Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Publiskais pārskats par CERT.LV uzdevumu izpildi

2016

2016. gada 3. ceturksnis (01.07.2016. – 30.09.2016.)

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

2016.gada 3.ceturksnī CERT.LV reģistrēja un apstrādāja 850 augstas prioritātes incidentus un 245 545 zemas prioritātes incidentus.

Viena no būtiskajām ceturkšņa iezīmēm ir mērķēti uzbrukumi, kas vērsti uz valsts un pašvaldību iestādēm, ar mērķi izkrāpt no darbiniekiem piekļuves datus iestāžu IT resursiem. Šādu uzbrukumu ietekmes mazināšanai ir svarīga lietotāju izglītošana, palielinot viņu spēju atpazīt šādus uzbrukumus un padarot viņus noturīgākus pret sociālās inženierijas paņēmieniem.

Otrs pārskata periodam raksturīgs incidentu veids ir "CEO krāpšana", kurā izmanto viltotus e-pastus, kas tiek sūtīti kompānijas vadītāja vai sadarbības partnera vārdā, lai panāktu nozīmīgu naudas summu pārskaitīšanu uz krāpnieku bankas kontiem. Ļaundari bieži piekļūst uzņēmumu e-pastiem, izmantojot sociālo tīklu piekļuves datu noplūdēs iegūto informāciju, jo daudzi lietotāji virknē interneta resursu izmanto identiskas paroles. Otrs biežākais paroles iegūšanas veids ir datora inficēšana ar ļaunatūru. Iegūstot kontroli pār e-pastu, ļaundari var precīzi izpētīt situāciju un atbilstošajā brīdī veikt ļoti ticami noformētu uzbrukumu. Lietotās programmatūras regulāra atjaunināšana un atšķirīgu paroļu izmantošana mazina e-pastu uzlaušanas risku.

Kā trešais būtiskais ceturksni raksturojošais incidentu veids saglabājas šifrējošie izspiedējvīrusi. Vīrusi kampaņveidīgi tika izplatīti e-pasta ziņojumos, kas saturēja Microsoft Word dokumentus ar Macros aktīvā koda funkcionalitāti. Kaitīgie e-pasti tika sūtīti gan uzņēmumiem, gan individuāliem datorlietotājiem. Atsevišķos gadījumos lietotājiem bija laicīgi sagatavotas svarīgo dokumentu rezerves kopijas, taču daļa lietotāju par rezerves kopijām nebija parūpējušies un nošifrētos failus atgūt nespēja.

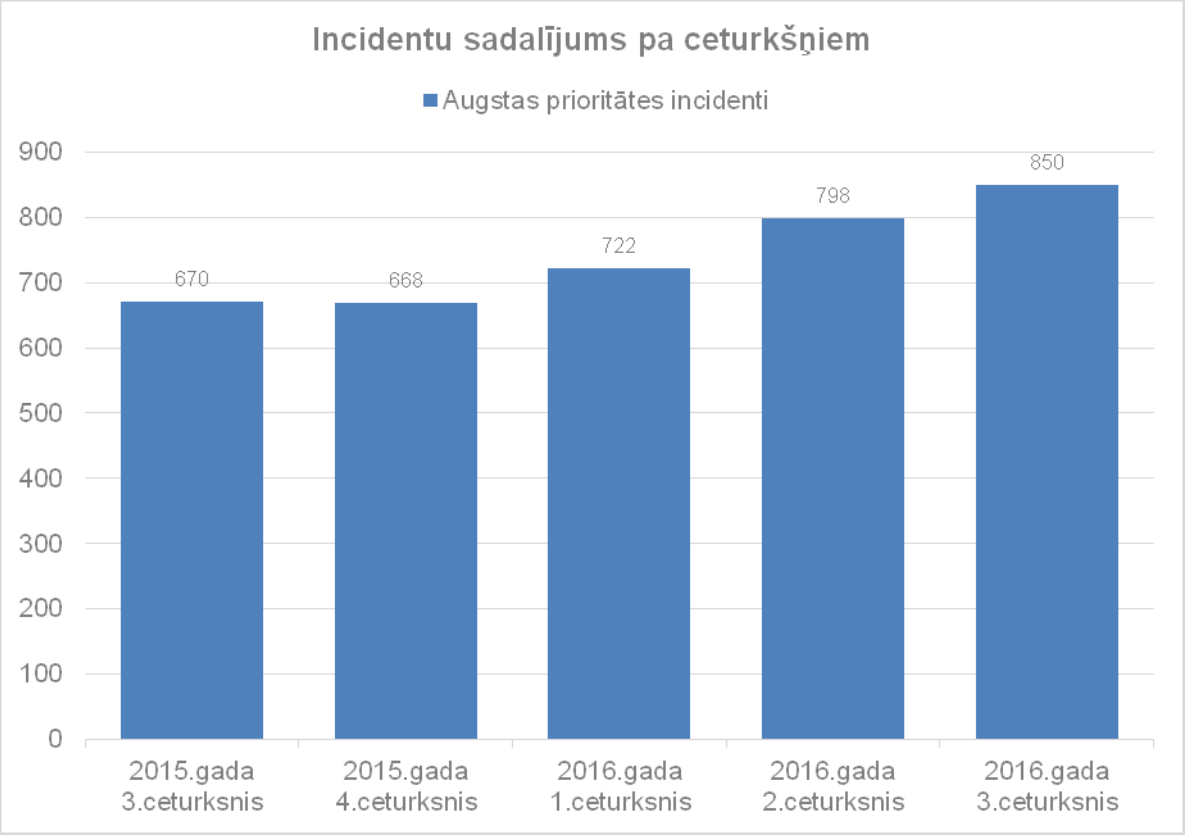
Pārskata periodā noritēja aktīvs sagatavošanās darbs oktobrī notiekošajai ikgadējai CERT.LV un ISACA Latvijas nodaļas konferencei "Kiberšahs 2016". Dalībnieku pieteikumu skaits šogad bija rekordliels un pārsniedza 700.

Pārskata periodā CERT.LV par IT drošību izglītoja 1987 cilvēkus, iesaistoties 19 izglītojošos pasākumos, ievietoja 28 jaunas ziņas vietnē www.cert.lv, piedalījās 2 radio pārraidēs un 4 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.

2016. gada 3. ceturksnī CERT.LV apstrādāja 850 augstas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti un apstrādāti 798 augstas prioritātes incidenti, bet 2015. gada 3. ceturksnī 670 augstas prioritātes incidenti.

