Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2020 C3

Publiskais pārskats par CERT.LV uzdevumu izpildi

2020. gada 3. ceturksnis (01.07.2020 – 30.09.2020.)

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

Saturs

Kopsavilkums

2020. gada 3. ceturksnī tika reģistrētas 159 019 unikālas apdraudētas IP adreses, kas ir par 20% mazāk nekā iepriekšējā ceturksnī un par 21% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (76 976 unikālas IP adreses) ar kritumu par 32% pret iepriekšējo periodu;
- otrs izplatītākais bija ļaundabīgs kods (14 036 unikālas IP adreses) ar kāpumu par 100%;
- bet trešais – ielaušanās mēģinājumi (1953 unikālas IP adreses) ar kritumu 12%.

Kāpums ļaundabīgā koda apjomā skaidrojums ar vairāku informācijas avotu pastiprinātu uzmanības pievēršanu noteiktām ļaunatūru grupām, kas, savukārt, noveda pie palielinātas ienākošo datu plūsmas, kas saistīta ar ļaundabīgo programmatūru.

Pārskata periodu iezīmēja intensīva *Emotet* spiegojošās ļaunatūras izplatība, kas skāra vairākus simtus uzņēmumu un organizāciju Latvijā. Ļaunatūra ne tikai iegūst dažādu sistēmu un iekārtu piekļuves datus no upura iekārtas, bet arī instalē iekārtā papildu ļaunatūras un nokopē upura kontaktu sarakstu un e-pastu saraksti, nosūtot šo informāciju uz saimniekserveri vēlākai izmantošanai. Pārtvertie e-pasti var saturēt arī sensitīvu informāciju.

Visa perioda garumā tika novērota arī intensīva telefonkrāpnieku aktivitāte, kuri, izmantojot viltotus telefona numurus un uzdodoties par banku vai Smart-ID darbiniekiem, parasti krievu, bet

dažos gadījumos nu jau arī latviešu valodā, zvanīja lietotājiem un, izmantojot lietotāju nezināšanu un izpratnes trūkumu par izmantoto drošības mehānismu darbību, lūdza nosaukt klientu norēķinu karšu datus, internetbankas datus (lietotāja numurs un paroli) vai Smart-ID kodus. Uzbrukumos cietuši vairāki tūkstoši lietotāju, kopējam zaudējumu apmēram sasniedzot vairākus simtus tūkstošu eiro.

Gan Eiropā, gan arī Latvijā uzņēmumi piedzīvoja naudas izspiešanas mēģinājumus, uzbrucējiem draudot apturēt uzņēmuma mājas lapu vai citu resursu, kas nodrošina uzņēmuma darbību, ar piekļuves atteices (DDoS) uzbrukumu līdz pat 2 Tb/s. Uzbrukumu mērķi bija gan finanšu institūcijas, gan citi privātā sektora uzņēmumi. Testa uzbrukumi ilga no nepilnas stundas līdz pāris dienām un sasniedza līdz pat 100 Gb/s, dažiem upuriem radot darbības traucējumus. Ieviešot labās prakses standartu BCP-38 vismaz Eiropas līmenī, būtu iespējams rast risinājumu DDoS uzbrukumu problēmai, novēršot iespēju izsūtīt tīkla paketes ar viltotu paketes avotu (IP *spoofing*), kas ir lielākās daļas DDoS uzbrukumu pamatā. Tas ļautu samazināt arī resursu uzturēšanas izmaksas uz DDoS aizsardzības risinājumu rēķina.

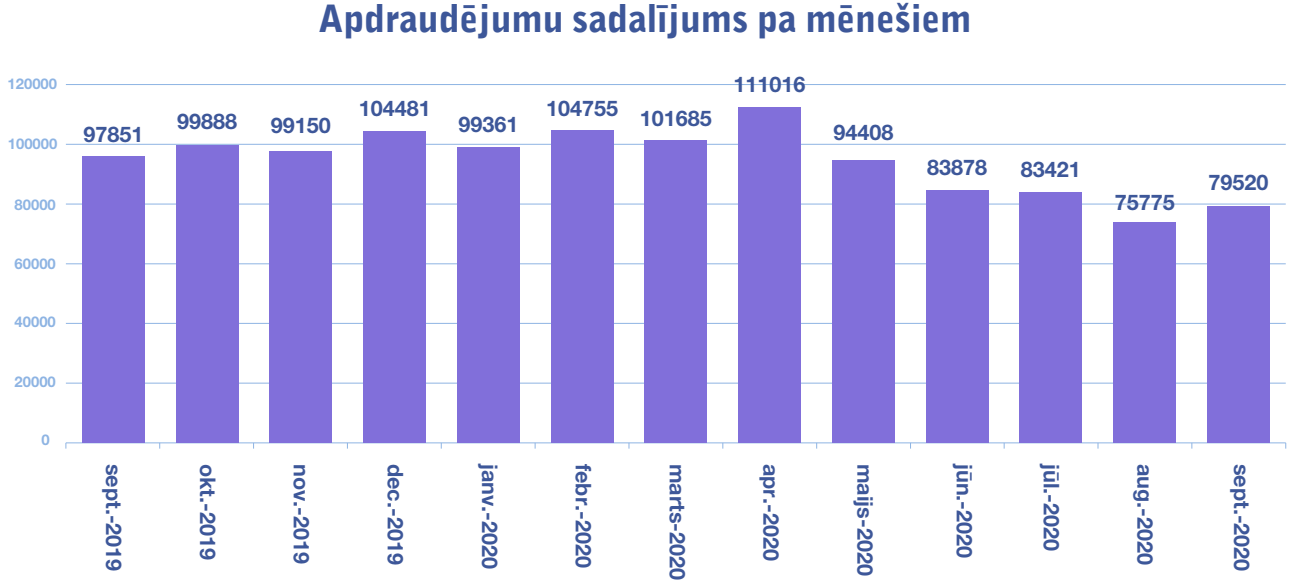
14. septembrī CERT.LV ar Eiropas Savienības līdzfinansējumu uzsāka mēnesi ilgu informatīvi izglītojošu kampaņu par kiberdrošību darbavietā. Kampaņa galvenokārt vērsta uz to, lai veicinātu valsts un pašvaldību darbiniekos izpratni par kiberhigiēnas principiem, kā arī spēju atpazīt un novērst iespējamo kiberuzbrukumu. 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.

Pārskata periodā CERT.LV par IT drošību izglītoja 915 cilvēkus, iesaistoties 9 izglītojošos pasākumos. Ņemot vērā epidemioloģisko situāciju valstī, lielākā daļa pasākumu notika tiešsaistē.

1. Elektroniskās informācijas telpā notiekošo darbību atainojums

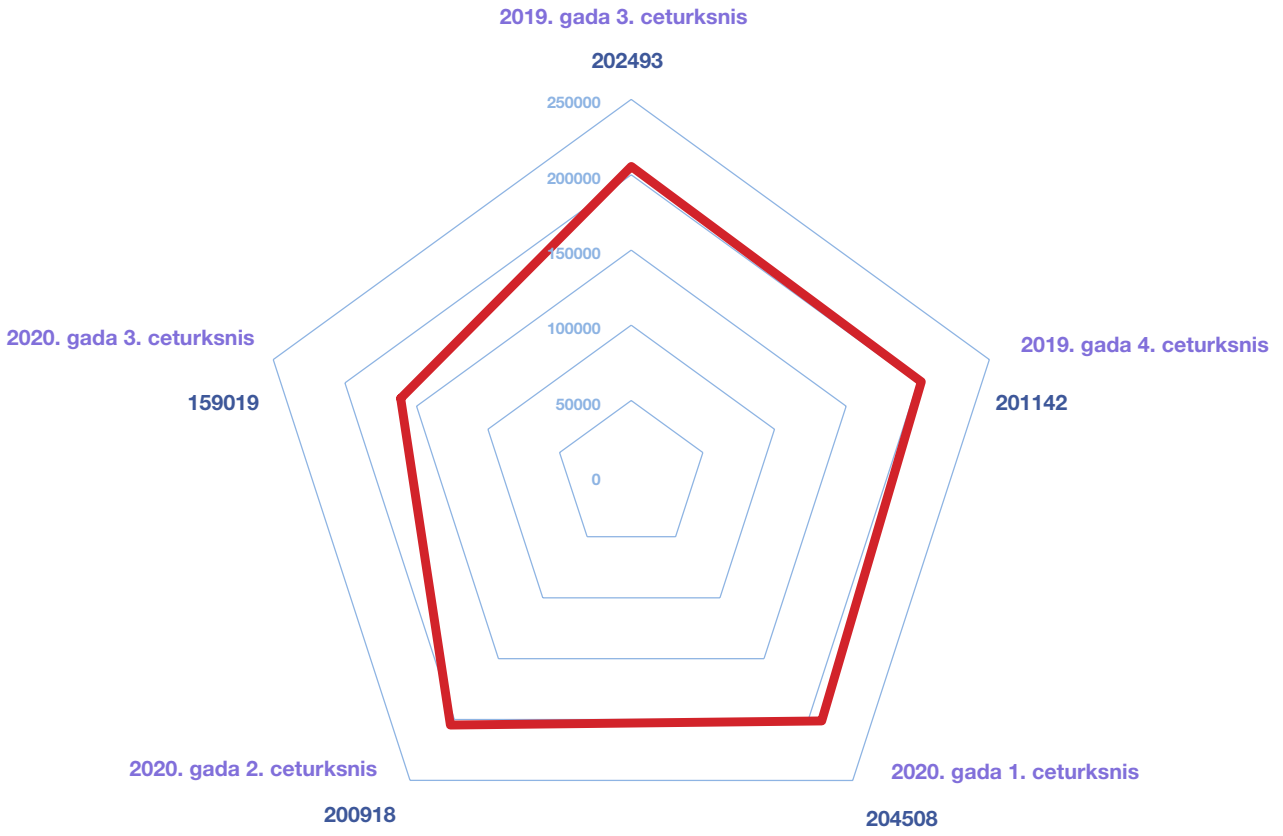
Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Lai sniegtu pilnvērtīgāku Latvijas kibertelpas pārskatu un nodrošinātu datu starptautisku salīdzināmību, CERT.LV apdraudējumu uzskaitei izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija,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

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju vidēji par 75 000 – 80 000 ievainojamu unikālu IP adrešu.



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

Apdraudējumu sadalījums pa ceturkšņiem



2. attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2019. un 2020. gadā.

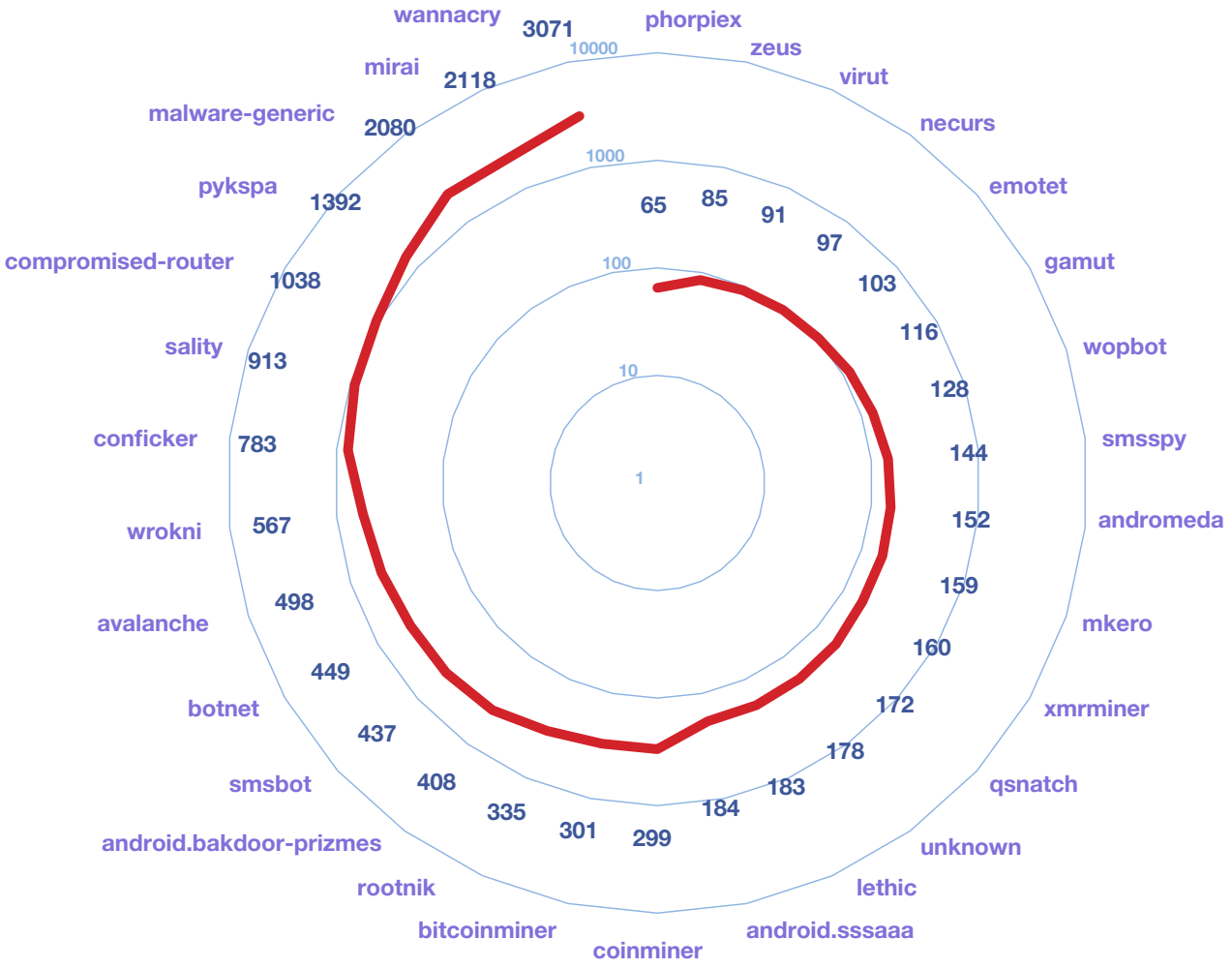
2020. gada 3. ceturksnī tika reģistrētas 159 019 unikālas apdraudētas IP adreses, kas ir par 20% mazāk nekā iepriekšējā ceturksnī un par 21% mazāk nekā šajā pašā periodā pirms gada.

Kopējo apdraudēto unikālo IP adrešu kritumu izraisīja svārstības ienākošo datu plūsmā, ko par Latvijas IP adresēm CERT.LV saņem no sadarbības partneriem. Tas, diemžēl, vienozīmīgi nenorāda uz kibertelpas kopējās drošības situācijas strauju uzlabošanos.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (76 976 unikālas IP adreses) ar kritumu par 32% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (14 036 unikālas IP adreses) ar kāpumu par 100%, bet trešais — ielaušanās mēģinājumi (1953 unikālas IP adreses) ar kritumu 12%.

3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 3. ceturksnī pa apdraudējumu veidiem.

Unikālo IP adrešu skaits – ļaundabīgs kods 2020. gada 3. ceturksnī



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 3. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

Ļaunatūras pieaugums, kas tika novērots, neskatoties uz kopējo ienākošo datu apjoma kritumu, skaidrojams ar pastiprinātu uzmanību, kuru informācijas avoti pārskata periodā pievērsa virknei ļaunatūru. Rezultātā palielinājās konkrētām ļaunatūrām veltītais informācijas apjoms, kā arī palielinājās ļaunatūru proporcija kopējā ienākošo datu plūsmā.

Pēc vairāku mēnešu pārtraukuma topā atgriezusies *WannaCry* (*WannaCrypt*) – ļaunatūra ar šifrējošo potenciālu. Šīs ļaunatūras izplatība vērojama galvenokārt privātajā sektorā. Izplatību iespējams novērst, uzstādot *Windows* iekārtu atjauninājumus.

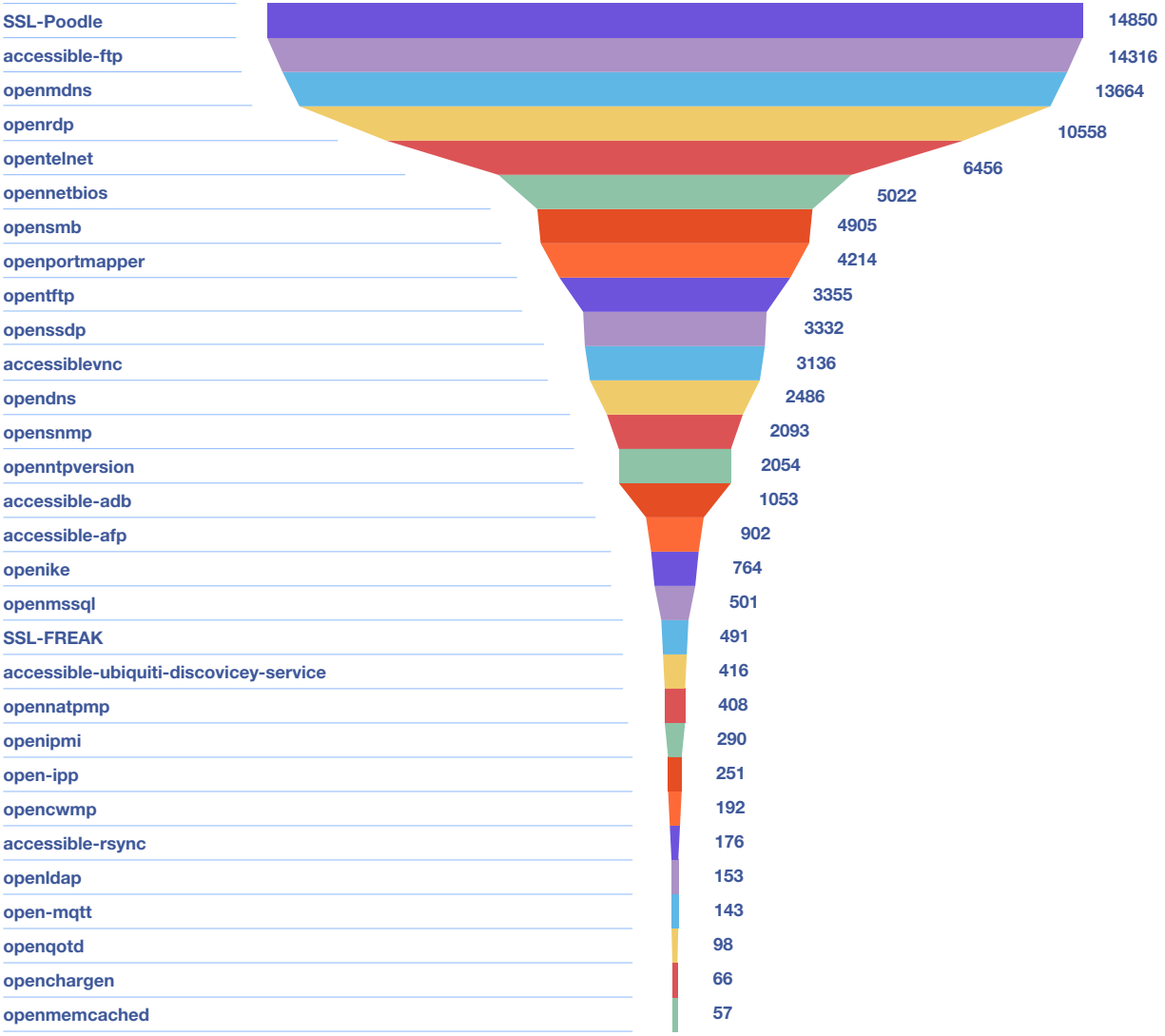
Nemainīgi topa augšgalā atrodas *Mirai* – ļaunatūra, kas inficē un iekļauj robotu tīklos jeb *botnetos* lietu interneta (IoT) iekārtas, lai izmantotu tās tālākiem uzbrukumiem un citām pretlikumīgām darbībām. Par uzbrucēju upuriem parasti kļūst iekārtas, kuras pēc iegādes pieslēgtas internetam, nenomainot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

Ļaunatūra *Conficker* joprojām atrodas topa augšgalā, kaut ir sen zināma un viegli ārstējama – nepieciešams veikt iekārtu atjauninājumus. *Conficker* plašā izplatība, iespējams, norāda uz internetam pieslēgtām novecojušām iekārtām, kurām vairs netiek nodrošināti atjauninājumi. Šādu iekārtu izmantošana pakļauj infrastruktūru un datus pastiprinātam uzbrukumu riskam.

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

Konfigurācijas nepilnība, kas ieņem trešo vietu, ir *OpenmDNS* (*multicast DNS*). Papildus tam, ka šīs iekārtas tiek pakļautas liela apjoma informācijas noplūdes riskam, tās var tikt izmantotas UDP amplifikācijas uzbrukumos, radot piekļuves traucējumus citām iekārtām un organizāciju resursiem.

Unikālo IP adrešu skaits - konfigurācijas nepilnības 2020. gada 3. ceturksnī



5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2020. gada 3. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

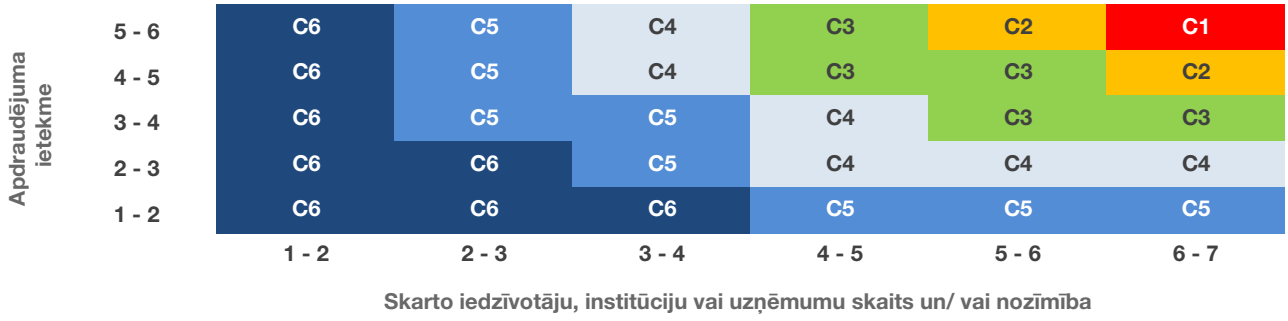
Arī konfigurācijas nepilnība *OpenRDP* pārskata periodā joprojām atrodas topa augšgalā. Tā bieži tiek izmantota, lai piekļūtu iekārtām un tās sašifrētu. Ja netiek ievērota labā prakse un netiek ierobežota piekļuve RDP servisam, piemēram, ierobežojot IP adreses, kurām atļauts pieslēgties, vai nosakot piekļuvi caur VPN, uzbrucējs var pārņemt kontroli pār neatbilstoši konfigurētām iekārtām, kurās attālinātās piekļuves porti ir brīvi atvērti uz internetu un nav uzstādīta pietiekami droša piekļuves parole.

Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV pirmajā ceturksnī ir uzsākusi Apvienotās Karalistes Nacionālā kiberdrošības centra (NCSC) izveidotās apdraudējumu matricas adaptāciju. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai cik plašu sabiedrības daļu apdraudējums ietekmē, kā arī pēc tā, cik būtiskas sekas attiecīgais apdraudējums radīs.

Apvienojot abus faktorus, apdraudējumi tiek iedalīti 6 kategorijās:

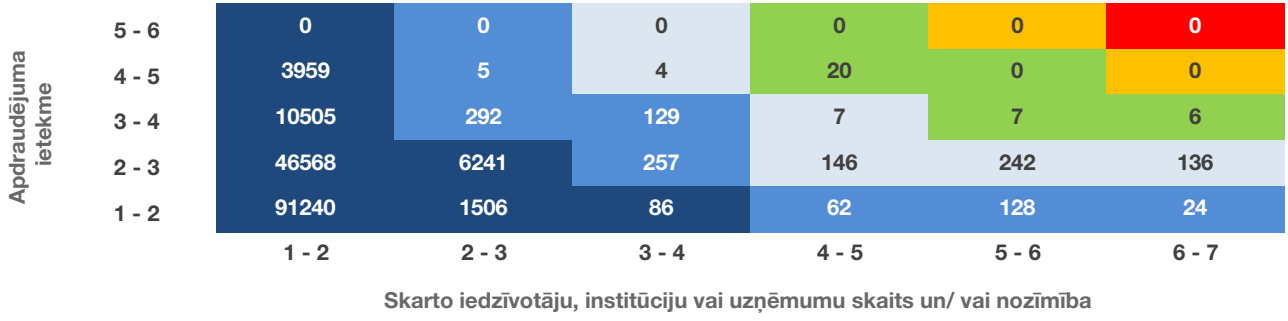
- C1 – nacionāla līmeņa apdraudējums, ietekmēta pamatpakalpojumu sniegšana, apdraudēta ekonomiskā vai politiskā stabilitāte;
- C2 – augstas nozīmes apdraudējumi, ietekmētas valsts iestādes, nacionālā infrastruktūra;
- C3 – nozīmīgi apdraudējumi, plaša ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm;
- C4 – būtiski apdraudējumi, vidēja ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm;
- C5 – mēreni apdraudējumi, neliela ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm;
- C6 – ikdienas apdraudējumi, ietekmē atsevišķus indivīdus, nenozīmīga ietekme uz uzņēmumiem vai valsts un pašvaldību iestādēm.

Apdraudējumu matrica



6. attēls – Apdraudējumu matricas sadalījums kategorijās.

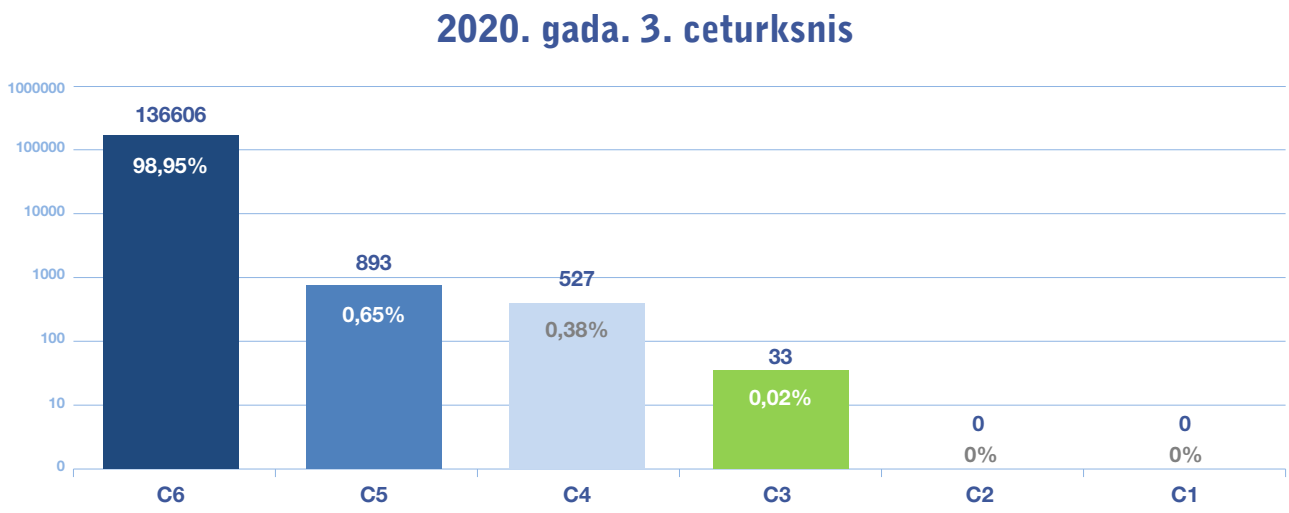
2020. gada. 3. ceturksnis



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2020. gada 3. ceturksnī valsts un pašvaldību institūcijās.

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

Nacionāla līmeņa apdraudējumi (C1) un augstas nozīmes apdraudējumi (C2) pārskata periodā nav reģistrēti. Nozīmīgi plašas ietekmes apdraudējumi (C3) veido 0,02% (33 unikālas apdraudētas



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2020. gada 2. ceturksnī valsts un pašvaldību institūcijās.

IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. Lielākā daļa šo apdraudēto IP adrešu saistītas ar ļaundabīgu kodu valsts un pašvaldību iestādēs, kā arī vairākās valsts kapitālsabiedrībās. Tās ir galvenokārt ļaunatūra *WannaCry* ar šifrējošo potenciālu, spiegojošā ļaunatūra *Emotet* un ļaunatūra *Sality* ar *backdoor* funkcionalitāti, kas paver ceļu uz iekārtu citām ļaunatūrām, kā arī pievieno inficētās iekārtas robotu tīklam.

Lielākā daļa C4 līmeņa incidentu (būtiski apdraudējumi ar vidēju ietekmi) bija konfigurācijas nepilnības (*Accessible-ftp*, *OpenRDP*, *Openntpversion*, *OpenDNS*, *Openike*, uc), ielaušanās mēģinājumi un vidējas ietekmes ļaundabīgs kods (*Avalanche*, *Kelihos* u.c.), kas novēroti augstas un vidēji augstas prioritātes iestādēs, virknē pašvaldību un vairākās universitātēs.

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

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

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

2.1 Krāpšana

Visa perioda garumā tika novērota paaugstināta telefonkrāpnieku aktivitāte, kas, izmantojot viltotus numurus un uzdodoties par banku vai Smart-ID darbiniekiem, parasti krievu, bet dažos gadījumos nu jau arī latviešu valodā, zvanīja lietotājiem un, izmantojot lietotāju nezināšanu un izpratnes trūkumu par izmantoto drošības mehānismu darbību, lūdza nosaukt klientu norēķinu karšu datus, internetbankas datus (lietotāja numurs un paroli) vai Smart-ID kodus. Uzbrukumos cietuši vairāki tūkstoši lietotāju, kopējam zaudējumu apmēram sasniedzot vairākus simtus tūkstošu eiro. CERT.LV un bankas atgādināja, ka bankas pašas nekad nezvana ar lūgumu izpaust šādu informāciju.

Jūlijā tika saņemti ziņojumi par krāpniekiem, kas zvanīja un uzdevās par *Bloomberg* pārstāvjiem un piedāvāja investēt, izmantojot nelicencētas finanšu platformas. Krāpnieki sazinājās krievu valodā. CERT.LV rekomendēja neiesaistīties piedāvātajos darījumos un telefona sarunu pēc iespējas ātrāk pārtraukt, kā arī ar informāciju par Latvijā licencētiem finanšu pakalpojumu sniedzējiem iepazīties Finanšu un kapitāla tirgus komisijas tīmekļa vietnē www.fktk.lv.

Tika novēroti arī vairāki centieni izkrāpt maksājumus no slimnīcām, par finansēm atbildīgajam personālam vadītāja vārdā nosūtot e-pastu ar aicinājumu veikt steidzamu starptautisku maksājumu. Neviens no uzbrukumiem nav bijis veiksmīgs.

2.2. Pikšķerēšana jeb svarīgo datu izkrāpšana

Sociālajos tīklos, galvenokārt *Facebook*, uzbrucēji ar uzlauztu kontu palīdzību dažādās tematiskās grupās (piem., lietu apmaiņas vai māmiņu grupā) publicēja ierakstu par fiktīviem nelaimes gadījumiem (ugunsgrēku, avāriju), aicinot lasītājus sekot saitei, lai atpazītu upurus. Saite lasītāju nogādāja uz sociālā tīkla vietnes kopiju, kurā tika lūgts atkārtoti autorizēties. Vietnē ievadītie piekļuves dati tika nosūtīti uz krāpnieku kontrolēto saimniekserveri. CERT.LV atgādināja par nepieciešamību rūpīgi pārbaudīt vietnes adresi pirms jebkādas personīgās informācijas ievadīšanas, un ziņot portālam un grupas administratoram par kaitnieciskiem ierakstiem.

Tika konstatēti arī mēģinājumi izkrāpt *Facebook* piekļuves informāciju no organizāciju *Facebook* lapu pārvaldniekiem, kuriem tika nosūtīti viltoti paziņojumi par konta bloķēšanu, atsaucoties uz autortiesību vai lietošanas noteikumu pārkāpumu. Paziņojumā tika ievietota saite uz viltus vietni, kas vizuāli līdzinājās *Facebook*. Ievadot piekļuves datus šajā vietnē, dati tika nosūtīti uz krāpnieku kontrolētu serveri. Uz laiku piekļuvi vietnēm zaudēja vairākas valsts iestādes.

Augustā tika fiksēti inovatīvi uzbrukumi *Office 365* piekļuves tiesību izkrāpšanai. Lietotājam tika nosūtīta saite uz it kā koplietotu dokumentu. Atverot saiti, lietotājs tika pārvirzīts uz leģitīmu *Microsoft* vietni un aicināts autentificēties. Pēc autentifikācijas veikšanas ļaunprātīga *Microsoft Azure* vidē izveidota lietotne (*Azure App*) aicināja apstiprināt piekļuvi dažādiem lietotājam pieejamiem resursiem. Uzbrukums bija grūti pamanāms ar tehniskiem līdzekļiem, jo netika veiktas ļaundabīgas darbības upura iekārtā, uzbrukums tika realizēts *Office 365* vidē.

Augusta izskaņā tika saņemti vairāki ziņojumi par pikšķerēšanas e-pastiem, ļaundariem izliekoties par *Swedbank*. Aizbildinoties ar drošību un it kā uzlauztu lietotāja kontu, krāpnieki aicināja pārbaudīt atsūtīto informāciju interneta saitē vai pievienotā e-pasta pielikumā. Atverot saiti vai pielikumu, lietotājs tika pārvirzīts un lapu, kas atgādina *Swedbank* sākumlapu, taču vietnes adresē bija redzams, ka tā ir krāpnieciska. Neuzmanības dēļ ievadot datus šajā vietnē, lietotājs tos brīvprātīgi atdotu krāpniekiem. CERT.LV un *Swedbank* atgādināja, ka banka nekad lietotājam neprasīs internetbankas piekļuves datus zvanot, rakstot e-pastu vai sūtot SMS. Ja tiek saņemta

aizdomīga ziņa, nekādā gadījumā neklikšķināt uz saitēm un neievadīt savus datus. Saņemot šādu e-pastu, lietotāji tika aicināti ziņot par to bankai.

Tika saņemti ziņojumi par mērķētiem uzbrukumiem (*spear-phishing*) valsts iestāžu darbiniekiem e-pasta piekļuves datu izkrāpšanai. Upuri saņēma kolēģu vārdā sūtītus e-pastus, kas saturēja saiti uz viltotu *Office 365* pierakstīšanās vietni. Viltus vietnes dizains tika pielāgots atbilstoši mērķa organizācijai, pat ja organizācija izmantoja īpaši personificētu risinājumu. Pēc pierakstīšanās veikšanas upuri tika pārvirzīti uz e-pastā norādītajiem resursiem (ziņojumu vai pārskatu), kas mazināja upuru aizdomas par iespējamu uzbrukumu.

Augusta beigās, īsi pirms jaunā mācību gada sākuma, izglītības iestādes saņēma pikšķerēšanas e-pastus Izglītības un zinātnes ministrijas vārdā it kā par izmaiņām COVID-19 infekcijas sakarā, aicinot informēt pedagogus, bērnus un vecākus.

2.3. Pakalpojuma pieejamība (DDoS)

Septembrī kļuva aktuāli naudas izspiešanas mēģinājumi, uzbrucējiem draudot apturēt uzņēmuma mājas lapu vai citu resursu, kas nodrošina uzņēmuma darbību, ar uzbrukumu līdz pat 2 Tb/s. Šāda veida uzbrukumi vienlaicīgi notika vairākās Eiropas valstīs. Naudas izspiešanas mēģinājumi bija mērķēti gan uz finanšu institūcijām, gan uz citiem privātā sektora uzņēmumiem. Testa uzbrukumi, lai arī īslaicīgi (atsevišķos gadījumos vairākas dienas, bet visbiežāk mazāk par stundu), izcēlās ar lielo apjomu – līdz 100 Gb/s, un dažiem no upuriem radīja piekļuves traucējumus.

CERT.LV iesaka šādās situācijās nekomunicēt ar izspiedējiem un nemaksāt izpirkuma maksu, jo tas neatturēs uzbrucējus, bet tieši pretēji – veicinās atkārtotus uzbrukumus nākotnē, jo būs gūts apliecinājums, ka attiecīgais mērķis ir spējīgs un gatavs maksāt.

2.4. Ļaundabīgs kods

Tika novērotas vairākas viltotu e-pastu izplatīšanas kampaņas, kurās e-pasti tika izsūtīti kāda pazīstama uzņēmuma vai organizācijas vārdā, piemēram, Latvijas Universitātes vai DHL. E-pastu pielikums saturēja vīrusu, kas paredzēts sensitīvas informācijas (lietotājvārdi, paroles u.c.) iegūšanai no upura iekārtas. CERT.LV aicināja e-pasta serveru uzturētājus serveru konfigurācijā izmantot atbilstošas aizsardzības metodes (SPF, DKIM, DMARC), lai pasargātu lietotājus no viltotu e-pastu saņemšanas, kā arī novērstu organizācijas vārdā izsūtītu viltotu e-pastu izplatību.

Visa pārskata perioda garumā turpinājās plašā *Emotet* izplatīšanas kampaņa. Tās ietvaros iestāžu un organizāciju darbinieki saņēma e-pastus, kas bija noformēti kā esošas sarakstes turpinājums un saturēja kaitīgu pielikumu vai saiti uz kaitīgu dokumentu. Atverot dokumentu, lietotājam tika lūgts iespējot *Macros* funkcionalitāti, lai aplūkotu saturu vai nodrošinātu dokumenta saderību, jo dokuments it kā izveidots vecākā *Office* versijā. Atļaujot *Macros*, dators tika inficēts ar *Emotet* ļaunatūru. *Emotet* ļaunatūra fiksēta vairāk nekā 200 organizācijās un uzņēmumos.

2.5. Ielaušanās mēģinājumi

Ielaušanās mēģinājumi vairāk nekā 95% gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi veikti pret vairākām valsts iestādēm, kā arī virkni pašvaldību un privāto sektoru. Pēc CERT.LV rīcībā esošās informācijas šie uzbrukumi nav bijuši sekmīgi.

2.6. Kompromitētas iekārtas un datu noplūdes

Galvenokārt tie bija kompromitēti maršrutētāji privātajā sektorā un uzņēmumos.

2.7. Ievainojamības

Tika konstatēta ievainojamība kādas valsts iestādes tīmekļa vietnes meklēšanas rīkā, kas pakļāva vietni potenciālam kiberuzbrukumam. Tika informēti vietnes uzturētāji.

2.8. Atbildīgu ievainojamību atklāšana

Pārskata periodā tika saņemti daži maznozīmīgi ziņojumi.

2.9. CERT.LV pasākumi incidentu novēršanā

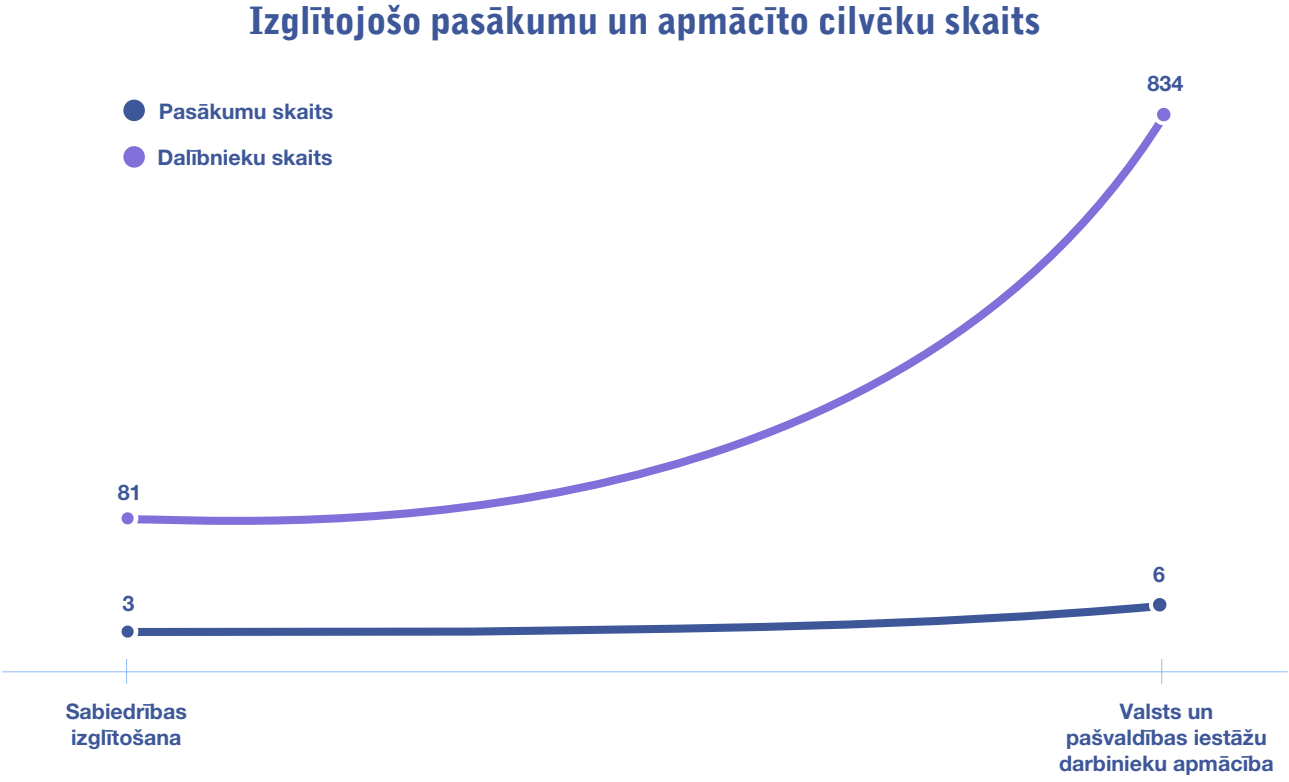
- 27. jūlijā valsts un pašvaldību iestāžu atbildīgajiem par IT drošību tika izsūtīta informācija par sagatavotajiem materiāliem e-pastu drošības veicināšanai, ņemot vērā novērotās ļaunatūras izplatīšanas kampaņas, kas veiktas dažādu uzņēmumu un organizāciju vārdā.
- 21. augustā valsts un pašvaldību iestāžu atbildīgajiem par IT drošību tika izsūtīta informācija par *Emotet* ļaunatūras izplatību un aizsardzības pasākumiem, kā arī par inovatīviem *Office 365* pikšķerēšanas uzbrukumiem.
- 15. septembrī valsts un pašvaldību iestāžu atbildīgajiem par IT drošību tika izsūtīta informācija par kritisku *Microsoft Netlogon* ievainojamību.

Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV tīmekļa vietnē un sociālo tīklu *Twitter* (@certlv) un *Facebook* (@cert.lv) kontos. Visā pārskata periodā CERT.LV ļoti aktīvi informēja sabiedrību par jaunām uzbrukumu kampaņām.

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

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

CERT.LV iesaistījās Finanšu nozares asociācijas un *Mastercard* organizētajā informatīvajā kampaņā #Viedpircējs par pirkumiem tiešsaistē, tajā skaitā par dažādiem šādu pirkumu drošības aspektiem (www.delfi.lv/bizness/viedpirceja-vestnieciba), piedaloties lekcijās un sniedzot intervijas.



10. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2020. gada 3. ceturksnī

14. augustā CERT.LV pārstāvis piedalījās Latvijas Sakaru darbinieku arodbiedrības (LSAB) organizētajā jauniešu forumā *Organizēta darba perspektīva nākotnē*, kurā stāstīja jauniešiem par drošību digitālajā vidē.

14. septembrī CERT.LV uzsāka informatīvi izglītojošu kampaņu par kiberdrošību darbavietā, lai veicinātu valsts un pašvaldību iestāžu un arī citu darbinieku izpratni par kiberdrošības labo praksi, kā arī veicinātu spēju atpazīt potenciālos kiberuzbrukumus un līdz ar to tos arī novērst. Kampaņas ietvaros tika izstrādāts kampaņai piesaistošais video materiāls un 3 informatīvi skaidrojošie video, kā arī vides plakāti un ekspertu viedokļraksti lielākajos portālos. Kampaņa noritēs 4 nedēļas.

Pārskata periodā CERT.LV par IT drošību izglītoja 915 cilvēkus, iesaistoties 9 izglītojošos pasākumos. Ņemot vērā epidemioloģisko situāciju valstī un ar to saistītos ierobežojumus, lielākā daļa pasākumu notika tiešsaistē.

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 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 līdzdarbojās Ministru kabineta noteikumu Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* izmaiņu izstrādē, sniedzot tehnisko kompetenci, lai nodrošinātu minimālo drošības ietvaru *Informācijas tehnoloģiju drošības likuma* aptvertajām mērķauditorijām.
- CERT.LV savas kompetences ietvaros sniedza konsultācijas valsts un pašvaldību iestādēm par MK noteikumu Nr. 442 un atsevišķu punktu, piemēram, par ielaušanās testu veikšanu un produktu lietojumu, implementēšanu iestādēs.
- CERT.LV piedalījās diskusijās par atbildīgas ievainojamību atklāšanas iekļaušanu normatīvajos aktos, sniedzot starptautiskās pieredzes piemērus un aplūkojot praktiskas ievainojamību atklāšanas situācijas.

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

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

CERT.LV starptautiskā sadarbība pārskata periodā:

- CERT.LV aktīvi piedalījās NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla *Cyber Weather* darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai, kā arī aktīvi darbojās *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu..

- Sadarbībā ar Itālijas CSIRT komandu tika veikta padziļināta krāpniecisko aktivitāšu platformas *Sp0m* izpēte, informējot par izpētes rezultātiem gan CERTu kopienu, gan arī plašāku sabiedrību. Izpēte ļāva noskaidrot veidus, kā tiek iegūtas kompromitētās tīmekļa vietnes, kuras attiecīgajā platformā tiek piedāvātas kaitīgā satura izvietošanai.
- CERT.LV piedalījās pārrunās ar Eiropas Komisijas pārstāvjiem par NIS direktīvas ieviešanu Latvijā, uzsverot pastāvošās neskaidrības Digitālo pakalpojumu sniedzēju (DPS) identificēšanā un izņēmumu pielietošanā mazajiem uzņēmumiem.
- Pārskata periodā NIS direktīvas CERTu tīkla ietvaros CERT.LV veica virtuālo CERT komandu savstarpējo auditu (*peer review*) Portugāles nacionālajai CERT vienībai. Audita ietvaros notika vairākas virtuālas sanāksmes.
- Pārskata periodā CERT.LV pārstāvis turpināja aktīvu darbību *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejā), lai palīdzētu uzlabot biedru uzņemšanas procesus un nodrošinātu augstāku kvalitāti informācijai, kas tiek iesniegta uzņemšanai FIRST organizācijā.
- 27. augustā CERT.LV pārstāvis piedalījās publiskā diskusijā par kritiskās infrastruktūras aizsardzību *Critical Infrastructure in the Baltic States and Norway*.
- 3. septembrī NIS direktīvas CERTu tīkla ietvaros CERT.LV pārstāvji piedalījās attālinātajā sanāksmē par ES Kiberdrošības akta izstrādi un tā ietekmi uz CERTu tīklu.
- Pārskata periodā CERT.LV pārstāvis piedalījās NATO CCDCoE organizēto tehnisko kiberdrošības mācību *Crossed Swords 2020/II* plānošanā un izpildes sagatavošanā.
- CERT.LV piedalījās diskusijā un sniedza atbildes uz diskusijas jautājumiem par vienotas Eiropas kibervienības izveidi, norādot, ka tehniskās sadarbības kapacitāte jau pastāv, bet nepieciešams sadarbību veicinošs juridiskais regulējums un politiskais atbalsts.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

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

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

Ievērojot COVID-19 vīrusa izplatības radītos ierobežojumus, darbs turpinājās visās sešās projektā definētajās darba pakās. Pārskata periodā no Eiropas Komisijas tika saņemts rakstisks apstiprinājums projekta pagarinājumam līdz 2020.gada 31.decembrim.

Pārskata periodā notika sagatavošanās darbi un 14. septembrī tika uzsākta sabiedrību izglītojoši informējoša kampaņa *Kiberdrošība darbavietā*. Kampaņas centrālā vietne ar videomateriāliem un rokasgrāmatu ar praktiskiem padomiem kiberdrošības un kiberhigiēnas uzlabošanai darba vietā ir www.esidross.lv. Kampaņas laikā tika sagatavoti arī vairāki tematiski raksti lielākajiem ziņu portāliem un sniegtas intervijas gan TV, gan radio.

7. Projekta "Cyber Exchange" īstenošana

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

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

2020. gada 3. ceturksnī COVID-19 vīrusa izplatības ierobežošanai noteikto ceļojumu ierobežojumu dēļ nebija iespējamas projekta ietvaros plānotās apmaiņas vizītes. Ir saņemts apstiprinājums projekta pagarinājumam. CyberExchange projekts turpināsies līdz 2021. gada 30. jūnijam.

8. Citi normatīvajos aktos noteiktie pienākumi

- Tika turpināts darbs pie CERT.LV un NIC.LV izstrādātā DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūra (*DNS firewall*) projekta īstenošanas. Projekts sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā, kas saistīts ar kiberdrošības institūcijām jau zināmiem incidentu identifikatoriem (domēna vārdi, IP adreses u.c.). Projekta ietvaros ir bijuši jau vairāki gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot iekārtas no inficēšanas. Daļu no DNS PRZ pakalpojuma var izmantot arī bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC.LV rekursīvie DNS serveri. Tīmekļa vietnē dnsmuris.lv pieejamas ērti lietojamas instrukcijas DNS ugunsmūra aktivizēšanai.
- CERT.LV pārstāvis sniedza interviju Valsts izglītības attīstības aģentūras (VIAA) administrētā informatīvā portāla *Profesiju pasaule*, kurā tiek ievietota informācija par tirgū pārstāvētām profesijām, sadaļas par kiberdrošības sfēru izveidei, aplūkojot nepieciešamās zināšanas un prasmes, kā arī karjeras izaugsmes iespējas.
- Drošības ekspertu grupas (DEG) sanāksmē tika prezentētas Ministru kabineta noteikumu Nr. 442 Kārtība, *kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām izmaiņu aktualitātes*, kā arī dažādas citas tēmas.
- Saskaņā ar MK 2015. gada 3. februāra sēdes protokolā Nr. 6 27. §, ar kuru pieņemts zināšanai informatīvais ziņojums “Par kompetento un atbildīgo iestādi, kura nodrošinās kvalificētu un kvalificētu paaugstinātas drošības elektroniskās identifikācijas pakalpojumu sniedzēju uzraudzību”, noteikto CERT.LV Digitālās drošības uzraudzības komitejas ietvaros veica izpēti par kvalificētas parakstu radīšanas ierīces sertificēšanas jautājumiem.

9. Papildu pasākumu veikšana

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.07.2020. līdz 30.09.2020. ir saņēmusi un izvērtējusi 1027 ziņojumus. No tiem 866 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 9 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 21 ziņojumā konstatēta personas goda un cieņas aizskaršana, 2 ziņojums saņemts par naida runu un 7 ziņojums par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 44 ziņojumi, 34 ziņojumu saturs nav bijis pretlikumīgs, 44 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 845 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā un 6 ziņojumi nosūtīt Valsts policijai par iespējamu sodāmu rīcību. 4 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, tika ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites. Pārskata periodā no Latvijā uzturētajiem 862 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 857 ziņojumi ir dzēsti no publiskas aprites internetā un 5 ziņojumi atrodas dzēšanas procesā.

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