Latvijas Universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

Līdzfinansē Eiropas Savienības Eiropas
infrastruktūras savienošanas instruments

Publiskais pārskats par CERT.LV uzdevumu izpildi

2019

2019. gada 4. ceturksnis (01.10.2019. – 31.12.2019.)

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

2019. gada 4. ceturksnī tika reģistrētas 201 142 unikālas apdraudētas IP adreses, kas ir par nepilnu 1% mazāk nekā iepriekšējā ceturksnī un par nepilniem 2% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (110 816 unikālas IP adreses) ar kritumu 6% pret iepriekšējo periodu;
- otrs izplatītākais bija ļaundabīgs kods (16 615 unikāla IP adrese) a kāpumu 4%;
- bet trešais - ielaušanās mēģinājumi (2354 unikālas IP adreses) ar kāpumu 28%.

Kāpums ielaušanās mēģinājumu apjomā skaidrojams ar viena no starptautiskajiem informācijas avotiem piegādātu pastiprinātu informācijas plūsmu par ielaušanās mēģinājumiem, kas nav apstiprinājušies. Nelielu pieauguma daļu veidoja arī aktīvi uzbrukumu mēģinājumi divu valsts iestāžu resursiem.

CERT.LV sabiedrības informēšanas aktivitāšu rezultātā lēnām turpina kristies potenciāli apdraudēto iekārtu skaits, kurās attālinātās piekļuves serviss (*Remote Desktop* jeb *RDP*) ir eksponēts internetā. *RDP* izmantošana bez pienācīgiem aizsardzības pasākumiem – drošas paroles, piekļuves ierobežošanas no noteiktām IP adresēm vai caur *VPN* - pakļauj lietotāju palielinātam uzbrukuma riskam. CERT.LV ikdienā apstrādā incidentus par uzlauztiem un nošifrētiem serveriem un darbstacijām, kurām uzbrucējs piekļuvis, uzminot pārāk vienkāršo lietotāja paroli, vai iegūstot to no publiski nopludinātām datu bāzēm.

Turpinājās krāpniecisku “finanšu speciālistu” zvani. Vienā no gadījumiem zaudējumu apjoms sasniedza 80 000 eiro. Viltus “finanšu speciālisti” mudināja veikt ieguldījumus nelicenzētās MarketCFD un CoinYards platformās, sākotnēji radot iespaidu, ka tiek gūta peļņa, bet vēlāk solot iespēju atgūt pirmajā reizē “ieguldīto”. Lai sevi pasargātu no krāpnieciskiem darījumiem, CERT.LV un Valsts policija aicināja pieņemt apdomīgus lēmumus, rīkojoties ar saviem finanšu līdzekļiem, un pirms ieguldījumu veikšanas pārbaudīt FKTK tīmekļa vietnē, vai minētais uzņēmums ir tiesīgs darboties Latvijā, kāds ir tā darbības veids un saņemtās licences.

Tika saņemti daudzi ziņojumi par krāpniecisku e-pastu kampaņu krievu valodā, kuros tika apgalvots, ka uzlauzts lietotāja e-pasts, nokopēts datora cietais disks un nofilmēts, kā lietotājs apmeklē pieaugušajiem domātas saites. Šāda satura e-pasti masveidā Latvijas kibertelpā izplatīti arī iepriekš, bet angļu valodā, un, iespējams, daļa lietotāju saturu iepriekš nav sapratuši un e-pastus ir ignorējuši, bet, saņemot draudus krievu valodā, ir ziņojuši CERT.LV.

Decembrī CERT.LV veica vairāku incidentu analīzi, kuru detaļas liecināja, ka vairāki valsts iestāžu darbinieki un politiķi ir piedzīvojuši mērķētu kiberuzbrukumu. Uzbrukums tika veikts, izsūtot ļaundabīgus e-pastus Krievijas vēstniecības vārdā, kas tika noformēti kā atbilde uz iepriekšēju saraksti. E-pastos tika iekļauta saite dokumenta lejupielādei, kurš bija paredzēts upuru datora inficēšana.

Pārskata periodā CERT.LV par IT drošību izglītoja 3324 cilvēkus, iesaistoties 39 izglītojošos pasākumos.

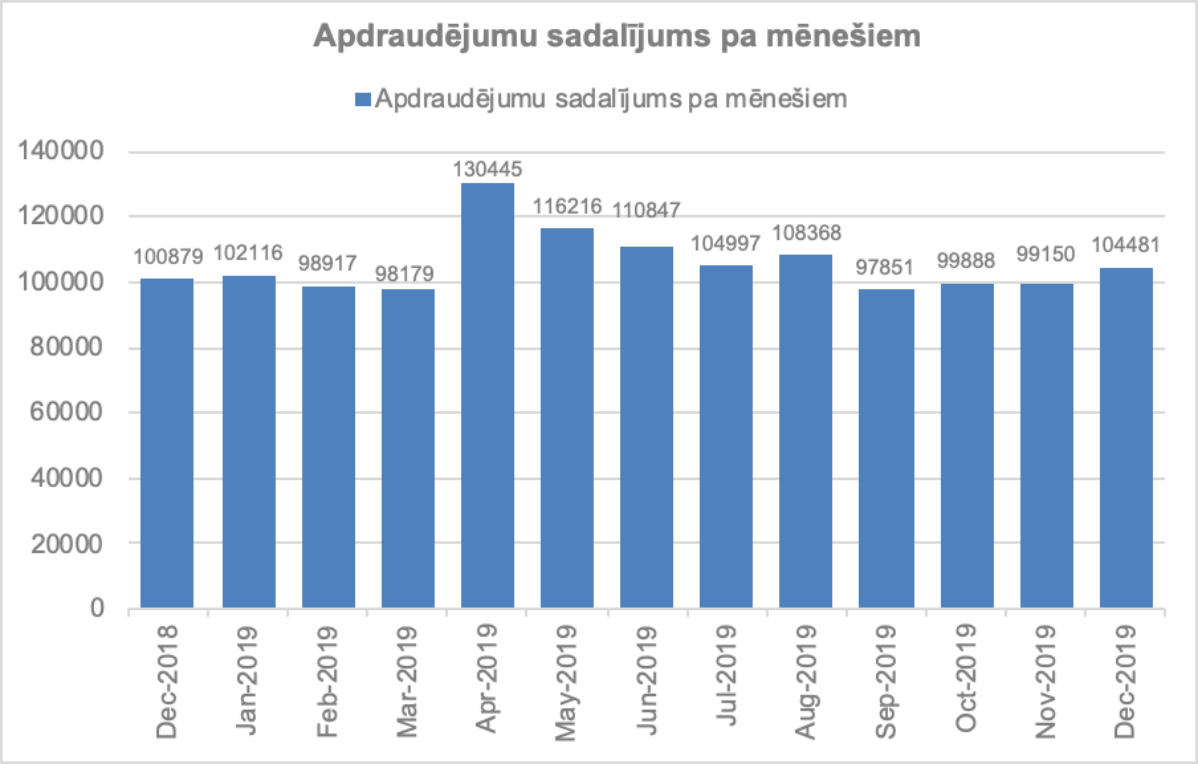
2.-3. oktobrī CERT.LV un ISACA Latvijas nodaļa sadarbībā ar LMT un dots. rīkoja starptautisku kiberdrošības jautājumiem veltītu konferenci "Kiberšahs 2019". Šogad konference norisinājās nevis vienu, bet divas dienas, un pirmās dienas sākumā dalībniekiem bija iespēja apmeklēt praktiskos seminārus-darbnīcas, kurus vadīja pasaules līmeņa kiberdrošības eksperti. Konferenci atklāja Latvijas Valsts prezidents Egils Levits, un konferences ietvaros tika aplūkotas tādas tēmas kā sociālā inženierija un kiberoperācijas - no politiskā, tehniskā un drošības aspekta, kā arī tika apspriestas jaunākās kiberdrošības tendences un tehnoloģijas. Šogad konferencē piedalījās pārstāvji no vairāk kā 30 valstīm. Pirmo reizi konferences vēsturē CERT.LV rīkoja arī „Capture the Flag (Jeopardy-style)" sacensības.

Notika aktīva gatavošanās NATO CCDCoE un CERT.LV kopīgi organizētajām tehniskajām kiberdrošības mācībām "Crossed Swords 2020", organizējot plānošanas vizītes, izstrādājot mācību vidi un tiekoties ar mācību dalībniekiem. 9.-13. decembrī Rīgā notika izmēģinājuma pasākums "Crossed Swords", kurā tika pilnveidota mācību vide un uzdevumi, lai nodrošinātu sekmīgu mācību norisi 2020.gada janvārī.

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 apdraudējumu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija, kas tagad nosaukta par „Reference Security Incident Taxonomy"). Taksonomija ir formalizēts veids kā CERT.LV apkopo, sadala kategorijās un reprezentē par incidentiem iegūto tehnisko informāciju. Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīti vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa infekciju (piemēram, *Confiker*, *Zeus*, *Mirai*) un ievainojamību (piemēram, *Opendns*, *Openrdp*) tipiem.

