Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2021 C1

Publiskais pārskats par CERT.LV uzdevumu izpildi

2021. gada 1. ceturksnis (01.01.2021 – 31.03.2021.)

Pārskatā iekļauta vispārpieejama informācija, un tas nesatur informāciju par tiem CERT.LV darbības rezultātiem, kas satur ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Saturs

Kopsavilkums 4

1. Elektroniskās informācijas telpā notiekošo darbību atainojums 6

2. Atbalsts informācijas tehnoloģiju drošības incidentu novēršanā vai to novēršanas koordinēšanā 15

2.1. Krāpšana 15

2.2. Pakalpojuma pieejamība (DDoS) 17

2.3. Ļaundabīgs kods 18

2.4. Ielaušanās mēģinājumi 19

2.5. Kompromitētas iekārtas un datu noplūdes 19

2.6. Ievainojamības 20

2.7. Atbildīga ievainojamību atklāšana 21

2.8. Drošības testi 21

3. Pētnieciskais darbs, izglītojošo pasākumu organizēšana un mācības informācijas tehnoloģiju drošības jomā **22**

4. Atbalsts valsts institūcijām valsts drošības sargāšanā, noziedzīgu nodarījumu un likumpārkāpumu atklāšanā **25**

5. Sadarbība ar starptautiski atzītām informācijas tehnoloģiju drošības incidentu novēršanas institūcijām **26**

6. Projekta "Cyber Exchange" īstenošana **28**

7. Citi normatīvajos aktos noteiktie pienākumi **29**

8. Papildu pasākumu veikšana **29**

Kopsavilkums

2021. gada 1. ceturksnī tika reģistrētas 143 884 unikālas apdraudētas IP adreses, kas ir par 13% mazāk nekā iepriekšējā ceturksnī un par 29% mazāk nekā šajā pašā periodā pirms gada. Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (78 854 unikālas IP adreses) ar procentuāli nemainīgu apdraudēto IP adrešu apjomu pret iepriekšējo periodu;
- otrs izplatītākais bija ļaundabīgs kods (17 121 unikāla IP adrese) ar kāpumu par 8%;
- bet trešais – ielaušanās mēģinājumi (2986 unikālas IP adreses) ar kāpumu 48%.

Ielaušanās mēģinājumu skaita pieaugums skaidrojams ar ienākošo datu apjoma palielināšanos attiecībā uz kompromitētām lietu interneta (IoT) iekārtām, kā arī palielinātu šo iekārtu aktivitāti, meklējot iespējas kompromitēt citas IoT iekārtas.

Pārskata periodu iezīmēja jauna krāpniecība maksājumu karšu datu un finanšu līdzekļu izkrāpšanai, kurā krāpnieki izmantoja preču piegādes kompāniju – *DPD Latvija* vai *Omniva Latvija* – zīmolus, lai izkrāptu no iedzīvotājiem maksājumu karšu datus un finanšu līdzekļus. Lielākā daļa krāpniecību atpazina, taču bija arī tādi, kas krāpnieciskajās vietnēs ievadīja karšu datus un cieta finansiālus zaudējumus.

Apjomīgu incidentu izraisīja martā publicētās kritiskās *Microsoft Exchange* e-pasta serveru ievainojamības. Veicot apdraudēto iekārtu apzināšanu Latvijas kibertelpā, tika konstatēti 165 ievainojami serveri. Analizējot augstas prioritātes iestādes (valsts un pašvaldību iestādes, valsts kapitālsabiedrības), tika konstatēti 7 veiksmīgi uzbrukumi, bet 4 organizācijās konstatēti

neveiksmīgi uzbrukumu mēģinājumi. Veiksmīga uzbrukuma gadījumā uzbrucēji gūst piekļuvi e-pastu plūsmai (e-pastu piekļuves datiem, pielikumiem, adrešu grāmatai, kalendāram), kā arī iespējama uzbrucēju tālāka pārvietošanās iekšējā tīklā. Ievērojamā incidenta apjoma dēļ incidenta risināšanā tika piesaistīta arī Zemessardzes Kiberaizsardzības vienība.

Aktualizējās arī datu drošības jautājums. Tika saņemta informācija par šifrējošā izspiedējvīrusa uzbrukumu uzņēmumam *Civinity*, kura rezultātā noplūdes draudiem tika pakļauti arī 30 000 klientu dati. Uzņēmums rīkojās atbildīgi un par iespējamo datu noplūdi informēja lietotājus, ar atklātību radot satraukumu sabiedrībā un medijos.

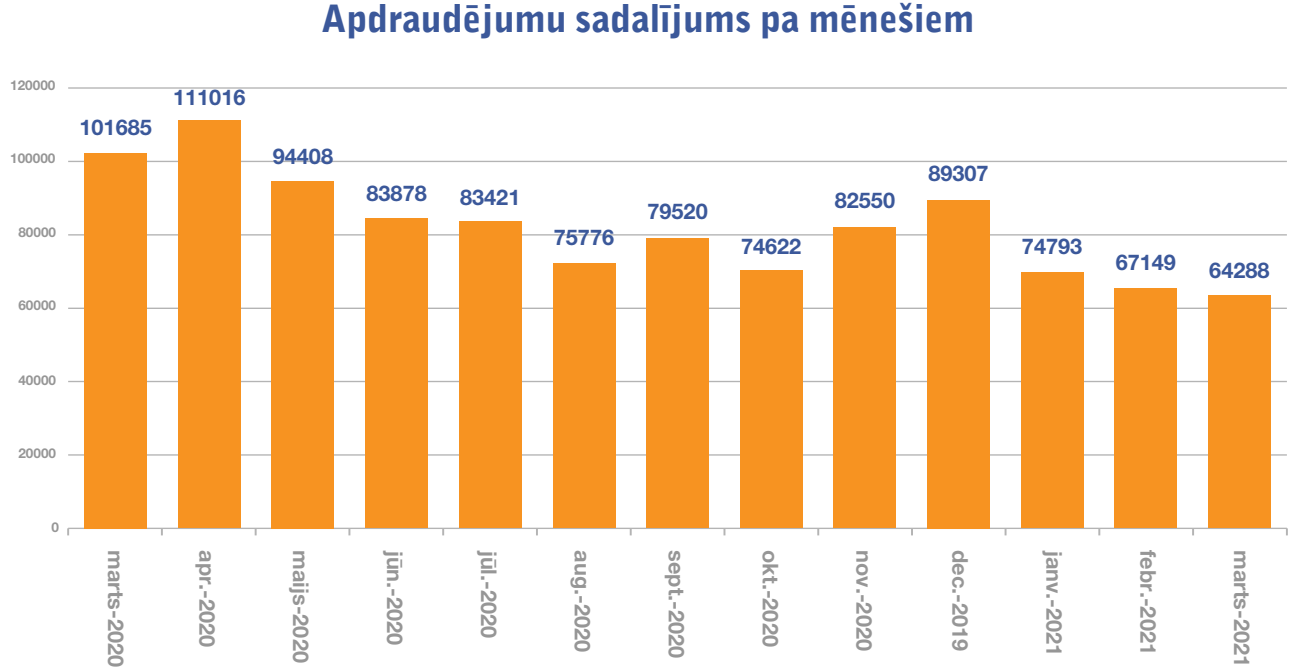
Informācijas izgūšanai un trešo pušu nesankcionētai piekļuvei bija pakļauti arī vairāk nekā 1000 ievainojamu individuālu apkures iekārtu, kuru saskarnes bija eksponētas publiskajā tīklā. CERT.LV publicēja brīdinājumu un aktualizēja viedo ierīču (IoT) drošības jautājumu. Pateicoties jautājuma aktualizēšanai, līdzīgu iekārtu pārbaudes un trūkumu novēršanu uzsāka Latvija elektroenerģijas piegādes uzņēmumu grupas un sakaru operatori.

31. martā tika rīkots IT drošības seminārs *Esi drošs*, kurā tika aplūkota droša e-pasta tehnoloģiju ieviešana, ES kiberdrošības stratēģija un NIS2 direktīva, veikts *Solarwind* incidenta apskats, aplūkoti efektīvi autentifikācijas mehānismi, *Emotet* otrā viļņa sakāve, kā arī veikts atskats uz aktuālajiem notikumiem kibertelpā 2021. gada 1. ceturksnī. Pasākumu attālināti vēroja 326 dalībnieki.