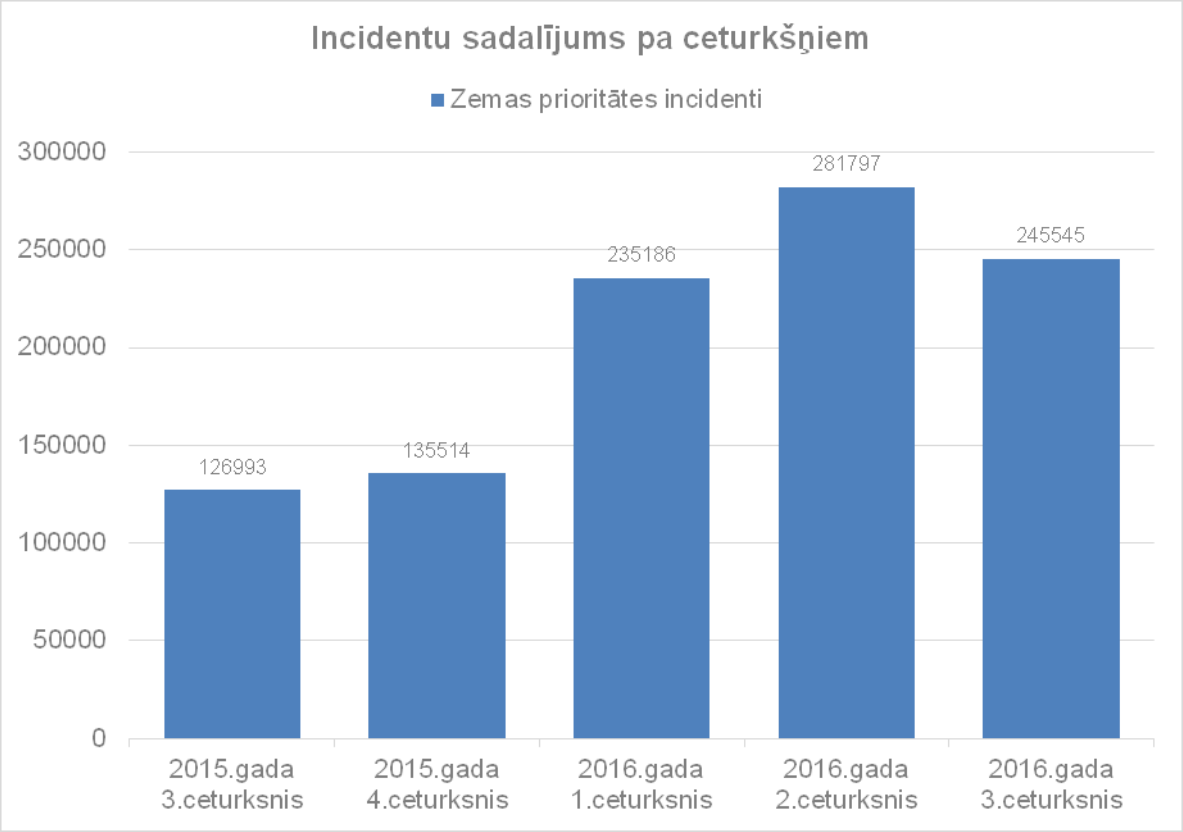


1.attēls – CERT.LV reģistrētie augstas prioritātes incidenti pa ceturkšņiem 2015. un 2016. gadā.

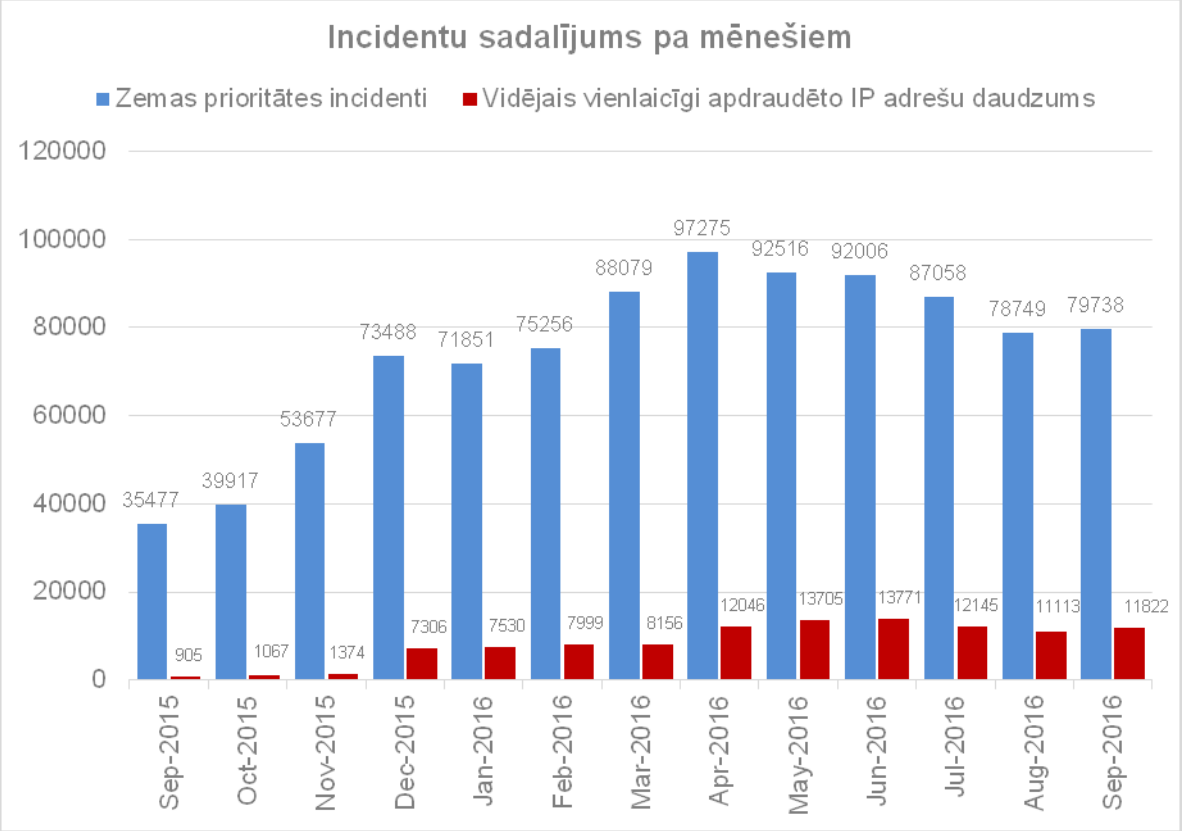
Vairāku ceturkšņu garumā vērojamais salīdzinoši nelielais, bet stabilais augstas prioritātes incidentu apjoma pieaugums skaidrojams ar to, ka CERT.LV ir vairojis sabiedrības uzticību un ziņojumi par IT drošības incidentiem tiek saņemti ne tikai no institūcijām, kurām par incidentiem ir pienākums ziņot likumā noteiktajā kārtībā, bet arī no privātā sektora uzņēmumiem un individuālām privātpersonām, gan situācijās, kad ziņotājs ir arī cietušais, gan situācijās, kad novēroti kaitnieciski resursi vai darbības virtuālajā vidē.