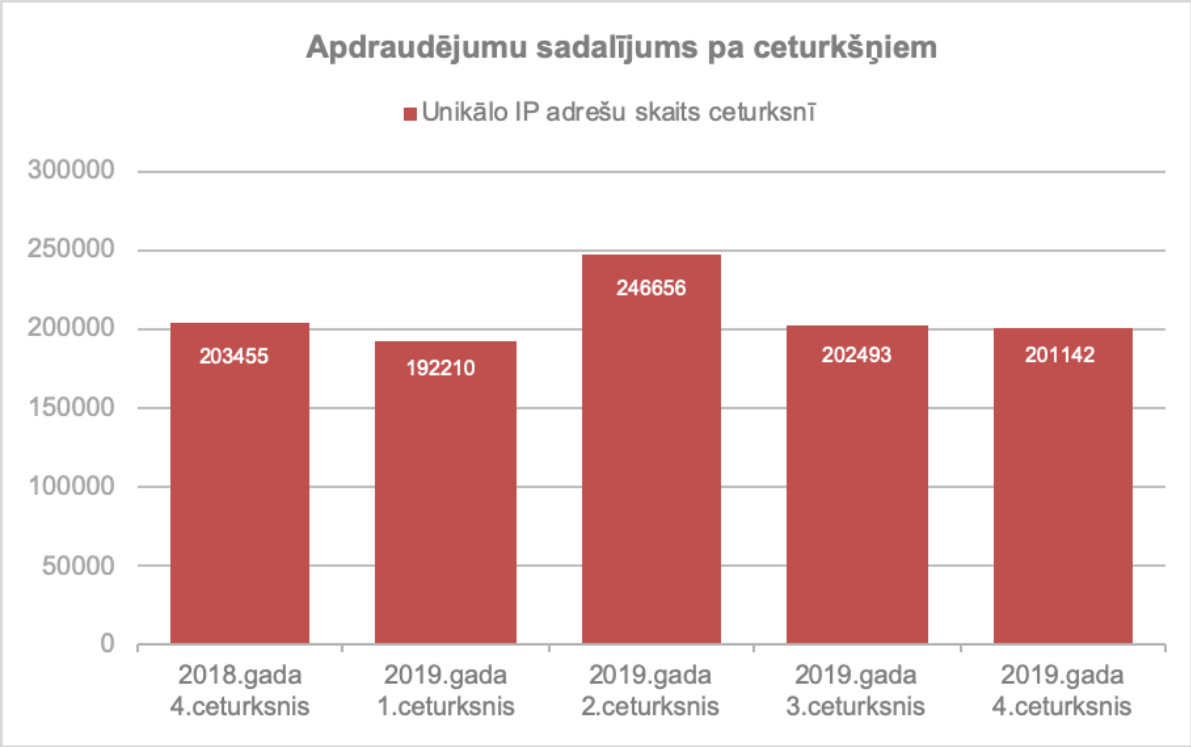
CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par 100 000 – 105 000 ievainojamu unikālu IP adrešu.



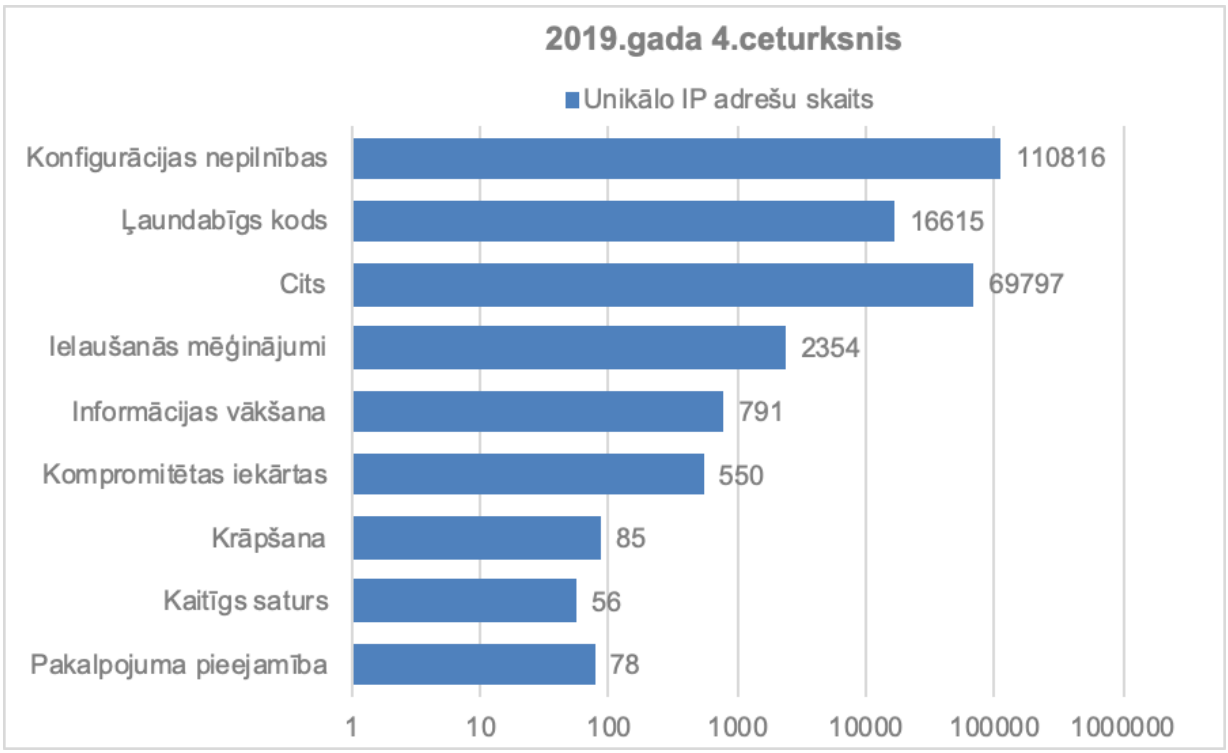
1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 12 mēnešu griezumā.

2019. gada 4. ceturksnī tika reģistrētas 201 142 unikālas apdraudētas IP adreses, kas ir par nepilnu 1% mazāk nekā iepriekšējā ceturksnī un par nepilniem 2% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā nav vērojamas būtiskas izmaiņas mēnesī reģistrēto apdraudēto IP adrešu daudzumā.



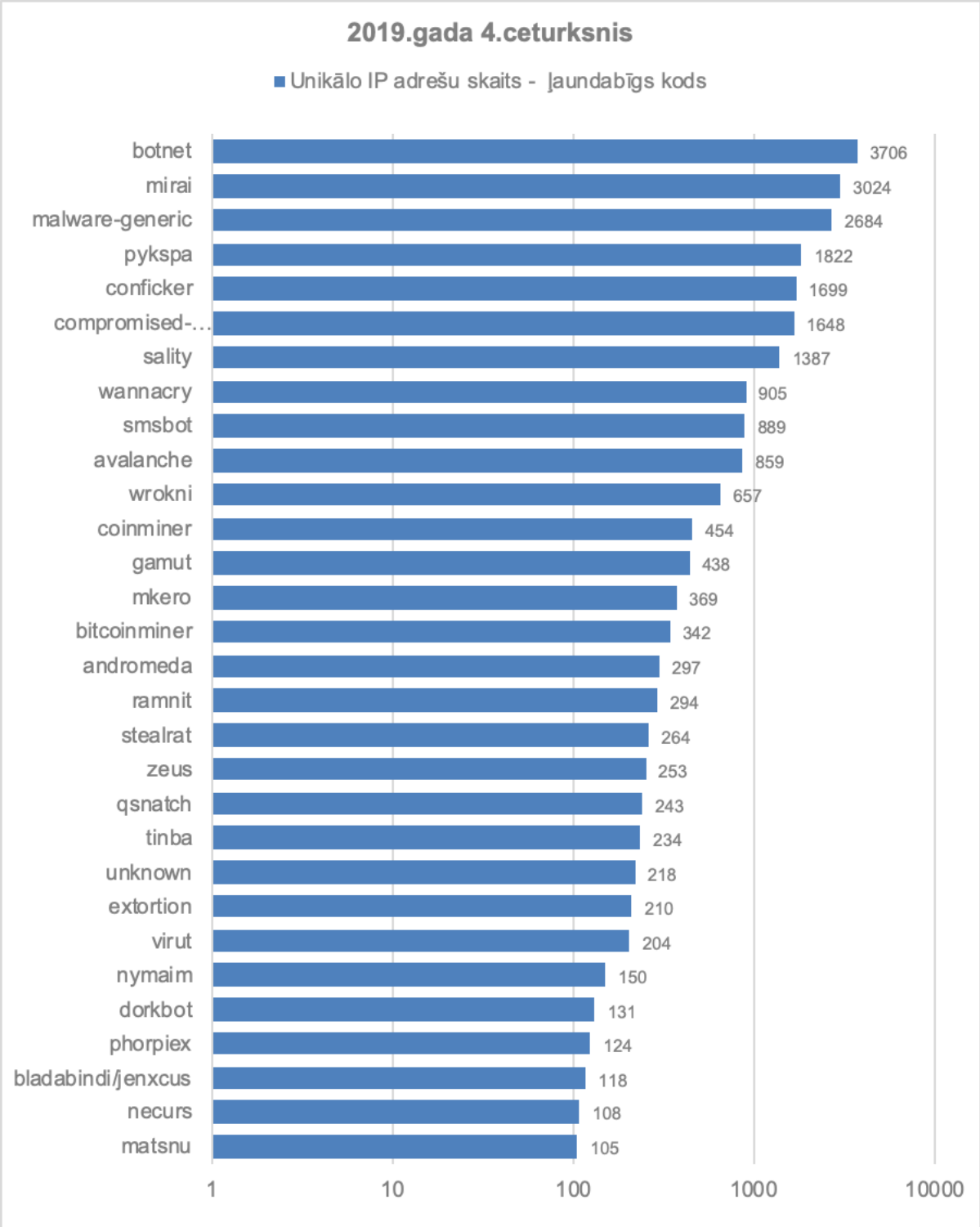
2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2018. un 2019. gadā.