Pārskata periodā CERT.LV par IT drošību izglītoja 5672 cilvēkus, iesaistoties 49 izglītojošos pasākumos.

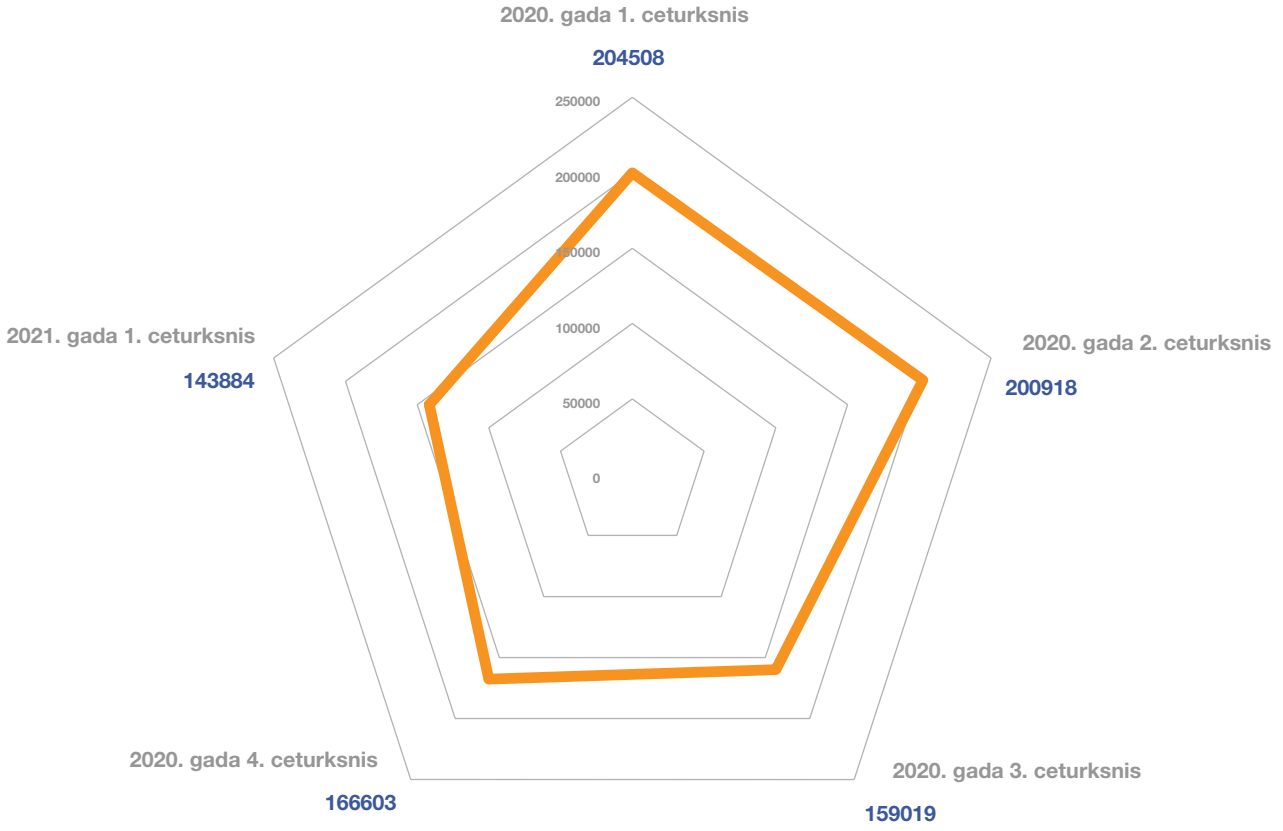
1. Elektroniskās informācijas telpā notiekošo darbību atainojums

Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, CERT.LV apdraudējumu uzskaitei izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija, kas nosaukta par *Reference Security Incident Taxonomy*). Taksonomija ir formalizēts veids kā CERT.LV apkopo, sadala kategorijās un reprezentē par apdraudējumiem iegūto tehnisko informāciju. Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīti vienkopus, sadalot tos pa apdraudējumu veidiem (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī pa ļaunatūru (piemēram, *Confiker*, *Zeus*, *Mirai*) un konfigurācijas nepilnību (piemēram, *Opendns*, *Openrdp*) tipiem.



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

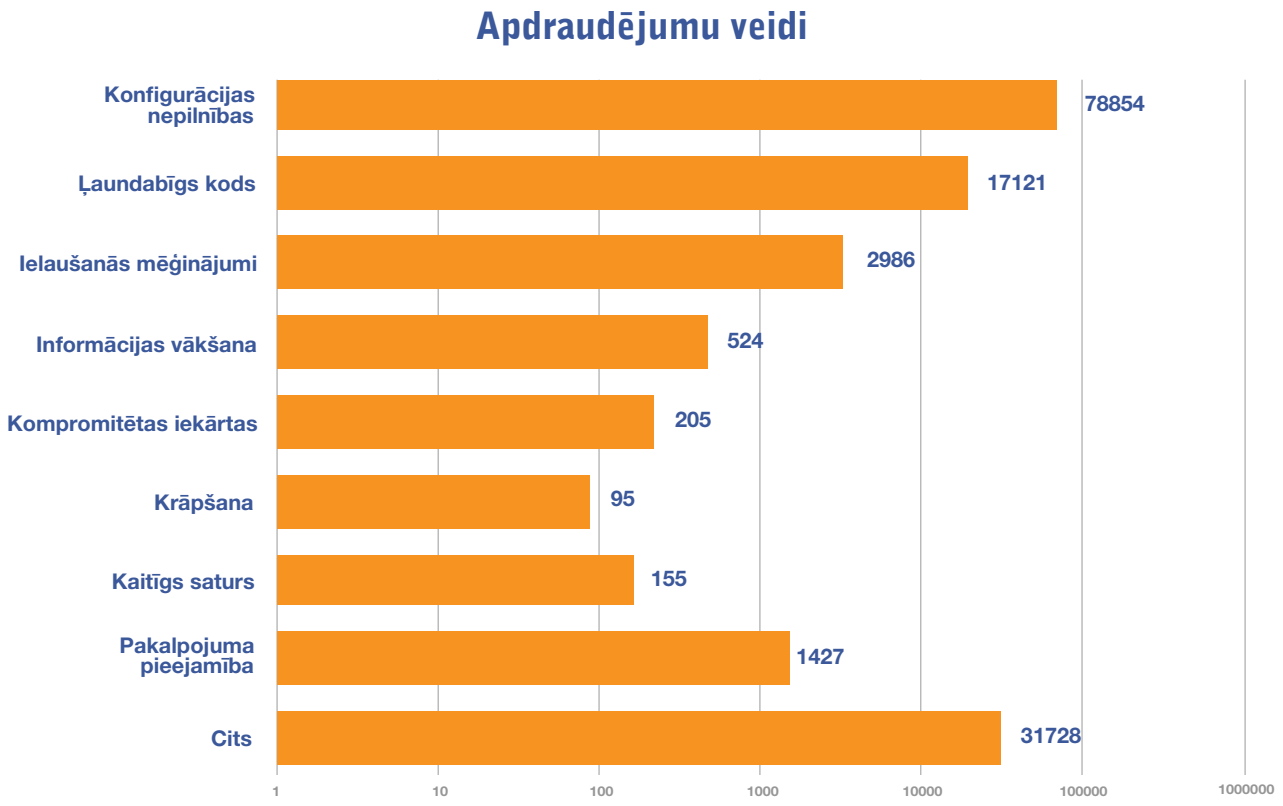
Apdraudējumu sadalījums pa ceturkšņiem



2. attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2020. un 2021. gadā.

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju vidēji par 68 000 – 70 000 ievainojamu unikālu IP adrešu.

2021. gada 1. ceturksnī tika reģistrētas 143 884 unikālas apdraudētas IP adreses, kas ir par 13% mazāk nekā iepriekšējā ceturksnī un par 29% mazāk nekā šajā pašā periodā pirms gada.

