CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Latvijas universitātes Matemātikas un informātikas institūts

Aizsardzības ministrija

2019

Publiskais pārskats par CERT.LV uzdevumu izpildi

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

Saturs

Kopsavilkums

2019. gads Latvijas kibervidē kopumā pagājis salīdzinoši mierīgi, lielu un postošu incidentu ar būtiskām sekām valsts mērogā nebija. Tomēr vidēji un mazi incidenti notika visu laiku, traucējot interneta lietotāju mieru un pārbaudot modrību. Īpaši pamanāmas un plašu rezonansi arī medijos izraisījušas dažādas krāpnieciska rakstura kampaņas, kas periodiski *uzliesmoja* visa gada garumā. Pie tādām pieskaitāmas, piemēram, uz *Smart-ID* lietotājiem orientētās kampaņas, kā arī krāpšana interneta vidē, pārliecinot lietotājus iesaistīties viltus kriptovalūtu biržās ar *ātru* peļņu, vai ievilināšana viltus interneta veikalos ar neticami labiem piedāvājumiem.

No šīm tendencēm iespējams secināt, ka Latvijas interneta lietotāja pirktspēja pieaug, līdz ar to arī uzbrucējiem un krāpniekiem interneta vidē kļūstam arvien interesantāki un tie velta laiku ticamākai uzrunāšanai un teksta sagatavošanai arī latviešu valodā.

Pēdējo divu gadu laikā ir ticis novērots, ka pielāgotos un personalizētos uzbrukumos (iejaukšanās biznesa sarakstē; e-pasti grāmatvežiem uzņēmuma vadītāja vārdā utt.) aizvien biežāk cieš tieši mazie un vidējie uzņēmumi (MVU). Lai mazinātu upuru skaitu MVU vidū, 2019. gadā CERT.LV sadarbībā ar NIC.LV un *Latvijas Tirdzniecības un rūpniecības* kameru organizēja izglītojošus seminārus par kiberdrošību, un plāno šos seminārus turpināt arī 2020. gadā.

Sabiedrības informēšanas un izglītošanas aktivitātēs par kiberdrošības jautājumiem 2019. gadā CERT.LV piedalījās 122 pasākumos, apmācot un izglītojot 7645 cilvēkus. Gada spilgtākā starptautiskā kiberdrošības konference *Kiberšahs* norisinājās divu dienu garumā un pulcēja kopā 630 dalībniekus no 30 valstīm. Tiešraidē konferenci vēroja vairāk nekā 4000 dalībnieku. *Kiberšahs* notika ar Eiropas Savienības Infrastruktūras savienošanas instrumenta atbalstu un sadarbībā ar *ISACA Latvijas nodaļu*, *LMT* un *dots*.

2019. gada maijā CERT.LV veiksmīgi noslēdz *TF-CSIRT/ Trusted Introducer* resertifikācijas procesu, tā turpinot apliecināt komandas augsto tehnisko briedumu un vispārējo sagatavotības līmeni. CERT.LV jau kopš 2016. gada ir viena no 26 Eiropas *TF–CSIRT/Trusted Introducer* sertificētajām komandām, un turpinās tāda būs arī nākamos 3 gadus, līdz nākamajam resertifikācijas periodam.

Valsts līmenī augstu tika novērtēti arī atsevišķi CERT.LV darbinieki:

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

Tika stiprināta CERT.LV komandas kapacitāte CERT.LV vadošajam pētniekam Bernhardam Blumbergam iegūstot doktora grādu, aizstāvot disertāciju *Specialized Cyber Red Team Responsive Computer Network Operations* Tallinas Tehniskajā universitātē.

CERT.LV ir ļoti svarīga atbildīgas un kopumā drošākas nākotnes kibervides veidošana, tāpēc 2019. gada 12. oktobrī CERT.LV pievienojās *Parīzes uzsaukuma (Paris call)* atbalstītāju lokam. *Parīzes uzsaukums* balstās uz deviņiem principiem un kopumā ir vērsts uz uzticības un drošības

veicināšanu internetā, uzsverot cilvēktiesību aizsardzību kibertelpā un valstu atbildību starptautisko normu ievērošanā arī digitālajā vidē.

Domājot par prognozi nākamajam gadam – visdrīzāk gaidāmi aktīvāki uzbrucēju centieni sasniegt mērķi, izmantojot sociālās inženierijas paņēmienus, kā arī lietotāju nezināšanu un labās prakses neievērošanu, jo, strauji attīstoties IT sistēmu tehniskajam drošības līmenim, tikai tehniski uzbrukumi kļūs dārgi un mazefektīvi.

Arvien vairāk uzmanības uzbrucēji pievērsīs arī lietu interneta (*IoT*) iekārtām, kuras lietotāji vieglprātīgi pieslēdz internetam un kuru ražotāju ieviestie drošības standarti neatbilst drošības izaicinājumiem interneta vidē.


Cyberchess
2019


PANEĻDISKUSIJA
CERT.LV


CERT.LV


LNT
900" 08:04 /+11°
KAMĀ GADA BUDŽETA LIKUMPROJEKTU
CVK SKATĪS IESNIEGU


KIBERDIENAKTS 2019
28.03.2019. | PLKST. 20.00 - 21.35
EKSPERTU DISKUSIJA


WWW.FIRST.ORG
FIRST
Improving Security Together
31ST ANNUAL
FIRST
CONFERENCE
EDINBURGH
JUNE 16-21 2019
DEFENDING THE CASTLE
#FIRSTCON19


Cyberchess
2019
#kibersahs 2019


POLICIJA

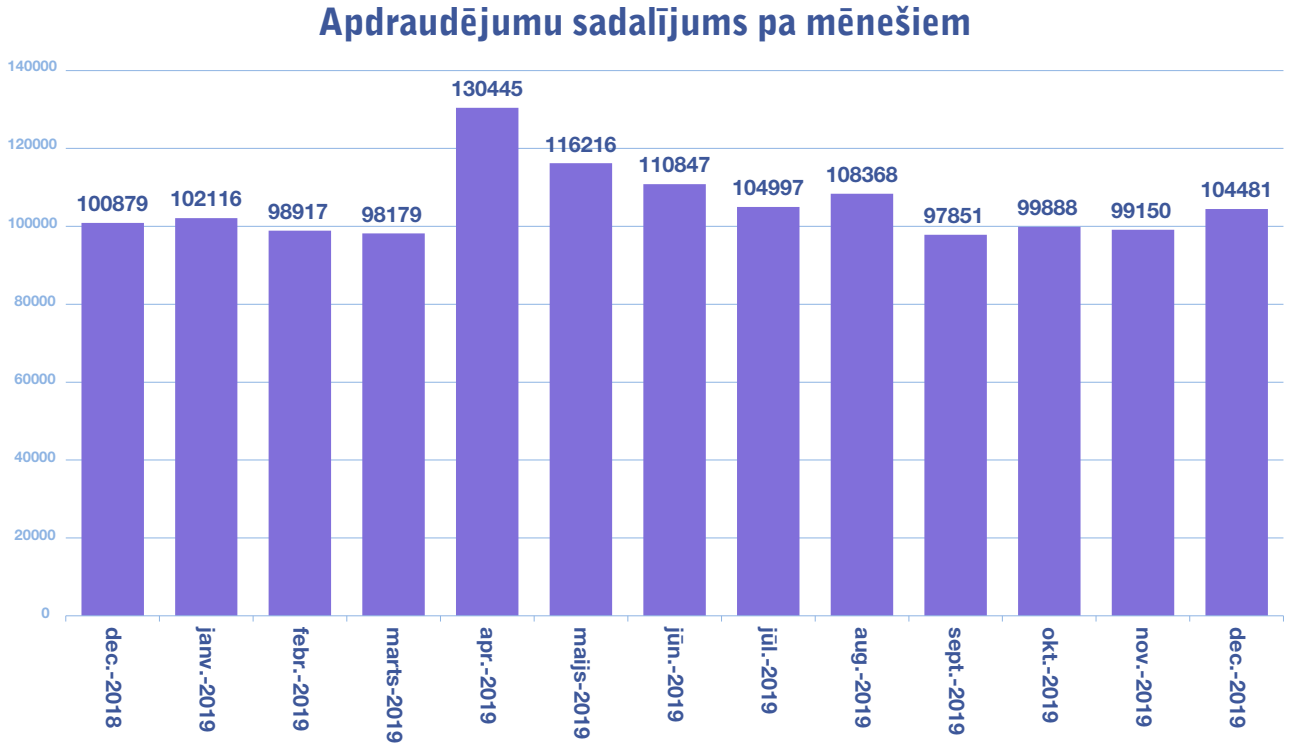

JAUNAS MAĢISTRA STUDIJU
PLATĪNA
PELE

1.