3.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 4. ceturksnī pa apdraudējumu veidiem.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (110 816 unikālas IP adreses) ar kritumu 6% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (16 615 unikāla IP adrese) a kāpumu 4%, bet trešais - ielaušanās mēģinājumi (2354 unikālas IP adreses) ar kāpumu 28%.

Kāpums ielaušanās mēģinājumu apjomā skaidrojams ar viena no starptautiskajiem informācijas avotiem piegādātu pastiprinātu informācijas plūsmu par ielaušanās mēģinājumiem, kas nav apstiprinājušies. Nelielu pieauguma daļu veidoja arī aktīvi uzbrukumu mēģinājumi divu valsts iestāžu resursiem.

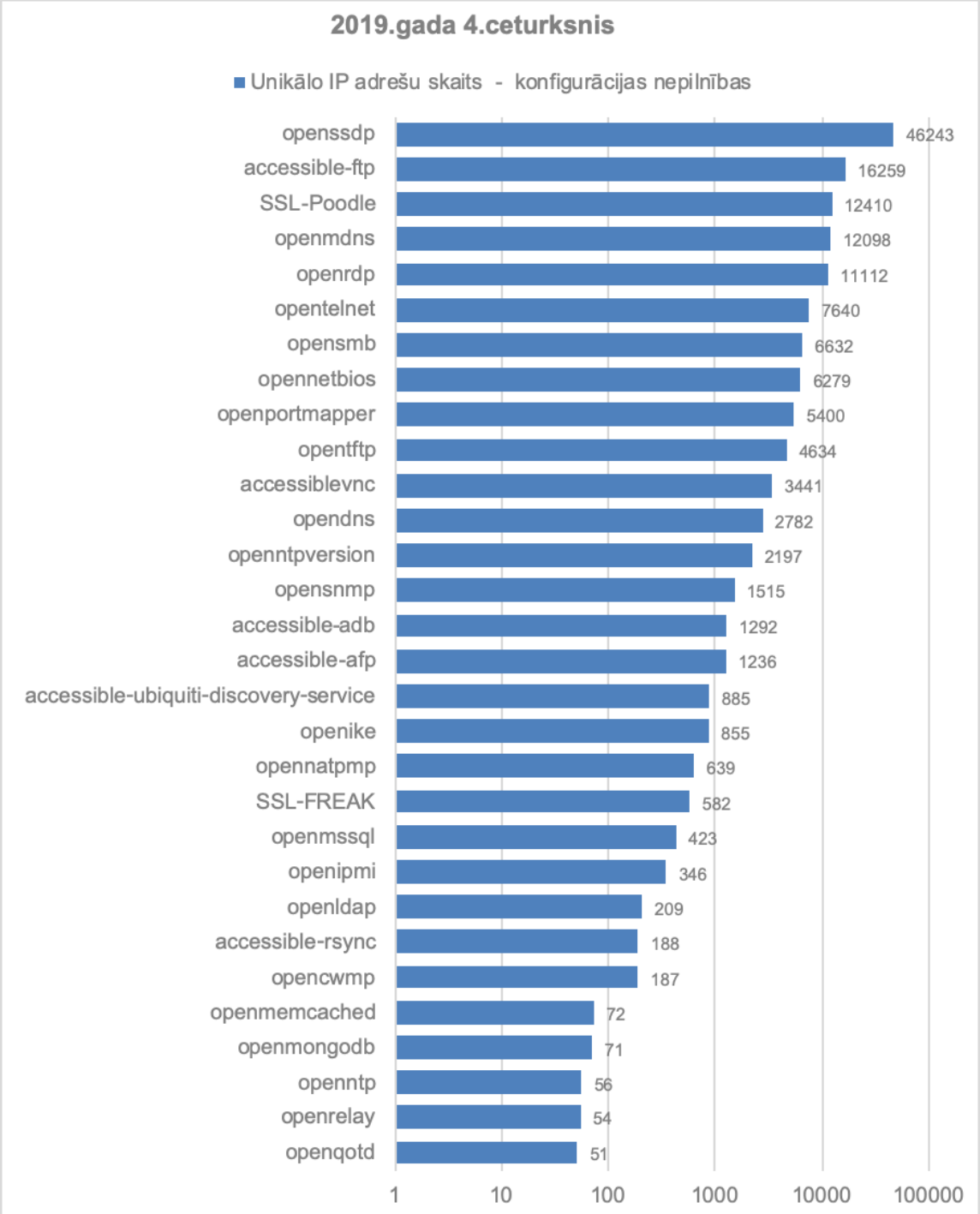


4.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 4. ceturksnī ar apdraudējuma veidu - Ļaundabīgs kods.

Pirmo vietu ļaunatūras izplatības topā ieņem *Mirai* – ļaunatūra, kas inficē un iekļauj robotu tīklos jeb *botnetos* lietu interneta (IoT) iekārtas, lai izmantotu tās tālākiem uzbrukumiem un citām pretlikumīgām darbībām. Par uzbrucēju upuriem parasti kļūst iekārtas, kuras pēc iegādes pieslēgtas internetam, nenomainot ražotāja uzstādītos iestatījumus – noklusēto lietotājvārdu un paroli. Lai pasargātu sevi no lieka riska un līdzcilvēkus no papildu apdraudējuma, pirms jebkuras jaunas iekārtas pieslēgšanas internetam rūpīgi jāizvērtē, vai konkrētajai iekārtai šis pieslēgums tiešām ir nepieciešams? Ja tomēr ir, tad jāparūpējas par iekārtas drošību, vismaz nomainot noklusēto paroli.

Otro vietu topā ieņem ļaunatūra *Pykspa.* Tas ir datortārps, kas izplatās Skype vidē, nosūtot citiem lietotājiem ziņas ar saiti lejupielādei. Lejupielādēta iekārtā, ļaunatūra zog personīga rakstura informāciju (piemēram, lietotājvārdus un paroles) un nosūta to uz attālinātu komand- un kontrolcentru.

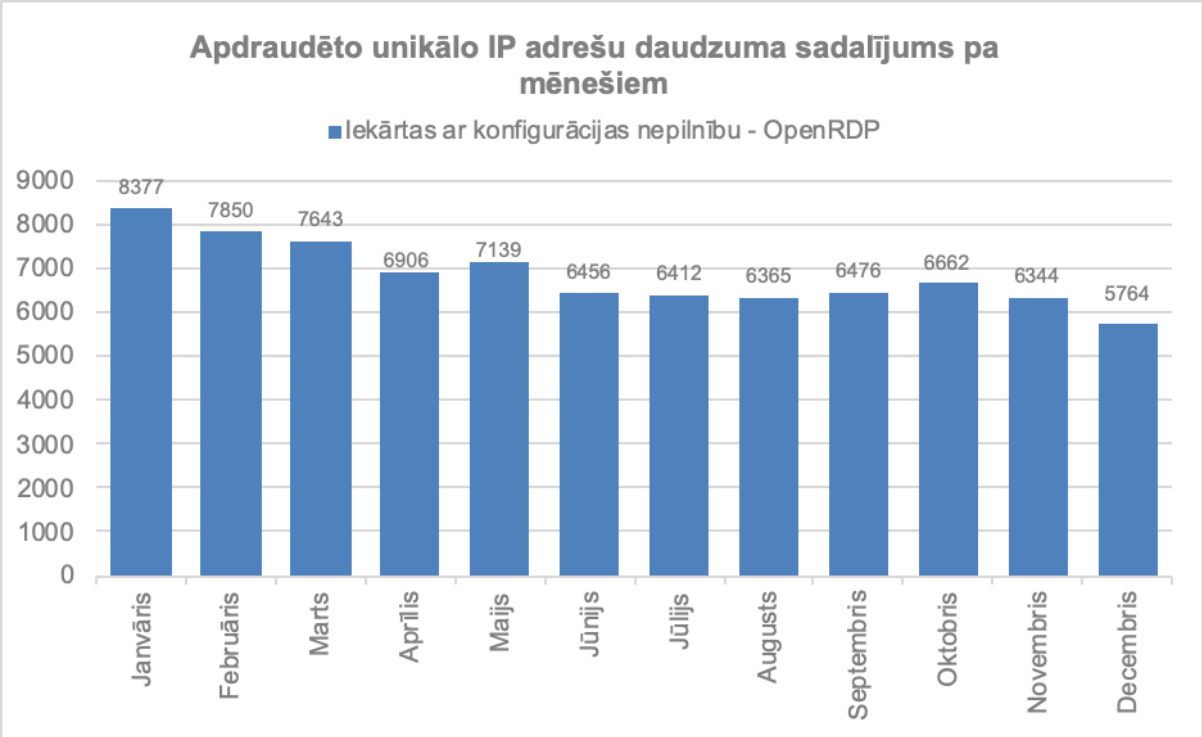
Topa trešajā vietā atrodas *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoši vienkārši „ārstējama" ļaunatūra. Šī indikācija vērojama tieši privātā sektorā un mājsaimniecībās, par ko CERT.LV regulāri informē elektronisko sakaru komersantus.