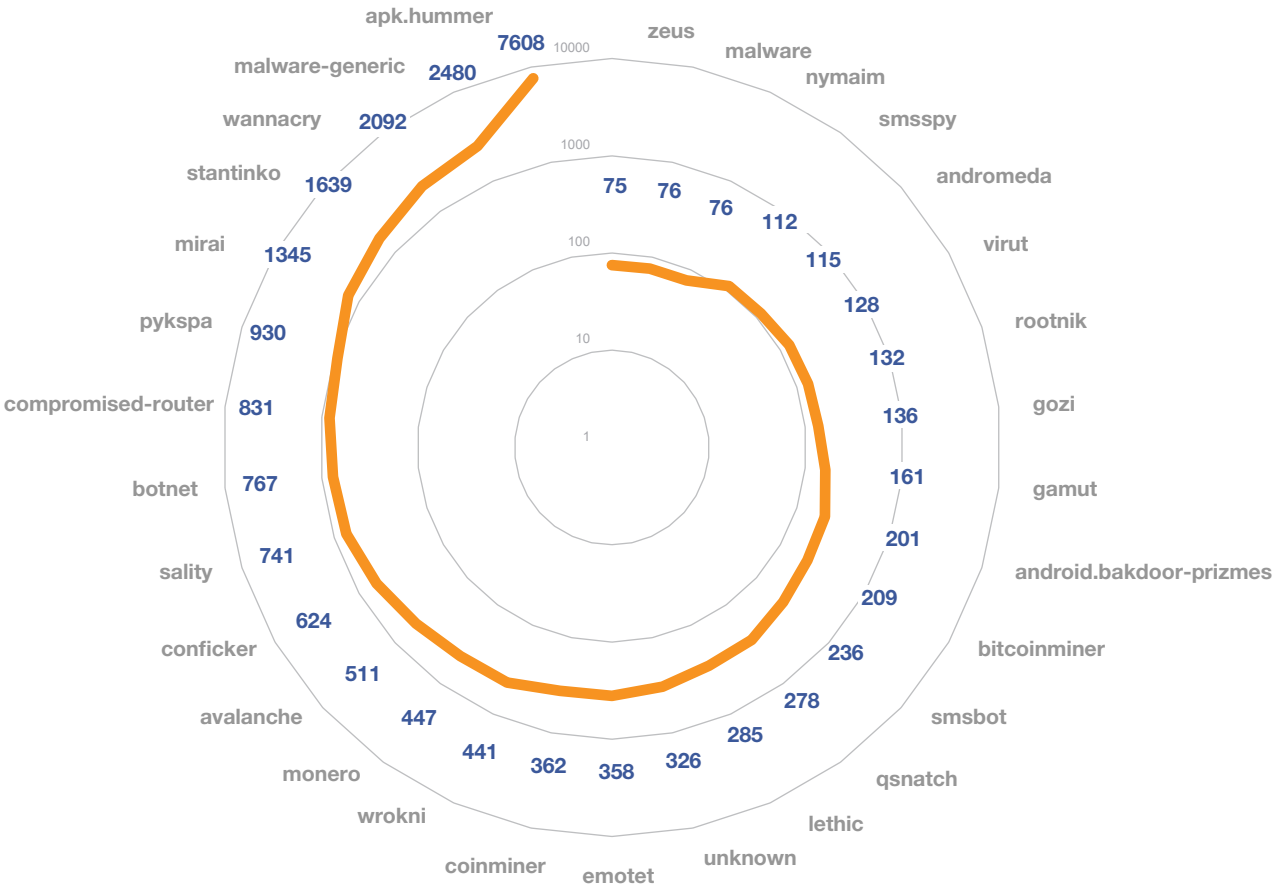


3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 1. ceturksnī pa apdraudējumu veidiem.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (78 854 unikālas IP adreses) ar procentuāli nemainīgu apdraudēto IP adrešu apjomu pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (17 121 unikāla IP adrese) ar kāpumu par 8%, bet trešais – ielaušanās mēģinājumi (2986 unikālas IP adreses) ar kāpumu 48%.

Ielaušanās mēģinājumu skaita pieaugums skaidrojams ar ienākošo datu apjoma palielināšanos attiecībā uz kompromitētām lietu interneta (IoT) iekārtām, kā arī palielinātu šo iekārtu aktivitāti, meklējot iespējas kompromitēt citas IoT iekārtas.

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 1. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

Topa pirmo vietu ieņem ļaunatūra *Android Hummer*, kas iekārtās ar *Android* operētājsistēmu (planšetdatoros un viedtālruņos) demonstrē uznirstošas (*pop-up*) reklāmas un patstāvīgi lejupielādē dažādas lietotnes.

Otro vietu ieņem *WannaCry* (*WannaCrypt*) – ļaunatūra ar šifrējošo potenciālu. Šīs ļaunatūras izplatība vērojama galvenokārt privātajā sektorā. Izplatību iespējams novērst, uzstādot *Windows* iekārtu atjauninājumus.

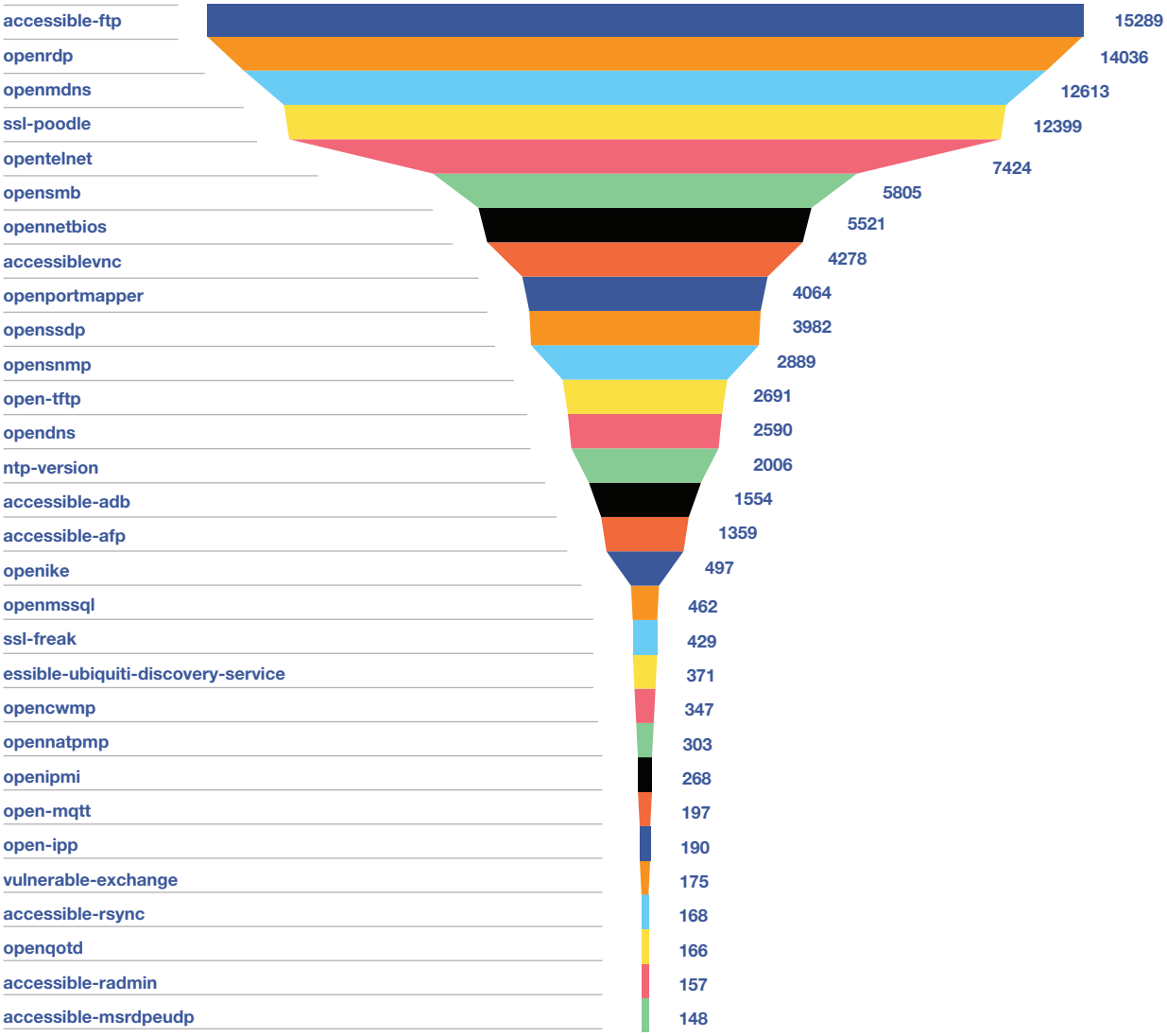
Trešo vietu ieņem topa jaunpienācēja – ļaunatūra *Stantinko*, kas paredzēta dažādu kriptovalūtu ieguvei, nesankcionēti izmantojot upura iekārtas resursus un potenciāli radot iekārtas pārslodzi, kā arī demonstrē lietotājam reklāmas, tā nodrošinot reklāmu izvietotājiem peļņu.