2016. gada 3. ceturksnī CERT.LV reģistrēja 245 545 zemas prioritātes incidentus. Iepriekšējā ceturksnī tika reģistrēti 281 797 zemas prioritātes incidenti, bet 2015. gada 3. ceturksnī 126

993 zemas prioritātes incidenti.



2.attēls – CERT.LV reģistrētie zemas prioritātes incidenti pa ceturkšņiem 2015. un 2016.gadā.



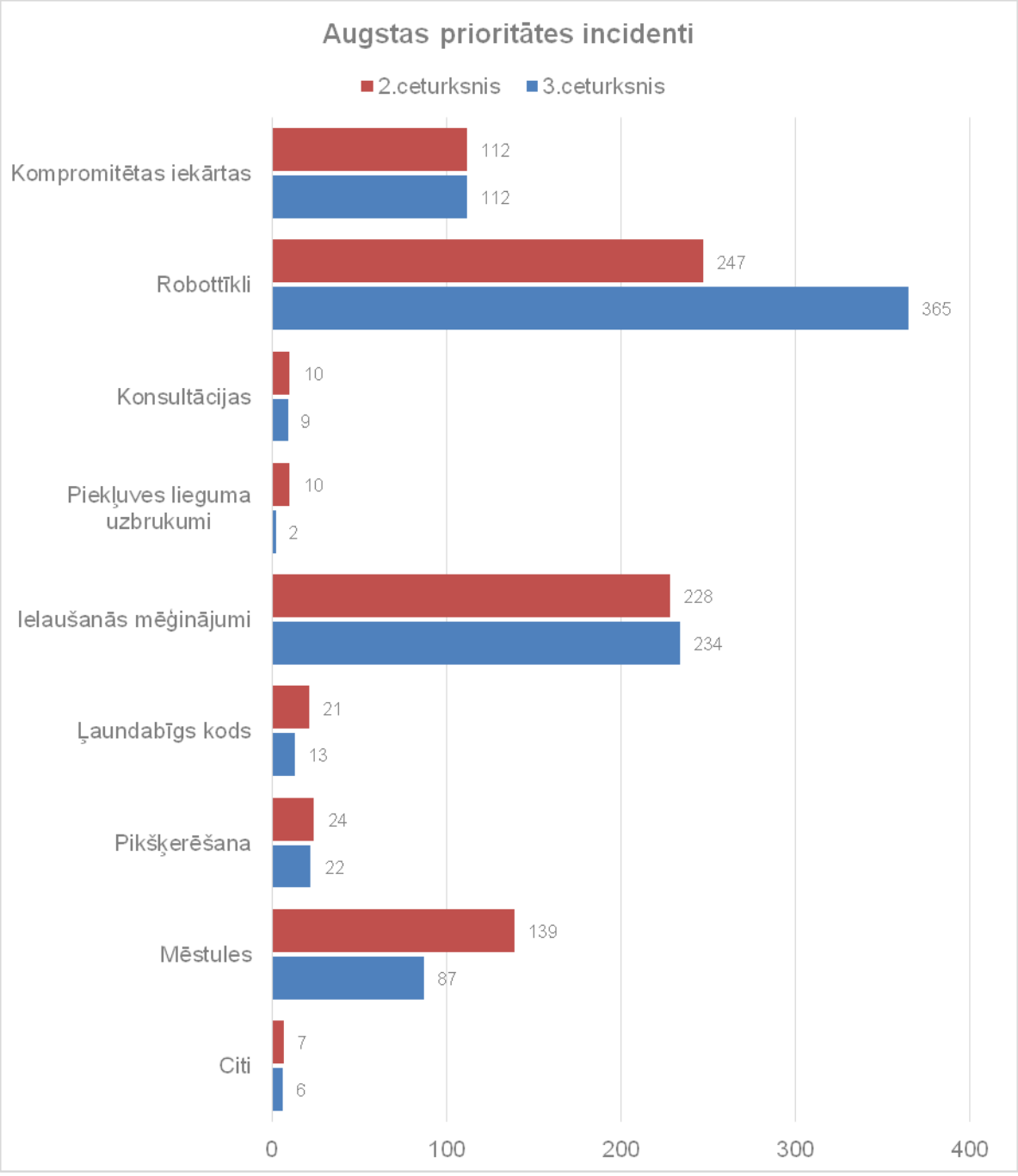
3.attēls – CERT.LV reģistrētie zemas prioritātes incidenti un vidējais vienlaicīgi apdraudēto IP adrešu daudzums 2015. un 2016. gadā.

Katru mēnesi CERT.LV rēķina vidējo vienlaicīgi apdraudēto unikālo IP adrešu skaitu Latvijā, kas pārskata periodā piedzīvojis nelielu kritumu, salīdzinot ar iepriekšējo pārskata periodu, kas savukārt saistīts ar kopējo zemas prioritātes incidentu apjoma samazinājumu.

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 gala lietotājus par to iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS kopskaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

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

Pārskata periodā CERT.LV reģistrēja un apstrādāja 850 augstas prioritātes incidentus.



