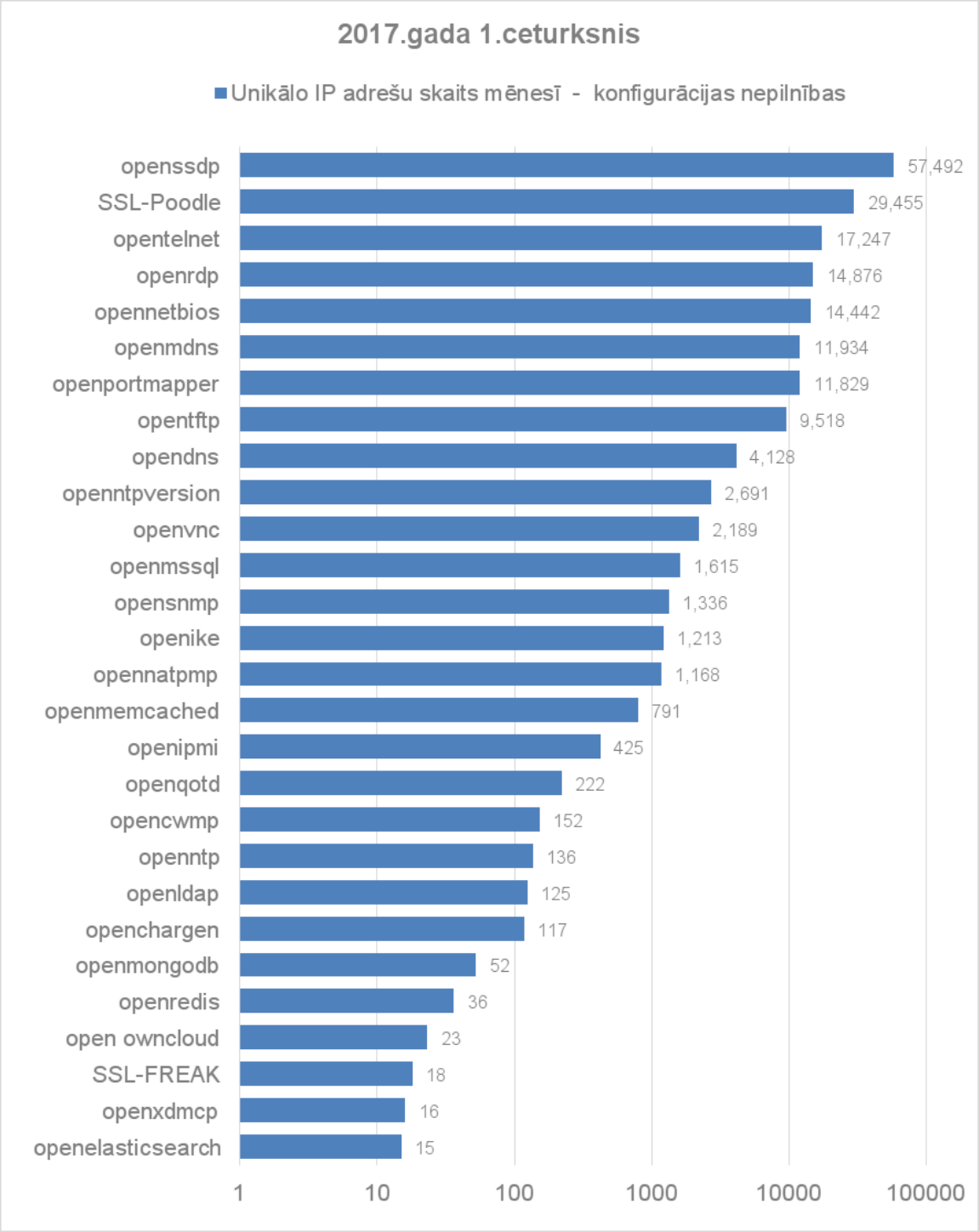
3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 1. ceturksnī pa apdraudējumu veidiem.

Izplatītākais apdraudējuma veids pārskata periodā bija konfigurācijas nepilnības, otrs izplatītākais bija ļaundabīgs kods, bet trešais izplatītākais bija ielaušanās mēģinājumi.



4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 1. ceturksnī ar apdraudējuma veidu - Ļaundabīgs kods.

Ļaunatūras izplatības topā nemainīgi atrodas Conficker, kaut arī ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra. Otro vietu stabili ieņem Mirai, kas lielākoties orientēta uz internetam pieslēgtām iekārtām (maršrutētājiem, novērošanas kamerām, u.tml.). Trešo vietu ieņem Pykspa, kas izplatās Skype platformā.



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2017. gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Lai samazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas Net-Safe Latvija Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar IPS, kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu sniedzējs" un informēt savus klientus par to iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS kopskaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

Uz to, ka atbildīga IPS nozīmība tiek novērtēta, norāda arī kādā publiski izsludinātā iepirkumā iekļautā prasība par „pretendenta sadarbību ar CERT.LV".

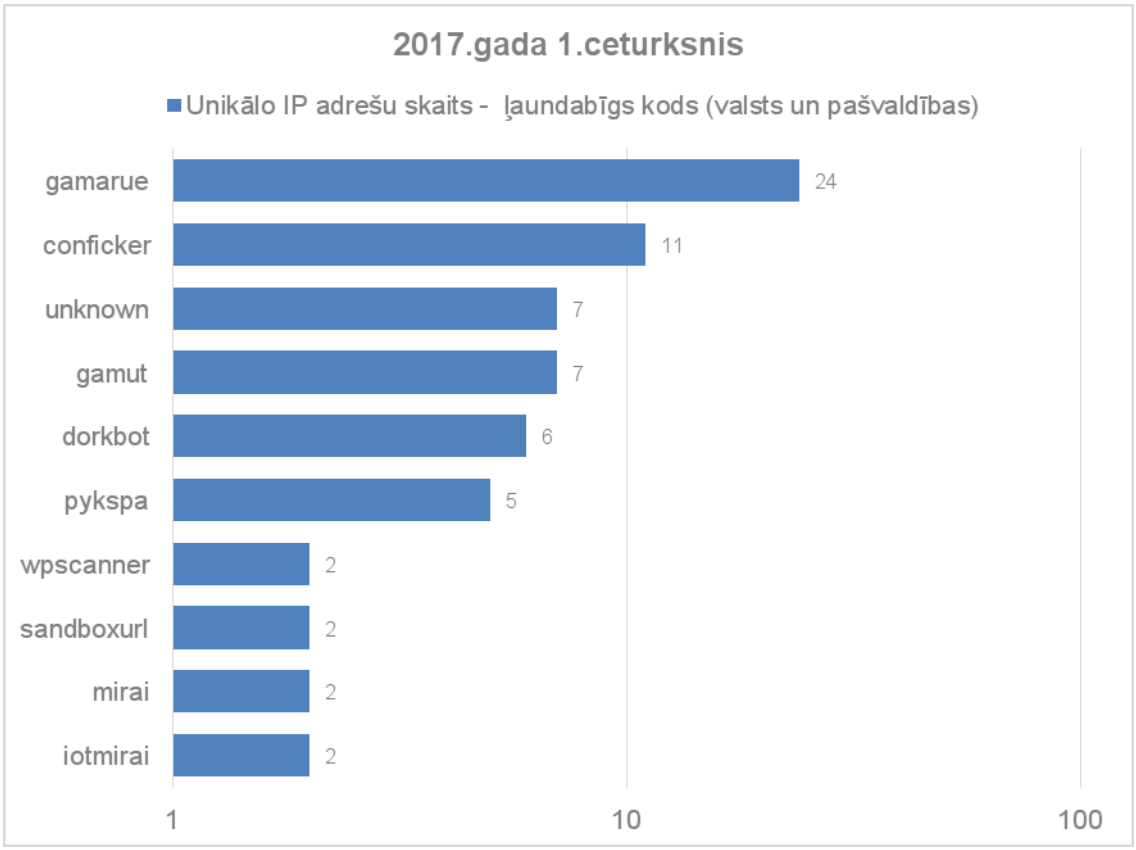
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