Konfigurācijas nepilnību topa augšgalā atrodas *Accessible-FTP*. *FTP* datu pārraides protokols nenodrošina pārraidāmo datu šifrēšanu, ja vien netiek izmatota papildu aizsardzība *TLS* vai *SSL* protokola formā (attiecīgi *FTPS*). Šī konfigurācijas nepilnība pakļauj noplūdes riskam sensitīvu informāciju un piekļuves datus.

Otrajā vietā atrodas konfigurācijas nepilnība *OpenRDP*. Tā bieži tiek izmantota, lai piekļūtu iekārtām un tās sašifrētu. Ja netiek ievērota labā prakse un netiek ierobežota piekļuve *RDP* servisam, piemēram, ierobežojot 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 uzstādīta pietiekami droša piekļuves parole.

Topa augšgalā atrodas arī konfigurācijas nepilnība *OpenmDNS (multicast DNS)*. Papildus tam, ka šīs iekārtas tiek pakļautas liela apjoma informācijas noplūdes riskam, tās var tikt izmantotas *UDP* amplifikācijas uzbrukumos, radot piekļuves traucējumus citām iekārtām un organizāciju resursiem.

Unikālo IP adrešu skaits – konfigurācijas nepilnības

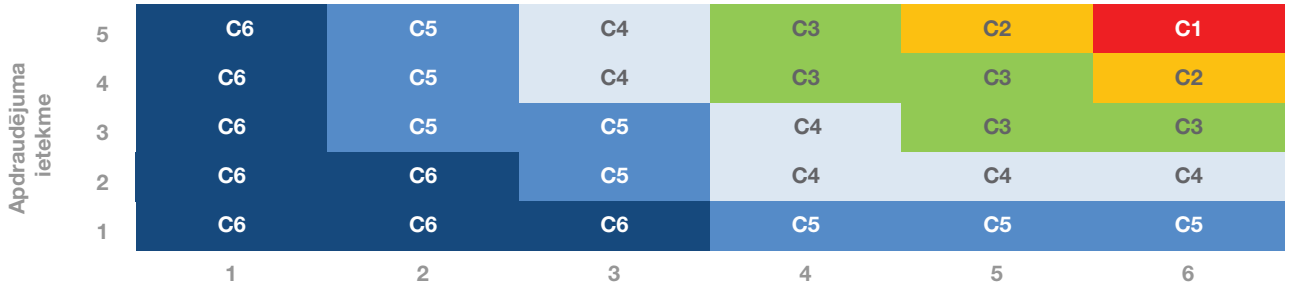


5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 1. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV 2020. gadā uzsāka Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC) izveidotās apdraudējumu matricas lietošanu. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības daļu apdraudējums ietekmē, kā arī pēc tā, cik būtiskas sekas attiecīgais apdraudējums radīs. Apvienojot visus faktorus, apdraudējumi tiek iedalīti 6 kategorijās:

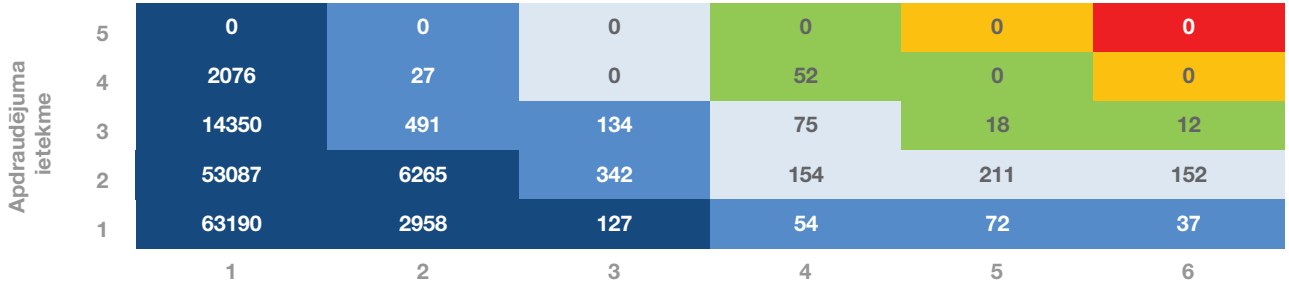
C1	Nacionāla līmeņa apdraudējums, ietekmēta pamatpakalpojumu sniegšana, apdraudēta ekonomiskā vai politiskā stabilitāte.
C2	Augstas nozīmes apdraudējumi, ietekmētas valsts iestādes, nacionālā infrastruktūra.
C3	Nozīmīgi apdraudējumi, plaša ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C4	Būtiski apdraudējumi, vidēja ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C5	Mēreni apdraudējumi, neliela ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.
C6	Ikdienas apdraudējumi, ietekmē atsevišķus indivīdus, nenozīmīga ietekme uz uzņēmumiem vai valsts un pašvaldību iestādēm.

Apdraudējumu matrica



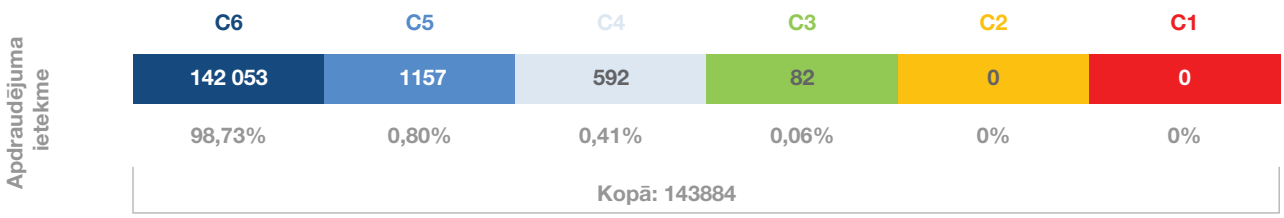
6. attēls – Apdraudējumu matricas sadalījums kategorijās.

Apdraudēto unikālo IP adrešu izvietojums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2021. gada 1. ceturksnī valsts un pašvaldību institūcijās.

Gandrīz 99% apdraudējumu ietilpst maznozīmīgu apdraudējumu kopā (C6), un ir saistīti ar individuālu lietotāju iekārtām vai plaši izplatītiem ikdienišķiem, automatizētiem uzbrukumu mēģinājumiem uzņēmumiem vai valsts un pašvaldību iestādēm.



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2021. gada 1. ceturksnī.

Nacionāla līmeņa apdraudējumi (C1) un augstas nozīmes apdraudējumi (C2) pārskata periodā nav reģistrēti. Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,06% (82 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. Lielākā daļa šo apdraudēto IP adrešu saistītas ar ievainojamām iekārtām vairākos interneta pakalpojumu sniedzējos un pašvaldību iestādēs, kā arī ļaunatūrām *Apk. Hummer, Wannacry, Emotet* un *Mirai* vairākās valsts un pašvaldību iestādēs.

Lielākā daļa C4 līmeņa apdraudējumu (būtiski apdraudējumi ar vidēju ietekmi) bija konfigurācijas nepilnības (*Accessible-ftp*, *OpenRDP, OpenDNS, Opentelnet*, uc), ielaušanās mēģinājumi, pakalpojuma atteices (*DDoS*) uzbrukumi un vidējas ietekmes ļaundabīgs kods (*Avalanche, Kelihos, Monero u.c.*), kas novēroti augstas un vidēji augstas prioritātes iestādēs un virknē pašvaldību.

Lai mazinātu kopējo apdraudēto IP adrešu skaitu, CERT.LV kopā ar Latvijas Interneta asociācijas (LIA) Latvija Drošāka interneta centru ir izveidojuši iniciatīvu *Atbildīgs interneta pakalpojumu sniedzējs*, kuras ietvaros saprašanās memorands tiek parakstīts ar ieinteresētajiem interneta pakalpojumu sniedzējiem (IPS), lai tie varētu informēt savus klientus par viņu iekārtās konstatētajiem apdraudējumiem. Atbildīgo IPS skaits līdz pārskata perioda beigām saglabājās bez izmaiņām – 13.

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

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.

2.1 Krāpšana

Pārskata periodā krāpnieciskās aktivitātes Latvijas kibertelpā bija vērstas galvenokārt uz lietotāju maksājuma karšu datu un finanšu līdzekļu izkrāpšanu. Vairumā gadījumu krāpniecības mēģinājumi tika atpazīti, taču atsevišķos gadījumos lietotāji ir ievadījuši krāpnieciskās vietnēs maksājumu karšu datus un cietuši finansiālus zaudējumus.

No janvāra beigām tika saņemti ziņojumi par jaunu krāpniecību maksājumu karšu datu un finanšu līdzekļu izkrāpšanai. Krāpnieki uzrunāja iedzīvotājus, kuri dažādās interneta platformās bija izvietojuši pārdošanas sludinājumus, un izrādīja vēlmi iegādāties pārdodamo preci, norādot, ka piegāde un arī apmaksa tiks veikta ar preču piegādes kompāniju – *DPD Latvija* vai *Omniva Latvija* – starpniecību. Maksājuma saņemšanai pārdevējs tika aicināts sekot saitei, kuru saņēma no pircēja. Saite norādīja uz viltotu *DPD Latvija* vai *Omniva Latvija* vietni, kurā pārdevējs tika aicināts ievadīt savas maksājumu kartes datus, tajā skaitā CVV kodu un kartē pieejamo atlikumu. Uzrunāti tika galvenokārt mēbeļu un lietotas elektrotehnikas pārdevēji, no kuriem lielākā daļa krāpniecību atpazina, taču bija arī tādi, kas krāpnieciskajās vietnēs ievadīja karšu datus un cieta finansiālus zaudējumus.

CERT.LV sadarbībā ar preču piegādes kompānijām informēja sabiedrību par krāpšanu, uzsverot, ka CVV kods norādāms tikai pirkuma izdarīšanai, nevis maksājuma saņemšanai.

Maksājumu karšu datu izkrāpšanai tika izmantoti arī banku (*SEB Latvia*, *Swedbank*) un pasta pakalpojumu sniedzēju (*Latvijas Pasts*) zīmoli, izsūtot e-pastus ar saņēmējam saistošu saturu – par sūtījuma saņemšanu vai darbībām kontā – aicinot sekot e-pastā norādītajai saitei uz krāpniecisku vietni un tajā ievadīt maksājumu karšu datus.

Vairāki Latvijas iedzīvotāji cieta no finanšu krāpniecības. Uzbrucēji veica telefona zvanus un pārliecināja iedzīvotājus veikt investīcijas krāpnieciskās platformās vai veikt darbības fiktīva kriptovalūtas konta aizvēršanai, tā iegūstot piekļuvi upura bankas kontam vai maksājumu līdzekļu informācijai. Kopējie iedzīvotāju zaudējumi pārskata periodā bija vismaz 10 000 EUR.

Februāra vidū tika saņemta informācija par krāpniecības mēģinājumiem, kuros uzņēmumu grāmatvežiem uzņēmumu vadītāju vārdā tika izsūtīti e-pasti ar lūgumu mainīt vadītāja vai kāda darbinieka algas kontu. Krāpniecībā ir cietušie.

CERT.LV aicināja pārbaudīt kontu maiņas pieprasījumus, izmantojot citus saziņas kanālus, piemēram, telefona zvanu, kā arī izmantot elektroniski parakstītus dokumentus.

Krāpnieki centās iegūt arī uzņēmumu kontus platformā *Facebook*, imitējot ziņojumus no *Facebook* administrācijas par autortiesību pārkāpumiem vai citām neatļautām darbībām. Ziņojumos tika iekļauta saite uz *Facebook* piekļuves datu izkrāpšanas vietni, kurā ziņojuma saņēmēji tika aicināti "autentificēties".

Lai pārņemtu individuālu lietotāju kontus, *Facebook* ziņu apmaiņas platformā tika izplatīta ziņa ar saiti uz videomateriālu, kura aplūkošanai aicināts atkārtoti autentificēties.

CERT.LV aicināja pirms jebkādu sensitīvu (tajā skaitā sociālo kontu piekļuves) datu ievades vēlreiz pārbaudīt vietnes adresi, lai pārliecinātos, ka tā ir īstā, kā arī iespējot vairākfaktoru autentifikāciju, kas apgrūtinātu kontu pārņemšanu, pat ja uzbrucēji iegūtu konta paroli.

2.2. Pakalpojuma pieejamība (DDoS)

Pārskata periodā turpinājās piekļuves lieguma (*DDoS*) uzbrukumi finanšu institūcijām ar mērķi veikt izspiešanu. Uzbrucēji veica iebiedēšanas uzbrukumus, kas pārsniedza 400 Gb/s, un pieprasīja veikt maksājumu kriptovalūtā, lai novērstu atkārtotu, vēl apjomīgāku uzbrukumu. Sākotnējos uzbrukumus institūcijas veiksmīgi atvairīja, tālāki uzbrukumi nesekoja.

CERT.LV ieteica nekomunicēt ar uzbrucējiem un neveikt maksājumu, jo tas apliecinātu upura spēju maksāt un varētu novest pie atkārtotiem uzbrukumiem nākotnē, kā arī veicinātu šādu uzbrukumu veikšanu.

25. janvārī CERT.LV tika informēta par darbības traucējumiem platformā *e-klase*. CERT.LV no *e-klase.lv* saņēma tikai daļu no analīzei nepieciešamās informācijas. Saņemtā informācija nebija pietiekama, lai izdarītu vienozīmīgus secinājumus par 25. janvārī notikušajiem platformas *e-klase* darbības traucējumiem un to cēloņiem, kā arī lai varētu apstiprināt vai noliegt nesankcionētu ārēju ietekmi.

5. februārī tika atvērta pieteikšanās vakcīnai pret Covid-19 vietnē www.manavakcina.lv tika novēroti vietnes darbības traucējumi, atsevišķos gadījumos gaidīšanas laikam virtuālajā rindā pārsniedzot stundu. *Slimību profilakses un kontroles centrs* darbības traucējumus skaidroja gan ar vakcinēties gribētāju lielo skaitu, gan to, ka reģistrācija vietnē notika, izmantojot *latvija.lv* autentifikācijas moduli, kas neizturēja lielo noslodzi. Pārslodzes dēļ *latvija.lv* autentifikācijas pakalpojums uz vairākām stundām nebija pieejams visiem lietojumiem – ne tikai *manavakcina.lv*, bet arī *e-veselība*, nodokļu deklarāciju iesniegšanai un citiem pakalpojumiem.

19. martā tika saņemta informācija par iekārtu darbības traucējumiem *Latvijas Dzelzceļš* infrastruktūrā. Bojāta mikroprocesora dēļ uz gandrīz 6 stundām tika apturēta vilcienu satiksme *Rīgas Centrālajā stacijā*.

19. martā lietotāji visā pasaulē un arī Latvijā piedzīvoja *Facebook* un tam piederošo pakalpojumu – *Instagram*, *WhatsApp*, *Messenger* – darbības traucējumus, kas ilga aptuveni stundu. Šajā laikā

šo platformu lietotāji nevarēja saņemt aktuālās ziņas un apskatīt jaunākās publikācijas ziņu lentēs. *Facebook* nav sniedzis komentārus, kas tieši izraisījis šādus traucējumus.

2.3. Ļaundabīgs kods

Pārskata periodā izplatītākās ļaunatūras bija orientētas galvenokārt uz lietotāju datu (lietotājvārdi, paroles u.tml.) izgūšanu, kā arī uz iekārtu inficēšanu reklāmu demonstrēšanai.

Turpinājās *Emotet* vīrusa izplatība. Pārskata perioda sākumā vīruss tika izplatīts kā novēlots svētku apsveikuma e-pasts ar ZIP arhīvu pielikumā. Vēstules sūtītāji parasti bija lietotājam pazīstami, kā arī vēstule vairumā gadījumu saturēja vēsturiskas sarakstes fragmentus.

