CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Latvijas universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

2020

Publiskais pārskats par CERT.LV uzdevumu izpildi

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

2020. gadā Latvija piedzīvoja vairākus izaicinājumus – strauju pielāgošanos attālinātajam darbam, virkni īpaši pielāgotu krāpšanas kampaņu un inovatīvus kiberuzbrukumus. Īpaši audzis kiberuzbrukumu skaits privātpersonu iekārtām mājsaimniecībās – privātajiem datoriem, maršrutētājiem, viedajiem televizoriem u.c. Salīdzinot ar pirms-pandēmijas periodu, uzbrukumu skaits audzis par 15-30%. Periodiski tika novēroti kiberuzbrukumi arī pret attālinātā darba instrumentiem, piemēram, virtuālo privāto tīklu jeb VPN (*Virtual Private Network*) un attālinātās piekļuves jeb RDP (*Remote Desktop Protocol)* tehnoloģijām – pieaugums par aptuveni 20%. Tika novērots arī ar pandēmiju nesaistītu krāpniecisku kampaņu pieaugums. Mērķauditorija šādās kampaņās pārsvarā bija gala lietotāji, savukārt mērķis – autentifikācijas datu izgūšana.

Pārskata periods izcēlās ar vairāku īpaši kritisku ievainojamību atklāšanu. Šis bija pirmais gads, kad šāds kritisku ievainojamību apjoms atklāts viena gada ietvaros. Uzbrucēji vairākas no šīm ievainojamībām veiksmīgi pielietoja uzbrukumos līdz atbilstošu atjauninājumu publicēšanai. CERT.LV veica potenciāli ievainojamo sistēmu apzināšanu valsts sektorā, informēja sistēmu uzturētājus, sniedza ieteikumus ievainojamību novēršanā un atbalstu incidentu risināšanā.

Steidzamības kārtā, ko diktēja COVID-19 pandēmijas straujā izplatība, virknē uzņēmumu un organizāciju tika pieļauti kompromisi attiecībā uz drošību, lai spētu pēc iespējas ātrāk pārslēgties uz pilnvērtīgu attālināto darbu. Neatbilstoši konfigurētas RDP piekļuves bija apdraudējums arī pirms-pandēmijas periodā, un pandēmijas apstākļos problēma tikai saasinājās. Uzbrucēji izmantoja gan nepietiekami aizsargātus RDP servisus, gan VPN vārtejas, lai kompromitētu sistēmas un piekļūtu uzņēmumu un organizāciju iekšējiem tīkliem. Biežākā problēma izrādījās nepietiekami drošu paroļu izvēle, kuras uzbrucējiem izdevās uzminēt vai piemeklēt, kā arī neatjaunotas VPN iekārtas un papildu drošības mehānismu neesamība.

Uzbrucēji turpināja izmantot iedzīvotāju nepietiekamās zināšanas un izpratnes trūkumu par vairākfaktoru autentifikācijas mehānismu darbību. Aktīvā uzbrukumu kampaņā iedzīvotāji saņēma telefona zvanus, kuros krāpnieki uzdevās, galvenokārt par banku vai Smart-ID darbiniekiem, lai panāktu otrā faktora apstiprināšanu un izkrāptu finanšu līdzekļus. Ticamības palielināšanai krāpnieki veiktajos zvanos viltoja banku telefona numurus.

Sociālajiem tīkliem ieņemot arvien lielāku lomu sabiedrības (arī iestāžu) komunikācijā, krāpnieki savā kontrolē centās pārņemt iestāžu un uzņēmumu kontus ar gana lielu lietotāju skaitu, lai tos izmantotu dažādu produktu vai pakalpojumu reklamēšanai, galvenokārt Tālo Austrumu reģionā. Krāpnieki izmantoja iebiedēšanas taktiku, izliekoties par sociālā tīkla administrāciju un draudot ar konta darbības apturēšanu lietošanas noteikumu pārkāpuma dēļ. Pieeja vairāku iestāžu kontiem tika zaudēta, kontu administratoriem ievadot piekļuves datus krāpnieku sagatavotajās vietnēs (nevienā no kontiem līdz tam netika izmantota divu faktoru autentifikācija).

Tika novērota jauna tendence ar izspiešanu saistītajos uzbrukumos. Apjomīgi (līdz pat 180 Gb/s) piekļuves atteices (DDoS) uzbrukumi tika vērsti pret finanšu institūcijām un lielajiem uzņēmumiem. Uzbrucēji pieprasīja izpirkuma maksu par uzbrukumu pārtraukšanu, draudot apturēt uzņēmuma darbību ar atkārtotu uzbrukumu līdz pat 2 Tb/s. Iebiedēšanas uzbrukumi gan neilga vairāk par dažām dienām, biežāk tie ilga mazāk par stundu. Atkārtoti uzbrukumi lielākajā daļā gadījumu nesekoja. Ja uzņēmums neuzsāka komunikāciju ar izspiedējiem, uzbrucēji zaudēja interesi un mainīja mērķi.

Ielaušanās gadījumos, kad uzbrucējiem bija izdevies iekļūt sistēmā, izmantojot, piemēram, nepietiekami aizsargātu attālinātās piekļuves servisu (RDP) vai VPN vārteju, uzbrucēji pieprasīja izpirkuma maksu ne tikai par nošifrēto datu atgūšanu, bet arī par datu nenopludināšanu (pirms nošifrēšanas tika veikta datu kopēšana).

2020. gada otrajā pusē bija vērojama strauja ļaunatūras *Emotet* izplatība gan globālajā, gan Latvijas tīmeklī. Ļaunatūra no inficētās iekārtas izplatīja sevi upura kontaktu lokam, palielinot ļaundabīgo e-pastu uzticamību ar sarakstes fragmentiem, kas iegūti no upura iekārtas, kā arī veica inficētajā iekārtā citas ļaundabīgas darbības. Latvijā īsā laika periodā ar *Emotet* tika inficētas vairāk nekā 200 organizācijas, kurās tika zaudēta kontrole pār e-pastu sarakstēm un citu informāciju.

Ir paredzams, ka pēc gada vai ilgāka perioda iegūtā informācija var parādīties atkārtotos uzbrukumos vai tikt izmantota citās mērķētās ļaundabīgās kampaņās.

Kopumā pārskata periodā CERT.LV reģistrēja 346 108 apdraudētas unikālās IP adreses. Pārskata periodā nav novērotas būtiskas svārstības apdraudēto IP adrešu apjomā.

2020.gadā CERT.LV piedalījās 58 par kiberdrošības jautājumiem izglītojošos pasākumos, apmācot un izglītojot 6758 cilvēkus. Pandēmijas ietekmē samazinājās 2. un 3. ceturksnī realizēto pasākumu apjoms. Ierobežojumu dēļ tika pārtraukti klātienes pasākumi, un pamazām uzsākta pārorientācija uz pasākumiem tiešsaistē.

No 14. septembra līdz 12. oktobrim CERT.LV ar Eiropas Savienības līdzfinansējumu īstenoja mēnesi ilgu informatīvi izglītojošu kampaņu par kiberdrošību darbavietā. Kampaņa tika vērsta uz to, lai veicinātu valsts un pašvaldību darbinieku izpratni par kiberhigiēnas principiem, kā arī spēju atpazīt un novērst iespējamos kiberuzbrukumus. Kampaņas ietvaros tika izstrādāti 4 skaidrojošie video, izveidota digitālā rokasgrāmata, izvietoti plakāti pilsētvidē, kā arī sagatavoti informatīvie raksti lielākajiem ziņu portāliem un uzturēta aktīva komunikācija sociālajos tīklos. Statistikas dati rāda, ka kampaņa sasniedza gandrīz 500 000 Latvijas interneta lietotāju.

1.-2. oktobrī, uzsākot *Eiropas Kiberdrošības mēnesi*, tiešsaistē notika CERT.LV organizētā tehniskā kiberdrošības konference *Kiberšoks 202*0, kurā ar praktiskiem piemēriem un demonstrācijām tika padziļināti aplūkotas dažādas tehniskas ar kiberdrošību saistītas tēmas. Konferencei pieteicās un to attālināti vēroja 760 dalībnieki; prezentācijas sniedza septiņi lektori no piecām dažādām valstīm. Paralēli konferencei sadarbībā ar *Cybexer Technologies* un *Tet group* norisinājās arī *Capture the Flag (CTF)* sacensības, kurās spēkiem mērojās 100 dalībnieki 29 komandās.

Nākamajā pārskata periodā, turpinoties attālinātā darba režīmam, paredzama uzbrucēju intereses saglabāšanās par attālinātai piekļuvei un saziņai izmantotajām tehnoloģijām – RDP, VPN un tiešsaistes saziņas rīkiem. Turpināsies paroļu piemeklēšana, nepietiekami aizsargātu sistēmu ļaunprātīga izmantošana, kā arī jaunu ievainojamību meklēšana. Tas vēl lielāku nozīmi piešķirs laicīgai atjauninājumu uzstādīšanai un kiberdrošības labās prakses ievērošanai. Efektīvākai

aizsardzībai CERT.LV iesaka izmantot *Zero Trust* pieeju, kas paredz rūpīgas pārbaudes jebkuram sistēmas procesam un pieslēguma mēģinājumam, sekojot principam – visu uztvert ar aizdomām, pirms gūta pārliecība par sistēmas, iekārtas vai pieslēguma drošību.

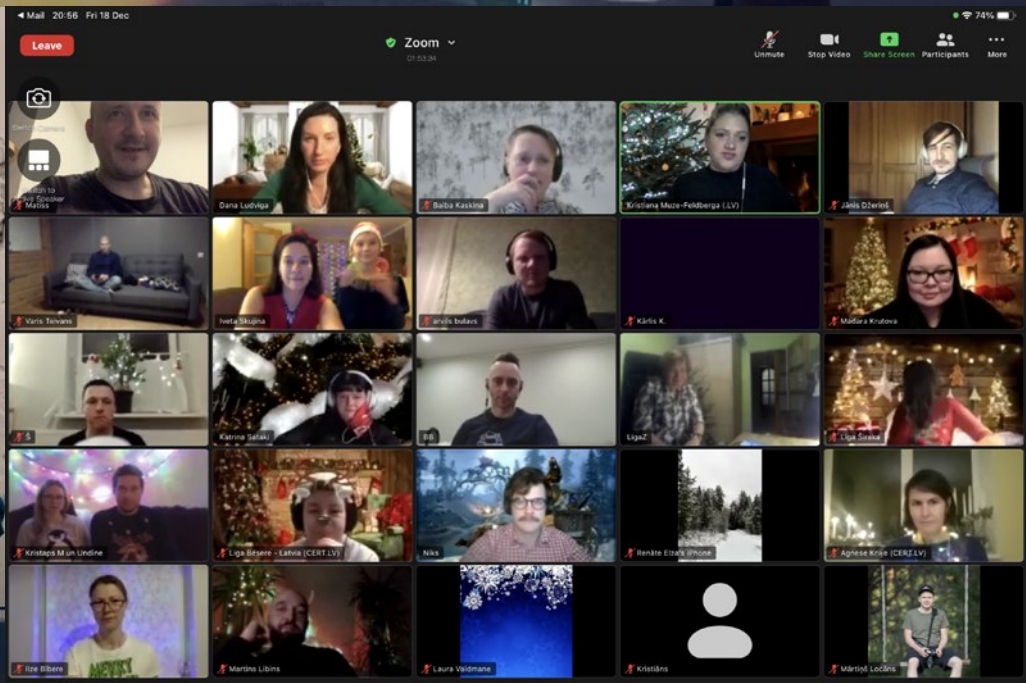
Būtiska būs ne tikai daudzfaktoru autentifikācijas ieviešana visur, kur vien tas ir iespējams, bet arī spēja nodrošināt lietotāju izpratni par daudzfaktoru autentifikācijas darbības principiem.

Ņemot vērā arvien pieaugušo tiešsaistē veicamo darbību apjomu – attālinātais darbs, sanāksmes, mācības, iepirkšanās, saziņa – kā arī jau notikušās datu noplūdes un potenciālās noplūdes nākotnē, jārēķinās ar pielāgotākiem un mērķētākiem kiberuzbrukumiem.

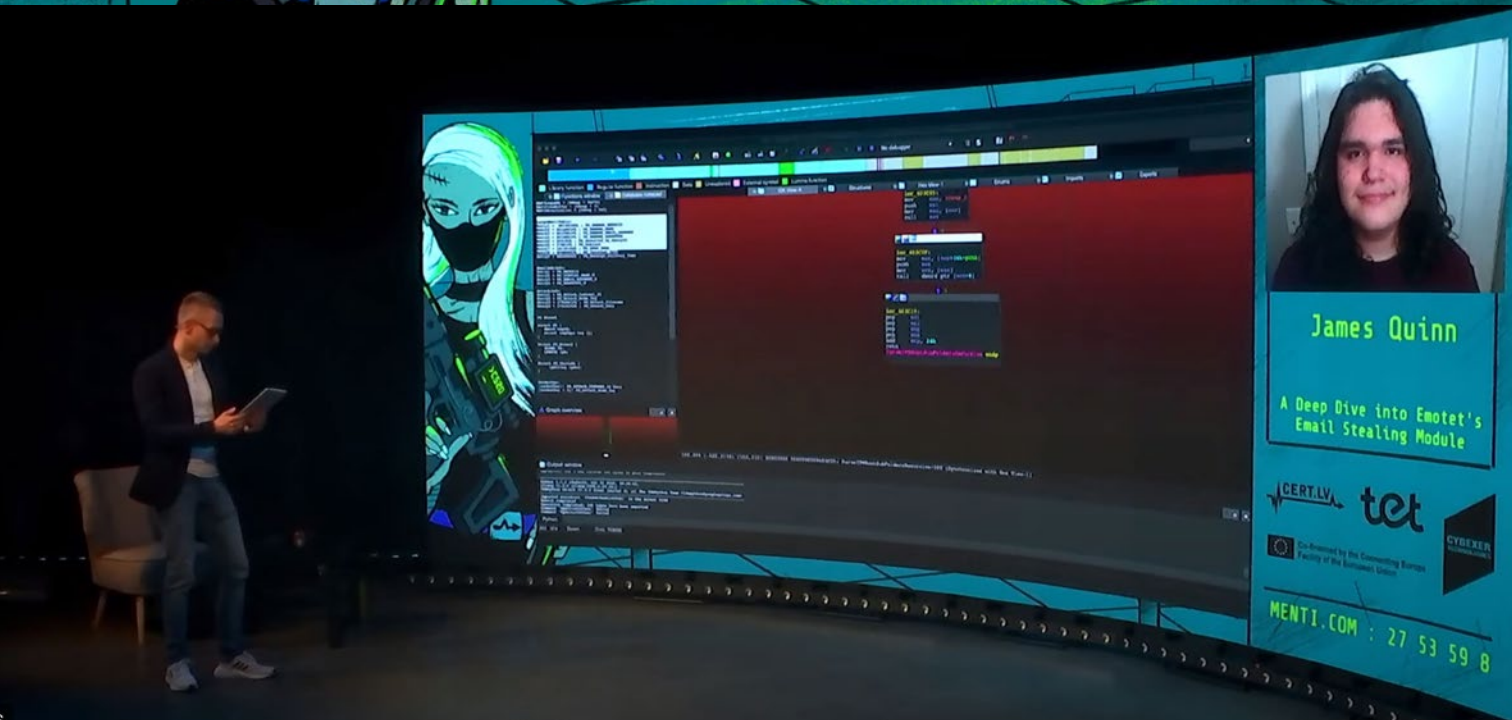
Arī 2020. gada ietekmē radītie ierobežojumi pārskata gada finansējumā radīs papildu izaicinājumus kiberdrošības pilnveidošanai – tāpēc izturību un spēku visiem 2021. gadā!