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 informē valsts un pašvaldību institūcijas, ja viņu IP adreses uzrādās kādā no ziņojumiem kā apdraudētas.

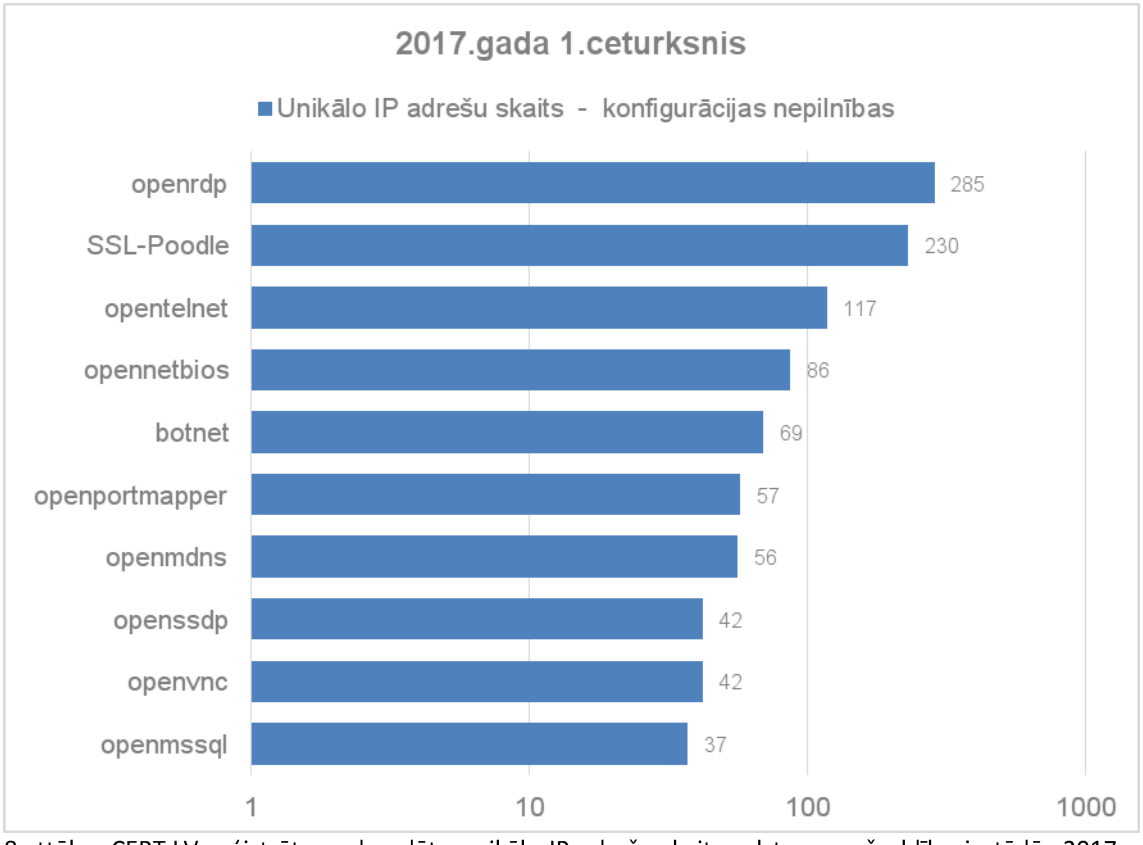
Izmaiņas katras dienas saņemtajos ziņojumos par valsts un pašvaldību iestādēm:

6.attēls – Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2017. gada 1. ceturksnī.

Palielinoties ziņojumu avotu skaitam, ir palielinājies arī katras dienas ziņojumos reģistrēto apdraudēto valsts un pašvaldību iestāžu IP adrešu skaits. Tādejādi CERT.LV iegūst pilnvērtīgāku ainu par valsts un pašvaldību iestāžu kibertelpā notiekošo.

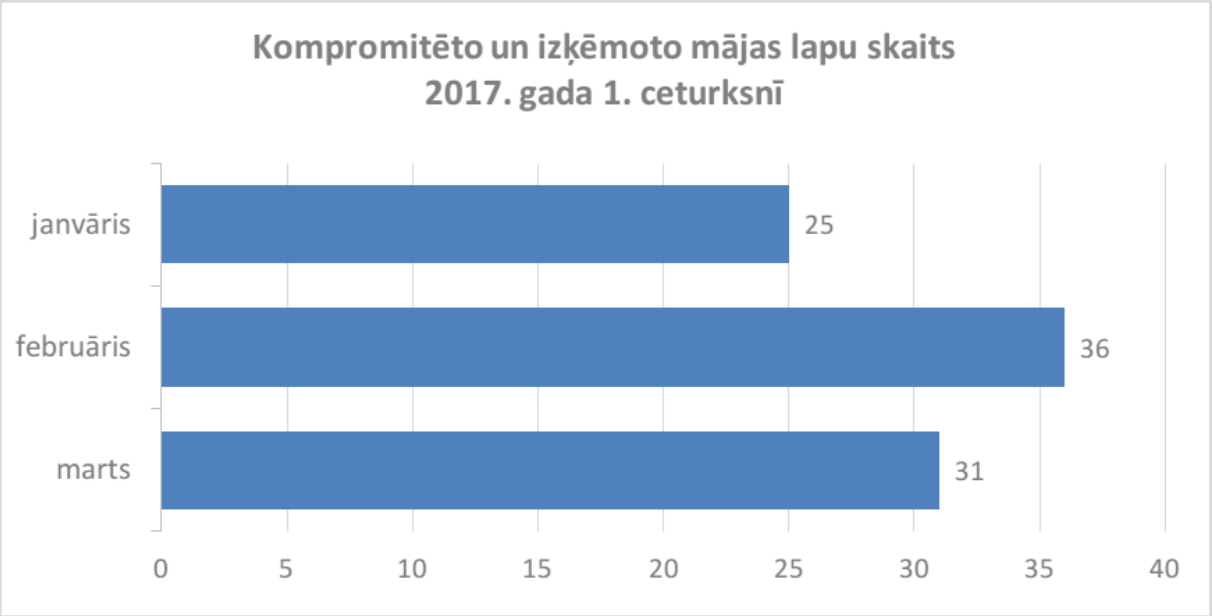


7.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2017. gada 1. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods (TOP 10).