Janvāra beigās vērienīgā starptautiskā operācijā, sadarbojoties vairāku valstu dienestiem, tika apturēta *Emotet* botneta darbība. Lai arī *Emotet* ļaunatūra tika deaktivizēta, pastāv risks, ka inficētajās iekārtās atrodas vēl citas ļaunatūras, piemēram, *Trickbot*, un nepieciešams veikt datora pārbaudi un iekārtā izmantoto paroļu nomaiņu.

Tika saņemti ziņojumi par mēģinājumiem inficēt datorus un izgūt piekļuves informāciju (lietotājvārdus, paroles u.tml.) kampaņveidīgi izplatot e-pastus gan dažādu banku, gan *Latvijas Universitātes* vārdā, pielikumā pievienojot vīrusu saturošu dokumentu.

Ļaunatūra tika izplatīta arī *Facebook* platformā. Uzlauztos lietotāju profilos tika ievietotas finansiāla rakstura ziņas, pie kurām tika atzīmēti profila īpašnieka draugi. Dažos gadījumos, atverot ziņā ietverto saiti, lietotāji tika pārvirzīti uz *Facebook* piekļuves datu izkrāpšanas vietni, bet vairumā gadījumu, atverot saiti, lietotāji tika aicināti veikt lejupielādi, kurā informācijas izgūšanai paredzēta ļaunatūra tika maskēta kā programmatūras atjauninājumi.

Lietotnē *WhatsApp* Valentīndienas nedēļā masveidā izplatījās krāpnieciska rakstura ziņas par iespēju laimēt dāvanu. Dāvanas saņemšanai lietotāji tika aicināti pārsūtīt ziņu 20 draugiem un

lejupielādēt piedāvāto lietotni. Lietotne saturēja adware ļaunatūru, kas interneta pārlūkā veica reklāmu demonstrēšanu.

Šifrējošo vīrusu uzbrukumos cieta vairāki uzņēmumi, tajā skaitā arī *Latvijas Pasts*. Uzbrukumi ietekmēja uzņēmumu darbību, dažos gadījumos uzbrukumā cieta arī datu rezerves kopijas. CERT.LV sniedza konsultācijas pierādījumu iegūšanā un incidenta analīzē.

2.4. Ielaušanās mēģinājumi

Ielaušanās mēģinājumi lielākajā daļā gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi veikti galvenokārt pret dažādiem interneta pakalpojumu sniedzējiem un dažām valsts un pašvaldību iestādēm, kā arī privāto sektoru. Pēc CERT.LV rīcībā esošās informācijas šie uzbrukumi ir bijuši nesekmīgi.

2.5. Kompromitētas iekārtas un datu noplūdes

Pārskata periodā 93 % kompromitēto iekārtu bija kompromitēti maršrutētāji nelielos uzņēmumos vai individuālās mājsaimniecībās.

Janvāra otrajā pusē tika saņemta informācija par šifrējošā izspiedējvīrusa uzbrukumu uzņēmumam *Civinity*, kurā iespējama arī 30 000 klientu datu noplūde. Uzņēmums rīkojās atbildīgi un informēja klientus par iespējamo datu noplūdi. CERT.LV sniedza uzņēmumam nepieciešamo atbalstu, lai veicinātu incidenta ietekmes pārvarēšanu.

Vairāki Latvijas uzņēmumi cieta no iejaukšanās biznesa sarakstē (*Business e-mail compromise* jeb *BEC*). Piekļūstot uzņēmuma vai sadarbības partnera e-pasta kontam, uzņēmumiem tika nosūtīti rēķini sadarbības partneru vārdā, bet ar mainītiem banku kontiem. Kopumā pārskata periodā šādi tika izkrāpti vairāk nekā 88 000 EUR.

CERT.LV aicināja uzņēmumus vienmēr, kad tiek veiktas izmaiņas finanšu datos, sazināties ar biznesa partneri pa citiem komunikācijas kanāliem (piemēram, piezvanot) un pārliecināties par informācijas patiesumu.

Plašu sabiedrības uzmanību un mediju interesi guva e-pasts no adreses *manavakcina@gmail.com*, kura saņēmēji tika aicināti aizpildīt anketu, norādot vārdu, uzvārdu, telefona numuru un to, vai būtu gatavi vakcinēties. CERT.LV saņēma informāciju par to, ka konkrēto e-pastu izveidojis kāds students pētnieciskos nolūkos, izstrādājot darbu par informācijas tehnoloģiju drošību. Pētījuma autors individuāli sazinājās ar katru respondentu, informējot par notikušo, un pētījuma rezultātā iegūtie lietotāju dati tika dzēsti.

CERT.LV aicināja sabiedrību sekot aktualitātēm un gūt informāciju par vakcinēšanos no oficiāliem avotiem – Veselības ministrijas un *Slimību profilakses un kontroles centra* tīmekļa vietnēs un sociālo tīklu profilos.

2.6. Ievainojamības

Turpinājās decembrī atklātā *SolarWinds* incidenta, kurā tika kompromitēta programmatūras Orion atjauninājumu piegādes sistēma, ietekmes izvērtēšana. Analizējot *SolarWinds* produktu lietojumu Latvijas kibertelpā, tika atklāti kompromitētās programmatūras lietojumi dažos Latvijā strādājošos uzņēmumos. Pasaulē *SolarWinds* incidents novērtēts kā viens no visapjomīgākajiem un sarežģītākajiem kiberuzbrukumiem.

CERT.LV aktualizēja viedo ierīču (IoT) drošību, izplatot brīdinājumu par vairāk nekā 1000 ievainojamām individuālajām apkures iekārtām, kuru saskarnes eksponētas publiskajā tīklā, sniedzot iespēju nepiederošām personām piekļūt šīm iekārtām un veikt izmaiņas iekārtu iestatījumos, piemēram, atslēdzot apkuri. Papildu apdraudējums bija iespēja attālināti izgūt informāciju par adresi un iekārtas konfigurāciju, piemēram, vai objektā kāds uzturas.

Pateicoties jautājuma aktualizēšanai, līdzīgu iekārtu pārbaudes un trūkumu novēršanu uzsāka Latvija elektroenerģijas piegādes uzņēmumu grupas un sakaru operatori. CERT.LV vērsa arī konkrēto iekārtu oficiālo izplatītāju Latvijā uzmanību uz identificētajiem riskiem.

2. martā tika publicētas četras jaunas kritiskas ievainojamības plaši izplatītā *Microsoft Exchange* e-pasta serveru programmatūrā. Veicot apdraudēto iekārtu apzināšanu Latvijas kibertelpā, tika konstatēti 165 ievainojami serveri. Analizējot augstas prioritātes iestādes (valsts un pašvaldību iestādes, valsts kapitālsabiedrības), tika konstatēti 7 veiksmīgi uzbrukumi, bet 4 organizācijās konstatēti neveiksmīgi uzbrukumu mēģinājumi. Veiksmīga uzbrukuma gadījumā uzbrucēji gūst piekļuvi e-pastu plūsmai (e-pastu piekļuves datiem, pielikumiem, adrešu grāmatai, kalendāram), kā arī iespējama uzbrucēju tālāka pārvietošanās iekšējā tīklā. Ievērojamā incidentu skaita un apjoma dēļ incidentu risināšanā tika piesaistīta arī Zemessardzes Kiberaizsardzības vienība.

2.7. Atbildīga ievainojamību atklāšana

Tika saņemts ziņojumi par starpvietņu skriptēšanas (XSS) ievainojamību divos valsts iestāžu tīmekļa resursos. Abos gadījumos ievainojamības tika novērstas. Starpvietņu skriptēšanas (XSS) ievainojamība sniedz uzbrucējam iespēju izpildīt patvaļīgu kodu citu lietotāju aplūkotajās tīmekļa vietnēs, piemēram, pārvirzot lietotāju uz kaitīgu vietni, kā arī apiet vietņu piekļuves drošības mehānismus.

Tika saņemts ziņojums arī par ievainojamību kādas iestādes tīmekļa vietnē, kas sniedza uzbrucējam iespēju piekļūt informācijai par reģistrētajiem lietotājiem.