CERT.LV komandas vārdā
Baiba Kaškina
CERT.LV vadītāja


CERT.LV
CERT.LV


Leave
Zoom
Unmute
Stop Video
Share Screen
Participants
More


Cyber Shiv
2020

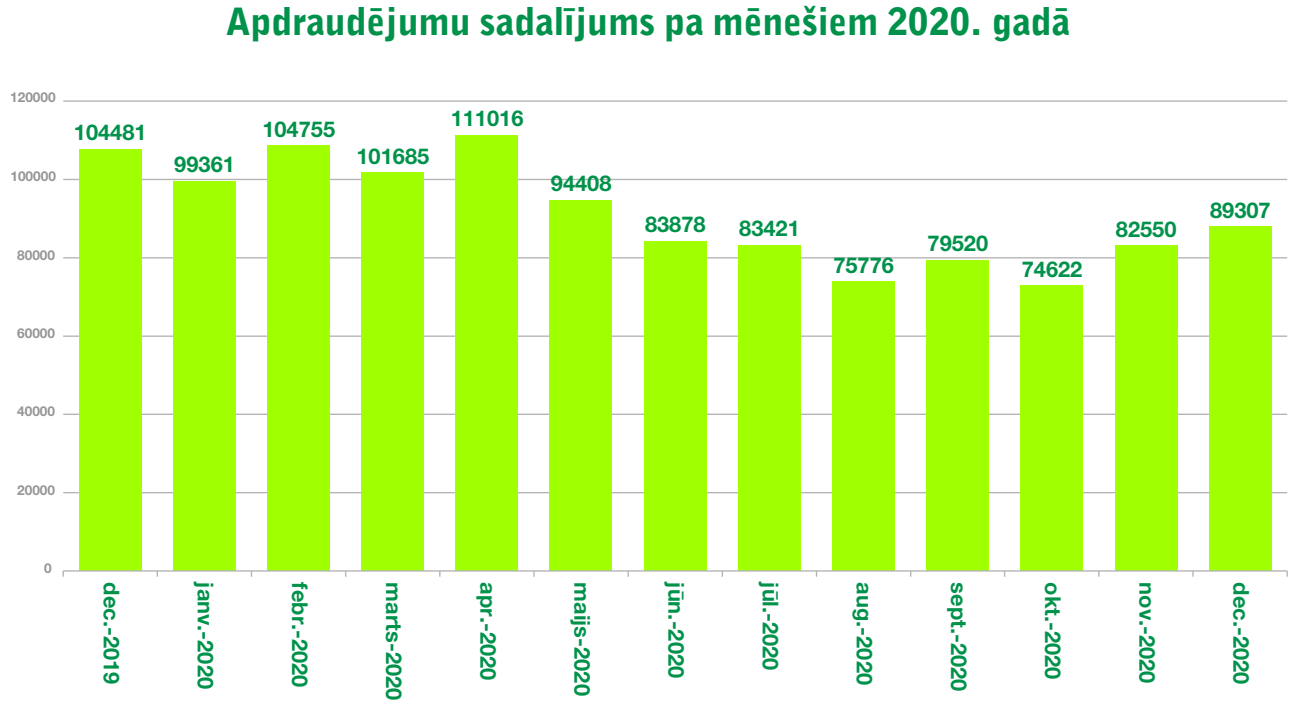

James Quinn
A Deep Dive into Emotet's Email Stealing Module
CERT.LV
tet
CYBEXER
MENTI.COM : 27 53 59 8

1.

Incidentu apstrāde

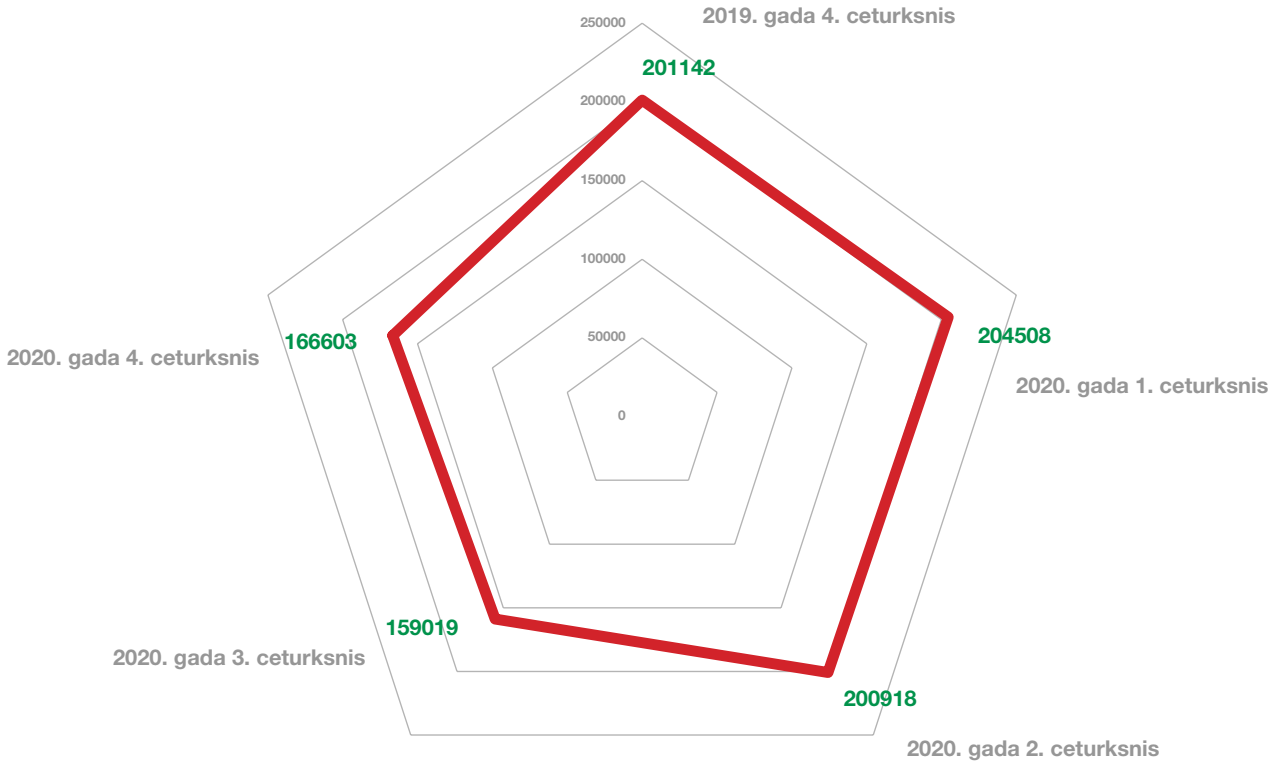
Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Apdraudējumu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija). Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīt vienkopus, sadalot tos apdraudējumu veidos (piemēram, ļaunatūra, ielaušanās, krāpšana), kā arī infekciju (piemēram, *Confiker*, *Zeus*, *Mirai*) un ievainojamību (piemēram, *Opendns*, *Openrdp*) tipos.

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju par vidēji 85 000 – 100 000 ievainojamu unikālu IP adrešu.



1. attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 2020. gadā.

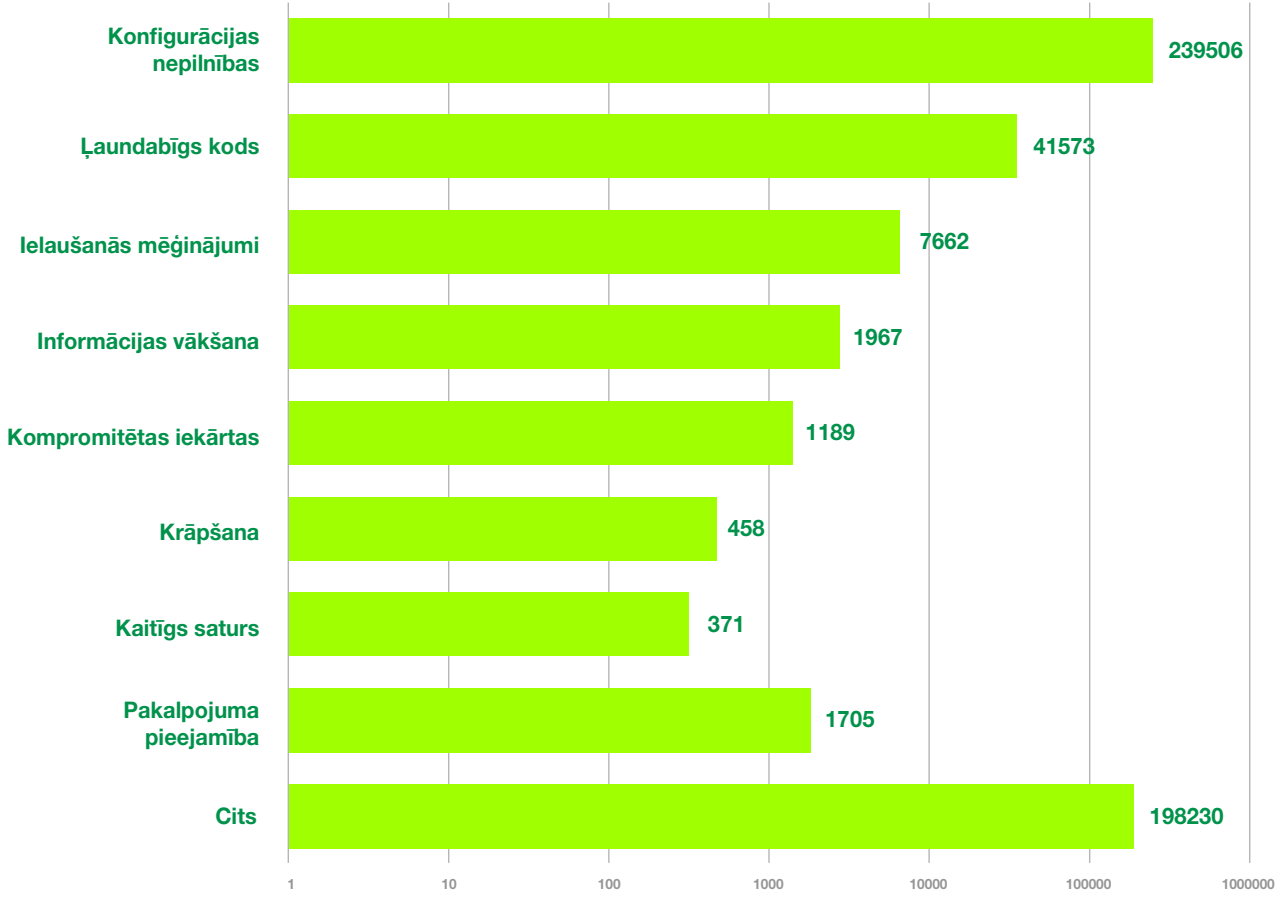
Apdraudējumu sadalījums pa ceturkšņiem 2020. gadā



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

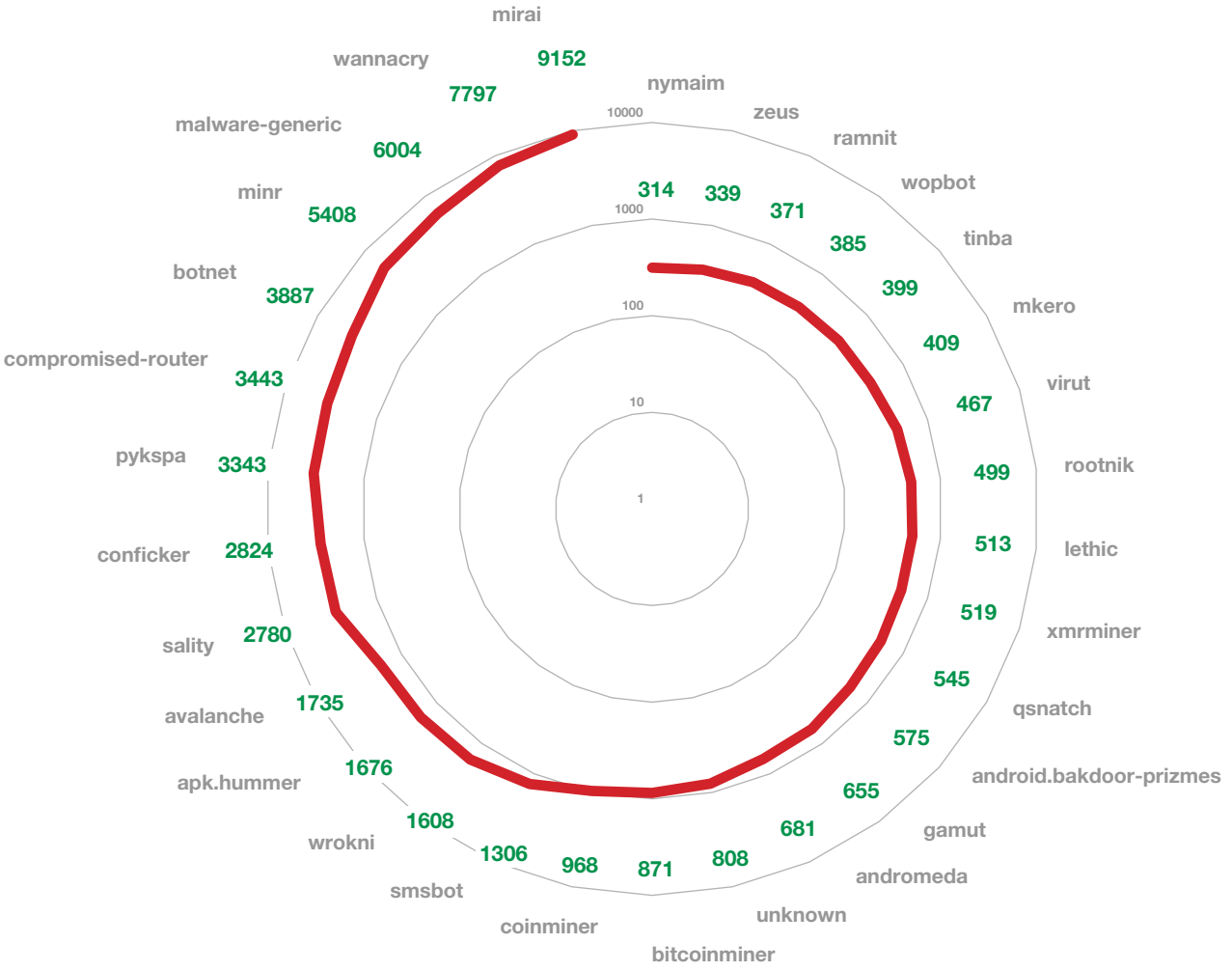
Izplatītākais apdraudējuma veids pārskata periodā nemainīgi bija konfigurācijas nepilnības, otrs izplatītākais bija ļaundabīgs kods, bet trešais – ielaušanās mēģinājumi. Kategorijā – *cits* – iekļaujama konsultatīvas informācijas sniegšana par dažādiem ar kiberdrošību saistītiem jautājumiem, galvenokārt valsts un pašvaldību institūcijām un Latvijas iedzīvotājiem, kā arī citi informācijas apstrādes gadījumi, kas nav tieši saistīti ar apdraudējumu novēršanu vai incidentu risināšanu.

