Latvijas universitātes
Matemātikas un informātikas institūts

CERT.LV
Informācijas tehnoloģiju
drošības incidentu
novēršanas institūcija

Aizsardzības ministrija

2021 C2

Publiskais pārskats par CERT.LV uzdevumu izpildi

2021. gada 2. ceturksnis (01.04.2021. – 30.06.2021.)

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

Saturs

Kopsavilkums

2021. gada 2. ceturksnī CERT.LV kibertelpā novēroja lielu skaitu krāpšanas kampaņu, labi pārdomātus pikšķerēšanas uzbrukumus, augstu šifrējošo vīrusu aktivitāti un daudz jaunu, kritisku ievainojamību.

2021. gada 2. ceturksnī tika reģistrētas 110 243 unikālas apdraudētas IP adreses, kas ir par 23% mazāk nekā iepriekšējā ceturksnī un par 45% mazāk nekā šajā pašā periodā pirms gada.

Pārskata periodā Latvijas interneta telpā izplatītākie apdraudējumi:

- konfigurācijas nepilnības (75 445 unikālas IP adreses) ar kritumu par 4% pret iepriekšējo periodu;
- ļaundabīgs kods (15 946 unikālas IP adreses) ar kritumu par 7%;
- ielaušanās mēģinājumi (3032 unikālas IP adreses) ar kāpumu par nepilniem 2%.

Pārskata periodā aktualizējies attālinātās piekļuves risinājumu (RDP, VNC) aizsardzības jautājums. Nepietiekami aizsargātu attālinātās piekļuves risinājumu izmantošanas rezultātā virkne uzņēmumu cietuši šifrējošo izspiedējvīrusu uzbrukumos. Bojāti galvenokārt grāmatvedības dati.

Latvijas iedzīvotājiem kļūstot par starptautisku pakalpojumu klientiem, piemēram, *Revolut*, *PayPal*, viņi kļūst par globālu pikšķerēšanas un identitātes zādzību kampaņu mērķiem. Nav nepieciešams laiks un resursi kampaņu pielāgošanai, zūd laika buferis un priekšrocības, ko sniedza nelielas valsts ar atšķirīgu valodu stāvoklis.

Attīstoties tehnoloģijām, pieejamāki kļūst risinājumi, kas ļauj uzdoties par kādu citu – viltotas e-pasta adreses, uzdodoties par sadarbības partneri un nosūtot viltotu rēķinu, viltoti telefonu numuri, uzdodoties par banku pārstāvjiem, viltoti video attēli (*deepfake*), telekonferencē uzdodoties par kādu citu. Līdzīgi incidenti notikuši arī citās valstīs.

CERT.LV norāda uz nepieciešamību ievērot procedūras, lai pārbaudītu kontaktpersonu, jo īpaši nepazīstamu, atbilstību īstenībai (e-pasts, telefons, sociālo tīklu konti).

Jauns uzbrukumu mērķis bija dažādi kriptovalūtas uzglabāšanas risinājumi. Vienā no incidentiem nodarītie materiālie zaudējumi Latvijas iedzīvotājam sasniedza 2 bitcoinus jeb gandrīz 100 000 eiro apmēru.

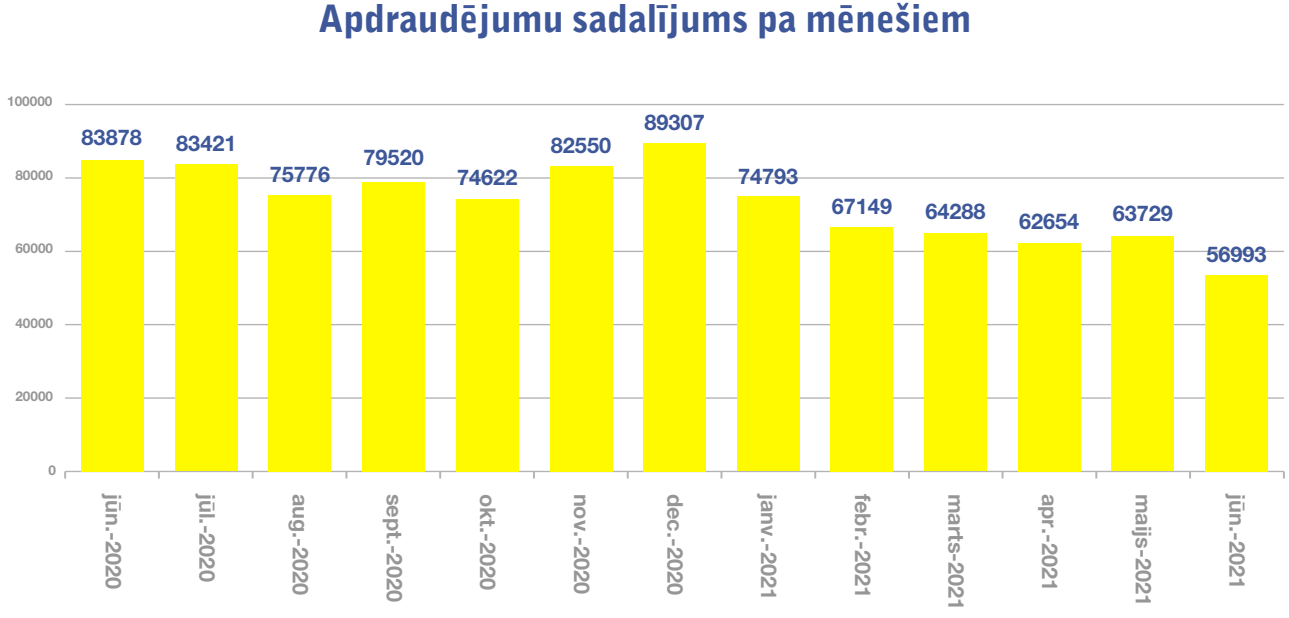
Noslēdzot pagājušajā ceturksnī atklātās kritiskās *Microsoft Exchange* e-pasta serveru ievainojamības skarto iekārtu apzināšanu, valsts un pašvaldību sektorā tika novērots manāmi zemāks kompromitēto iekārtu skaits, kā arī serveri tika atjaunināti nedēļas laikā, pretēji privātajam sektoram, kurā serveri bija ievainojami pat vairākas nedēļas. Jāatzīmē, ka līdzīga situācija kā Latvijas privātajā sektorā, bija novērojama arī ārvalstīs.

Aprīlī notika pasaulē lielākās un sarežģītākās ikgadējās starptautiskās reālā laikā notiekošās kiberaizsardzības mācības *Locked Shields*. Šogad Latvijas komanda īstenoja līdz šim nepieredzētu starpreģionālu sadarbību, mācībās startējot Latvijas – Korejas Republikas apvienotajā komandā un sekmīgi pārvarot laika zonu un valodu atšķirību radītos izaicinājumus, kā arī attīstot abu nāciju kiberspējas un pilnveidojot kā iekšējo, tā ārējo sadarbību.

Pārskata periodā CERT.LV par IT drošību izglītoja 1627 cilvēkus, iesaistoties 23 izglītojošos pasākumos.

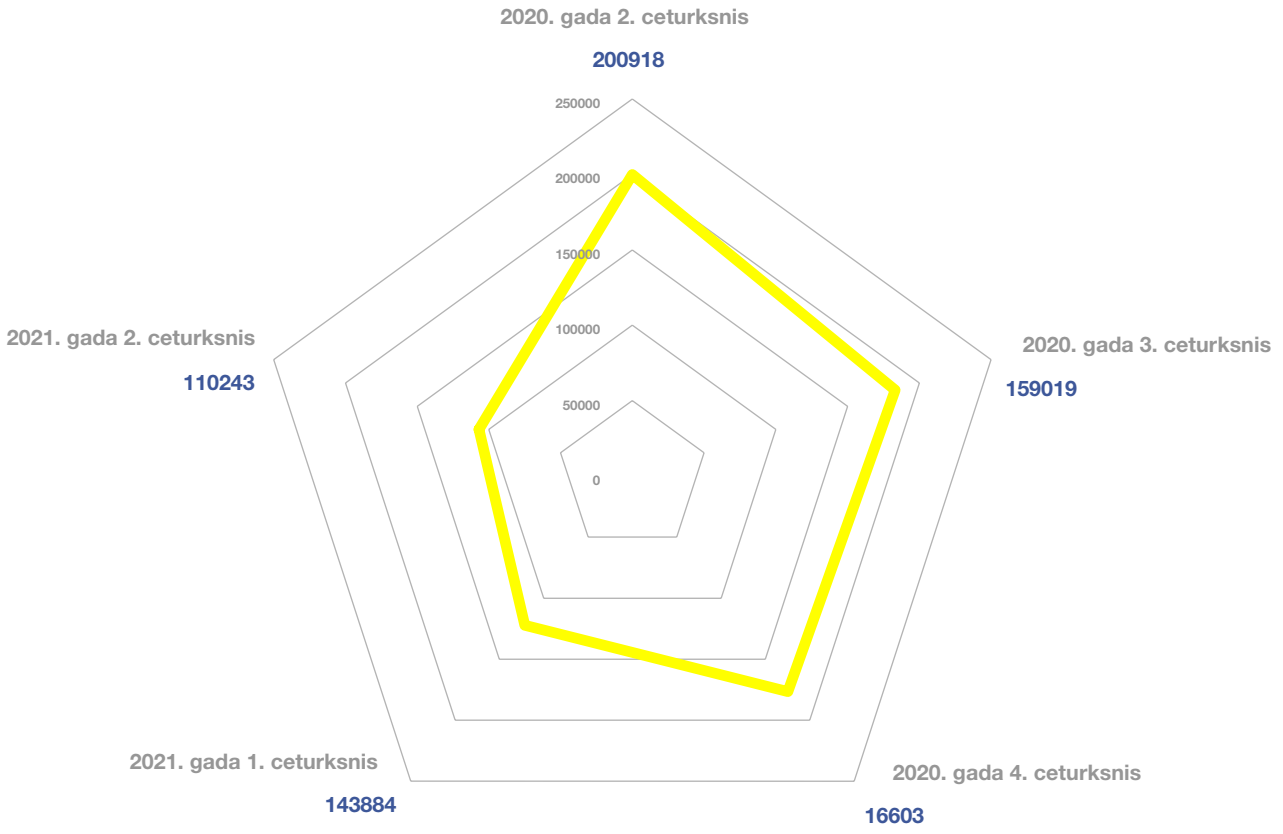
1. Elektroniskās informācijas telpā notiekošo darbību atainojums

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



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

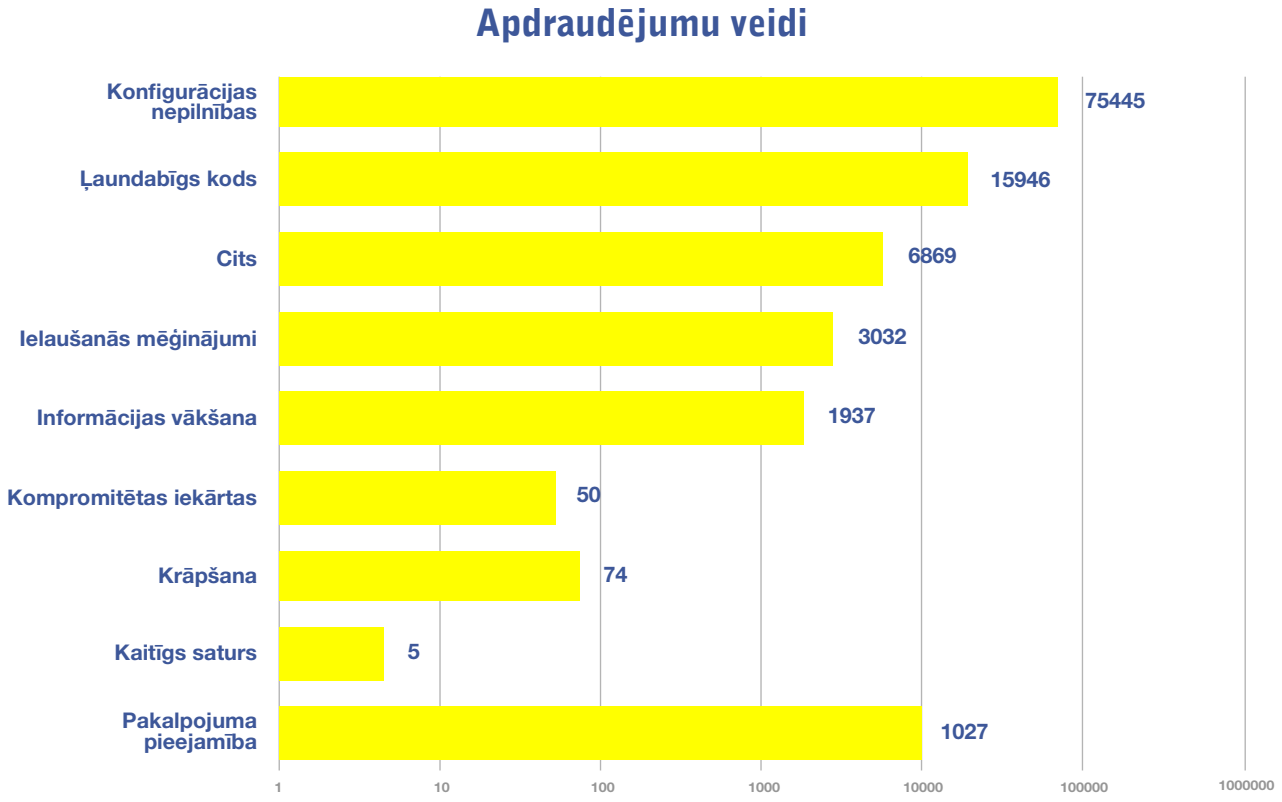
Apdraudējumu sadalījums pa ceturkšņiem



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

CERT.LV pārskata periodā ik mēnesi apkopoja informāciju vidēji par 60 000 ievainojamu unikālu IP adrešu.

2021. gada 2. ceturksnī tika reģistrētas 110 243 unikālas apdraudētas IP adreses, kas ir par 23% mazāk nekā iepriekšējā ceturksnī un par 45% mazāk nekā šajā pašā periodā pirms gada.

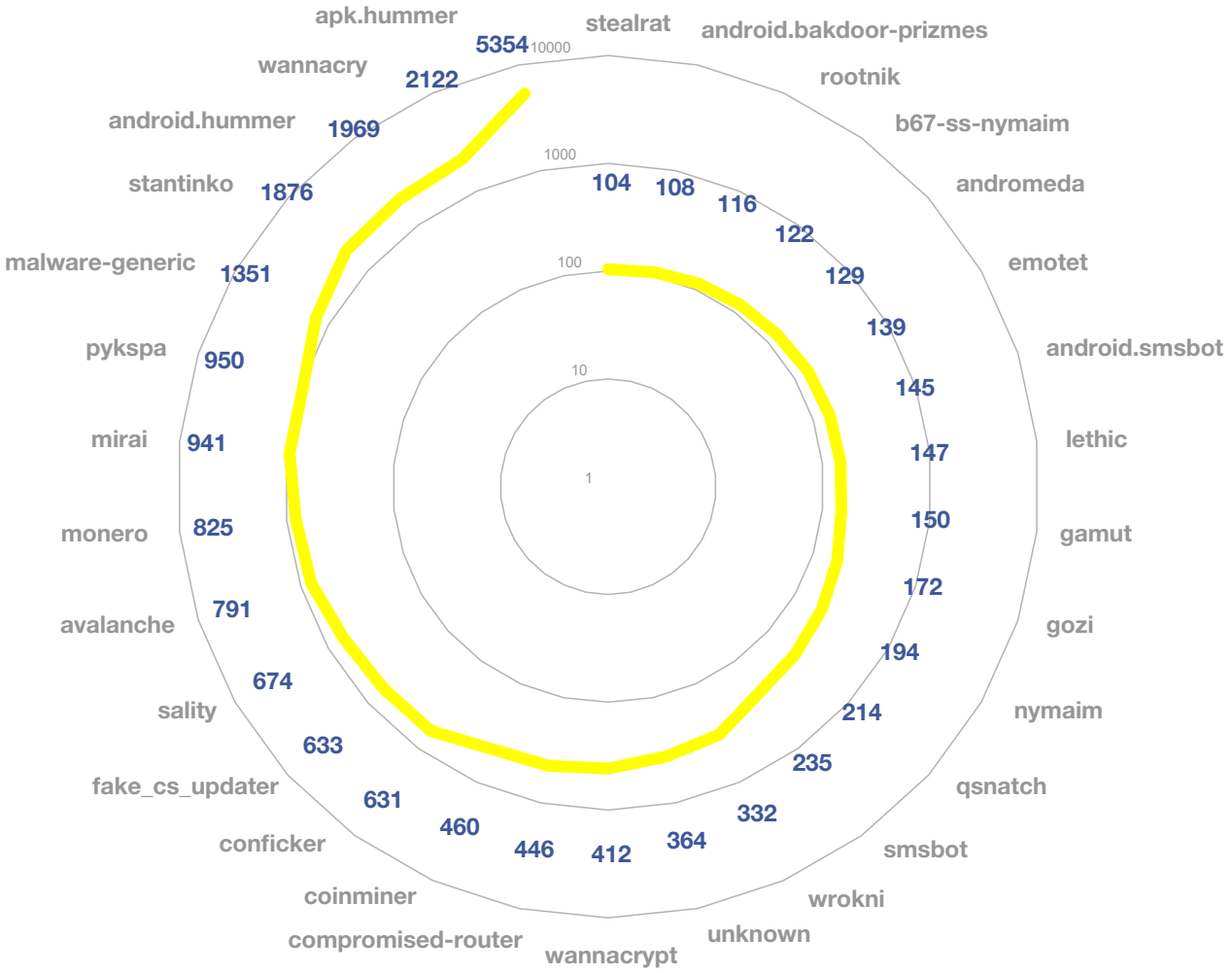


3. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 2. ceturksnī pa apdraudējumu veidiem.

Kopējo apdraudēto IP adrešu skaita kritumu veido kategorijā *Cits* (3. attēls) iekļauto notikumu apjoma samazinājums, kas aptver konsultācijas un citus pārējās kategorijās neietilpstošus notikumus.

Pārskata periodā izplatītākais apdraudējums nemainīgi bija konfigurācijas nepilnības (75 445 unikālas IP adreses) ar kritumu par 4% pret iepriekšējo periodu, otrs izplatītākais bija ļaundabīgs kods (15 946 unikālas IP adreses) ar kritumu par 7%, bet trešais – ielaušanās mēģinājumi (3032 unikālas IP adreses) ar kāpumu par nepilniem 2%.

Unikālo IP adrešu skaits – ļaundabīgs kods



4. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 2. ceturksnī ar apdraudējuma veidu – ļaundabīgs kods.

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

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

Vietu topa augšgalā saglabā arī iepriekšējā ceturkšņa jaunpienācēja – 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.

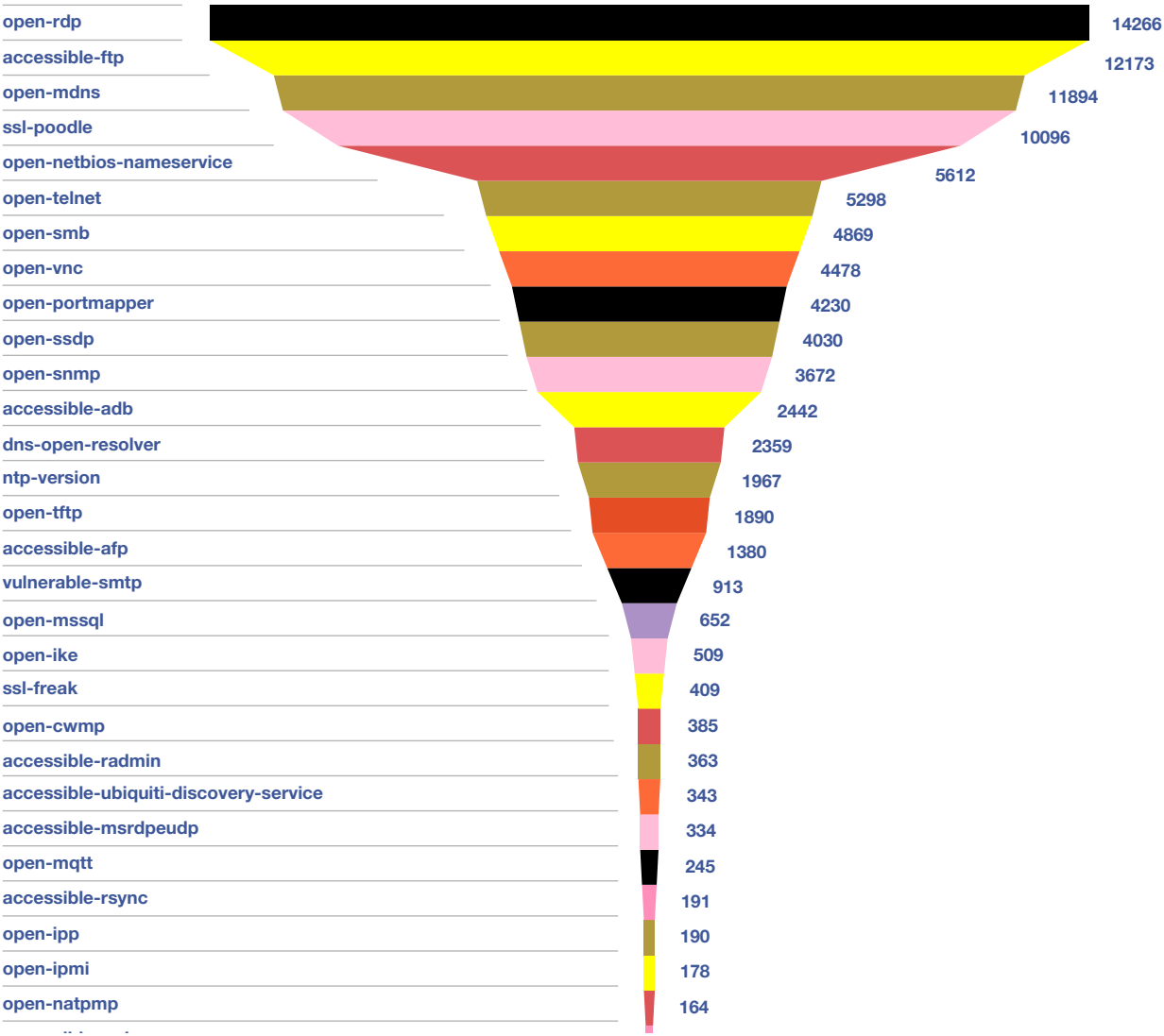
Konfigurācijas nepilnību topa līderpozīcijas ieņem ievainojamība *OpenRDP*. RDP ir attālās piekļuves risinājums, kas bieži tiek izmantots arī uzbrukumos. Ja netiek ievērota labā prakse un netiek ierobežota piekļuve RDP servisam, piemēram, ierobežojot IP adreses, kurām atļauts pieslēgties, vai nosakot piekļuvi caur VPN, uzbrucējs var pārņemt kontroli pār neatbilstoši konfigurētām iekārtām, kurās attālinātās piekļuves porti ir brīvi atvērti uz internetu un nav uzstādīta pietiekami droša piekļuves parole.

Otrajā vietā 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.

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

Pilnvērtīgākam kibersituācijas novērtējumam CERT.LV 2020. gadā ir uzsākusi Apvienotās Karalistes Nacionālā kiberdrošības centra (*NCSC*) izveidotās apdraudējumu matricas lietošanu. Matricā ievietotie apdraudējumi tiek grupēti pēc tā, cik nozīmīga ir skartā iestāde vai uzņēmums un/vai

Unikālo IP adrešu skaits – konfigurācijas nepilnības

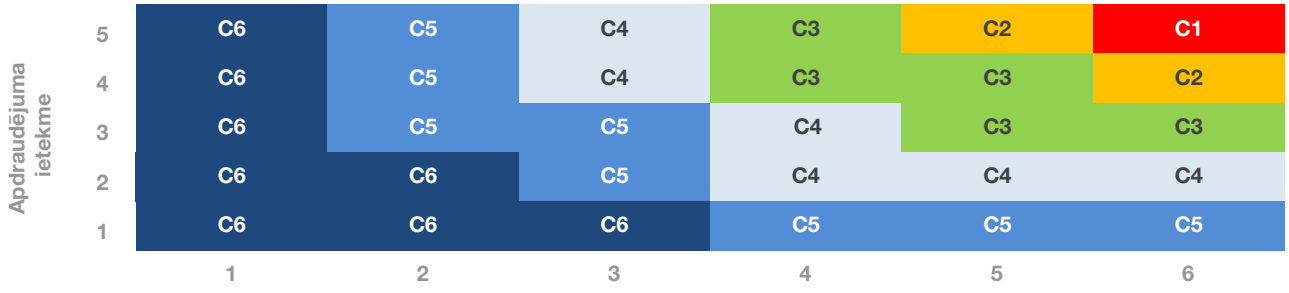


5. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits 2021. gada 2. ceturksnī ar apdraudējuma veidu – konfigurācijas nepilnība.

cik plašu sabiedrības daļu apdraudējums ietekmē, kā arī pēc tā, cik būtiskas sekas attiecīgais apdraudējums radīs. Apvienojot visus faktorus, apdraudējumi tiek iedalīti 6 kategorijās:

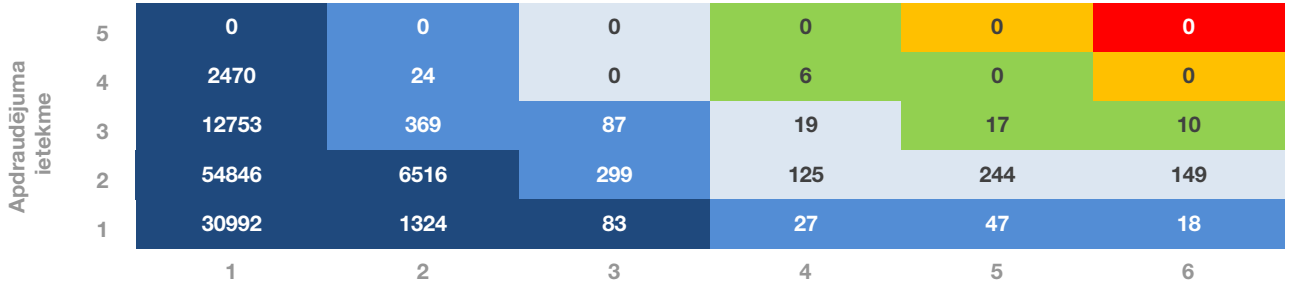
C1	Nacionāla līmeņa apdraudējums, ietekmēta pamatpakalpojumu sniegšana, apdraudēta ekonomiskā vai politiskā stabilitāte.
C2	Augstas nozīmes apdraudējumi, ietekmētas valsts iestādes, nacionālā infrastruktūra.
C3	Nozīmīgi apdraudējumi, plaša ietekme uz komerciālo sektoru, valsts un pašvaldību iestādēm.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

Apdraudējumu matrica

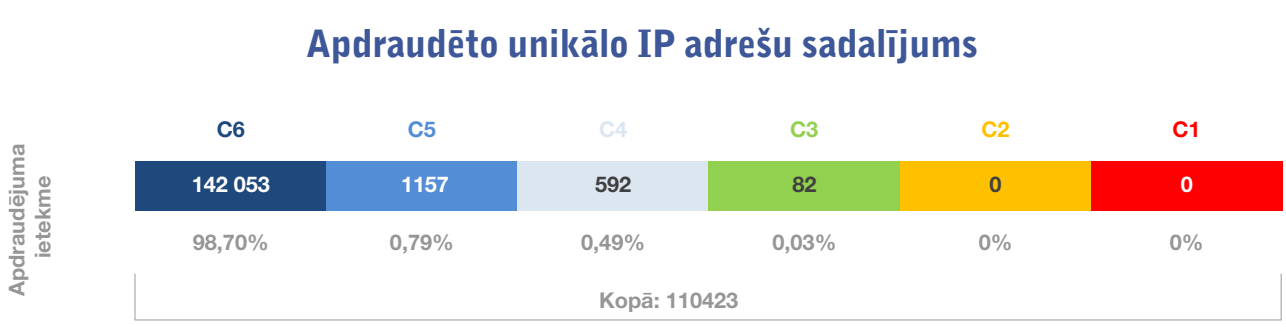


6. attēls – Apdraudējumu matricas sadalījums kategorijās.

Apdraudēto unikālo IP adrešu izvietojums



7. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu izvietojums matricā 2021. gada 2. ceturksnī valsts un pašvaldību institūcijās.



8. attēls – CERT.LV reģistrēto apdraudēto unikālo IP adrešu sadalījums apdraudējumu kategorijās pēc apdraudējuma ietekmes (matrica) 2021. gada 2. ceturksnī.

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 0,03% (33 unikālas apdraudētas IP adreses/gadījumi) no visiem kategorizētajiem apdraudējumiem. Lielākā daļa šo apdraudēto IP adrešu saistītas ar ļaunatūrām *Apk.Hummer*, *Emotet* un *Mirai* vairākās valsts un pašvaldību iestādēs.

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

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

Pārskata periodā lielākā daļa krāpniecību joprojām bija vērstas uz iedzīvotāju maksājumu karšu piekļuves datu un finanšu līdzekļu izkrāpšanu, zvanot vai sūtot iedzīvotājiem *sms* un uzdodoties par banku, kā arī imitējot populāru loģistikas uzņēmumu (*Omniva*, *DPD*) tīmekļa vietnes.

Vairumā gadījumu krāpniecības mēģinājumi tika atpazīti, tomēr atsevišķos gadījumos lietotāji ir ievadījuši krāpnieciskās vietnēs maksājumu karšu datus un cietuši finansiālus zaudējumus.

CERT.LV turpināja informēt iedzīvotājus par krāpniecībām un atgādināt, ka bankas nekad nezvana un nelūdz klientus nosaukt maksājumu karšu vai bankas konta piekļuves datus.

Latvijā 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, apdraudējumu loks, kuram iedzīvotāji tiek pakļauti, paplašinās. Latvijas iedzīvotāji kļūst par globālu pikšķerēšanas un identitātes zādzību kampaņu mērķi. Valsts valoda vairs nav šķērslis, un kampaņas vairs nav nepieciešams pielāgot, līdz ar ko zūd laika buferis un priekšrocības, ko sniedza nelielas valsts ar atšķirīgu valodu stāvoklis.

Krāpnieciskās aktivitātēs tika izmantoti arī Latvijas un ārvalstu kompāniju zīmoli, izveidojot

krāpnieciskus interneta veikalus, sociālo tīklu kontus, kā arī izplatot ziņas lietotnē *Whatsapp* par bezmaksas dāvanu, lai iegūtu lietotāju norēķinu karšu piekļuves datus.

CERT.LV informēja iedzīvotājus par krāpniecībām un centās kliedēt mītu, ka krāpnieciska rakstura ziņas lietotnē *Whatsapp* izplatās bez lietotāju starpniecības, skaidrojot, ka vairumā gadījumu šādas ziņas tiek saņemtas, jo kāda no kontaktpersonām šo ziņu ir apzināti pārsūtījusi tālāk.

Tika saņemti ziņojumi arī par pikšķerēšanas mēģinājumiem, kuros uzbrucēji centās iegūt sociālo tīklu (*Facebook*) vai e-pasta kontu piekļuves datus, uzdodoties par sociālā tīkla vai e-pasta pakalpojuma sniedzēja administrācijas pārstāvi un aicinot novērst kādu radušos problēmu, piemēram, it kā notikušu autortiesību pārkāpumu, ievadot piekļuves datus ziņojumā norādītajā saitē.

Pārskata periodā tika fiksēts arī incidents ar inovatīvu raksturu. Tika saņemts ziņojums par kādu videokonferenci, kurai pievienojusies persona, izmantojot svešu identitāti. Līdzīgi incidenti ar viltus personu pieslēgšanos videokonferencei tajā pašā laika posmā notikuši arī Lietuvā, Nīderlandē un Lielbritānijā un jāuzskata par vienotu kampaņu. Uzbrucēji varētu būt izmantojuši video attēla izmainīšanas tehnoloģijas (*deepfake*).

Paredzams, ka nākotnē šādi uzbrukumi varētu notikt arvien biežāk, jo īpaši ņemot vērā videokonferenču joprojām augošo popularitāti, kas sniedz arvien plašākas iespējas uzbrukt. Savukārt tehnoloģiju attīstība padarīs pieejamākus kvalitatīvākus un lētākus video attēla apstrādes risinājumus lielākam skaitam uzbrucēju. Plaši lietoto videokonferenču rīku nekvalitatīvais video signāls palīdz uzbrucējiem noslēpt attēla apstrādes artefaktus, kas būtu redzami augstas kvalitātes attēlā un ļautu viltojumu atpazīt.

CERT.LV aicina ieviest un ievērot procedūras, lai pārbaudītu nepazīstamu kontaktpersonu (e-pasts, telefons, sociālo tīklu konti) atbilstību īstenībai.

2.2. Pakalpojuma pieejamība (DDoS)

Pārskata periodā notikuši joprojām populārie pakalpojuma atteices (*DDoS*) uzbrukumi, šoreiz par mērķi izvēloties kādu sabiedrisko mediju un vairākus publiskā sektora interneta resursus. Vietņu *DDoS* aizsardzības risinājumi uzbrukumus veiksmīgi atvairījuši.

Apjomīgā uzbrukumā sabiedriskajam medijam Latvijā tika ietekmēts viens no tā resursiem, kas īsu brīdi bija nepieejams. Situāciju izdevās veiksmīgi atrisināt, atslēdzot resursam pieeju no ārzemēm. CERT.LV rīcībā nav informācijas, ka uzbrucēji būtu pieprasījuši izpirkuma maksu, kā tas bija iepriekšējos pārskata periodos notikušajos uzbrukumos citām Latvijas organizācijām.

CERT.LV atgādina, ka šādi pakalpojumu atteices uzbrukumi, kad uzbrucēju veiktie pieprasījumi nonāk līdz gala serverim, ir iespējami, ja nav pabeigta drošības pakalpojuma ieviešana un saskaņota resursa drošības politika.

2.3. Ļaundabīgs kods

Pārskata periodā novērotas galvenokārt divas ļaunatūras izplatīšanas metodes – šifrējošo izspiedējvīrusu nogādāšana sistēmā, izmantojot nepietiekami aizsargātus attālinātās piekļuves risinājumus (RDP, VNC), un vīrusu izplatīšana e-pastu pielikumos.

Šifrējošo izspiedējvīrusu uzbrukumos cietuši vairāki uzņēmumi. Vairumā gadījumu nošifrēti tieši grāmatvedības dati.

Lai mazinātu apdraudējumu, CERT.LV sagatavoja un publicēja rekomendācijas sistēmu administratoriem lietotāju bloķēšanai pēc vairākiem neveiksmīgiem pieslēgšanās mēģinājumiem. Šādas konfigurācijas ieviešana mazinātu uzbrucēju iespējas veikt paroļu automātisku piemeklēšanu attālinātās piekļuves risinājumiem.

E-pasti ar ļaundabīgiem pielikumiem tika izplatīti finanšu institūciju un kāda Latvijas uzņēmuma vārdā. Pielikumi saturēja galvenokārt vīrusus (*Lokibot* u.tml.), kas paredzēti lietotāja iekārtas inficēšanai un sensitīvas informācijas (lietotājvārdi, paroles) ievākšanai. Uzbrukumā cietusi kāda novada pašvaldība.

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.

2.4. Ielaušanās mēģinājumi

Ielaušanās mēģinājumi lielākajā daļā gadījumu veikti, izmantojot paroļu minēšanu (*brute-force*). Uzbrukumi veikti galvenokārt pret dažādiem interneta pakalpojumu sniedzējiem un pret dažām valsts iestādēm, kā arī dažām pašvaldībām un privātā sektora iestādēm. Pēc CERT.LV rīcībā esošās informācijas šie uzbrukumi nav bijuši sekmīgi.

2.5. Kompromitētas iekārtas un datu noplūdes

Pārskata periodā 90% kompromitēto iekārtu bija kompromitēti maršrutētāji nelielos uzņēmumos vai individuālās mājsaimniecībās.

Uzbrucēji savu uzmanību vērsa arī uz sociālā tīkla *Facebook* lietotājiem, kuru pārziņā ir uzņēmuma vai organizācijas *Facebook* profils, ar mērķi pārņemt šī lietotāja kontu.

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

2.6. Ievainojamības

Kritiska *nulles dienas* ievainojamība tika konstatēta *Pulse Secure* ražotajās privātā tīkla (VPN) iekārtās. Ievainojamība sniedza uzbrucējiem iespēju veikt attālinātu koda izpildi. CERT.LV veica ievainojamo iekārtu apzināšanu Latvijā. Tika konstatētas četras potenciāli ievainojamas iekārtas, no kurām viena bija kādā no Latvijā esošām maksājumu transakciju apstrādes uzņēmumiem. Uzņēmums demonstrēja augstu gatavības pakāpi un operatīvi novērsa apdraudējumu.

Kāda uzņēmuma ražotai produkcijai tika konstatēta ievainojamība, par kuru ražotājs informēja arī savus klientus, taču vairākos gadījumos jau bija noticis veiksmīgs uzbrukums – serverī glabātie faili tika sašifrēti un par datu atgūšanu pieprasīts izpirkums. Uzbrukumā cieta daži Latvijas uzņēmumi. CERT.LV cietušajiem ieteica sazināties ar ražotāju.

Tika noslēgta pagājušajā ceturksnī atklātās kritiskās *Microsoft Exchange* e-pasta serveru ievainojamības skarto iekārtu apzināšana. Valsts sektorā un pašvaldībās tika novērots manāmi zemāks kompromitēto iekārtu skaits, iespējams, pateicoties salīdzinoši ātrai un aktīvai komunikācijai no CERT.LV puses par iespējamo apdraudējumu. Valsts un pašvaldību e-pasta serveri tika atjaunināti nedēļas laikā, pretēji privātajam sektoram, kurā serveri bija ievainojami pat vairākas nedēļas. Jāatzīmē, ka līdzīga situācija kā Latvijas privātajā sektorā, bija novērojama arī ārvalstīs.

Gadījumos, kad tika atklāta servera kompromitēšana, nav novērotas pazīmes, kas liecinātu par uzbrucēju pārvirzīšanos uz iekšējo tīklu. Infekcija tika laicīgi atpazīta un serveri tika fiziski atslēgti no tīkla. Taču jāņem vērā, ka, lai gan šobrīd nav gūti pierādījumi tam, ka uzbrucēji būtu pārvirzījušies uz citām iekšējām sistēmām, nevar pilnīgi droši pieņemt, ka viņi to nav izdarījuši, tāpēc jāturpina sistēmu novērošana.

2.7. Atbildīga ievainojamību atklāšana

Tika saņemts ziņojums par starpvietņu skriptēšanas (*XSS*) ievainojamību kādā plaši apmeklētā tīmekļa vietnē. Starpvietņu skriptēšanas ievainojamība sniedz uzbrucējam iespēju izpildīt patvaļīgu kodu citu

lietotāju aplūkotajās tīmekļa vietnēs, piemēram, pārvirzot lietotāju uz kaitīgu vietni, kā arī apiet vietņu piekļuves drošības mehānismus.

Tika saņemti pāris ziņojumi par *SQL* injekcijas ievainojamībām iestāžu tīmekļa vietnēs. *SQL* injekcijas sniedz uzbrucējam iespēju viltot savu identitāti, piekļūt uz servera esošiem datiem, tos patvaļīgi mainīt, dzēst vai nodot trešajām pusēm. Par ievainojamībām tika informēti vietņu uzturētāji un vienā no gadījumiem to izdevās novērst uzreiz, otrā – norit darbs.

2.8. Drošības testi

Tika veikti apjomīgi drošības testi kādas valsts iestādes resursam. Testu gaitā tika konstatētas dažas vidējas nozīmes nepilnības, par kurām tika informēts resursa uzturētājs.

Notika arī atkārtota pārbaude kādam valsts iestādes resursa autentifikācijas modulim. Lai arī sākotnējā testēšanā tika atklātas būtiskas moduļa drošības nepilnības, atkārtotā testēšana ļāva secināt, ka visi iepriekš atklātie trūkumi ir novērsti.

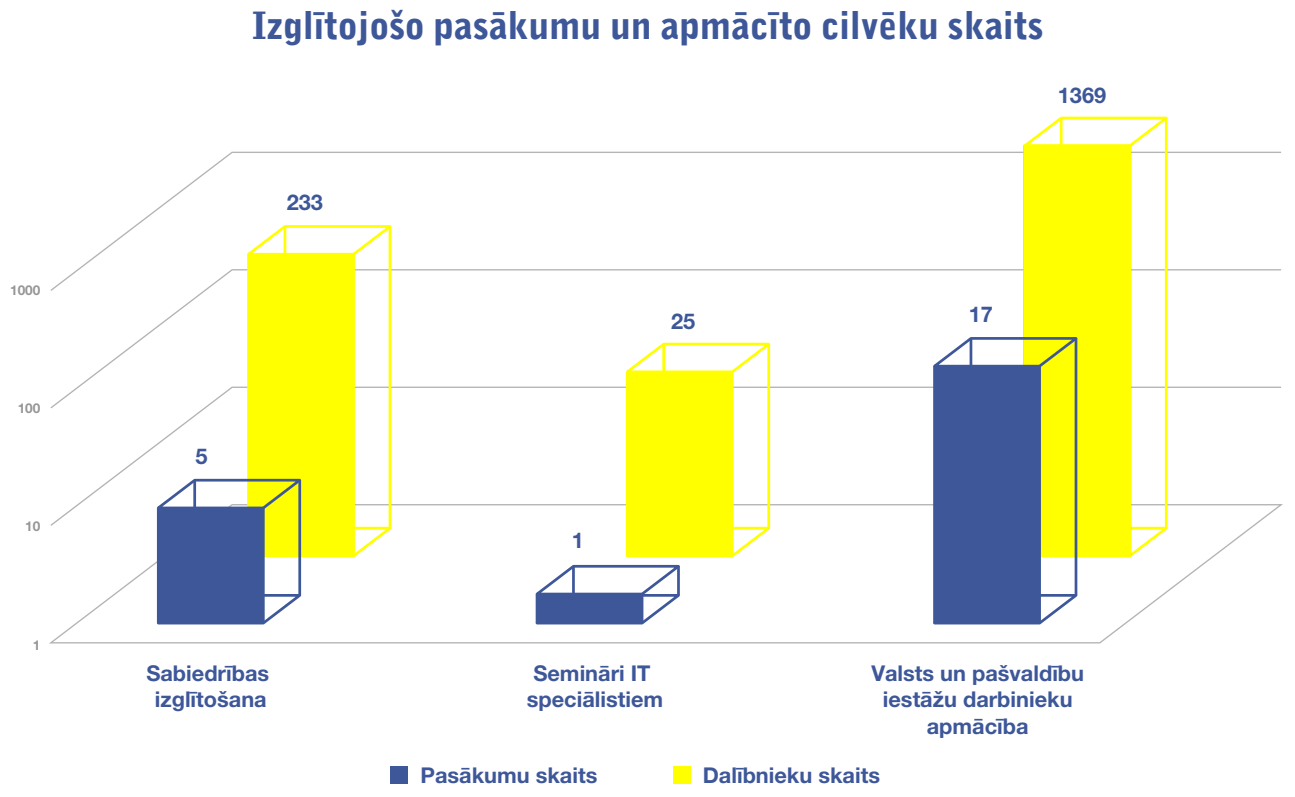
Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta arī CERT.LV tīmekļa vietnē un sociālo tīklu *Twitter* (@certlv) un *Facebook* (@cert.lv) kontos.

Cita veida sadarbība ar dažādām iestādēm ir norādīta pārskata 4. un 5.punktā.

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

13. – 16. aprīlim notika pasaulē lielākās un sarežģītākās ikgadējās starptautiskās reālā laikā notiekošās kiberaizsardzības mācības *Locked Shields*. Tās organizē NATO apvienotais

kiberaizsardzības izcilības centrs (*NATO CCDCoE*). Šogad Latvijas komanda īstenoja līdz šim nepieredzētu starpreģionālu sadarbību, piedaloties mācībās Latvijas – Korejas Republikas apvienotā komandā. Latvijas – Korejas Republikas apvienotās komandas uzdevums bija, sacensībā ar 21 citu valstu komandu, atbilstoši mācību scenārijam atvairīt kiberuzbrukumus, nosargāt infrastruktūru un reaģēt uz dažādiem stratēģiskiem izaicinājumiem, respektējot starptautiskos normatīvos aktus un likumus. COVID-19 pandēmijas apstākļos apvienotās komandas darbs tika koordinēts attālināti, sekmīgi pārvarot izaicinājumus, kurus sagādāja būtisko laika zonu un valodu atšķirības. Šādas, starpreģionālas apvienotās komandas pieredze sniedza iespēju attīstīt abu nāciju kiberspējas un pilnveidot kā iekšējo, tā ārējo sadarbību.



9. attēls – Izglītojošo pasākumu un apmācīto cilvēku skaits 2021. gada 2. ceturksnī

Pārskata periodā CERT.LV par IT drošību izglītoja 1627 cilvēkus, iesaistoties 23 izglītojošos pasākumos. Ņemot vērā epidemioloģisko situāciju valstī un ar to saistītos ierobežojumus, visi pasākumi notika tiešsaistē.

CERT.LV iepazinās ar *SIA Smart* use izstrādāto galda spēli ikdienas kiberdrošības pratības apguvei un pilnveidošanai, sniedzot rekomendācijas spēles uzlabojumiem.

Ar starptautiskās kiberdrošības konferences Kiberšahs organizēšanu saistītie darbi:

Ņemot vērā pandēmijas apstākļus un ar to saistītos ceļošanas un pulcēšanās ierobežojumus, konference *Kiberšahs* arī 2021. gadā netiks rīkota. Rudenī tiek plānota tehniskā tiešsaistes konference *Kiberšoks 2021*, kurā ar praktiskiem piemēriem un demonstrācijām zināšanās dalīsies pasaules līmeņa kiberdrošības eksperti, darba valoda – angļu. Plānots, ka šogad konference norisināsies 6. – 7. oktobrī. Konferences programma šobrīd vēl ir skaņošanas procesā, tā būs pieejama konferences tīmekļa vietnē https://cybershock.lv. Aktuālā informācija tiks publicēta arī CERT.LV sociālo tīklu *Twitter* (@certlv) un *Facebook* (@cert.lv) kontos, kā arī CERT.LV tīmekļa vietnē https://www.cert.lv.

Pārskata periodā mediju uzmanības centrā bija praktiskā kiberdrošība gan iedzīvotājiem, gan uzņēmumiem, un krāpnieciskie telefona zvani, kuri tika veikti ar mērķi izkrāpt no iedzīvotājiem maksājumu karšu piekļuves datus un finanšu līdzekļus.

Eiropas Savienības Tīklu un informācijas sistēmu direktīvas (NIS Directive) CSIRT tīkla darba grupa *Cyber Weather* regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai. Izmantojot šīs grupas izstrādātās vadlīnijas, CERT.LV savā tīmekļa vietnē https://www.cert.lv ievieto ikmēneša kiberlaikapstākļu informāciju, kas ir atskats uz Latvijas kibertelpas iepriekšējā mēneša aktuālākajiem notikumiem.

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

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

Sadarbības tikšanās, konsultācijas un prezentācijas:

- 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.
- Dalība Izglītības un zinātnes ministrijas vadītajā darba grupā, un iesniegti komentāri par profesijas standarta *Informācijas drošības vadītājs* izmaiņām.
- CERT.LV piedalījās Ministru kabineta noteikumos Nr. 442 *Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām* (MK Nr. 442) izmaiņu sagatavošanas darbā.
- CERT.LV piedalījās VARAM organizētā sanāksmē 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*, apspriežot privātā sektora komersantiem izvirzāmās prasības, lai pieslēgtos valsts IKT infrastruktūrai. CERT.LV un Aizsardzības ministrija pauda viedokli par nepieciešamību arī šajā gadījumā piemērot MK Nr. 442 noteiktās prasības.
- Sadarbībā ar Latvijas Zinātnes padomi (LZP) un Elektronikas un datorzinātņu institūtu (EDI) projektā par valkājamo ierīču drošību tika veikta testējamā prototipa modeļa izstrāde.
- Iesaiste mācību *Medus pods 2022* plānošanā, kurās tiks iekļautas vairākas kiberkomponentes, kā arī tiks iekļauti elektroenerģijas apgādes elementi un iesaistīti kritiskās infrastruktūras pārstāvji, veicinot sinerģiju starp nozari un NBS.

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

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

CERT.LV starptautiskā sadarbība pārskata periodā:

- CERT.LV aktīvi piedalījās trijās no piecām NIS (Tīklu un informācijas drošības) direktīvas CERTu tīkla darba grupām:
  - *Cyber Weather* darba grupā, kura regulāri apkopo informāciju par būtiskākajiem kiberincidentiem un reizi ceturksnī izstrādā kiberlaikapstākļu pārskatu Eiropai.
  - *Maturity* darba grupā, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.
  - *Terms of Reference Review* darba grupā, kas pārskata tīkla statūtus un nolikumu, atbilstoši tos aktualizējot.
- Darbs FIRST darba grupas *CSIRT Framework* darbā, lai izstrādātu vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm.
- CERT.LV vadītāja Baiba Kaškina turpināja darbu kā *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejas) līdzpriekšsēdētāja (*co-chair*), piedaloties jauno biedru pieteikumu izskatīšanā un veicinot biedru uzņemšanas procesa uzlabošanu.
- CERT.LV turpināja darbu TF-CSIRT *Futures* darba grupā, lai izstrādātu jaunu pārvaldības modeli TF-CSIRT un Trusted Introducer Eiropas CERTu sadarbībai.
- 13. – 16. aprīlī notika pasaulē lielākās un sarežģītākās ikgadējās starptautiskās reālā laikā notiekošās kiberaizsardzības mācības *Locked Shields*. Tās organizē NATO Apvienotais kiberaizsardzības izcilības centrs (NATO CCDCoE). Šogad Latvijas komanda īstenoja līdz šim nepieredzētu starpreģionālu sadarbību, piedaloties mācībās Latvijas – Korejas Republikas apvienotā komandā. COVID-19 pandēmijas apstākļos apvienotās komandas darbs tika koordinēts attālināti, sekmīgi pārvarot izaicinājumus,

kurus sagādāja būtisko laika zonu un valodu atšķirības. Šādas, starpreģionālas apvienotās komandas pieredze sniedza iespēju attīstīt abu nāciju kiberspējas un pilnveidot kā iekšējo, tā ārējo sadarbību.

- 15. maijā CERT.LV pārstāvis piedalījās darba grupas *EU Cybersecurity Index Working Group* sanāksmē. Darba grupas mērķis ir ES dalībvalstu kiberdrošības līmeņa novērtēšana, lai noteiktu kopējo ES kiberdrošības līmeni, kā arī pastāvošo noteikumu un vadlīniju ietekmes uz kiberdrošību un kiberdrošības ietekmes uz uzņēmumu darbību izvērtēšana.
- 31. maijā – 4. jūnijam dalība 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*) *TTX*, kuru mērķis ir veicināt un pilnveidot kritiskas enerģētikas sektora infrastruktūras kiberdrošību Baltijas valstīs.
- 2. – 3. jūnijā notika NIS direktīvas CERTu tīkla sanāksme, kurā CERT.LV sniedza prezentāciju *Trust Issues in Digital Signing*, aplūkojot dinamiskā satura aspektu parakstāmajos dokumentos.
- 7. – 9. jūnijā notika FIRST konference. CERT.LV darbojās konferences programmkomitejā un palīdzēja izveidot konferences saturu.
- CERT.LV pārstāvis aktīvi piedalījās NATO CCDCoE organizēto praktisko kiberdrošības mācību *Crossed Swords 2021* organizēšanā, iesaistoties mācību plānošanā un veidojot tehnisko scenāriju. Mācības plānotas 2021.gada decembrī.
- Dalība *EU CyberNet* projektā kā vienam no partneriem. Projekta mērķis ir stiprināt kiberdrošības ekspertīzi un attīstīt to ne tikai Eiropas Savienībā, bet arī ārpus tās robežām (www.eucybernet.eu). Dalība projektā sniegs iespēju CERT.LV ekspertiem, iesaistoties projekta dalībvalstu projektos, stiprināt savas zināšanas un kapacitāti, kā arī dalīties ar to ārpus Eiropas Savienības robežām, tā stiprinot starptautisko kiberdrošības kopienu.

- Dalība ENISA veiktā 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 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, kas dokumenta formā tiktu izplatīti visu dalībvalstu pārstāvjiem.
- Turpinājās aktīva dalība enerģētikas informācijas apmaiņas un sadarbības grupā *Energy ISAC Camelot*, lai veicinātu informācijas apmaiņu un sekmētu enerģētikas sektora kiberdrošību. Pārskata periodā grupas ietvaros tika prezentēta CERT.LV izveidotā SCADA laboratorija, kas tika ļoti atzinīgi novērtēta.
- CERT.LV pārstāvis piedalījās divos Kanādas valdības semināros, lai diskutētu par koordinētas ievainojamību atklāšanas labo praksi pasaulē un sekmētu Kanādai piemērotākā modeļa izvēli. 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.

Sadarbība konkrētu incidentu risināšanā aplūkota pārskata 2. punktā.

6. Projekta "Cyber Exchange" īstenošana

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

Projekta mērķis ir stiprināt starptautisku sadarbību starp nacionālajām un valdības CSIRT/CERT organizācijām. *Cyber Exchange* projekts ir kā atbilde arvien pieaugošajiem draudiem kiberdrošības jomā, īpašu akcentu vēršot uz nepieciešamo pārrobežu sadarbību cīņā pret tiem. Latvija ir viena no 10 Eiropas valstīm, kas piedalās projektā. Projekta pamata aktivitāte ir pieredzes apmaiņas vizīšu organizēšana – Latvijas CERT.LV pārstāvjiem viesojoties pie citu projekta dalībvalstu CSIRT/CERT komandām vai uzņemot vizītē kolēģus no citām CSIRT komandām.

Pārskata periodā COVID-19 ierobežojumu dēļ projektā paredzēto apmaiņas vizīšu īstenošana nebija iespējama, un projekta termiņš tika pagarināts līdz 2022. gada 30. jūnijam.

7. Citi normatīvajos aktos noteiktie pienākumi

- Tika turpināts darbs pie CERT.LV un NIC.LV (Augstākā līmeņa domēna .lv reģistra uzturētājs) izstrādātā DNS RPZ (*Domain Name Service Response Policy Zone*) jeb DNS ugunsmūra (*DNS firewall*) projekta īstenošanas. DNS mūris ik dienu tiek papildināts ar Latvijas iedzīvotāju un kiberdrošības ekspertu sniegto informāciju par kiberuzbrucēju aktivitātēm Latvijas kibertelpā un sniedz iespēju aizsargāt lietotājus no ļaundabīga satura internetā.

  Projekta ietvaros ir bijuši jau daudzi gadījumi, kuros nostrādājusi aktīvā aizsardzība, pasargājot lietotājus no ļaundabīga satura un iekārtas no inficēšanas. Nozīmīgākās apturētās kampaņas:

  - viltus loterijas un tīmekļa vietnes maksājumu karšu datu izkrāpšanai – apturēti 8022 lapu pieprasījumi;
  - viltus banku tīmekļa vietnes – novērsti 274 vietņu atvēršanas mēģinājumi;
  - viltus kurjerkompāniju vietnes – novērsti 120 vietņu atvēršanas mēģinājumi;
  - novērsti 312 datora inficēšanas mēģinājumi.

Daļu no DNS PRZ pakalpojuma var izmantot bez līguma slēgšanas un autorizēšanās jebkurš interneta lietotājs. Lai to izmantotu, jālieto NIC.LV rekursīvie DNS serveri. Tīmekļa vietnē https://dnsmuris.lv pieejamas ērti lietojamas instrukcijas DNS ugunsmūra aktivizēšanai.

- 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 turpināja uzraudzīt Sertificētu uzticamības pakalpojumu sniedzēju darbību.

8. Papildu pasākumu veikšana

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.04.2021. līdz 30.06.2021. ir saņēmusi un izvērtējusi 11 690 ziņojumus. No tiem 11 504 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 7 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 18 ziņojumos konstatēta personas goda un cieņas aizskaršana, 4 ziņojumi saņemti par naida runu un 2 ziņojumi par vardarbību atainojošiem materiāliem. Par finanšu krāpšanas mēģinājumiem internetā saņemti 43 ziņojumi, 52 ziņojumu saturs nav bijis pretlikumīgs, 60 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 11180 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 11 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem 11 493 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 11 382 ziņojumi ir dzēsti no publiskas aprites un 122 ziņojuma saturs atrodas dzēšanas procesā sadarbībā ar Valsts policiju un interneta pakalpojumu sniedzējiem.

2021. gada 12. jūlijā.

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