5.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gada 4. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Pirmo vietu konfigurācijas nepilnību topā ieņem *OpenSSDP* – iekārtas ar nedrošu konfigurāciju, kas var tikt izmantotas apjomīgos piekļuves atteices (*DoS*) uzbrukumos. *Simple Service Discovery Protocol* (*SSDP*) ir iebūvēts daudzās tīkla iekārtās, lai tās veiklāk varētu „atrast" viena otru un savstarpēji sazināties.

Konfigurācijas nepilnība *OpenRDP* pārskata periodā joprojām atrodas topa augšgalā. Tā bieži saistīta ar iekārtu un datu nesēju nošifrēšanu. Ja netiek ievērota labā prakse un netiek ierobežota piekļuve *RDP* servisam, piemēram, limitējot IP adreses, kurām atļauts pieslēgties, vai nosakot piekļuvi caur *VPN*, uzbrucējs var pārņemt kontroli pār neatbilstoši konfigurētām iekārtām, kurās attālinātās piekļuves porti ir brīvi atvērti uz internetu un nav pietiekami droša vai vispār nav uzstādīta piekļuves parole. Šādu gadījumu mazināšanai CERT.LV veica neatbilstoši konfigurēto iekārtu īpašnieku apziņošanu. Rezultātā potenciāli apdraudēto iekārtu apjoms ar atvērtu *Remote Desktop* servisu, lai arī lēnām, bet samazinājās (5.1. att.).



5.1.attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gadā ar konfigurācijas nepilnību *OpenRDP*.

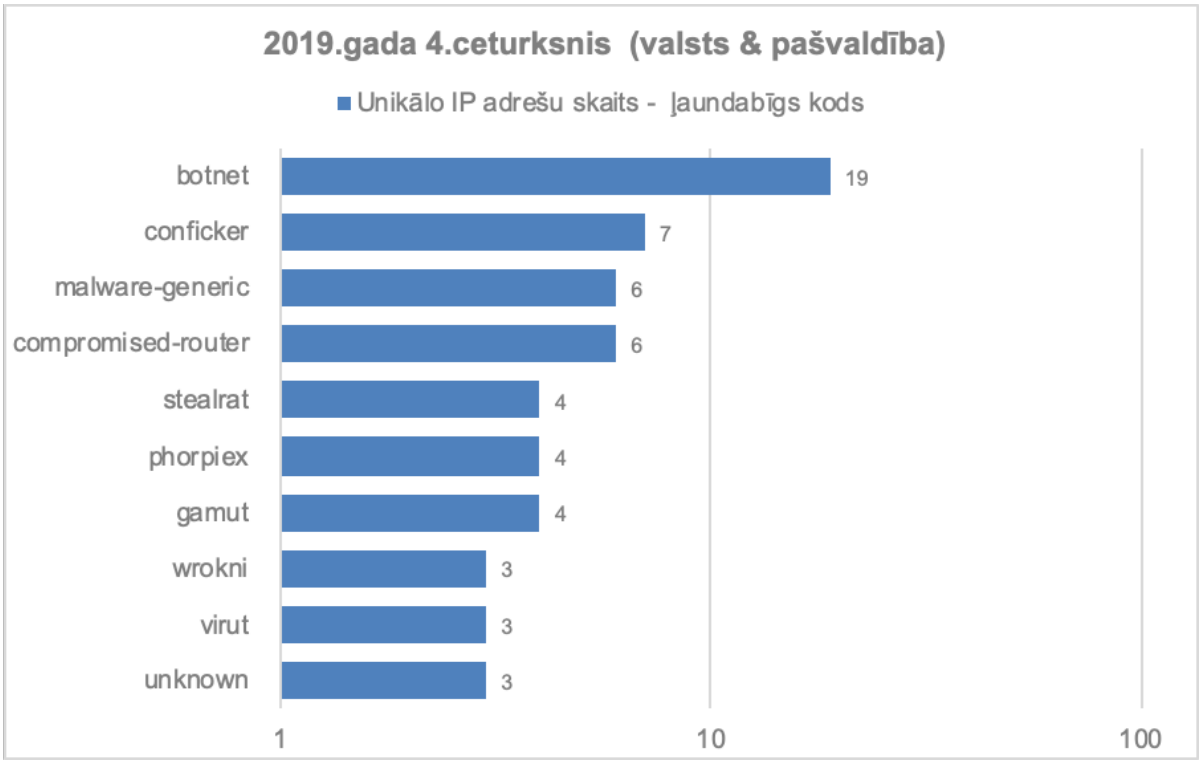
Lai samazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas (LIA) Net-Safe Latvija Drošāka interneta centru ir izveidojuši saprašanās memorandu, kas tiek slēgts ar interneta pakalpojumu sniedzējiem (IPS), kas vēlas pievienoties iniciatīvai „Atbildīgs interneta pakalpojumu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

Lai aktualizētu sadarbību ar interneta pakalpojumu sniedzējiem un iniciatīvu "Atbildīgs interneta pakalpojumu sniedzējs", 31.oktobrī CERT.LV un LIA rīkoja semināru IPS pārstāvjiem, kurā informēja par sadarbības iespējām. Pārskata periodā tika aktualizēts arī sadarbības memorands.

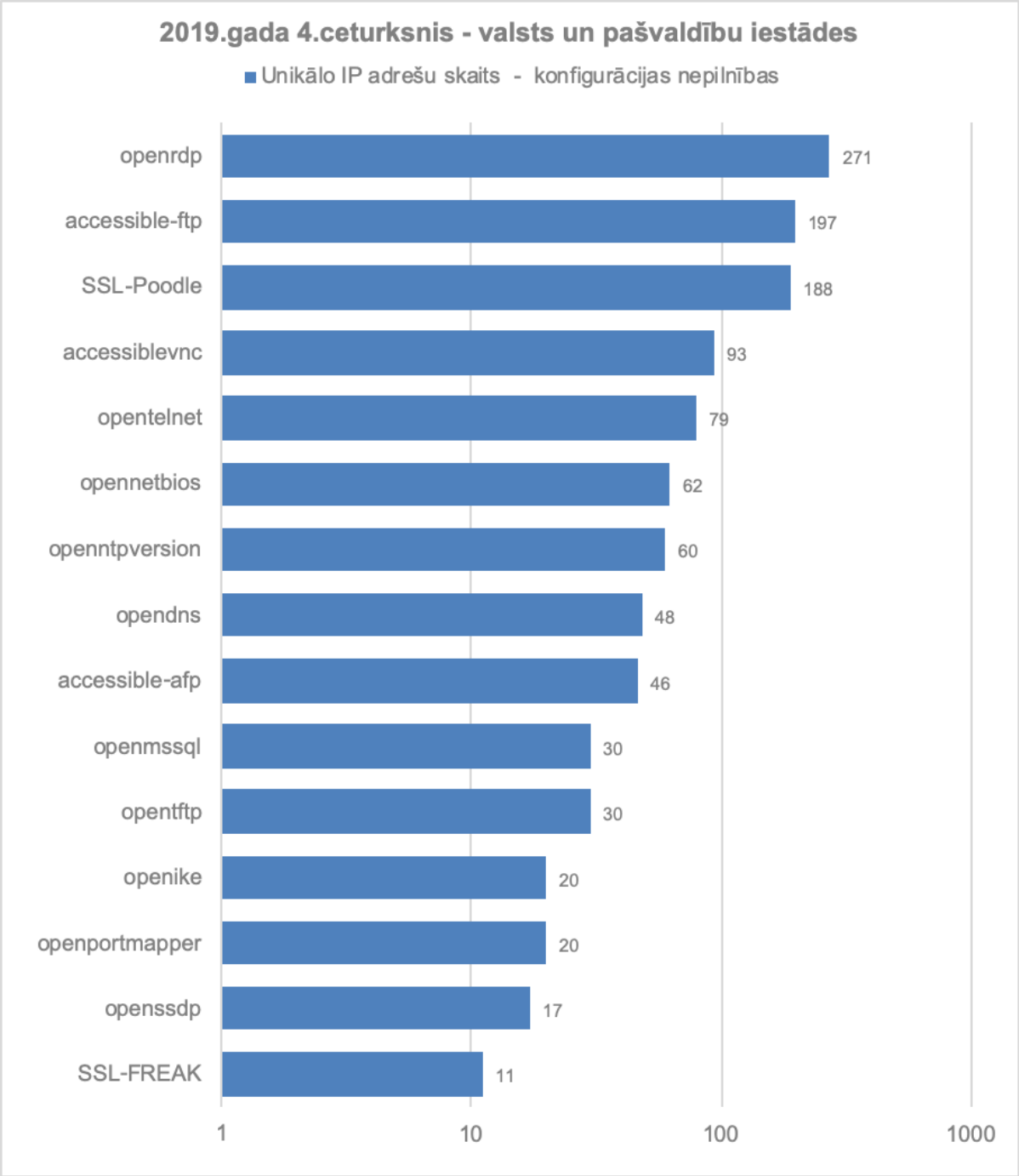
2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā.

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.

Vidējais apdraudēto valsts un pašvaldību iestāžu IP adrešu daudzums katras dienas saņemtajos ziņojumos pārskata periodā bija 550 unikālas IP adreses dienā. Galvenokārt tās ir iekārtas, kuru konfigurācijā vērojamas nepilnības vai iekārtu konfigurācija neatbilst labajai praksei, pakļaujot tās uzbrukuma riskam un padarot par apdraudējumu vai nu pašam iekārtas lietotājam, piemēram, zaudējot datus, vai sabiedrībai kopumā, piemēram, iekārta var tikt izmantota uzbrukumā citām iekārtām.



6.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2019.gada 4.ceturksnī ar apdraudējuma veidu – Ļaundabīgs kods.



7.attēls - CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits valsts un pašvaldību iestādēs 2019.gada 4. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

CERT.LV uzskaita arī kompromitēto un izķēmoto tīmekļa vietņu gadījumus. Pārskata periodā tika fiksētas 37 kompromitētas un izķēmotas tīmekļa vietnes. 31 gadījumā izķēmotās vietnes uzturēšanai tika izmantota Linux operētājsistēma, bet 2 gadījumos - Windows. Trīs no izķēmotajām vietnēm pēdējā gada laikā tikušas izķēmotas atkārtoti.

CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā. Visos tālāk aplūkotajos incidentos uzbrukumu mēģinājumi bijuši nesekmīgi un zaudējumi nav radīti, ja vien nav norādīts citādi

Krāpšana

Krāpnieciskā vietnē, kas tika uzdota par Delfi.lv portāla daļu, tika izplatītas viltus ziņas. Ziņās tika popularizētas investīcijas kriptovalūtā, maldinoši atsaucoties uz vairākām Latvijā pazīstamām personām. Viltus ziņas tika reklamētas arī sociālajā tīklā Facebook. Līdzīgas krāpniecības kampaņas tika īstenota ne tikai Latvijas, bet arī starptautiskā mērogā, un par tās upuriem kļuvuši gan vairāki pasaulē pazīstami ziņu portāli, gan arī ietekmīgi politiķi, aktieri un investori, kuru vārdi iesaistīti viltus reklāmās.

Izveidojot Latvijas Nacionālās operas un baleta (LNOB) mājaslapas viltus kopiju, krāpnieki izplatīja neīstas pasākumu biļetes, dažkārt pat par divkāršu cenu. Krāpnieciskā vietne Google meklētājā tika piedāvāta kā pirmā izvēle, jo krāpnieki šo iespēju bija iegādājušies kā reklāmas pakalpojumu krievvalodīgajai auditorijai, nodrošinot krāpnieciskajai vietnei labāku vietu meklēšanas rezultātos nekā oriģinālajai vietnei. Krāpnieciskā kampaņa tika vērsta pārsvarā uz ārzemju tūristiem, kas vēlējās iegādāties biļetes uz LNOB pasākumiem.

Turpinājās krāpniecisku "finanšu speciālistu" zvani. Vienā no gadījumiem zaudējumu apjoms sasniedza 80 000 eiro. Viltus "finanšu speciālisti" mudināja veikt ieguldījumus nelicenzētās MarketCFD un CoinYards platformās, sākotnēji radot iespaidu, ka tiek gūta peļņa, un vēlāk solot iespēju atgūt pirmajā reizē "ieguldīto". Lai sevi pasargātu no krāpnieciskiem darījumiem, CERT.LV un Valsts policija aicināja pieņemt apdomīgus lēmumus, rīkojoties ar saviem finanšu līdzekļiem, un pirms ieguldījumu veikšanas pārbaudīt, vai minētais uzņēmums ir tiesīgs darboties Latvijā, kāds ir tā darbības veids un saņemtās licences. To iespējams izdarīt Finanšu un kapitāla tirgus komisijas mājas lapā (https://www.fktk.lv/tirgus-dalibnieki/), kur ir atrodama informācija par licencētiem noguldījumu pakalpojumu sniedzējiem Latvijā. Ja tajā neatrodiet informāciju par izvēlēto investīciju platformu vai ieguldījumu brokera sabiedrību, tad to darbība Latvijā nav atļauta vai ir aizliegta.

Novembra sākumā tika saņemti neskaitāmi ziņojumi par krāpnieciska rakstura SMS it kā uzņēmuma VAS „Latvijas Pasts" vārdā. SMS saņēmējs tika aicināts samaksāt 1,00 EUR par aizturētu sūtījumu it kā no "Elkor". Sūtījuma aprakstā tika minēts: „Tālrunis, kuru jūs uzvarējāt mūsu konkursā".

Decembra vidū masveidā tika izplatīti krāpnieciski e-pasti krievu valodā, kuros apgalvots, ka ticis uzlauzts lietotāja e-pasts, nokopēts datora cietais disks un nofilmēts, kā lietotājs apmeklē pieaugušajiem domātas saites. Šādi e-pasti masveidā Latvijas kibertelpā izplatīti arī iepriekš – tikai angļu valodā.

Arī šogad decembrī tika saņemti vairāki ziņojumi par krāpnieciskiem interneta veikaliem, kas tapuši īsi pirms svētku sezonas sākuma, lai aktīvos dāvanu meklētājus kārdinātu ar nepieklājīgi zemām cenām. Vienā no gadījumiem, interneta veikalā tika pārdotas kāda slavena zīmola preces ar 80% atlaidi. Krāpnieki bija izveidojuši līdzīgu vietnes nosaukumu oriģinālā zīmola i-veikala nosaukumam.

Pikšķerēšana jeb svarīgo datu izkrāpšana

Krāpniecisku e-pastu kampaņa tika vērsta pret populāru Instagram kontu īpašniekiem Latvijā. Mēģinot izvilināt Instagram kontu piekļuves informāciju, lietotājiem tika nosūtīts e-pasts it kā no Instagram ar brīdinājumu, ka lietotāja darbībās ir konstatēti autortiesību pārkāpumi un lietotājs tiek aicināts aizpildīt pievienoto formu, lai novērstu konta darbības apturēšanu.

Otrā gadījumā populāriem lietotājiem tika nosūtīti krāpnieciski sadarbības piedāvājumi ar saiti uz piekļuves datu izkrāpšanas vietni.

Loterijās dažādu interneta pārlūkprogrammu lietotājiem tika solīts jaunākais Samsung viedtālrunis par atbildēm uz 4 vienkāršiem jautājumiem. Balvas saņemšanai laimīgajam "uzvarētājam" tika lūgts samaksāt 1 USD par piegādi, ievadot savas maksājumu kartes datus norādītajā formā. Tā krāpnieki ieguva piekļuvi upuru maksājumu karšu informācijai. Komiski, ka atsevišķos gadījumos tika uzrunāti iPhone īpašnieki ar piedāvājumu laimēt Samsung viedtālruni.

Novembrī aktīvi izplatījās vairākas pikšķerēšanas kampaņas gan publiskajā, gan privātajā sektorā. No publiskā sektora vairāki ziņojumi tika saņemti par e-pastiem latviešu valodā, kuros teikts, ka e-pasta atmiņas limits ir ticis sasniegts, ienākošie e-pasti tiek aizturēti, un problēmas risināšanai tiek piedāvāta „ātrā verificēšanās". Kampaņas mērķis bija iegūt lietotāju e-pastu piekļuves datus. Otra kampaņa skāra publisko sektoru, un aicināja tur strādājošos nomainīt e-pastu paroles, kuru termiņš ir „šodiena".

Bankas "Citadele" vārdā tika izplatīti krāpnieciski e-pasti ar paziņojumu "Jaunais uzlabojums internetabanka" - ar mērķi izkrāpt internetbankas lietotāju datus. E-pastā tika norādīta saite, kas veda uz viltus bankas "login" lapu, kas vizuāli atgādināja oriģinālo lapu. CERT.LV aicināja iedzīvotājus būt modriem, šādus e-pastus ignorēt un vienmēr pievērst uzmanību tīmekļa vietnes adresei pirms datu ievades.

Gada nogalē tika saņemti vairāki ziņojumi par viltus loteriju, kurā nesankcionēti izmantots mazumtirdzniecības tīkla "Maxima" zīmols. Loterijā kā ēsma (laimests) tika piedāvāti jaunākie viedtālruņi – Samsung Galaxy Note 10+, Apple iPhone 11 Pro un Huawei Mate 30 Pro. Tāpat kā citos gadījumos, arī šoreiz loterijas apraksts bija sastādīts nekorektā latviešu valodā.

Pakalpojuma pieejamība (DDoS)

Uz vairāk nekā astoņām stundām internetā nebija pieejams Latvijas Radio (LR), iemesls - novecojusī infrastruktūra. Klausītājiem nebija pieejams programmu saturs LR mājaslapās, sabiedrisko mediju portālā "lsm.lv" un "replay.lv". Tāpat ziņu un programmu veidotājiem nebija piekļuves ziņu lentām, e-pastiem un lokālo tīklu resursiem.

Novembrī tika saņemti vairāki ziņojumi no dažādām valsts iestādēm par DDoS uzbrukumiem to resursiem. Gandrīz visos gadījumos, izņemot vienu – uzbrukumi tika veiksmīgi atvairīti un vietņu darbība netika traucēta. CERT.LV sniedza rekomendācijas, kā nākotnē vēl sekmīgāk aizkavēt līdzīgus uzbrukumus.

Ļaundabīgs kods

Tika saņemta informācija par komand- un kontrolcentru, kas tika uzturēts Latvijā un bija paredzēts maršrutētāju un lietu interneta (IoT) iekārtu kompromitēšanai.

Virkne uzņēmumu saņēma viltotu e-pastu eksistējoša grāmatvedības uzņēmuma vārdā, ar lūgumu apstiprināt maksājuma saņemšanu, kurš veikts šī grāmatvedības uzņēmuma klienta vārdā, norādot uz pielikumā pievienoto maksājuma uzdevuma kopiju. Izsūtītāja e-pasta adrese tika viltota, pielikumā esošais dokuments saturēja datorvīrusu.

Divu valsts iestāžu darbinieki saņēma aizdomīgus e-pastus ar dīvainiem pielikumiem. Neuzmanības dēļ abās iestādēs pielikums tika atvērts. Pēc pārbaudes veikšana CERT.LV konstatēja, ka pielikumā bija Emotet saimes datorvīruss. Emotet ir modulārs banku trojānis

(*Banking Trojan*), kas lejupielādē citus Trojas vīrusus, kā arī iespējo sevī vairākus moduļus, piemēram, paroļu zagšanu. CERT.LV informēja iestādes par pārbaudes rezultātiem un turpmāk veicamajām darbībām.

Decembrī CERT.LV veica vairāku incidentu analīzi, kuru detaļas liecināja, ka vairāki valsts iestāžu darbinieki un politiķi ir piedzīvojuši mērķētu kiberuzbrukumu. Uzbrukums tika veikts, izsūtot ļaundabīgus e-pastus Krievijas vēstniecības vārdā, kas tika noformēti kā atbilde uz iepriekšēju saraksti. E-pastos tika iekļauta saite dokumenta lejupielādei, kurš bija paredzēts upuru datora inficēšanai.

Ielaušanās mēģinājumi

Saņemts ziņojums no kāda uzņēmuma par lielu apjomu dažādu drošības notikumu, kuru izcelsmes valsts bija Ēģipte. Mēneša laikā tika fiksēti vairāk nekā 50 000 šādu drošības notikumu. Visi skenēšanas un vīrusa augšupielādes mēģinājumi tikuši veiksmīgi bloķēti un nav atstājuši ietekmi uz uzņēmuma darbību.

Tika saņemta informācija par SQL injekciju uzbrukumu mēģinājumiem vairākiem valsts iestāžu resursiem. Uzbrukumu apjoms sasniedza no 60 000 līdz pat 80 000 SQL un koda injekciju mēģinājumiem viena uzbrukuma ietvaros, kas visi tika veiksmīgi atvairīti.

Kāda valsts iestāde piedzīvoja masveida paroļu minēšanas uzbrukumu ar mērķi iegūt piekļuvi iestādes e-pasta sistēmai. Piekļuve e-pasta sistēmai, izmantojot interneta pārlūku, tika aizsargāta ar divu faktoru aizsardzības risinājumu, kā rezultātā uzbrukums bija neveiksmīgs, taču izraisīja masveida lietotāju kontu bloķēšanu, apgrūtinot piekļuvi e-pastiem.

Kompromitētas iekārtas un datu noplūdes

Krievijas vēstniecība Latvijā informēja par hakeru uzbrukumu tās e-pastu sistēmai. Uzbrukuma ietvaros notika masveida mēstuļu nosūtīšana Krievijas diplomātiskās pārstāvniecības vārdā.

Neatbilstošas konfigurācijas rezultātā (nedrošas paroles) piekļuve kāda uzņēmuma video kameru ierakstam bija nesankcionēti pieejama internetā. Tas sniedza iespēju trešajām pusēm, pieslēdzoties kamerām, vērot ražošanas procesu, kas notika uzņēmumā. CERT.LV informēja uzņēmumu, un sniedza ieteikumus drošības uzlabošanai.

Kādā Latvijas interneta veikalā tika konstatēta ļaunatūra, kas zog apmeklētāju norēķinu karšu datus. Uzņēmums tika informēts par incidentu un to operatīvi novērsa, kā arī sazinājās ar skartajiem klientiem un informēja par notikušo.

Kādā pašvaldībā tika konstatēta inficēta iekārta, kas piedalījās SPAM e-pastu izsūtīšanā. Pēc pārbaudes tika konstatēts, ka kļūda Mikrotik maršrutētāja konfigurācijā bija ļāvusi inficēt iekārtu ar Kelihos ļaunatūru. Iekārta tika iztīrīta un konfigurācijas nepilnība novērsta.

Ilgākā laika periodā tika novērota ierobežotas pieejas informācijas noplūde no iekšējās Nacionālo bruņoto spēku (NBS) apziņošanas sistēmas. Nopludinātās īsziņas nesaturēja klasificētu informāciju, bet tām ir ierobežotas pieejamības statuss. Incidents netika klasificēts kā kiberuzbrukums, jo tam pamatā bija cilvēciskais faktors.

Novembra izskaņā tika saņemts ziņojums no kādas skolas par „pazudušu mājas lapu". Lapa bija izvietota uz servera, kura uzturētāji nebija sasniedzami un neatbildēja uz telefona zvaniem. Pēc izpētes tika secināts, ka uzņēmumam, kuram piederēja serveri, uzsākts likvidācijas process.

Ievainojamības

Novembrī tika saņemti vairāki ziņojumi par ievainojamām valsts iestāžu un pašvaldību vietnēm, kur potenciāli būtu iespējams izgūt klientu datus. Ievainojamības saistītas gan ar novecojušām lapu versijām, gan vietņu izstrādātāju kļūdām. CERT.LV apzināja konkrētās valsts un pašvaldību iestādes, un informēja par apdraudējumiem, kā arī sniedza rekomendācijas situācijas uzlabošanai.

Tika saņemts ziņojums par kādu interneta veikalu Latvijā, kas klientu pieejas paroles uzglabā nedrošā veidā. Attiecīgi, mēģinot atjaunot aizmirstu paroli, uz klienta e-pastu tiek atsūtīta nevis jauna pagaidu parole vai maiņas saite, bet gan lietotāja vecā parole, kas liecina par vāju paroļu drošības politiku. CERT.LV informēja interneta veikalu par pastāvošajiem riskiem, kā arī sniedza rekomendācijas situācijas uzlabošanai, lai nākotnē izvairītos no paroļu noplūdes.

Tika saņemta informācija par novecojuša sertifikāta izmantošanu kādas valsts iestādes uzturētajā informācijas sistēmā. Sistēmā obligāti veicama personas datu ievade, taču novecojušā sertifikāta izmantošana datu ievadi portālā padarīja nedrošu.

Kādas iestādes resursos tika konstatēta ievainojamība, kas ļāva piekļūt visu lietotāju augšupielādētajiem dokumentiem. Par ievainojamību tika informēts izstrādātājs, izmantotajā platformā tika ieviesti labojumi.

Decembra otrajā pusē CERT.LV saņēma ziņojumu par drošības caurumu kādā interneta veikalā. Caurums sniedza iespēju trešajām pusē izgūt sensitīvu klientu informāciju. Minētajā interneta veikalā, klientam veicot pasūtījumu, apmaksas rēķins tika saņemts e-pastā kā interneta vietne, kuru atverot, redzams pats rēķins. Rēķina formā redzama informācija par pircēju un precēm, ko tas iegādājies. Trešajām personām, zinot šo interneta vietni un pamainot pēdējo skaitli aiz "/invoice- ", bija iespējams redzēt citu klientu rēķinus ar datiem. CERT.LV sazinājās ar interneta veikala īpašniekiem un informēja par konstatēto drošības caurumu, kā rezultātā nepilnības tika veiksmīgi novērstas.

Atbildīga ievainojamību atklāšana

Atbildīgas ievainojamību atklāšanas ietvaros tika saņemts ziņojums par starpvietņu skriptēšanas (XSS) ievainojamību kādas valsts iestādes tīmekļa vietnē. Iestāde tika informēta, ievainojamība tika novērsta.

CERT.LV pasākumi incidentu novēršanā:

- Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta CERT.LV sagatavotajās ziņās un sociālā tīkla Twitter kontā (@certlv).

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 4. punktā.

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

2.-3. oktobrī CERT.LV un ISACA Latvijas nodaļa sadarbībā ar LMT un dots. rīkoja starptautisku kiberdrošības jautājumiem veltītu konferenci "Kiberšahs 2019". Šogad konference norisinājās nevis vienu, bet divas dienas, un pirmās dienas sākumā dalībniekiem bija iespēja apmeklēt praktiskos seminārus-darbnīcas, kurus vadīja pasaules līmeņa kiberdrošības eksperti. Konferenci atklāja Latvijas Valsts prezidents Egils Levits, un konferences ietvaros tika aplūkotas tādas tēmas kā sociālā inženierija un kiberoperācijas - no politiskā, tehniskā un drošības aspekta, kā arī tika apspriestas jaunākās kiberdrošības tendences un tehnoloģijas. Šogad konferencē piedalījās pārstāvji no vairāk kā 30 valstīm. Pirmo reizi konferences vēsturē CERT.LV rīkoja arī „Capture the Flag (Jeopardy-style)" sacensības.

15. oktobrī CERT.LV un NIC.lv pārstāvji piedalījās 9.-12. klašu skolēnu karjeras dienās, kas notika Radisson Blu Latvia Omega zālē. Ikgadējās Karjeras nedēļas ietvaros CERT.LV iepazīstināja skolēnus ar profesionālajām iespējām un izaicinājumiem IT drošības sfērā.

16. oktobrī CERT.LV pārstāvis piedalījās Valmieras Attīstības aģentūras organizētajā "Iedvesmas forumā" Valmierā, kurā Karjeras nedēļas ietvaros stāstīja jauniešiem par karjeras iespējām kiberdrošībā, iepazīstinot ar dažādiem profesionālās darbības aspektiem un atbildot uz jauniešu jautājumiem.

17. oktobrī CERT.LV pārstāvis uzstājās ar prezentāciju "Email (In)Security: Tragedy of the Commons" IT drošības konferencē DSS ITSEC, stāstot par e-pastu drošību.

29. oktobrī CERT.LV pārstāvis piedalījās Finanšu nozares asociācijas un partneru rīkotajā ekspertu diskusijā "DROŠI e-pirkumi", runājot par to, kādi kiberhigiēnas pasākumi jāievēro, iepērkoties internetā, kas ir pikšķerēšana un citi datu zādzības paveidi, kā arī ko darīt, ja lietotājs ir kļuvis par kiberkrāpnieku upuri. Diskusija notika semināru telpās "Birojnīca" kampaņas "Piik un gatavs" ietvaros.

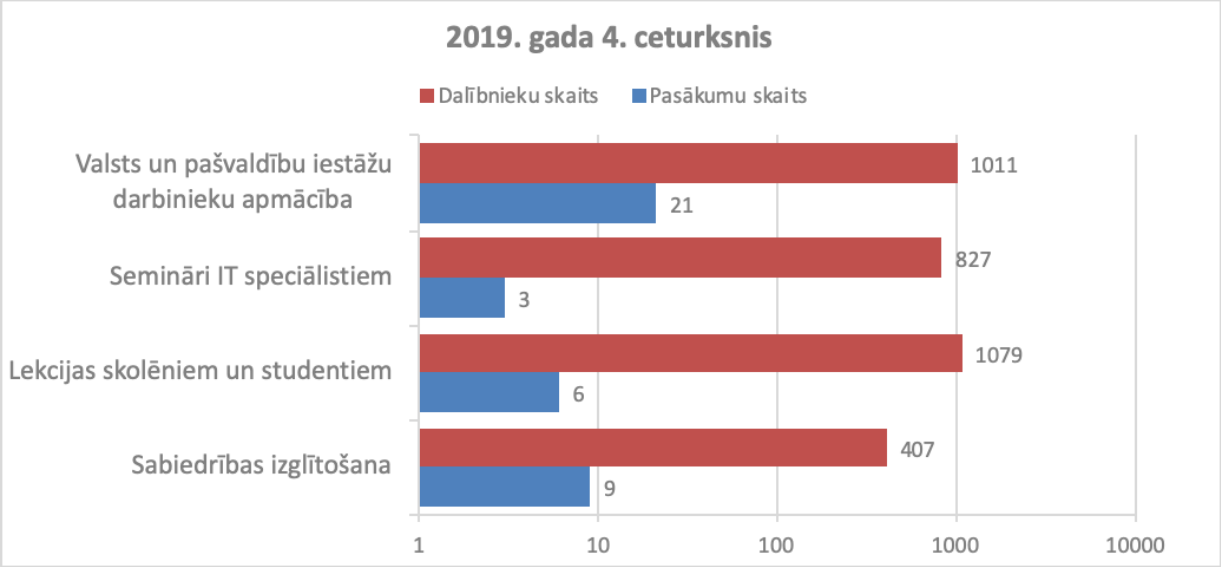
1. novembrī CERT.LV pārstāvis piedalījās Latvijas Ārpolitikas institūta un Eiropas Komisijas pārstāvniecības Latvijā organizētajā diskusijā "Cik droši Tu jūties, dzīvojot Eiropā?", paužot viedokli par kiberdrošību un kiberdraudiem Latvijā un Eiropā.

8. novembrī CERT.LV pārstāvis uzstājās ar prezentāciju "Prasme pasargāt sevi digitālajā laikmetā" un piedalījās paneļdiskusijā par drošību internetā Valsts bērnu tiesību aizsardzības inspekcijas (VBTAI) rīkotajā ikgadējā konferencē "Internets un Tu - kurš kuru?".

28. novembrī CERT.LV organizēja kārtējo semināru "Esi drošs", kurā klausītājus iepazīstināja ar IT riskiem un kiberdraudiem valsts iestādēm un pašvaldībām, inficētu IT sistēmu radītajām problēmām, e-pastu uzturēšanas labo praksi, pamatpakalpojumu un digitālo pakalpojumu sniedzēju iesaisti kiberdrošības vidē un CERT.LV piedāvātajiem drošības risinājumiem. Pasākumu apmeklēja 152 dalībnieki.

CERT.LV pārstāvis piedalījās Latvijas Informācijas un komunikācijas tehnoloģiju asociācijas (LIKTA) balvas "Platīna Pele 2019" pieteikumu izvērtēšanā kategorijā labākā "Kiberdrošības iniciatīva". Balva tika pasniegta 5. decembrī LIKTA gadskārtējā konferencē "Zināšanu Arēna", un attiecīgajā kategorijā to ieguva Vidzemes Augstskola par jaunu maģistra studiju programmu izveidi un aprobāciju.

Pārskata periodā CERT.LV par IT drošību izglītoja 3324 cilvēkus, iesaistoties 39 izglītojošos pasākumos.



8.attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2019. gada 4. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- CERT.LV piedalījās Saeimas Juridiskās komisijas sēdē, kurā tika apskatīti grozījumi likumā "Par tautas nobalsošanu, likumu ierosināšanu un Eiropas pilsoņu iniciatīvu", kas CERT.LV funkcijas vēlēšanu platformas sertifikācijā nodod Digitālās drošības uzraudzības komitejai.
- CERT.LV piedalījās sanāksmē Centrālajā vēlēšanu komisijā (CVK) par iespējamo Rīgas domes ārkārtas vēlēšanu nodrošināšanu un katras iestādes veicamajiem uzdevumiem.
- CERT.LV piedalījās sanāksmē Ārlietu ministrijā par Eiropas savienības izstrādātā sankciju mehānisma, kas piemērojams kiberuzbrukumu veicējiem, ieviešanu.
- CERT.LV piedalījās Ekonomiskās sadarbības un attīstības organizācijas (OECD) uzsāktā Latvijas Digitālās transformācijas izvērtējuma "Going Digital in Latvia" korekciju ieviešanā, komentējot un papildinot izvērtējumā iekļauto informāciju par Latvijas kiberdrošības aspektiem.
- CERT.LV piedalījās grozījumu sagatavošanā Ministru kabineta noteikumos (MKN) Nr.442, kas papildus esošajām prasībām paredz arī prasības informācijas sistēmām izstrādes laikā, prasības atsevišķām IKT komponentēm, tās iepērkot, un prasības ārpakalpojumu sniedzējiem.
- CERT.LV iesaistījās likumprojekta par e-pārvaldības regulējumu, kura izveide balstīta uz ITIL standartu, kas velta nepietiekamu uzmanību IT drošībai, komentēšanā, ierosinot pieņemt un e-pārvaldības regulējumā minēt, ka IT drošības jomu Latvijā reglamentē Informācijas tehnoloģiju drošības likums un MKN Nr.442.
- CERT.LV piedalījās LMT rīkotajā seminārā, lai paustu viedokli par Ekonomikas ministrijas gatavoto likumprojektu "Kārtība, kādā Centrālā statistikas pārvalde pieprasa un elektronisko sakaru komersants sniedz informāciju oficiālās statistikas

nodrošināšanai", norādot, ka izvēlētais datu anonimizācijas modelis ir situācijai neatbilstošs un nepietiekami pilda anonimizācijas funkciju, ļaujot ar vienkāršu algoritmu palīdzību ar augstu precizitāti identificēt konkrētas personas

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

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

CERT.LV starptautiskā sadarbība pārskata periodā:

- 28. - 29. oktobrī NIS direktīvas CERTu tīkla ietvaros notika CERT komandu savstarpējais audits (peer review). CERT.LV pārstāvis viesojās Zagrebā un veica auditu CERT.HR komandai.
- 4. – 7. novembrī CERT.LV pārstāvis kā uzaicinātais runātājs piedalījās "Future Forces Forum SCADA Security Conference" Prāgā, sniedzot prezentāciju "Weekend Warrior: Hacking Future SCADA Now" par uzbrukumu tendencēm un to realizāciju pret industriālās vadības sistēmām.
- 11. – 12. novembrī CERT.LV pārstāvis piedalījās "NIS CSIRT network" sanāksmē Helsinkos, Somijā. Sanāksmes ietvaros notika arī tematiskās darba grupas un CERT.LV aktīvi piedalījās divās darba grupās: "Cyber Weather" darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai, un "Maturity" darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
- 13. novembrī CERT.LV pārstāvji tikās ar Izraēlas vēstnieci Latvijā un vēstniecības darbiniekiem, lai apspriestu iespējamo sadarbību kiberdrošības jomā starp Latviju un Izraēlu.
- 18. – 21. novembrī CERT.LV pārstāvis piedalījās "Regional Cyber Resilience Forum" Moldovā, Kišiņevā, kur paneļdiskusijā "Regulation and Legislation. The Directive of Security of Network and Information Systems (NIS Directive) implementation, lessons learned, challenges" dalījās pieredzē par NIS direktīvas ieviešanu Latvijā, uzsverot sadarbība nepieciešamību.
- 12. decembrī CERT.LV pārstāvis piedalījās Tieslietu ministrijas organizētajā sanāksmē ar Kosovas delegācijas pārstāvjiem, sniedzot prezentāciju "Making Latvia more cyber resilient", kurā dalībniekus iepazīstināja ar CERT.LV īstenotajām sabiedrības informēšanas un izglītošanas aktivitātēm, īpaši akcentējot iesaisti Eiropas Savienības mēroga iniciatīvās, piemēram, Kiberdrošības mēnesis un Drošāka interneta diena. Kosovas delegāciju veidoja valsts iestāžu un ministriju pārstāvji. Sanāksmē piedalījās arī dalībnieki no citām Latvijas valsts iestādēm.
- 2. – 7. decembrī CERT.LV pārstāvji piedalījās NATO kiberdrošības mācībās "Cyber Coalition", kas ir vienas no lielākajām pasaulē un ir orientētas uz Alianses dalībvalstu kiberdrošības ekspertu spēju stiprināšanu NATO un nacionālās infrastruktūras aizsardzībai.

- 9. – 10. decembrī NIS direktīvas CERTu tīkla ietvaros notika CERT komandu savstarpējais audits (peer review). CERT.LV pārstāvis viesojās Tallinā un veica auditu CERT-EE komandai.
- 26. decembrī – 01. janvārī CERT.LV pārstāvis piedalījās Chaos Computer Club (CCC) organizētajā "Chaos Communication Congress" (36c3) konferencē Leipcigā, Vācijā, kurā uzstājās ar rezentāciju "Email Authentication for Penetration Testers".
- Visa pārskata perioda garumā notika sanāksmes ar potenciālajiem NATO kiberdrošības mācību "Locked Shields" dalībniekiem, pārrunājot potenciālās komandas veidošanu un citus ar sagatavošanos saistītus uzdevumus.
- Notika aktīva gatavošanās NATO CCDCoE un CERT.LV kopīgi organizētajām tehniskajām kiberdrošības mācībām "Crossed Swords", organizējot plānošanas vizītes, izstrādājot mācību vidi un tiekoties ar mācību dalībniekiem. 9.-13. decembrī Rīgā notika izmēģinājuma pasākums kiberdrošības mācībām "Crossed Swords", kurā tika pilnveidota mācību vide un uzdevumi, lai nodrošinātu sekmīgu mācību norisi 2020.gada janvārī.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Projekta "Improving Cyber Security Capacities in Latvia" īstenošana

Turpinājās 2018. gada 1.septembrī CERT.LV uzsāktā 2017 CEF Telecom-Cyber Security uzsaukumā apstiprinātā projekta "Improving Cyber Security Capacities in Latvia" (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528784) (turpmāk – Projekts) īstenošana.

Darbs turpinājās visās sešās projektā definētajās darba pakās:

- Nodrošināta dalība 18.oktobrī Briselē notikušajā projekta uzraudzības padomes sēdē – CEF Governance Board Meeting.
- Tiek turpināta "Deep Analysis System" izstrāde, gatavojoties 2020. gada 1. ceturksnī paredzētajai beta versijas publiskošanai.
- No 2. – 4. decembrim Madridē norisinājās MeliCERTes – Cybersecurity Core Service Platform – funkcionalitātes pārskatīšanas darba seminārs, kurā piedalījās CERTu tīkla un CEF projekta pārstāvji no dažādām Eiropas valstīm, ieskaitot CERT.LV pārstāvjus. Darbsemināra mērķis bija identificēt trūkums platformas funkcionalitātē un pārrunāt platformas integrāciju CERTu tīkla pārstāvju ikdienas darbā.
- Ar projekta atbalstu notika starptautiskā kiberdrošības konference "Kiberšahs 2019". Tā pulcēja kopā 630 dalībniekus no 30 valstīm. Tiešraidē konferenci vēroja 4000 dalībnieki. Konferenci atklāja Valsts prezidents E.Levits un Aizsardzības ministrs A.Pabriks. Vairāk informācijas par konferenci un konferences prezentācijas pieejamas šeit: https://www.cert.lv/lv/2019/10/pieejami-kibersahs-2019-video-materiali-un-prezentacijas
- Īss video kopsavilkums par konferenci pieejams šeit: https://www.youtube.com/watch?v=oA9AZ5uX1yg&t=17s

- Turpinājās darbs pie sabiedrību izglītojošas kampaņas "Informācijas tehnoloģiju drošība darbavietā" – pārskata periodā noslēdzās iepirkuma procedūras pirmā kārta, un tika uzsākts darbs pie otrās kārtas sagatavošanas. Plānotais kampaņas norises laiks ir 2020. gada 1./2. ceturksnis.

7. Projekta "Cyber Exchange" īstenošana

Turpinājās 2018. gada 1. novembrī CERT.LV uzsāktā 2017 CEF Telecom-Cyber Security uzsaukumā apstiprinātā projekta "Cyber Exchange" (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528866) (turpmāk – Sadarbības projekts) īstenošana.

Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības CSIRT/CERT organizācijām. CyberExchange projekts ir kā atbilde arvien pieaugošajiem draudiem kiberdrošības jomā, īpašu akcentu vēršot uz nepieciešamo pārrobežu sadarbību cīņā pret tiem. Latvija ir viena no 10 Eiropas valstīm, kas piedalās projektā.

2019. gada 4. ceturksnī projekta ietvaros CERT.LV pieredzes apmaiņas vizītē uzņēma kolēģi no CERT-RO – Rumānijas, kurš 2 nedēļu garumā iepazinās ar labo praksi un CERT.LV pieredzi kiberdrošības incidentu apstrādē, kā arī piedalījās konferencē "Kiberšahs 2019".

28. - 29. oktobrī NIS direktīvas CERTu tīkla ietvaros notika CERT komandu savstarpējais audits (peer review). CERT.LV pārstāvis viesojās Zagrebā un veica auditu CERT.HR komandai.

8. Citi normatīvajos aktos noteiktie pienākumi.

- Tika turpināts darbs pie CERT.LV un NIC.lv izstrādātā DNS RPZ (Domain Name Service Response Policy Zone) jeb DNS ugunsmūra (DNS firewall) projekta īstenošanas. Projekts sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā, kas saistīts ar kiberdrošības institūcijām jau zināmiem incidentu identifikatoriem (domēna vārdi, IP adreses u.c.). Daļu no DNS PRZ pakalpojuma var izmantot arī bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC.lv rekursīvie DNS serveri.
- Pārskata periodā tika aktualizēts jautājums par iniciatīvu "Atbildīgs interneta pakalpojumu sniedzējs", tiekoties ar LIA (Latvijas Interneta asociācija), tika atjaunots sadarbības memorands, un plānota jaunu dalībnieku piesaiste. 31. oktobrī organizētajā informatīvajā seminārā interneta pakalpojumu sniedzējiem piedalījās 45 Latvijas interneta pakalpojumu sniedzēju pārstāvji. 2020. gadā tiks turpināts darbs pie jaunu dalībnieku piesaistes iniciatīvai. Vairāk par iniciatīvu informācija atrodama šeit: https://www.cert.lv/lv/interneta-pakalpojumu-sniedzejiem/atbildigs-ips.
- 12.oktobrī CERT.LV pievienojās Parīzes uzsaukuma (Paris call) atbalstītāju lokam. Parīzes uzsaukums ir vērsts uz uzticības un drošības veicināšanu internetā, uzsverot cilvēktiesību aizsardzību kibertelpā un valstu atbildību starptautisko normu ievērošanā arī digitālajā vidē.
- Tika organizētas un īstenotas tikšanās ar pamatpakalpojumu sniedzēju statusu ieguvušajām organizācijām, lai informētu organizācijas par jaunajiem pienākumiem, kas izriet no Informācijas tehnoloģiju drošības likuma un Ministru kabineta noteikumiem Nr.442, kā arī lai sniegtu informāciju par CERT.LV nodrošinātajiem pakalpojumiem.

- 8. novembrī Aizsardzības ministrijas pateicību par ieguldījumu un sniegto atbalstu Latvijas valsts aizsardzības spēju stiprināšanā un pilnveidošanā saņēma attīstības projektu vadītājs Egils Stūrmanis, sabiedrisko attiecību projektu grupas vadītāja Līga Besere un IT drošības speciālists Kristiāns Teters.
- Par sevišķiem nopelniem Latvijas valsts labā Latvijas Universitātes Matemātikas un informātikas institūta struktūrvienības – Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas CERT.LV vadītāja Baiba Kaškina tika iecelta par Triju Zvaigžņu ordeņa virsnieci. Ordenis tika pasniegts svinīgā ceremonijā 18. novembrī Rīgas pilī.
- 11. decembrī par sekmīgu sadarbību un atbalstu valsts drošībai "Valsts Drošības Dienesta" pateicības rakstu saņēma CERT.LV vadītājas vietnieks Varis Teivāns.
- 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 veica atbilstošas konsultatīvās funkcijas.

9. Papildu pasākumu veikšana.

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

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.10.2019. līdz 31.12.2019. ir saņēmusi un izvērtējusi 988 ziņojumus. No tiem 864 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 6 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 24 ziņojumos konstatēta personas goda un cieņas aizskaršana un 7 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 16 ziņojumi, 22 ziņojumu saturs nav bijis pretlikumīgs, 49 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 820 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.

Pārskata periodā no Latvijā uzturētajiem 858 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 852 ziņojumu saturs ir dzēsts no publiskas aprites un 6 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

Sagatavotājs – Līga Besere,
tālrunis 67085888
e-pasts liga.besere@cert.lv