Unikālo IP adrešu skaits 2020. gadā



3. attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa apdraudējuma veidiem 2020. gadā.

Unikālo IP adrešu skaits – ļaundabīgs kods 2020. gadā



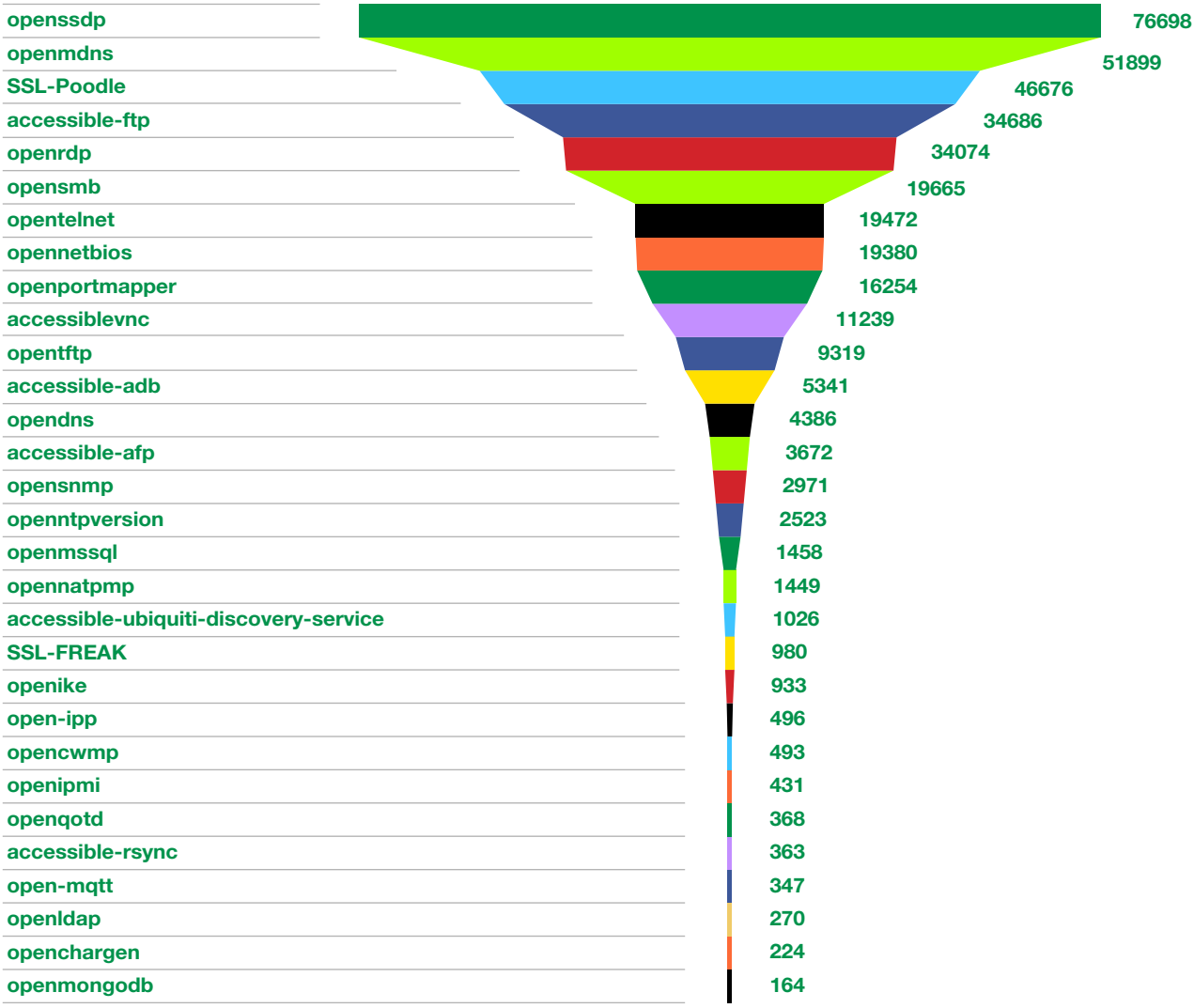
4. attēls – CERT.LV kopējais reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gadā ar apdraudējuma veidu – ļaundabīgs kods.

2020. gadā izplatītākā ļaunatūra Latvijas tīmeklī bija *Mirai* – ļaunatūra, kas apdraud neatbilstoši aizsargātas lietu interneta (IoT) iekārtas. Visbiežāk inficēti tiek viedie televizori, interneta maršrutētāji, drošības kameras un citas līdzīgas iekārtas, kas pēc iegādes tiek pieslēgtas internetam, nenomainot ražotāja iestatīto lietotājvārdu un paroli. Šie ražotāja iestatījumi jeb noklusējuma paroles ir plaši zināmas, un to izmantošana pakļauj iekārtas uzbrukumu riskam.

Otro vietu ļaunatūru izplatības topā ieņēma *WannaCrypt* jeb *Wannacry* šifrējošais izspiedējvīruss. Tas ietekmē iekārtas ar *Microsoft Windows* operētājsistēmu un izplatās, izmantojot ievainojamību *Server Message Block (SMB)* protokolā, kas tiek lietots failu apmaiņai iekšējā tīklā. Vīrusa ietekmi un izplatību iespējams novērst, uzstādot programmatūras atjauninājumus, kas pieejami pat tādām atbalstu zaudējušām *Windows* versijām kā *Windows XP* un *Windows Server 2003*.

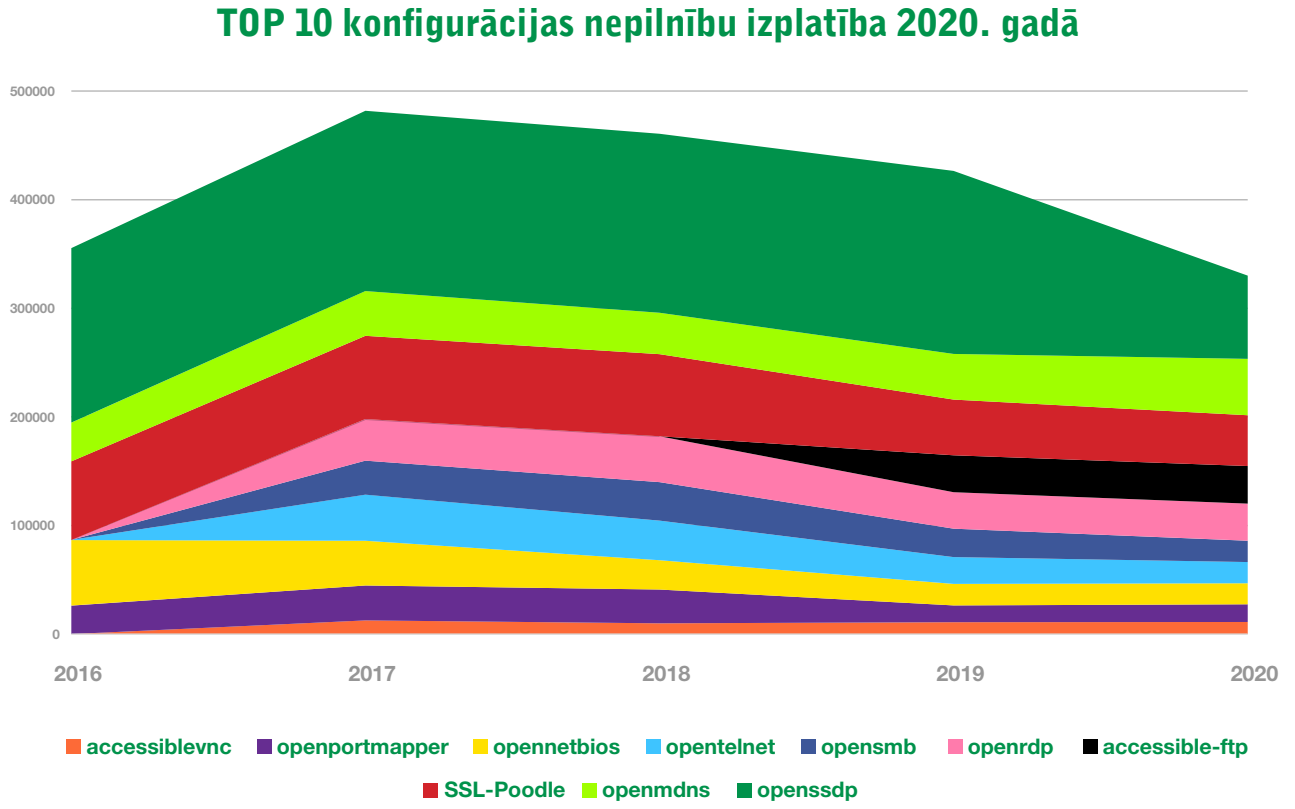
Trešo vietu ļaunatūru izplatības topā ieņem *Minr* – ļaundabīgs kods, kas tiek bieži tiek ievietots uzlauztās tīmekļa vietnēs, lai izmantotu apmeklētāju datoru jaudu kriptovalūtas *Monero* (uz privātumu orientēta kriptovalūta, kas ieguvusi popularitāti kriminālajās aprindās) ieguvei, lietotājam to nezinot. Nesaudzīgi izmantojot iekārtas jaudu, var bīstami noslogot iekārtu, tā radot neatgriezeniskus bojājumus.

Unikālo IP adrešu skaits – konfigurācijas nepilnības 2020. gadā

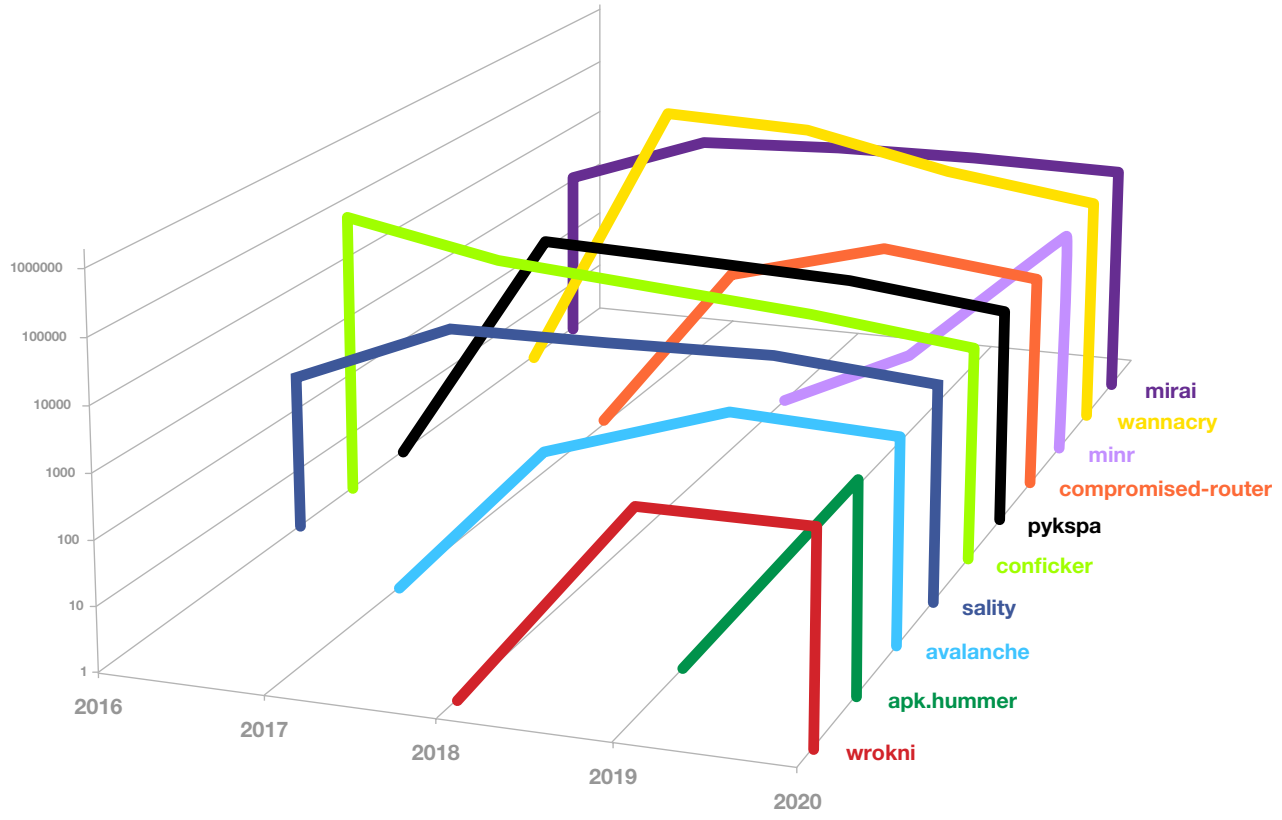


5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gadā ar apdraudējuma veidu – konfigurācijas nepilnība.

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. Neatbilstošas konfigurācijas rezultātā bieži SSDP funkcionalitāte lietotājam nemaz nav pieejama, vienlaicīgi padarot iekārtu par spēcīgu ieroci uzbrucēju rokās.



6. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ar 2020. gadā izplatītākajām konfigurācijas nepilnībām.



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ar 2020. gadā izplatītākajām ļaunatūrām.

Openrdp ievainojamība, kas konfigurācijas nepilnību jeb ievainojamību topā (3. attēls) ieņem piekto vietu, norāda uz aktivizētu attālināto piekļuvi jeb *RDP (Remote Desktop Protocol)*, kas pieejama no publiskā tīkla un rada apdraudējumu, ja tiek izmantota pārāk vienkārša parole un netiek ierobežota piekļuve, piemēram, izmantojot privāto savienojumu jeb VPN. Uzbrucēji var izmantot nepietiekami aizsargātu RDP piekļuvi, lai iekļūtu sistēmā, izgūtu datus vai pieprasītu izpirkuma maksu par bojātu datu atgūšanu.

Palūkojoties uz 2020. gada 10 izplatītākajām konfigurācijas nepilnībām un ļaunatūrām, var novērot, ka pārskata periodā izplatītākās konfigurācijas nepilnības ir bijušas klātesošas un ar gana plašu izplatību pēdējo piecu gadu periodā[1] (6. attēls), atšķirībā no 2020. gadā izplatītākajām ļaunatūrām, no kurām lielākā daļa pirms pieciem gadiem nemaz nepastāvēja, bet 3 no pārskata periodā izplatītākajām ļaunatūrām ir nonākušas Latvijas kibervidē tikai pirms pāris gadiem (7. attēls). Tas ļauj secināt, ka iekārtu īpašnieki ilglaicīgi nepievērš pienācīgu uzmanību savu iekārtu aizsardzībai, nenovēršot konfigurācijas nepilnības, kas pakļauj iekārtas uzbrukumu riskam, savukārt uzbrucēji cenšas pilnveidot uzbrukumu metodes un radīt arvien jaunas ļaunatūras, lai spētu kompromitēt pēc iespējas vairāk iekārtu.

CERT.LV sadarbībā ar interneta pakalpojumu sniedzējiem veica regulāru ievainojamo iekārtu uzturētāju informēšanu *Atbildīgs interneta pakalpojumu sniedzējs* iniciatīvas ietvaros, skaidrojot potenciālo apdraudējumu ietekmi un sniedzot rekomendācijas apdraudējuma novēršanai, taču daļa lietotāju, saņemot paziņojumu no sava pakalpojumu sniedzēja par apdraudējumu iekārtai, diemžēl, bieži vien izvēlas šo paziņojumu ignorēt.

[1] Par konfigurācijas nepilnībām *OpenSMB*, *OpenRDP*, *Accessible-ftp* un *accessiblevnc* ir nepietiekami dati par 2016. gada periodu.

2.

Nozīmīgākie incidenti 2020. gadā

Pārskata periodā CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā. Ik mēnesi apkopojumu par būtiskākajiem incidentiem CERT.LV publicē savā vietnē sadaļā *Kiberlaikapstākļi*. Tā, izmantojot laika ziņām ierasto simboliku, vienkāršā veidā iespējams atskatīties uz iepriekšējā mēnesī notikušo.

Šeit apkopoti nozīmīgākie incidenti, kas iezīmē gada tendences.

2.1. Piekļuves lieguma uzbrukumi (DoS un DDoS)

Pandēmijas ietekmē pastiprinātu noslodzi piedzīvoja vairākas populāras tīmekļa vietnes: www.spkc.gov.lv, www.e-klase.lv, www.eveseliba.gov.lv un citas kā arī www.latvija.lv lietotāju autentifikācijas modulis. Visi darbības traucējumi bija leģitīmi, proti, netika konstatētas ārējas ietekmes.

No septembra gan Latvijā, gan citviet Eiropā kļuva aktuāli naudas izspiešanas mēģinājumi, kas primāri tika vērsti pret finanšu institūcijām kā arī citiem privātā sektora uzņēmumiem. Uzbrucēji draudot apturēt uzņēmuma tīmekļa vietnes vai citu resursu darbību ar uzbrukumu līdz pat 2 Tb/s, ja netiks veikta izpirkuma samaksa, īstenoja testa uzbrukumu sērijas. Lai arī īslaicīgi (atsevišķos gadījumos vairākas dienas, bet visbiežāk mazāk par stundu), tie izcēlās ar lielo apjomu – līdz 180 Gb/s. Uzbrukumu rezultātā atsevišķu uzņēmumu resursi / pakalpojumi vairāku stundu garumā bija pieejami ar darbības pārtraukumiem.

CERT.LV publicēja rekomendācijas apdraudējumu novēršanai un aktīvai aizsardzībai pret DoS uzbrukumiem. Svarīgi ir nekomunicēt ar izspiedējiem un neveikt maksājumus, lai neveicinātu šādu uzbrukumu atkārtošanos nākotnē.

2.2. Pikšķerēšana jeb personīgo datu izkrāpšana

Pikšķerēšanas uzbrukumi ir bijuši ļoti aktīvi visa gada garumā. Vairumā gadījumu kampaņas bija vērstas uz e-pasta un *Office 365* piekļuves datu izkrāpšanu, uz banku, starptautisku maksājumu sistēmu, to skaitā *Smart-ID* piekļuves datu iegūšanu un uz populārāko sociālo tīklu – *Facebook*, *Instagram* – piekļuves datu izkrāpšanu. Lietotāju uzmanības piesaistīšanai krāpnieciskajos e-pastos un sociālo tīklu paziņojumos periodiski tika izmantota COVID-19 tematika.

Pandēmijas periodā tika novēroti pastiprināti datu izkrāpšanas mēģinājumi, izmantojot sūtījumu piegādes pakalpojumu sniedzēju zīmolus, piemēram, *Latvijas Pasts*, *DHL*, *Omniva*, *DPD*, *AliExpress* u.c. Šīs pikšķerēšanas kampaņas, tāpat kā citus gadus īpaši pastiprinājās pirmssvētku periodā gada nogalē.

Augustā tika saņemta informācija par inovatīviem uzbrukumiem *Office 365* piekļuves tiesību izkrāpšanai. Uzbrukums bija grūti pamanāms ar tehniskiem līdzekļiem, jo netika veiktas ļaundabīgas darbības upura iekārtā, bet uzbrukums tika realizēts pašā *Office 365* vidē, izmantojot *Microsoft* aplikāciju veikalā *Azure* izveidotu krāpniecisku lietotni.

Visa pārskata perioda garumā CERT.LV, redzot aktīvas pikšķerēšanas kampaņas, izplatīja informatīvus materiālus un brīdināja konkrēto pakalpojumu lietotājus būt īpaši vērīgiem un uzmanīgiem, kā arī aicināja papildu drošībai uzstādīt un izmantot divu faktoru autentifikāciju, kur vien tas ir iespējams, lai būtiski apgrūtinātu uzbrucēju piekļuvi lietotāju datiem, pat ja viņu rokās būtu nonākušas lietotāju izmantotās paroles.

2.3. Krāpšana

Krāpniecības ziņā 2020. gads ir bijis ļoti aktīvs un piesātināts, Latvijas interneta lietotājiem periodiski nācās izturēt aktīvus krāpniecības mēģinājumus, sākot ar izspiešanas kampaņām, kurās

uzbrucēji apgalvoja, ka viņiem izdevies uzlauzt lietotāja ierīci un iegūt kompromitējošus materiālus, par kuru neizplatīšanu tika pieprasīta izpirkuma maksa, līdz zināmu uzņēmumu vārdā izplatītām krāpnieciskām loterijām, kurās piedāvāts laimēt jaunākos viedtālruņu modeļus vai iegūt citas vērtīgas balvas.

Tika novērota jauna tendence – izspiešanas e-pasti ar draudiem nopludināt datus tika izplatīti arī uzņēmumiem. Šajos e-pastos uzbrucēji apgalvoja, ka uzlauzuši uzņēmuma tīmekļa vietni un ieguvuši klientu datus, par kuru nepublicēšanu pieprasīja izpirkuma maksu.

Turpinājās maldinošas reklāmas sociālajos tīklos. Reklāmās, nesakcionēti izmantojot Latvijā pazīstamu personu vārdus, interneta lietotāji tika aicināti ieguldīt naudu kriptovalūtā. Krāpnieki aktīvi veica arī telefona zvanus un centās pārliecināt iedzīvotājus veikt investīcijas. Atsevišķos gadījumos tika novēroti atkātoti krāpniecības mēģinājumi, kuros tika uzrunāti finanšu krāpniecībās cietušie upuri, un tiem, šķietami, piedāvāts palīdzēt atgūt zaudētos līdzekļus. CERT.LV zināms par kādu Latvijas iedzīvotāju, kurš sekojot krāpnieku ieteikumiem un iemaksājot naudu nelicencētā finanšu platformā, zaudēja 60 000 eiro, un vēl 10 000 eiro atkārtotā krāpniecībā, mēģinot līdzekļus atgūt.

CERT.LV aicināja iedzīvotājus neiesaistīties piedāvātajos darījumos un telefona sarunu pēc iespējas ātrāk pārtraukt, zvanītāju bloķēt savā iekārtā, kā arī informēt savu mobilo sakaru operatoru. Informācija par Latvijā licencētiem finanšu pakalpojumu sniedzējiem pieejama *Finanšu un kapitāla tirgus komisijas* tīmekļa vietnē www.fktk.lv.

Viltojot dažādu kredītiestāžu telefona numurus un uzdodoties par banku vai *Smart-ID* darbiniekiem, krāpnieki, izmantojot iedzīvotāju vājās zināšanas par papildu autentifikācijas līdzekļu darbību, nozaga finanšu līdzekļus no vairākiem tūkstošiem lietotāju, radot Latvijas kredītiestādēm kopējos zaudējumus vairākus simtu tūkstošu apmērā. Bankas un CERT.LV atgādināja, ka bankas nekad nezvanīs un nelūgs nosaukt savu lietotājvārdu, paroli, vai *Smart-ID* kodus.

Uzbrucēji pielāgoja savus uzbrukumus uzņēmumu un iestāžu nepieciešamībai pāriet uz attālināto darbu un steidzami uzsākt dokumentu apriti elektroniski, kas pieļautu novirzes no iepriekš apstiprinātām normām. Virkne uzņēmumu grāmatvežu saņēma e-pastus vadītāja vai citu

darbinieku vārdā ar aicinājumu veikt steidzamu maksājumu vai mainīt algas izmaksas kontus. Vairākos gadījumos uzbrukumi ir bijuši veiksmīgi, dažos no tiem krāpniecība operatīvi atpazīta un finanšu līdzekļus izdevās atgūt.

Tika saņemti ziņojumi no uzņēmumiem arī par iejaukšanos biznesa sarakstē. Kompromitējot uzņēmuma vai tā sadarbības partnera e-pasta kastīti un sekojot sarakstei, uzbrucēji atbilstošajā brīdī vienai no pusēm nosūtīja rēķinu ar mainītu bankas kontu. Vairumā gadījumu krāpniecība tika atpazīta, taču zināms par vismaz diviem gadījumiem, kad maksājums uz krāpnieku norādīto kontu tika veikts un līdzekļi zaudēti.

Iedzīvotājos satraukumu radīja īsziņas ar saišu saīsinātāju (ej.uz), kuras izsūtīja valsts iestādes, veicot iedzīvotāju apziņošanu par ārkārtas stāvokli un epidemioloģisko situāciju valstī. Saišu saīsinātājus bieži vien izmanto arī krāpnieciskos paziņojumos, kad krāpnieki cenšas noslēpt patieso saites galamērķi. CERT.LV vērsa uzmanību uz nepieciešamību savlaicīgai izvietot informāciju attiecīgo iestāžu tīmekļa vietnēs un sociālo tīklu profilos, tajā skaitā arī par paredzamo informācijas izplatīšanu un metodēm, lai izvairītos no pārpratumiem.

Gada nogalē neizpalika viltus interneta veikali. Lai arī tie pastāv visa gada garumā, pirmssvētku periodā šādu veikalu skaits un to aktivitāte būtiski pieaug, piemēram, izvietojot reklāmas sociālajos tīklos. Tā tiek pievilināti arvien jauni potenciālie iepirkties gribētāji un palielinās krāpnieku peļņas iespējas.

2.4. Ielaušanās mēģinājumi

Informācija par ielaušanās mēģinājumiem tika saņemta visa gada garumā, taču pietiekami zemā intensitātē. Ielaušanās mēģinājumi notika gan pret valsts un pašvaldību iestāžu serveriem no citām valstīm, gan arī tika konstatēti automatizēti uzbrukumi citu valstu iestāžu serveriem no Latvijas IP adresēm.

Līdz ar organizāciju pārslēgšanos attālinātā darba režīmā, tika novērota palielināta botu aktivitāte, kas meklē ievainojamas, neatbilstoši konfigurētas un/vai ar vājām parolēm aizsargātas tīmeklī pieslēgtas iekārtas. Kā iespējamie mērķi šiem botiem bija darba devēja steigā izsniegtas, nepietiekami droši konfigurētas iekārtas vai personīgie datori, kuri pēkšņi tiek izmantoti darbam, kā arī attālinātās piekļuves pakalpojumi (RDP) ar vāju paroli un nepietiekamu papildu aizsardzību.

Ielaušanās mēģinājumu īstenošanas metodes ir bijušas atšķirīgas. Kā rāda CERT.LV novērojumi, tad populārākās uzbrucēju izvēlētās metodes iekļāva paroļu minēšanu, izmantojot Internet *Message Access Protocol (IMAP)* servisu un datu izgūšanas mēģinājumus, izmantojot SQL injekcijas.

2.5. Ļaunatūra

Ļaunatūra arī 2020. gadā tika izplatīta galvenokārt diviem mērķiem – lai iegūtu informāciju vai gūtu peļņu. Informācijas gūšanai tika izplatīta spiegojošā ļaunatūra, kas nosūtīja upura iekārtā iegūtos datus, piemēram, paroles, uzbrucējam. Peļņas gūšanai tika izplatīti šifrējošie izspiedējvīrusi, kuru uzbrukuma rezultātā dati upura iekārtā tika nošifrēti un datu atgūšanai tika pieprasīta izpirkuma maksa. Tās lielums bija atkarīgs gan no šifrētās iekārtas, gan cietušā, gan šifrēto datu apjoma – jo svarīgāki dati, jo augstāka cena. Cietušo vidū bija vairāki uzņēmumi, valsts un pašvaldību iestādes, kā arī kāda veselības aprūpes iestāde.

CERT.LV atgādināja ka, ja vien iespējams, izpirkuma maksu nemaksāt! Maksāšana negarantē datu atgūšanu, kā arī veicina šādu ļaundabīgu praksi un kalpo kā rādītājs, ka upuris ir gatavs maksāt, kas var novest pie atkārtotiem uzbrukumiem.

Virkne ļaunatūras izplatīšanas mēģinājumu tika veikti COVID-19 piesegā:

- Izsūtīti e-pasti, šķietami, *Pasaules Veselības organizācijas* vārdā, norādot, ka pielikumā pievienota jaunākā informācija par COVID-19.

- Publicējot saites uz COVID-19 izplatību attēlojošu lietotni, kuras funkcionalitāte paredzēja lietotāju datu izgūšanu.
- Veselības aprūpes iestādēm tika izplatīti ļaundabīgi e-pasti par COVID-19 aizsarglīdzekļu piegādi u.c.

2020. gada otrajā pusē bija vērojama strauja ļaunatūras *Emotet* izplatība gan globālajā, gan Latvijas tīmeklī. *Emotet* upura iekārtā parasti nonāca no kādas jau inficētas kontaktpersonas e-pasta. Ļaunatūra paredzēta sensitīvas informācijas iegūšanai. Saņēmēju maldināšanai un uzticamības palielināšanai *Emotet* saturošie e-pasti ietvēra arī fragmentus no iepriekšējām sarakstēm, kas aicināja domāt, ka saņemtais e-pasts ir uzsāktas sarakstes turpinājums. Latvijā tika inficētas vairāk nekā 200 organizācijas. Ir paredzams, ka pēc kāda laika uzbrukumos iegūtā informācija var tikt izmantota atkārtotos uzbrukumos vai citās mērķētās ļaundabīgās kampaņās.

Ļaunatūras izplatīšanai, galvenokārt, tika izmantoti e-pasti, kuri saturēja inficētus pielikumus. Šifrējošie izspiedējvīrusi atsevišķos gadījumospārsvarā gadījumu sistēmā nonāca, uzbrucējiem uzminot vājas izmantojot nepietiekami aizsargātu attālinātās piekļuves pakalpojumapakalpojumu (RDP). Uzbrucēji uzminēja vājas paroles vai piemeklēja paroles, izmantojot citos uzbrukumos vai datu noplūdēs iegūtas datubāzes.

2.6. Kompromitētas iekārtas un datu noplūdes

Iekārtu kompromitēšanas gadījumi skāra gan privātpersonas, gan uzņēmumus, gan arī valsts un pašvaldību iestādes. Kā uzbrukuma vektors tika izmantoti jau kompromitēti e-pastu konti un organizāciju darbinieki savas iekārtas inficēja, atverot e-pastu pielikumus vai saites no šķietami zināmiem kontaktiem e-pasta adrešu grāmatiņā – kolēģiem un sadarbības partneriem. Darbību mērķis – iegūt e-pastu piekļuves un citu sensitīvu informāciju.

CERT.LV kā galveno aizsardzības mehānismu ieteica iestatīt divu faktoru autentifikāciju arī e-pastu, tajā skaitā *Microsoft*, kontu aizsardzībai.

Kompromitēto tīmekļa vietņu gadījumā uzbrukuma vektors bieži vien bija novecojis spraudnis vai neatjaunināta satura vadības sistēma. Vairumā gadījumu kompromitētajās vietnēs tika ievietots kaitīgs kods lietotāju pārvirzīšanai uz kaitīgo vietni, taču dažos gadījumos bija notikusi arī datu noplūde. Tas vēlreiz apliecina nepieciešamību paredzēt gan resursus, gan finansējumu sistēmas uzturēšanai un atjaunināšanai, kā arī sekot līdzi pieejamajiem atjauninājumiem un tos laicīgi uzstādīt.

Vairākas valsts iestādes uz laiku zaudēja piekļuvi saviem sociālo tīklu kontiem, uzbrucējiem pārņemot kontroli pār kādu no konta administratoru profiliem. Nevienā no gadījumiem papildu drošībai netika izmantota divu faktoru autentifikācija, kas būtu apgrūtinājusi kontu pārņemšanu. Tika saņemti ziņojumi par ielaušanos *Zoom*, *MS Teams* un citu platformu sanāksmēs. Taču, iepazīstoties ar situāciju, nācās konstatēt, ka sanāksmju organizētāji nav izmantojuši pieejamos aizsargmehānismus (uzgaidāmā telpa, ierobežotas iespējas pievienoties no ārzemēm u.c.), lai novērstu nepiederošu personu dalību sanāksmē.

Novembrī Latvijas medijos plašu rezonansi ieguva ziņa par datu noplūdi no Ķīnas uzņēmuma *Zhenhua Data*, kas skārusi aptuveni 2,4 miljonus iedzīvotāju visā pasaulē. To vidū bija atrodama arī informācija par 480 iedzīvotājiem no Latvijas. Nopludinātie dati liecināja, ka uzņēmums par personām vācis publiski pieejamu informāciju – no medijiem, sociālajiem tīkliem utt. Informācijas vākšanai izmantotas speciāli tam izstrādātas programmas.

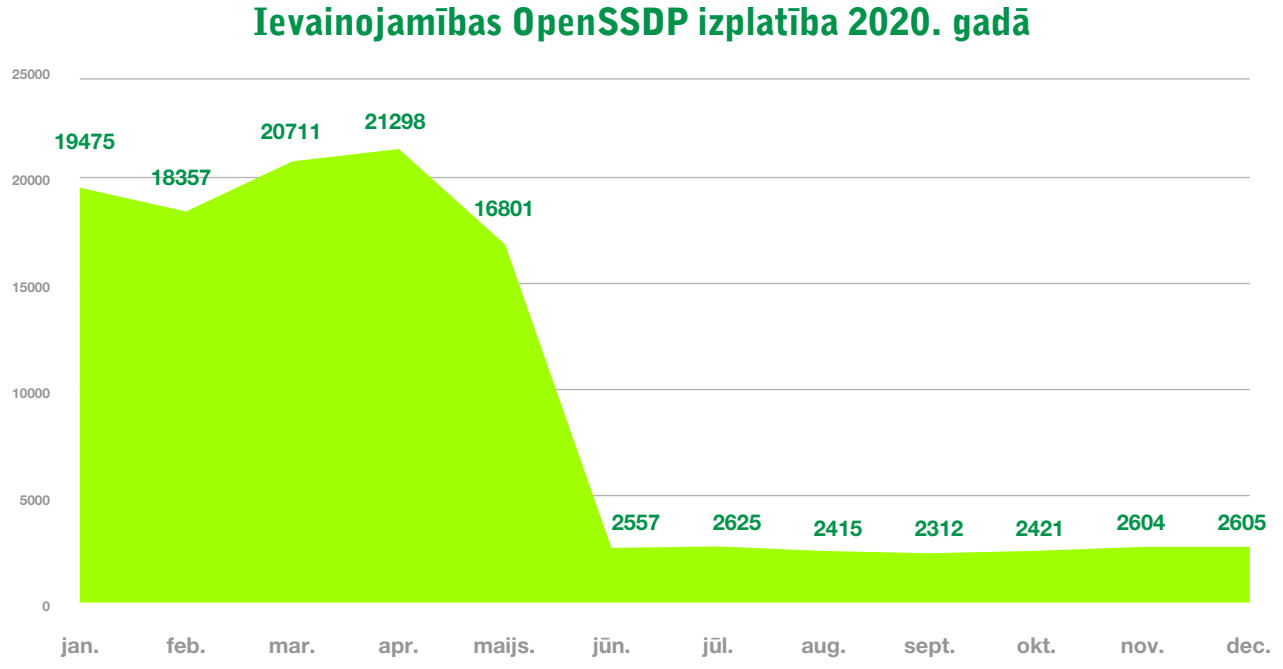
2.7. Ievainojamības un konfigurācijas nepilnības

Pārskata periods izcēlās ar kritisku ievainojamību (*Windows DNS: CVE-2020-1350*, *SMB: CVE-2020-0796*, *Windows Server: CVE-2020-1472*, *SAP: CVE-2020-6287* u.c.) atklāšanas apjomu. Ievainojamības vai nu sniedza uzbrucējiem iespēju veikt attālinātu patvaļīga koda izpildi mērķa iekārtā, vai arī iespēju izgūt sensitīvu informāciju no mērķa sistēmas. Dažas no šīm ievainojamībām tika aktīvi izmantotas uzbrukumos pirms ražotāji bija paguvuši publicēt atjauninājumus ievainojamību novēršanai. Tas nodrošināja šīm ievainojamībām *nulles dienas (zero day)* ievainojamību statusu.

CERT.LV veica potenciāli ievainojamo sistēmu apzināšanu valsts sektorā, informēja sistēmu uzturētājus, sniedza ieteikumus ievainojamību novēršanā un atbalstu incidentu risināšanā.

Tika saņemti ziņojumi par vairāku uzņēmumu un iestāžu tīmekļa vietnēm, kuras neatbilstošas konfigurācijas rezultātā bija pakļautas personas datu izgūšanas uzbrukumiem. CERT.LV informēja resursu uzturētājus un koordinēja ievainojamību novēršanu.

2020. gada sākumā ik mēnesi tika reģistrētas vidēji 20 000 unikālas IP adreses ar konfigurācijas nepilnību *OpenSSDP (Open Simple Service Discovery Protocol)*, kuras pakļautas izmantošanas riskam DoS uzbrukumos. Daļa no neatbilstoši konfigurētajām iekārtām bija viedie televizori. Maijā CERT.LV aicināja interneta pakalpojumu sniedzējus (IPS) ne tikai informēt klientus par nekorekti pieslēgtām UpnP *(Universal Plug and Play)* iekārtām, jo UPnP tehnoloģija ir paredzēta



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gadā ar ievainojamību OpenSSDP.

lietošanai tikai iekšējā tīklā, bet arī rekomendēja tīkla līmenī ierobežot piekļuvi SSDP servisam, kas tiek izmantots UPnP funkcijas nodrošināšanai, bloķējot UDP1900 portu vai centralizēti izslēdzot UPnP funkcionalitāti vadāmajās klientu interneta piekļuves iekārtās. Sākot no jūnija, vidējais mēnesī reģistrētais unikālo IP adrešu daudzums ar konfigurācijas nepilnību *OpenSSDP* bija 2500 IP adreses – samazinājums par 87,5% (8. attēls).

CERT.LV veica pašvaldību un valsts iestāžu e-pasta iestatījumu pārbaudes, lai konstatētu to atbilstību MK noteikumiem Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām*. Prasības paredz *DMARC (Domain-based Message Authentication, Reporting & Conformance)* protokola izmantošanu. Pārbaužu rezultātā tika atklāts, ka tikai viena trešā daļa no pārbaudītajiem resursiem atbilda noteiktajām prasībām, jo tika konstatēta atbilstošo tehnoloģiju izmantošana, tomēr jāuzsver, ka šāda veida pārbaudēs nav iespējams pilnībā pārliecināties, vai tehnoloģijas ieviestas korekti.

Par visām ievērojamākajām ievainojamībām, tajā skaitā *receptēm*, kā tās ārstēt, CERT.LV ar interneta pakalpojumu sniedzēju starpniecību regulāri informēja interneta lietotājus. *Receptes* pieejamas: https://www.esidross.lv/informacija-par-apdraudejumiem/

3!

Atbildīga ievainojamību atklāšana

CERT.LV atbalsta atbildīgas IT drošības nepilnību atklāšanas labo praksi, un aicina drošības pētniekus ziņot CERT.LV par ievainojamībām, lai CERT.LV varētu aktīvi koordinēt ievainojamību novēršanu, tā labāk pasargājot Latvijas interneta telpu.

Pārskata periodā CERT.LV saņēma vairākus ziņojumus, kas informēja par atklātām ievainojamībām dažādos valsts un pašvaldību iestāžu resursos. Pateicoties šiem ziņojumiem, vairākas valsts iestāžu tīmekļa vietnes tika pasargātas galvenokārt no starpvietņu skriptēšanas (XSS) uzbrukumiem, kuri veiksmīgas izpildes gadījumā sniegtu uzbrucējam iespēju veikt darbības lietotāja pārlūkā, piemēram, manipulēt ar vietnes saturu un sīkdatnēm vai izmantot pārlūkam piemērotus mūķus (*exploits*). Vienā no gadījumiem tika konstatēts, ka, veicot ievainojamību novēršanu, izstrādātāji radīja jaunas nepilnības, kas ietekmēja resursa funkcionalitāti un drošību. Ievainojamību atklāšanai un novēršanai resursam tika veikts papildu drošības audits.

No drošības pētnieka Oskara Veģera tika saņemta informācija par jaunatklātu nulles dienas (*zeroday*) ievainojamību *MS Teams* platformā. Ievainojamība sniedza uzbrucējam iespēju pārņemt visu infrastruktūru un *Office 365* kontus, veicot attālinātu koda izpildi (remote code execution). Uzbrukuma realizācijai nebija nepieciešama lietotāja iesaiste (*zero-click*), vien atbilstoši sagatavota ziņojuma nosūtīšana lietotājam. Šāda līmeņa atklājums tikai vēlreiz apliecina augsto mūsu speciālistu augsto zināšanu un sagatavotības līmeni ar ko noteikti ir vērts lepoties!

Arī 2021. gadā CERT.LV aicina ziņot par atklātām ievainojamībām, rakstot uz cert@cert.lv, vairāk par atbildīgu ievainojamību atklāšanu CERT.LV tīmekļa vietnē www.cert.lv/lv/par-mums/atbildiga-ievainojamibu-atklasana.

4.

Ielaušanās testi

Ielaušanās testi ir nozīmīgs solis, lai nodrošinātu un pārliecinātos, ka izveidotais tiešsaistes resurss – sistēma, datubāze, tīmekļa vietne u.c. – atbilst noteiktajām drošības prasībām un labajai praksei. CERT.LV speciālisti gada laikā veica vairākus ielaušanās testus dažādiem valsts nozīmes informācijas resursiem, dažos gadījumos darot to atkārtoti. Daļā gadījumu tika atklātas būtiskas nepilnības, taču dažos no testiem tika konstatēts, ka sistēmas izstrādātas atbilstoši drošības prasībām un drošības nepilnības netika konstatētas vai arī tika konstatētas nebūtiskas, viegli novēršamas nepilnības. Informācijas sistēmu uzturētājiem CERT.LV sagatavoja pārskatu par veiktajiem testiem un to rezultātiem, kā arī sniedza ieteikumus nepilnību novēršanai.

Atsevišķos gadījumos tika konstatēts, ka sistēmā tiek izmantotas novecojušas, apdraudētas tehnoloģijas, kurām ražotājs vairs nenodrošina tehnisko atbalstu un atjauninājumus. Drošības prasību ilgtermiņa ievērošana tiek apgrūtināta, ja resursi un finansējums tiek paredzēti tikai projekta izstrādei, bet netiek paredzēti projekta tālākai uzturēšanai un atbilstoša drošības līmeņa nodrošināšanai visā projekta vai resursa dzīves laikā.

5.

Informatīvie komunikācijas pasākumi


15° SALDUS
IZGLĪTOTS DARBINIEKS - LABĀKAIS PRETTRIECIENS KIBERUZBRUKUMIEM REĀLAJĀ DZĪVĒ
PANORĀMA
7:25


.LV


CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija
Gints Mālkalnietis
CERT.LV KIBERDROŠĪBAS EKSPERTS


KĀ SARGĀJAM LATVIJU?
Latvijā kiberuzbrukumi uzņēmumiem tiek konstatēti ik dienu


FINANŠU
NOZARES
ASOCIĀCIJA
mastercard
viedpircējs


Baiba Kaskina
zoom

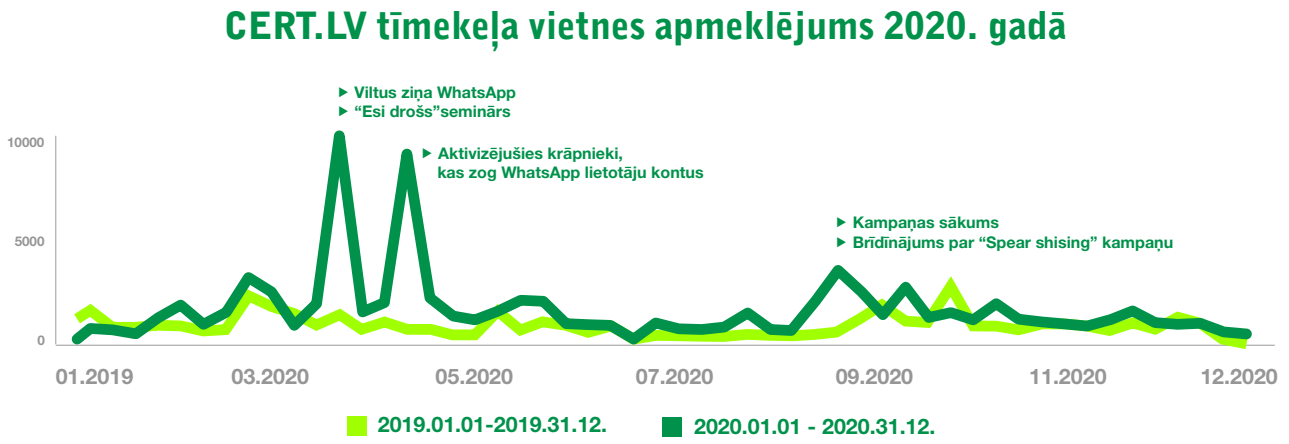

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija


KĀ SARGĀJAM LATVIJU?
Latvijā kiberuzbrukumi uzņēmumiem tiek konstatēti ik dienu

CERT.LV ekspertu viedoklis 2020. gadā ir bijis īpaši svarīgs – sniegtas intervijas un atbildes uz mediju jautājumiem gan TV, gan radio par dažādām aktuālām ar kiberdrošību saistītām tēmām. Kopā CERT.LV izskanējis vairāk nekā 422 TV, radio, portālu un drukāto mediju publikācijās gan latviešu, gan krievu valodā.

Pārskata periodā mediju interesi īpaši piesaistīja ar pandēmiju saistīti kiberuzbrukumi, datu vākšanas kampaņas (pikšķerēšana), krāpnieciskas loterijas, telefonkrāpnieku zvani banku vārdā. CERT.LV ekspertu viedoklis visaktīvāk – 49.3% no visām publikācijām – ir pausts interneta portālos, 30.6% – radio, 11.1% – TV un 9.0% – drukātajos izdevumos. Aptuveni sasniegtais Latvijas iedzīvotāju skaits pārsniedz 1.2 miljonus.

CERT.LV uztur tīmekļa vietni www.cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. 2020. gadā vietnē publicētas 104 ziņas, no kurām ikmēneša, ceturkšņa un gada pārskati un ziņas ir 32.7%, savukārt brīdinājumi par krāpniecībām un ļaunatūrām – 28.8%, informatīvi paziņojumi – 16.3%, ieteikumi rīcībai – 15.4% un vien 6.7% par rīkotajiem pasākumiem. Kopā gada laikā CERT.LV vietnei bijuši 108 007 unikāli apmeklējumi jeb sesijas, kurus veikuši 70 935 lietotāji.



9. attēls – CERT.LV tīmekļa vietnes apmeklējums 2020. gadā.

CERT.LV uztur arī lietotāju izglītošanas portālu www.esidross.lv, regulāri publicējot jaunus rakstus ar padomiem un ieteikumiem, kā lietotājiem drošāk darboties virtuālajā vidē. Pārskata periodā svarīgs informācijas komunikācijas pasākums bija sabiedrību izglītojoši informatīvā kampaņa Kiberdrošība darbavietā (14.09.-11.10.). Tās ietvaros portāls www.esidross.lv piedzīvoja vizuālas izmaiņas, lai lietotājiem būtu ērtāk to lietot. Kampaņas laikā sabiedrība tika iepazīstināta ar jaunvārdiem parolīze, muļķerēšana un spaidonis ar īpašu video, reklāmas un rakstu palīdzību.

Kopumā tika sasniegti vairāk nekā 500 tūkstoši Latvijas interneta lietotāji. Kampaņas materiālos CERT.LV eksperti sniedza padomus, kā veidot noturīgus un efektīvus kiberdrošības paradumus, kā vislabāk rūpēties par savu iekārtu drošību, kā veidot efektīvas paroles un atcerēties tās. Kampaņas video materiālu kopējais skatījumu skaits platformā *YouTube* sasniedza 427 tūkstošus, gandrīz 400 dalībnieki savas jauniegūtās zināšanas nolēma pārbaudīt arī praktiski, atbildot uz ākļīgiem jautājumiem kampaņas digitālajā rokasgrāmatā – rokasgramata.esidross.lv.

Visi kampaņas materiāli arī turpmāk būs pieejami vietnē www.esidross.lv.

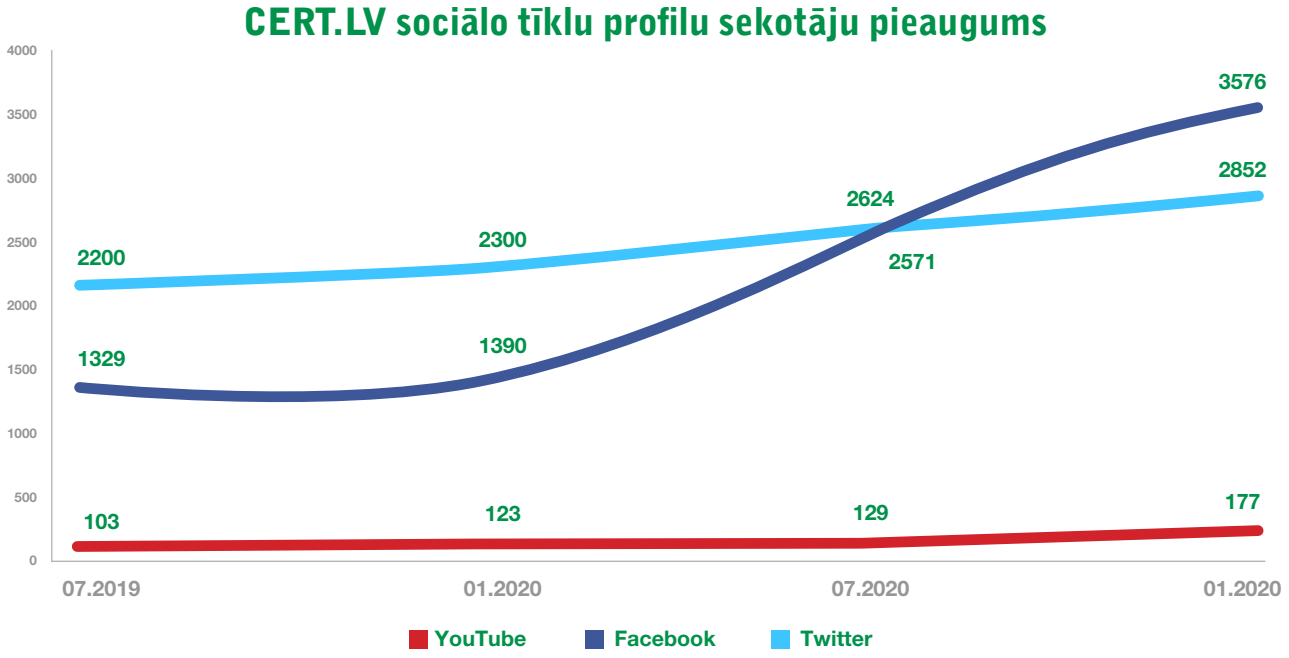
Lai atvieglotu iniciatīvas *Atbildīgs interneta pakalpojumu sniedzējs* dalībnieku saziņu ar gala lietotājiem par viņu iekārtās konstatētajiem apdraudējumiem, kā arī sniegtu lietotājiem iespēju jebkurā laikā iepazīties ar informāciju par dažādiem apdraudējumiem, to ietekmi un novēršanas iespējām, CERT.LV tīmekļa vietnē esidross.lv publicēja aktīvo apdraudējumu aprakstus www.esidross.lv/informacija-par-apdraudejumiem/.

Pārskata periodā katru mēnesi sadarbībā ar SANS institūtu tika izdoti un publicēti vietnē www.cert.lv un portālā www.esidross.lv informatīvie kiberdrošības biļeteni OUCH!. Tajos starptautiski atzīti kiberdrošības speciālisti ikvienam interneta lietotājam saprotamā veidā sniedz komentārus par aktuālajiem kiberapdraudējumiem un praktiskus ieteikumus individuālās kiberdrošības uzlabošanai. Arī 2021. gadā CERT.LV turpinās nodrošināt šo ikmēneša biļetenu pieejamību Latvijas interneta lietotājiem. Ikdienas komunikācijā arvien lielāku nozīmi ieņem CERT.LV izmantotās sociālo tīklu platformas – *Facebook*, *Twitter* un arī *YouTube*.

CERT.LV kiberdrošības ekspertu viedokļiem, brīdinājumiem un ieteikumiem:

- *Twitter* kontā twitter.com/certlv seko 2852, vidēji vienai CERT.LV ziņai sasniedzot 2 000 *Twitter* lietotāju.
- *Facebook* profilā facebook.com/certlv – 3576, vidēji vienai CERT.LV ziņai sasniedzot 11 000 *Facebook* lietotāju.
- *YouTube* kanālā – 177 sekotāju.

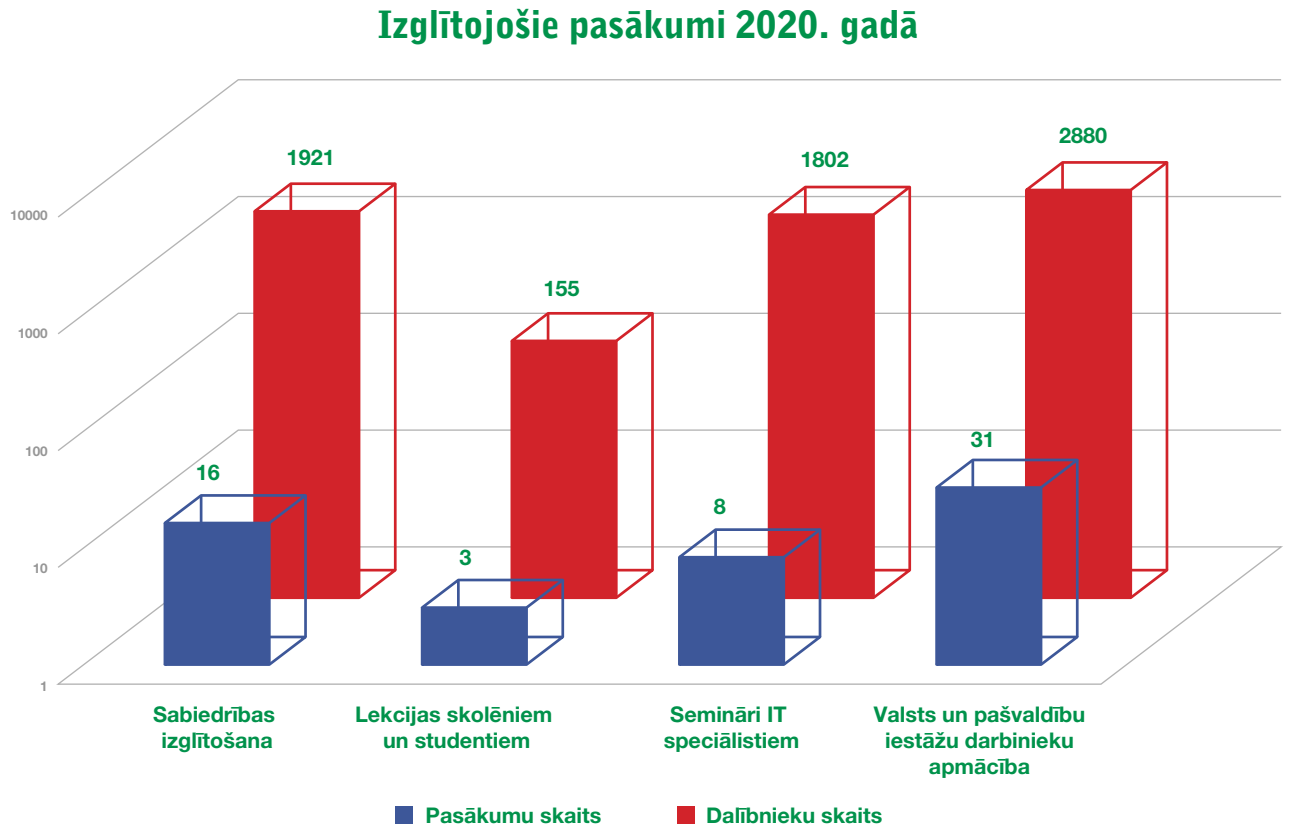
Pandēmijas iespaidā bija vērojams būtisks sekotāju skaita pieaugums CERT.LV sociālo tīklu profiliem – *Facebook* par 63.5%, bet *Twitter* – 19.3%. Tas nozīmīgi palielināja CERT.LV ziņu sasniedzamo auditoriju salīdzinājumā ar iepriekšējo gadu, tā nodrošinot lielāku Latvijas sabiedrības daļas informētību par aktuālajiem notikumiem valsts kibertelpā.



10. attēls – CERT.LV sociālo tīklu profilu popularitāte.

6. Izglītojošie pasākumi

2020. gadā notikušo pasākumu skaitu būtiski ietekmēja COVID-19 pandēmija un nepieciešamība pasākumus organizēt attālināti. Otrajā un trešajā ceturksnī notikušo pasākumu skaits ir neliels, jo tikai neliela daļa organizatoru un arī dalībnieku bija paguvuši pārorientēties uz pasākumu norisi tiešsaistē. CERT.LV turpināja rīkot izglītojošus pasākumus par kiberdrošības jautājumiem IT drošības speciālistiem, valsts un pašvaldību iestāžu darbiniekiem un sabiedrībai kopumā. Pārskata periodā CERT.LV piedalījās 58 pasākumos un izglītoja 6758 dalībniekus.



11.attēls – Pasākumu un apmācīto cilvēku skaits 2020. gadā.

6.1. Starptautiskā kiberdrošības konference Kiberšoks 2020

Pandēmijas ietekmē tika pieņemts lēmums pārskata periodā neorganizēt ikgadējo starptautisko IT drošības konferenci *Kiberšahs*. Pielāgojoties epidemioloģiskajām prasībām, 1. un 2. oktobrī, uzsākot *Eiropas Kiberdrošības mēnesi*, tiešsaistē notika CERT.LV organizētā tehniskā kiberdrošības konference *Kiberšoks 2020* (https://cybershock.lv/). Tajā ar praktiskiem piemēriem un demonstrācijām tika padziļināti aplūkotas dažādas tehniskas ar kiberdrošību saistītas tēmas, piemēram, šifrējošo izspiedējvīrusu izmantotās metodes aizsardzībai pret atklāšanu, *Yara* rīka izmatošana un digitālo attēlu metadatu analīze. Konferencei pieteicās un to attālināti vēroja 760 dalībnieki; prezentācijas sniedza septiņi lektori no piecām dažādām valstīm. Paralēli konferencei sadarbībā ar *Cybexer Technologies* un *Tet group* norisinājās arī *Capture the Flag (CTF)* sacensības, kurās spēkiem mērojās 100 dalībnieki 29 komandās.


Cyber Stuck
2020
YC520


VBS & VTL
• Virtualization Based Security
• Virtual Trust Levels
• Created via SLAT and Hypervisor
• Used for kernel exploits mitigation
• Partition still same
• Rings still same
• VTL1 > VTL0

Dan Demeter, Cybershock 2020

Copy link

Dan Demeter

Up your Threat Hunting Game using Yara

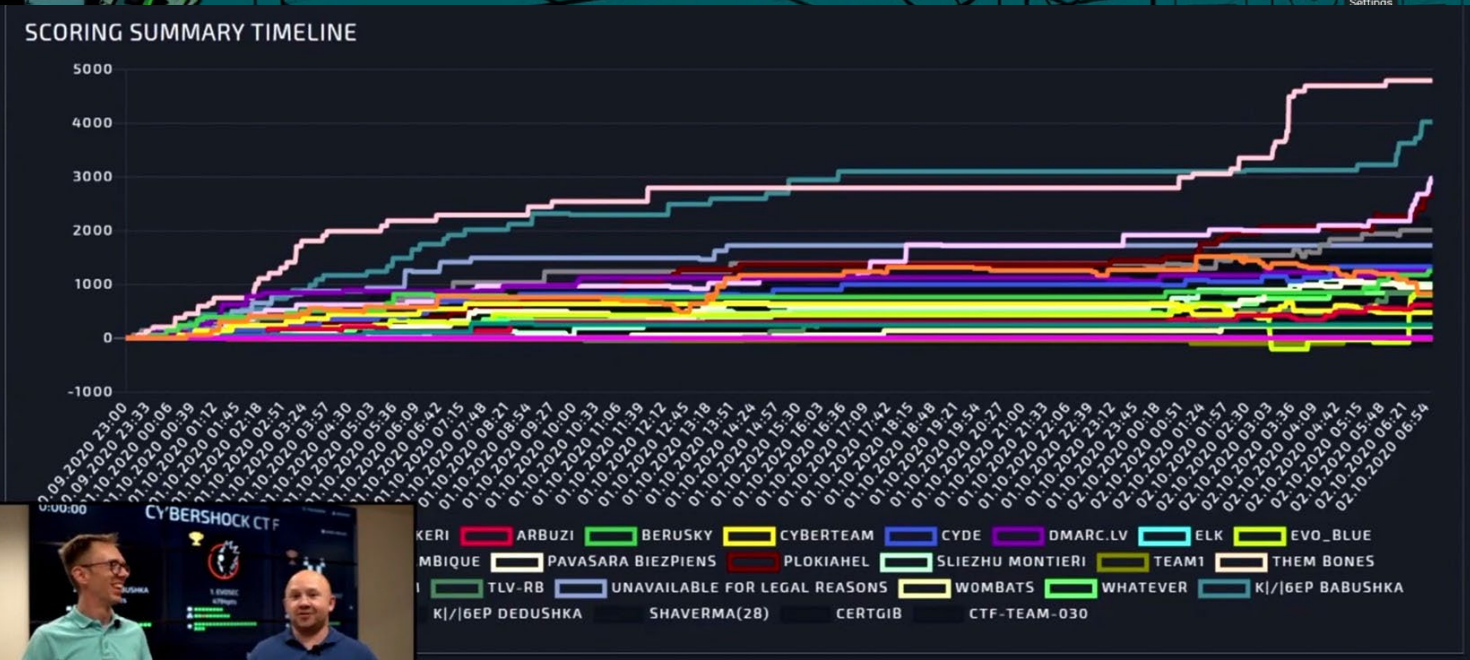
CERT.LV tet CYBEXER TECHNOLOGIES

Co-financed by the Connecting Europe Facility of the European Union

MENTI.COM : 27 53 59 8

MORE VIDEOS

Settings



Dan
@_xdanx

One of the most kick-ass virtual stages I've seen :)

> **CERT** @certlv · Oct 2, 2020
> Ready to start second day of the technical cybersecurity conference CyberShock with @_xdanx @lazyactivist192 @hanskan @bb_certlv Kārlis Apalups and Uldis Lībietis

2:03 PM · Oct 2, 2020 · Twitter for Android

Hans Lõugas @hanskan · 1h
Thanks for the cool shirt, was a great CTF 👏 @certlv @bb_certlv @CybexExchange @ctf_tech

Kelsey Hightower @kelseyhightower · Dec 6
If virtual events are going to become the norm, then I hope a bunch of local studios and sound stages pop up, as I can't be the only one tired of these talking head videos.

31 35 590

Randy Pargman
@rpargman

Replying to @kelseyhightower

Did you happen to see the CyberShock 2020 conf put on by @certlv? That was an outstanding effort with a proper stage setup and good production quality. I'd like to see more great events like that!

2:53 AM · Dec 6, 2020 · Twitter for iPhone

6.2. CERT.LV organizētie pasākumi IT drošības speciālistiem

Papildus starptautiskai kiberdrošības konferencei *Kiberšoks 2020*, kuras galvenā mērķauditorija bija IT drošības speciālisti, tika organizēti vēl divi tematiskie semināri *Esi drošs*. Ik gadu pavasarī un rudenī tie pulcē galvenokārt valsts un pašvaldību iestāžu par IT drošību atbildīgos un citus IT nozares pārstāvjus. Pandēmijas apstākļos *Esi drošs* semināri bija vērojami tiešsaistē. Vidēji semināram ik reizi pieteicās un to vēroja 400 dalībnieki. Prezentācijas un ieraksti pieejami www.cert.lv tīmekļa vietnē.

Martā: Digitālās nedēļas ietvaros organizētajā *Esi drošs* tika aplūkoti dažādi ar attālinātā darba organizēšanu saistīti jautājumi un drošības aspekti.

Decembrī: *Esi drošs* seminārā dalībnieki tika iepazīstināti ar aktuālajiem IT riskiem un kiberdraudiem valsts iestādēm un pašvaldībām, uzticamības pakalpojumu sniedzējiem un elektronisko identitāti, pētījumu par Eiropas komisijas digitālās drošības likumu, *Valsts un pašvaldību vienotā tīmekļa platformas* ieviešanu, rīcību kiberincidenta gadījumā, kā arī ar aktuālajām kiberuzbrukumu kampaņām Latvijā 2020. gadā.

Oktobra vidū CERT.LV organizēja praktiskus seminārus IT drošības speciālistiem *E-pastu sistēmas aizsardzības labā prakse*, sniedzot praktiskas zināšanas par *DMARC* ieviešanas procesu un e-pastu sistēmas drošības auditēšanu. Lielās intereses rezultātā semināri tika organizēti atkārtoti. Semināros kopumā piedalījās 113 informācijas tehnoloģiju drošības speciālisti.

6.3. CERT.LV prezentācijas par IT drošību sabiedrības izglītošanai

Ik gadu CERT.LV veic aktīvu darbu sabiedrības izglītošanai, gan organizējot, gan piedaloties dažādos tematiskos semināros, informējot par aktualitātēm kiberdrošības jomā, kā arī atgādinot par labo praksi sevis un savu iekārtu pasargāšanai.

14. septembrī CERT.LV uzsāka mēnesi ilgu informatīvi izglītojošu kampaņu *Kiberdrošība darbavietā*, lai veicinātu valsts un pašvaldību iestāžu un arī citu darbinieku izpratni par kiberdrošību. Tas tika darīts ar mērķi veicināt darbinieku spēju atpazīt potenciālos kiberuzbrukumus un tos novērst. Kampaņas ietvaros tika izstrādāti 3 informatīvi skaidrojoši videomateriāli par paroļu izmantošanu (https://www.esidross.lv/2020/09/13/apturi-parolizi) datu izkrāpšanas mēģinājumiem (https://www.esidross.lv/2020/09/13/nepaklaujies-mulkeresanai) un citām krāpnieciskām aktivitātēm tiešsaistē (https://www.esidross.lv/2020/09/13/neesi-spaidonis), kā arī apkopoti praktiski padomi kiberdrošības labās prakses ievērošanai, izveidojot Digitālo rokasgrāmatu (https://rokasgramata.esidross.lv/). Atraktīvākai kiberdrošības jautājumu aktualizēšanai tika izmantoti jaunvārdi: *parolīze*, *muļķerēšana* un *spaidonis*. Kampaņas laikā tika sagatavoti arī vairāki tematiski raksti lielākajiem ziņu portāliem un sniegtas intervijas gan TV, gan radio. Kampaņa noritēja ar Eiropas Savienības CEF projekta *Improving Cyber Security Capacities in Latvia* (INEA/CEF/ICT/A2017/1528784) atbalstu.

Kā citi nozīmīgākie pasākumi 2020. gada griezumā jāmin:

30. janvārī dalība ikgadējā *Latvijas atvērto tehnoloģiju asociācijas (LATA)* konferencē, prezentācijā *Atvērto datu iniciatīvas Latvijā un piemēr ipasaulē*, aplūkojot dažādus atvērto datu projektus un aicinot izvērtēt šādu projektu drošības aspektus.

11. februārī dalība projekta *SkeptiCafe* (zinātnes un kritiskās domāšanas popularizēšanas kafejnīca – domubiedru vakars) ietvaros organizētā diskusijā par to *Ko internets tev nestāsta? Jeb indivīda un valsts digitālā drošība*.

11. februārī kopā ar NIC.LV dalība *Rīgas Centrālās bibliotēkas* filiālbibliotēkas *Pūce* organizētā *Drošāka interneta dienas* pasākumā, kurā skolēnus iepazīstināja ar domēnvārdiem, pikšķerēšanu un citiem ar interneta drošu lietošanu saistītiem aspektiem.

26. martā dalība *Eiropas Digitālās nedēļas* ietvaros organizētā attālinātā informatīvā pasākumā *Mazā Kibernakts*, kuru organizēja LVRTC. Arī šis pasākums bija veltīts attālinātā darba jautājumiem un ar to saistītiem izaicinājumiem, ieskaitot dažādus kiberuzbrukumu riskus, dokumentu parakstīšanu un bērnu pieskatīšanu, izmantojot digitālās tehnoloģijas. Pasākumu varēja vērot sociālajā tīklā *Facebook* un vietnē lmt.straume.lv (pieejama caur LMT viedtelevīziju).

29. oktobrī dalība Latvijas Zinātnes padomes (LZP) organizētajā sarunā par datu drošību un aizsardzību – *Kā dzīvot sociālajos tīklos?* Pasākuma mērķis bija dot iespēju dzirdēt atzītu profesionāļu vai zinātnieku viedokļus par sabiedrībā aktuāliem jautājumiem.

11. novembrī dalība *Riga Conference 2020* ietvaros sniegta intervija par personīgās kiberdrošības jautājumiem (https://www.rigaconference.lv/video/).

2. decembrī LIKTA ikgadējās IKT nozares konferences *DIGI–>FIT 2020* ietvaros tika piešķirta IKT nozares prestižākā balva *Platīna pele 2020* arī kategorijā Labākā kiberdrošības iniciatīva. To šogad saņēma *PwC cyber security escape room*, kas kiberdrošības izlaušanās spēles (*escape room*) formā izglīto darbiniekus par kiberdrošību. Kategorijas mērķis ir palielināt kiberdrošības jautājumu nozīmi IKT risinājumu izstrādē, veicinot izpratni par kiberdrošību, kā arī sekmēt inovatīvu risinājumu radīšanu un veicināt to atpazīstamību. Balvas tika pasniegtas vēl 4 kategorijās, kā arī pasniegta viena specbalva. CERT.LV piedalījās balvai *Platīna pele 2020* iesniegto pieteikumu vērtēšanas komisijā.

7.

Stratēģiskā sadarbība Latvijā

CERT.LV darbojas *Informācijas tehnoloģiju drošības likuma* ietvaros, kas ir galvenais kiberdrošības jomu regulējošais likums Latvijā.

Latvijā darbu turpināja **Nacionālā informācijas tehnoloģiju drošības padome**, kuras mērķis ir koordinēt ar informācijas tehnoloģiju drošību saistīto uzdevumu un pasākumu plānošanu un veikšanu Latvijā. Padomes darbā iesaistīti arī pārstāvji no CERT.LV.

CERT.LV cieši sadarbojās ar Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļu, un savas kompetences ietvaros aktīvi piedalījās Nacionālās kiberdrošības stratēģijas īstenošanā. Svarīgākās valsts mēroga aktivitātes 2020. gadā, kurās piedalījās CERT.LV:

- Pētījuma veikšana par populārākajiem attālinātās komunikācijas rīkiem, lai ar detalizētiem rezultātiem iepazīstinātu galvenās sadarbības organizācijas un veicinātu citu sadarbības partneru informētu lēmumu pieņemšanu un atbilstošu IT drošības līmeni. Veicot rīku analīzi, tie tika izvērtēti gan no datu drošības aspekta, gan piedāvātās funkcionalitātes, izcelsmes valsts, konstatētajām ievainojamībām u.c.
- Sagatavotas instrukcijas *MS Exchange* serveru konfigurācijai, kas veicinātu efektīvāku mēstuļu filtrēšanu un potenciāli kaitīgu e-pastu atpazīšanu. Ieteikumi ar Aizsardzības ministrijas starpniecību tika izplatīti arī citām valsts iestādēm.
- CERT.LV sniedza konsultācijas valsts un pašvaldību iestādēm MK noteikumu Nr.442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* piemērošanā, kā arī izmaiņu izstrādes un saskaņošanas gaitā, lai nodrošinātu minimālo drošības ietvaru *Informācijas tehnoloģiju drošības likuma* aptvertajām mērķauditorijām.
- CERT.LV pārstāvji piedalījās atklāšanas sanāksmē, kas tika veltīta *NIS (Tīklu un informācijas drošības direktīvas)* ieviešanas izvērtējumam un iespējamām izmaiņām. CERT.LV pārstāvji sniedza novērtējumu NIS direktīvas ieviešanai Latvijā, kā arī piedalījās EK pārstāvju organizētā intervijā par šo jautājumu, gan kā nacionālā CERT vienība, gan kā *Digitālās drošības uzraudzības komitejas* pārstāvji. CERT.LV pauda viedokli

par NIS direktīvas problēmjautājumiem, piemēram, nepieciešamajiem precizējumiem NIS direktīvā digitālo pakalpojumu sniedzēju identifikācijai saistībā ar izņēmumiem. CERT.LV arī pauda bažas par plāniem veidot arvien jaunus ES mēroga administratīvos regulējumus, radot papildu slogu.

- CERT.LV piedalījās *Digitālās drošības un uzticamības* darba grupas sanāksmēs, sniedzot atbalstu VARAM Digitālās transformācijas pamatnostādņu sagatavošanā.
- CERT.LV sniedza ieteikumus *Elektronisko sakaru likuma* izmaiņām par CERT.LV tiesībām prasīt .lv domēna vārdu atslēgšanu, lai tiesības atslēgt vai mainīt domēna vārdu ierakstus būtu regulētas vienkopus *Informācijas tehnoloģiju drošības likumā*.
- CERT.LV piedalījās sanāksmēs un sniedza komentārus par *Saeimas vēlēšanu likuma* grozījumiem, kas paredzētu izmantot elektronisko tiešsaistes vēlētāju reģistru iecirkņos ārvalstīs, kas pēc vēlētāju priekšlikuma izvietoti ārpus Latvijas Republikas diplomātiskajām un konsulārajām pārstāvniecībām.
- CERT.LV sniedza komentāru par Satiksmes ministrijas un VARAM sagatavotā informatīvā ziņojuma projektu un protokollēmuma projektu par *Par Interneta protokola ceturtās un sestās versijas lietošanu valsts pārvaldē*, paužot satraukumu par pastāvošajiem drošības riskiem.
- CERT.LV piedalījās diskusijās par atbildīgas ievainojamību atklāšanas iekļaušanu normatīvajos aktos, sniedzot starptautiskās pieredzes piemērus un aplūkojot praktiskas ievainojamību atklāšanas situācijas.
- CERT.LV piedalījās *Finanšu nozares asociācijas* organizētā sanāksmē par banku, elektronisko sakaru komersantu un regulatora sadarbību. CERT.LV sniedza konsultācijas par tehniskajiem aspektiem attiecībā uz krāpnieciskajiem telefona zvaniem, zvanu numerāciju un iepriekš notikušajiem incidentiem.
- Tika uzsākta sadarbība ar *Patērētāju tiesību aizsardzības centru (PTAC)* lietu interneta (IoT) iekārtu pētīšanā, lai novērtētu IoT lietu drošību.

- CERT.LV piedalījās sanāksmē ar Valsts kontroli par to, kā valsts iestādes nodrošina pakalpojuma nepārtrauktību, kādi incidenti ir bijuši, kā tiek organizēta un kontrolēta paziņošana par incidentu.

CERT.LV ir aktīvs **Digitālās drošības uzraudzības komitejas** biedrs, kuras darbību nosaka 2016. gada 1. novembrī apstiprināti MK noteikumi Nr. 695. Komiteja ir koleģiāla uzraudzības institūcija Aizsardzības ministra pakļautībā, kuras mērķis ir:

- Uzraudzīt un reģistrēt kvalificētus elektroniskās identifikācijas pakalpojuma sniedzējus un kvalificētus paaugstinātas drošības elektroniskās identifikācijas pakalpojuma sniedzējus un to sniegtos pakalpojumus kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju reģistrā.
- Uzraudzīt un apstiprināt uzticamus sertifikācijas pakalpojumu sniedzējus un to sniegtos pakalpojumus un izveidot, uzturēt un publicēt uzticamības sarakstus.

Komiteja 2020. gadā, īstenojot LVRTC un citu uzticamības pakalpojumu sniedzēju uzraudzību, izskatīja un pārapstiprināja LVRTC kā kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju un tā kvalificētos elektroniskās identifikācijas līdzekļus, veica LVRTC pakalpojuma *eParaksts* sertifikāciju atbilstoši *eIDAS* prasībām, atzīstot to par kvalificētu elektronisko parakstu pēc pozitīva audita ziņojuma saņemšanas, izvērtēja un akceptēja izmaiņas *eID* karšu PIN/PUK koda izsniegšanas kārtībā un veica izpēti par kvalificētas parakstu radīšanas ierīces sertificēšanas jautājumiem.

CERT.LV cieši sadarbojās ar Zemessardzes **Kiberaizsardzības vienību (KAV)**, kas IT drošības krīzes vai apdraudējuma situācijā sadarbībā ar CERT.LV varētu sniegt atbalstu valstij un privātam sektoram. Kiberaizsardzības vienība veidota saskaņā ar *Zemessardzes likumu*, apvienojot privātajā sektorā nodarbinātos un brīvprātīgi iesaistīties gribošus ekspertus, kuri brīvajā laikā ir ieinteresēti veidot regulāru sadarbību IT drošības jautājumos, pilnveidojot ekspertīzi un zināšanas nacionālā un starptautiskā līmenī. 2020. gadā svarīgākā sadarbība notika kiberdrošības mācībās *Crossed Swords*, gan veidojot mācību vidi, gan piedaloties mācību norisē. Vienība tika iesaistīta arī atsevišķu incidentu risināšanā, kurā KAV sniedza atbalstu sistēmu drošības novērtēšanā. Ikviens interesents – informācijas tehnoloģiju eksperts – tiek aicināts sniegt savu ieguldījumu

valsts drošībā, pievienojoties Kiberaizsardzības vienībai. Papildu informācija par vienību un pieteikšanos Zemessardzes tīmekļa vietnē www.zs.mil.lv/lv/zemessardzes-vienibas/zemessardzes-kiberaizsardzibas-vieniba.

CERT.LV turpināja koordinēt arī **Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupu (DEG)**, kura neformāli savu darbību uzsāka jau 2007. gada martā, bet formāli to nostiprināja 2012. gadā, izveidojot grupas statūtus un ētikas kodeksu. DEG sanāksmes notiek katra mēneša otrajā ceturtdienā – tajās, brīvā formātā, tiek apspriestas kiberdrošības aktualitātes. DEG ir vieta, kur Latvijas IT eksperti no dažādām iestādēm un organizācijām var apmainīties ar viedokļiem, labo praksi un pieredzi. DEG var pievienoties ikviens, kurš apņemas ievērot DEG ētikas kodeksu un statūtus, kā arī saņem rekomendācijas no diviem jau esošiem DEG biedriem. Vairāk informācijas CERT.LV tīmekļa vietnē www.cert.lv/lv/iniciativas-un-aktivitates/drosibas-ekspertu-grupa-deg.

Kopā ar Latvijas Interneta asociāciju (LIA) turpinājās iniciatīva ***Atbildīgs interneta pakalpojumu sniedzējs***, kas aicina Latvijā reģistrētus interneta pakalpojuma sniedzējus (IPS) uz sadarbību, piesakoties saņemt CERT.LV rīcībā esošo informāciju par apdraudētām gala lietotāju iekārtām un nogādāt to saviem klientiem – interneta lietotājiem. Iniciatīvas ietvaros IPS tiek aicināti reaģēt uz ziņojumiem, kas saņemti no Latvijas Interneta asociācijas drošāka interneta centra par nelegālu interneta saturu uz IPS serveriem, attiecīgi informējot atbilstošo satura izvietotāju un aicinot pārkāpumu novērst, un nelegālo saturu dzēst. Šobrīd iniciatīvai pievienojušies 13 lielākie IPS Latvijā. Vairāk informācijas CERT.LV tīmekļa vietnē www.cert.lv/lv/elektronisko-sakaru-komersantiem/atbildigs-ips.

8.

Starptautiskā sadarbība

Pārskata periodā CERT.LV nemainīgi stiprināja sadarbību ar citu valstu IT drošības incidentu novēršanas vienībām un starptautiskām organizācijām. Tāpat CERT.LV speciālisti uzstājās ar prezentācijām starptautiskās konferencēs un semināros. Neizpalika arī jaunu prasmju apgūšana, un kvalifikācijas celšana, piedaloties starptautiskās tehniskās mācībās.

CERT.LV regulāri piedalījās *NIS CSIRT Network* (NIS direktīvas CERTu sadarbības tīkla) sanāksmēs. To mērķis ir nodrošināt sadarbības stiprināšanu starp IT drošības incidentu novēršanas vienībām Eiropas mērogā. Sanāksmes notiek 3 reizes gadā, un tās organizē konkrētajā brīdī Eiropas Savienības Padomes prezidējošā valsts sadarbībā ar ENISA. Reizi gadā sanāksmē notiek arī apvienotās sesijas kopā ar NIS direktīvas sadarbības grupu.

NIS CSIRT Network ietvaros darbojas vairākas tematiskas darba grupas. Divās no tām aktīvi darbojas arī CERT.LV pārstāvji: *Cyber Weather* darba grupa regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai; *Maturity* darba grupa rūpējas par ES dalībvalstu IT drošības incidentu novēršanas vienību brieduma līmeņa paaugstināšanu.

COVID-19 pandēmijas ietekmē martā tika izveidota *NIS CSIRT Network* informācijas apmaiņas grupa. Grupas mērķis bija operatīva informācijas aprite par incidentiem, kas saistīti ar COVID-19 tematiku, kā arī par kiberdrošības aktualitātēm veselības aprūpes nozarē. Vairāku mēnešu garumā ik nedēļu tika apkopota informācija par situāciju visās Eiropas valstīs un gatavots pārskats lēmumu pieņēmējiem *NIS Cooperation grupā* un citās.

Apliecinot komandas briedumu un augsto kvalifikāciju, CERT.LV regulāri piedalās NIS direktīvas CERTu sadarbības tīkla IT drošības incidentu novēršanas vienību savstarpējos auditos (*peer review*). 2020. gadā CERT.LV veica auditu Slovēnijas nacionālajai CERT vienībai SI-CERT un Portugāles nacionālajai vienībai.

CERT.LV ir aktīvs FIRST biedrs un turpināja darbību *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejā), palīdzot uzlabot biedru uzņemšanas procesus, lai nodrošinātu augstāku kvalitāti informācijai, kas tiek iesniegta uzņemšanai FIRST organizācijā. CERT.LV vadītāja Baiba Kaškina tika ievēlēta par *FIRST Membership Committee* līdzpriekšsēdētāju (*co-chair*).

CERT.LV piedalījās arī FIRST konferences programmkomitejā, sniedzot atbalstu konferences programmas veidošanā, kā arī piedalījās TF-CSIRT/FIRST simpozijā Malagā, kurā sniedza vairākas prezentācijas.

Ļoti būtiska CERT.LV ir sadarbība ar *NATO Cooperative Cyber Defence Centre of Exelence (NATO CCDCoE)*, kas atrodas Tallinā, Igaunijā. CERT.LV regulāri vada mācību kursus NATO CCDCoE un sniedz atbalstu NATO CCDCoE tehnisko kiberdrošības mācību, piemēram, *Crossed Swords* un *Locked Shields* organizēšanā un nodrošināšanā.

CERT.LV piedalījās *Crossed Swords* organizēšanā, iesaistoties mācību satura sagatavošanā, izspēles dizaina izstrādē un attīstāmo spēju virzienu noteikšanā. 2020. gada janvārī kiberdrošības mācības *Crossed Swords* notika Rīgā. Tās kopā pulcēja vairāk nekā 120 tehnisko ekspertu, nacionālo Kiberpavēlniecību, speciālo vienību un militārās policijas pārstāvjus no 26 valstīm. *Crossed Swords* no tehniskām sarkanā karoga komandas mācībām ir attīstījušās par unikālu un kompleksu ofensīvo kiberoperāciju treniņu programmu, kas apvieno dažādas tehniskās prasmes ar kinētisko spēku komponenti, un aptver vairākus ģeogrāfiskos atrašanās punktus vienlaicīgi. Mācību galvenais uzsvars 2020. gadā tika likts uz starpvalstu un starpdisciplināro sadarbību pilna spektra ofensīvas kiberoperācijas realizācijā. *Crossed Swords 2020/II* notika decembrī Tallinā, un arī šeit CERT.LV iesaistījās gan mācību plānošanas un izstrādes procesā, gan mācību norises vadībā.

Pandēmijas ietekmē kiberdrošības mācību *Locked Shields 2020* norise pārskata periodā tika atcelta. Tika uzsākti sagatavošanās darbi dalībai kiberdrošības mācībās *Locked Shields* 2021 un veiktas pārrunas ar potenciālajiem sadarbības partneriem. Latvijas komanda 2021. gada mācībās piedalīsies apvienībā ar Korejas republikas (Dienvidkorejas) komandu. Tā būs pirmā reize *Locked Shields* mācību vēsturē, kad notiks šāda starpreģionālā sadarbība vienas komandas ietvaros, sniedzot vērtīgu pieredzi gan kulturālo, gan tehnoloģisko, gan arī ģeogrāfisko faktoru ietekmē.

CERT.LV regulāri piedalās *ENISA* (Eiropas Tīkla un informācijas drošības aģentūras) organizētajās starptautiskajās kiberdrošības mācībās *Cyber Europe*. 2020. gadā plānotās mācības gan tika atceltas COVID-19 pandēmijas dēļ, taču turpinās gatavošanās nākamai reizei 2021. gada rudenī.

Pārskata periodā CERT.LV piedalījās arī vairākās diskusijās un sniedza ieteikumus un atgriezenisko saiti par NIS direktīvas ieviešanu, ES Kiberdrošības akta izstrādi un tā ietekmi uz CERTu tīklu, vienotas Eiropas kibervienības izveidi, kiberdrošību prasību tiesisko regulējumu attiecībā uz IKT produktiem, kā arī kritiskās infrastruktūras aizsardzību.

Sadarbībā ar Itālijas CSIRT komandu tika veikta padziļināta krāpniecisko aktivitāšu rīka *Sp0m* izpēte. Rīks paredzēts izmantošanai sociālo tīklu platformās un kiberuzbrucējiem nodrošina daļēju ļaundabīgo aktivitāšu automatizēšanu. Par izpētes rezultātiem tika informēta gan CERTu kopiena, gan arī sabiedrība kopumā. Izpēte ļāva noskaidrot veidus, kā tiek iegūtas kompromitētās tīmekļa vietnes, kuras attiecīgajā rīkā tiek piedāvātas kaitīgā satura izvietošanai.

20. novembrī CERT.LV tika uzņemta enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*. Šo grupu šobrīd veido EEZ valstu enerģētikas un nacionālo CERT vienību komandas no Austrijas, Zviedrijas, Norvēģijas, Šveices, Somijas un Latvijas.

9.

ES līdzfinansētu projektu īstenošana

Projekta ***Improving Cyber Security Capacities in Latvia*** (līguma ar Eiropas Komisiju Nr.INEA/CEF/ICT/A2017/15287842018) īstenošana sākās 2018. gada 1. septembrī un turpinājās līdz 2020. gada 31. decembrim. Projekta mērķis, kā norāda tā nosaukums, bija stiprināt Latvijas kiberdrošības kapacitāti. 2020. gada laikā projekta ietvaros:

- Turpinājās aktīva iesaiste *MeliCERTes – Cybersecurity Core Service Platfrom* izstrādē un testēšanā. Platformas mērķis ir, apkopojot IT drošības incidentu novēršanas vienību prasības starptautiskai sadarbībai, nodrošināt vienotu sistēmu, kurā varētu notikt starptautisku kiberincidentu risināšana un informācijas apmaiņa par kiberincidentiem.
- Turpinājās darbs pie *Deep Analysis System: Pastelyzer – the Paste Analyzser* izstrādes. Tika publiskota *Deep Analysis System* beta versija, un TF-CSIRT konferencē Malagā sistēma tika prezentēta plašākai CERTu kopienai, aicinot CERTu komandas uz sadarbību tālākai sistēmas attīstīšanai. Sistēmas mērķis ir, iekļaujoties esošajā IT drošības incidentu novēršanas vienību ikdienas darbā, nodrošināt apjomīgu datu automatizētu atlasi un analīzi. Vairākas komandas atsaucās aicinājumam. Sistēma, uzstādīšanas instrukcija un lietotāju rokasgrāmata.
- Tika nodrošināta kvalifikācijas celšana gandrīz 40% CERT.LV darbinieku ļaujot iegūt starptautiski atzītus sertifikātus un stiprinot kopējo CERT.LV komandas briedumu.
- Tika aktīvi gatavota un realizēta informatīvi izglītojoša kampaņa Kiberdrošība darbavietā. Kampaņa norisinājās vienu mēnesi no 14. septembra līdz 11. oktobrim. Ar jaunvārdiem parolīze, muļķerēšana un spaidonis atraktīvā veidā tika uzrunāti organizāciju un uzņēmumu darbinieki – interneta lietotāji. Četru nedēļu garumā, uzrunājot sabiedrību ar īpašu video, reklāmas un rakstu palīdzību, tika sasniegti vairāk nekā 500 tūkstoši Latvijas interneta lietotāji. Kampaņas materiālos CERT.LV eksperti sniedza padomus, kā veidot noturīgus un efektīvus kiberdrošības paradumus, kā vislabāk rūpēties par savu iekārtu drošību, kā veidot efektīvas paroles un atcerēties tās. Kampaņas video materiālu kopējais skatījumu skaits platformā *YouTube* sasniedza 427 tūkstošus, gandrīz 400 dalībnieki savas jauniegūtās

zināšanas nolēma pārbaudīt arī praktiski, atbildot uz āķīgiem jautājumiem kampaņas digitālajā rokasgrāmatā – rokasgramata.esidross.lv. Visi kampaņas materiāli arī turpmāk būs pieejami vietnē www.esidross.lv.

Projekta ***Cyber Exchange*** (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528784) īstenošana sākās 2018. gada 1.novembrī un turpināsies līdz 2022. gada 31. decembrim. Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības IT drošības incidentu vienībām (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 ietvaros paredzētas pieredzes apmaiņas vizītes.

COVID-19 vīrusa izplatības ierobežošanai noteikto ceļojumu ierobežojumu rezultātā projektā plānotās apmaiņas vizītes, kas ir projekta pamata aktivitāte, 2020. gadā tika atceltas, un projekta īstenošana tiks turpināta epidemioloģiskai situācijai uzlabojoties.

10.

Pakalpojumi Latvijas kibertelpas stiprināšanai

DNS Ugunsmūris: Tika turpināts darbs pie CERT.LV un NIC.LV izstrādātā DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūra (*DNS firewall*) projekta attīstīšanas. Projekts sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā, kas saistīts ar kiberdrošības institūcijām jau zināmiem incidentu identifikatoriem (domēnu vārdi, IP adreses u.c.). DNS PRZ pakalpojumu var izmantot arī bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC.LV rekursīvie DNS serveri. Vairāk informācijas un detalizētas instrukcijas, pieejamas vietnē https://dnsmuris.lv.

Agrās Brīdināšanas Sistēma (ABS): ABS jeb sensors ir pasīva drošības iekārta, kas ļauj apzināt apdraudējumu un aizsargāt lietotāju. ABS nodrošina datu pārraides tīkla plūsmas anomāliju analīzi, ļaunatūras atpazīšanu un brīdinājumu saņemšanu par konstatētajiem apdraudējumiem.

ABS iekārtas uzstādīšanu un konfigurāciju nodrošina CERT.LV, organizācijai ir jānodrošina divi elektrības pieslēgumi un divi tīkla pieslēgumi (*access* + *mirror*). Par ABS uzstādīšanu tiek slēgts sadarbības līgums. Pakalpojums primāri pieejams valsts un pašvaldību iestādēm kā arī pamatpakalpojumu un digitālo pakalpojumu sniedzējiem. Lai uzzinātu vairāk par ABS un lemtu par tā uzstādīšanu savā organizācijā, lūgums rakstīt: cert@cert.lv.

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

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments