CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Latvijas universitātes Matemātikas un informātikas institūts

Aizsardzības ministrija

2021

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 4

1. Incidentu apstrāde 9

2. Nozīmīgākie incidenti 2021. gadā 18

2.1. Pakalpojuma pieejamība 19

2.2. Krāpšana 20

2.3. Ielaušanās mēģinājumi 22

2.4. Ļaundabīgs kods 23

2.5. Kompromitētas iekārtas un datu noplūdes 24

2.6. Ievainojamības un konfigurācijas nepilnības 26

3. Atbildīga ievainojamību atklāšana 27

4. Drošības testi 29

5. Informatīvie komunikācijas pasākumi 31

6. Izglītojošie pasākumi 35

6.1. Starptautiskā kiberdrošības konference Kiberšoks 2021 37

6.2. CERT.LV organizētie pasākumi IT drošības speciālistiem 42

6.3. CERT.LV prezentācijas par IT drošību sabiedrības izglītošanai 43

7. Stratēģiskā sadarbība Latvijā 45

8. Starptautiskā sadarbība 49

9. ES līdzfinansētu projektu īstenošana 56

10. Pakalpojumi Latvijas kibertelpas stiprināšanai 59

Kopsavilkums

Izmaiņas ikdienas gaitās arī 2021. gadā turpināja ietekmēt mūs visus, un, pirms ķeramies klāt nākamajiem darbiem strauji mainīgajā kibertelpā, aicinām kopīgi atskatīties uz pagājušo gadu.

2021. gadā globālā kibertelpa piedzīvoja pamatīgu viļņošanos, kas bija sajūtama arī Latvijā. Elpu aizturēt lika gan virkne kritisku ievainojamību (*MS Exchange* serveru, *Print Spooler*, *Log4j* u.c. ievainojamības), gan iespaidīgi kiberuzbrukumi ārvalstu uzņēmumiem (degvielas piegādes tīklam *Colonial Pipeline*, gaļas pārstrādes kompānijai *JBS*, attālinātās IT pārvaldības rīkam *Kaseya* un Īrijas e-veselības sistēmai).

Tomēr, lai arī gads bija jaunatklātām ievainojamībām bagāts, daudzos incidentos, kas notika Latvijas kibertelpā, uzbrucēju veiksmes pamatā bija nepietiekama sistēmu aizsardzība – novecojis programmnodrošinājums un vājas paroles. Papildu apdraudējumus radīja pandēmijas ietekmē sadrumstalotā IT infrastruktūra, kurā būtiski pieauga atsevišķu darbstaciju drošības un lietotāju kiberhigiēnas paradumu nozīme.

Kā papildu pārbaudījums iedzīvotāju modrībai bija kiberuzbrucēju inovatīvā pieeja krāpnieciskajiem telefona zvaniem, īstenojot tos ar viltotiem zvanītāju identifikatoriem (ID) – gan izliekoties par banku, gan "aizņemoties" iedzīvotāju mobilo telefonu numurus.

Pasaulē novērotie uzbrukumi tieši piegāžu ķēžu uzņēmumiem aktualizēja drošības jautājumu arī Latvijā. Tas iezīmēja izaicinājumus gan Latvijas uzņēmumiem, kas nodrošina produkciju globālajam tirgum, gan Latvijas uzņēmumu un organizāciju sadarbībai ar informācijas un komunikācijas tehnoloģiju (IKT) piegādātājiem un uzturētājiem.

Ņemot vērā, ka būtiski palielinājusies sabiedrības atkarība no digitāliem risinājumiem un tehnoloģijām, bet aizsardzība pret kiberuzbrukumiem kļūst izaicinājumiem pilnāka, svarīgi šiem izaicinājumiem sagatavoties savlaicīgi.

Kopumā pārskata periodā CERT.LV reģistrēja 254 392 apdraudētas unikālās IP adreses, kas ir par aptuveni 36% mazāk nekā 2020.gadā. Pārskata periodā nav novērotas būtiskas svārstības apdraudēto IP adrešu apjomā.

2021. gadā CERT.LV organizēja un piedalījās 123 pasākumos sasniedzot un informējot 13 619 dalībniekus. Pandēmijas ierobežojumi lika pārcelt klātienes pasākumus tiešsaistē, un, lai arī tiešsaistes pasākums pilnībā neaizstāj klātieni – tas ļāva būtiski palielināt aptvertās auditorijas apjomu.

Eiropas Kiberdrošības mēneša ietvaros 6.-7. oktobrī CERT.LV rīkoja tehnisko tiešsaistes konferenci kiberdrošības profesionāļiem *Kiberšoks 2021*, kurā starptautiski novērtēti eksperti dalībniekiem sniedza padziļinātu ieskatu plašā, ar kiberdrošību saistītu jautājumu klāstā, prezentācijās iekļaujot arī reāllaika demonstrācijas. *Kiberšoks 2021* piedalījās 923 dalībnieki no 53 valstīm. Paralēli konferencei norisinājās arī CTF (*Capture the Flag*) sacensības, kurās dažādiem kiberdrošības izaicinājumiem pretī stājās 31 komanda.

Nākamajā pārskata periodā digitālās vides aizsardzība pret kiberuzbrukumiem kļūs arvien nozīmīgāka un reizē ar izaicinājumiem pilnāka. **Svarīgi ir sagatavoties savlaicīgi šiem izaicinājumiem, neatstājot rīcību uz pēdējo brīdi, kad jau iestājušies apdraudējumi ar potenciāli būtiskām sekām.**

Lielai daļai sabiedrības turpinot darba pienākumus veikt attālināti, organizācijām un uzņēmumiem kiberdrošības uzlabošanai **jāraugās uz individuālu, savstarpēji neatkarīgu atsevišķu iekārtu kiberdrošības risinājumu izveidi.** Daudzkārt pieminētais *Zero Trust* modelis ir viens no virzieniem, kā to veicināt, papildus iespējojot arī daudzfaktoru autentifikāciju visur, kur tas ir iespējams. Svarīgi gan uzsvērt, ka tieši **katra indivīda kiberhigiēnas izpratnes stiprināšana** ir viens no kiberdrošības stūrakmeņiem jaunajos darba apstākļos.

Kaut arī piegāžu ķēžu uzbrukumi Latviju līdz šim skāruši maz, globālajā kibertelpā tie strauji iegūst popularitāti noziedznieku vidū, jo sniedz iespēju, kompromitējot vienas komponentes piegādātāju, kompromitēt virkni šī piegādātāja klientus un to izstrādātos produktus. **Latvijas uzņēmumiem, kas ražo produktus globālajam tirgum, jārēķinās ar iespēju kļūt par kiberuzbrucēju mērķi un pastiprināta uzmanība jāpievērš kiberdrošības jautājumiem**, lai novērstu piegādes ķēdes kompromitēšanas uzbrukumus.

Arī briestošie saspīlējumi ģeopolitiskajā situācijā radīs papildu izaicinājumus kiberdrošības jomā – tāpēc izturību un spēku visiem 2022. gadā!

CERT.LV komandas vārdā
Baiba Kaškina
CERT.LV vadītāja


AIZSARDZĪBAS
MINISTRIJA
CERT.LV
10. GADADIENĀ
Paldies par
sadarbību kiberdrošības stiprināšanā!
2021. gada 1. februārī

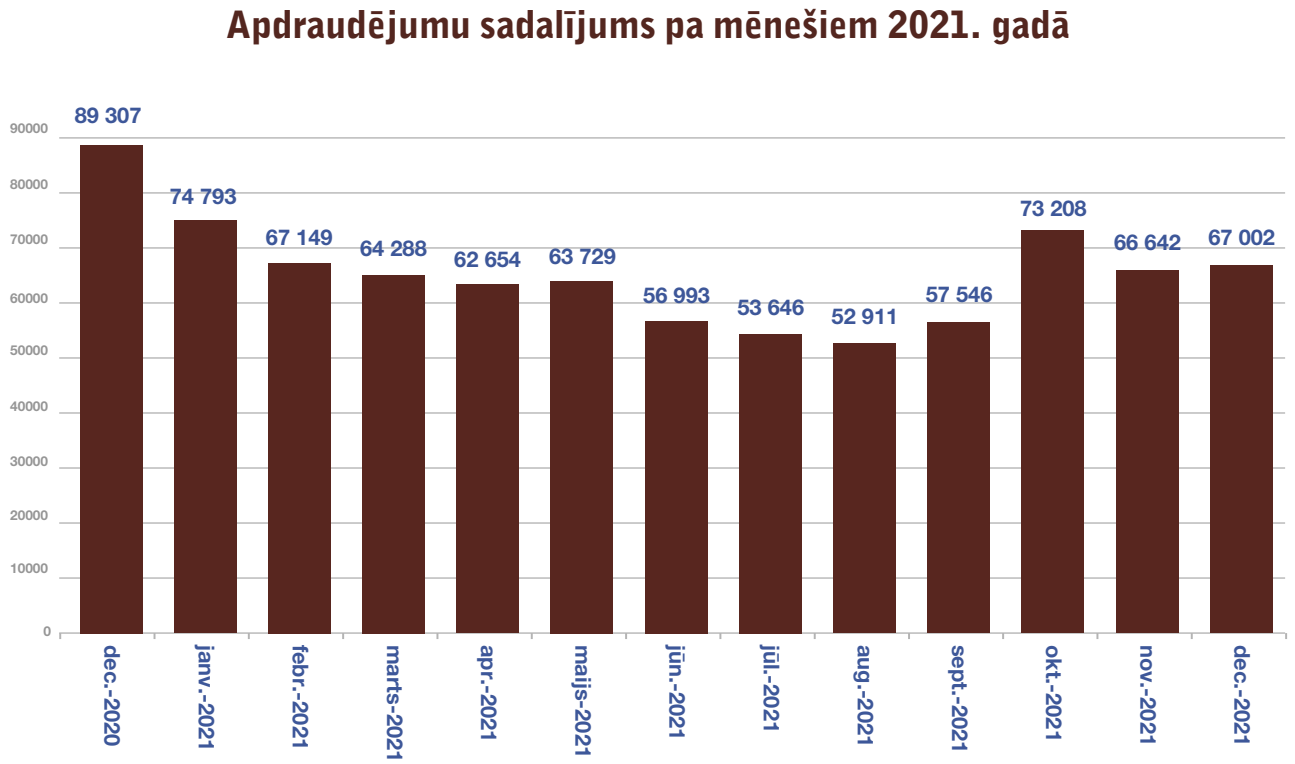

Cyber
SHOCK
2021
CS21
CS21

1.

Incidentu apstrāde

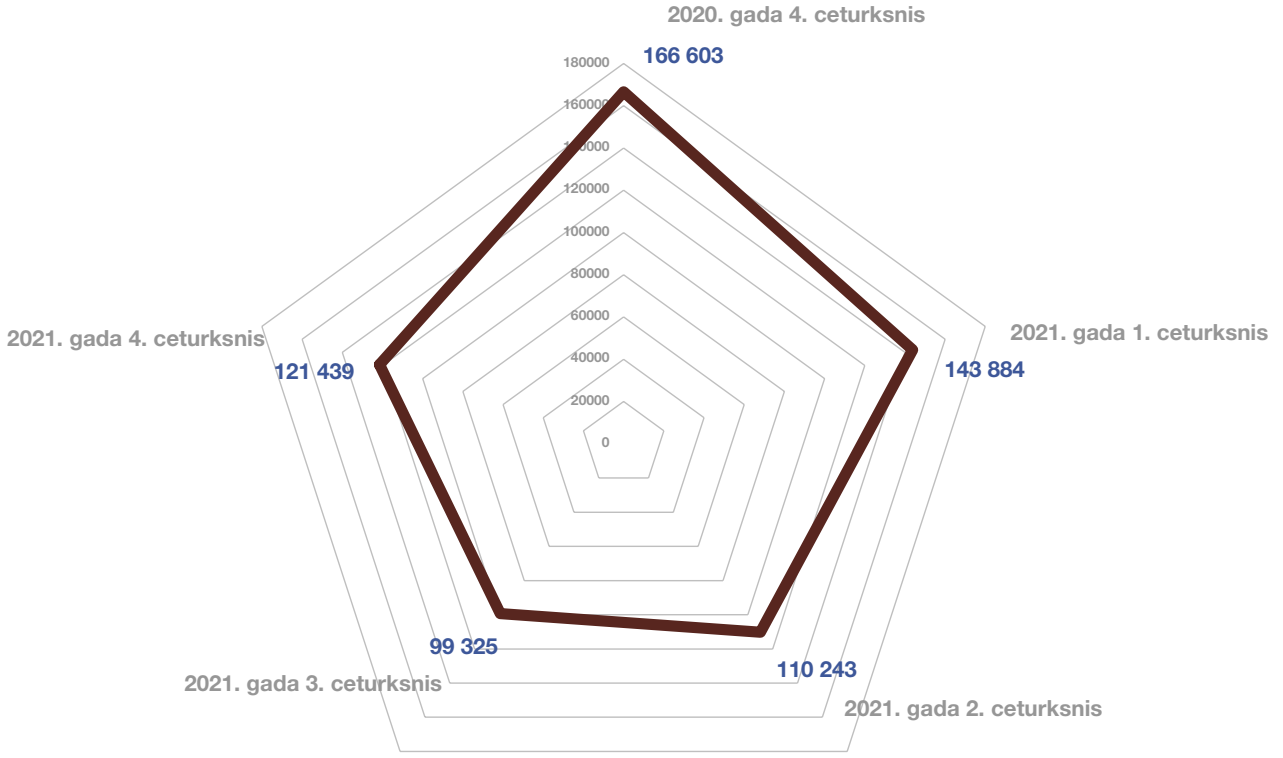
Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Apdraudējumu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija). Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīt vienkopus, sadalot tos apdraudējumu 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 64 000 ievainojamu unikālu IP adrešu.



1. attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 2021. gadā.

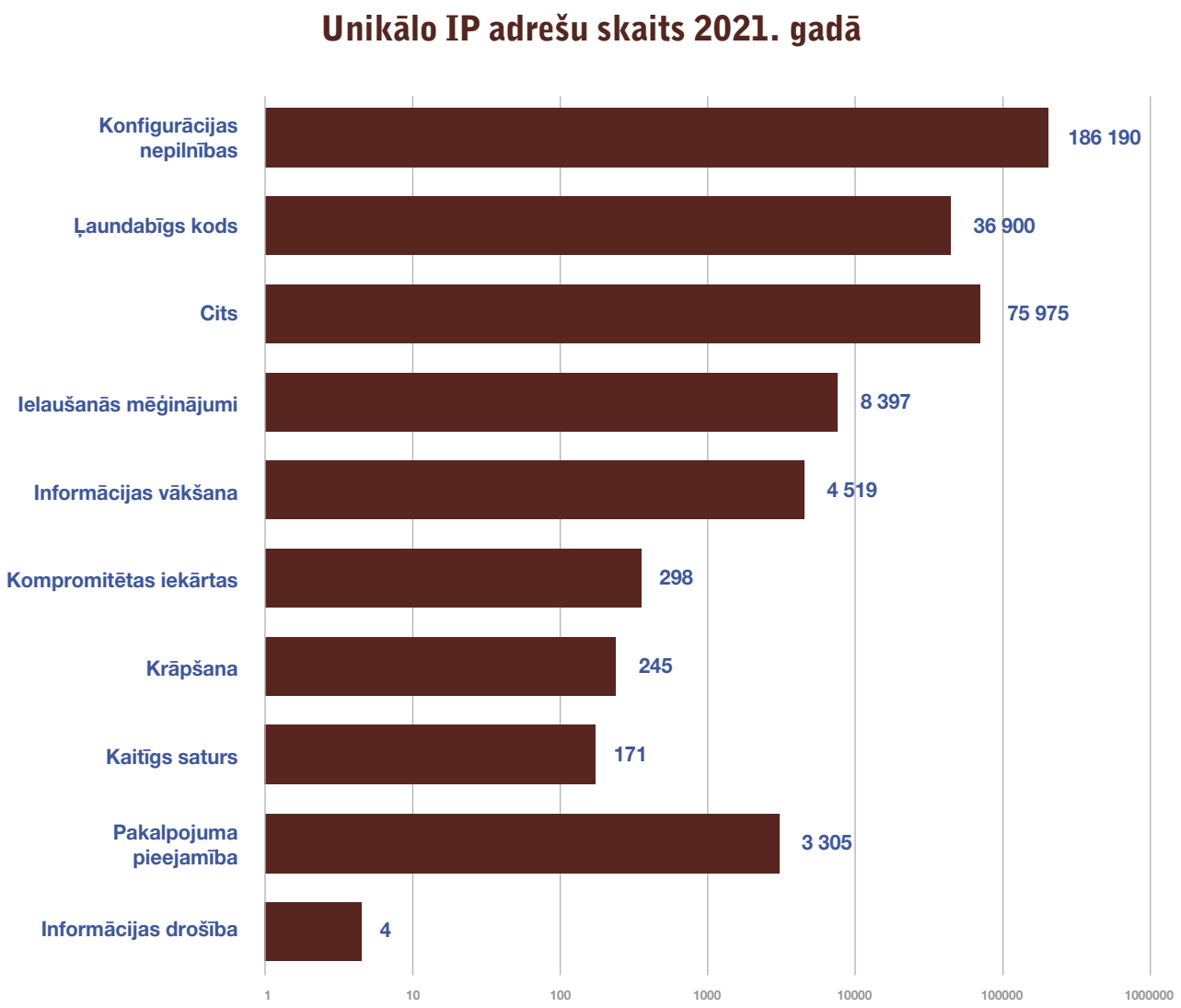
Apdraudējumu sadalījums pa ceturkšņiem 2021. gadā



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

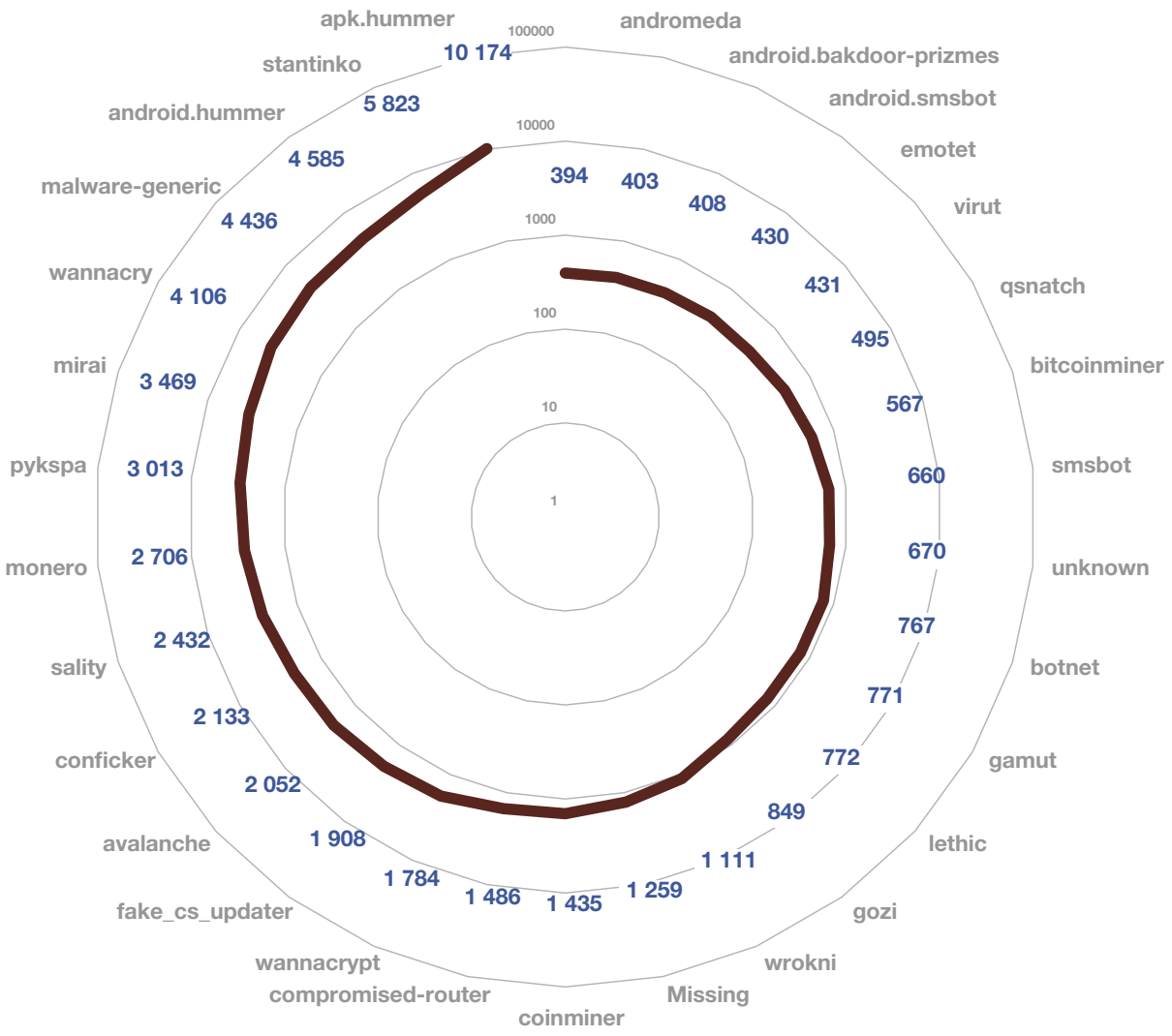
Kopumā pārskata periodā CERT.LV reģistrēja 254 392 apdraudētas unikālās IP adreses. Pārskata periodā nav novērotas būtiskas svārstības apdraudēto IP adrešu apjomā.

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



3. attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa apdraudējuma veidiem 2021. gadā.

Unikālo IP adrešu skaits – ļaundabīgs kods 2021. gadā



4. attēls – CERT.LV kopējais reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gadā ar apdraudējuma veidu – ļaundabīgs kods.

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

Otrajā vietā atrodas ļaunatūra *Stantinko*, kas paredzēta dažādu kriptovalūtu ieguvei, nesankcionēti izmantojot upura iekārtas resursus un potenciāli radot iekārtas pārslodzi, kā arī demonstrē lietotājam reklāmas, tādējādi nodrošinot reklāmu izvietotājiem peļņu.

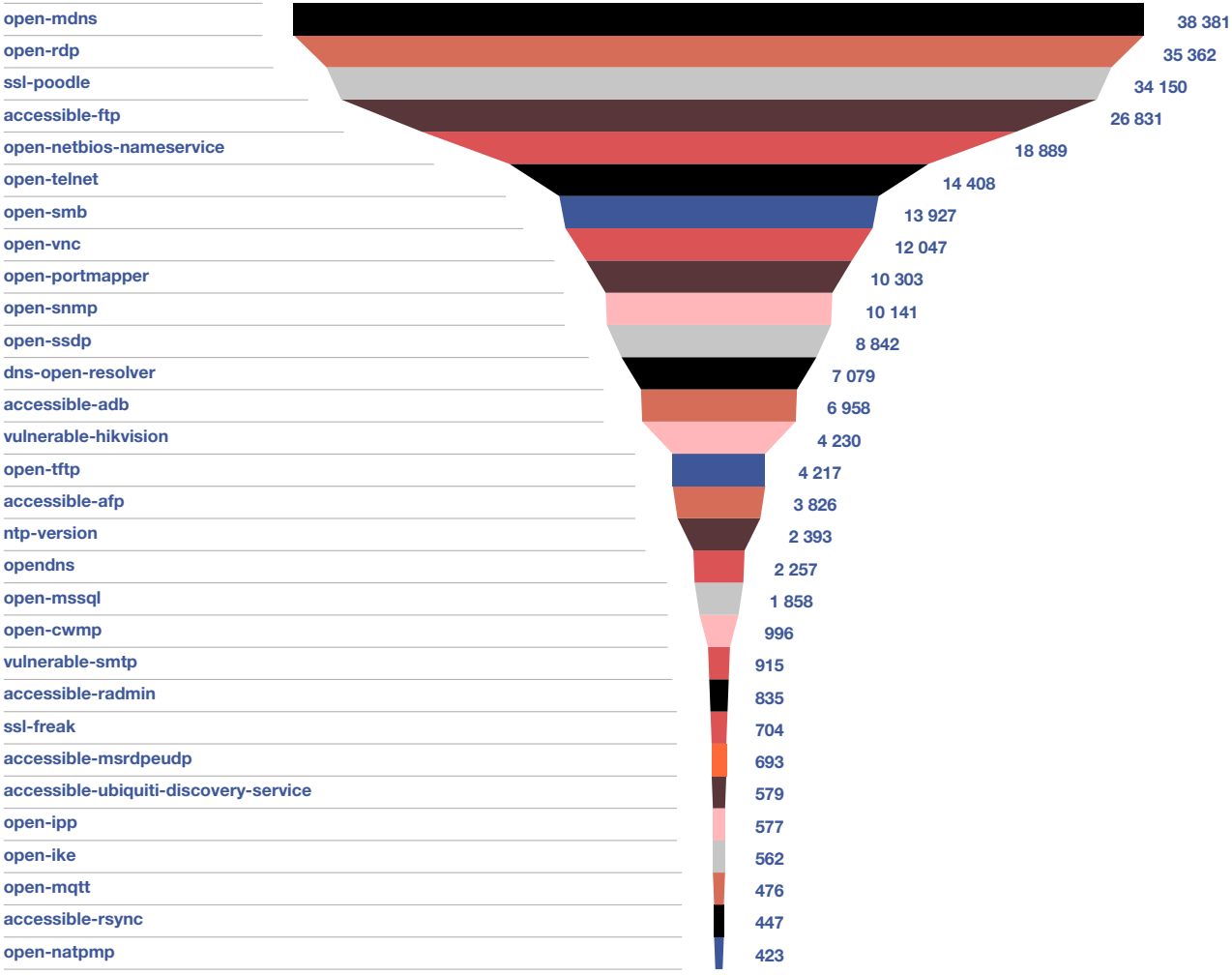
Trešo vietu ieņem *WannaCrypt* jeb *Wannacry* šifrējošais izspiedējvīruss. Tas ietekmē iekārtas ar *Microsoft Windows* operētājsistēmu un izplatās, izmantojot ievainojamību *Server Message Block* (SMB) protokolā, kas tiek lietots failu apmaiņai iekšējā tīklā. Vīrusa ietekmi un izplatību iespējams novērst,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

Pirmo vietu konfigurācijas nepilnību topā ieņem *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.

Otrajā vietā atrodas *OpenRDP*. RDP ir attālās piekļuves risinājums, kas bieži tiek izmantots arī uzbrukumos. 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 internetā un nav uzstādīta pietiekami droša piekļuves parole.

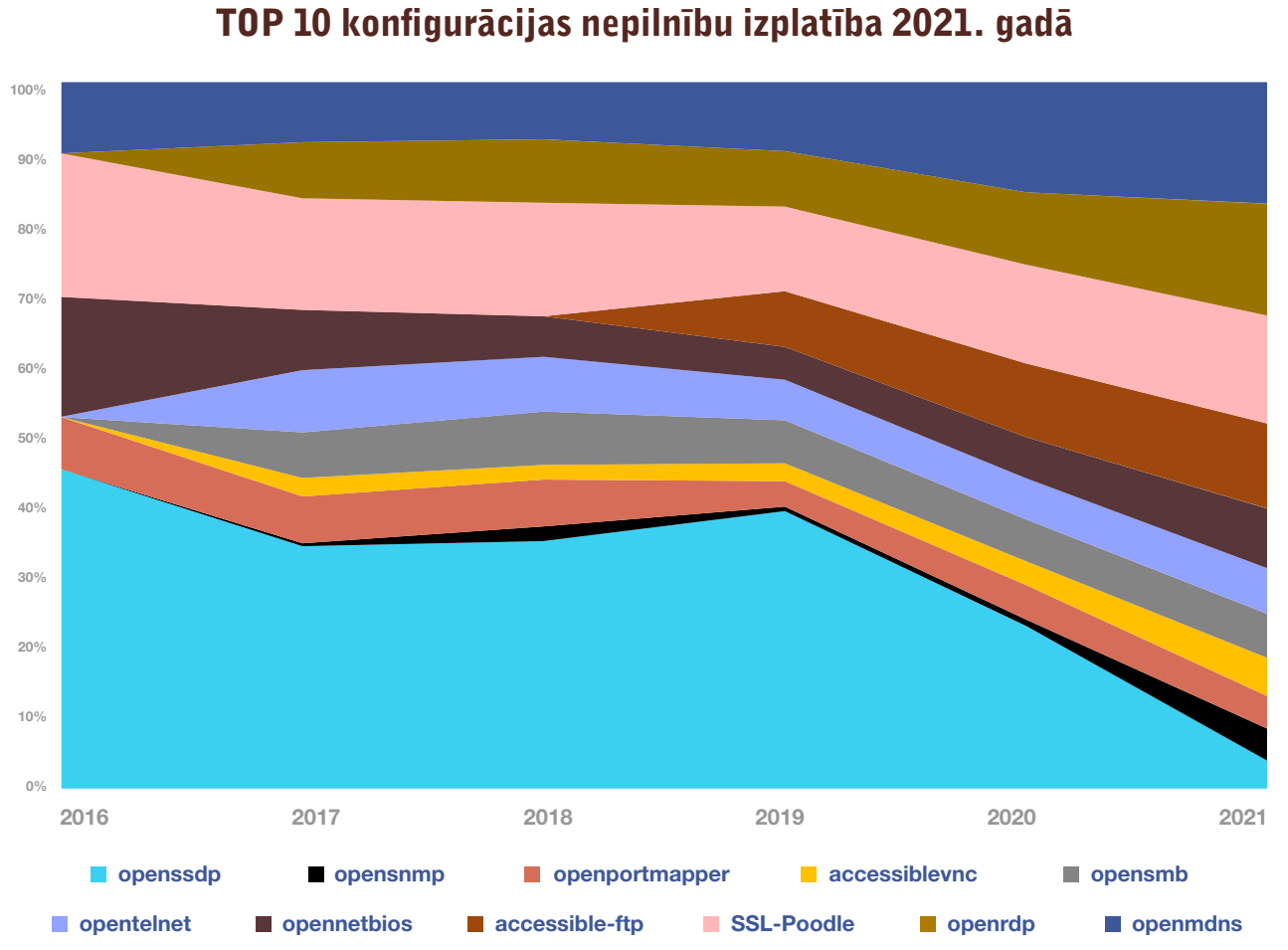
Trešo vietu ieņem konfigurācijas nepilnība *SSL-Poodle*, kas pakļauj iekārtu POODLE (*Padding Oracle On Downgraded Legacy Encryption*) uzbrukumam, sniedzot uzbrucējiem iespēju pārtvert šifrētu datu plūsmu, piemēram, lietotājvārdus, paroles, *cookies* u.c., un izlikties par iekārtas lietotāju.

Unikālo IP adrešu skaits – konfigurācijas nepilnības 2021. gadā

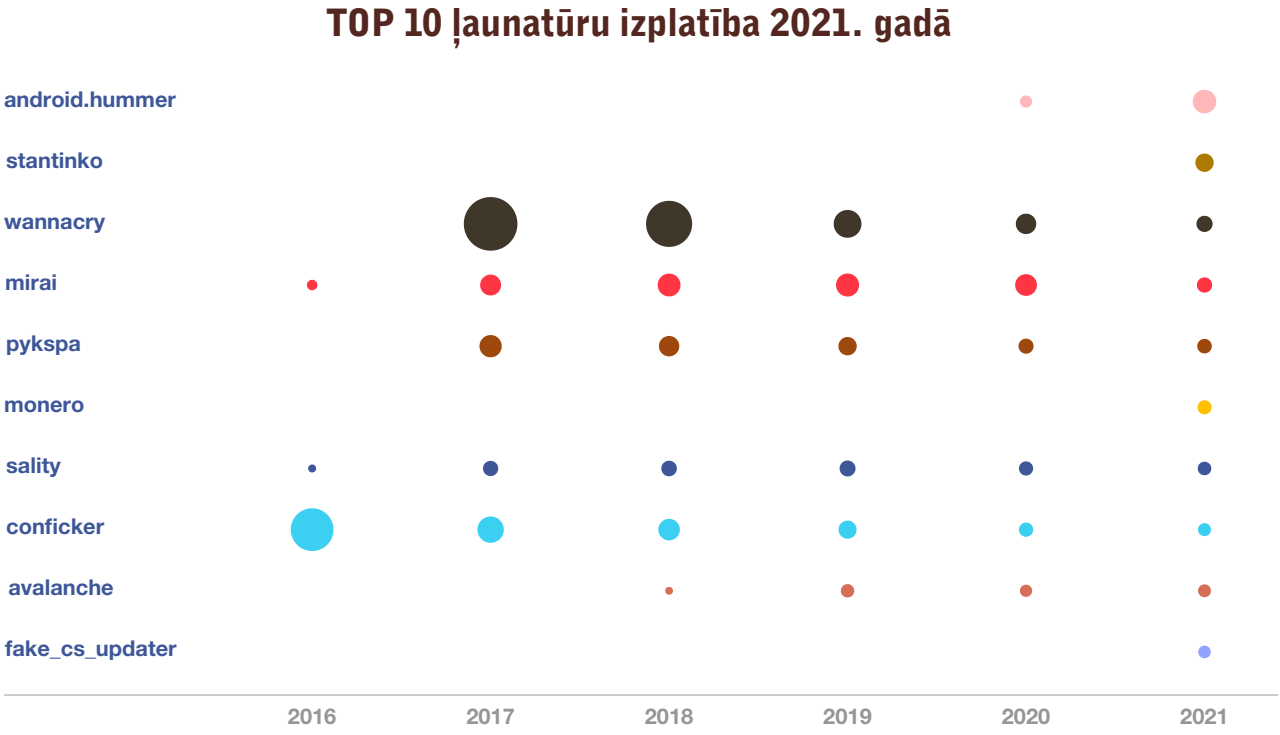


5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gadā ar apdraudējuma veidu – konfigurācijas nepilnība.

Aplūkojot konfigurācijas nepilnību un ļaunatūru topu, var novērot, ka desmit 2021. gadā visizplatītākās konfigurācijas nepilnības Latvijas kibertelpā ir bijušas klātesošas jau kopš 2017. gada (6.attēls), savukārt no desmit 2021. gadā visizplatītākajām ļaunatūrām 2017. gadā Latvijas kibertelpā tika novērotas tikai piecas (7.attēls).



6. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ar 2021. gadā izplatītākajām konfigurācijas nepilnībām.



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ar 2021. izplatītākajām ļaunatūrām.

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.

2.

Nozīmīgākie incidenti 2021. 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. Pakalpojuma pieejamība

Gada sākumā 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. Bija vērojama arī pieaugoša pakalpojuma atteices uzbrukumu aktivitāte pret Latvijas publiskā sektora resursiem un atsevišķiem medijiem. Gada nogalē DDoS uzbrukumi, galvenokārt, bija vērsti pret telekomunikāciju pakalpojumu sniedzējiem.

Tika saņemti vairāki ziņojumi par traucējumiem valsts līmeņa resursu darbībā. Veicot tehnisko datu analīzi, tika konstatēts, ka resursi ārējai ietekmei netika pakļauti. Īslaicīgus resursu darbības traucējumus izraisīja nepilnības sistēmu darbībā vai neatbilstoša DDoS aizsardzības risinājuma konfigurācija.

Gada sākumā vietnē *www.manavakcina.lv* tika atvērta pieteikšanās vakcīnai pret Covid-19. Vietnes apmeklētāji saskārās ar vietnes darbības traucējumiem, gaidīšanas laiks virtuālajā rindā atsevišķos gadījumos pārsniedza stundu. Traucējumus radīja gan lielais apmeklētāju skaits, gan vietnē izmantotā *latvija.lv* autentifikācijas moduļa nespēja tikt galā ar 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.

Vairākas mācību iestādes piedzīvoja mācību procesa traucējumus, kurus izraisīja DDoS uzbrukumi pret skolas infrastruktūru. Ņemot vērā, ka uzbrukumi tika novēroti tikai aktīvajā mācību laikā, laika posmā starp pulksten 9:00 un 14:00, visticamāk šo uzbrukumu iniciatori bija skolu audzēkņi, kuri uzbrukumu veikšanai izmantoja atbilstošus maksas pakalpojumus. Ar līdzīgiem izaicinājumiem saskārās arī izglītības iestādes citviet Eiropā.

Gan starptautiskā sabiedrība, gan arī Latvijas iedzīvotāji pastiprināti izjuta starptautisko sociālo tīklu ietekmi uz ikdienas gaitām. Šie tīkli kalpo ne tikai par saziņas platformu, bet tiek plaši izmantoti arī kā pierakstīšanās rīks citās vietnēs un tiešsaistes pakalpojumos, piemēram, tirdzniecības vietnēs vai viedtelevīzijā. Sociālo tīklu nepieejamība vairāku stundu garumā radīja apgrūtinājumu saņemt ierastos pakalpojumus arī iedzīvotājiem Latvijā.

2.2. Krāpšana

Pandēmijai turpinoties, arvien lielākai daļai iedzīvotāju dažādas ikdienišķas aktivitātes nācās pārcelt tiešsaistē, piemēram, preču vai pakalpojumu iegādi. Savukārt citi tiešsaistē meklēja iespēju uzlabot savu finansiālo stāvokli – to veicināja gan brīvie finanšu līdzekļi, kas netika iztērēti atvaļinājumu braucienos, gan kriptovalūtu pieaugošā pieejamība, kas plašākai sabiedrībai pavēra piekļuvi dažādām mikroinvestīciju platformām un jauniem finanšu spekulāciju virzieniem.

Diemžēl daudzos gadījumos, uzsākot jaunas digitālās gaitas, iedzīvotājiem trūka pieredzes un zināšanu gan savu datu un finanšu aizsardzībā, gan uzticamas komunikācijas atpazīšanā. To centās nelaist garām krāpnieki, izmantojot plašu uzbrukumu spektru. Tika izkrāpti maksājumi, izmantojot viltus tirdzniecības vietnes un krāpnieciskas investīciju platformas, kā arī izgūti maksājumu karšu piekļuves dati, izmantojot viltus preču piegādes servisus vai zvanot no viltotiem numuriem un uzdodoties par bankas vai tiesībsargājošas organizācijas pārstāvjiem un draudot ar finansiāliem zaudējumiem vai sodiem par pārkāpumiem. Uzbrucēju rīcībā bieži vien bija informācija, kas ļāva veikt personalizētu uzbrukumu, piemēram, upura vārds, uzvārds, vecums, kontaktinformācija. Šie dati visbiežāk tika iegūti no publiski pieejamiem profiliem

sociālajos tīklos vai no dažādām datu noplūdēm, piemēram, *Facebook* vai *LinkedIn* ietotāju datu noplūdēm.

Krāpnieki arī pilnveidoja uzbrukumu metodes un sāka izmantot zvanītāja identitātes viltošanu krāpnieciskos telefona zvanos. Uzbrucēji viltoja banku telefona numurus un uzdevās par banku darbiniekiem, kā arī tie viltoja dažādu mobilo operatoru klientu numurus un zvanot uzdevās par tiesībsargājošu iestāžu pārstāvjiem, lai it kā brīdinātu zvana saņēmēju par viņa vārdā izdarītu pārkāpumu un piedraudētu ar sodu, ja netiks veiktas zvanītāju (krāpnieku) pieprasītās darbības.

Jaunā situācija radīja sašutumu un neizpratni, kad ļaunprātīgi izmantoto mobilo telefonu numuru lietotāji saņēma telefona zvanus no svešiniekiem ar pārmetumiem, kāpēc tie ir zvanījuši un rīkojušies tik nekrietni, kā arī būtiski apgrūtināja tiesībsargājošo iestāžu darbu. Lai arī izaicinājumiem bagāta, šīs problēmas sekmīga atrisināšana ir būtiska, lai neradītu drošības riskus un traucējumus zvanu centrāļu un glābšanas dienestu darbībā.

Latvijā tika konstatēti mēģinājumi izkrāpt personu apliecinošu dokumentu fotogrāfijas. Iegūtos attēlus var izmantot, lai reģistrētos citiem pakalpojumiem, piemēram, kriptovalūtu platformās, izmantojot upura identitāti un bez tā ziņas. Latvijas iedzīvotājiem, kļūstot par starptautisku pakalpojumu klientiem, paplašinās apdraudējumu loks, kuram viņi pakļauti, piemēram, kļūstot par globālu pikšķerēšanas un identitātes zādzību kampaņu mērķi. Kampaņas vairs nav nepieciešams pielāgot un atšķirīga valsts valoda vairs nav šķērslis.

Krāpnieki tīkoja arī pēc uzņēmumu sociālo tīklu kontiem, imitējot sociālo tīklu administrāciju. Tika izsūtīti draudīgi paziņojumi par noteikumu pārkāpumiem, lai izprovocētu kontu pārvaldniekus rīkoties steigā un pieņemt kļūdainus lēmumus, tai skaitā ievadīt konta piekļuves datus krāpnieku sagatavotā fiktīvā sociālā tīkla vietnē.

Tika saņemts ziņojums par incidentu ar inovatīvu raksturu – kādai videokonferencei pievienojusies persona, izmantojot svešu identitāti. Līdzīgi incidenti ar viltus personu pieslēgšanos videokonferencei tajā pašā laika posmā notikuši arī Lietuvā, Nīderlandē un Lielbritānijā, un tie uzskatāmi par vienotu kampaņu. Tiek pieņemts, ka uzbrucēji izmantojuši video attēla izmainīšanas

tehnoloģijas (*deepfake*). Prognozējams, ka nākotnē šādi uzbrukumi varētu notikt arvien biežāk, īpaši ņemot vērā videokonferenču augsto popularitāti un augošo video attēla apstrādes risinājumu pieejamību.

Informāciju par krāpnieciskām saitēm, kuras iesūtījuši iedzīvotāji un identificējusi CERT.LV, operatīvi tiek ievietotas CERT.LV un NIC.LV uzturētajā DNS ugunsmūrī https://dnsmuris.lv. Izmantojot DNS ugunsmūri iespējams veiksmīgi pasargāt tā lietotājus no uzbrukumiem. DNS ugunsmūris bez maksas ir pieejams ikvienam Latvijas iedzīvotājam, uzņēmumam, iestādei un organizācijai.

2.3. Ielaušanās mēģinājumi

Informācija par ielaušanās mēģinājumiem tika saņemta visa gada garumā, taču pietiekami zemā intensitātē. Šie uzbrukumi lielākajā daļā gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi veikti pret dažādiem interneta pakalpojumu sniedzējiem, valsts un pašvaldību iestādēm, kā arī privāto sektoru.

Lielākā uzbrucēju interese bija par attālinātajam darbam izmantotajām tehnoloģijām, tādām kā RDP (*Remote Desktop Protocol*), VPN (*Virtual Private Network*) un tiešsaistes sanāksmju un tērzēšanas platformām. Noziedznieki, pielietojot dažāda veida uzbrukumus, tajā skaitā jaunatklātas ievainojamības, uzstājīgi meklēja iespējas iekļūt uzņēmumu un organizāciju iekšējos tīklos, lai nesankcionēti piekļūtu sensitīvai informācijai vai nošifrētu iekārtas un pieprasītu maksu par datu atgūšanu.

Uzbrucēji ķērās arī pie sen zināmām konfigurācijas nepilnībām plaši lietotos produktos, piemēram, neierobežotas *Macros* izmantošanas *MS Office* programmatūrā. Primārais risinājums cīņai ar šādiem uzbrukumiem ir iekārtu konfigurācija atbilstoši labajai praksei, lietotāju izglītošana un sistēmu ievainojamību novēršana, sekojot līdzi atjauninājumiem.

2.4. Ļaundabīgs kods

Ļaunatūra arī 2021. gadā tika izplatīta galvenokārt diviem mērķiem – lai iegūtu datus vai gūtu peļņu. Informācijas izgūšanai banku, iestāžu un uzņēmumu vārdā kampaņveidīgi tika izplatīti e-pasti ar kaitīgiem pielikumiem. Atverot pielikumu, iekārta tika inficēta ar ļaunatūru, kas ievāc lietotājvārdus, paroles, kriptovalūtu maciņu un to piekļuves informāciju u.tml., lai nosūtītu to uz uzbrucēja kontrolētu serveri.

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. Šifrējošo vīrusu uzbrukumi tika piedzīvoti gan privātajā, gan publiskajā sektorā.

Svarīgi gan atzīmēt, ka visbiežāk pie nošifrētām sistēmām noveda nevis jaunatklātu ievainojamību izmantošana, bet gan nepietiekama resursu aizsardzība. Vājas paroles un novecojis programmnodrošinājums ar vairākus gadus publiski zināmām ievainojamībām, kuras bija iespējams novērst, savlaicīgi veicot programmatūras atjauninašanu. Atsevišķos gadījumos papildu veicinošais faktors vīrusa izplatībā bija nepārdomāts IT infrastruktūras plānojums.

Ļaunatūras izplatīšanai tika izmantota arī mazāk tradicionāla metode, ievietojot apmaksātu reklāmu *Google* meklētājā. Meklējot *AnyDesk* attālinātās pārvaldes programmu, šī reklāma tika parādīta kā pirmais rezultāts un aizveda uz ļaunatūru (trojāni) saturošu vietni. Uzbrucēji bija veikuši arī ļaunatūras kriptogrāfisku parakstīšanu, kas samazināja iespēju, ka sistēma brīdinās lietotāju par potenciālu apdraudējumu.

2.5. Kompromitētas iekārtas un datu noplūdes

Iekārtu kompromitēšanas gadījumi skāra gan iedzīvotājus, gan uzņēmumus, gan arī valsts un pašvaldību iestādes, taču lielākoties kompromitētās iekārtas bija maršrutētāji nelielos uzņēmumos vai individuālās mājsaimniecībās.

Uzbrukumu veikšanai tika izmantoti gan e-pasti ar ļaundabīgiem pielikumiem no jau kompromitētiem kolēģu vai sadarbības partneru kontiem, gan trūkumi dažādu IKT resursu aizsardzībā, kas izpaudās kā vājas paroles un novecojis programmnodrošinājums ar vairākus gadus publiski zināmām ievainojamībām.

Uzbrukumu mērķi – iegūt datus, manipulēt ar maksājumu informāciju, panākot maksājumu veikšanu uz uzbrucēju bankas kontiem, vai nošifrēt iekārtas, lai pieprasītu izpirkuma maksu par datu atgūšanu un, iespējams, nenopludināšanu.

Gada sākumā tika saņemta informācija par šifrējošā izspiedējvīrusa uzbrukumu uzņēmumam *Civinity* ar potenciāli 30 000 skartiem klientiem. Uzņēmums rīkojās atbildīgi un informēja klientus par iespējamu datu noplūdi. CERT.LV sniedza uzņēmumam nepieciešamo atbalstu, lai veicinātu incidenta ietekmes pārvarēšanu.

Vairāki Latvijas uzņēmumi cieta no iejaukšanās biznesa sarakstē (BEC), kurā uzbrucēji piekļuva uzņēmuma vai sadarbības partnera e-pasta kontam, lai pusēm izsūtītu viltotus rēķinus ar mainītu bankas kontu. Kopējais zaudējumu apjoms CERT.LV saņemtajos ziņojumos sasniedza gandrīz 500 000 eiro. CERT.LV aicināja uzņēmumus vienmēr, kad tiek veiktas izmaiņas finanšu datos, sazināties ar biznesa partneri, izmantojot citus komunikācijas kanālus, piemēram, piezvanot, un pārliecinoties par informācijas patiesumu.

Salīdzinoši jauns uzbrukumu mērķis bija kriptovalūtu maciņi kompromitētajās iekārtās un specializēti kriptovalūtu uzglabāšanas risinājumi. Vienā no incidentiem nodarīti materiālie zaudējumi 2 bitcoinu jeb gandrīz 100 000 eiro apmērā.

Pasaulē tika novēroti uzbrukumi piegādes ķēžu uzņēmumiem, kas aktualizēja drošības jautājumus arī Latvijā. Pastiprināta uzmanība kiberdrošības jautājumiem bija jāpievērš Latvijas uzņēmumiem, kuri nodrošina produkciju globālajam tirgum, jo šie uzņēmumi var kļūt potenciāli interesanti uzbrucējiem, lai piekļūtu uzņēmumu klientu iekārtām un infrastruktūrai. Līdzīga piesardzība jāievēro Latvijas uzņēmumiem un organizācijām, kuras izmanto ārvalstu IKT piegādātāju un uzturētāju sniegtos pakalpojumus, lai mazinātu uzbrukumu iespējamību, kas veikti, kompromitējot kādu no piegādes uzņēmumiem.

Realizējot plašas ietekmes piegāžu ķēdes integritātes uzbrukumu (*supply chain attack*), gada nogalē tika kompromitēta populārā *JavaScript* bibliotēka. Tā tiek plaši izmantota dažādos IT risinājumos , piemēram, lietotāja iekārtas parametru atpazīšanai. Uzbrukuma rezultātā miljoniem *Linux* un *Windows* iekārtu tika inficētas ar ļaunatūru, kas paredzēta paroļu pārtveršanai un nesankcionētai iekārtas resursu izmantošanai kriptovalūtu ieguvē. Šī *JavaScript* bibliotēka tiek izmantota arī *Facebook*, *Microsoft*, *Amazon, Instagram, Google, Slack, Mozilla, Discord, Elastic* un daudzu citu kompāniju produktos. CERT.LV aicināja pārbaudīt, vai sistēma nav kompromitēta, ja projektā tiek izmantota šī bibliotēka, kā arī sekot norādēm drošības pasākumu ieviešanā.

Kā svarīgu iekārtu un kontu aizsardzības mehānismu CERT.LV aicināja izmantot vairāku (2FA, MFA) faktoru autentifikāciju visur, kur tas vien ir iespējams. Kā papildu rīks apdraudējumu novēršanai izmantojams CERT.LV un NIC.LV piedāvātais DNS ugunsmūris https://dnsmuris.lv/, kurā operatīvi tiek iekļauta informācija par aktuālajiem apdraudējumiem un kuru bez maksas var lietot ikviens Latvijas iedzīvotājs, uzņēmums un organizācija.

2.6. Ievainojamības un konfigurācijas nepilnības

2021. gads bija jaunatklātām kritiskām ievainojamībām bagāts (*MS Exchange: CVE-2021-26855, MSHTML: CVE-2021-40444, Log4j: CVE-2021-44228, GlobalProtect: CVE-2021-3064* u.c.). Kritiskās ievainojamības sniedza uzbrucējiem iespēju veikt attālinātu koda izpildi, iegūstot piekļuvi ievainojamajai sistēmai. Veicot apdraudēto iekārtu apzināšanu Latvijas kibertelpā, tika konstatēts, ka valsts sektorā un pašvaldībās tika novērots manāmi zemāks kompromitēto iekārtu skaits, iespējams, pateicoties salīdzinoši ātrai un aktīvai komunikācijai ar CERT.LV par iespējamo apdraudējumu. Atsevišķu incidentu ietvaros tika novērots, ka valsts un pašvaldību iestāžu serveri tika atjaunināti nedēļas laikā, pretēji privātajam sektoram, kurā atklātās ievainojamības, pat pēc saziņas ar CERT.LV, serveros saglabājās vairākas nedēļas. Jāatzīmē gan, ka situācija nav unikāla tikai Latvijai, zināms, ka arī ārvalstīs privātais sektors ir kūtrāks kā valsts un pašvaldību iestādes.

CERT.LV apziņoja ievainojamo sistēmu turētājus valsts sektorā, kā arī sniedza atbalstu incidentu analīzē un novēršanā, atsevišķos gadījumos incidentu risināšanā piesaistot arī Zemessardzes Kiberaizsardzības vienību.

Tika aktualizēts viedo ierīču (IoT) drošības jautājums, izplatot brīdinājumus par vairākiem tūkstošiem ievainojamām apkures sistēmu un video novērošanas iekārtām. Ievainojamības sniedza uzbrucējiem iespēju attālināti pārņemt kontroli pār iekārtu, radot tiešu (atslēgta apkure) vai netiešu (iegūta informācija par to, vai objektā kāds uzturas) apdraudējumu īpašniekam. Brīdinājumu ietekmē Latvija elektroenerģijas piegādes uzņēmumu grupas un sakaru operatori uzsāka līdzīgu apkures iekārtu pārbaudes un trūkumu novēršanu.

Par visām ievērojamākajām ievainojamībām un ieteikumiem to novēršanai CERT.LV ar interneta pakalpojumu sniedzēju starpniecību regulāri informēja interneta lietotājus. Apdraudējumu informācija pieejama: 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. Tas ļauj CERT.LV aktīvi koordinēt ievainojamību novēršanu, tā labāk pasargājot Latvijas interneta telpu.

Pārskata periodā CERT.LV saņēma vairākus ziņojumus par atklātām ievainojamībām dažādos valsts un pašvaldību iestāžu resursos. Pateicoties ziņojumiem, vairākas valsts iestāžu tīmekļa vietnes tika pasargātas galvenokārt no starpvietņu skriptēšanas (XSS) uzbrukumiem. Tie veiksmīgas izpildes gadījumā sniegtu uzbrucējam iespēju veikt darbības lietotāja pārlūkā, piemēram, manipulēt ar vietnes saturu un sīkdatnēm vai izmantot pārlūkam piemērotus mūķus (*exploits*).

29. jūlijā tika publicēts pētījums par drošības problēmām, kas radās, elektroniski parakstot dokumentus ar dinamisku saturu. Apdraudējums nebija kritisks, taču tika ņemts vērā, jo elektroniskā paraksta joma sabiedrībā ir sensitīva.

Problēmu radīja elektroniskā paraksta sistēmas dizains, kas ir identisks praktiski visās pasaules valstīs. Lietotāja skatījumā elektroniskais paraksts apliecina ekrānā redzamo informāciju, taču tehniski tiek parakstīta datne, neiedziļinoties tās saturā. Populārākie datņu formāti .docx (*Microsoft Office*), .odt (*Libre Office*) un .pdf var saturēt dinamiskas daļas, kas var būt mainīgas no dokumenta atvēršanas reizes uz reizi, t.sk. dinamiski lejupielādējamas no interneta, piemēram, var mainīties summas, apjomi, atrunas, utt. LVRTC kā e-paraksta uzturētājs sadarbībā ar CERT.LV publicēja informāciju par atklāto ievainojamību un uzrunāja starptautisko CERTu kopienu, lai meklētu iespējas centralizētam risinājumam.

Arī 2022. gadā CERT.LV aicina ziņot par atklātām ievainojamībām, rakstot uz cert@cert.lv.

Vairāk par atbildīgu ievainojamību atklāšanu CERT.LV tīmekļa vietnē:
https://www.cert.lv/lv/par-mums/atbildiga-ievainojamibu-atklasana.

4.

Drošības testi

Drošības jeb 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. Informācijas sistēmu uzturētājiem CERT.LV sagatavoja pārskatu par veiktajiem testiem un to rezultātiem, kā arī sniedza ieteikumus nepilnību novēršanai.

5.

Informatīvie komunikācijas pasākumi


digiTuvi
KIBERDROŠĪBAS AKTUALITĀTES
#digiTuvi


esi drošs
IT drošība darba vietā - 2021
CERT.LV
CERT.LV 2021.gads


Latvijas
Digitālās inovā
centrs
ARMĪNS PALMS
KIBERDROŠĪBAS EKSPERTS CERT.LV
DIGITĀLAIS CILVĒKS


IKT RESURSU CENTRALIZĀCIJA| IZDEVĪGI, DROŠI, ĒRTI
#digiTuvi


RE!

CERT.LV ekspertu viedoklis arī 2021. gadā ir bijis plaši pieprasīts. Covid-19 pandēmijai zaudējot aktualitāti, publicitāte salīdzinājumā ar iepriekšējo gadu ir nedaudz pierimusi, samazinoties par 3,5%, tomēr salīdzinājumā ar iepriekšējiem gadiem tā joprojām ir augsta – piemēram, salīdzinājumā ar 2019. gadu 2021. gadā tā pieaugusi par 67,2%.

CERT.LV eksperti savu viedokli pauduši, sniedzot intervijas, komentārus, atbildes uz mediju jautājumiem TV, radio, drukātajos un tiešsaistes medijos par dažādām ar kiberdrošību saistītām aktuālām tēmām. Kopā CERT.LV izskanējis vairāk nekā 725 TV, radio, interneta portālu un drukāto mediju publikācijās – latviešu (75,1%), krievu (24,0%), angļu (1,0%) valodā.

Pārskata periodā mediju interesi piesaistīja kiberuzbrukumi, kas saistīti ar lietotāju datu vākšanas kampaņām (pikšķerēšanu), krāpnieciskām loterijām un telefonkrāpnieku zvaniem banku vārdā. CERT.LV ekspertu viedoklis visaktīvāk – 59,3% no visām publikācijām – ir pausts, kā ierasts, interneta portālos, 22,8% – radio, 7,8% – TV un 10,2% – drukātajos izdevumos.

CERT.LV uztur tīmekļa vietni www.cert.lv, kurā tiek publicēta informācija par aktuālajiem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. 2021. gadā vietnē publicētas 90 ziņas, no kurām ikmēneša, ceturkšņa un gada pārskati un ziņas ir 37,8%, savukārt brīdinājumi par krāpniecībām un ļaunatūrām – 21,1%, informatīvi paziņojumi – 22,2%, ieteikumi rīcībai – 8,9% un 10% par rīkotajiem pasākumiem. **Kopā gada laikā CERT.LV vietnei bijuši 82 073 apmeklējumi jeb sesijas, kuras veikuši 55 354 lietotāji.**

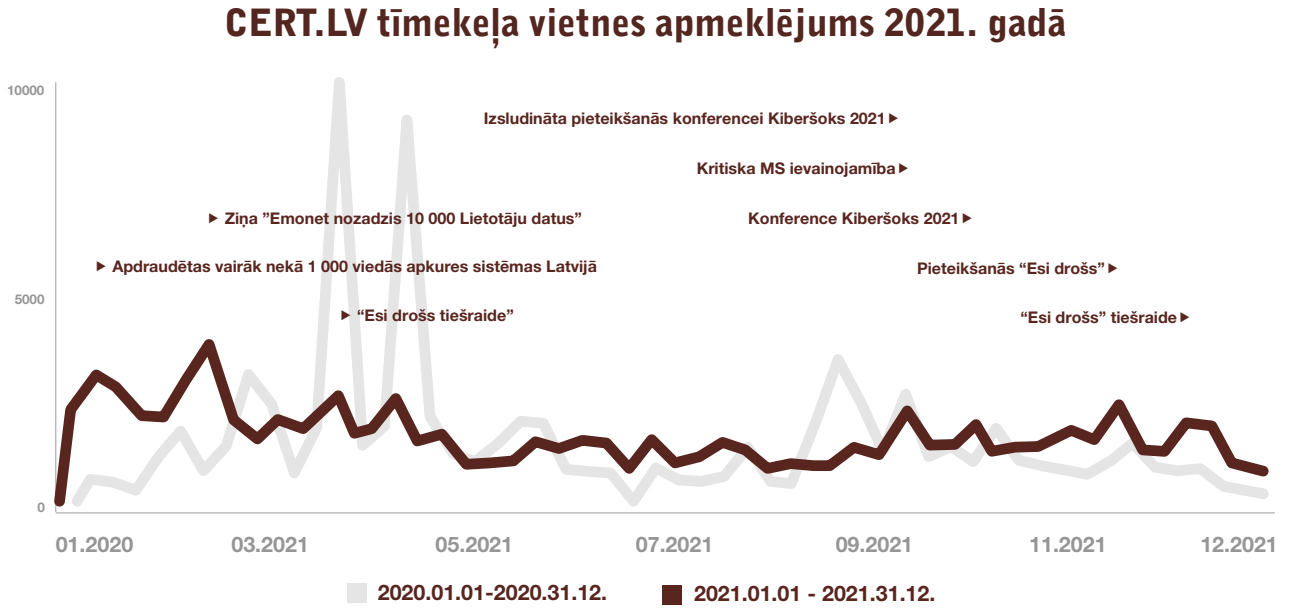
CERT.LV uztur arī lietotāju izglītošanas portālu www.esidross.lv, regulāri publicējot jaunus rakstus ar padomiem un ieteikumiem, kā lietotājiem drošāk darboties virtuālajā vidē. Portālam bija 44 699 apmeklējumi jeb sesijas, kuras veica 33 139 unikāli lietotāji.

Lai atvieglotu iniciatīvas *Atbildīgs interneta pakalpojumu sniedzējs* dalībnieku saziņu ar saviem 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 www.esidross.lv publicēja aktīvo apdraudējumu aprakstus https://www.esidross.lv/informacija-par-apdraudejumiem/.

Pārskata periodā katru mēnesi sadarbībā ar *SANS* institūtu tika izdoti un publicēti vietnē https://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 2022. 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:

- ***Twitter*** kontam *twitter.com/certlv* seko 3264 lietotāji
- ***Facebook*** profilam *facebook.com/certlv* – 4534 lietotāji
- ***YouTube*** kanālam seko 267 lietotāji.



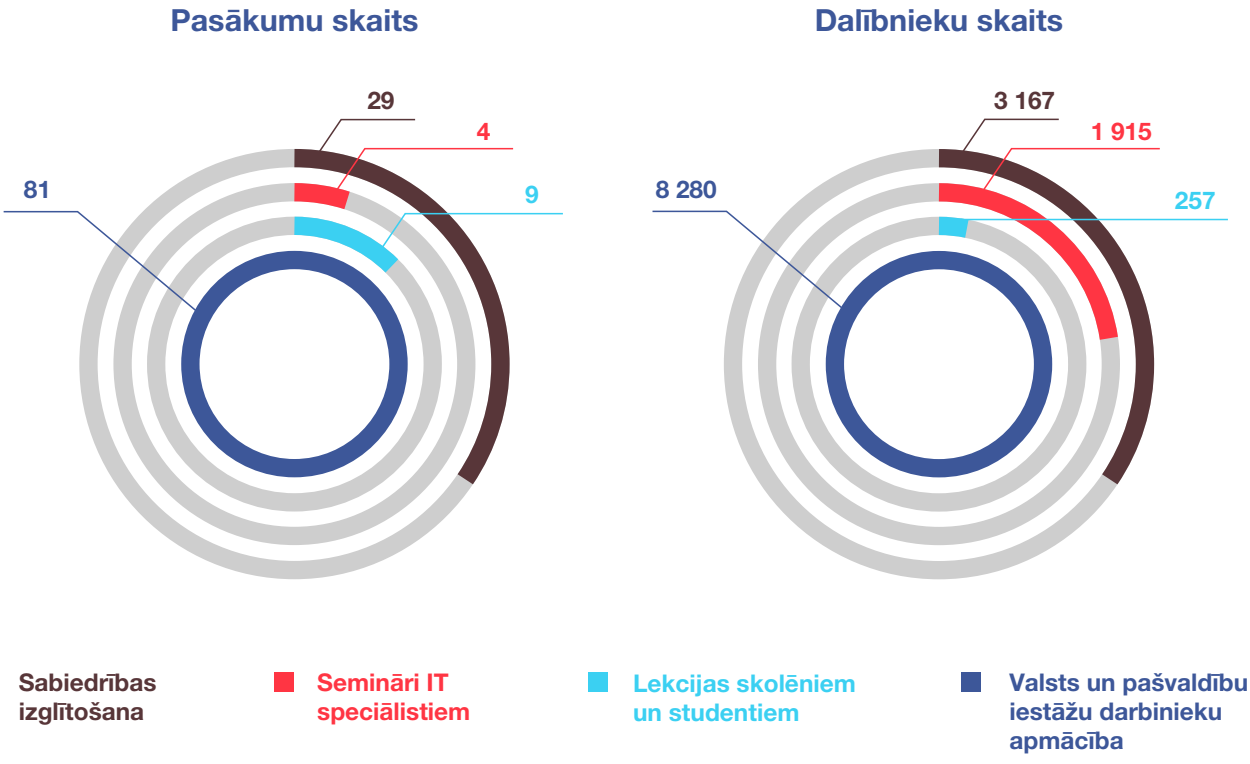
8. attēls – CERT.LV tīmekļa vietnes apmeklējums 2021. gadā.

6.

Izglītojošie pasākumi

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 123 pasākumos un izglītoja 13 619 dalībniekus.

Izglītojošie pasākumi 2021. gadā



9. attēls – Pasākumu un apmācīto cilvēku skaits 2021. gadā.

6.1. Starptautiskā kiberdrošības konference Kiberšoks 2021

Eiropas Kiberdrošības mēneša ietvaros 6.-7. oktobrī CERT.LV rīkoja tehnisko tiešsaistes konferenci kiberdrošības profesionāļiem *Kiberšoks 2021*, kurā starptautiski novērtēti eksperti dalībniekiem sniedza padziļinātu ieskatu plašā ar kiberdrošību saistītu jautājumu klāstā, prezentācijās iekļaujot arī reāllaika demonstrācijas. *Kiberšoks 2021* piedalījās 923 dalībnieki no 53 valstīm. Paralēli konferencei norisinājās arī CTF (*Capture the Flag*) sacensības, kurās dažādiem kiberdrošības izaicinājumiem pretī stājās 31 komanda. (https://cybershock.lv/).


2021
CS21


KT SERVISS


Cyber SHOCK
2021
47:18
Gil Biton
Offensive security engineer, Sygnia [IL]
Scaling up offensive pipelines
47:17
ON AIR
STOP
7.29
OK
SAMSUNG

From: Koichiro Komiyama (JPCERT/CC)
To: Baiba Kaskina
Date: Wednesday, September 15, 2021, 6:16:31 AM
Subject: [1st-news] Cybershock conference
6-7 October 2021 - invitation

===Original message text=========================
Baiba, The event page looks pretty cool! Is this
by a professional designer? Sparky

--
Koichiro Komiyama, Ph.D, CISSP / 小宮山 功一朗
Director, Global Coordination Division
Our latest activities on http://blogs.jpcert.or.jp

6.2. CERT.LV organizētie pasākumi IT drošības speciālistiem

Papildus starptautiskajai kiberdrošības konferencei *Kiberšoks 2021*, 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, kā arī video ieraksti publicēti CERT.LV *YouTube* kanālā.

Martā: *Esi drošs* seminārā dalībnieki tika iepazīstināti ar droša e-pasta tehnoloģiju ieviešanu, ES kiberdrošības stratēģiju un NIS2 direktīvu, *Solarwinds* incidenta apskatu, efektīviem autentifikācijas mehānismiem, *Emotet* otrā viļņa sakāvi, kā arī atskatu uz aktuālajiem notikumiem kibertelpā 2021. gada 1. ceturksnī.

Decembrī: Seminārā tika aplūkota kritiskās infrastruktūras darbības nepārtrauktības plānošana, kiberdrošības krīzes plāns un krīzes simulācijas, rezerves kopiju pareiza izveide un glabāšana, domēnu vārdi administratīvi teritoriālās reformas kontekstā, spēles izmantošana kiberdrošības apmācībās un atskats uz 2021. gada kiberdrošības notikumiem.

Augustā notika CERT.LV organizētais praktiskais tiešsaistes seminārs par pierādījumu apkopošanu pēc kiberincidenta, kurā tika aplūkota kiberincidentu izvērtēšana (triāža), pierādījumi un to vākšanas procedūra, kā arī sniegti praktiski padomi un demonstrācijas. Pasākumam tiešsaistē sekoja 280 dalībnieki.

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.

Nozīmīgākie pasākumi 2021. gada griezumā:

22. – 26. martā norisinājās Eiropas Digitālās nedēļas aktivitātes, kurās aktīvi piedalījās arī CERT.LV. 22. martā CERT.LV sadarbībā ar NIC.LV prezentācijā *Kā viegli nePAZAUDĒT naudu internetā* stāstīja uzņēmējiem par finansiālo drošību digitālajā vidē, kiberuzbrukumu veidiem, e-pastu viltošanu, domēna vārdu izmantošanu kiberuzbrukumos un biežāk pieļautajām lietotāju kļūdām (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/),
- *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-/) un
- 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/).

Septembra noslēgumā CERT.LV eksperti iesaistījās Latvijas Eiropas Kopienas studiju asociācijas (LECSA) vadītajā projektā CYBER.EU.VET, kura mērķis ir jauniešu un pedagogu izpratnes veicināšana un zināšanu pilnveidošana par kiberdrošības jautājumiem. Projekta ietvaros jauniešiem bija jāizveido spēle, kas palīdzētu sasniegt projekta mērķus. CERT.LV eksperti iepazīstināja jauniešus ar informāciju par aktuālajiem kiberapdraudējumiem, kā arī piedalījās vērtēšanas komisijā.

21. oktobrī Eiropas Kiberdrošības mēneša ietvaros SIA Tet rīkoja kiberdrošības forumu *CyberShield*, kura mērķis bija pievērst sabiedrības un uzņēmēju uzmanību virtuālajai drošībai, iedzīvinot kiberhigiēnas labāko praksi, analizējot aktuālākās tendences kibertelpā un aicinot ikvienu būt vērīgiem un ieguldīt enerģiju savu digitālo prasmju pilnveidē. CERT.LV pārstāvis forumā sniedza pārskatu par Latvijas un globālās kibertelpas aktualitātēm. (https://www.tet.lv/uznemumiem/vairak/forums-cybershield).

5. novembrī CERT.LV sadarbībā ar NIC.LV piedalījās *Zemgales uzņēmējdarbības centra* organizētajā seminārā uzņēmējiem *IT risinājumi biznesa attīstībai*, kurā iepazīstināja klausītājus ar ieteikumiem, kā atpazīt kiberuzbrukumus, un kā pasargāt gan savu uzņēmumu, gan domēna vārdu digitālajā vidē.

No 26.novembra pēc Aizsardzības ministrijas iniciatīvas CERT.LV organizēja piecus kiberdrošības seminārus Latvijas Republikas Saeimas deputātiem un viņu palīgiem par informācijas drošības pamatprincipiem un labo praksi.

CERT.LV pārstāvji piedalījās arī vairākos ar karjeru un izaugsmi saistītos pasākumos, stāstot jauniešiem par zināšanām un prasmēm, kas nepieciešamas, darbojoties kiberdrošības jomā, un potenciālajiem izaicinājumiem kibervidē.

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

CERT.LV turpināja tulkot un portālā https://www.esidross.lv publicēt informatīvi izglītojošu materiālu – SANS institūta sagatavoto ikmēneša drošības biļetenu *OUCH!*, kur apkopoti ieteikumi ikvienam datorlietotājam.

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 2021. gadā, kurās piedalījās CERT.LV:

- Konsultāciju sniegšana par IT drošības prasībām un to ieviešanu Veselības ministrijas un Nacionālā veselības dienesta (NVD) vadītā *Vakcinācijas projekta* IT risinājuma izstrādē.
- Dalība Iekšlietu ministrijas organizētajā Kritiskās infrastruktūras darba grupā, kurā tika izskatīta jaunā direktīva *Directive on the resilience of critical entities* (CER), kas paredz kritiskās infrastruktūras aizsardzību Eiropas mērogā, un citi jautājumi.
- Notika darbs pie jaunas Elektronisko sakaru likuma redakcijas, kurā tiktu iestrādātas arī Elektronisko sakaru kodeksa prasības. CERT.LV uzsvēra nepieciešamību spēt turpināt informēt gala lietotājus par visiem šo lietotāju iekārtās konstatētajiem apdraudējumiem, ne tikai par būtiskajiem, kā arī nepieciešamību saņemt ziņojumus ne tikai par pakalpojumu pieejamības traucējumiem, bet arī par būtiskiem incidentiem plašākā tvērumā. CERT.LV piedalījās arī ar Elektronisko sakaru likumu saistītu Ministru kabineta noteikumu izstrādē, savas kompetences ietvaros sniedzot komentārus par vēlamo rezultātu.
- Dalība sanāksmēs un komentāru sagatavošana Izglītības un zinātnes ministrijas vadītajā profesijas standarta *Informācijas drošības vadītājs* darba grupā. 11. augustā Profesionālās izglītības un nodarbinātības trīspusējās sadarbības apakšpadomes (PINSTA) sēdē tika pieņemts atbilstošais profesijas standarts.

- CERT.LV piedalījās Aizsardzības ministrijas informatīvā ziņojuma *Par valsts kiberdrošības pārvaldības uzlabošanu* sagatavošanā. Valsts kibertelpas stiprināšanai un ar kiberdrošību saistītu jautājumu koordinācijas nodrošināšanai, jo īpaši jaunā Eiropas Savienības regulējuma (NIS2 direktīvas) kontekstā, ziņojums paredz Nacionālā kiberdrošības centra izveidi.
- Uzsākta projekta vadība, kurā sadarbībā ar Latvijas Zinātnes padomi (LZP) trīs gadu periodā tiks veikts pētījums par valkājamo ierīču drošību. Pārskata periodā uzsākta automatizētu attālinātu sistēmu testēšana un veikta testējamā prototipa modeļa izstrāde.

Sniegti komentāri, ieteikumi un rekomendācijas:

- NIS2 Direktīvas priekšlikuma dokumentam;
- Par Digitālo pakalpojumu aktu un Digitālo tirgu aktu;
- Par nepieciešamajām izmaiņām Ministru kabineta noteikumos Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām*;
- Digitālās transformācijas pamatnostādnēm 2021.-2027. gadam;
- Par grozījumiem Ministru kabineta noteikumos Nr. 764 *Valsts informācijas sistēmu vispārējās tehniskās prasības* un Ministru kabineta noteikumos Nr. 71 *Valsts informācijas sistēmu attīstības projektu uzraudzības kārtība;*
- Latvijas kiberdrošības stratēģijai 2023.-2026. gadam.

CERT.LV aktīvi piedalās **Digitālās drošības uzraudzības komitejā** (DDUK), kuras darbību nosaka 2016. gada 1. novembrī apstiprinātie Ministru kabineta noteikumi Nr. 695. CERT.LV komitejas ietvaros turpināja darbu pie uzticamības pakalpojumu sniedzēju un kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzības, kā arī turpināja uzturēt Latvijas uzticamības pakalpojumu sniedzēju un uzticamības pakalpojumu sarakstu (*trust list*).

CERT.LV cieši sadarbojās ar Zemessardzes **Kiberaizsardzības vienību,** kas IT drošības krīzes vai apdraudējuma situācijā sadarbībā ar CERT.LV varētu sniegt atbalstu valstij un privātajam 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. 2021. gadā svarīgākā sadarbība notika, piedaloties kiberdrošības mācību *Locked Shields* norisē, kā arī iesaistot vienības pārstāvjus dažādu incidentu risināšanā.

Ikviens interesents – informācijas tehnoloģiju eksperts – tiek aicināts sniegt savu ieguldījumu valsts drošībā, pievienojoties Kiberaizsardzības vienībai. Papildu informācija par vienību un pieteikšanos Zemessardzes tīmekļa vietnē https://www.zs.mil.lv/lv/zemessardzes-vienibas/zemessardzes-kiberaizsardzibas-vieniba.

CERT.LV turpināja organizēt arī **Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupas (DEG) sanāksmes,** 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 https://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 https://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.

Sadarbība ar CERTu tīklu

NIS direktīvas CERTu sadarbības tīklu (NIS Computer Security Incident Response Team's Network) veido Eiropas Savienības dalībvalstu IT drošības incidentu novēršanas vienību (CERT) un CERT-EU pārstāvji, bet Eiropas Komisija tīklā darbojas kā novērotājs. Sadarbības tīkla izveidi noteica NIS direktīva. Direktīvas mērķis ir panākt vienoti augstu kiberdrošības līmeni ES dalībvalstu tīklos un informācijas sistēmās, paaugstinot katras valsts individuālo kiberdrošību, kā arī veicinot ES līmeņa sadarbību un risku vadību.

CERT.LV regulāri piedalījās 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.

2. – 3. jūnijā notikušajā NIS direktīvas CERTu tīkla sanāksmē CERT.LV sniedza prezentāciju *Trust Issues in Digital Signing*, aplūkojot dinamiskā satura aspektu parakstāmajos dokumentos.

1. oktobrī CERT.LV piedalījās ENISA rīkotajās Eiropas CERTu tīkla mācībās *CyberSOPex 2021*, lai paaugstinātu dalībnieku gatavību reaģēt liela apjoma pārrobežu incidenta gadījumā.

NIS CSIRTs Network ietvaros darbojas vairākas tematiskas darba grupas. Trijās 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;
- *Terms of Reference Review* darba grupa pārskata tīkla statūtus un nolikumu, atbilstoši tos aktualizējot.

Sadarbība FIRST ietvaros

FIRST ir globāls incidentu novēršanas un drošības komandu forums, un ļauj dalībniekiem efektīvāk risināt IT drošības incidentus, kā arī veikt preventīvus pasākumus. Tas ir uzticams sadarbības partneru tīkls, kas veido globālu incidentu novēršanas ekspertu kopienu.

CERT.LV ir aktīvs FIRST biedrs un piedalījās *FIRST Framework* darba grupā, 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 piedalījās arī FIRST konferences programmkomitejā, sniedzot atbalstu konferences programmas veidošanā.

Sadarbība TF-CSIRT ietvaros

TF-CSIRT (*The Task Force on Computer Security Incident Response Teams*) ir Eiropas mēroga CERTu sadarbības forums, kas veicina pieredzes apmaiņu un vienotu standartu un procedūru izmantošanu incidentu risināšanā, kā arī koordinē dažādas kopienas aktivitātes, kā piemēram, mācības vai jaunu CERT vienību izveidi. TF-CSIRT uztur arī uzticamu CERT vienību reģistru un veic vienību akreditāciju un sertifikāciju atbilstoši komandas demonstrētajam brieduma līmenim (*Trusted Introducer Service* jeb TI). CERT.LV kopš 2016. gada uztur sertificētas komandas statusu (uz pārskata perioda beigām reģistrā iekļautas 437 komandas, no kurām 40 ir sertificētas), kas apliecina CERT.LV komandas augsto brieduma un sagatavotības līmeni.

CERT.LV turpināja darbu *TF-CSIRT Futures* darba grupā, lai izstrādātu jaunu pārvaldības modeli *TF-CSIRT* un *Trusted Introducer* Eiropas CERTu sadarbībai. Darba grupas darbība tika noslēgta

2021. gada septembrī, jo darba grupas mērķi tika sasniegti – kā nākotnes modelis TF-CSIRT tika rekomendēts dibināt bezpeļņas organizāciju Nīderlandē. TF-CSIRT vadības grupa (*Steering Commitee)* turpinās darbu, lai šo rekomendāciju īstenotu.

CERT.LV vadīja TF-CSIRT starptautisko CERT komandu sabiedrisko attiecību speciālistu darba grupas (*CERTS PR Working Group*) sanāksmes, kuru ietvaros CERTu pārstāvji informēja par aktuālajiem izaicinājumiem kiberdrošības izpratnes veicināšanas jomā, dalījās pieredzē par izglītojošu kampaņu organizēšanu un sniedza ieteikumus veiksmīgākas komunikācijas organizēšanai.

Eiropas Savienības un ENISA iniciatīvas

CERT.LV piedalījās darba grupas *EU Cybersecurity Index Working Group* sanāksmēs, kurās tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija. Darba grupas mērķis ir ES dalībvalstu kiberdrošības līmeņa novērtēšana, lai noteiktu kopējo ES kiberdrošības līmeni, kā arī noteiktu pastāvošo noteikumu un vadlīniju ietekmi uz kiberdrošību un uz uzņēmumu darbību.

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 sniedz iespēju CERT.LV ekspertiem stiprināt savas zināšanas un kapacitāti.

CERT.LV piedalījās a ENISA (Eiropas Savienības kiberdrošības aģentūras) veiktajā pētījumā par ES dalībvalstu pieredzi ar medicīnas sektorā notikušu kiberdrošības incidentu ziņošanu, sniedzot informāciju par nacionālo praksi, normatīvo regulējumu, veiktajiem pasākumiem kiberdrošības pilnveidošanā un sadarbības stiprināšanā, kā arī informācijas plūsmu starp sektora pārstāvjiem, CERT.LV un Aizsardzības ministriju.

CERT.LV piedalījās arī ENISA pētījumā par ES dalībvalstu iedzīvotāju izpratnes veidošanu un stiprināšanu par kiberdrošības jautājumiem. Pētījuma mērķis ir iegūt informāciju par dažādu valstu pieredzi iedzīvotāju izpratnes veicināšanā, apzināt izaicinājumus un apkopot ieteikumus par

efektīvākajām metodēm. Pētījuma rezultāti tiks apkopoti dokumenta formā un tiks izplatīti visu dalībvalstu pārstāvjiem.

3. decembrī CERT.LV piedalījās Eiropas Kiberdrošības kompetences centra (*European Cyber security Competence Centre*, ECCC) sanāksmē par SOC (*Security Operation Centres*) idejas tālāku virzību, lai veicinātu Eiropas līmeņa informācijas apmaiņu par aktuālajiem apdraudējumiem kibertelpā saskaņā ar ES Kiberdrošības stratēģiju.

7. decembrī CERT.LV piedalījās ENISA organizētajā sanāksmē par apvienotās kiberdrošības vienības (*Joint Cyber Unit*, JCU) veidošanu. Valstu pārstāvji piedalījās diskusijā, daloties pieredzē, informējot par līdz šim izmantotajiem rīkiem un uzsāktajiem projektiem, lai sekmētu vienības izveidi ar skaidri definētiem uzdevumiem un darbības principiem. Vienības mērķis ir sekmēt koordinētu Eiropas līmeņa atbildes reakciju apjomīga kiberdrošības apdraudējuma gadījumā.

Sadarbība ar NATO dalībvalstīm

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* organizēšanā un nodrošināšanā.

13. – 16. aprīlī notika pasaulē lielākās un sarežģītākās ikgadējās starptautiskās reālā laikā notiekošās kiberaizsardzības mācības ***Locked Shields***, kuras organizēja NATO CCDCoE. Latvijas komanda īstenoja līdz šim nepieredzētu starpreģionālu sadarbību, piedaloties mācībās Latvijas – Korejas Republikas apvienotajā komandā. Covid-19 pandēmijas apstākļos apvienotās komandas darbs tika koordinēts attālināti, sekmīgi pārvarot izaicinājumus, kurus sagādāja būtisko laika zonu un valodu atšķirības. Šāda starpreģionālas apvienotās komandas pieredze sniedza iespēju attīstīt abu nāciju kiberspējas un pilnveidot kā iekšējo, tā ārējo sadarbību.

CERT.LV piedalījās NATO CCDCoE ikgadējo tehnisko sarkano komandu kiberdrošības mācību ***Crossed Swords*** *2021* plānošanā, notika darbs pie mācību vides tehnisko elementu izstrādes,

mācību izpildes koordinācija un industriālo vadības sistēmu uzbrukuma scenārija vadīšana. Mācības paredzētas ne tikai ielaušanās testētāju, digitālās kriminālistikas un apdraudējumu ekspertu tehnisko prasmju pilnveidei, bet arī vadītprasmju papildināšanai. CERT.LV pārstāvis piedalījās arī mācību izspēlē, kas notika **7.-9. decembrī**, vadot vienu no mācību komandām. Mācībās piedalījās gandrīz 100 dalībnieki no 21 valsts.

No 31. maija līdz 4. jūnijam CERT.LV piedalījās NATO Enerģētikas drošības ekselences centra (NATO ENSEC CoE) un Eiropas Komisijas Kopīgā pētniecības centra organizētajās teorētiskajās (tabletop) kiberdrošības mācībās ***The Coherent Resilience 2021 Baltic*** (*CORE 2021-B*), kuru mērķis bija veicināt un pilnveidot kritiskas enerģētikas sektora infrastruktūras kiberdrošību Baltijas valstīs.

No 29. novembra līdz 3. decembrim CERT.LV piedalījās NATO organizētajās kiberdrošības mācībās ***Cyber Coallition 2021***. Mācību mērķis ir veicināt sadarbību – alianses dalībnieku un partneru veiktās aktivitātes tika vērstas uz kopīgu mērķu sasniegšanu, lai tā pilnveidotu spējas novērst un atvairīt apdraudējumus kibertelpā un sniegtu ieguldījumu alianses izaugsmē. Mācībās piedalījās 1000 dalībnieki, kas pārstāvēja 30 NATO sabiedrotos, vairākus partnerus un Eiropas Savienību.

Citas starptautiskās aktivitātes

CERT.LV piedalījās enerģētikas informācijas apmaiņas un sadarbības grupas ***Energy ISAC Camelot*** sanāksmēs, lai veicinātu informācijas apmaiņu un sekmētu enerģētikas sektora kiberdrošību. Grupas ietvaros tika prezentēta CERT.LV izveidotā industriālo iekārtu izpētes laboratorija, kas tika ļoti atzinīgi novērtēta.

CERT.LV sniedza atbalstu Kanādai piemērotākā koordinētas ievainojamību atklāšanas modeļa izvēlē, piedaloties seminārā *Coordinated Vulnerability Disclosure*, kuru organizēja Kanādas valdības pārstāvji, lai apkopotu informāciju par atbildīgas ievainojamību atklāšanas procesiem un citu valstu pieredzi. Diskusiju rezultātā tapa dokuments *See Something, Say Something. Coordinating the Disclosure of Security Vulnerabilities in Canada*, lai veicinātu publiskā sektora informācijas tehnoloģiju drošību, sniedzot ietvaru ārējo drošības pētnieku un publiskā sektora sadarbībai.

8. septembrī CERT.LV uzņēma Igaunijas kolēģu delegāciju no RIA un CERT-EE, lai veicinātu pieredzes apmaiņu sarežģītu incidentu risināšanā, efektīvākā rīku un risinājumu izmantošanā, preventīvajos pasākumos un sabiedrības informēšanā.

9.

ES līdzfinansētu projektu 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 *Cyber Exchange*) īstenošana.

Projekta mērķis ir stiprināt starptautisko sadarbību starp nacionālajām un valdības CERTu 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 CERT komandām vai uzņemot vizītē kolēģus no citām CERT vienībām.

Projekta ietvaros CERT.LV pārstāvis pieredzes apmaiņas vizītē devās uz Poliju, kur tika apskatīta un analizēta pikšķerēšanas incidentu automatizācija, kā arī iepazīti citi incidentu automatizācijas rīki un CERT.PL pieredze kiberdrošības incidentu apstrādē. Vizītes rezultātā tika uzlabotas attiecības starp CERT.LV un CERT.PL komandām, kas ir ļoti noderīgi gan ikdienas sadarbībai, gan kopīgu projektu un aktivitāšu īstenošanai.

Covid-19 ierobežojumu ietekmē projekta termiņš tika pagarināts līdz 2022. gada 30. jūnijam.

2021. gada 1. jūlijā CERT.LV uzsāka *2020 CEF Telecom Call – Cybersecurity* uzsaukumā apstiprinātā projekta ***Joint Threat Analysis Network (JTAN)***, līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2020/2373165, īstenošanu.

Projekta vadošais partneris ir Informācijas tehnoloģiju drošības incidentu novēršanas institūcija Polijā CERT.PL, kas darbojas institūta *Naukowa i Akademicka Sieć Komputerowa* (NASK) struktūrā. JTAN projektā piedalās arī partneri no Austrijas, Francijas, Igaunijas, Luksemburgas, Rumānijas un Slovākijas. Kopējais JTAN projekta mērķis ir izveidot vienotu apdraudējumu analīzes tīklu (*Joint Threat Analysis Network* – JTAN). CERT.LV galvenā iesaiste šajā projektā saistīta ar *Graphoscope* rīka izstrādi un attīstīšanu.

2021. gadā CERT.LV darbojās pie *Graphoscope* izstrādes, attīstīšanas un pilnveidošanas.

2021. gada 9. decembrī tika publicēta *Graphoscope* atvērtā koda licence, lai arī citi projekta partneri varētu rīku testēt, novērtēt un sniegt priekšlikumus uzlabojumiem. Rīks publiski pieejams https://github.com/cert-lv/graphoscope. Pārskata periodā CERT.LV piedalījās attālinātās JTAN projekta sanāksmēs.

Graphoscope ir rīks, kas paredzēts, lai korelētu datus no dažādiem datu avotiem un parādītu tos vizuālā formā. Kā datu avotu var izmantot arī rīku *Pastelyzer*, kas tika izstrādāts iepriekšējā Eiropas finansētajā projektā (*Improving Cyber Security Capacities in Latvia*, 2017-LV-IA-0058). Galvenās *Graphoscope* iezīmes: 1) atbalsts daudziem datu avotiem; 2) tīmekļa bāzēta saskarne, kas nav atkarīga no iepriekš instalētām datu bāzēm; 3) vienkārša sistēmas uzstādīšana; 4) saskarne nodrošina elastīgu filtrus, kas atvieglo liela apjoma datu analīzi.

JTAN projekta īstenošana plānota līdz 2024. gada 30. jūnijam.

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 projekta attīstīšanas. Kā minēts iepriekš, risinājums sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā, kas saistīts ar kiberdrošības institūcijām jau zināmiem incidentu identifikatoriem (domēna vārdi, IP adreses u.c.). Jebkurš Latvijas interneta lietotājs (kā privātpersonas tā organizācijas) var izmantot DNS PRZ pakalpojumu bez līguma slēgšanas un autorizēšanās. Lai to izmantotu, jālieto NIC.LV rekursīvie DNS serveri. Vairāk informācijas un detalizētas instrukcijas pieejamas vietnē https://dnsmuris.lv.

Vairāk nekā 50 000 apturētu potenciālo kiberincidentu 2021. gadā!

DNS ugunsmūris

CERT.LV uzsāka sarunas ar vairākiem interneta pakalpojumu sniedzējiem (IPS), ar kuriem noslēgts sadarbības memorands *Atbildīgs IPS*, par DNS RPZ zonu piedāvāšanu pakalpojuma sniedzēju klientiem. Notika arī kopīga sanāksme ar Sabiedrisko pakalpojumu regulēšanas komisiju, lai vienotos par šādas sadarbības iespējamību no regulatora skatu punkta.

Agrās Brīdināšanas Sistēma (ABS): agrās brīdināšanas sensors ir pasīva drošības iekārta, kas ļauj apzināt apdraudējumus un izmeklēt incidentus. 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. Par ABS uzstādīšanu tiek slēgts sadarbības līgums. Pakalpojums primāri pieejams kritiskās infrastruktūras organizācijām, 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.

Uzstādīts jauns **publiskais pirmā līmeņa (Stratum 1) NTP laika serveris.** Serveris saņem precīzu laiku no GPS, un tajā ir iebūvēts oscilators, kura kļūda ir ne vairāk kā 1.6s gada laikā. Līdz ar jauno serveri CERT.LV nodrošina kopā 3 publiskos NTP serverus, no kuriem divi ir pirmā līmeņa un viens – otrā līmeņa serveris. Visi serveri ir pievienoti Latvijas NTP serveru kopai “lv.pool.ntp.org”. CERT.LV rekomendē izmantot šo kopu kā precīzā laika avotu.

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