8.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2017. gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība (TOP 10).

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 92 kompromitētas un izķēmotas tīmekļa vietnes. No visām izķēmotajām vietnēm 81 gadījumā vietnes uzturēšanai tika izmantota Linux operētājsistēma, 2 gadījumos Windows, 3 gadījumos FreeBSD, bet 6 gadījumos par izmantoto operētājsistēmu nav informācijas.



9.attēls – Kompromitēto un izķēmoto tīmekļa vietņu skaits pa mēnešiem 2017. gada 1. ceturksnī.

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

Svarīgākie CERT.LV risinātie drošības incidenti pārskata periodā:

- 10.01. Kāda uzņēmuma grāmatvedība saņēma viltotu e-pastu, kur tās valdes locekļa vārdā pieprasīts veikt 15 000 eiro pārskaitījumu uz banku Austrijā. Grāmatvede sazinājās ar uzņēmuma vadību un maksājumu neveica.
- 12.01. Tika saņemta informācija par Latvijas IP adresē esošu Cerber izspiedējvīrusa komand- un kontrolcentru. Resursa uzturētāji tika brīdināti un problēma atrisināta.
- Pērnā gada nogalē, atsaucoties uz publiski izskanējušo informāciju par CERT.LV veiktajām drošības pārbaudēm valsts un pašvaldību iestāžu interneta vietnēs, savā pārvaldībā esošo resursu pārbaudi lūdza vēl viena pašvaldība.

  Veiktās pārbaudes atklāja, ka pašvaldības resursos tiek lietota satura vadības sistēma (CMS) ar novecojušu versiju, kā arī tika konstatētas virkne citu ievainojamību, par kurām pašvaldība saņēma detalizētu pārskatu.
- 23.01. Vairāki lietotāji informēja CERT.LV par kredītkaršu datu krāpniecību Whatsapp vārdā. No domēna www.wathsappsoftware2017.com tika mēģināts izkrāpt kredītkaršu datus, brīdinot, ka pakalpojumam beidzas derīguma termiņš. Zemāk atradās lauki, kuros jāievada kredītkartes dati. CERT.LV brīdināja lapas uzturētāju Itālijā par to, ka vietne satur pikšķerēšanas lapu un aicināja vietni slēgt. Vietne tika slēgta un krāpnieciskas aktivitātes pārtrauktas.

- 23.01. Kāda komercbanka informēja CERT.LV par pārdomātu un mūsdienīgu SPAM uzbrukumu ar naudas izspiešanas mērķi. Sākot ar 22.01. iestādei tika nosūtīti ap 60 tūkstošiem e-pastu un tika veikts neliels demonstratīvs DDoS uzbrukums, izmantojot UDP Flood. Izsūtītie e-pasti bija no leģitīmiem serveriem, piemēram, scientificamerican.com, robly.com, u.t.t. No katra e-pasta izsūtīšanas servera tika nosūtītas ne vairāk par 20-30 vēstulēm. Pamatā tika izmantoti dažādi ziņu un mediju portāli, kuriem ir iespēja pierakstīties uz paziņojumiem par kādu raksta tēmu. CERT.LV sniedza ieteikumus, kā rīkoties šādos izspiešanas gadījumos – nekomunicēt ar izspiedējiem un nemaksāt. Tika pieprasīts slēgt uzbrucēju Google e-pasta adresi. Reāls pilna apjoma uzbrukums nesekoja.
- 24.01. Kāda uzņēmuma jaunā kases sistēma tika kompromitēta. Uzņēmums saņēma paziņojumu, ka datorā esošie faili ir šifrēti. CERT.LV informēja par tālāko rīcību šāda vīrusa gadījumā, un, ja datorvīrusa radītie bojājumi uzņēmumam radījuši būtiskus zaudējumus, lūdza informēt Valsts policiju.
- 26.01. Tika saņemta informācija par Latvijas IP adresi, kura tika izmantota *Cerber* šifrējošā izspiedējvīrusa un datu atgūšanas rīka "Cerber decryptor" izplatīšanai.
- 26.01. Pie CERT.LV vērsās vīrietis, kas iesaistījās akciju tirdzniecībā, izmantojot nelicenzētas kompānijas "Everest trade" pakalpojumus, un kļuva par kiberkrāpniecības upuri. Vīrietis nosūtījis krāpniekiem savu pases kopiju, vadītāja apliecības kopiju, rēķina paraugu, kur redzama viņa dzīvesvietas adrese, un bankas kartes kopijas, aizsedzot tikai pēdējos 3 ciparus, kā arī devis piekļuvi pie sava datora caur remote desktop, lai saņemtu apmācību tirdzniecības platformas lietošanā.

  Vīrietis vēlējās, lai CERT.LV pārbauda šīs kompānijas mājaslapu un nosaka, vai tā ir viltojums? Akciju tirdzniecībā vīrietis zaudēja vairāk kā 10 000 Eiro. Naudu nebija iespējams atgūt, gadījumu izskata policija. CERT.LV sniedza konsultācijas, kā labāk sevi pasargāt turpmāk.
- 30.01. CERT.LV sniedza informāciju kādai valsts iestādei par tās vārdā izveidotu viltus Twitter kontu, un aicināja iestādi kā oriģinālā iestādes konta uzturētāju pieprasīt viltus konta slēgšanu. Līdzīgi viltus konti tika konstatēti arī citām valsts institūcijām. Visi konstatētie viltus konti pāris dienu laikā tika slēgti.
- 09.02. Tika saņemta informācija par krāpšanas mēģinājumu, atsaucoties uz sludinājumu par automobiļa pārdošanu. Krāpnieki piedāvāja pārdevējam saņemt naudu uz PayPal kontu. Ja pārdevējs piekristu, viņam tiktu atsūtīts viltots naudas saņemšanas paziņojums. Šajā paziņojumā saņemtā summa pārsniegtu pārdošanas cenu un krāpnieki lūgtu pārskaitīt pārmaksu caur Western Union (vai līdzīgu servisu) viņu "aģentam" vai "kurjeram". Ja pārdevējs nepārbaudītu savu PayPal kontu un veiktu pārskaitījumu, viņš zaudētu naudu. Konkrētajā gadījumā pārdevējs krāpšanu atklāja un finansiāli zaudējumi radīti netika.

- 09.02. Kādas valsts iestādes darbinieks savā e-pastā saņēma 40 000 ziņas par nepiegādātiem SPAM e-pasta sūtījumiem. SPAM izsūtītāji kā atpakaļadresi bija norādījuši šī darbinieka e-pasta adresi. CERT.LV ieteica iestādei izveidot e-pasta filtru, kas dzēstu “bounce” atbildes.
- 10.02. CERT.LV saņēma informāciju par Facebook paroļu izkrāpšanas mēģinājumu. Sākumā lietotājs saņem brīdinājumu par to, ka viņa konts tiks deaktivizēts, un, lai tas nenotiktu, jānospiež uz saites. Lai neradītu aizdomas, lietotājs sākotnēji tiek pārvirzīts uz Facebook lapu, kura satur paziņojumu par konta slēgšanu un saiti, kuru aicina nospiest konta saglabāšanai. Tā kā sākotnējais paziņojums ir ievietots Facebook lapā, tas izskatās autentiski. Nospiežot uz saites, lietotājs tiek pārvirzīts uz viltotu lapu, kurā tiek aicināts ievadīt savu e-pastu un Facebook paroli. Ja lietotājs savus datus ievada, tie nonāk pie krāpniekiem. CERT.LV lūdza Facebook krāpniecisko lapu slēgt. Lapa tika slēgta.
- 14.02. Kāda uzņēmuma grāmatvede uz darba e-pastu saņēma vēstuli, kas sūtīta uzņēmuma vadītāja vārdā un lūdz veikt steidzamu maksājumu. Sūtītais e-pasts izrādījās viltots, un tam nebija nekāda saistība ar uzņēmuma vadītāju. Uzņēmums ziņoja par krāpniecību un lūdza CERT.LV šo e-pasta ziņojumu pārbaudīt. Krāpnieki nebija īpaši centušies pielāgot e-pasta adresi, bet izmantoja Yandex e-pastu.

  Krāpnieciskā teksta paraugs:
  "Mums nepieciešams veikt SEPA maksājumus €13,805(Euros) uz Angliju. Kādu informāciju jums ir nepieciešams saņemt šo izdarīt tagad?"
- 16.02. Pie CERT.LV vērsās kāds vīrietis, kas cietis no krāpniecības nelicenzētājā "Everest trade" akciju tirdzniecības platformā. Tirdzniecība ar akcijām sākusies ar nelielu summu, 500 dolāriem, taču ar laiku vīrietis ticis pārliecināts investēt arvien vairāk.

  Kopumā vīrietis ieguldījis ap desmit tūkstošiem savas naudas, bet kopējā akciju tirdzniecības bilance uzrādījusies lielāka - pat līdz 45 tūkstošiem, taču, lai naudu izņemtu, bija jāiemaksā vēl 15 tūkstoši eiro, operācijas pabeigšanai. Līdzīga situācija atkārtojusies vēl vairākas reizes, kamēr bilance izaugusi līdz 100 tūkstošiem, bet prasīts ieskaitīt vēl naudu operācijas pabeigšanai un konvertācijai. Ne ieguldīto, ne nopelnīto naudu vīrietim neizdevās saņemt, tāpēc viņš vērsās pie pašas platformas, ar ko strādā "Everest trade", taču arī tur nav saņēmis nekādu palīdzību naudas atgūšanai.

  CERT.LV ieteica vīrietim vērsties ar iesniegumu policijā. Arī Finanšu un kapitāla tirgus komisija (FKTK) brīdina par nelicencētas atvasināto finanšu instrumentu tirdzniecības platformas "Everest Trade" finanšu pakalpojumiem tās interneta vietnē https://everest.trade/en/. FKTK norāda, ka minētajam pakalpojumu sniedzējam nav tiesību nodarboties ar ieguldījumu pakalpojumu un ieguldījumu blakus pakalpojumu sniegšanu, tajā skaitā uzturēt atvasināto finanšu instrumentu tirdzniecības platformu.
- 17.02. Tika saņemta informācija par neautorizētu datu izgūšanu no kādas skolas tīmekļa vietnes. Analizējot tīklā pārraidītās datu plūsmas un veicot nelielu funkcionalitātes pārbaudi skolas mājas lapā, tika konstatēta SQL injekcijas ievainojamība. Par notikušo tika informētas atbildīgās iestādes, lapa uz laiku tika bloķēta, tika uzsākts darbs pie ievainojamības novēršanas.

- 22.02. Latvijā vairākas inficētas tīmekļa vietnes apmeklētājiem piedāvāja viltus Adobe Flash atjauninājumus. Ja lietotājs instalēja piedāvāto, tas tika inficēts ar banku vīrusu *Qadars*. Kompromitētas tika dažādas tīmekļa vietnes. Iespējams, ka tīmekļa vietnes tika kompromitētas, jo izmantoja novecojušu satura vadības sistēmas versiju Joomla 1.5.

  CERT.LV apzināja visas kompromitētās vietnes un lūdza nekavējoties izņemt kaitniecisko skriptu no vietnes, lai neapdraudētu lietotājus, atgādinot, ka satura vadības sistēmu (CMS) nepieciešams atjaunināt un pārbaudīt lapas drošību, lai nepieļautu atkārtotu kaitīgā skripta ievietošanu.

- 24.02. Atbildīgas ievainojamību atklāšanas procesa ietvaros CERT.LV saņēma ziņu par XXE ievainojamību programmatūrā eParakstītājs un Java bibliotēkās. Atklātā ievainojamība neapdraudēja eParakstīšanas procesu, taču izmantojot ievainojamību, būtu iespējams uzbrukums eParaksta lietotājiem, attālināti piekļūstot lietotāja failiem, bet, izmantojot Java bibliotēkas, arī servera failiem.

  CERT.LV veica ievainojamības novēršanas koordinēšanu, kā rezultātā ievainojamība tika novērsta, izdodot jaunāko eParakstītāja versiju 1.3.9.

  Programmatūras ievainojamību atklāja IT drošības speciālists Oskars Veģeris, kas jau iepriekš veiksmīgi un saskaņā ar atbildīgas ievainojamību atklāšanas labo praksi sadarbojies ar CERT.LV un LVRTC programmatūras drošības testēšanā. Par atklāto nepilnību tika informēts CERT.LV, kā arī sertifikācijas pakalpojumu sniedzējs - VAS LVRTC.

  Iesaistīto pušu rīcībā nav informācijas par gadījumiem, kad kāds ļaunprātīgi būtu izmantojis šo ievainojamību.

- 27.02. CERT.LV saņēma informāciju par vairāk kā 700 kompromitētiem maršrutētājiem, kas sūtīja lietotāju datus uz komandu un kontroles serveri. Minētās iekārtas izmantoja novecojušas DD-WRT programmatūras versijas, kas saturēja kritisku ievainojamību. Rezultātā uzbrucējs uz kompromitētajām iekārtām uzstādīja skriptu, lai ievāktu pa nešifrētajiem kanāliem pārsūtītus datus, ftp, http, pop u.c. paroles. CERT.LV uzsāka iekārtu turētāju apziņošanu un ieteica, kā atbrīvoties no ļaunatūras. Latvijā tika apzinātas piecas šādas iekārtas, pārējās iekārtas atradās citās pasaules valstīs.

- 28.02. Tika saņemta informācija par publiski pieejamiem personas datiem kādā tīmekļa vietnē. CERT.LV sazinājās ar vietnes uzturētājiem un lūdza informāciju dzēst vai padarīt publiski nepieejamu. Dati tika padarīti nepieejami.

- 28.02. Notika tikšanās ar LVRTC par jaunatklātu ievainojamību eParakstītāja programmatūrā. Ievainojamība LVRTC un CERT.LV tika paziņota atbilstoši atbildīgas ievainojamību atklāšanas labajai praksei.

- 01.03. Kāds vīrietis CERT.LV ziņoja par krāpniekiem, kas veica šantāžu un naudas izspiešanu. Vīrieti sociālajā tīklā uzrunājusi kāda sieviete no Lielbritānijas ar mērķi iepazīties un aicinājusi sarunu turpināt Skype platformā, kur lietotājs tika mudināts veikt dažādas intīmas darbības. Viss Skype notiekošais video zvans esot ticis nofilmēts. Vīrietim tika pieprasīta 500 mārciņas liela samaksa un piedraudēts, ka video tiks izplatīts Youtube un tiks nosūtīts visiem vīrieša kontaktiem Facebook, ja

samaksa netiks veikta. CERT.LV ieteica nekādā gadījumā nemaksāt izspiedējiem, jo izspiedēji var draudēt atkārtoti, un pieprasīt lielāku summu. CERT.LV ieteica vērsties policijā.

- 01.03. Kļuva pieejams programmatūras eParakstītājs 1.4.1. atjauninājums, kurā mainīts eParaksta radīšanai izmantotais kriptogrāfijas algoritms.

  Drošības atjauninājums tika ieviests, ņemot vērā pirms nedēļas starptautiskā tehnoloģiju uzņēmuma Google publiskoto informāciju par kriptogrāfijas algoritma SHA1 ievainojamību. Latvijā šāds kriptogrāfijas algoritms tiek izmantots virknē informācijas sistēmu un lietotņu, tostarp eParaksta radīšanai kopš tā ieviešanas 2006.gadā. Kopš Google paziņojuma par SHA1 ievainojamību š.g. 23.februārī, LVRTC speciālisti veica eParaksta un saistīto sistēmu drošības auditu un izstrādāja programmatūras atjauninājumu, izmantojot jaunākas paaudzes kriptogrāfijas algoritmu SHA256.

- 03.03. CERT.LV saņēma informāciju, ka satura vadības sistēmā "RIDemo CMS" atrasta ievainojamība. Ievainojamība ļāva veikt neautorizētu piekļuvi tīmekļa vietnes datubāzei, un iegūt paroles, kuras šī vadības sistēma šifrēja nedrošā veidā. Ievainojamības tips – SQL injekcija.

  Ietekmētas tika apmēram desmit tīmekļa vietnes, to starpā vairākas pašvaldību pārraudzībā esošas vietnes. CERT.LV sazinājās ar lapu uzturētājiem un informēja par atklāto ievainojamību. Vietņu turētāji uzsāka lapu labošanas darbus.

- 29.03. Tika saņemta informācija par infekciju kādas pašvaldības tīmekļa vietnē, kas apmeklētājus, kuri tīmekļa vietnē mēģināja nokļūt no Google meklēšanas rezultātiem, pārvirzīja uz reklāmvietnēm. Vietnes uzturētāji tika brīdināti.

- 29.03. Tika saņemta informācija par kādas valsts iestādes tīmekļa vietnes izķēmošanu. Vietnē tika izmantots failu menedžeris, kas bez autorizācijas atļāva augšupielādēt izpildāmus failus un kuru uzbrucējs izmantoja, lai augšupielādētu kaitīgo kodu. CERT.LV sniedza rekomendācijas vietnes drošības uzlabošanai.

CERT.LV pasākumi incidentu novēršanai:

- 08.02. CERT.LV izsūtīja informāciju valsts un pašvaldību iestādēm par pieejamajiem eParakstītāja atjauninājumiem.
- 06.03. CERT.LV izsūtīja informāciju valsts un pašvaldību iestādēm par nepieciešamību atjaunināt eParakstītāja programmatūru uz jaunāko versiju, jo programmatūrā tika mainīts kriptogrāfijas algoritms.
- Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta CERT.LV sagatavotajās iknedēļas ziņās un sociālā tīkla Twitter kontā (@certlv).

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 6. punktā.

3. Mobilo ierīču ļaunatūras pētniecība.

Mobilā ļaunatūra kļūst arvien aktuālāks apdraudējums. Par to liecina gan CERT.LV saņemtie ziņojumi, gan sabiedrības un mediju interese par mobilo ierīču drošības jautājumiem, gan arvien pieaugošais mobilo ierīču skaits, kas pie CERT.LV speciālistiem nonāk Datorologa akciju laikā.

Līdz šim CERT.LV eksperti saskārušies tikai ar tādu mobilo ļaunatūru, kas nav specifiska Latvijai, bet tas ir tikai laika jautājums, līdz parādīsies arī mobilā ļaunatūra, kas tiks mērķēta tieši uz Latvijas mobilo iekārtu lietotājiem.

Pārskata periodā tika saņemta informācija, ka Check Point pētnieki ir atklājuši nopietnu infekciju 38 dažādu ražotāju Android iekārtās. Tika noskaidrots, ka ļaunatūra telefonos uzinstalēta telefonu piegādes, ne ražošanas procesā.

Pētnieki iekārtās veica ļaunatūras izpēti un atklāja divus ļaunatūras paveidus - *Loki* un *SLocker*. Loki ir trojāns, kas darbojas pašā *Android* operētājsistēmas kodolā un iegūst "root" privilēģijas. Šis trojāns spēj piekļūt aplikāciju sarakstam, pārlūka vēsturei, kontaktu sarakstiem, zvanu vēsturei un atrašanās vietas datiem. *SLocker*, savukārt ir mobilais izspiedējvīruss.

Iegādājoties mobilās iekārtas no neautorizētiem piegādātājiem, lietotājiem ir lielāks risks, ka viņu iekārtas var būt jau inficētas ar kādu no augstāk minētajām ļaunatūrām.

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

Informācija par CERT.LV sadarbību ar medijiem

Pārskata perioda aktuālākās tēmas bija jaunā banku autentifikācija un ar to saistīto iekārtu drošība, kā arī E-prasmju nedēļas pasākumi.

1) **Intervijas un ziņas radio:**
   - 05.01. diskusija LR1 raidījumā „Kā labāk dzīvot" par maršrutētāju drošību
   - 10.01. diskusija LR1 raidījumā „Krustpunktā" par viltus ziņām un to, cik pasargāti esam no iespējamiem kiberuzbrukumiem
   - 13.02. diskusija LR1 raidījumā „Krustpunktā" par jauno banku autentifikāciju un mobilo iekārtu drošību
   - 16.02. komentārs LR1 raidījumā "Krustpunktā" par e-velēšanām
   - 16.02. diskusija LR4 raidījumā „Открытый вопрос" par jauno banku autentifikāciju un kiberdrošību
   - 24.02. diskusija LR1 raidījumā „Kā labāk dzīvot" par jauno banku autentifikāciju un kiberdrošību
   - 03.03. intervija LR4 ziņās par kiberriskiem
   - 21.03. sižets LR1 ziņās par to, kā Saeimas Cilvēktiesību un sabiedrisko lietu komisija kopā ar atbildīgajām iestādēm plāno pievērsties aktuālajiem jautājumiem kiberdrošības jomā un kiberdrošības politikas īstenošanā
   - 21.03. Intervija LR1 raidījumam "Pusdiena" par kiberdrošības situāciju Latvijā
   - 27.03. komentārs LR1 raidījumam "Pēcpusdiena" par atšķirībām starp kiberuzbrukumiem un troļļu darbību internetā

2) **Sižeti televīzijā, tiešraides:**
   - 12.01. intervija LTV raidījumam "Panorāma" par vīrusiem mobilajos telefonos
   - 13.01. intervija TV24 par kiberdrošības aktualitātēm
   - 15.01. komentārs LNT ziņās par kiberdrošības situāciju valstī
   - 29.01. intervija LTV raidījumam "De Facto" par atbildīgu ievainojamību atklāšanu un politiski motivētiem kiberuzbrukumiem
   - 07.02. intervija TV24 par kiberdrošības aktualitātēm
   - 13.02. intervija LTV raidījumam „4. studija" par datoru un viedtālruņu drošību
   - 20.02. sižets LTV raidījumā "Aizliegtais paņēmiens" ar praktisku eksperimentu, cik grūti ir iekļūt svešā datorā, un speciālistu ieteikumiem sevis pasargāšanai
   - 26.02. komentārs LNT ziņās par populāru interaktīvo lelli, kas var kļūt par spiegošanas rīku
   - 28.02. sižets LNT raidījumā "Bez Tabu" par sociālo tīklu viltus laimētavām
   - 22.03. dalība MixTV apaļā galda diskusijā "Дети и родители. Заметить друг друга" par bērnu drošību internetā
   - 23.03. intervija LTV7 raidījumā „Zhiznj segodnja" par kiberdrošību un sižets par Datorologu
   - 29.03. intervija studentu KIWI TV par paroļu drošību

3) Informācija par CERT.LV tīmekļa vietnēm:

https://www.cert.lv publicētas 33 ziņas. Populārākā bija Kontaktu sadaļa, kurai bija 1463 unikāli skatījumi. Otra populārākā bija sadaļa valsts un pašvaldību iestādēm par IT drošības pārvaldību, kuru skatījuši 1349 unikāli apmeklētāji. Trešā populārākā bija ziņa par aprīlī notiekošo IT drošības semināru "Esi drošs" ar 802 unikāliem skatījumiem. Kopā CERT.LV mājaslapai bijuši 15,293 lapu skatījumi, kurus veido 8,896 unikāli lapu skatījumi.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 13,899 apmeklējumi, no tiem 11,378 unikāli apmeklējumi. Portālā izveidota jauna sadaļa APSTĀJIES. PADOMĀ. PIESLĒDZIES., kurā tiek publicēti starptautiskās kiberdrošības iniciatīvas STOP. THINK. CONNECT. ieteikumi un materiāli. CERT.LV iniciatīvai pievienojās 2016. gada septembrī.

a izdevumus (Informācijas drošības biļetens, ko sagatavo SANS institūts). Pārskata periodā nopublicēti 3 jauni OUCH! numuri.

Portālā esidross.lv publicētie raksti:

- Sociālā inženierija
- Drošība ceļojot
- 29. martā CERT.LV aicina uz bezmaksas datora pārbaudi pie datorologa
- Mobilo aplikāciju droša izmantošana
- Digitālās drošības diena 28. martā

CERT.LV sociālo tīklu konti:

- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1666.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 519.
- CERT.LV draugiem.lv profila http://www.draugiem.lv/certlv sekotāju skaits pārskata perioda beigās bija 73.
- Sociālajā tīklā Google+ konts pārskata periodā tika dzēsts zemās aktivitātes dēļ.

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

10. janvārī CERT.LV tikās ar Vidzemes augstskolu, lai apspriestu maģistra programmas par kiberdrošību izveidi - tēmas un iespējamo CERT.LV iesaisti.

12. janvārī CERT.LV tikās ar LIKTA, lai vienotos par sadarbību E-prasmju nedēļas pasākumu organizēšanā, ņemot vērā, ka kiberdrošība šogad tika izvirzīta par vienu no prioritārajām tēmām e-prasmju apgūšanai.

25. janvārī un 3.martā CERT.LV pārstāvis piedalījās E-prasmju nedēļas pasākumu reģionālo koordinatoru sanāksmē VARAM.

14. februārī CERT.LV pārstāvis piedalījās bankas Citadele organizētajā pasākumā, kas veltīts mobilo iekārtu un bankas pakalpojumu drošībai.

20. februārī tikšanās ar Security Training Group pārstāvi, lai pārrunātu sadarbības iespējas IT drošības semināra „Esi drošs" ietvaros.

16. martā tikšanās ar LIKTA un citiem sadarbības partneriem par organizatoriskajiem jautājumiem E-prasmju nedēļas Digitālās drošības dienas semināriem-diskusijām.

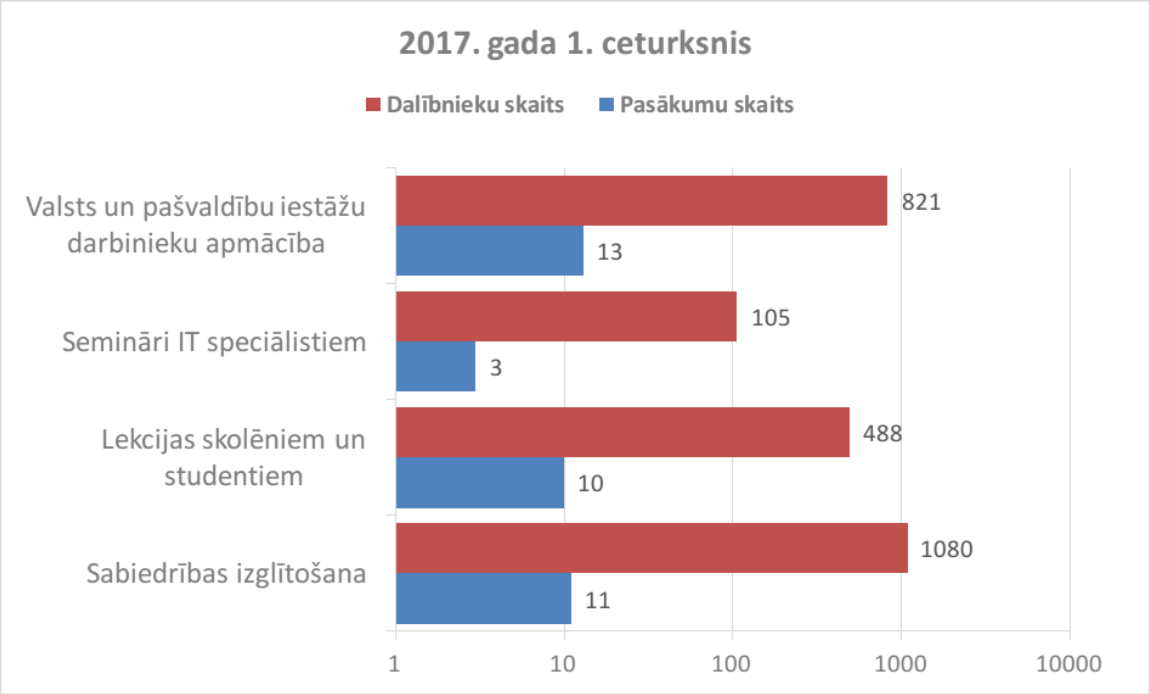
No 27. marta līdz 2. aprīlim Latvijā un visā Eiropā notika jau astotā E-prasmju nedēļa. Šogad pasākumā uzsvars tika likts ne tikai uz e-prasmju apgūšanu, bet arī uz kiberdrošību, tādēļ 28. marts tika izvēlēts par Digitālās drošības dienu. Šajā dienā tika organizēti trīs semināri-diskusijas, kas veltīti dažādām kiberdrošības tēmām: kiberdrošības politikai Latvijā, mobilai drošībai un lietu internetam un tā drošībai. CERT.LV pārstāvji piedalījās visās trijās diskusijās.

27. martā tika publiski paziņota CERT.LV gatavība pievienoties LIKTA sadarbības memorandam.

29. martā E-prasmju nedēļas ietvaros CERT.LV telpās norisinājās kārtējā Datorologa akcija, kuras laikā katrs interesents bez maksas varēja atnestu uz pārbaudi pie IT speciālista savu datoru, planšetdatoru vai viedtālruni un saņemt padomus savas iekārtas un datu aizsardzībai.

31. martā CERT.LV pārstāvis E-prasmju nedēļas ietvaros piedalījās VARAM organizētajā seminārā-tiešraidē "Tavas e-iespējas" un uzstājās ar prezentāciju „Realitāte virtuālajā vidē".

Pārskata periodā CERT.LV par IT drošību izglītoja 2494 cilvēkus, iesaistoties 37 izglītojošos pasākumos.



10.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2017. gada 1. ceturksnī.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 12.01., 09.02., 09.03. Notika kārtējās DEG sanāksmes.
- 13.01. Tikšanās Iekšlietu ministrijā par 7. savstarpējās novērtēšanas kārtu.
- 16.01. Tikšanās ar Valsts policiju par iespējamo sadarbību izglītošanas un apmācības jautājumos.
- 08.02. Tikšanās ar Kiberaizsardzības vienību.
- 16.02. Tikšanās Aizsardzības ministrijā par Kiberjaunsardzes projekta norisi.
- 27.02. Tikšanās Aizsardzības ministrijā par 2016. gada 6. jūlija direktīvas par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Eiropas Savienībā ieviešanu.
- 07.03. Tikšanās ar Tiesu administrāciju par sadarbības iespējām apmācību projekta īstenošanā
- 21.03. Dalība Saeimas Cilvēktiesību komisijas sēdē.
- 29.03. CERT.LV piedalījās sanāksmē Aizsardzības ministrijā par atbildīgu ievainojamību atklāšanas politiku. Sanāksmē tika apspriesti Valsts policijas un VARAM iebildumi un iespējamie nākotnes risinājumi.
- 29.03. CERT.LV pārstāvis piedalījās Saeimas Aizsardzības, iekšlietu un korupcijas novēršanas komisijas sēdē, kur 1. lasījumā tika izskatītas Informācijas tehnoloģiju drošības likuma izmaiņas.

- 30.03. Sanāksme Aizsardzības ministrijā par 2016. gada 6. jūlija direktīvas par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Eiropas Savienībā ieviešanas pasākumiem nacionālajā līmenī, tajā skaitā par pamatpakalpojumu sniedzēju identifikāciju

Sadarbība ar valsts iestādēm incidentu risināšanā aprakstīta atskaites 2. punktā.

7. 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.

Pārskata periodā CERT.LV izsūtīja 153 elektroniskās vēstules Elektronisko sakaru komersantiem par rīcības plānu atjaunošanu un izveidošanu. Tika saņemti 14 atjaunoti un 14 jauni ESK rīcības plāni. 10 ESK rakstiski apliecināja, ka neuztur publisko elektronisko sakaru tīklu, bet 2 ESK lūdza pagarināt rīcības plāna iesniegšanas termiņu.

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).

ITDL 61 pantā minētie gadījumi aplūkoti atskaites 2. punktā.

8. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām.

Pārskata periodā notika aktīva gatavošanās aprīlī notiekošajām NATO CCDCOE organizētajām kiberdrošības mācībām „Locked Shields 2017".

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 12.01. Kiberdrošības mācību „Locked Shields 2017" plānošanas konference.
- 17.01. CERT.LV pārstāvis piedalījās GEANT organizētajā "The Networking Conference" (TNC) programkomitejas sēdē, kurā tika veidota konferences programma.
- 17.01. Telekonferences zvans ar CyberGreen projekta pārstāvjiem par CyberGreen jaunā portāla izstrādi.
- 19.01. Telekonferences zvans ar United States European Command (EUCOM) par sadarbību kiberdrošības mācībās „Locked Shields 2017".
- 23.01. Tikšanās Aizsardzības ministrijā ar EUCOM par kiberdrošības mācībām „Locked Shields 2017".
- 23-25.01. CERT.LV pārstāvji piedalījās TF-CSIRT sanāksmē un FIRST reģionālajā simpozijā Valensijā, CERT.LV pārstāvis prezentēja „Firmware over the air, case study of ADUPS Fota".
- 30.01. CERT.LV pārstāvis telefoniski piedalījās publiskajās konsultācijās par ENISA aģentūras darba novērtēšanu.
- 08.02. Tikšanās ar Kiberaizsardzības vienību par sadarbību un dalību kiberdrošības mācībās „Locked Shields 2017".
- 21.02. CERT.LV pārstāvji piedalījās Tīklu un informācijas drošības direktīvas izveidotā Informācijas tehnoloģiju drošības incidentu novēršanas institūciju sadarbības tīkla (CSIRT network) sanāksmē Maltā.
- 01.03. CERT.LV pārstāvji piedalījās CENTR General assembly Jūrmalā un iepazīstināja pasākuma dalībniekus ar TF-CSIRT aktualitātēm, kā arī sniedza prezentāciju „Cybercrime friendly sales policy... Who is happier in the long run?".
- 06.-10.03. CERT.LV pārstāvis piedalījās CCDCOE organizētajos kursos „Cyber Defence Monitoring Course Suite Module 1" Tallinā.
- 11.-17.03. CERT.LV pārstāvis piedalījās Microsoft Digital Crimes Consortium konferencē.
- 13.03. CyberGreen projekta jaunā portāla beta versijas izvērtēšana un atzinumu sniegšana.
- 14.-15.03. CERT.LV pārstāvis piedalījās kiberdrošības mācību „Locked Shields 2017" izmēģinājumā.
- 15.03. CERT.LV pārstāvis piedalījās TF-CSIRT Steering committee stratēģijas sanāksmē Šveicē.
- 20.03. Telekonference ar ENISA pārstāvjiem par kiberdrošības apmācību organizēšanu Rīgā.
- 21.03. CERT.LV pārstāvis piedalījās seminārā Briselē, Beļģijā, kurā tika vērtēta ENISA aģentūras darbība pēdējos 8 gados un diskutēts par ENISA nākotnes uzdevumiem, mandātu un stratēģiju.

- 22.03. Tikšanās ar Kiberaizsardzības vienību par kiberdrošības mācībām „Locked Shields 2017”.
- 30.03. CERT.LV pārstāvis piedalījās kiberdrošības mācību „Locked Shields 2017” sagatavošanās konferencē Tallinā, Igaunijā.

Sadarbība konkrētu incidentu risināšanā aprakstīta pārskata 2.punktā.

9. Citi normatīvajos aktos noteiktie pienākumi.

- 16.01. Tikšanās ar Lattelecom, lai apspriestu līdzšinējo sadarbības modeli un iespējamos uzlabojumus.
- 15.02. Ēnu dienas ietvaros CERT.LV ekspertu ēno 10. klases skolnieks.
- 09.03. CERT.LV pārstāvis nokārtoja Fizisko personu datu aizsardzības speciālista eksāmenu, iegūstot tiesības veikt personas datu aizsardzības speciālista pienākumus.
- 31.03. CERT.LV pārstāvis saņēma ISACA sertifikācijas komisijas piešķirto CISA kvalifikāciju.
- 31.03. Tikšanās ar Eiropas Komisijas nolīgtajiem konsultantiem par aptauju un pētījumu par to, kā Latvijā darbojas Eiropas pilsoņu iniciatīvas regula Nr. 211/2011.

10. Ar Elektroniskās identifikācijas uzraudzību saistīto pienākumu izpilde.

Saskaņā ar MK 2015. gada 3. februāra sēdes protokolā Nr. 6 27. §, ar kuru pieņemts zināšanai informatīvais ziņojums “Par kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību noteikto’’ CERT.LV pārskata periodā turpināja noteikto funkciju veikšanu.

Iepriekšminēto funkciju izpildei veikto darbu uzskaitījums:

- CERT.LV pārstāvji piedalījās sanāksmē, kurā izskatīja uz Fizisko personu elektroniskās identifikācijas likuma pamata izstrādāto Ministru kabineta noteikumu projektus. Sanāksmē piedalījās arī informācijas tehnoloģiju eksperti no privātā sektora, kuri sniedza savu redzējumu un ieteikumus šo noteikumu precizēšanai.
- CERT.LV pārstāvji piedalījās LVRTC rīkotajā sanāksmē, kurā LVRTC informēja par uzticamu sertifikācijas pakalpojumu sniedzēju audita gaitu.
- CERT.LV pārstāvis piedalījās Coopertion Network group sanāksmē, lai runātu par Vācijas elektroniskās identifikācijas shēmas priekšpaziņošanu un peer review jautājumiem.
- CERT.LV pārstāvis savas kompetences ietvaros sniedza komentārus pārskatam par uzticamības pakalpojumu sniedzējiem (UPS) Latvijā Eiropas Komisijai, ko veidoja Datu valsts inspekcija. UPS jautājumā izveidots informatīvais ziņojums par uzticamības

pakalpojumu pārņemšanas iespēju, uzticamības pakalpojumu sniedzējam beidzot savu darbību.

- CERT.LV piedalījās sanāksmē ar privātā sektora un Ministru kabineta noteikumu izstrādē iesaistītās institūcijas piedalīšanos par Fizisko personu elektroniskās identifikācijas likuma Ministru kabineta noteikumiem.

11. 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 01.01.2017. līdz 31.03.2017. ir saņēmusi un izvērtējusi 150 ziņojumus. No tiem 33 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 13 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 23 ziņojumos konstatēta personas goda un cieņas aizskaršana, 16 gadījumos konstatēti vardarbīga rakstura materiāli un 3 ziņojumi saņemti par naida runu. Par finanšu krāpšanas mēģinājumiem internetā saņemti 2 ziņojumi, 25 ziņojumu saturs nav bijis pretlikumīgs, 35 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 23 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 6 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.

2017. gada 3. maijā
Sagatavotājs – Līga Besere
Tālrunis: 67085888
E-pasts: liga.besere@cert.lv