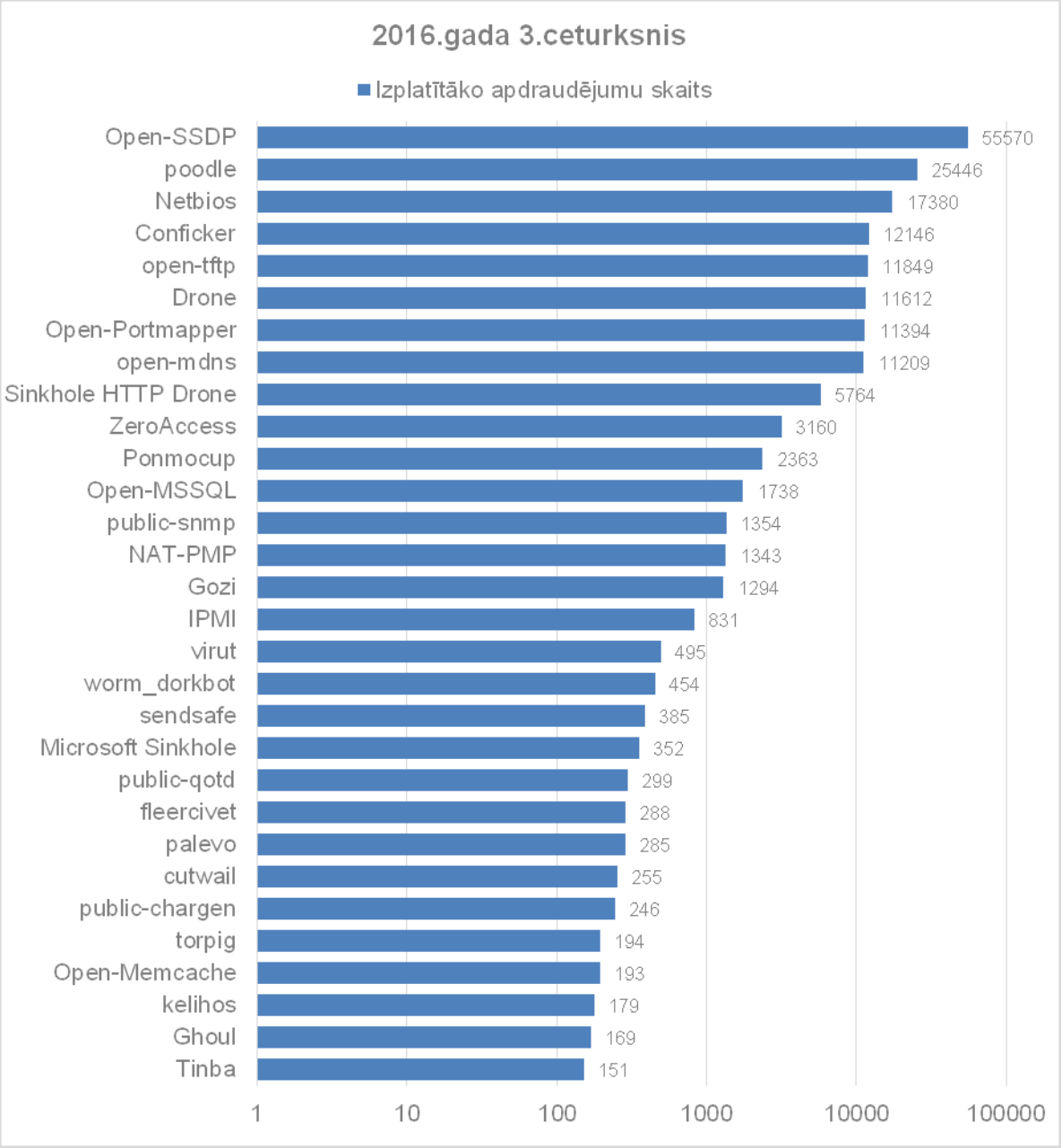
4.attēls – CERT.LV apstrādātie augstas prioritātes incidenti pa tipiem 2016. gada 2. un 3. ceturksnī.

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:

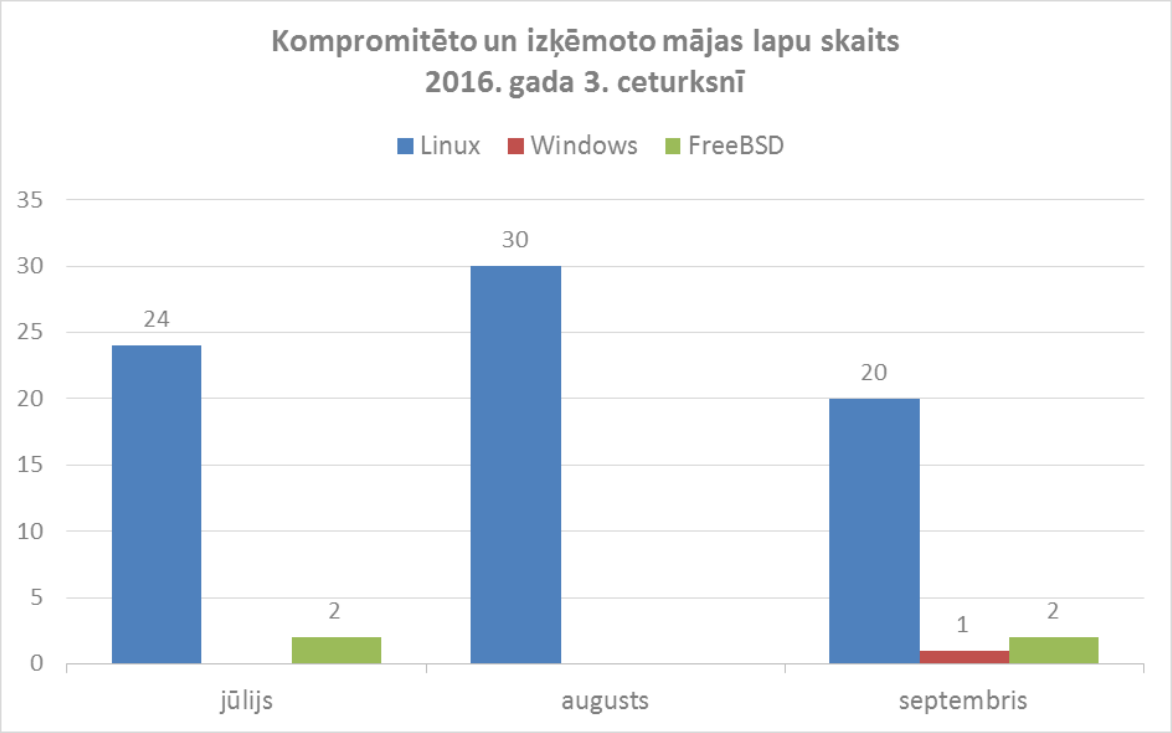
5.attēls - Iestāžu apdraudēto IP adrešu daudzums katras dienas saņemtajos ziņojumos 2016.gada 3.ceturksnī.

2016. gada 3. ceturksnī CERT.LV reģistrēja 245 545 zemas prioritātes incidentus.



6.attēls – CERT.LV reģistrētie zemas prioritātes incidenti no 2016. gada 1. jūlija līdz 30. septembrim pa apdraudējumu veidiem.

CERT.LV uzskaita arī kompromitēto un izķēmoto mājaslapu gadījumus.



7.attēls – Kompromitēto un izķēmoto mājas lapu skaits pa mēnešiem 2016. gada 3. ceturksnī.

Pārskata periodā kompromitēto un izķēmoto mājas lapu skaits nav būtiski mainījies, salīdzinot ar iepriekšējo periodu.

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:

- 04.07. CERT.LV turpināja veikt ievainojamību novēršanas koordināciju sadarbībā ar Ķīnas nacionālo CSIRT vienību CNCERT, IP kameru ražotāju Milesight un ievainojamību atklājēju Kirilu Solovjovu.. CERT.LV uzstāja uz ražotāja atbilstošu reakciju un nepieciešamību iegūt programmatūras labojumus, jo vairāki simti ievainojamu iekārtu tika atklāti kādā valsts iestādē. Tika panākta atklāto ievainojamību novēršana un ražotājs izsniedza programmatūras ielāpus. Šis process prasīja koordinēšanas darbu 8 mēnešu garumā.
- 07.07. Kāda novada pašvaldības tīkla maršrutētājos tika mēģināts iekļūt, piemeklējot paroli standarta “admin” lietotājam. Tas neizdevās, jo šis lietotājs bija pārsaukts. Šādi uzbrukumi apdraud iekārtas, kam ir atstāta ražotāja konfigurācija un uzstādīta vāja parole.
- 12.07. Klients ziņoja CERT.LV par ievainojamību kādas iestādes e-pakalpojumā. Ar šīs ievainojamības starpniecību bija iespējams nesankcionēti piekļūt citu personu datiem iestādes datu bāzē pēc līdzīga principa, kā tas bija iespējams VID (Neo) gadījumā. CERT.LV, veicot pārbaudes, identificēja vēl vairākas ievainojamības, kuru novēršanu koordinēja ar sistēmas turētāju. Ievainojamības tika novērstas.

- 16.07. CERT.LV saņēma informāciju par uzbrukumu kādai elektronisko biļešu tirdzniecības vietnei. Uzbrukuma rezultātā uzbrucēji ieguva informāciju, kuru izmantoja viltotu biļešu izgatavošanai. CERT.LV sniedza atbalstu Valsts policijai incidenta izmeklēšanā.
- 02.08. No kāda uzņēmuma partneriem, izmantojot viltotu rēķinu, izkrāpta samaksa par kokmateriālu sūtījumu. Ziņas par darījumu iegūtas, ielaužoties uzņēmuma e-pastā, kura piekļuves dati iegūti no datora, kas inficēts ar ļaunatūru. Pēc datoru iztīrīšanas un paroļu maiņas atkārtotie uzbrukumi nav bijuši sekmīgi.
- 05.08. Kādas valsts iestādes datorā tika atklāta kriptovīrusa infekcija. Ar vīrusu inficēts e-pasts tika nosūtīts sekretārei, kura atvēra saņemto e-pastu. Rezultātā tika sašifrēts dators un tīkla mape. Saturs tika atjaunots no rezerves kopijām, būtisks kaitējums iestādei netika nodarīts.
- 09.08. Tika identificēts un novērsts mērķēts kiberuzbrukums kādai valsts iestādei. Uzbrukumā tika izmantots e-pasts, kas noformēts kā uzaicinājums uz Orlando, ASV notiekošu konferenci par cilvēktiesību aizstāvību. Lai arī uzbrucēji mēģināja e-pastu noformēt kā Starptautiskās cilvēktiesību organizācijas sūtītu, tehniskās indikācijas norādīja uz resursiem Ungārijā un ASV, kuriem nav nekādas saistības ar Starptautisko cilvēktiesību organizāciju.
- 10.08. CERT.LV nodeva informāciju Valsts policijai par Latvijā uzturētu šifrējošā vīrusa Zepto kontrolcentru.
- 10.08. Kādas iestādes izmantotais BARRACUDA mēstuļu filtrs no izstrādātājiem saņēma atjauninājumu, kas saturēja kļūdainu CVE-2016-3316 (Microsoft Office Memory Corruption Vulnerability) detektēšanas nosacījumu. Rezultātā vairākas stundas caur iestādes e-pasta sistēmu nebija iespējams nosūtīt MS Office Word dokumentus. Nākamais filtru atjauninājums šo kļūdu izlaboja.
- 11.08. CERT.LV atklāja virkni kritisku ievainojamību kādas iestādes tīmekļa vietnē. Atbildīgās personas par atklātajām ievainojamībām tika informētas un ievainojamības tika novērstas.
- 19.08. Vairāku finanšu institūciju darbinieki savos pasta kontos saņēma krāpnieku sagatavotus e-pastus, kas sūtīti ar mērķi izkrāpt lietotāja datus, ievilnot saņēmēju apmeklēt interneta vietni, kas noformēta līdzīgi leģitīma pasta pakalpojumu sniedzēja vietnei. Kaitīgā vietne izvietota uz uzlauzta tīmekļa serveru pakalpojumu sniedzēja servera Čehijā.
- 23.08. Kādas skolas tīmekļa vietne tika izmantota kā starpniekserveris piekļuvei inficētiem resursiem tīmeklī. Identificētais apdraudējums tika novērsts.
- 23.08. Kādas skolas mājaslapa tika kompromitēta, un apmeklētāji tika pāradresēti uz reklāmvietnēm. CERT.LV brīdināja atbildīgās personas, lapa tika salabota, atjauninot tās satura vadības sistēmu.
- 24.08. Kādas valsts iestādes adresātiem tika mēģināts iesūtīt šifrējošā datorvīrusa Zepto lejupielādētāju. To pārtvērusi izmantotā antivīrusu programma.
- 25.08. Identificēts krāpšanas mēģinājums, kura realizācijā uzbrucēji ieguldījuši lielāku izdomu un sagatavošanos nekā parasti. Lai veiktu krāpnieciskas darbības, uzbrucēji

pierеģistrējuši viltus uzņēmuma domēna vārdu .lv zonā, kas ir līdzīgs Latvijā strādājoša uzņēmuma nosaukumam, kā arī mēnesi pirms uzbrukuma izveidojuši Wikipēdija ierakstus par viltus uzņēmuma identitāti, lai potenciāliem upuriem izskatītos ticamāki. Uzbrucēju darbības veids ir CEO krāpšana (CEO fraud), jeb šogad izplatītie sociālās inženierijas un elektroniskās sarakstes iejaukšanās/pārtveršanas uzbrukumi, ar mērķi partneru vārdā izkrāpt naudu. Lieki teikt, ka sarakstē norādītie kontu numuri nepieder patiesajiem partneriem, bet gan uzbrucējiem.

- 26.08. CERT.LV informēja Valsts policiju par identificētu LuminosityLink botnet kontrolcentra uzturēšanu Latvijā.
- 30.08. Vairāki uzņēmumi cietuši no šifrējošo datorvīrusu Zepto un Crysis darbības. Vīrusi aktivizēti, atverot Microsoft Office Macro komandas saturošus dokumentus, kas atsūtīti e-pastā.
- 31.08. CERT.LV nodeva uzbrukuma indikatorus Latvijas komercbankām, lai informētu par identificētajiem uzbrukumu mēģinājumiem.
- Augustā tika novērota agresīva Locky vīrusa izsūtīšanas kampaņa vairāku nedēļu garumā. Vīruss tika izsūtīts e-pasta ziņojumos, kas saturēja .docm paplašinājuma failus, kas ir Microsoft Word dokuments ar Macros aktīvā koda funkcionalitāti. Lai arī šī vīrusa aktivitāte vairs nepārsteidz, tā piegādes veidi ir cieši saistīti ar sociālās inženierijas elementiem un nereti tomēr panāk rezultātu neuzmanīgu lietotāju dēļ.
- 02.09. Konstatēta paroļu atjaunošanas rīka *LaZagne* izmantošana ļaunatūras izplatīšanas kampaņā. Rīks tika izplatīts ļaunprātīgos nolūkos e-pastos ar .jar pielikumiem. E-pasti noformēti angļu valodā ar banku maksājumu uzdevumiem saistītu tematiku.
- 05.09. Kāds Latvijas uzņēmums saņēma draudu vēstuli grupējuma *Armada Collective* vārdā. Tika draudēts veikt apjomīgu DDOS uzbrukumu, kas traucēs uzņēmuma darbību, ja uz e-pastā norādītu Bitcoin adresi netiks pārskaitīts 1 BTC. CERT.LV informēja uzņēmumu, ka šis ir krāpšanas mēģinājums, *Armada Collective* nekad neveic reālus uzbrukumus, bet izspiež naudu ar tukšiem draudiem. Līdzīgas draudu vēstules vairāki Latvijas uzņēmumi saņēmuši arī iepriekš.
- 05.09. IT drošības speciālists Nils Putniņš sadarbībā ar uzņēmumu *Influent Solutions* un *Digital Security Alliance* biedrību informēja CERT.LV par atklātu kritisku ievainojamību kādas pašvaldības tīmekļa vietnē. Izmantojot ievainojamību, bija iespējams nesankcionēti iegūt datu bāzes ierakstus un potenciāli pārņemt serveri uzbrucēja kontrolē. Ievainojamības atklāšanā ievēroti atbildīgas ievainojamību atklāšanas (RDP) pamatprincipi un apdraudējumu izdevās operatīvi novērst.
- 07.09. Kāda uzņēmuma serveris cieta no šifrējošā datorvīrusa Cryptolocker aktivitātes. Pārbaudot serveri, tika konstatēts, ka tas ir kompromitēts un uzbrucēji tajā izveidojuši papildu lietotāja kontu. CERT.LV konsultēja uzņēmumu par darbiem, kas veicami datortīkla drošības uzlabošanai. Šifrētie faili tika atgūti no rezerves kopijām.
- 09.09. CERT.LV kādas valsts iestādes tīkla segmentā konstatēja no publiskā interneta tīkla pieejamu maršrutētāja vadības paneli. Tajā bez autentifikācijas bija redzama uzstādītā konfigurācija, kas gan nebija izmaināma. Tāpat šis maršrutētājs bija

izmantojams kā DNS *open resolver*. Pēc CERT.LV brīdinājuma piekļuve šim panelim tika slēgta, kā arī tika salabota DNS servisa konfigurācija.

- 13.09. No kāda novada pašvaldības servera tika izsūtīti vairāki tūkstoši mēstuļu. Tas tika izdarīts, piemeklējot testa lietotāja paroli, kas bija vienkārša un īsa. Atklājot incidentu, parole tika nomainīta pret drošāku un serverī iesūtītās mēstules tika dzēstas. Iestādes e-pasta pakalpojumus šis gadījums nav ietekmējis.
- 14.09. IBM incidentu novēršanas vienība publicēja banku vīrusa Dridex analīzi, kurā kā vīrusa mērķis tika identificētas arī liela daļa Latvijā strādājošu komercbanku. CERT.LV informēja par apdraudējumu un izplatīja uzbrukuma indikatorus identificētajām komercbankām. CERT.LV veica arī padziļinātu vīrusa analīzi un nekonstatēja nevienu pilnvērtīgi realizētu šīs kampaņas uzbrukumu, kurā Latvijas banku klientiem būtu sagatavoti pārlūku pārtveršanas skripti. To varētu skaidrot kā iespējamu gatavošanos uzbrukumam, kas nav noticis, vai uzbrucēju pieļautu kļūdu, kas netieši norāda uz uzbrucēju saistību ar Latviju.
- 19.09. Tika konstatēts, ka kāds skolnieks labojis savas un klasesbiedru atzīmes e-klase.lv portālā, izmantojot skolotājas paroli. Parole iegūta no LinkedIn uzlaušanā iegūtiem datiem, kas ir brīvi pieejami internetā. Nodarījums nav radījis smagas sekas, bet atgādina par vajadzību izmantot dažādas paroles dažādiem resursiem.
- 19.09. CERT.LV identificēja apjomīga *double fastflux* botu tīkla kontroles posmu Latvijā. Inficēti bija vairāki desmiti tūkstošu iekārtu. CERT.LV veica incidenta analīzi un informēja ietekmēto valstu CERT kolēģus. Kibernoziedznieki šo metodi izmantoja savu pēdu slēpšanai un pārdeva to kā servisu.
- 21.09. Kādas valsts iestādes pārvaldībā esošais portāls tika izķēmots, izmantojot publiski zināmu CMS ievainojamību. Pēc brīdinājuma saņemšanas iestāde veica portāla satura vadības sistēmas labojumus, kā arī identificēja uzbrucēju izmantotās IP adreses un CMS kļūdas, kas ļāvušas lapu uzlauzt.
- 22.09. Kādā valsts iestādē vairāki darbinieki saņēma savu kolēģu vārdā nosūtītus e-pastus ar virsrakstu "Latvijas Stabilitātes programma 2016.-2019.gadam", kas izsūtīti no inbox.lv servera. To pielikums saturēja Microsoft Office formāta dokumentu ar Makro funkciju, kas lejupielādēja un izpildīja datorvīrusu. Inbox.lv portālā sūtītāju e-pasta adreses izveidotas tajā pašā dienā no Korejas IP adresēm. Datoru inficēšana iestādē netika konstatēta.
- Augustā un septembrī CERT.LV veica atkārtotu kādas valsts iestādes vietnes drošības testēšanu. Iestādei tika nosūtīti drošības testu rezultāti ar ieteikumiem uzlabojumu veikšanai, kurus iestāde tālāk nodeva vietnes izstrādātājiem.

CERT.LV pasākumi incidentu novēršanai:

- 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. Lai pilnvērtīgi sagatavotos jaunās mobilās ļaunatūras analīzei, CERT.LV turpina darbu pie laboratorijas izveidošanas.

Pārskata periodā tika saņemta ziņa par jaunatklātu Android ļaundabīgo programmatūru, kas zog finanšu informāciju (kredītkaršu numuri u.c.), un bloķē zvanus uz bankas zvanu centriem, tādējādi traucējot īpašniekam laikus bloķēt maksājumu karti. Nākotnē paredzams, ka ar šādas ļaunatūras palīdzību būs iespējama arī zvanu pāradresēšana uz viltotu zvanu centru, kas radītu papildu riskus. Līdz šim par šīs ļaunatūras upuriem Latvijas iedzīvotāji nav kļuvuši, bet jāatceras, ka mobilās iekārtas savas popularitātes dēļ ir kļuvušas par iekārojamu mērķi ļaundariem, tādēļ vieglprātīga rīcība ar savu viedierīci un izmantojamo programmatūru nav pieļaujama.

Jūnija sākumā pasaulē globālu popularitāti iekaroja Nintendo mobilā lietotne Pokemon GO, taču Latvijā oficiālā lietotnes versija vēl nebija pieejama. Tas neatturēja daudzus lietotājus no Pokemon GO lejupielādes no neleģitīmām vietnēm, neskatoties uz brīdinājumiem par atklātām ļaundabīgām lietotnes versijām, kas saturēja kaitīgas komponentes un nepamatoti pieprasīja piekļuvi plašam mobilās ierīces funkciju klāstam. Iespējams, pateicoties salīdzinoši drīzai oficiālās versijas pieejamībai, ziņojumi par incidentiem, kas saistīti ar Pokemon GO lietotni, saņemti netika.

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

Informācija par CERT.LV sadarbību ar medijiem

1) Intervijas un ziņas radio:

- 29.07. komentārs LR1 raidījumam "Labrīt stāsti" par izspiedējvīrusiem
- 29.09. komentārs LR1 raidījumam "Pēcpusdiena" par VID likumā paredzētajām izmaiņām interneta vietņu bloķēšanai

2) Sižeti televīzijā, tiešraides:

- 03.08. intervija LNT raidījumam "900 sekundes" par "CEO krāpšanu", izspiedējvīrusiem un parolēm
- 16.08. intervija RIGATV 24 raidījumam "Pilsētas Pulss" par datu aizsardzību telefonos, kuros tiek izmantotas aplikācijas, piemēram, spēle Pokemon Go
- 24.08. komentārs LTV par banku bezkontakta kartēm un to drošību
- 29.08. komentārs MixTV raidījumam "Разворот" par darknet

3) Informācija par CERT.LV tīmekļa vietnēm:

Pārskata perioda sākumā tika veikta pāreja uz CERT.LV jauno mājas lapu. Mainījās gan mājas lapas dizains, gan informācijas izvietojums.

Pārskata periodā vietnē https://www.cert.lv publicētas 28 ziņas. Populārākā bija ziņa ar uzaicinājumu pieteikties IT drošības konferencei "Kiberšahs 2016", kurai ir 2,558 unikāli skatījumi. Otra populārākā bija sadaļa par vīrusiem, kuru skatījuši 921 unikāls apmeklētājs. Trešā populārākā bija Kontaktu sadaļa ar 885 unikāliem skatījumiem. Kopā CERT.LV mājaslapai bijuši 11,990 lapu skatījumi, kurus veido 7,033 unikāli lapu skatījumi.

CERT.LV uzturētajam portālam https://www.esidross.lv pārskata periodā bija 11,210 apmeklējumi, no tiem 9,189 unikāli apmeklējumi.

CERT.LV turpina tulkot un portālā esidross.lv publicēt OUCH! ikmēneša izdevumus (Informācijas drošības biļetens, ko sagatavo SANS institūts). Pārskata periodā publicēti 3 jauni OUCH! numuri.

Portālā esidross.lv publicētie raksti:

- Kas ir "CEO krāpšana"?
- Šifrējošie vīrusi
- Ko darīt un ko nedarīt e-pastā
- Interneta likumi
- Sevis un savas ģimenes pasargāšana
- Personīgās informācijas ievietošana internetā. Privātums
- Darbības ar mantu, iepirkšanās internetveikalos
- Sociālo mediju profilu uzstādījumi, paroles

- Saziņa ar svešiniekiem sociālajos tīklos
- Emocionāla pazemošana virtuālajās platformās
- Bērni nekautrējas jautāt par emocionālo drošību un privātumu internetā
- Lekciju kursa "Kibernoziedznieku vēsture" video (1. daļa)
- Lekciju kursa "Kibernoziedznieku vēsture" video (2. daļa)

CERT.LV sociālo tīklu konti:

- Twitter konta https://twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 1577.
- CERT.LV Facebook profila http://www.facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 416.
- CERT.LV draugiem.lv profila http://www.draugiem.lv/certlv sekotāju skaits pārskata perioda beigās bija 69.
- Sociālajā tīklā Google+ https://www.google.com/+CertLv ir 27 sekotāji.

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

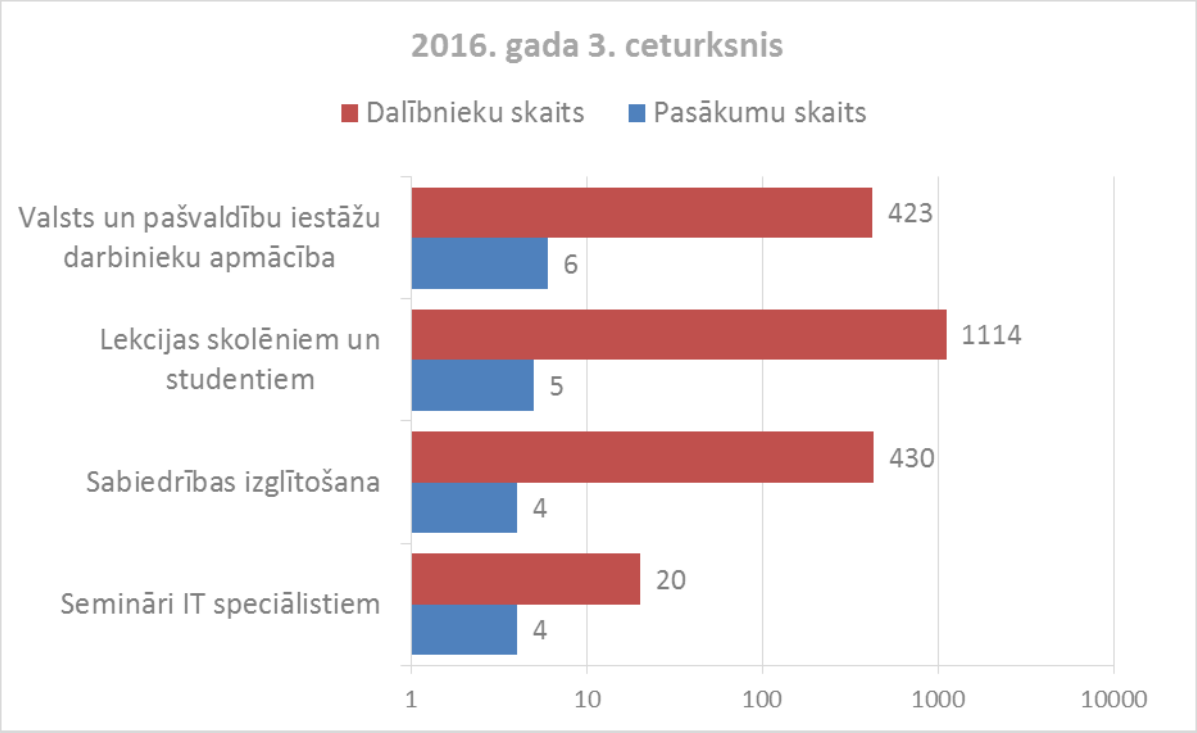
5. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā.

16. augustā un 21. septembrī CERT.LV pārstāvji tikās ar Digitālās drošības aliansi (DDA), lai sagatavotos kampaņai "Mirklis pirms klik", kas sāksies oktobrī un tiks vērsta uz uzņēmējiem un darbinieku izglītošanu par digitālās drošības jautājumiem.

30. augustā notika tikšanās ar bankas Citadele pārstāvjiem par bankas plānoto mobilo iekārtu drošības kampaņu.

07.septembrī CERT.LV uzsāka lekciju kursu IT drošības speciālistiem "Kibernoziedznieku vēsture". Lekcijas tika ierakstītas un videomateriāls būs pieejams tīmekļa vietnē esidross.lv.

Pārskata periodā CERT.LV par IT drošību izglītoja 1987 cilvēkus, iesaistoties 19 izglītojošos pasākumos.



8.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2016. gada 3. ceturksnī.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 06.07. Tikšanās ar Rīgas domes pārstāvjiem par MK Noteikumu 442.ieviešanu
- 14.07. DEG sanāksme
- 16.08. Tikšanās ar CVK par pašvaldību vēlēšanu sistēmu
- 08.09. DEG sanāksme
- 28.09. Tikšanās ar Nacionālā veselības dienesta pārstāvjiem par e-veselības projektu

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. 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.

Uz pārskata perioda beigām informācija ir saņemta no 64 ESK. 59 ESK ir iesnieguši rīcības plānu, bet 5 ESK rakstiski apliecinājuši, ka neuztur publisko elektronisko sakaru tīklu, no tiem 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).

Attiecībā uz ITDL 6^1 panta izpildi, pārskata periodā nav saņemts neviens ziņojums.

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

Pārskata periodā notika intensīvas pārrunas ar iespējamajiem IT drošības mācību "Cyber Europe 2016" dalībniekiem. Mācības notiek 13.-14. oktobrī, un Latvijas pusē tās koordinēs CERT.LV.

19.-22. septembrī TF-CSIRT sanāksmē Cīrihē CERT.LV vadītāja Baiba Kaškina atkārtoti tika ievēlēta par TF-CSIRT grupas priekšsēdētāju. Šajā sanāksmē tika arī oficiāli paziņots par CERT.LV sertifikāciju Trusted Introducer servisā un izsniegts apliecinājums. CERT.LV sertificēts no 2016. gada 1. septembra uz trīs gadiem.

Pārskata periodā tika parakstīti sadarbības līgumi ar starptautiskiem IT drošības veicināšanas projektiem CyberGreen un STOP.THINK.CONNECT.

CERT.LV pārstāvji pārskata periodā piedalījušies šādos starptautiskos pasākumos:

- 04.-15.07. Tikšanās ar potenciālajiem dalībniekiem par dalību IT drošības mācībās "Cyber Europe 2016"
- 07.07. Tikšanās ar NBS pārstāvjiem, lai apspriestu Latvijas komandas dalību NATO mācībās Cyber Coalition
- 18.07. videokonference ar *Cybergreen* pārstāvjiem par iespējamo dalību projektā
- 16.08. parakstīts sadarbības līgums ar projektu *CyberGreen*
- 01.09. CERT.LV sertificēts Trusted Introducer servisā
- 01.-02.09. dalība starptautiskā projekta STOP.THINK.CONNECT. sanāksmē Bernē, Šveicē, kur tika parakstīts sadarbības līgums
- 12.-14.09. CERT.LV pārstāvis piedalās "The Networking Conference" (agrāk TERENA konference) programkomitejas sanāksmē Amsterdamā
- 12.-16.09. CERT.LV pārstāvis piedalās "IT Systems Attack and Defence Course (ITSADC)" Tallinā, Igaunijā
- 13.09. CERT.LV pārstāvis piedalījās "European cyber security challenge" sanāksmē
- 14.-15.09. CERT.LV piedalījās mācību "Cyber Europe 2016" simulācijā (*dry run*)
- 19.09. CERT.LV pārstāvji tikās ar SWITCH CERT pārstāvjiem (Šveices nacionālā CSIRT vienība), tika apspriestas sadarbības iespējas
- 19.-22.09. Septembra TF-CSIRT sanāksme Cīrihē, Šveicē
- 29.09. Maķedonijas pārstāvju vizīte Aizsardzības ministrijā, CERT.LV iepazīstina viesus ar savu darbību

Sadarbība konkrētu incidentu risināšanā aprakstīta pārskata 2.punktā.

9. 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 ir uzsācis noteikto funkciju veikšanu.

Iepriekšminēto funkciju izpildei veikto darbu uzskaitījums:

- CERT.LV pārstāvis piedalījās elektroniskās identifikācijas uzraudzības komiteju gadskārtējā CA day seminārā Berlīnē, kas tika veltīts uzticamības pakalpojumu sertifikācijas un autentifikācijas jautājumiem;
- CERT.LV pārstāvis piedalījās ENISA izveidotās darba grupas, kas saistīta ar IKT produktu sertifikācijas vadlīniju izstrādes jautājumiem ES līmenī, virtuālajās sanāksmēs, kā arī, pēc saskaņošanas ar Aizsardzības ministrijas kolēģiem, sniedza Latvijas redzējumu par minētajiem jautājumiem;
- Elektroniskās uzraudzības komitejas pārstāvji no CERT.LV piedalījās sanāksmēs ar VRAA, VARAM, LVRTC pārstāvjiem, lai iegūtu informāciju par Latvijas eID shēmu, tās nodrošināšanā iesaistītajām pusēm, to atbildības sadalījumu, kā arī pielietotajiem tehniskajiem risinājumiem;
- CERT.LV kopīgi ar Aizsardzības ministrijas kolēģiem veica Eiropas Komisijas īstenošanas lēmuma 2015/1984, kas reglamentē eID shēmu paziņošanas mehānismu ES, izpēti, lai uzsāktu sagatavošanos nacionālās eID shēmas paziņošanai ES līmenī.
- Veikta eID shēmas sākotnējai novērtēšanai nepieciešamo standartu pasūtīšana, kā arī tika veikta informācijas analīze (standartu un EK normatīvo aktu, kas definē tehniskās un organizatoriskās prasības, līmenī), lai apkopotu informāciju, kas nepieciešama Fizisko personu elektroniskās identifikācijas likumā noteikto MK noteikumu izstrādei.

10. 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 01.07.2016. līdz 30.09.2016. ir saņēmusi un izvērtējusi 86 ziņojumus. No tiem 35 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 10 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 13 ziņojumos konstatēta personas goda un cieņas aizskaršana. Par finanšu krāpšanas mēģinājumiem internetā saņemti 5 ziņojumi, 6 ziņojuma saturs nav bijis pretlikumīgs, 17 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 19 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 15 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.

2016. gada 7. novembrī
Sagatavotājs – Līga Besere
Tālrunis: 67085888
E-pasts: liga.besere@cert.lv