Incidentu apstrāde

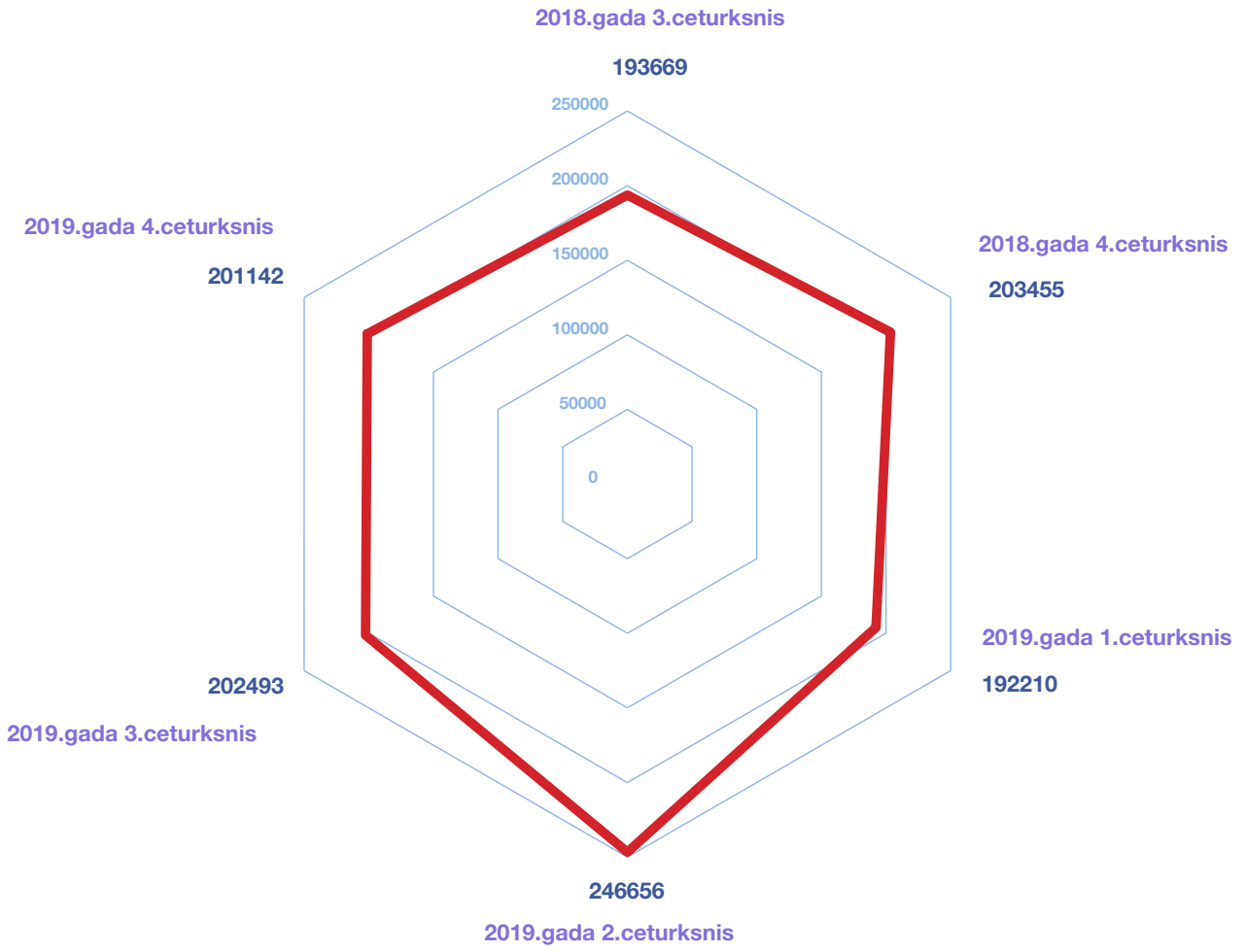
Ik mēnesi CERT.LV apkopo informāciju par apdraudētajām Latvijas IP adresēm. Apdraudējumu uzskaitei CERT.LV izmanto starptautiski lietotu incidentu taksonomiju (eCSIRT.net projekta izveidotā taksonomija). Statistikā visi CERT.LV reģistrētie apdraudējumi tiek uzskaitīt vienkopus, sadalot tos pa apdraudējumu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

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



1.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa mēnešiem 2019. gadā.

Apdraudējumu sadalījums pa ceturkšņiem 2019. gadā



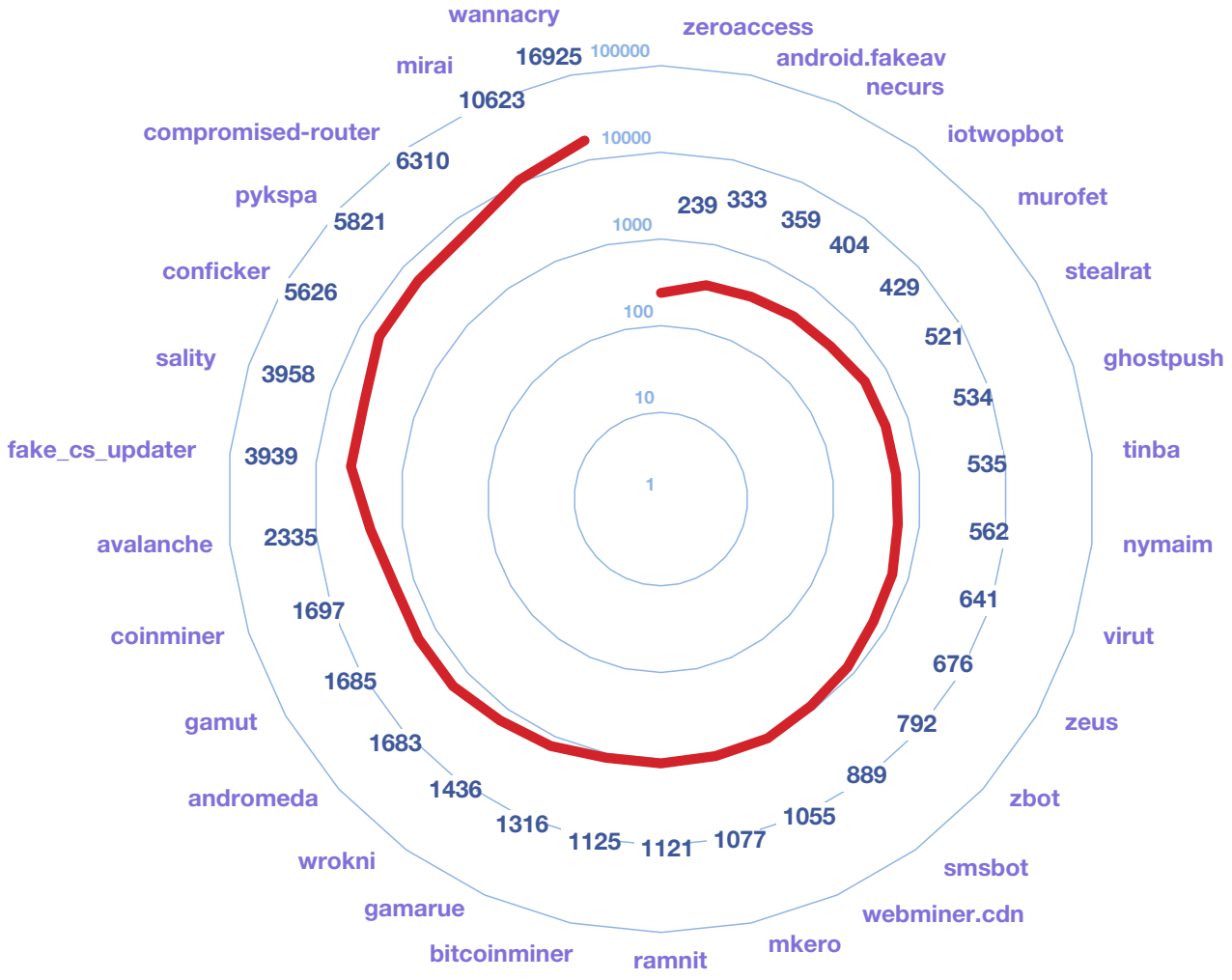
2.attēls – CERT.LV reģistrētās apdraudētās IP adreses pa ceturkšņiem 2019. gadā.

Izplatītākais apdraudējuma veids pārskata periodā nemainīgi bija konfigurācijas nepilnības, otrs izplatītākais bija ļaundabīgs kods, bet trešais – ielaušanās mēģinājumi. Kategorijā *Cits* iekļaujama

konsultatīvas informācijas sniegšana par dažādiem ar kiberdrošību saistītiem jautājumiem, galvenokārt valsts un pašvaldību institūcijām un Latvijas iedzīvotājiem, kā arī citi informācijas apstrādes gadījumi, kas nav tieši saistīti ar apdraudējumu novēršanu vai incidentu risināšanu.

3.attēls – CERT.LV reģistrētās apdraudētās unikālās IP adreses pa apdraudējuma veidiem 2019. gadā.

Unikālo IP adrešu skaits - ļaundabīgs kods 2019. gadā



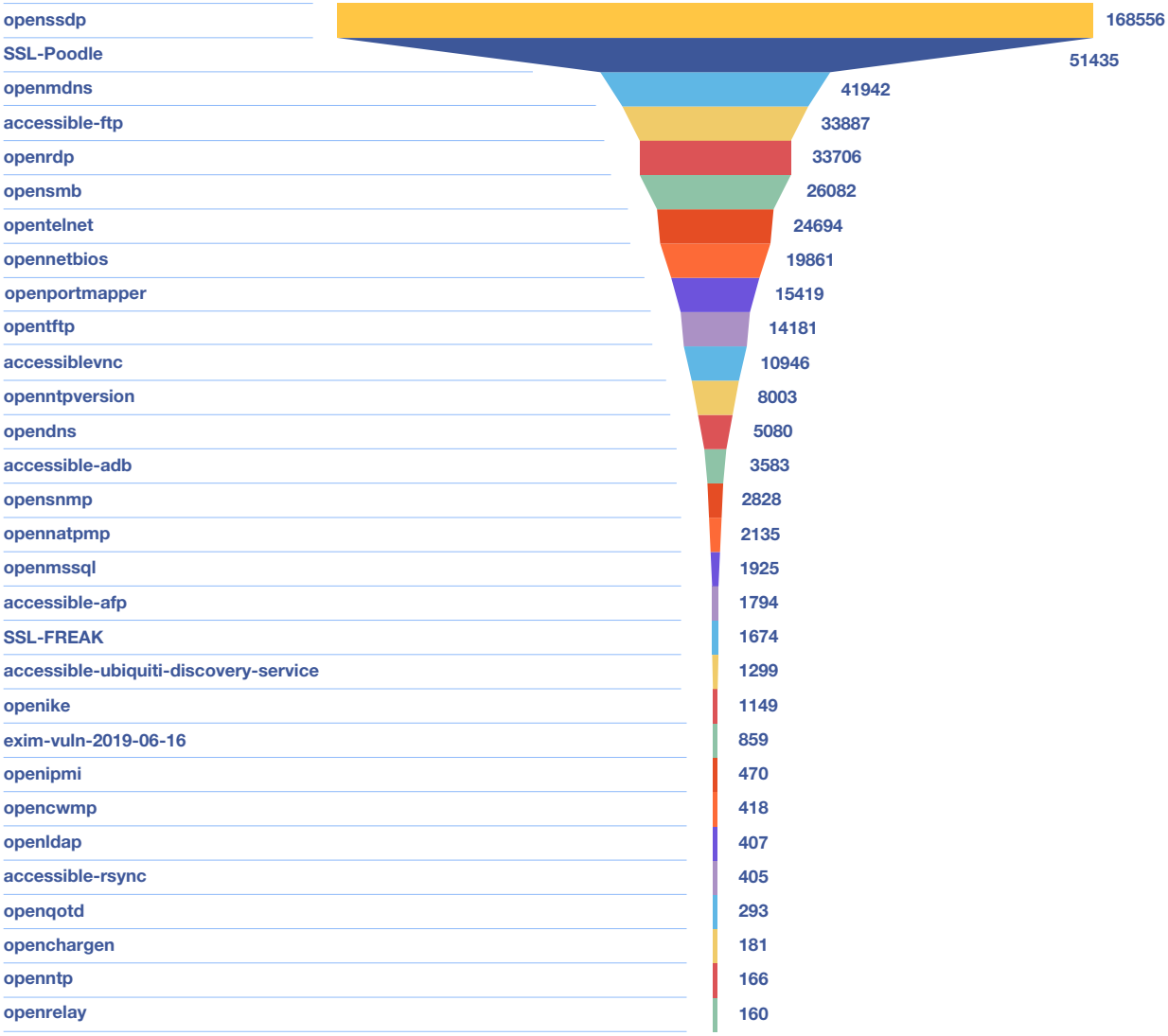
4.attēls – CERT.LV kopējais reģistrēto apdraudēto unikālo IP adrešu skaits 2019. gadā ar apdraudējuma veidu - ļaundabīgs kods.

Pirmo vietu ļaunatūras izplatības topā šajā gadā stabili ieņēma *WannaCrypt* jeb *Wannacry*, šifrējošais izspiedējvīruss. Tas ietekmē iekārtas ar *Microsoft Windows* operētājsistēmu un izplatās, izmantojot ievainojamību *SMB* protokolā. Vīrusa ietekmi un izplatību iespējams novērst, uzstādot *Microsoft* sagatavotos programmatūras atjauninājumus, kas pieejami pat tādām *Windows* versijām kā *Windows XP* un *Windows Server 2003*. Jāatzīst gan, ārkārtīgi lielais šīs ļaunatūras skarto unikālo IP adrešu skaits, kas būtiski pārsniedz visu pārējo ļaunatūru apjomu, varētu norādīt uz to, ka inficētas ir iekārtas, kurām piešķirtas dinamiskas adreses, izmantojot *DHCP (Dynamic Host Configuration Protocol)*, un patiesais inficēto iekārtu apjoms ir mazāks. Taču tas nenozīmē, ka apdraudējums nav būtisks un vērā ņemams, īpaši tāpēc, ka norāda uz inficētām iekārtām ar, ticamākais, novecojušu operētājsistēmu, piemēram *Windows XP*, kura vairs nesaņem automātiskos atjauninājumus un pakļauj iekārtu paaugstinātam riskam.

Topa otrajā vietā atrodas *Mirai* – ļaunatūra, kas apdraud neatbilstoši aizsargātas lietu interneta (*IoT*) iekārtas. Visbiežāk inficēti tiek viedie televizori, interneta maršrutētāji vai citas līdzīgas iekārtas, kas pēc iegādes tiek pieslēgtas internetam, nenomainot ražotāja iestatīto lietotājvārdu un paroli. Šīs iestatītās jeb noklusējuma paroles ir plaši zināmas, un to izmantošana pakļauj iekārtas uzbrukuma riskam.

Vietu ļaunatūras topa augšgalā nemainīgi saglabā *Conficker*, kaut arī tā ir jau sen pazīstama un salīdzinoša vienkārši *ārstējama* ļaunatūra – nepieciešama vien regulāra programmatūras atjaunināšana. Tas, visticamāk, norāda uz novecojušām neatjauninātām iekārtām, kas pakļautas augstam apdraudējumu riskam, vai zemu izpratni par kiberdrošību un pastāvošajiem riskiem iekārtu lietotāju vidū.

Unikālo IP adrešu skaits - konfigurācijas nepilnības 2019. gadā



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

Pirmo vietu konfigurācijas nepilnību topā ieņem *OpenSSDP* – iekārtas ar nedrošu konfigurāciju, kas var tikt izmantotas apjomīgos piekļuves atteices (*DoS*) uzbrukumos. *Simple Service Discovery Protocol (SSDP)* ir iebūvēts daudzās tīkla iekārtās, lai tās veiklāk varētu *atrast* viena otru un savstarpēji sazināties. Bieži neatbilstošas konfigurācijas rezultātā *SSDP* funkcionalitāte lietotājam nemaz nav pieejama, reizē padarot iekārtu par spēcīgu ieroci uzbrucēju rokās.

Openrdp ievainojamība, kas konfigurācijas nepilnību jeb ievainojamību topā (3.attēls) gada laikā pozīciju zaudējusi par divām vietām, ieņemot piekto vietu, norāda uz aktivizētu attālināto piekļuvi jeb *RDP (Remot Desktop Protocol)*, kas pieejama no publiskā tīkla un rada apdraudējumu, ja tiek izmantota pārāk vienkārša parole un netiek ierobežota piekļuve, piemēram, izmantojot privāto savienojumu jeb *VPN*. Uzbrucēji var izmantot nepietiekami aizsargātu *RDP* piekļuvi, lai iekļūtu sistēmā, izgūtu datus, vai pieprasītu izpirkuma maksu par bojātu datu atgūšanu. CERT.LV sadarbībā ar interneta pakalpojumu sniedzējiem veica regulāru ievainojamo iekārtu uzturētāju informēšanu *Atbildīgs interneta pakalpojumu sniedzējs* iniciatīvas ietvaros, skaidrojot potenciālo apdraudējumu un sniedzot rekomendācijas apdraudējuma novēršanai.

CERT.LV uzskaita arī uzlauzto un izķēmoto tīmekļa vietņu gadījumus. 2019. gadā tika uzlauztas un izķēmotas 132 tīmekļa vietnes. Piecos gadījumos tīmekļa vietne gada laikā tika uzlauzta un izķēmota atkārtoti. No visām kompromitētajām tīmekļa vietnēm 120 gadījumos vietnes uzturēšanai tika izmantota *Linux*, desmit gadījumos *Windows*, bet divos – *FreeBSD* operētājsistēma.

2.

Nozīmīgākie incidenti 2019. gadā

Pārskata periodā CERT.LV sadarbojās ar valsts un pašvaldību institūcijām, bankām, interneta pakalpojumu sniedzējiem un citām organizācijām dažādas bīstamības incidentu risināšanā. Pārskatā apkopoti nozīmīgākie incidenti, kas iezīmē gada tendences.

2.1. Piekļuves lieguma uzbrukumi (DoS un DDoS)

Būtiski piekļuves lieguma uzbrukumi un ilgstošu ietekmi 2019. gadā Latvijā netika novēroti. Daudzos gadījumos uzbrukumi notika, taču resursu pieejamība netika ietekmēta, jo tos aizsargāja gan LVRTC, gan citu pakalpojumu sniedzēju nodrošinātie *anti-DDoS* risinājumi. Zīmīgi, ka daļā no gadījumiem piekļuves liegums notika bez ļaunprātīgas ārējas ietekmes, bet gan izveidojās no lietotāju leģitīmajiem pieprasījumiem.

2.2. Pikšķerēšana jeb personīgo datu izkrāpšana

Kopumā pikšķerēšanas uzbrukumi ir bijuši ļoti aktīvi visa gada garumā. Vairumā gadījumu kampaņas bija vērstas uz e-pasta piekļuves datu izkrāpšanu, uz bankas, starptautisku maksājumu sistēmu un *Smart-ID* piekļuves datu iegūšanu un populārāko sociālo tīklu (*Facebook*, *Instagram*) piekļuves datu izkrāpšanu.

2019. gadā tika novēroti arī individualizēti uzbrukumi tieši valsts pārvaldes darbiniekiem; vienā no gadījumiem saņemtajos e-pastos bija iestrādāts skripts, kas, e-pastu atverot, ievāca informāciju par saņēmēju.

Visa pārskata perioda garumā CERT.LV, redzot aktīvas pikšķerēšanas kampaņas, izplatīja informatīvus materiālus un brīdināja konkrēto pakalpojumu lietotājus būt īpaši vērīgiem un uzmanīgiem.

2.3. Krāpšana

Krāpšanu ziņā 2019. gads ir bijis ļoti aktīvs un piesātināts, Latvijas interneta lietotājiem nācies periodiski izturēt aktīvas krāpšanas kampaņas.

Sākot ar izspiešanas kampaņām, kurās uzbrucēji apgalvoja, ka ir uzlauzuši lietotāja ierīci un ieguvuši kompromitējošus materiālus, par kuru neizplatīšanu pieprasīja izpirkuma maksu līdz zināmu uzņēmumu vārdā izplatītām krāpnieciskām loterijām, kurās piedāvāts laimēt jaunākos viedtālruņu modeļus vai apjomīgas naudas balvas. Neiztika arī bez krāpnieciskām tīmekļa vietnēm, e-veikaliem ar neticami zemām cenām un naudas aizdevējiem, kuri pirms piešķirt aizdevumu, aizdevuma saņēmēju aicināja veikt dažādas iemaksas par it kā aizdevuma pārskaitīšanas komisijām un tml.

Skaļākie incidenti, par kuriem informācija izskanēja arī presē, bija Latvijas slavenību aicinājumi investēt kriptovalūtā. Uzmanības piesaistei tika norādīts, ka minētās slavenības to jau ir izdarījušas un guvušas peļņu. Līdzīgas krāpniecības kampaņas tika īstenotas arī starptautiskā mērogā, un par to upuriem kļuvuši gan vairāki pasaulē pazīstami ziņu portāli, gan arī ietekmīgi politiķi, aktieri un investori.

Turpinājās krāpnieciski *finanšu speciālistu* zvani. Ir zināms, ka vienā no gadījumiem zaudējumu apjoms sasniedza 80 000 eiro. Viltus *finanšu speciālisti* mudināja veikt ieguldījumus nelicenzētās platformās, sākotnēji radot iespaidu, ka tiek gūta peļņa, un vēlāk solot iespēju atgūt pirmajā reizē *ieguldīto*.

Netika aizmirsti arī visu nozaru uzņēmumi, kur, izmantojot inovatīvas pieejas biznesa e-pastu krāpšanas realizācijā, tika izkrāpti ievērojami naudas līdzekļi. CERT.LV ir zināms par vienu uzņēmumu, kurš tikai pēc atkārtotas finanšu līdzekļu zaudēšanas ieviesa CERT.LV ieteikumus sūtītāja lauka viltošanas (*spoofing*) novēršanai.

2.4. Ielaušanās mēģinājumi

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

Ielaušanās mēģinājumu īstenošanas metodes ir bijušas atšķirīgas. Kā rāda CERT.LV novērojumi, tad populārākās uzbrucēju izvēlētās metodes iekļāva paroļu minēšanu, izmantojot *IMAP* servisu, pakalpojuma pārslodzes mēģinājumus, izmantojot *TCP* pieprasījumus, un datu izgūšanas mēģinājumus, izmantojot *SQL* injekcijas.

2.5. Ļaunatūra

Ļaunatūra 2019. gadā galvenokārt tika izplatīta diviem mērķiem – lai iegūtu informāciju vai gūtu peļņu. Informācijas gūšanai tika izplatīta spiegojošā ļaunatūra, kas nosūtīja upura iekārtā iegūtos datus, piemēram, paroles, uzbrucējam. Peļņas gūšanai tika izplatīti šifrējošie izspiedējvīrusi, kuru uzbrukuma rezultātā dati upura iekārtā tika nošifrēti, un datu atgūšanai tika pieprasīta izpirkuma maksa, kuras lielums bieži vien bija atkarīgs no tā, vai nošifrētā iekārta ir darbstacija vai serveris, vai cietušais ir uzņēmums vai privātpersona un vai ai nošifrētie dati ir dokumenti vai datubāzes – jo svarīgāki dati, jo augstāka cena. Cietušo vidū bija gan privātpersonas, gan dažādu nozaru uzņēmumi, kā arī valsts un pašvaldību iestādes. Pastāvot rezerves kopijām, visbiežāk datus izdevās veiksmīgi atgūt, taču zināms arī par gadījumiem, kur bez izpirkuma maksas, datu atgūšana nebija iespējama. CERT.LV gan iesaka, ja vien iespējams, izpirkuma maksu nemaksāt, jo maksāšana negarantē datu atgūšanu, kā arī veicina šādu ļaundabīgu praksi un kalpo kā rādītājs, ka upuris ir gatavs maksāt, un var rezultēties atkārtotā uzbrukumā.

Metodes ļaunatūras izplatīšanai bija dažādas, galvenokārt e-pasti, kas sagatavoti diezgan labā latviešu valodā un saturēja kaitīgu pielikumu, kura nosaukums veidots tā, lai maksimāli slēptu

patieso pielikuma paplašinājumu (piemēram, PO#august_pdf.img kurā .IMG fails tiek maskēts par .PDF) un izvēloties e-pasta tēmu, lai tā šķistu pašsaprotama, piemēram, neapmaksāts rēķins, maksājuma uzdevums, u.tml.

Gada nogalē kādā Latvijas interneta veikalā tika konstatēta ļaunatūra, kas zog apmeklētāju norēķinu karšu datus. CERT.LV informēja uzņēmumu par incidentu, kurš to operatīvi novērsa, kā arī sazinājās ar skartajiem klientiem un informēja par notikušo.

2.6. Kompromitētas iekārtas

Arī iekārtu kompromitēšanas gadījumi skāra gan privātpersonas, gan uzņēmumus, gan arī valsts un pašvaldību iestādes. Ievērojamāko gadījumu vidū uzsverama *Atlassian Confluence* lietotnes ievainojamības izmantošana, kā arī nepareizi konfigurētu iekārtu pieslēgšana internetam, kas ļāva uzbrucējiem piekļūt sensitīvai informācijai. Bieži tika novēroti gadījumi, kur, iegūstot superlietotāja tiesības, uzbrucēji spēja modificēt servera saturu vai izmantot organizācijas infrastruktūru SPAM e-pastu izsūtīšanai. Tika saņemts ziņojums no kāda tiešsaistes medija par vietnes uzlaušanu un nepatiesa satura ievietošanu – vietnes uzturētāji viltus saturu dzēsa un informēja savus lasītājus par vietnes kompromitēšanas faktu.

2.7. Ievainojamības un konfigurācijas nepilnības

Arī no ievainojamībām un konfigurācijas nepilnībām nebija pasargāta Latvijas IT telpa 2019. gadā. Par visām ievērojamākajām ievainojamībām, tajā skaitā receptēm, kā tās ārstēt, CERT.LV regulāri informēja interneta lietotājus.

Kā nozīmīgākie apdraudējumi, kuri skāra ievērojamu interneta lietotāju skaitu un kuru ietekmes mazināšanā iesaistījās arī CERT.LV speciālisti, jāmin *Confluence* kritiskā ievainojamība

CVE-2019-3396, kā arī *Oracle* serveru programmatūras ievainojamība CVE-2019-2729. Tāpat tika konsultēti vairāki tīmekļa vietņu uzturētāji, kuru vietnēs konstatētas drošības nepilnības, ļaujot vairākkārtēji izmantot autentifikācijas drošības marķierus, vai apiet vietnēs uzstādītos autentifikācijas procesa aizsardzības mehānismus. Gada izskaņā tika konsultēta iestāde, kuras darbinieki saņēma e-pasta ziņojumus paši no sevis. Tika ieteikts ieviest *DMARC - Domain-based Message Authentication*, *Reporting & Conformance* (iekļaujot *SPF* un *DKIM*) tehnoloģiju e-pasta serverī, kas liegtu lietotājiem saņemt viltotas e-pasta vēstules un vairākas citas SPAM vēstules kopumā.

3.

Atbildīga ievainojamību atklāšana

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

Pārskata periodā CERT.LV saņēma vairākus ziņojumus, kas informēja par atklātām ievainojamībām dažādos valsts un pašvaldību iestāžu resursos. Pateicoties šiem ziņojumiem, vairākas valsts iestāžu tīmekļa vietnes tika pasargātas no starpvietņu skriptēšanas (*XSS*) uzbrukumiem, kuri veiksmīgas izpildes gadījumā sniegtu uzbrucējam iespēju veikt darbības lietotāja pārlūkā, piemēram, manipulēt ar vietnes saturu un sīkdatnēm vai izmantot pārlūkam piemērotus mūķus (*exploits*). Tika saņemts ziņojums arī par kādas valsts iestādes tīmekļa vietni, kura tika uzturēta uz ievainojamas *Nginx* servera versijas, radot pārmērīgas procesora (*CPU*) noslodzes un pārmērīgas atmiņas patēriņa draudus.

Arī 2020. gadā CERT.LV aicina ziņot par atklātām ievainojamībām, rakstot uz cert@cert.lv vai iepazīstoties ar informāciju tīmekļa vietnē.

4.

Ielaušanās testi

Ielaušanās testi ir nozīmīgs solis, lai pārliecinātos par izveidotā tiešsaistes resursa – sistēmas, datubāzes, tīmekļa vietnes u.c. – atbilstību drošības prasībām. CERT.LV speciālisti gada laikā veica vairākus desmitus ielaušanās testus dažādiem valsts nozīmes informācijas resursiem. Lielākajā daļā testu tika atklātas būtiskas ievainojamības, daļā gadījumu tika konstatēta virkne nepilnību. Informācijas sistēmu uzturētājiem CERT.LV sagatavoja pārskatu par veiktajiem testiem un to rezultātiem, kā arī sniedza ieteikumus nepilnību novēršanai.

Biežāk atklātās ievainojamības CERT.LV veiktajos ielaušanās testos:

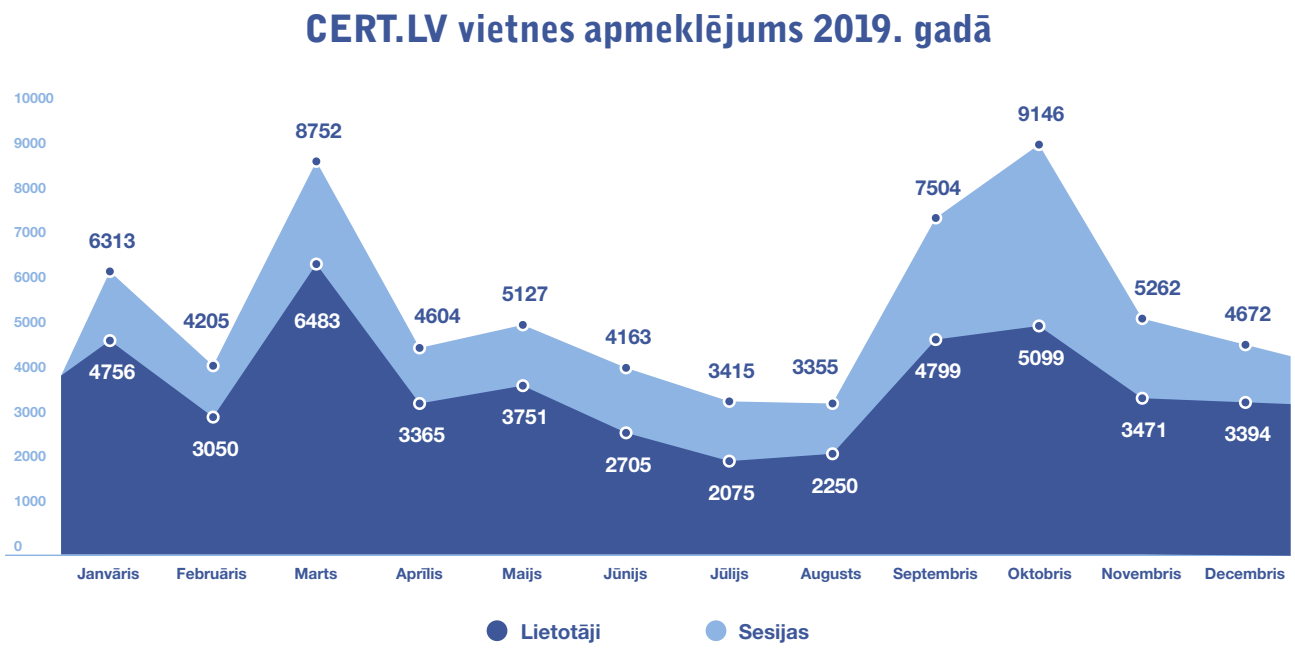
- Starpvietņu skriptēšanas (*XSS*) ievainojamības, kas pakļauj resursus informācijas izgūšanas riskam;
- Tiek izmantota novecojusi satura vadības sistēma (*CMS*), kura satur kritikas ievainojamības un pakļauj vietnes automatizētu uzbrukumu riskam;
- Resursu konfigurācijas nepilnības, kas sniedz uzbrucējam papildinformāciju par resursu.

5.

Informatīvie komunikācijas pasākumi

CERT.LV eksperti arī 2019. gadā turpināja sniegt intervijas un atbildēt uz mediju jautājumiem gan TV, gan presē un radio par dažādām aktuālām ar kiberdrošību saistītām tēmām. Pārskata periodā mediji lielāko interesi izrādīja par viedierīču drošību un drošiem lietotņu iestatījumiem, krāpnieciskām loterijām un pikšķerēšanas kampaņām, to, kā CERT.LV darbību ir ietekmējušas izmaiņas Informācijas tehnoloģiju drošības likumā, kas saistītas ar Tīklu un Informācijas sistēmu direktīvas (*NIS Directive*) ieviešanu Latvijas normatīvajos aktos, par 25. maijā notikušo Eiropas Parlamenta vēlēšanu procesa drošību un par konferences *Kiberšahs 2019* norisi.

CERT.LV uztur tīmekļa vietni cert.lv, kurā tiek publicēta informācija par aktuāliem apdraudējumiem, ieteikumi IT drošības līmeņa paaugstināšanai, informācija par dažādiem notikumiem un pasākumu kalendārs. **Kopā gada laikā CERT.LV vietnei bijuši 66,518 unikāli apmeklējumi jeb sesijas, kurus veikuši 39,335 lietotāji.**



6. attēls – CERT.LV tīmekļa vietnes apmeklējums 2019. gadā.

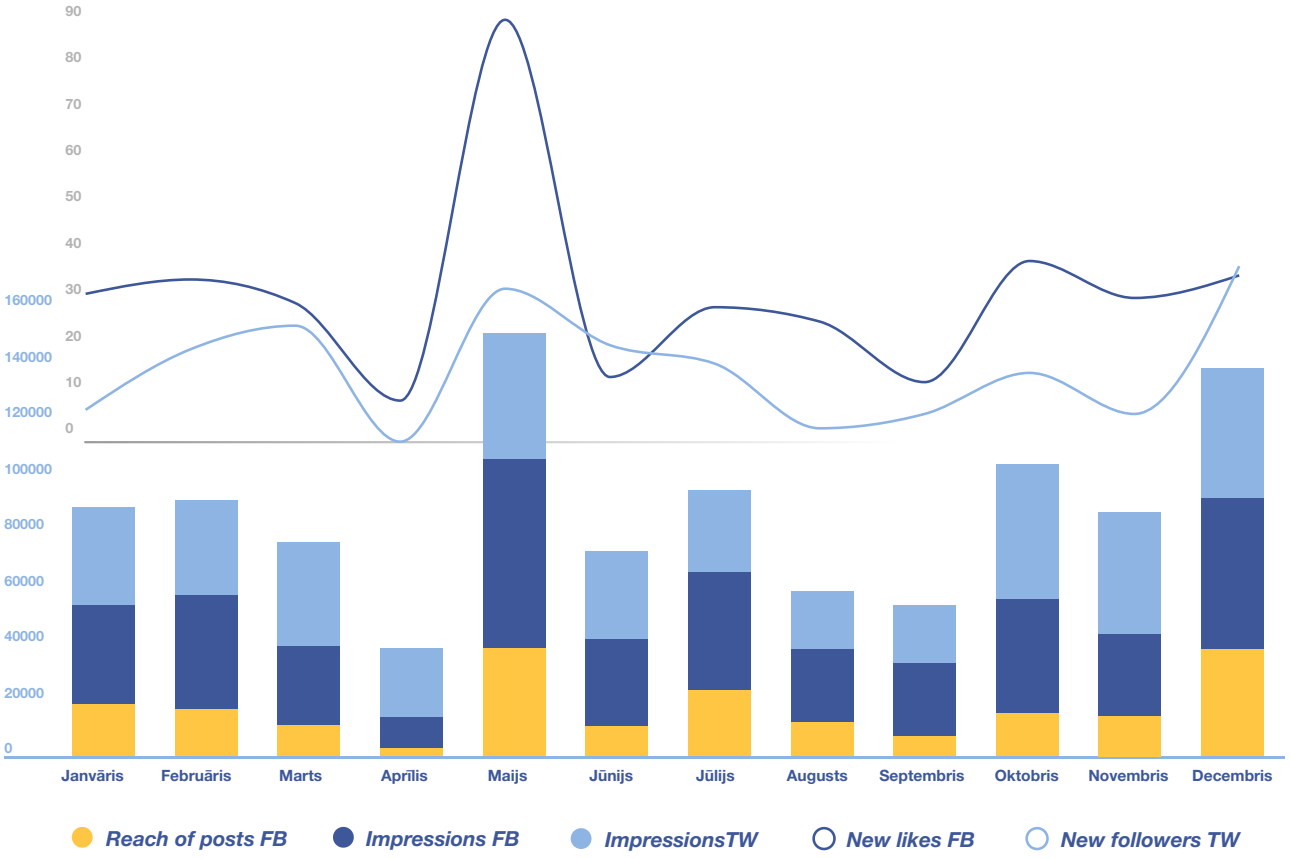
CERT.LV turpināja uzturēt arī lietotāju izglītošanas portālu www.esidross.lv, regulāri publicējot jaunus rakstus un atbildot uz lietotāju komentāriem.

Pārskata periodā katru mēnesi sadarbībā ar *SANS* institūtu tika izdoti informatīvie kiberdrošības biļeteni *OUCH!*, kuros, ikvienam interneta lietotājam saprotamā veidā kāds starptautiski atzīts kiberdrošības speciālists sniedz komentāru par aktuālajiem kiberapdraudējumiem un praktiskus ieteikumus lietotāja kiberdrošības uzlabošanai.

2019. gada laikā stabili pieauga sekotāju skaits populārajās sociālo tīklu platformās *Twitter* un *Facebook*:

- *Twitter* konta twitter.com/certlv sekotāju skaits pārskata perioda beigās bija 2301.
- *Facebook* profila facebook.com/certlv sekotāju skaits pārskata perioda beigās bija 1306.

CERT.LV sociālo tīklu profili 2019. gadā

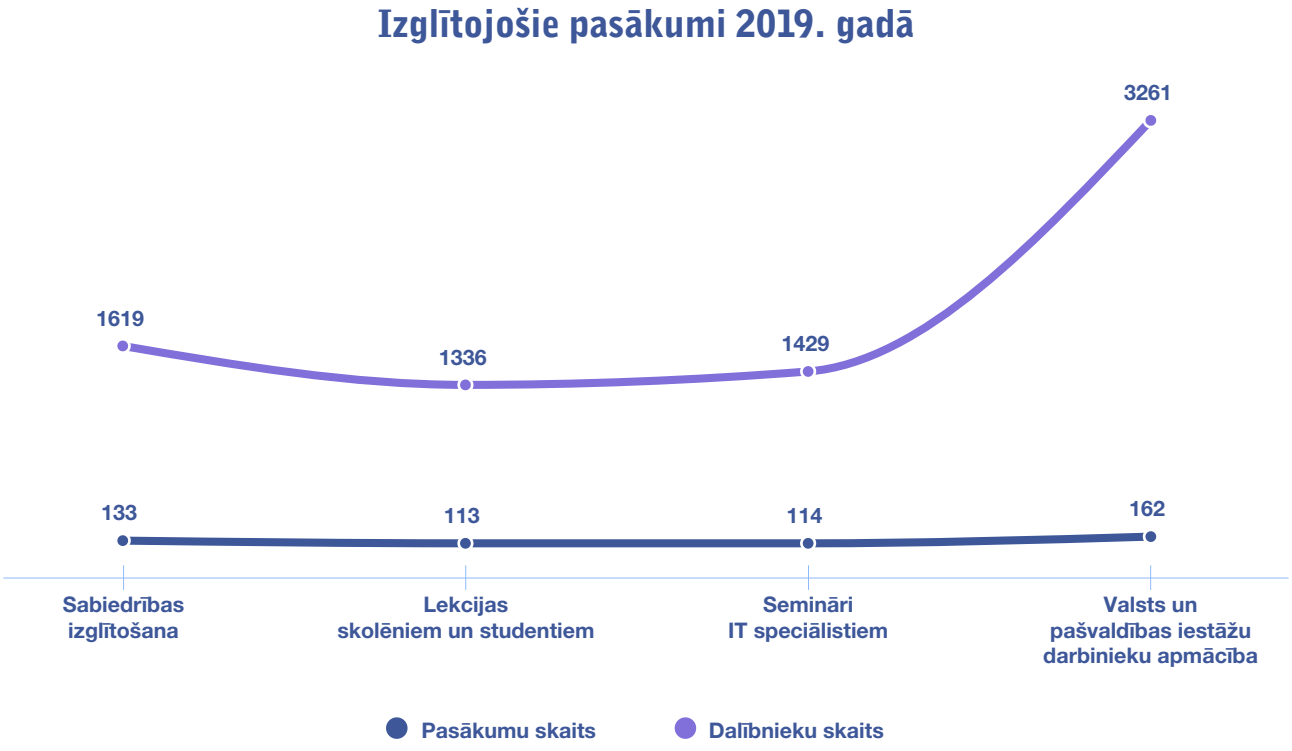


7. attēls – CERT.LV tīmekļa vietnes apmeklējums 2019. gadā.

6.

Izglītojošie pasākumi

2019. gadā CERT.LV turpināja rīkot izglītojošus pasākumus par kiberdrošības jautājumiem IT drošības speciālistiem, valsts un pašvaldību iestāžu darbiniekiem, studentiem, skolēniem un citiem interesentiem. Pārskata periodā CERT.LV piedalījās **122** pasākumos un izglītoja **7645** dalībniekus.



8.attēls – Pasākumu un apmācīto cilvēku skaits 2019. gadā.

6.1. Starptautiskā kiberdrošības konference Kiberšahs

Gada lielākais pasākums bija ikgadējā starptautiskā IT drošības konference *Kiberšahs 2019*, kas notika 2. un 3. oktobrī *Radisson Blu Hotel Latvija* telpās. Konferences tēmas bija vērstas uz kiberrisku novērtējumu, kibertelpas monitoringu, tehnoloģiskiem izaicinājumiem un inovatīvām metodēm datu un infrastruktūras aizsardzībai. Tika aplūkotas jaunākās kiberdrošības tendences un tehnoloģijas, politiskie, tehniskie un drošības aspekti kiberoperācijās, kā arī analizēta arvien pieaugošā sociālās inženierijas loma kiberuzbrukumos. Konferenci atklāja Latvijas Valsts prezidents Egils Levits un Aizsardzības ministrs Artis Pabriks.

Šī bija pirmā reize, kad konference norisinājās nevis vienu, bet divas dienas. Konferencei iesākoties, bija iespēja piedalīties vairākos praktiskos semināros. Konferenci klātienē divu dienu laikā apmeklēja 630 dalībnieki no vairāk nekā 30 valstīm. Tiešsaistē konferenci vēroja vairāk nekā 4000 skatītāju. Konferences prezentācijas un ieraksti joprojām pieejami gan cert.lv tīmekļa vietnē, gan vietnē straume.lmt.lv. Īss kopsavilkums par konferenci videoformātā skatāms šeit.

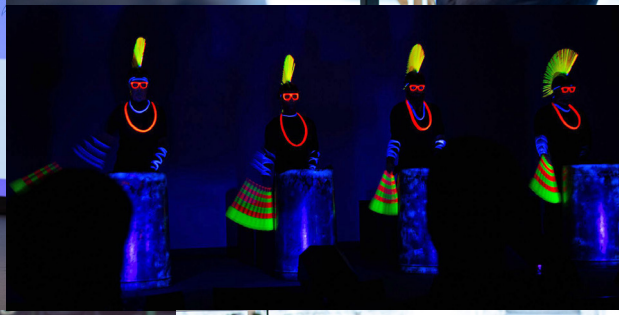
Konferences laikā interesenti varēja piedalīties *CTF* (*Capture the Flag*) sacensībās – tās ir īpašas kiberdrošības sacensības, kuru ietvaros dalībnieki tiek aicināti stāties pretī dažādiem kiberdrošības izaicinājumiem tādās kategorijās kā, piemēram, kriptogrāfija, tīkla analīze, kriminālistika, binārais kods un citas. Sacensībās dalību reģistrēja vairāk nekā 90 komandas, no kurām 46 komandas bija aktīvas un ieguva vismaz 100 punktus (maksimāli iespējamais punktu skaits bija 9100) , liels prieks bija par dalībniekiem no Saldus tehnikuma, kur studentu komanda godam cīnījās kopā ar spēcīgākajiem Latvijas un ārvalstu kiberdrošības ekspertiem.

Konference tika organizēta sadarbībā ar *ISACA Latvijas nodaļu*. *LMT* un *dots*. arī šogad sniedza savu atbalstu. Konference tika līdzfinansēta no Eiropas Savienības infrastruktūras savienošanas instrumenta īstenotā projekta Improving *Cyber Security Capacity in Latvia*.


Cyberchess
2019
Cybersecurity Conference
2 - 3 October
dots.
CYBECIRCLE


Cyberchess
2019
Cybersecurity Conference
2 - 3 October
CYBECIRCLE
Ministry of Defence
Republic of Latvia
#kibersahs 2019


Romania - It just
cant get any easier
than this




DATA IS YOUR FUT


HIGH BUSINESS VALUE
#kibersahs 2019


Cyberchess
2019


Cyberchess CTF award ceremony
Cyberchess
2019
#kiberšahs 2019

6.2. CERT.LV organizētie pasākumi IT drošības speciālistiem

Papildus starptautiskai kiberdrošības konferencei *Kiberšahs*, kuras galvenā mērķauditorija ir IT drošības speciālisti, tika organizēti vēl divi tematiskie semināri *Esi došs*. Ik gadu pavasarī un rudenī tie pulcē galvenokārt valsts un pašvaldību iestāžu par IT drošību atbildīgos un citus IT nozares pārstāvjus. *Esi drošs* semināru iespējams apmeklēt gan klātienē, gan vērot tiešsaistē. Vidēji semināru ik reizi apmeklē 100 – 150 dalībnieki. Prezentācijas un ieraksti pieejami CERT.LV tīmekļa vietnē.

Martā: Digitālās nedēļas ietvaros organizētajā *Esi drošs* tika aplūkotas tādas tēmas kā *DNS over HTTPS*, tīmekļa lietojumu drošība, mobilo iekārtu droša izmantošana valsts un pašvaldību iestādēs. Notika arī aktīva paneļdiskusija par e-adreses ieviešanu un izaicinājumiem.

Novembrī: *Esi drošs* seminārā dalībnieki tika iepazīstināti ar aktuālajiem IT riskiem un kiberdraudiem valsts iestādēm un pašvaldībām, inficētu IT sistēmu radītajām problēmām, e-pastu uzturēšanas labo praksi, pamatpakalpojumu un digitālo pakalpojumu sniedzēju iesaisti kiberdrošības vidē un CERT.LV piedāvātajiem drošības risinājumiem.

6.2. 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. Kā nozīmīgākie pasākumi 2019. gada griezumā jāmin:

12. februārī jaunuzņēmumu akselerators *Startup Wise Guys* organizēja pasākumu *CyberNorth Warm Up*, kurā CERT.LV piedalījās paneļdiskusijā par kiberuzbrukumiem, kā arī iesaistījās žūrijā un vērtēja uz kiberdrošību orientēto jaunuzņēmumu prezentācijas.

13. februārī CERT.LV piedalījās *Ēnu dienas* projektā un uzņēma ēnotājus, lai iepazīstinātu topošos profesionāļus ar nozari un palīdzētu veikt sev atbilstošu, jēgpilnu karjeras izvēli.

27. martā CERT.LV tikās ar Vidzemes augstskolas pārstāvi, lai pārrunātu sadarbības iespējas kiberdrošības maģistra programmas atbalstam.

28. martā LVRTC organizētā *Kibernakts 2019*, kas notika *Eiropas Digitālās nedēļas* laikā.

11. aprīlī dalība laikraksta *Dienas Bizness* organizētajā konferencē *Uzņēmuma digitālā drošība*.

16. aprīlī dalība semināru cilkā *GDPR Rīgas Forums 2019*.

29. maijā dalība *Data Security Solutions (DSS)* organizētajā forumā *Digitālā ēra*.

5. jūnijā un 24. septembrī sadarbībā ar NIC.LV *Latvijas Tirdzniecības un rūpniecības kamerā (LTRK)* semināri uzņēmējiem *Kā uzņēmējam viegli (ne)pazaudēt naudu kibertelpā*.

28. jūnijā dalība sarunu festivāla *Lampa* diskusijās: *Glabā savas paroles, tāpat kā savu apakšveļu par paroļu drošību* un *Maldināšana – katra diena kā 1.aprīlis*?

15. oktobrī CERT.LV un NIC.LV pārstāvji piedalījās 9. – 12. klašu skolēnu karjeras dienās, iepazīstinot skolēnus ar profesionālajām iespējām un izaicinājumiem IT drošības sfērā.

16. oktobrī dalība *Valmieras Attīstības aģentūras* organizētajā *Iedvesmas forumā* Valmierā.

17. oktobrī dalība IT drošības konferencē *DSS ITSEC*.

29. oktobrī dalība *Finanšu nozares asociācijas* un partneru rīkotajā ekspertu diskusijā *DROŠI e-pirkumi*, kampaņas *Piik un gatavs* ietvaros.

1. novembrī dalība Latvijas Ārpolitikas institūta un Eiropas Komisijas pārstāvniecības Latvijā organizētajā diskusijā *Cik droši Tu jūties, dzīvojot Eiropā*?

8. novembrī dalība *Valsts bērnu tiesību aizsardzības inspekcijas (VBTAI)* rīkotajā ikgadējā konferencē *Internets un Tu -kurš kuru?*.

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

7.

Stratēģiskā sadarbība Latvijā

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

Latvijā darbu turpina **Nacionālā informācijas tehnoloģiju drošības padome**, kuras mērķis ir koordinēt ar informācijas tehnoloģiju drošību saistīto uzdevumu un pasākumu plānošanu un veikšanu Latvijā. Padomes priekšsēdētājs ir Aizsardzības ministrijas valsts sekretārs, Padomes priekšsēdētāja vietnieks ir VARAM valsts sekretāra vietnieks informācijas un komunikācijas tehnoloģiju jautājumos, un tajā darbojas pārstāvji gan no CERT.LV, gan Ārlietu ministrijas, Ekonomikas ministrijas, Finanšu ministrijas, Finanšu un kapitāla tirgus komisijas, Iekšlietu ministrijas, Izglītības un zinātnes ministrijas, Labklājības ministrijas, Latvijas Bankas, LVRTC, Militārās izlūkošanas un drošības dienesta, Militāro informācijas tehnoloģiju drošības incidentu novēršanas komandas (MilCERT), Nacionālajiem bruņotajiem spēkiem, Satiksmes ministrijas, Satversmes aizsardzības biroja, Tieslietu ministrijas, Valsts drošības dienesta, Valsts ieņēmumu dienesta, Valsts kancelejas, Valsts policijas, Veselības ministrijas. Padome tiekas ne retāk kā reizi četros mēnešos, padomes sekretariāta funkcijas veic Aizsardzības ministrijas Krīzes vadības departamenta Nacionālās kiberdrošības politikas koordinācijas nodaļa.

CERT.LV cieši sadarbojas ar Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļu, un savas kompetences ietvaros aktīvi piedalās Nacionālās kiberdrošības stratēģijas īstenošanā. Kā svarīgākās, valsts mēroga aktivitātes 2019. gadā, kurās piedalījās CERT.LV ir jāmin dalība:

- Eiropas Parlamenta vēlēšanu darba grupā. Vēlēšanu laikā CERT.LV veica nepārtrauktu vēlēšanu sistēmu uzraudzību.
- Saeimas Nacionālās drošības komisijas sanāksmēs par 5G jautājumiem sniedzot atbalstu 5G tehnoloģiju tehnisko risku novērtēšanā.
- Darba grupā ar Aizsardzības ministriju prasību identifikācijai pamata pakalpojumu sniedzēju definēšanai atbilstoši *NIS direktīvai*.
- Darba grupā ar Centrālo vēlēšanu komisiju (CVK) par iespējamo Rīgas domes ārkārtas

vēlēšanu nodrošināšanu un katras iestādes veicamajiem uzdevumiem.

- Grozījumu sagatavošanā Ministru kabineta noteikumos (MKN) Nr.442, kas papildus esošajām prasībām paredz arī prasības informācijas sistēmām izstrādes laikā, prasības atsevišķām IKT komponentēm, tās iepērkot, un prasības ārpakalpojumu sniedzējiem.
- LMT rīkotajā seminārā, paužot viedokli par Ekonomikas ministrijas gatavoto likumprojektu *Kārtība, kādā Centrālā statistikas pārvalde pieprasa un elektronisko sakaru komersants sniedz informāciju oficiālās statistikas nodrošināšanai*, norādot, ka izvēlētais datu anonimizācijas modelis ir situācijai neatbilstošs un nepietiekami pilda anonimizācijas funkciju, ļaujot ar vienkāršu algoritmu palīdzību ar augstu precizitāti identificēt konkrētas personas.

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

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

Komiteja, papildus ikdienas uzdevumiem, 2019. gadā īstenojot LVRTC uzraudzību, apstiprināja LVRTC pār-sertifikāciju kā uzticama sertifikācijas pakalpojumu (uzticams e-paraksts, laika zīmogs un elektroniskais zīmogs) sniedzēju, pēc pozitīva audita ziņojuma saņemšanas.

Komiteja veica Latvijas elektroniskās identifikācijas shēmas, kas sastāv no 4 elektroniskās identifikācijas līdzekļiem (eID karte, ePraksts mobile, eParaksts karte un eParaksts karte+), paziņošanu Eiropas Komisijai, Latvijā esošā shēma atbilstoši iepriekš veiktajām pārbaudēm tika novērtēta augstā uzticamības līmenī. Tāpat tika izskatīti grozījumi, kas skāra jauno veida eID karšu

izsniegšanu. Papildus tam komiteja koordinēja informācijas apmaiņu ar starpvalstu sadarbības grupām, tostarp arī par potenciāliem drošības riskiem un ievainojamībām.

CERT.LV cieši sadarbojās ar Zemessardzes **Kiberaizsardzības vienību (KAV)**, kas IT drošības krīzes vai apdraudējuma situācijā sadarbībā ar CERT.LV varētu sniegt atbalstu valstij un privātam sektoram. Kiberaizsardzības vienība veidota saskaņā ar Zemessardzes likumu, apvienojot privātajā sektorā nodarbinātos un brīvprātīgi iesaistīties gribošus ekspertus, kuri brīvajā laikā ir ieinteresēti veidot regulāru sadarbību IT drošības jautājumos, pilnveidojot ekspertīzi un zināšanas nacionālā un starptautiskā līmenī. 2019. gadā svarīgākā sadarbība notika tieši kiberuzbrukumu novēršanas mācībās – *Crossed Swords* un *Locked Shields*.

Ikviens interesents - informācijas tehnoloģiju eksperts - tiek aicināts sniegt savu ieguldījumu valsts drošībā, pievienojoties Kiberaizsardzības vienībai. Saņemt papildu informāciju par vienību un pieteikties var rakstot uz: kibersargs@mil.lv.

CERT.LV turpina koordinēt arī 2012. gadā izveidotās **Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupas (DEG)** darbību. 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. Dalībai DEG nepieciešama rekomendācija no diviem jau esošiem DEG biedriem.

Kopā ar *Latvijas Interneta asociāciju (LIA)* turpinās 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. 2019. gada 31. oktobrī tika organizēts seminārs IPS pārstāvjiem, lai pilnveidotu sadarbību. Seminārā piedalījās 45 interneta pakalpojumu sniedzēju pārstāvji. Šobrīd iniciatīvai pievienojušies 13 lielākie IPS Latvijā.

8.

Starptautiskā sadarbība

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

CERT.LV regulāri piedalījās *NIS CSIRT Network* sadarbības tīkla sanāksmēs, to mērķis ir nodrošināt sadarbības stiprināšanu starp IT drošības incidentu novēršanas vienībām Eiropas mērogā. Sanāksmes notiek līdz 3 reizēm gadā, norises vieta ir konkrētajā brīdī Eiropas Savienības Padomes prezidējošā valsts. Pārrunājamās tēmas sakrīt ar prezidējošās valsts noteiktajām prioritātēm kiberdrošības jomā. Reizi gadā sanāksmē notiek arī apvienotās sesijas kopā ar *NIS* direktīvas sadarbības grupu.

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

CERT.LV vadītāja Baiba Kaškina turpināja pildīt *TF-CSIRT* Steering komitejas vadītāja pienākumus, piedaloties gan klātienes, gan attālinātās sanāksmēs un organizējot *TF-CSIRT* darbu. Baiba Kaškina pildīja šos pienākumus 5 gadus, un tie noslēdzās 58. *TF-CSIRT* sanāksmē, Kiprā 16.-17. septembrī.

CERT.LV ir aktīvs *FIRST* biedrs un piedalījās 31. *FIRST* konferencē Edinburgā. Šī bija lielākā *FIRST* konference vēsturē, pulcējot vairāk nekā 1000 pārstāvjus no dažādām CERT komandām un citām saistītām organizācijām no vairāk nekā 80 valstīm. CERT.LV piedalījās konferences programmkomitejā un konferences ietvaros vadīja vairākas tehniskās sesijas, pārstāvēja Latviju ikgadējā biedru kopsapulcē, kā arī startēja *capture the flag* izaicinājumu risināšanas sacensībās.

2019. gadā CERT.LV piedalījās arī vairākās akadēmiskās un praktiskās konferencēs, to vidū īpaši izceļamas – Čehijā notikušajās *ICISSP2019 – Information Systems Security and Privacy*, 5th

International Conference un *Future Forces Forum: SCADA Security Conference*. Portugālē notikusī *ECCWS2019 – 18th European Conference on Cyber Warfare and Security*, Moldovas *Regional Cyber Reslilience Forum*, un gada nogalē Vācijā notikušais *Chaos Computer Club* organizētais *Chaos Communication Congress*. Visās konferencēs CERT.LV uzstājās, daloties ar labo praksi un gūto praktisko pieredzi.

CERT.LV regulāri piedalās *ENISA* (Eiropas Tīkla un informācijas drošības aģentūras) organizētajās starptautiskajās kiberdrošības mācībās.

2019. gadā CERT.LV veiksmīgi piedalījās Eiropas Parlamenta, ES dalībvalstu, Eiropas Komisijas un *ENISA* organizētajās krīzes vadības mācībās *EU ELEx19* Briselē, lai uzlabotu gatavību potenciāliem kiberdrošības incidentiem Eiropas Parlamenta vēlēšanu laikā. Kā arī Eiropas kiberdrošības mācībās *CyberSOPEx*, to mērķis bija veicināt ES dalībvalstu sadarbību liela mēroga kiberincidenta gadījumā.

11.–12. septembrī CERT.LV komanda piedalījās *Organization of American States*, *INCIBE (Spanish National Cybersecurity Institute)* un *CNPIC (Spanish National Centre for Infrastructure and Cybersecurity)* organizētajās starptautiskajās kiberdrošības mācībās *CyberEx 2019*, kurās 87 komandu konkurencē ieguva augsto 16. vietu. Mācību mērķis ir stiprināt dalībnieku spēju reaģēt uz kiberdrošības incidentiem, veicinot sadarbību šādu incidentu risināšanā.

Apliecinot komandas briedumu un augsto kvalifikāciju, CERT.LV regulāri piedalās *NIS* direktīvas CERTu tīkla IT drošības incidentu novēršanas vienību savstarpējos auditos (*peer review*), kas ir būtiska vienību darbības kvalitātes un kvalifikācijas pārbaude. 2019. gadā CERT.LV veica auditu Lietuvas CERT-LT, Horvātijas CERT.HR un Igaunijas CERT-EE komandām. Kā minēts iepriekš, 2019. gada maijā CERT.LV veiksmīgi pabeidza *TF-CSIRT/ Trusted Introducer* resertifikācijas procesu, tā turpinot apliecināt komandas augsto tehnisko briedumu un vispārējo sagatavotības līmeni. CERT.LV jau kopš 2016. gada ir viena no 26 Eiropas *TF–CSIRT/Trusted Introducer* sertificētajām komandām, un turpinās tāda būs arī nākamos 3 gadus, līdz nākamajam resertifikācijas periodam.

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*. CERT.LV un *NATO CCDCoE* ir galvenie organizatori un sadarbības partneri tehnisko kiberdrošības mācību *Crossed Swords* un *Locked Shields* nodrošināšanā.

2019. gadā *Locked Shields* mācībās tika uzsvērta nepieciešamība tehnisko ekspertu un lēmumu pieņēmēju dialoga uzlabošanai. Šim nolūkam mācībās tika integrēta tehniskā, un stratēģiskā spēle, ļaujot dalībvalstīm būtiskas kiberkrīzes apstākļos pilnveidot dažādus komunikāciju posmus, iekļaujot gan civilos, gan militāros aspektus. Mācībās tika aplūkoti reāli kiberapdraudējumi, par galveno uzdevumu liekot kritiskās infrastruktūras aizsardzību. Tika palielināta mācībās izmantoto sistēmu sarežģītība, salīdzinājumā ar iepriekšējo gadu. Kopumā mācībās piedalījās vairāk nekā 1200 eksperti no gandrīz 30 valstīm. Latvijas komandas sastāvā bija gan CERT.LV, gan KAV, gan arī Kanādas un ASV pārstāvji.

2019. gadā tehniskajās kiberdrošības mācībās *Crossed Swords* galvenā uzmanība tika vērsta uz *sarkanā karoga* komandu ofensīvo prasmju attīstību kiberoperāciju plānošanā, izpildē un reaģēšanā uz apdraudējumu. Mācībās piedalījās vairāk nekā 100 dalībnieki no 21 valsts.

9.

ES līdzfinansētu projektu īstenošana

Projekta ***Improving Cyber Security Capacities in Latvia*** (līguma ar Eiropas Komisiju Nr.INEA/CEF/ICT/A2017/15287842018) īstenošana sākās 2018. gada 1. septembrī un turpināsies līdz 2020. gada 31. decembrim. Projekta mērķis, kā norāda tā nosaukums, ir stiprināt Latvijas kiberdrošības kapacitāti. 2019. gada laikā projekta ietvaros:

- Turpinājās aktīva iesaiste *MeliCERTes – Cybersecurity Core Service Platfrom* izstrādē un testēšanā, platformas mērķis ir, apkopojot IT drošības incidentu novēršanas vienību prasības starptautiskai sadarbībai, nodrošināt vienotu sistēmu, kurā varētu notikt starptautisku kiberincidentu risināšana un informācijas apmaiņa par kiberincidentiem.
- Turpinājās darbs pie *Deep Analysis System: Pastelyzer – the Paste Analyzser* izstrādes, rīka mērķis ir, iekļaujoties esošajā IT drošības incidentu novēršanas vienību ikdienas darbā, nodrošināt apjomīgu datu automatizētu atlasi un analīzi.
- Regulāri norisinājās informatīvi un izglītojoši semināri visā Latvijā.
- Ar projekta atbalstu notika starptautiskā kiberdrošības konference Kiberšahs 2019.
- Uzsākta iepirkuma procedūra kampaņai Informācijas tehnoloģiju drošība darbavietā, realizējot iepirkuma pirmo kārtu. Plānotais kampaņas norises laiks 2020. gada 3. ceturksnis.

Projekta ***Cyber Exchange*** (līguma ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2017/1528784) īstenošana sākās 2018. gada 1.novembrī un turpināsies līdz 2019. gada 30. novembrim. Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības IT drošības incidentu vienībām (CSIRT/CERT organizācijām). *Cyber Exchange* projekts ir kā atbilde arvien pieaugošajiem draudiem kiberdrošības jomā, īpašu akcentu vēršot uz nepieciešamo pārrobežu sadarbību cīņā pret tiem. Latvija ir viena no 10 Eiropas valstīm, kas piedalās projektā. Projekta ietvaros notiek pieredzes apmaiņas vizītes.

2019. gadā Latvijā viesojās Horvātijas CERT.HR un Rumānijas CERT-RO pārstāvji, lai vairāku dienu garumā veiktu vērtīgu pieredzes apmaiņu par organizācijas procesu norisi, incidentu risināšanu,

apstrādes metodēm, izmantotajiem rīkiem un apstrādes kārtību, incidentu prevencijas metodēm, izglītošanas jautājumiem un citiem aktuāliem darbības aspektiem.

Savukārt CERT.LV pārstāvis viesojās *CIRCL*, Luksemburgā, kur tikās ar plaši izmantotās platformas *MISP (Malware Information Sharing Platform)* izstrādātājiem, gūstot vērtīgu pieredzi darbam ar platformu, sniedzot atgriezenisko saiti platformas izmantošanā un saņemot padomus no ārvalstu kolēģiem platformas efektīvākai lietošanai. Apmaiņas vizīte veicināja platformas funkcionalitātes paplašināšanu. Paralēli tika iepazīti arī jauni rīki, kuri sniegs iespēju pilnveidot CERT.LV ikdienas darbu.

```
(defun nbytes (stream n &opt
  "Formats amount of N bytes in a human-r
of 1024, or powers of 1000 if COLON-P is true."
  (declare (ignore at-sign-p)
           (type unsigned-byte n))
  (cond ((zerop n)
         (write-string "0B" stream))
        (t
         (multiple-value-bind (base units)
             (if colon-p
                 (values 1000.0d0 "BkMGTPEZY")
                 (values 1024.0d0 "BKMGTPEZY"))
           (loop for i fixnum from 0 below (1- (length units))
                 for f double-float = (coerce n 'double-float) then (/ f base)
                 until (< f base)
                 finally (let ((unit (schar units i)))
                           (if (and (< f 10) (plusp i))
                               (format stream "~,1F~A" f unit)
                               (format stream "~D~A" (round f) unit))))))))

(defun bytes (stream bytes &optional colon-p at-sign-p)
  "Formats a sequence of BYTES as hex-digit pairs."
  (declare (ignore colon-p at-sign-p))
  (etypecase bytes
    (vector
     (loop for byte of-type (unsigned-byte 8) across bytes
           do (when (< byte #x10)
                (write-char #\0 stream))
              (write byte :stream stream
                          :base 16
                          :radix nil
                          :readably nil
                          :escape nil)))
    (list
     (format stream "~{~2,'0x~}" bytes))))
```

10.

Pakalpojumi Latvijas kibertelpas stiprināšanai

DNS Ugunsmūris: Tika turpināts darbs pie CERT.LV un NIC.LV izstrādātā DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūra (*DNS firewall*) projekta ieviešanas.

Projekts sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā, kas saistīts ar kiberdrošības institūcijām jau zināmiem incidentu identifikatoriem (domēnu vārdi, IP adreses u.c.).

Projekta ietvaros ir bijuši jau vairāki gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot iekārtas no inficēšanas. DNS PRZ pakalpojumu var izmantot arī bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC.LV rekursīvie DNS serveri.

Vairāk informācijas un detalizētas instrukcijas, pieejamas vietnē https://dnsmuris.lv.

DNS ugunsmūris

Līdzfinansē Eiropas Savienības Eiropas infrastruktūras savienošanas instruments