2.8. Drošības testi

Tika veikta drošības pārbaude kādas valsts iestādes resursa autentifikācijas modulim. Ņemot vērā, ka resursa izstrāde veikta uz atvērtā koda *Drupal* bāzes, tika plānots arī jaunizveidotos moduļus atvērt izmantošanai citos risinājumos. Pārbaužu rezultātā modulim tika atklāti vairāki būtiski

drošības trūkumi, par kuriem tika informēta iestāde. Pēc drošības trūkumu novēršanas modulim tika veikts atkārtots drošības tests, kas apliecināja moduļa drošības atbilstību labajai praksei un nepieciešamajiem drošības standartiem.

Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV tīmekļa vietnē un sociālo tīklu *Twitter* (@certlv) un *Facebook* (@cert.lv) kontos.

Cita veida sadarbība ar dažādām iestādēm ir norādīta atskaites 7. un 12.punktā.

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

25. janvārī CERT.LV piedalījās Latvijas Universitātes Sociālo zinātņu fakultātes studentu un radio NABA gatavota raidieraksta izveidē par drošu interneta izmantošanu attālinātā darba un mācību vajadzībām, kurā notika eksperta diskusija ar studentiem. Raidījums: https://naba.lsm.lv/lv/raksts/info-demija/kiberdrosiba.a139409

9. februārī tika atzīmēta vispasaules Drošāka interneta diena. Arī CERT.LV savos resursos publicēja informatīvus materiālus drošākai interneta lietošanai.

22. – 26. martam norisinājās *Eiropas Digitālās nedēļas* aktivitātes, kurās aktīvi piedalījās arī CERT.LV:

- 22. martā CERT.LV sadarbībā ar NIC.LV stāstīja uzņēmējiem par finansiālo drošību digitālajā vidē, kiberuzbrukumu veidiem, e-pastu viltošanu, domēnvārdu izmantošanu kiberuzbrukumos un biežāk pieļautajām lietotāju kļūdām prezentācijā *Kā viegli nePAZAUDĒT naudu internetā* (https://www.digitalaiscentrs.lv/skaties/2021/certlv-ka-viegli-nepazaudet-naudu-interneta).

- 25. martā tika atzīmēta *Digitālās identitātes un drošības diena*, kuras ietvaros CERT.LV piedalījās *RigaTV24* raidījumā *Digitālā nedēļa #digiTuvi*, sniedzot ieskatu kiberdrošības aktualitātēs (https://fb.watch/4KztHjUhgb/), piedalījās *LVRTC* organizētajā kiberdrošības seminārā *KIBERNAKTS dienas vidū*, sniedzot prezentācijas *Kiberdrošības dzeņa vēders. Cik atšķirīga ir izpratne par drošību uzņēmumos* un *Paroļu ēras beigas, jeb kāpēc identitātei ir jābūt drošai* (https://fb.watch/4KzHj6xUp-/), kā arī piedalījās augsta līmeņa ekspertu diskusijā *KIBERNAKTS 2021 | Kiberneatkarība,* diskutējot par digitālajām prasmēm *jaunajā* realitātē, apdraudējumiem digitālajā telpā, valsts kiberaizsardzības stratēģiju un tās īstenošanu, kā arī preventīvajiem pasākumiem kiberdrošības uzlabošanai (https://fb.watch/4KAdNLyYW7/).

23. martā CERT.LV piedalījās Biznesa tehnoloģiju platformas *Bismart* organizētajā *IT nozares konferencē 2021* un sniedza prezentāciju *"Draugi, nav labi!" jeb Exchange ievainojamību sekas* (konferences ieraksts: https://www.bismart.lv/pasakumu-arhivs/it-nozares-konference-2021-418).

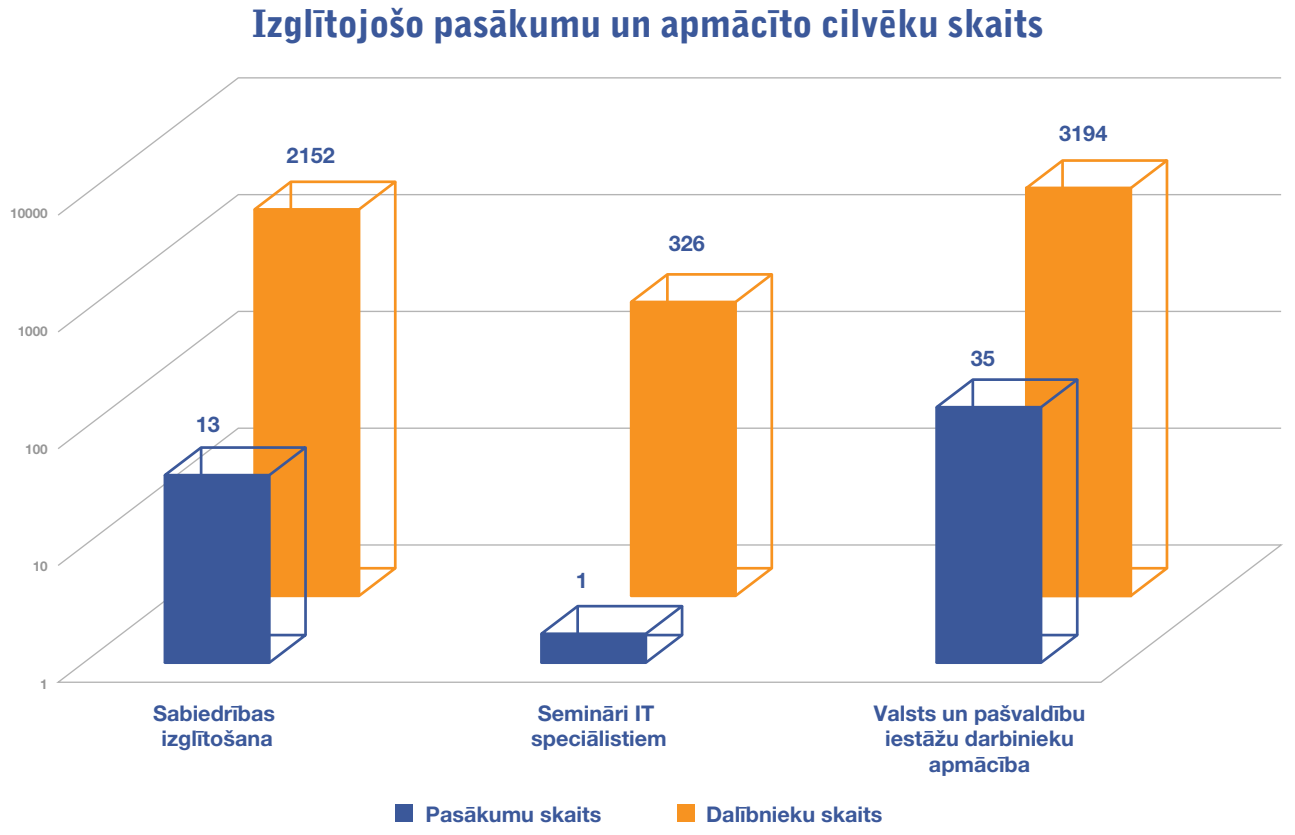
26. martā CERT.LV piedalījās diskusijā, kuru organizēja *META Advisory Latvia* un Eiropas Komisijas Pārstāvniecība Latvijā vebināru ciklā *Digitālā transformācija*. Diskusijas notika par kiberdrošību attālinātā darba laikmetā. Ieraksts: https://youtu.be/6tEszqU79jc

31. martā tika rīkots IT drošības seminārs *Esi drošs*, kurā tika aplūkota droša e-pasta tehnoloģiju ieviešana, ES kiberdrošības stratēģija un NIS2 direktīva, veikts *Solarwind* incidenta apskats, aplūkoti efektīvi autentifikācijas mehānismi, *Emotet* otrā viļņa sakāve, kā arī veikts atskats uz aktuālajiem notikumiem kibertelpā 2021. gada 1. ceturksnī. Pasākumu attālināti vēroja 326 dalībnieki.

CERT.LV atvērtā pirmkoda risinājums *Pastelyzer* ieguva nominanta statusu Latvijas atvērto tehnoloģiju asociācijas (LATA) balvai kategorijā *Atvērtākais risinājums*.

CERT.LV iesaistījās *Finanšu nozares asociācijas* organizētajā informatīvajā kampaņā *Neuzķeries! Esi gudrāks par krāpniekiem*, lai veicinātu iedzīvotāju izpratni par finanšu krāpšanas veidiem un rīcību ar to saistītās situācijās.

Pārskata periodā CERT.LV par IT drošību izglītoja 5672 cilvēkus, iesaistoties 49 izglītojošos pasākumos. Ņemot vērā epidemioloģisko situāciju valstī un ar to saistītos ierobežojumus, visi pasākumi notika tiešsaistē.



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2021. gada 1. ceturksnī

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- Aktīva dalība Veselības ministrijas un Nacionālā veselības dienesta (NVD) vadītā *Vakcinācijas projekta* IT risinājuma izstrādē, konsultējot par IT drošības prasībām un to ieviešanu.
- 23. februārī dalība Iekšlietu ministrijas organizētajā *Kritiskās infrastruktūras darba grupas* sanāksmē, kurā tika izskatīta jaunā direktīva *Directive on the resilience of critical entities (CER)*, kas paredz kritiskās infrastruktūras aizsardzību Eiropas mērogā, un citi jautājumi.
- Uzsākta sadarbība ar Latvijas Zinātnes padomi (LZP) un trīs gadu periodā tiks vadīts projekts par valkājamo ierīču drošību. Pārskata periodā uzsākta automatizētu attālinātu sistēmu testēšana.

Pārskata periodā CERT.LV sniedzis komentārus, viedokli un rekomendācijas par:

- *NIS2 Direktīvas* priekšlikuma dokumentu.
- *Digitālo pakalpojumu aktu* un *Digitālo tirgu aktu.*
- Nepieciešamajām izmaiņām Ministru kabineta noteikumos Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām.*
- *Digitālās transformācijas pamatnostādņu 2021.-2027. gadam* tapšanā.
- *Kompromitēta domēna atpazīšana un uzbrukuma seku pārvarēšana* un *IT drošības incidenta pierādījumu materiāla iegūšana.*

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:

- CERT.LV aktīvi piedalījās trijās no piecām NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla darba grupām:
  - *Cyber Weather* darba grupā (moderē un vada CERT.LV pārstāvis), kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai.
  - *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
  - *Terms of Reference Review* darba grupā, kas pārskata tīkla statūtus un nolikumu, atbilstoši tos aktualizējot.
- Dalība FIRST darba grupas *CSIRT Framework* darbā, lai izstrādātu vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm. CERT.LV vadītāja Baiba Kaškina turpināja darbu kā *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejas) līdzpriekšsēdētāja (*co-chair*), piedaloties jauno biedru pieteikumu izskatīšanā un veicinot biedru uzņemšanas procesa uzlabošanu.
- CERT.LV pārstāvis piedalījās *FIRST* konferences programmkomitejā un pārskata periodā vērtēja konferencei iesniegtos pieteikumus, kā arī piedalījās vairākās attālinātās sanāksmēs, lai izveidotu konferences programmu. Konferences norise plānota 7.-10. jūnijā attālināti.
- CERT.LV turpināja darbu *TF-CSIRT Futures* darba grupā, lai izstrādātu jaunu pārvaldības modeli *TF-CSIRT* un *Trusted Introducer* Eiropas CERTu sadarbībai.

- Notika aktīvi sagatavošanās darbi dalībai kiberdrošības mācībās *Locked Shields 2021*, kuru norise plānota 2021. gada aprīlī. Notika vairākas koordinācijas sanāksmes ar Dienvidkorejas republikas komandu, kas būs Latvijas komandas partneri šī gada *Locked Shields* mācībās, radot nebijušu precedentu *Locked Shields* mācību norisē šāda mēroga starpreģionālajai sadarbībai.
- CERT.LV pievienojās *EU CyberNet* projektam kā viens no partneriem. Projekta mērķis ir stiprināt kiberdrošības ekspertīzi un attīstīt to ne tikai Eiropas Savienībā, bet arī ārpus tās robežām (www.eucybernet.eu). Dalība projektā sniegs iespēju CERT.LV ekspertiem, iesaistoties projekta dalībvalstu projektos, stiprināt savas zināšanas un kapacitāti, kā arī dalīties ar to ārpus Eiropas Savienības robežām, tā stiprinot starptautisko kiberdrošības kopienu. 12. martā notika virtuāls projekta atklāšanas pasākums.
- 26. februārī dalība enerģētikas informācijas apmaiņas un sadarbības grupas *Energy ISAC Camelot* sanāksmē, lai diskutētu par enerģētikas sektora MISP (*malware information sharing platform*) platformas izveidi.
- 26. martā CERT.LV piedalījās seminārā *Coordinated vulnerability disclosure*, kuru organizēja Kanādas valdības pārstāvji.
- Semināra mērķis bija apkopot informāciju par ievainojamību atklāšanas procesiem un citu valstu pieredzi, lai sekmētu Kanādai piemērotākā modeļa izvēli.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. 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 CyberExchange) īstenošana.

Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības CSIRT/CERT organizācijām. *Cyber Exchange* 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. Projekta pamata aktivitāte ir pieredzes apmaiņas vizīšu organizēšana – Latvijas CERT.LV pārstāvjiem viesojoties pie citu projekta dalībvalstu CSIRT/CERT komandām vai uzņemot vizītē kolēģus no citām CSIRT komandām.

Pārskata periodā COVID-19 ierobežojumu dēļ projekta īstenošana nebija iespējama. Projekta konsorcijs ir iesniedzis pieprasījumu Eiropas Komisijai projekta īstenošanu pagarināt līdz 2022. gada 30. jūnijam.

7. 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. DNS ugunsmūris ik dienu tiek papildināts ar Latvijas iedzīvotāju un kiberdrošības ekspertu sniegto informāciju par kiberuzbrucēju aktivitātēm Latvijas kibertelpā un sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā. Projekta ietvaros ir bijuši jau daudzi gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot iekārtas no inficēšanas. 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. Tīmekļa vietnē dnsmuris.lv pieejamas ērti lietojamas instrukcijas DNS ugunsmūra aktivizēšanai.

- Lai attīstītu sadarbību ar Interneta pakalpojumu sniedzējiem (IPS), CERT.LV ir uzsākusi sarunas ar vairākiem Atbildīgajiem IPS par DNS RPZ zonu piedāvāšanu pakalpojuma sniedzēju klientiem. Pārskata periodā notika arī kopīga sanāksme ar Sabiedrisko pakalpojumu regulēšanas komisiju, lai vienotos par šādas sadarbības iespējamību no regulatora skatu punkta.
- 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 Digitālās drošības uzraudzības komitejas ietvaros veica atbilstošo uzdevumu izpildi, kā arī iesniedza apkopojumu ENISA par 2020. gadā notikušajiem incidentiem, kas saistīti ar uzticamības pakalpojumu sniegšanu (šādi incidenti 2020. gadā nav novēroti) un ikgadējo pārskatu par savu darbību Eiropas Komisijai.

8. Papildu pasākumu veikšana

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija laika posmā no 01.01.2021. līdz 31.03.2021. ir saņēmusi un izvērtējusi 6435 ziņojumus. No tiem 6156 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 12 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 25 ziņojumos konstatēta personas goda un cieņas aizskaršana, 4 ziņojumi saņemti par naida runu un 1 ziņojums par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 84 ziņojumi, 44 ziņojumu saturs nav bijis pretlikumīgs, 109 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 6081 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 8 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 6156 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 6105 ziņojumi ir dzēsti no publiskas aprites un 51 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2021. gada 20. aprīlī

CERT.LV misija ir veicināt informācijas tehnoloģiju (IT) drošību Latvijā.

Galvenie CERT.LV uzdevumi ir uzturēt un aktualizēt informāciju par IT drošības apdraudējumiem, sniegt atbalstu valsts institūcijām IT drošības jomā, sniegt atbalstu IT drošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai .LV domēns, organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan citiem interesentiem.

Saziņa ar CERT.LV:

Telefons: +371 67085888

E-pasts: cert@cert.lv

Tīmekļa vietne: www.cert.lv

Sekot CERT.LV aktualitātēm:

www.twitter.com/certlv

www.facebook.com/certlv

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija