CERT.LV DARBĪBAS PĀRSKATS

2024

CERT.LV
Informācijas tehnoloģiju drošības incidentu novēršanas institūcija

Latvijas universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Pārskatā iekļauta vispārpieejama informācija par CERT.LV aktivitātēm un darbības rezultātiem, neietverot ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

Satura rādītājs

Kopsavilkums

Latvija turpina sastapties ar augtu kiberapdraudējumu līmeni, ko rada gan finansiāli, gan politiski un ideoloģiski motivēti kiberuzbrukumi. Kiberapdraudējumu ainava mainās sarežģītu kiberuzbrukumu rezultātā, kuros tiek izmantota gan cilvēku neuzmanība, gan tehnoloģiju ievainojamības, kiberuzbrucējiem gudri pielietojot pikšķerēšanu, mērķētu ļaunatūras piegādi un vāju autentifikāciju.

2024. gada 2. ceturksnī CERT.LV tika reģistrētas 388 922 apdraudētas unikālas IP adreses, kas ir augstākais rādītājs pēdējo divu gadu laikā. Pret iepriekšējo ceturksni kāpums ir 11% un salīdzinājumā ar pagājušā gada 2. ceturksni par 16% vairāk.

Vienlaikus situācija kibertelpā vērtējama kā stabila, un tā ir labi aizsargāta. Latvijas informācijas un komunikāciju tehnoloģiju (IKT) infrastruktūra ir arvien noturīgāka pret kiberuzbrukumiem – līdz šim tie nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību, tās drošību un svarīgajiem pakalpojumiem. Varam lepoties ar izciliem kiberdrošības profesionāļiem. Tomēr tam nevajadzētu mums ļaut atslābt, jo kiberdrošības jomā attīstība notiek nepārtraukti, kas liek meklēt un ieviest arvien jaunus kibernoturības celšanas pasākumus.

Būtiskākie kiberdrošības apdraudējumi un tendences: Pārskata periodā fiksēts viens augstas nozīmes kiberuzbrukums, kas tika veikts valsts iestādē, izmantojot VPN, kam nebija iespējota divfaktoru autentifikācija. Taču tas neradīja paliekošas sekas uz sabiedrību. Nozīmīgi apdraudējumi ar plašu ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 0,02% no visiem kategorizētajiem apdraudējumiem, kas ir gandrīz uz pusi mazāk nekā 1. ceturksnī, bet par 75% vairāk nekā pagājušā gada 2. ceturksnī. Savukārt būtiski apdraudējumi ar vidēju ietekmi veido 0,65% no visiem kategorizētajiem apdraudējumiem: apdraudēto IP adrešu skaits ir par 11% vairāk nekā 1. ceturksnī un par 16% lielāks nekā pagājušā gada 2. ceturksnī.

Kompromitētas iekārtas, ļaundabīgs kods un ielaušanās mēģinājumi no visiem apdraudējuma veidiem bija ar lielāko aktivitātes pieaugumu 2024. gada 2. ceturksnī. Ielaušanās mēģinājumu skaits turpina virzīties uz augšu, sasniedzot augstāko rādītāju pēdējo divu gadu laikā, turklāt kopš gada sākuma tas ir palielinājies par 56% un salīdzinājumā ar pagājušā gada 2. ceturksni vairāk nekā 2 reizes. No ģeopolitiskās situācijas skatupunkta tas skaidrojams ar Krievijas atbalstītiem hakeru kiberuzbrukumiem un centieniem kompromitēt IKT kritisko infrastruktūru NATO un ES dalībvalstīs, kuras pauž nelokāmu atbalstu Ukrainas tautai cīņā pret Krieviju.

Lai piekļūtu valsts iestāžu un IKT kritiskās infrastruktūras resursiem, naidīgu valstu, tostarp Krievijas, atbalstīti kiberuzbrucēji izmantojuši dažādas ielaušanās mēģinājumu metodes: pielietota autentifikācijas līdzekļu piemeklēšana, publiski zināmu ievainojamību izmantošana, tīmekļvietņu kompromitēšana, VPN un e-pasta vārteju kompromitēšana, pikšķerēšana un mērķēta ļaunatūras piegāde ar e-pasta starpniecību. Šādas tendences norāda uz nepieciešamību pastiprināt drošības pasākumus un izglītot sabiedrību par potenciālajiem kiberdraudiem.

Turklāt tas apstiprina, ka valstī nepieciešama minimālo kiberdrošības prasību ievērošanas uzraudzība, kā arī viegli pieejami efektīvi kiberdrošības pakalpojumi un IKT drošības telemetrijas apstrāde, kas kvalitatīvi un atbilstoši aktuālajiem izaicinājumiem spētu atbalstīt publiskā sektora tehniskos un cilvēkresursus pret aizvien pieaugošiem kiberdraudiem. Par CERT.LV nodrošināto bezmaksas pakalpojumu klāstu plašāk: **https://www.cert.lv/pakalpojumi**.

Krāpniecības apmēri uzņem apgriezienus: 2024. gada 2. ceturksnī CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits apdraudējumu veidā "Krāpšana" ir palielinājies par 45% salīdzinājumā ar 1. ceturksni un par 70% salīdzinājumā ar pagājušā gada 2. ceturksni; ik mēnesi tiek izkrāpts vismaz 1 miljons eiro. 3 izplatītākie krāpniecības veidi - vikšķerēšana, pikšķerēšana un smikšķerēšana. Visbiežāk dažādu valsts iestāžu, kurjerpastu un finanšu iestāžu vārdā masveidā tiek sūtītas īsziņas un e-pasta vēstules ar viltus saitēm, iestrādātu QR kodu vai pievienotu ļaunprātīgu

pielikumu maskētu kā rēķinu. Sekojot līdzi aktualitātēm, krāpnieki aktivizējas un izmanto tās, it īpaši ienākumu deklarācijas iesniegšanas laiku, naudas izkrāpšanai. Mānīšanās zvani un darījuma sarakstes kompromitēšanas gadījumi ir kļuvuši par nopietnu problēmu, kas ietekmē daudzus uzņēmumus un iedzīvotājus. Neuzmanība un slikta kiberhigiēna palielina krāpniecības riskus.

CERT.LV turpina veicināt kiberdrošību un būt par uzticamu viedokļa līderi Latvijas kibertelpā.

Pakalpojuma pieejamība: Turpinās viļņveidīgi piekļuves lieguma jeb DDoS uzbrukumi, tostarp Krievijas un to atbalstošo haktīvistu mērķēti kiberuzbrukumi pret valsts iestāžu un specifisku nozaru uzņēmumiem, taču tie tika veiksmīgi atvairīti, turklāt liela daļa automātiski. Salīdzinot ar 2023. gada 2. ceturksni, DDoS uzbrukumu skaits ir samazinājies teju uz pusi. Un tā nav nejaušība – Latvija prot sevi aizstāvēt, padarot sevi par grūtu un neinteresantu mērķi šādiem kiberuzbrukumiem.

Ievainojamības un ietekmējamas sistēmas: Tas ir pastāvīgs risks, ko ietekmē jaunatklātās kritiskās ievainojamības, nepareiza IT sistēmu konfigurācija un piegādes ķēžu uzbrukumi. Joprojām lielākā daļa kiberuzbrukumu tiek veikti, izmantojot publiski zināmas ievainojamības, tāpēc savlaicīga konfigurācijas nepilnību apzināšana un ievainojamību lāpīšana var būtiski uzlabot kiberdrošības situāciju.

Draudu medību operācijas: Līdz pārskata perioda beigām analizētas vairāk nekā 140 000 iekārtas 31 organizācijā – Latvija ir līderis draudu medību operāciju organizēšanā un vadīšanā Eiropas Savienībā (ES). 25% jeb 8 organizācijās ar augstu ticamību identificēta citu valstu iebrucēju (APT) klātbūtne, veikta identificētās uzbrucēja klātbūtnes likvidēšana, kā arī atklāti citi būtiski apdraudējumi, kurus mērķa organizācijām bija iespēja novērst, pieņemot datos balstītus lēmumus.

Pārskata perioda beigās CERT.LV noslēdza paplašinātas klātbūtnes draudu medību operāciju, kurā piedalījās Kanādas bruņoto spēku kiberpavēlniecības, Kanādas kiberdrošības centra un Latvijas bruņoto spēku pārstāvji. Paplašinātā klātbūtne spēcināja un papildināja pastāvīgi notiekošās draudu medības. Vairākas sabiedroto valstis apmeklēja notiekošo paplašinātās klātbūtnes operāciju, lai mācītos no Latvijas un Kanādas veiksmīgās sadarbības, un, iespējams, pārņemtu labo praksi, lai īstenotu to atbildības jomās savās valstīs.

Drošības testi un izvērtējumi: CERT.LV, cieši sadarbojoties ar Centrālās vēlēšanu komisijas, Valsts kanceleju un citām vēlēšanu procesā iesaistītajām institūcijām, strādāja, lai veiktu ielaušanās testus visām sistēmām, kas iesaistītas Eiropas Parlamenta (EP) vēlēšanu norises nodrošināšanā. Pārskata periodā Latvijā netika novērots neviens incidents, kas būtu tieši saistāms ar vēlēšanu sistēmām vai vēlēšanu drošību.

DNS ugunsmūra efektivitāte: 2. ceturksnī apstrādātais pieprasījumu skaits DNS ugunsmūra pakalpojuma ietvaros bija vairāk nekā 1 miljons, pasargājot pakalpojuma lietotājus no ļaundabīgu vietņu apmeklēšanas. Ikviens atklātais apdraudējuma indikators nonāk centralizētā aktīvās aizsardzības infrastruktūrā, lai pasargātu visus Latvijas iedzīvotājus un organizācijas, kas izmanto CERT.LV un NIC.LV nodrošināto bezmaksas aizsardzību.

Sensoru tīkla (ABS) efektivitāte: ABS ik mēnesi fiksē vidēji 6 000 augstas prioritātes incidentus valsts, pašvaldību un IKT kritiskās infrastruktūras iestādēs. 2. ceturksnī ABS ģenerēto brīdinājumu skaits bija gandrīz divreiz lielāks nekā 1. ceturksnī. Šāda pieauguma iemesls galvenokārt bija ļoti plaša mēroga un apjoma pikšķerēšanas kampaņas VID un "Latvijas Pasts" vārdā, attiecīgi pārskata periodā pārspējot visus iepriekšējos rekordus.

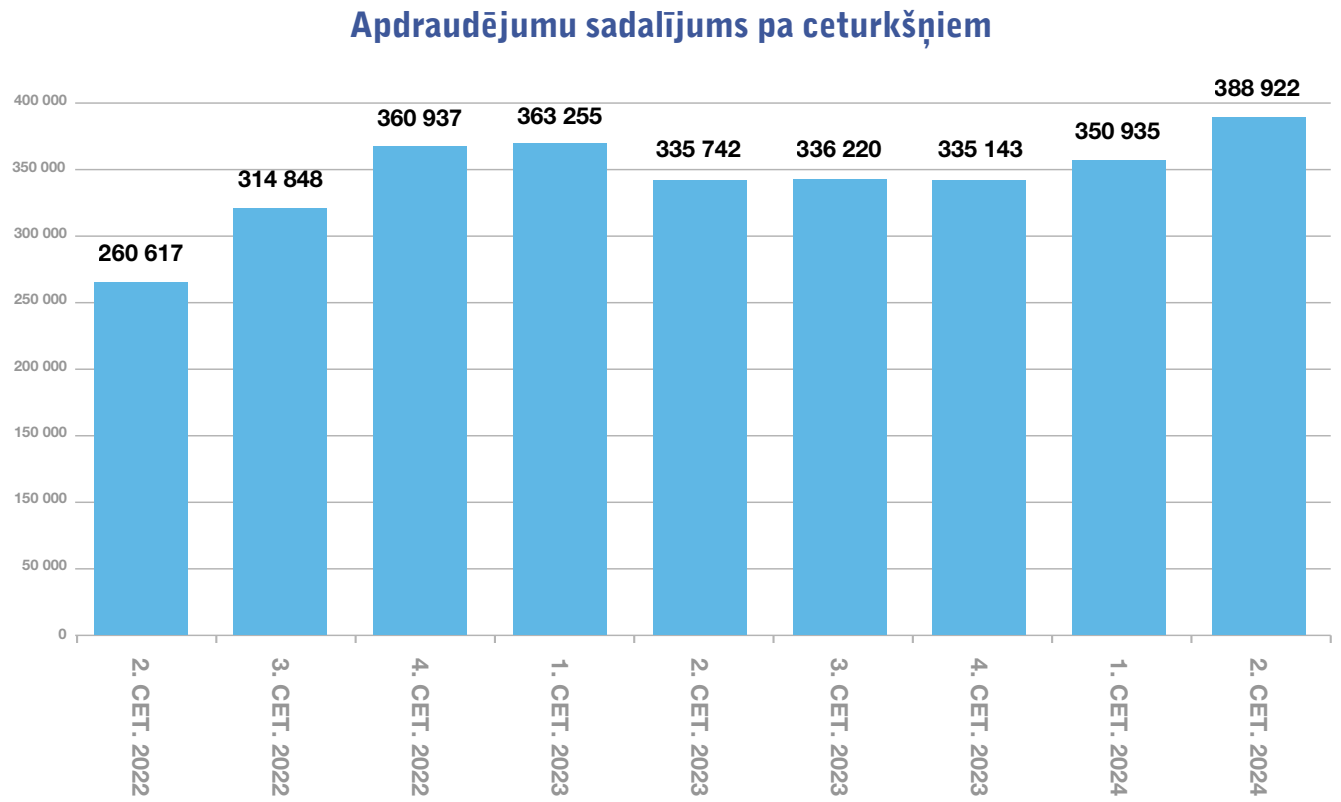
Koordinētas ievainojamību atklāšanas (CVD) platforma: Turpinot CVD platformas darbības attīstīšanu, 2. ceturksnis ir bijis īpaši ražīgs - Drošības pētnieku skaits pieauga par 57%, uz konkrētām iestāžu programmām reģistrēto ievainojamību skaits pieauga pieckārtīgi, reģistrēto ziņojumu skaits par CERT.LV klientūras ievainojamībām pieauga trīskārtīgi.

Apmācības un izglītojošie pasākumi: Pārskata periodā, iesaistoties 52 izglītojošos pasākumos, CERT.LV par IKT drošību izglītoja 10 742 dalībniekus, pilnveidojot gan individuālu lietotāju, gan organizāciju zināšanas un prasmes nodrošināt savu datu un sistēmu drošību.

1. Kibertelpas drošības apdraudējumi: statistika un tendences

Pārskata periodā CERT.LV tika reģistrētas 388 923 apdraudētas unikālas IP adreses, kas ir augstākais rādītājs pēdējo divu gadu laikā. Pret iepriekšējo ceturksni kāpums bija gandrīz 11% un salīdzinājumā ar 2023. gada 2. ceturksni tas bija gandrīz par 16% vairāk.

Neskatoties uz ļoti augstu kiberuzbrukumu intensitāti jau kopš 2022. gada sākuma, kas ir izraisījis kiberapdraudējumu līmeņa celšanos par 40% Latvijas kibertelpā, Latvija ir demonstrējusi augstu kibernoturības līmeni. Līdz šim fiksētie kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību. Tomēr tam nevajadzētu mums ļaut atslābt, kiberdrošības jomā attīstība notiek nepārtraukti, kas liek meklēt un ieviest arvien jaunus noturības celšanas pasākumus.



1. attēls. Apdraudētās unikālās IP adreses pa ceturkšņiem 2022. - 2024. gadā

Kiberapdraudējumu turpmākās attīstības dinamika saglabājas augsta. CERT.LV aktīvi uzrauga situāciju un iespējamos apdraudējumus.

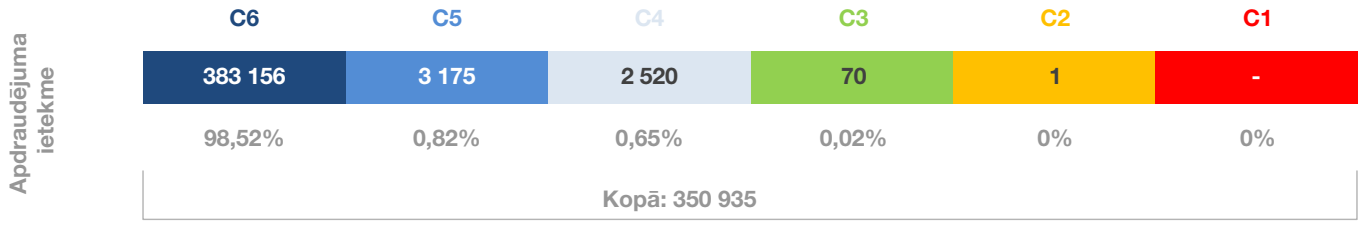
Apdraudēto IP adrešu izvietojums matricā pēc svarīguma un ietekmes

Pilnvērtīgākam kiberdrošības situācijas ikmēneša novērtējumam CERT.LV izmanto Apvienotās Karalistes Nacionālā kiberdrošības centra izstrādāto apdraudējumu matricas metodoloģiju. Apdraudējumi tiek ievietoti matricā, un tajā redzams, cik daudz apdraudējumu atrodas katrā svarīguma kategorijā, sākot no zemākās (C6) līdz pat augstākajai (C1). Matricā ievietotie kiberapdraudējumi tiek grupēti pēc trim būtiskākajiem kritērijiem:

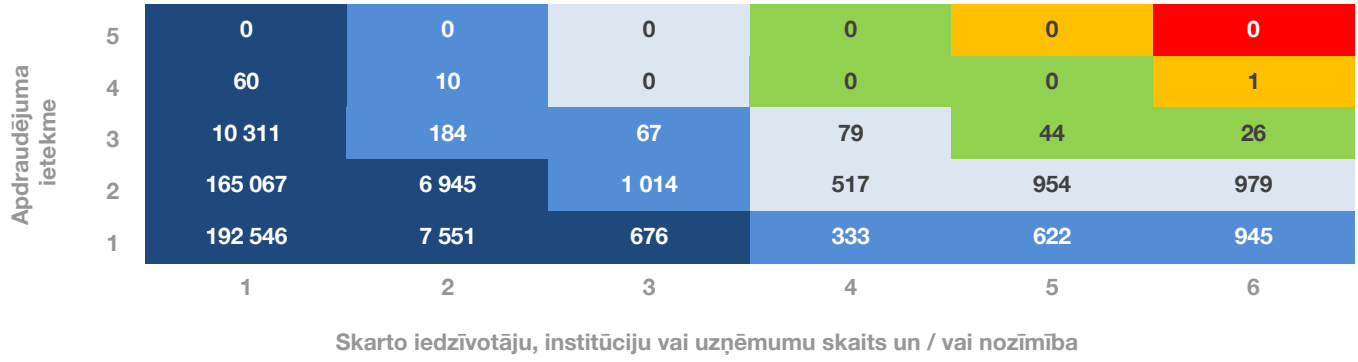
- **cik nozīmīga ir skartā klientūra (iestāde/uzņēmums/gala lietotājs);**
- **cik plašu sabiedrības daļu apdraudējums ietekmē;**
- **cik būtiskas sekas attiecīgais apdraudējums rada.**

Šie trīs kritēriji nosaka to, kāda svarīguma kategorija attiecīgajam apdraudējumam tiek piešķirta (C6-C1). Apvienojot visus faktorus un izmantojot krāsas, apdraudējumi 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.



2. attēls. 2. ceturksnī apdraudēto unikālo IP adrešu sadalījums kategorijās pēc apdraudējuma ietekmes



3. attēls. 2. ceturksnī apdraudēto unikālo IP adrešu izvietojums matricā pēc ietekmes, skaita un/vai nozīmības

C1 kategorijas jeb nacionāla līmeņa apdraudējumi pārskata periodā nav fiksēti.

C2 kategorijā, kas ietver augstas nozīmes apdraudējumus, pārskata periodā tika reģistrēta viena apdraudēta unikāla IP adreses no visiem kategorizētajiem apdraudējumiem. Fiksētais kiberuzbrukums valsts iestādē tika veikts, izmantojot VPN vārtejas programmnodrošinājumā. Kiberuzbrukums neradīja paliekošas sekas, un tā ierobežotais ilgums (apmēram 30 min.) neļāva kiberuzbrucējiem veikt papildu darbības tīkla izpētei un kompromitācijai. Detalizētāk šis notikums tiks aplūkots tālāk 2. nodaļas 2.5. sadaļā.

C3 jeb nozīmīgi apdraudējumi ar indikatīvi plašu ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 0,02% jeb 70 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem, kas bija gandrīz uz pusi mazāk nekā 1. ceturksnī, bet par 75% vairāk nekā pagājušā gadā. Fiksētie kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību. Kiberapdraudējumi reģistrēti vairākās pašvaldību un valsts iestāžu, valsts kapitālsabiedrību, veselības aprūpes un izglītības iestāžu, enerģētikas un elektronisko sakaru komersantu iekārtās un sistēmās. Lielāko daļu apdraudējumu veidoja ļaunatūras, kam seko kompromitētas iekārtas un ielaušanās mēģinājumi.

C4 jeb būtiski apdraudējumi ar vidēju ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 0,65% jeb 2 520 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem. 2. ceturksnī C4 kategorijā apdraudēto IP adrešu skaits bija par 11% vairāk nekā 1. ceturksnī un par 16% lielāks nekā pirms gada. Kiberapdraudējumu TOP 3 pirmajā vietā ierindojas konfigurācijas nepilnības, kam seko ielaušanās mēģinājumi un krāpšanas mēģinājumi. Kiberapdraudējumi reģistrēti gan publiskā, gan privātā sektora dažādu iestāžu, organizāciju un komersantu iekārtās un sistēmās.

C5 jeb mēreni apdraudējumi ar nelielu ietekmi uz komerciālo adrese sektoru, valsts un pašvaldību iestādēm veido 0,8% jeb 3 175 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem. Pret iepriekšējo ceturksni pieaugums bija bikls (+6%), bet salīdzinājumā ar 2023. gada 2. ceturksni bija par 21% vairāk. Kiberapdraudējumi reģistrēti gan publiskā, gan privātā sektora organizāciju un komersantu iekārtās un sistēmās. C5 līmeņa apdraudējumu TOP3 pirmajā vietā ierindojas ļaundabīgs kods, kam seko ielaušanās mēģinājumi un konfigurācijas nepilnības.

Lielākais īpatsvars jeb 98% apdraudējumu ietilpst maznozīmīgu apdraudējumu kopā jeb C6 kategorijā. Šie kiberapdraudējumi ir saistīti ar individuālu lietotāju iekārtām vai plaši izplatītiem ikdienišķiem, automatizētiem kiberuzbrukumu mēģinājumiem uzņēmumiem vai valsts un pašvaldību iestādēm. Šogad 2. ceturksnī pret iepriekšējo ceturksni kāpums bija 11% un par 16% vairāk salīdzinājumā ar to pašu periodu pērn.
C6 līmeņa kiberapdraudējumu TOP3 pirmajā vietā ierindojas konfigurācijas nepilnības, kam seko ļaundabīgs kods un ielaušanās mēģinājumi.

"Šobrīd draudu līmenis nav samazinājies visās jomās, bet tomēr esam iemācījušies daudz labāk ar to tikt galā, liela daļa uzbrukumu tiek atvairīti automatizēti, līdz ar to slodze gan mums, gan citām institūcijām pašlaik ir mazāka, bet turpinām intensīvi strādāt."

Baiba Kaškina, CERT.LV vadītāja

Var secināt, ka pārskata periodā visās kategorijās ievērojams pieaugums bija vērojams šādos kiberapdraudējuma veidos: kompromitētas iekārtas, ļaundabīgs kods un ielaušanās mēģinājumi.

Kibernoturības līmenis ir ļoti atšķirīgs starp dažādām iestādēm un uzņēmumiem, kā arī starp atšķirīgiem sektoriem, tomēr kopumā var novērot pastiprinātu interesi par kibernoturības uzlabošanu, kā arī par savu IKT resursu stiprināšanu. Kopš 2022. gada sākuma publiskā un privātā sektora organizācijas biežāk ziņo par kiberuzbrukumiem un ievainojamībām, kā arī biežāk lūdz CERT.LV atbalstu, kas liecina par pieaugošu uzticības līmeni starp publiskā un privātā sektora organizācijām un kiberdrošības incidentu reaģēšanas vienībām.

Satraucoši ir CERT.LV draudu medību operācijās iegūtie secinājumi, ka gandrīz ceturtdaļā gadījumu publiskā sektora mērķa iestādes ir lielākā vai mazākā mērā cietušas no kiberuzbrukumiem, kas saistīti ar citu valstu sponsorētām kiberoperācijām (tostarp Krievijas).

Pašreizējā ģeopolitiskajā situācijā var pieņemt, ka ielaušanās mēģinājumu skaita pieaugums ir skaidrojams ar politiski motivētiem Krievijas hakeru kiberuzbrukumiem, kas saistīti ar acīmredzamiem centieniem kompromitēt NATO un ES dalībvalstu IKT kritisko infrastruktūru.

Tas vēlreiz apstiprina, ka valstī nepieciešama minimālo kiberdrošības prasību ievērošanas uzraudzība, kā arī viegli pieejami efektīvi kiberdrošības pakalpojumi un IKT drošības telemetrijas apstrāde, kas kvalitatīvi un atbilstoši aktuālajiem izaicinājumiem spētu atbalstīt publiskā sektora tehniskos un cilvēkresursus pret aizvien pieaugošiem kiberapdraudējumiem.

CERT.LV piedāvā Informācijas tehnoloģiju drošības likuma subjektiem plašu kiberdrošības pakalpojumu klāstu. Plašāk: **https://cert.lv/lv/pakalpojumi**

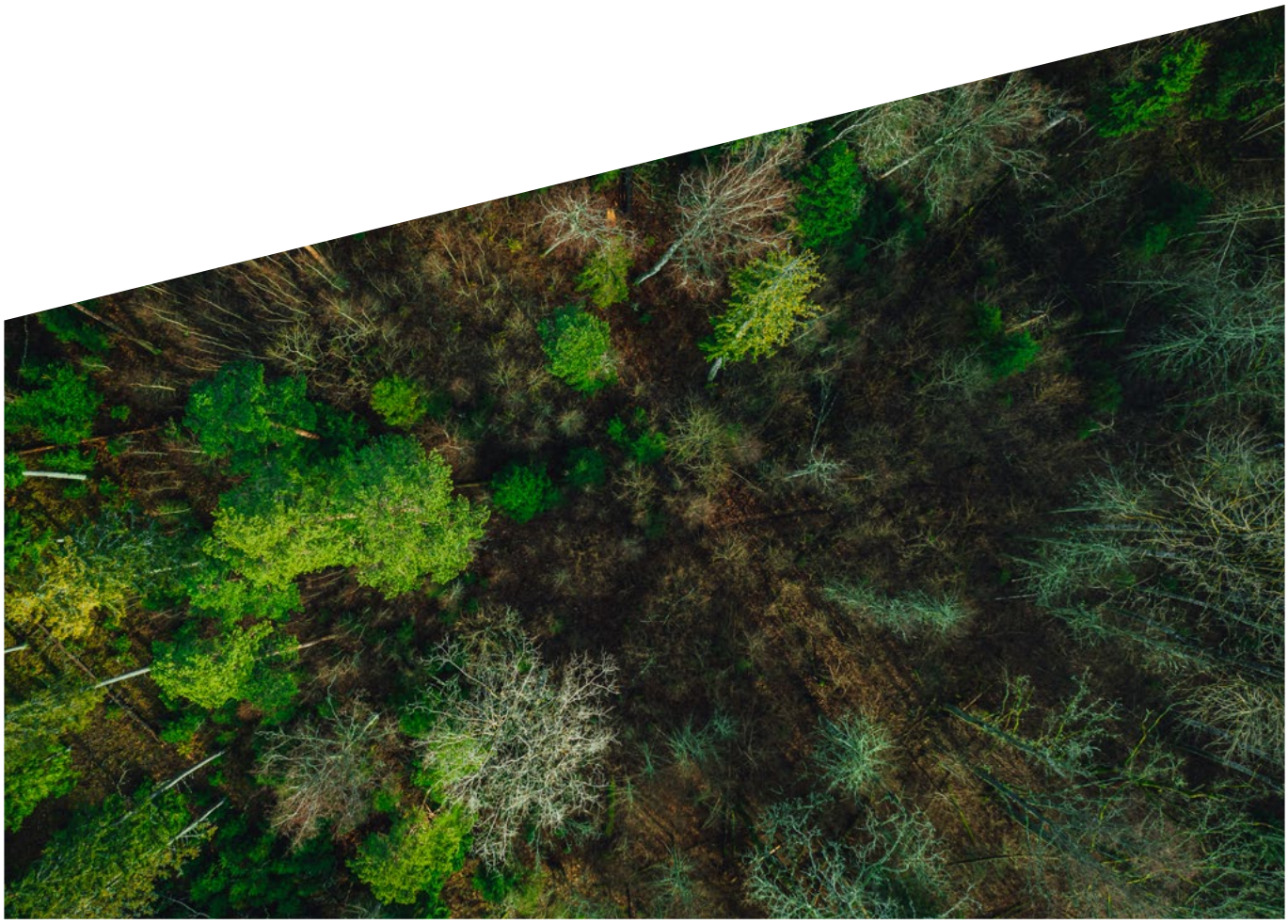
Svarīgi atzīmēt, ka pārskata periodā, 20. jūnijā, Saeimā tika pieņemts Nacionālās kiberdrošības likums (NKDL), kas ir būtisks un liels solis uz priekšu, lai stiprinātu kiberdrošību Latvijā un ieviestu pārskatītās Eiropas Savienības (ES) Tīklu un informācijas sistēmu drošības direktīvas (NIS2) prasības vienādi augsta kiberdrošības līmeņa panākšanai visā ES.

CERT.LV EKSPERTU KOMENTĀRS

Latvijas kiberdrošības situāciju ietekmē vairākas tendences, tostarp arvien biežāk sastopamie izspiedējvīrusu un infozadzējvīrusu uzbrukumi, citu valstu sponsorētu kiberoperāciju ļaunprātīgās aktivitātes un pieaugošo kiberapdraudējumu riski IKT kritiskai infrastruktūrai. Kiberapdraudējumu dinamiskā un mainīgā daba prasa pastāvīgu modrību un pielāgošanos, jo pieaug mākslīgā intelekta integrēšana uzbrukuma un aizsardzības kiberoperācijās. Turklāt lietu interneta potenciālās ievainojamības rada pieaugošus riskus, jo palielinās kiberuzbrukumu virsma.

Lai pretstāvētu jauniem kiberdraudiem, būtiska ir informācijas apmaiņa un sadarbība ar starptautiskajiem partneriem, piemēram NATO, ES, EU CSIRT, CyCLONe, ENISA u.c.

Turklāt ikvienā organizācijā ir jāakcentē stingra paroļu politika, daudzfaktoru autentifikācija un regulāra programmatūru atjaunināšana, lai uzlabotu vispārējo kiberhigiēnu. Šie piesardzības pasākumi, kas varētu šķist vienkārši un viegli pirmajā acu uzmetienā, var ievērojami uzlabot kibernoturību, saskaroties ar iespējamiem kiberapdraudējumiem.



2. TOP kiberincidenti un apdraudējumi: atbalsts un rekomendācijas to novēršanā

Veicinot kiberdrošību Latvijā un stiprinot kibernoturību, 2024. gada 2. ceturksnī tika turpināta CERT.LV aktīva sadarbība ar valsts un pašvaldību institūcijām, bankām, elektronisko sakaru komersantiem un citām organizācijām un kiberdrošības ekosistēmas partneriem dažādas bīstamības incidentu risināšanā.

Kiberdrošības incidents – notikums, kas apdraud apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību.

Ziņošana par incidentiem, sadarbība un informācijas apmaiņa joprojām ir būtiski efektīvas kiberdrošības priekšnoteikumi. CERT.LV turpina regulāri informēt valdības pārstāvjus, valsts institūciju vadītājus un kiberdrošības speciālistus par notikumiem Latvijas kibertelpā. Tāpat CERT.LV turpina nodrošināt ikmēneša notikumu apkopošanu un analīzi, sniedzot lēmumu pieņēmējiem informāciju, kas nepieciešama, lai savlaicīgi prognozētu un novērstu valsts iekšējo un ārējo apdraudējumu, kā arī uzlabotu valsts IKT kritiskās infrastruktūras aizsardzību un noturību.

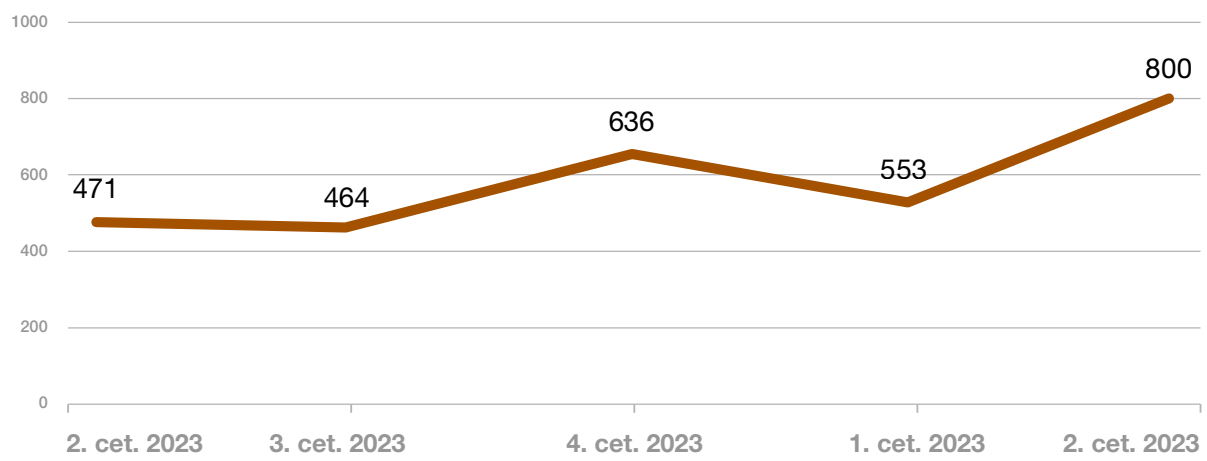
CERT.LV ir valstī lielākais kiberapdraudējumu datu un informācijas apkopotājs, kas automatizēti apstrādā un analizē vairākus miljonus ienākošo signālu mēnesī.

CERT.LV komandas atbalsts incidentu izmeklēšanā		
15-20 manuāli risināti incidenti katru dienu	Vairāk nekā 6,5 miljoni kiberdrošības telemetrijas signālu mēnesī	Atbalsts ikvienam, bet prioritāri: pamatpakalpojumu un digitālo pakalpojumu sniedzējiem, kritiskās infrastruktūras turētājiem un valsts iestādēm

Būtiskākie kiberincidenti un kiberapdraudējumi, kas izgaismo 2. ceturksnī novērotās tendences, aplūkoti turpinājumā – 2.1. līdz 2.6. apakšnodaļās.

2.1. Krāpšana

Krāpniecības apmēri uzņem apgriezienus. 2024. gada 2. ceturksnī CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits apdraudējumu veidā "Krāpšana" ir palielinājies par 45% salīdzinājumā ar iepriekšējo ceturksni un par 70% salīdzinājumā ar pagājušā gada 2. ceturksni.



4. attēls. Apdraudēto unikālo IP adrešu skaits ar apdraudējuma veidu – krāpšana

Arī Valsts policijas publiskotie dati liecina, ka ik mēnesi tiek izkrāpts vismaz viens miljons eiro.

Būtiskākie kiberdrošības riski pārskata periodā īsumā:

- Latvijas kibertelpā izplatītākie krāpniecības veidi pārskata periodā: vikšķerēšana, pikšķerēšana, smikšķerēšana un investīciju krāpšana.
- Krāpnieki izmanto uzticamu organizāciju nosaukumus, lai masveidā sūtītu īsziņas vai e-pasta vēstules ar krāpnieciskām saitēm, iestrādātu QR kodu vai e-pasta vēstulē pievienotu ļaunprātīgu pielikumu maskētu kā rēķinu.
- Krāpnieki seko līdzi aktualitātēm un izmanto tās savā labā, aktivizējoties brīdī, kad, piemēram, iedzīvotājiem sākas gada ienākumu deklarāciju iesniegšana.
- Mānīšanās zvani un darījuma sarakstes kompromitēšanas gadījumi ir kļuvuši par nopietnu problēmu, kas ietekmē daudzus pilsoņus arī Latvijā.
- Neuzmanība un elementāras kiberhigiēnas neievērošana palielina krāpniecības riskus.

Krāpšanas kampaņas visbiežāk tika sūtītas dažādu valsts iestāžu, kurjerpastu un finanšu pakalpojumu sniedzēju vārdā. Neskatoties uz dažādu iestāžu brīdinājumiem par finanšu krāpnieku shēmām, iedzīvotāji aizvien turpina uzķerties uz noziedznieku ēsmu, jo krāpnieku shēmas šķiet ticamas, tostarp tīmekļvietnes, kas izveidotas, lai izvilinātu piekļuves datus, izskatās ļoti līdzīgas to oriģināliem.

Lai izkrāptu finanšu līdzekļus, joprojām ļoti izplatīti ir mērķēti kiberuzbrukumi, izmantojot īsziņas vai e-pasta vēstules ar pievienotu krāpniecisku saiti. Pikšķerēšana un smikšķerēšana tika novērota ‘“Omniva”, DPD, DHL, “Paysera”, “SEB banka”, “Citadele banka”, un it īpaši intensīvi Valsts ieņēmumu dienesta (VID) un AS “Latvijas Pasts” vārdā. Tas ir skaidrojams ar to, ka pavasarī, kad sākas gada ienākumu deklarāciju iesniegšana VID, aktuāli kļūst e-pasti saistībā ar pārmaksātajiem nodokļiem. Tāpat krāpnieki aktīvi izmanto arī mūsdienās aktuālo iepirkšanos internetā, gandrīz katru dienu “Latvijas Pasts” vārdā, izsūtot viltus ziņas iedzīvotājiem par vajadzību precizēt piegādes adresi.

Tāpat parādījās viltus e-pasta vēstules par laimestu “EuroMillions” loterijā un pieprasījumu steidzami dalīties ar savu personīgo informāciju. Bezmaksas laimesti ir vilinoši kā siers peļu slazdā, diemžēl šajā gadījumā steiga un labticība beidzas ar sensitīvas un personīgas informācijas izpaušanu vai naudas zaudēšanu.

Aktuāls krāpnieku fokuss pārskata periodā bija arī viltus ziņu sūtīšana ar darba piedāvājumiem it kā personālatlases kompāniju vārdā (gan vietējo, gan ārvalstu) saziņas vietnē “WhatsApp”. Lai pieteiktos darbam, personai tikai prasīts atklāt detalizēti savus bankas un personu identificējošus datus.

Spūfings jeb mānīšanās zvani ir kļuvuši par nopietnu problēmu, kas ietekmē daudzus cilvēkus arī Latvijā. Šādā krāpniecības shēmā izmanto tehnoloģiju, lai viltotu zvanītāja numuru (identitāti) un ģenerētu zvanus no tīši izvēlētiem vai nejaušiem numuriem, izmantojot Latvijas un dažādu valstu reālu vai izdomātu parastu lietotāju tālruņa numurus. Krāpnieku mērķis ir tieši zvana laikā izvilināt personiskos datus, lai pēc tam tālāk tos izmantotu nelikumīgām darbībām. Vērojama tendence, ka krāpnieki izmanto Latvijas operatoru klientu numurus. Savukārt pats numura īpašnieks nezina, ka viņa tālruņa numuru ir izmantojis kāds krāpnieks.

Novērojama arī tendence, ka tiek zvanīts it kā no VID, Valsts policijas vai kādas iestādes drošības dienesta, lai aicinātu piedalīties, piemēram, krāpšanas gadījuma izmeklēšanā, kas sevī iekļauj lūgumu izņemt skaidru naudu no banku kontiem un novietot kādā konkrētā vietā, nodot kādai nepazīstamai personai vai nosūtīt it kā drošai glabāšanai, izmantojot pakomātu pakalpojumus. Cilvēkiem tiek radīta pārliecība, ka ir jāiesaistās, lai notvertu noziedznieku vai pasargātu savu naudu. Kā liecina Finanšu nozares asociācijas apkopotie dati, joprojām daudz ir to, kuri nespēj atpazīt krāpnieku shēmas un uzķeras.

Aktivizējušies viltvārži, kuri, uzdodoties par mobilo sakaru operatoru drošības speciālistiem, cenšas pārliecināt upuri, ka viņa viedtālrunis ir inficēts ar vīrusu vai pat uzlauzts. Sarunas laikā krāpnieki cenšas noskaidrot, kurās bankās iedzīvotājam ir aktīvi konti, un informē, ka drīzumā gaidāms zvans arī no bankas un policijas. Lai izkrāptu naudu, krāpnieki pārliecina upuri, ka tā telefons ir inficēts ar vīrusu, un liek dalīties ar ekrāna saturu. Ar attālinātās pieejas rīku, piemēram, "AnyDesk", krāpnieki iegūst piekļuvi upura internetbankai, savukārt pēc tam var sekot aicinājums pārskaitīt naudu.

Tāpat daudzi iedzīvotāji saņēma viltus paziņojumus it kā "Facebook" atbalsta komandas vārdā ar draudiem 24 stundu laikā dzēst lietotāja kontu sakarā ar preču zīmju tiesību pārkāpumu. Šādi paziņojumi tika sūtīti "Facebook Messenger" ziņā ar pievienotu saiti uz pikšķerēšanas vietni, kur, upurim ievadot lietotāja piekļuves datus, šī informācija nonāk krāpnieku rīcībā.

Lai gan kopumā kopš gada sākuma investīciju krāpšanas gadījumu skaits samazinās, investīciju krāpnieki aizvien turpina uzdarboties. Piemēram, kāda nozīmīga enerģētikas uzņēmuma vārdā tika izveidots viltus "Facebook" profils, kur iedzīvotājus aicināja ieguldīt uzņēmuma attīstībā. Krāpnieku mērķis bija potenciālā upura konta iztukšošana. Ievērojami pieaudzis pret uzņēmumiem vērsto krāpšanas shēmu apjoms – gan viltus rēķinu izsūtīšana un lūgumi mainīt bankas konta datus ar mērķi panākt maksājuma veikšanu uz krāpnieka kontu, gan pikšķerēšanas e-pasti uzņēmumu grāmatvežiem it kā vadītāju vai citu darbinieku vārdā, lai pēc tam krāpnieki īstenotu savus finansiālos mērķus. Šogad pastiprinājušies algu kontu izkrāpšanas mēģinājumi, maskējoties ar kādas bankas vārdu.

Jūnijā uzliesmoja īpaši ciniska krāpniecības kampaņa, kas mērķēta uz "WhatsApp" lietotājiem. Krāpnieki, ar šķietami no paziņas vai tuvas personas sūtītiem aicinājumiem balsot par bērnu zīmējumiem, mēģina nozagt "WhatsApp" lietotāju kontus. No nozagtā konta tālāk var tikt izplatītas krāpnieciskās ziņas kontaktos esošajām personām ar mērķi gūt materiālu labumu. Vairāki šīs krāpniecības upuri konstatēti arī Latvijā, par līdzīgu kampaņu jau iepriekš ziņojis arī Ukrainas CERT-UA.

Joprojām izaicinājums ir neuzmanība un nepietiekama kiberhigiēna individuālo lietotāju līmenī. Jāsaprot, ka pat viens lietotāja klikšķis var nodarīt milzīgu kaitējumu ne tikai pašas personas datu drošībai, bet arī tā darbvietas iestādei. Elementāras kiberhigiēnas neievērošana ir viens no iemesliem, kāpēc daudzi lietotāji ir pakļauti krāpniecības riskiem kibertelpā.

CERT.LV operatīvi ievieto krāpniecisku aktivitāšu indikatorus DNS ugunsmūrī, lai tā lietotājus pasargātu no krāpniecisku un ļaundabīgu vietņu apmeklēšanas un pārvirzītu uz brīdinājuma vietni. Arī gadījumos, kad ļaunatūra jau ir inficējusi iekārtu, DNS ugunsmūris dod iespēju laikus identificēt šādas iekārtas, lai sistēmu administratori varētu operatīvi likvidēt sekas.

CERT.LV mudina iedzīvotājus pastiprināt modrību, domāt kritiski par katru pieprasījumu dalīties ar personīgo informāciju un savai drošībai izmantot DNS ugunsmūri – aktīvās aizsardzības rīku, ko bez maksas nodrošina CERT.LV un NIC.LV. Lai pasargātu arī citus lietotājus, CERT.LV aicina ikvienu ziņot uz cert@cert.lv par krāpnieku aktivitātēm un ļaundabīgām vietnēm.

CERT.LV EKSPERTU KOMENTĀRS

Kiberapdraudējumu ainava mainās sarežģītu kiberuzbrukumu rezultātā, kuros tiek izmantota gan cilvēku neuzmanība, gan tehnoloģiju ievainojamības, kiberuzbrucējiem gudri pielietojot mākslīgā intelekta rīkus ļaunprātīgiem nolūkiem, mērķtiecīgu pikšķerēšanu, mērķētu ļaunatūras piegādi un vāju autentifikācijas praksi. Krāpnieki nemitīgi attīsta savas prasmes un viņu shēmas kļūst arvien atjautīgākas, tāpēc ir ļoti svarīgi nodrošināt izglītošanu un apmācību attiecībā uz būtiskākajiem kiberdrošības riskiem, kā arī regulāri veikt pikšķerēšanas testus.

Vairāk informācijas par pikšķerēšanas uzbrukumu simulāciju, ko nodrošina CERT.LV – https://www.cert.lv/lv/pakalpojumi#3-pikskeresanas-uzbrukumu-simulacija

Izplatītākās TOP 4 krāpšanas shēmas pārskata periodā

Krāpnieku treknākā ēsma nodokļu atmaksas sezonā – ienākumu deklarācijas: KCERT.LV reģistrēts ievērojams ziņojumu skaits par e-pastiem un īsziņām, kurās krāpnieki uzdodas par VID un aicina veikt noteiktas darbības saistībā ar nodokļu atmaksu. Krāpšanas shēmās tika izmantots arī kvadrātkods (QR kods).

CERT.LV aicināja iedzīvotājus būt vērīgiem un, saņemot viltus paziņojumu ar iestrādātu QR kodu, to noteikti neskenēt, jo visu informāciju, ko VID sūta, iespējams apskatīt Elektroniskās deklarēšanas sistēmā (EDS). E-pastā iedzīvotāji no VID var saņemt tikai paziņojumus par informāciju, kas pieejama EDS, turklāt šajā paziņojumā ir saite uz EDS eds.vid.gov.lv. CERT.LV atgādina, ka neviena valsts institūcija un to pārstāvji e-pasta vēstulēs, īsziņās vai telefonsarunās nemudinās uz tūlītēju rīcību un neaicinās dalīties ar bankas konta pieejas vai maksājumu karšu datiem. Par zvana vai ziņas leģitimitāti jāpārliecinās, apmeklējot iestādes oficiālo tīmekļa vietni un sazinoties, izmantojot tur norādīto telefona numuru.

Krāpnieku īsziņas "Latvijas Pasts" vārdā tiek saņemtas masveidā teju katru dienu: CERT.LV reģistrēti ziņojumi no personām, kas saņēmušas īsziņu no krāpniekiem it kā "Latvijas Pasts" vārdā, turklāt neatkarīgi no tā, vai persona ir vai nav veikusi pirkumu interneta veikalā. Viltus īsziņas tika masveidā sūtītas ar melīgu informāciju par kavētām vai nepareizi norādītām piegādēm. Šāda īsziņa satur bīstamu saiti, kur upuris tiek mudināts sniegt personīgos datus krāpnieciskā vietnē, kas atdarina izmantotā servisa vietnes izskatu. Krāpnieku paziņojumi īsziņu vai e-pastu formātā tiek ģenerēti automātiski, un, jo plašākam cilvēku lokam ziņojumi tiek izsūtīti, jo lielāka iespējamība, ka to saņems arī kāds, kurš patiesi gaida savu sūtījumu. Tomēr nevar izslēgt risku, ka iedzīvotājiem, iepērkoties dažādās ārzemju tiešsaistes platformās, kur, veicot pasūtījumu, jānorāda pasūtītāja dati, var notikt datu noplūde no šīm tīmekļa vietnēm.

Pikšķerēšanas paziņojumi "SEB banka" vārdā: Maijā krāpnieki pārsteidza ar kārtējo jauno stratēģiju krāpšanas kampaņai, kuras ietvaros vairāki iedzīvotāji saņēma e-pasta vēstules ar maldinošu informāciju par to, ka kodu kalkulatoram beidzies reģistrācijas derīguma termiņš. Taču, rūpīgi apskatot vēstuli, skaidri redzams, ka tā nav no bankas, bet gan krāpnieku mēģinājums izvilināt personas datus un izkrāpt naudu. Tāpat otra tendence – e-pasta vēstules ar paziņojumu par bloķētu kontu it kā autentifikācijas kļūdas dēļ. Savukārt jūnijā plosījās pikšķerēšanas viļņi ar krāpnieciska satura e-pasta vēstules paziņojumiem: "Steidzami: mobilā tālruņa numurs nav apstiprināts".

Iedzīvotāji tika aicināti pastiprināt modrību, jo neviena banka īsziņās, e-pasta ziņojumos vai telefonsarunās nemudinās uz tūlītēju rīcību un neaicinās dalīties ar paroli, bankas konta pieejas vai maksājumu karšu datiem vai citu personisku informāciju.

10 IETEIKUMI DROŠĪBAI

1. Pārbaudīt avotus un datu precizitāti, kritiski izvērtējot saņemtās ziņas patiesumu un sūtītāja e-pasta adresi un saturu, rūpīgi pievēršot uzmanību valodas kļūdām un stilam.
2. Regulāri un savlaicīgi atjaunināt viedierīču un iekārtu lietotnes un operētājsistēmu.
3. Neievadīt informāciju uznirstošajos logos un neklikšķināt uz saitēm tajos.
4. Neklikšķināt uz e-pasta vēstulē vai īsziņā norādītās saites, ja neesat pārliecinājies, ka saite ved uz vietni, kas saistīta ar uzticamu vēstules sūtītāju! Ja ir šaubas par kādu informāciju, zvanīt uz attiecīgās organizācijas oficiālo tālruni un pārbaudīt.
5. Papildu aizsardzībai izmantot divfaktoru autentifikāciju: tas pasargās no konta pārņemšanas, pat ja uzbrucējs būs ieguvis jūsu paroli.
6. Nekādā gadījumā nesūtīt citām personām attēlus vai video ar bankas kartēm vai personu apliecinošiem dokumentiem!
7. Nepakļauties krāpnieku prasībām viedierīcēs instalēt attālinātas piekļuves programmatūru.
8. Veikt DMARC un SPF pārbaudes ienākošajiem e-pastiem, lai ierobežotu viltoto vēstuļu saņemšanu. Plašāk: **https://cert.lv/lv/2020/05/e-pastu-drosiba-aizsardziba-pret-izejoso-e-pastu-viltosanu**
9. Ziņot par krāpnieku aktivitātēm un ļaundabīgām vietnēm, pārsūtot kaitīgos e-pastus uz cert@cert.lv, tādējādi pilnveidojot DNS ugunsmūra efektivitāti.
10. Izmantot CERT.LV un NIC.LV nodrošināto bezmaksas aktīvo aizsardzības pakalpojumu – **https://dnsmuris.lv/**, lai pasargātos no krāpniecisku vietņu apmeklēšanas.

2.2. Pakalpojuma pieejamība (DDoS)

Līdzīgi kā 2024. gada pirmajos trijos mēnešos, tā arī 2. ceturksnī tika novēroti viļņveidīgi piekļuves lieguma jeb DDoS kiberuzbrukumi, tostarp Krievijas agresiju atbalstošu haktīvistu grupējumu veikti kiberuzbrukumi, gan enerģētikas un transporta nozarēm, gan virknei valsts iestāžu resursu, taču tie tika veiksmīgi atvairīti, turklāt liela daļa automātiski, un tie nav radījuši ilgstošus traucējumus to pakļauto sistēmu darbībai.

DDoS (Distributed Denial of Service) uzbrukums – organizācijas tīmekļa vietne vai servisi kļūst publiski nepieejami, jo vietnes serveri ir pārpludināti ar milzīga apjoma pieprasījumiem no ārpuses un netiek ar galā pieprasījumiem. DDoS uzbrukumi var izraisīt gan finanšu zaudējumus, gan reputācijas kaitējumu.

Kopumā, salīdzinot ar 2023. gada 2. ceturksni, piekļuves lieguma uzbrukumu skaits ir samazinājies teju uz pusi. Un tā nav nejaušība – Latvija lieliski prot sevi aizstāvēt, padarot sevi par grūtu mērķi kiberuzbrukumiem.

Tomēr izaicinājumi nav sarukuši, jo Baltijas reģionam ir sava specifika paaugstinātu naidīgo valstu kiberuzbrukumu risku dēļ. Krievijas spēka struktūrās integrētu ideoloģiski vai politiski motivēta kiberuzbrucēju pastiprināta interese par Latvijas resursiem saglabāsies. Viņu mērķis ir noslogot interneta infrastruktūru Ukrainas atbalstītājiem NATO un ES dalībvalstīs (arī Latvijā). Attiecīgi sistēmu uzturētājiem jāturpina DDoS aizsardzības mehānismu pilnveidošana un nostiprināšana, un jāseko līdzi kiberdrošības ekspertu ieteikumiem.

Būtiski nepieļaut Latvijas IKT infrastruktūras iesaistīšanu kiberuzbrukumos, jo ar Krieviju saistīti telekomunikāciju uzņēmumi apzināti veido klātesamību Latvijā un citās ES valstīs.

Tendence pirms kiberuzbrukumiem veikt izpēti, meklēt organizācijas resursa vājās vietas un veikt ielaušanās mēģinājumus, nav mazinājusies arī šajā pārskata periodā. Kiberuzbrukums tiek mērķēts tieši caur "vājāko" ķēdes posmu.

Drošības eksperti brīdina, ka nereti naidīgo valstu kibervienības uzbrukumu veikšanai izmanto privātpersonu iekārtas, kā, piemēram, Wi-Fi piekļuves un lietu interneta iekārtas. Kibernoziedznieki pastāvīgi meklē neaizsargātas tīkla ierīces gan manuāli, gan ar automatizētiem līdzekļiem. Pārtvertas tīkla ierīces var izmantot, lai, piemēram, veiktu DDoS uzbrukumus.

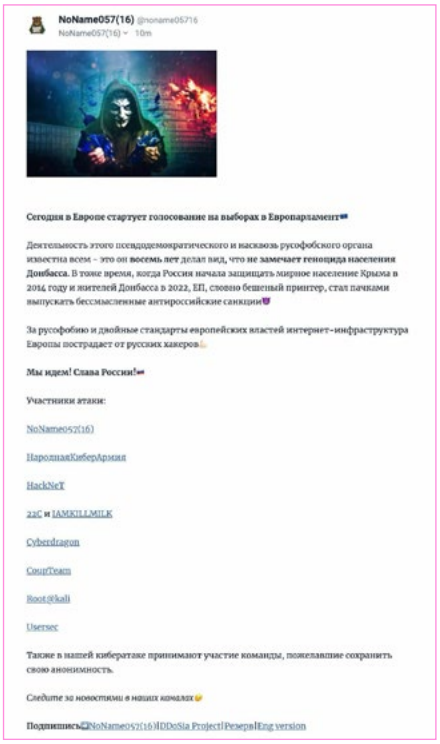
Izplatītākie DDoS uzbrukumi bieži vien tiek veikti, izmantojot attālināti kontrolētas ierīces, kuras kiberuzbrucējs ir pārtvēris. Turklāt kiberuzbrucējs var arī izmantot nolaupītas tīkla ierīces, lai slēptu savas pēdas vai veiktu uzbrukumus no IP adresēm mērķa valstī. Pēdējais veids ir īpaši efektīvs, jo ļaunprātīgu datu plūsmu, kas nāk no vietēja interneta pakalpojumu sniedzēja tīkla, nav tik viegli atklāt kā ļaunprātīgu datplūsmu, kas nāk no ārvalstu tīkla.

Krievijas atbalstītāju "Telegram" kontos izplatītie aicinājumi traucēt vēlēšanu procesu nav nesuši panākumus

Īsi pirms Eiropas Parlamenta (EP) vēlēšanu sākuma Krievijas atbalstītāju "Telegram" kontos tika izplatīti aicinājumi traucēt vēlēšanu procesu gan Latvijā, gan citās ES dalībvalstīs, taču šie mudinājumi nav nesuši panākumus.

Latvijas kibertelpā EP vēlēšanu laiks aizritēja bez starpgadījumiem. Latvijā nav novērots neviens incidents, kas būtu tieši saistāms ar vēlēšanu sistēmām vai vēlēšanu drošību.

Vēlēšanu laikā pastiprināta kibertelpas uzraudzība notika visu nedēļu, tostarp uzmanība tika pievērsta ne tikai vēlēšanu sistēmas, bet arī vēlēšanu procesā iesaistīto organizāciju drošībai.



Krievijas agresīvā režīma atbalstītāju "Telegram" kontos izplatītie aicinājumi traucēt vēlēšanu procesu

Traucēta "Smart-ID" darbība

Pirms Līgo svētku brīvdienām kiberuzbrukuma rezultātā radās traucējumi elektroniskās identifikācijas un parakstīšanās rīka "Smart-ID" darbībā - bija apgrūtināta "Smart-ID" transakciju izsaukšana lietotāju pusē. Pret "Smart-ID" veiktais kiberuzbrukums īslaicīgi ietekmēja tikai pakalpojuma pieejamību, bet tas nekādi neapdraudēja lietotāju datu drošību. Šis kiberuzbrukums vēlreiz demonstrē, cik būtiska ir virzība uz pieejamo autentifikācijas līdzekļu diversifikāciju jeb, ka sabiedrībā plaši izmantoti pakalpojumi, atbalsta iespēju autentificēties ar dažādiem risinājumiem. Arī šajā gadījumā banku klientiem bija iespēja autentifikācijai izmantot citus pieejamos risinājumus, piemēram, "eParaksts mobile" vai kodu kalkulatorus.

"ABC CEĻVEDIS" KIBERDROŠĪBAS VEICINĀŠANAI IESTĀŽU VADĪTĀJIEM

Pārskata periodā Aizsardzības ministrija sadarbībā ar CERT.LV ir apkopojusi iestāžu vadītājiem padomus kiberdrošības veicināšanai - neatkarīgi no iestādes vai organizācijas lieluma un darbības profila vai jomas. Izveidotie padomi radīti ar mērķi, lai mazinātu potenciālos riskus un apzinātu potenciālos draudus, ar ko iestādes un uzņēmumi varētu saskarties kibertelpā. "ABC ceļvedī" ietverti arī ieteikumi, kas noderēs, lai plānotu pakalpojumu un darbības nepārtrauktībai kritisko datu pieejamību gadījumos, kad pamata infrastruktūra varētu nebūt pieejama.

Plašāk: **https://cert.lv/lv/2024/04/padomi-kiberdrosibas-veicinasanai-iestazu-vaditajiem**

CERT.LV aicina nekavējoties sazināties ar CERT.LV komandu, ja ir nepieciešams atbalsts DDoS kiberincidenta izmeklēšanā, seku novēršanā un prevencijas plānošanā, zvanot uz tālruni 670 858 88 vai rakstot uz **cert@cert.lv** .

IETEIKUMI DROŠĪBAI

1. Apzināt IKT kritiskos resursus, kuri varētu būt pakļauti DDoS uzbrukumam.
2. Pieslēgt monitoringu, lai pamanītu, ka kritiskais resurss nav sasniedzams no interneta.
3. Izveidot papildu interneta pieslēgumu, lai spētu piekļūt tīkla iekārtu vadībai laikā, kad interneta kanāls un iekārtas ir pārslogotas (out-of-band, atsevišķs VPN/jump host cita interneta pakalpojumu sniedzēja tīklā).
4. Pārliecināties, ka ir zināmas un testētas metodes, kā noskaidrot tehniskas detaļas par uzbrukumu: mērķis, uzbrukuma veids (piemēram, netflow/ugunsmūra žurnālfaili, prasīt interneta pakalpojumu sniedzējam).
5. Ir izstrādāts un testēts rīcības plāns, kā rīkoties uzbrukuma laikā:
   - 5.1. Pieslēgt DDoS aizsardzību, ko nodrošina interneta pakalpojumu sniedzējs (ieslēgts pastāvīgi vai pēc pieprasījuma). Latvijā DDoS aizsardzības pakalpojumus piedāvā SIA "TET", Aizsardzības ministrija sadarbībā ar VAS LVRTC un citi pakalpojumu sniedzēji;
   - 5.2. Pēc pieprasījuma interneta pakalpojumu sniedzējs var izfiltrēt/ierobežot lieko datu plūsmu automātiski (BGP RTBH – Border Gateway Protocol Remotely Triggered Black Hole) vai manuāli;
   - 5.3. Migrēt atsevišķas svarīgākās sistēmas aiz DDoS aizsardzības uz mākoņpakalpojumu satura piegādes tīkliem (CDN – Content Delivery Network). Kā piemēram, "Cloudflare", "Microsoft Azure", "Google", "AWS";
   - 5.4. Filtrēt piekļuvi resursam pēc ģeolokācijas, atstājot piekļuvi svarīgākajiem klientiem vai tikai Latvijas IP adrešu diapazoniem.

Vēlamie ieteikumi: Ir izveidoti tieši savienojumi ar vienu vai vairākiem lokāliem interneta apmaiņas punktiem, sadarbības partneriem; ir pieejams brīvs, ar datu apjoma rezervi interneta pieslēguma kanāls un tīkla iekārtas, kas spēj turēt slodzi; ir decentralizēta svarīgāko resursu izvietošana (piemēram, CDN).

2.3. Ievainojamības un konfigurācijas nepilnības

CERT.LV regulāri veic visaptverošu monitoringu, kas ir sasaistāms ar eksponētiem servisiem/iekārtām.

Ievainojamība – informācijas un komunikācijas tehnoloģiju vai to pakalpojumu vājums, uzņēmība pret tehniskām problēmām vai nepilnība, kas var tikt izmantota kiberapdraudējumam.

2. ceturksnī CERT.LV proaktīvi izplatīja brīdinājumus par 16 jaunatklātām kritiskām ievainojamībām (CVE), tostarp individuāli informēja ievainojamo sistēmu turētājus, kā arī atbalstīja incidentu analīzē un novēršanā, sniedzot koordinētus norādījumus un ieteikumus kiberdrošības pārvaldības stiprināšanai.
Joprojām lielākā daļa kiberuzbrukumu tiek veikti, izmantojot publiski zināmas ievainojamības, nevis jaunatklātas ievainojamības, tāpēc savlaicīga konfigurācijas nepilnību apzināšana un ievainojamību lāpīšana var būtiski uzlabot kiberdrošības situāciju.

Jaunatklāto kritisko ievainojamību tops 2024. gada 2. ceturksnī

CVE	Ietekmētie produkti	Apraksts
CVE-2024-24919	*Check Point Security*	3. jūnijā tika izsūtīti brīdinājumi par augsta riska ievainojamību (CVSS* vērtējums: 8.6), kas tiek izmantota kiberuzbrukumos, lai iegūtu attālinātu piekļuvi ugunsmūriem un mēģinātu ielauzties uzņēmumu tīklos. Šīs ievainojamības izmantošana tika konstatēta arī Latvijā. Plašāk: **https://cert.lv/lv/2024/06/augsta-riska-ievainojamiba-check-point-security-varteju-produktos**
CVE-2024-29849 **CVE-2024-29850** **CVE-2024-29851**	*Veeam Backup Enterprise Manager*	23. maijā tika izsūtīts brīdinājums par 3 ievainojamībām: • CVE-2024-29849 (CVSS vērtējums: 9,8) ļauj neautentificētiem kiberuzbrucējiem apiet autentifikāciju un iegūt piekļuvi tīmekļa saskarnei kā jebkuram lietotājam. • CVE-2024-29850 (CVSS vērtējums: 8,8) sniedz kiberuzbrucējam iespēju pārņemt kontu, izmantojot NTLM datu pārraides funkciju. • CVE-2024-29851 (CVSS vērtējums: 7,2) sniedz iespēju lietotājam ar paaugstinātām tiesībām nozagt Veeam Backup Enterprise Manager pakalpojuma konta NTLM šifrēšanas kodu, ja šis pakalpojuma konts ir kas cits, nevis noklusējuma vietējās sistēmas konts. Plašāk: **https://cert.lv/lv/2024/05/atklatas-kritiskas-ievainojamibas-veeam-backup-enterprise-manager-programmatura**
CVE-2024-340	*Palo Alto Networks*	12 aprīlī tika izplatīts brīdinājums par ievainojamību (CVSS vērtējums: 10), kas saistīta ar komandu ievadīšanu un var tikt izmantota Palo Alto Networks piedāvātajās VPN-GlobalProtect vārtejās. Ietekmē PAN-OS 10.2, PAN-OS 11.0 un PAN-OS 11.1 ugunsmūra versijas, kurām konfigurācijā iespējota gan VPN - GlobalProtect vārteja, gan ierīces telemetrija. Plašāk: **https://cert.lv/lv/2024/04/kritiska-ievainojamiba-palo-alto-networks-pan-os-programmatura**
CVE-2023-45590 **CVE-2023-45588** **CVE-2024-31492** **CVE-2024-23671** **CVE-2024-21755** **CVE-2024-21756** **CVE-2023-41677**	*Fortinet*	10. aprīlī tika izplatīts brīdinājums par 7 kritiskām un ļoti nopietnām ievainojamībām Fortinet ražotajās iekārtās. Nopietnākās ievainojamības ļauj veikt attālināto koda izpildi (RCE), nesankcionēti dzēst datnes, patvaļīgi izpildīt OS komandas. Ietekmētās iekārtas ietver FortiClient (Linux un macOS), FortiSandbox, FortiOS un FortiProxy. Plašāk: **https://cert.lv/lv/2024/04/vairakas-kritiskas-ievainojamibas-fortinet-produktos**
CVE-2023-6317 **CVE-2023-6318** **CVE-2023-6319** **CVE-2023-6320**	*"LG" TV*	10. aprīlī tika izplatīts brīdinājums par atklātām 4 ievainojamībām, kas ietekmē vairākas WebOS operētājsistēmas versijas, un kas tiek izmantotas viedajos LG televizoros. Šīs ievainojamības uzbrucējam var sniegt nesankcionētu piekļuvi un kontroli pār skartajām TV iekārtām, tostarp - autorizācijas apiešanu, privilēģiju palielināšanu un komandu ievadīšanu. No visā pasaulē internetā eksponētām un riskam pakļautām iekārtām vairāk nekā 3000 iekārtu atrodas Latvijā (Shodan dati). Plašāk: **https://cert.lv/lv/2024/04/interneta-eksponeti-3000-potenciali-ievainojami-lg-televizori-latvija**

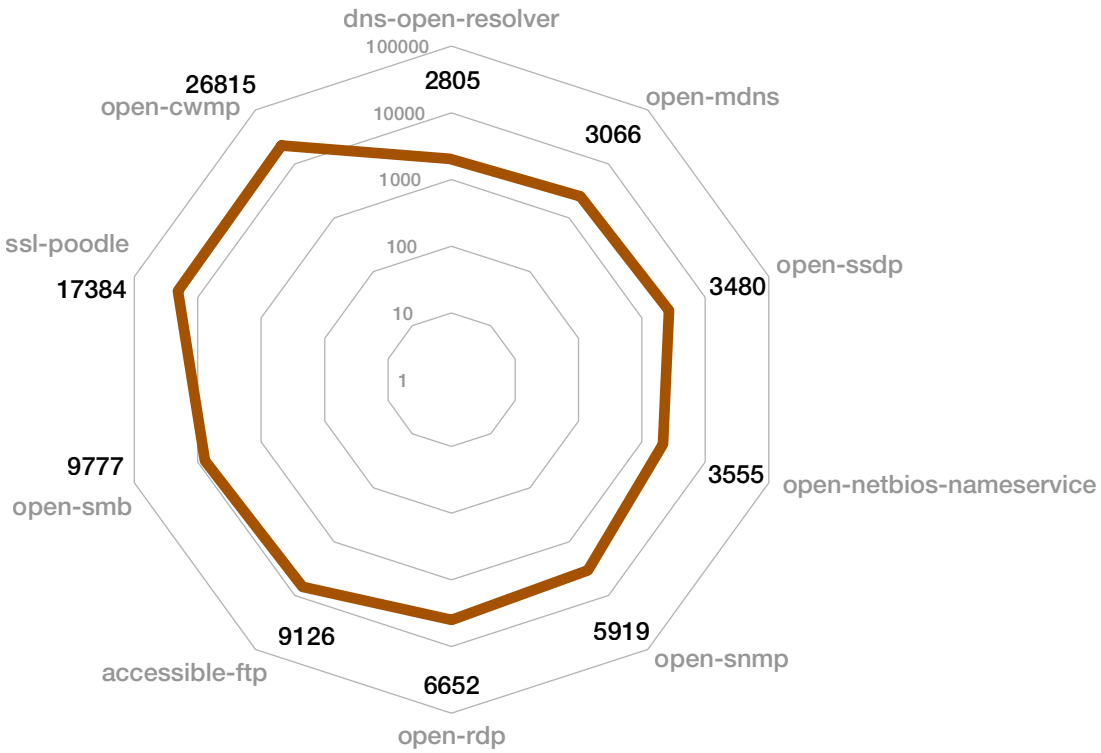
*CVSS: nozares standarta datorsistēmu drošības ievainojamību nopietnības novērtēšanas metodoloģija

CERT.LV EKSPERTU KOMENTĀRS

Ievainojamības un ietekmējamas IT sistēmas ir pieaugošs risks, ko ietekmē jaunatklātās kritiskās ievainojamības, nepareiza IT sistēmu konfigurācija, kā arī novecojuši IT risinājumi. Spējīgākie kiberuzbrucēji kļūst arvien ātrāki, pielietojot jaunatklātās ievainojamības plašā mērogā jau 1-2 dienu laikā kopš to izziņošanas. Pret organizācijām ar augstu drošības līmeni novēroti piegādes ķēžu uzbrukumi – piekļuvi mērķim iegūst, veicot uzbrukumus programmatūras izstrādātājiem u.c. ārpakalpojumu sniedzējiem.

Top 10 konfigurācijas nepilnības 2024. gada 2. ceturksnī

Pārskata periodā turpināja pieaugt konfigurācijas nepilnību skaits, uzrādot augšupejošu tendenci un sasniedzot augstāko rādītāju pēdējo 22 mēnešu laikā.



5. attēls. Top 10 Konfigurācijas nepilnības 2024. gada 2. ceturksnī

Konfigurācijas nepilnības aizvien veido lielāko daļu no visiem CERT.LV reģistrētajiem apdraudējuma veidiem Latvijas kibertelpā.

2024. gada 2. ceturksnī būtiskas izmaiņas Konfigurācijas nepilnību TOP 10 saraksta augšgalā nav notikušas. Topa līderis nemainīgi ir Open-cwmp – pārvaldības protokols, kas tiek izmantots, lai nodrošinātu individuālu iekārtu, piemēram, maršrutētāju vai VoIP telefonu pieslēgšanos pie telekomunikāciju pakalpojumu sniedzēja nodrošinātā tīkla. Lai šim pārvaldības rīkam novērstu neautorizētas piekļuves riskus, tiek rekomendēts ierobežot piekļuves tiesības, piemēram, izmantojot VPN.

2. vietā ierindojas SSL-poodle, kas pēdējo gadu laikā nav bijis augstāk par 4. vietu. SSL-poodle saistīta ar iespēju "atvērt/uzlauzt" SSL 3.0 šifrētu tīkla plūsmu, tādējādi tiekot vaļā no šifrēšanas un iegūstot iespēju lasīt tīkla plūsmu. Ja uzbrucējs pārtver ierīces datu paketes, teorētiski tās var tikt atšifrētas.

3. vietu ieņem Open-smb, kas līdz šim ilgstoši turējās topa otrajā vietā. Ievainojamība norāda, ka konkrētajām iekārtām uz publisko internetu ir atvērts ports, kuru izmanto SMB protokols, kas paredzēts, lai piekļūtu datnēm un iekārtām iekšējā tīklā. Kompromitējot SMB protokolu, uzbrucēji iegūtu iespēju piekļūt iekšējā tīkla iekārtām un inficēt tās, piemēram, ar izspiedējvīrusu.

CERT.LV EKSPERTU KOMENTĀRS

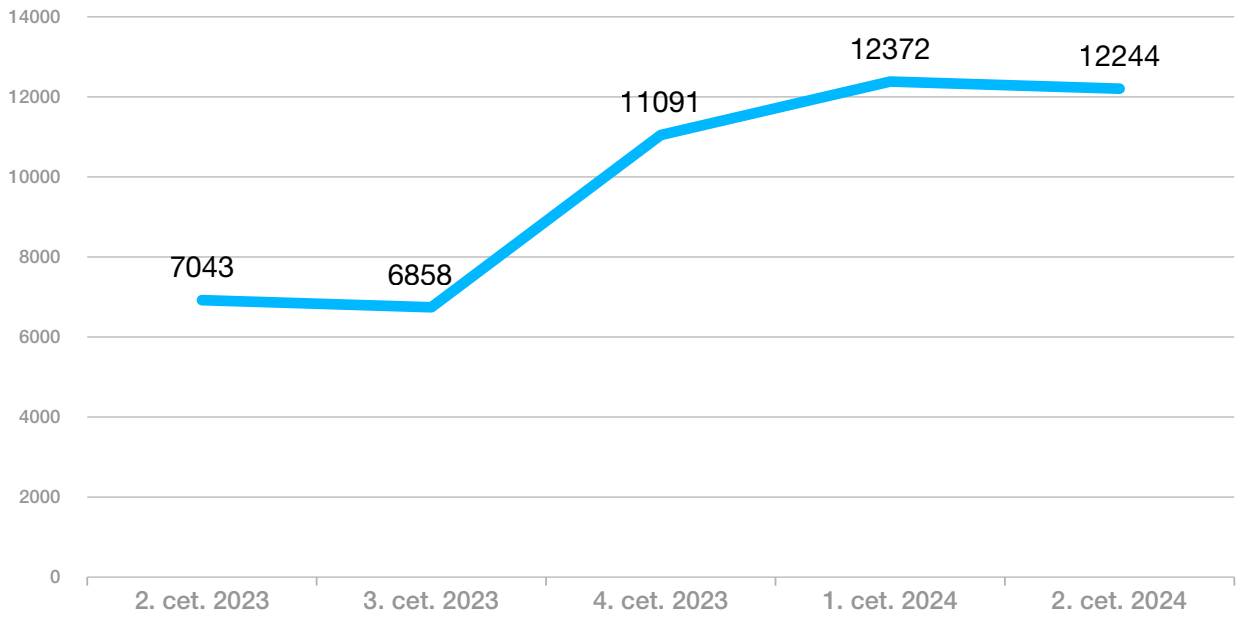
Dinamiskā kiberdrošības ainava prasa patstāvīgu modrību, savlaicīgus programmatūras atjauninājumus, kā arī ievainojamību atklāšanas rīku uzlabošanu, jo kibernoziedznieki nemitīgi pielāgo un uzlabo savu taktiku. CERT.LV aicina sekot līdzi izstrādātāju norādījumiem un nevilcinoties atjaunināt programmatūras uz jaunāko pieejamo versiju. Ar visiem aktuālajiem brīdinājumiem var iepazīties tīmekļvietnes cert.lv sadaļā "Brīdinājumi": **https://cert.lv/lv/incidenti/bridinajumi**

IETEIKUMI DROŠĪBAI

1. **Servisu eksponēšana:** Pārskatīt un apzināt servisus, kas tiek nodrošināti. Neeksponēt servisus publiski, ja tas nav nepieciešams. Ja tas tomēr ir nepieciešams, veikt ierobežojošus pasākumus – piekļuve no konkrēta IP apgabala, VPN u.c.
2. **Regulāra IS atjaunināšana:** Regulāri un savlaicīgi atjaunināt programmatūru/ operētājsistēmas un citas trešo pušu komponentes, lai novērstu ievainojamības savlaicīgi.
3. **Tiesību/autorizāciju politika:** Izveidot stingras ierobežojošas politikas piekļuvju administrēšanas caurskatāmībai. Tiesības piešķirt pēc principa least privilege, nodrošinot lietotāju piekļuvi sistēmām un resursiem atbilstoši veicamajam darbam. Veikt regulāru auditu.
4. **Iebrukumu atklāšana/novēršana:** Savlaicīga iebrukumu apzināšana nereti palīdz novērst uzbrukumu no tālākas eskalācijas. Nodrošināties ar agrīnās brīdināšanas sistēmu un/vai novēršanas sistēmām, lai identificētu un bloķētu nevēlamas aktivitātes.
5. **Drošības auditi:** Regulāri veikt vietnes auditus, kas iekļauj aktīvus un/vai pasīvus drošības skenēšanas pasākumus un aplikācijas koda auditu. Ja tas nav iespējams, piesaistīt ārpakalpojumus. Koordinētai ievainojamību atklāšanai ieteicams izmantot platformu cvd.cert.lv.
6. **Darbinieku apmācības:** Nodrošināt regulāras darbinieku apmācības kiberdrošības jautājumos, lai mazinātu sociālās inženierijas riskus, kas bieži vien ir uzbrukumu sākotnējā fāze.

2.4. Ļaundabīgs kods

Attiecībā pret iepriekšējo ceturksni 2024. gada 2. ceturksnī CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ar ļaundabīgu kodu ir nedaudz samazinājies, taču salīdzinājumā ar pagājuša gada 2. ceturksni kāpums ir par 74%.



6. attēls. Apdraudēto unikālo IP adrešu skaits ar apdraudējuma veidu – ļaundabīgs kods

Visbiežāk pielietotās metodes sistēmu uzlaušanai un inficēšanai:

- Pikšķerēšana;
- Publiski zināmu ievainojamību ļaunprātīga izmantošana;
- Nekorektas konfigurācijas rezultātā tīmeklī eksponēto servisu ļaunprātīga izmantošana – noklusējuma autentifikācijas piekļuves dati, paroļu uzlaušana ar pilno pārlasi (*brute-force*), versiju ievainojamības;
- Inficēti datu nesēji – USB zibatmiņas;
- Pirātiskas programmatūras uzstādīšana;
- Nopludinātas un viegli uzminamas lietotāju paroles;
- Automatizētie uzbrukumi.

Galvenie ļaunatūras tipi pārskata periodā:

- Lietotāju datu zadzēji;
- *Bot-net* jeb botu tīkli;
- Izspiedējvīrusi;
- Attālinātās kontroles ļaunatūras, mērķētas uz datu izgūšanu vai tālāko infrastruktūras kompromitēšanu.

Apdraudēto unikālo IP adrešu skaits Latvijas kibertelpā joprojām saglabājas augsts.

Ļaunatūras tiek izplatītas galvenokārt diviem mērķiem – lai izvilinātu datus vai gūtu peļņu. Atverot ļaundabīgo pielikumu, iekārta tiek inficēta ar ļaunatūru, kas ievāc lietotājvārdus, paroles, kriptovalūtu maciņu un to piekļuves informāciju u.tml., lai nosūtītu to uz uzbrucēja kontrolētu infrastruktūru.

Visbiežāk lietotāju datu zadzēju ļaunatūras tiek mērķētas uz nedroši, lokāli glabāto autentifikācijas datu un paroļu zagšanu, proti, paroļu iegūšanu no tīmekļa pārlūka vai nešifrētiem failiem. Šāda veida ļaunatūra tiek izplatīta kā ļaundabīgs tīmekļa pārlūka spraudnis vai kā izpildfails, pievienots pie pikšķerēšanas e-pasta vēstules.

Ļaunatūras tiek radītas un izmantotas neatļautiem un ļaunprātīgiem mērķiem. Tie var būt gan datorvīrusi, kas domāti datora nelikumīgai attālai administrēšanai, gan klaviatūras nolasītājprogrammas paroļu zagšanai, pikšķerēšanas programmas, spiegu programmas u.c.

Ievērojami pieaudzis pret uzņēmumiem vērsto krāpšanas shēmu apjoms – gan viltus rēķinu izsūtīšana un "lūgumi" mainīt bankas konta datus ar mērķi panākt maksājuma veikšanu uz kiberuzbrucēja kontu, gan pikšķerēšanas e-pasta vēstules, lai pēc tam īstenotu savus finansiālos mērķus.

Kompromitēti e-pasti vai lietotņu konti tiek aktīvi izmantoti, lai tālāk izplatītu ļaunatūras. Maijā un jūnijā tika konstatēti gadījumi, kad uzņēmuma vārdā no kompromitētiem e-pastiem tika izplatīti e-pasti ar kaitīgu pielikumu, kurā iekļautā *AgentTesla* ļaunatūra tika maskēta kā rēķins. Piemēram, *AgentTesla* kāda uzņēmuma, kas nodarbojas ar tirdzniecību, datorā izraisīja nopietnus kiberapdraudējumus tā tīmekļvietnēm. *AgentTesla* ļaunatūras mērķis ir informācijas zagšana, piemēram, nozagt paroles, kas saglabātas datora interneta pārlūkos, un pārsūtīt tās tālāk. Pēc uzbrucēju izvēles šī ļaunatūra var veikt arī cita veida programmatūras izpildi inficētajā datorā, bet primārais mērķis ir informācijas zagšana.

Latvijā joprojām vērojama arī aktīva *RaspberryRobin* ļaunatūras izplatība starp datoriem, izmantojot inficētus ārējos datu nesējus (t.sk. USB zibatmiņas). Inficētajos datoros *RaspberryRobin* var izpildīt kiberuzbrucēja izvēlētu kodu. Ja tiek iegūta sākotnējā piekļuve, vēlāk šo ļaunatūru var izmantot, lai veiktu tālākus kiberuzbrukumus. Tās klātbūtne tika identificēta, īstenojot pārbaudes kādas pašvaldības IT infrastruktūrā.

Pārskata periodā tika konstatēts, ka vairākas reģionālo mediju tīmekļa vietnes ir kompromitētas ar ļaunatūru *AdWare.JS.Agent.hk* - tā, pēc izpildes, apmeklētāju tīmekļa pārlūkos lejupielādē neautorizētu reklāmas saturu.

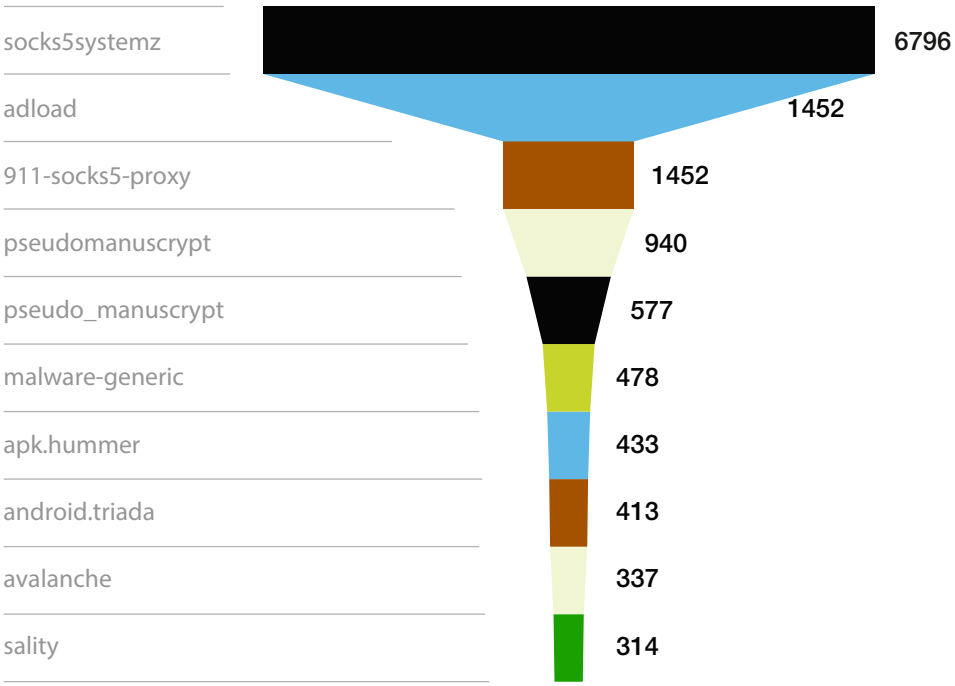
CERT.LV sazinājās ar šo tīmekļvietņu uzturētāju pārstāvjiem, sniedzot ieteikumus drošības incidenta novēršanā. Zināms, ka ļaunatūras dzēšana izdevusies veiksmīgi un visas vietnes ir atjaunotas.

Pārskata periodā aktivizējās krāpnieki, kas it kā LMT vārdā sūtīja īsziņas ar ļaunprātīgām saitēm, kuras, iespējams, saturēja ļaunatūru vai bija paredzētas upura personīgo datu izkrāpšanai. CERT.LV tika reģistrēti vairāku iedzīvotāju iesniegumi, kuri bija saņēmuši šādu viltus ziņu ar tekstu par abonementa apturēšanu un aicinājumu izmantot pievienoto tiešsaistes adresi abonementa atjaunošanai.

Visos gadījumos CERT.LV informēja iestāžu un uzņēmumu atbildīgās personas, un sniedza konsultācijas tālākai rīcībai.

Ļaundabīgu kodu jeb ļaunatūru TOP 10

2024. gada 2. ceturksnī ļaunatūru TOP 10 saraksta 1. vietā ierindojas ļaunatūra *Socks5systemz*, kas inficē iekārtas un pārvērš tās par pāradresācijas proxy jeb starpniekserveriem, savukārt ļaundari tos varētu izmantot, lai padarītu grūtāku viņu nelegālo un kaitīgo darbu izsekošanu. Tādējādi ar *Socks5systemz* inficēta ierīce tiek neautorizēti pārņemta no trešo personu puses un ar lielu varbūtību tiek iesaistīta nelegālo darbību atbalstīšanā.



7. attēls. Apdraudēto unikālo IP adrešu skaits 2. ceturksnī – ļaunatūru TOP 10

2. vietā ierindojusies ļaunatūra *Adload*, kas zog upuru pārlūkmeklētāju datus un ievieto viltus/krāpnieciskas reklāmas upura interneta pārlūkā. Ja ierīcei ir konstatēta Adload ļaunatūra, nepieciešams veikt pilnu datora pārbaudi ar atjauninātu antivīrusu programmu.

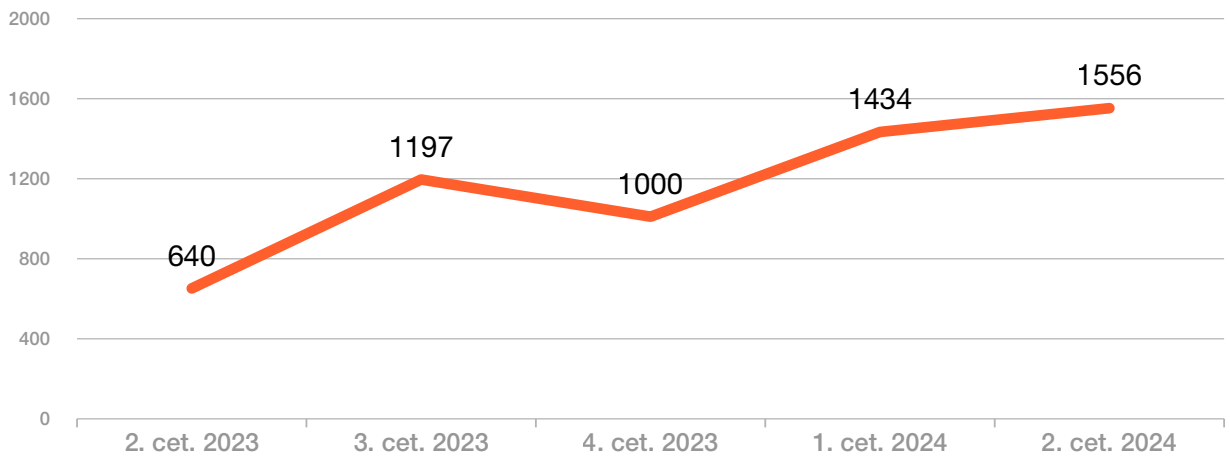
TOP 3 noslēdz topa jaunpienācēja - ļaunatūra *911-socks5-proxy*, kas uz iekārtas lejupielādē kādu no sekojošiem bezmaksas VPN rīkiem: *MaskVPN*, *DewVPN*, *PaladinVPN*, *ProxyGate*, *ShieldVPN* vai *ShineVPN* un papildus nokonfigurējot iekārtu par starpniekserveri. Tādējādi inficētās iekārtas, lietotājam nenojaušot, tiek izmantotas

ļaunprātīgu darbību veikšanai. Nereti šī ļaunatūra nonāk upuru iekārtās no aizdomīgiem resursiem lejupielādējot, piemēram, filmas, mūziku vai datorspēles.

CERT.LV aicina ziņot uz e-pastu cert@cert.lv par ļaunprātīgām saitēm un tīmekļvietnēm. CERT.LV mudina iedzīvotājus un organizācijas izmantot aktīvās aizsardzības pakalpojumu, DNS ugunsmūri, ko bez maksas nodrošina CERT.LV un NIC.LV. Ļaunprātīgu aktivitāšu indikatori tiek operatīvi ievietoti DNS ugunsmūrī, tādejādi pasargājot tā lietotājus no identificētajiem apdraudējumiem.

2.5. Ielaušanās mēģinājumi

CERT.LV reģistrētie dati rāda, ka 2024. gada 2. ceturksnī kiberuzbrucēju ielaušanās mēģinājumi apdraudēja vairāk nekā 1 500 unikālas IP adreses, kas ir augstākais rādītājs pēdējo divu gadu laikā. Ielaušanās mēģinājumu skaits kopš gada sākuma ir palielinājies par 56% un salīdzinājumā ar 2023. gada 2. ceturksni vairāk nekā divas reizes.
Informācija par ielaušanās mēģinājumiem tika saņemta visa 2. ceturkšņa garumā ievērojamā intensitātē. Fiksētie kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz resursiem.



8. attēls. Apdraudēto unikālo IP adrešu skaits ar apdraudējuma veidu – ielaušanās mēģinājumi

Lielākajā daļā gadījumu tika izmantota paroļu uzlaušana ar pilno pārlasi (brute-force) pret elektronisko sakaru komersantiem, dažām valsts un pašvaldību iestādēm, kā arī uzņēmumiem.

Ielaušanās mēģinājumos tiek izmantotas arī sen zināmas konfigurācijas nepilnības plaši lietotos produktos. Tāpat, izmantojot jaunatklātas ievainojamības, kibernoziedznieki uzstājīgi meklē iespējas iekļūt organizāciju iekšējos tīklos, lai nesankcionēti piekļūtu personu datiem un sensitīvai informācijai, nošifrētu iekārtas un pieprasītu maksu par datu atgūšanu.

Novērots, ka uzņēmumi, sociālos tīklus izmantojot par tirdzniecības un reklāmas platformu, bieži cieš no pikšķerēšanas – kibernoziedznieki iekļūst tā kontā un iztērē visu reklāmai paredzēto budžetu. Ja nav noteikts konkrēts limits, cik šim mērķim tērēt, zaudējumi var sasniegt vairākus tūkstošus. CERT.LV norāda, ka ieteicams limitu tomēr noteikt un piesaistīt atsevišķu kredītkarti, kurā netiek turēts pārāk daudz naudas. Tāpat vajadzētu sekot līdzi, lai sociālo tīklu kontiem ir divfaktoru autentifikācija, un pārdomāt, kurām personām tiek dota pieeja un vai tās izmanto labi aizsargātas viedierīces.

Pārskata periodā tika fiksēts kiberuzbrukums kādā valsts iestādē, kas tika veikts, izmantojot VPN vārtejas programmnodrošinājumā. Izmantojot VPN, kam nebija iespējota divfaktoru autentifikācija, kiberuzbrucēji īslaicīgi ielauzās iestādes datorsistēmā. Izmantojot augstas privilēģijas kontu, tika iegūta piekļuve iestādes “Windows” domēna kontroliera serverim. Tīkla aizsardzībai izmantotā IDS sistēma šo pieslēgumu konstatēja un pēc situācijas precizēšanas nelegālais pieslēgums tika pārtraukts. Kiberuzbrukums neradīja paliekošas sekas, tā ierobežotais ilgums (apmēram

30 min.) neļāva uzbrucējiem veikt papildu darbības tīkla izpētei un kompromitācijai. Saņemtie žurnālfaili neliecina, ka kiberuzbrucēji būtu paguvuši izplatīt savus rīkus vai ļaunatūru iestādes datorsistēmā. Aktīvās direktorijas stāvoklis atjaunots no iepriekšējās dienas rezerves kopijas. CERT.LV agrās brīdināšanas sistēma bija detektējusi šī veida kiberuzbrukumu vērstu arī pret citu valsts iestādi, taču šis gadījumā tas nav bijis sekmīgs.

VPN (Virtual Private Network) virtuālais privātais tīkls ir risinājums drošai datu pārraidei starp klienta ierīcēm, sistēmām un lietotājiem.
Plašāk: **https://cert.lv/lv/2019/07/ouch-julija-numuravirtualie-privatie-tikli-vpn**

Šis kiberincidents kārtējo reizi apliecina divfaktoru autentifikācijas nepieciešamību – CERT.LV aicina to iespējot visur, kur vien ir tāda iespēja. Šādi uzbrukumi caur kontiem bez divfaktoru autentifikācijas maija mēnesī tika veikti daudzviet pasaulē, vēstīja arī starptautiskais kiberdrošības uzņēmums "CheckPoint". Turklāt "CheckPoint" ir publicējis atjauninājumu, kas automātiski šādus kontus atslēdz.

IETEIKUMI DROŠĪBAI

1. Regulāri atjaunināt programmatūru sistēmas.
2. Izmantot divfaktoru (2FA) autentifikāciju, nodrošinot stingras paroles politiku.
3. Šifrēt sensitīvus datus gan pārsūtīšanas, gan to glabāšanas laikā.
4. Veikt regulāras drošības pārbaudes un risku novērtējumus.
5. Izglītot darbiniekus par kiberdrošības jautājumiem.
6. Izstrādāt skaidru rīcības plānu kiberincidentu gadījumos un apmācīt darbiniekus.
7. Veikt regulāru datu rezerves kopēšanu.
8. Izmantot efektīvu ugunsmūri (piemēram, DNS ugunsmūri) un antivīrusu programmatūru.

2.6. Kompromitētas iekārtas un datu noplūdes

Pārskata periodā iekārtu kompromitēšanas gadījumi skāra gan privātpersonas, gan privātā un publiskā sektora organizācijas.

Visbiežāk pielietotās metodes sistēmu uzlaušanai un inficēšanai:

- **Pikšķerēšana:** Kiberuzbrucēji veic pikšķerēšanas satura izvietošanu vai arī izmanto tīmekļa serveri kā prettiesiski iegūto datu kolektoru.
- **Publiski zināmu ievainojamību izmantošana:** Versiju ievainojamības un jaunatklātas (*zero-day*) ievainojamības.

Datu zādzība vai noplūde – nozagti vai nopludināti uzņēmuma konfidenciālie dati, piemēram, klientu informācija, finanšu dati vai intelektuālais īpašums. Šādi uzbrukumi var ietvert gan ārējus uzbrukumus, gan iekšējus, kas saistīti ar personālu.

- **Nepareizas konfigurācijas rezultātā tīmeklī eksponēto servisu ļaunprātīga izmantošana:** Noklusējuma autentifikācijas piekļuves dati, paroļu uzlaušana ar pilno pārlasi (*brute-force*), versiju ievainojamības.
- **Pirātiskas programmatūras** uzstādīšana.
- **Paroļu pārvaldība:** Nopludinātas un viegli uzminamas lietotāju paroles, datora paroles uzglabātas nešifrētā veidā.
- **Automatizētie** kiberuzbrukumi.
- **Kompromitēti lietotāju sociālo mediju konti:** Piekļuve iegūta, izmantojot sociālo inženieriju.

Biežāk novērotie "klupšanas akmeņi", kurus CERT.LV identificēja kā būtiskus traucējumus, kas liedz pašai mērķa iestādei laicīgi un efektīvi uzraudzīt savu infrastruktūru un reaģēt uz potenciāliem incidentiem, ir šādi:

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

- nav centralizēta auditācijas pierakstu uzkrāšana un analīze;
- tīkla segmentācijas un IT infrastruktūras inventarizācijas neesamība;
- nepareizi konfigurēta vai neeksistējoša SIEM (*Security Information and Event Management*) sistēma;
- nepareizi konfigurēta vai neeksistējoša lietotāju tiesību pārvaldība un izpildāmo failu politika.

Fiksēti gadījumi, kad datora paroles tika glabātas nešifrētā veidā, lokāli uz inficēta datora, līdz ar to ierīces inficēšanas gadījumā uzbrucēji guva pieeju pie vairākiem lietotāju kontiem, kuriem nebija aktivizēta divfaktoru autentifikācija.

Kibervidē organizācijām nākas saskarties ar aizvien sarežģītākiem kiberapdraudējumiem. Šādi kiberuzbrukumi pret uzņēmumiem tiek veidoti, lai nepamanīti ielauztos to sistēmās un nozagtu vajadzīgo informāciju. Tad mērķis ir uzvesties pēc iespējas nemanāmāk, lai varētu turpināt informāciju zagt, cik ilgi vien iespējams. Nereti pikšķerēšanas uzbrukumus izmanto arī Krievijas specdienestu kibervienības, lai iegūtu piekļuvi iestāžu e-pastiem un datortīkliem.

Pārskata periodā palielinājies tādu kiberuzbrukumu skaits, kur izmantotas tā saucamās piegāžu ķēdes. Gan aprīlī, gan maijā tika ziņots par piegādes ķēžu kompromitēšanas uzbrukumu pret TV kanāliem, kas tiek retranslēti Latvijā.

Īsi pirms Eiropas Parlamenta vēlēšanām Latvijā tika kompromitēta kādas politiskās partijas tīmekļvietne. Kiberuzbrukuma rezultātā tika nopludināti vietnes satura vadības sistēmas administratora dati, kas saturēja piekļuves paroles. CERT.LV savas kompetences ietvaros sniedza atbalstu izmeklēšanā un noskaidroja, ka no upura datora tika izgūtas piekļuves paroles partijas tīmekļvietni uzturošajam serverim. Tīmekļvietne uz laiku bija nepieejama, bet tās saturs netika izķēmots. Nav pamata uzskatīt, ka kiberuzbrukums saistīts ar vēlēšanām.

TOP incidenti pārskata periodā

Kompromitētas iekārtas ar infozadzēju *AgentTesla*: Maija sākumā krāpnieki kāda datortehnikas vairumtirdzniecības uzņēmuma vārdā izplatīja ļaundabīgas e-pasta vēstules ar saiti, uz kuru noklikšķinot, tiek lejupielādēts *AgentTesla* datorvīruss. Lielākas ticamības radīšanai, krāpnieki izmantoja gan uzņēmuma logo, gan arī reāla darbinieka vārdu un uzvārdu.

Vēstulei pievienotajā saitē paslēptā ļaunatūra tika maskēta kā rēķins. *AgentTesla* mērķis ir sniegt kiberuzbrucējam piekļuvi inficētajai iekārtai un veikt informācijas zagšanu uz upura iekārtas. Pēc vīrusa izpildes inficētajā datorā, krāpniekiem tiek aizsūtīta ievāktā informācija, piemēram, paroles.

CERT.LV veiktās izpētes rezultātā tika identificētas kompromitēto datoru izejošās IP adreses, kā arī veiktas preventīvas darbības, lai apturētu turpmāku datu nosūtīšanu. Šādos gadījumos ir noteikti jāpārbauda e-pasta filtri un ielogošanās autentifikācijas faili, lai saprastu, vai nav jau kāda cita persona veikusi autentifikāciju un pārsūtījusi ienākošos e-pastus uz citu e-pastu. Tāpat nekavējoties ir jānomaina visas paroles, kas ir inficētajā datorā, kā arī jāizmanto divfaktoru autentifikāciju.

Kiberuzbrukumā Igaunijā nozagti teju 700 000 "Apotheka", "Apotheka Beauty" un "Pet City" klientu dati: Aprīlī Igaunijas aptieku tīkls "Apotheka" piedzīvoja kiberuzbrukumu, kurā tika nelikumīgi lejupielādēti vairāki simti tūkstošu aptiekas klienta kartes īpašnieku datu. SIA "Apotheka", kas pārvalda aptieku tīklu Latvijā, apgalvo, ka Latvijas

klientu dati kiberuzbrukumā nav skarti. Tomēr potenciāli ietekmētajiem lietotājiem ir jābūt gataviem iespējamiem pikšķerēšanas mēģinājumiem un krāpnieciskiem e-pasta ziņojumiem, jo pastāv identitātes zādzības risks. Šāda veida kiberuzbrukumā cietušam uzņēmumam noteikti jāinformē savi klienti par notikušo, savukārt klientiem nekavējoties jānomaina paroles un jāizmanto divfaktoru autentifikācija, lai pasargātu savus datus no kiberuzbrucējiem.

Notikuši kiberuzbrukumi TV apraides satelītiem, lai pārraidītu Krievijas propagandu

17. aprīlī notika iejaukšanās satelīta darbībā, kas nodrošina apraidi Ukrainas "Freedom" kanālam, netieši ietekmējot arī SIA "TET" televīzijas apraides saturu, ar nolūku apslāpēt leģitīmo signālu un aizstāt to ar uzbrucēja raidīto signālu tajā pašā frekvenču diapazonā. Satelīts nepieder ne Ukrainai, ne Latvijai, un ar to operē kādas citas valsts kompānija.

Ir pietiekami daudz pirmšķietamu pierādījumu tam, ka uzbrukuma izcelsme ir saistāma ar Krieviju. Ir gūta pārliecība, ka veikts apzināts uzbrukums konkrētajam satelītam, manipulējot ar satelīta signāla frekvencēm, signālu un pārraidīto saturu. Tehniskie parametri liecina par to, ka neleģitīmā signāla pārraide ir notikusi no cita, nenoskaidrota objekta. Incidenta ietekme Latvijā ir bijusi salīdzinoši neliela un SIA "TET" infrastruktūra nav tikusi ietekmēta – pats kiberuzbrukums nav bijis vērsts tieši pret Latviju. Ietekme Ukrainā un, iespējams, citās kaimiņvalstīs ir lielāka. Zināms, ka Ukrainā tika ietekmēti gandrīz 30 kanāli. Pēc šī incidenta SIA "TET" mainījuši TV kanālu signāla saņemšanu no satelīta uz IP savienojumu, kas šāda incidenta ietekmi ar satelītsignāla pārtveršanas starpniecību novērš.

Kiberdrošības eksperti prognozē, ka šādi un līdzīgi gadījumi, visticamāk, atkārtosies, jo agresorvalsts Krievija mērķtiecīgi piekopj provokācijas metodes. Tādēļ Latvijas iedzīvotāji aicināti būt modri un ziņot par novērotajiem incidentiem.

Nesankcionētas manipulācijas ar "Balticom" retranslētās interaktīvās televīzijas saturu

9. maijā notika kiberdrošības incidents, kura rezultātā AS "Balticom" interaktīvās televīzijas pakalpojuma klientiem vairākos kanālos trešo pušu rīcības rezultātā tika translēta Krievijas militārā parāde un dažādi vēstījumi krievu valodā. Kiberuzbrukums noticis satura piegādes partnera "iTV" no Bulgārijas serveriem, un "Balticom" retranslēja šo mainīto saturu. "Balticom" operatora paša infrastruktūra nav tikusi kompromitēta.

CERT.LV savas kompetences ietvaros veica tehniskās darbības un incidenta digitālo materiālu analīzi. AS "Balticom" sadarbojās ar CERT.LV komandu un incidenta izmeklēšanas laikā sniedza izmeklēšanai nepieciešamo informāciju, kā arī veica darbības incidenta ietekmes mazināšanai. Izmeklēšanas rezultātā noskaidrots, ka incidenta iemesls ir bijis uzlauzts starpniekserveris, kas pieder satura piegādes partnerim ārpus Latvijas, un "Balticom" retranslēja šo mainīto saturu. Šis incidents uzskatāmi parāda piegādes ķēžu drošības nozīmīgumu.

Analizējot publiski pieejamo informāciju, secināms, ka, iespējams, televīzijas satura ietekmēšana bija novērota arī Krievijā – Omskas, Irkutskas, Baškortostānas apgabalā. Grupējums Русский Порядок Един, kas pozicionē sevi kā esošās Krievijas varas pretinieku, ir publiski paziņojis, ka ir atbildīgs par šo kiberuzbrukumu.

CERT.LV akcentēja, ka šis nav bijis kiberuzbrukums, kas būtu vērsts pret Latvijas infrastruktūru, taču ir daļa no Krievijas hibrīdkara, un šādas provokācijas, visticamāk, turpināsies arī nākotnē, un tām ir jābūt gataviem.

IETEIKUMI DROŠĪBAI

1. **Veikt paroļu uzglabāšanu šifrētā veidā**, piemēram, izmantojot paroļu pārvaldnieku.
2. **Izmantot divfaktoru autentifikāciju visur**, kur vien tas iespējams.
3. Saņemot e-pastu no personām, ar kurām tiek veikta regulāra komunikācija, pārbaudīt, vai tiek izmantots kāds no e-pasta kontiem, kuri figurē regulārajā komunikācijā. **Sistēmu administratoriem ieteicams izmantot DMARC, SPF un DKIM tehnoloģijas.**
4. Uzturot sistēmas, kurās pieejama iekšējās lietošanas informācija, **pastāvīgi uzraudzīt eksponētos servisus**, it īpaši pie sistēmu atjauninājumu veikšanas.
5. Tīmekļa vietnēm, kurās iespējams norēķināties ar maksājumu kartēm, **veikt vietnes drošības auditu, ideālā gadījumā arī PCI sertifikāciju**.
6. Izmantojot "WordPress" vai cita veida atvērtā koda CMS, izvēlēties automātisko atjauninājumu iespēju vai **veikt regulārus atjauninājumus**. Rūpīgi izvērtēt uzstādītos spraudņus un to nepieciešamību.
7. Uzturot augstas nozīmības sistēmas vai tādas, kurās tiek glabāta informācija lielā apjomā, kas ir grūti atjaunojama, **obligāti izmantot ārējo rezerves kopiju uzturēšanu**.
8. Uzturot resursus, it īpaši informatīvus un/vai kur minētas konkrētas personas un tām piesaistītā informācija, ko iespējams izmantot jebkāda veida ļaunprātīgos nolūkos, piemēram, pikšķerēšanā, norādot jau pieejamu informāciju, aicināt vai, kur tas iespējams, **pieprasīt uzglabāt žurnālfailus**, kas satur informāciju par piekļuvi šiem resursiem un to saglabāšanu/lejupielādi, ja informācija tiek nodrošināta dokumentos ar lejupielādes iespēju.
9. **Izmantot efektīvu aktīvo aizsardzību – CERT.LV DNS ugunsmūri** (**https://dnsmuris.lv/**), lai pasargātu no ļaunprātīgu vietņu apmeklēšanas.
10. **Plānot un organizēt regulāras darbinieku apmācības un zināšanu pārbaudi** vismaz reizi gadā. Regulāri informēt darbiniekus par biežāk iespējamajiem kiberapdraudējumiem.
11. **Ieteicams regulāri sekot līdzi CERT.LV sociālo mediju kontiem un vietnei cert.lv**, kur pieejama informāciju par aktualitātēm kiberdrošības jomā.

3. Kiberapdraudējumu prevencija

3.1. DNS ugunsmūris: aktīvā aizsardzība

Latvijā regulāri notiek kampaņveidīgas krāpnieciskās aktivitātes – gan novirzīšana uz viltus vietnēm bankas kontu, e-pasta vai sociālo tīklu piekļuves datu izkrāpšanai, gan ļaunatūru izplatīšana kibertelpā. CERT.LV novēro šādas aktivitātes un operatīvi ievieto kampaņu indikatorus DNS ugunsmūrī, tādejādi pasargājot tā lietotājus no identificētajiem apdraudējumiem.

DNS UGUNSMŪRIS – aktīvās aizsardzības pakalpojums individuālu lietotāju un organizāciju pasargāšanai no kiberapdraudējumiem, tādiem kā krāpniecisku vai vīrusu izplatošu tīmekļvietņu apmeklēšanas, nodrošinot valstī vienotu ierobežojamo domēnu zonu apstrādi un izplatīšanu. Pakalpojumu bez maksas nodrošina CERT.LV un NIC.LV.

Plašāk: **https://dnsmuris.lv/**

Pārskata periodā kopskaitā apstrādātais pieprasījumu skaits DNS ugunsmūra pakalpojuma ietvaros bija vairāk nekā 1 miljons, savukārt no ļaundabīgu vietņu apmeklēšanas DNS ugunsmūra lietotāji tika pasargāti gandrīz 300 000 reižu. Pēdējo divu gadu laikā DNS ugunsmūra pakalpojuma lietošana pieaugusi aptuveni 5 reizes.

DNS ugunsmūris nodrošina aktīvu aizsardzību, kā, piemēram, ļaunatūras lejupielādes bloķēšanu, tādējādi novēršot lietotāju piekļūšanu bīstamajiem resursiem un pārvirzot tos uz brīdinājuma vietni. Arī gadījumos, kad ļaunatūra jau ir inficējusi kādu iekārtu, DNS ugunsmūris sniedz iespēju ātrāk identificēt šādas iekārtas, kas sistēmu administratoriem dod iespēju operatīvi veikt seku novēršanu.

Nozīmīgākās aktīvas aizsardzības epizodes pārskata periodā

Brīdinājumi	Skaits
Par viltus elektroniskās deklarēšanas sistēmas (EDS) lapu aktivitātēm	1 061
Par "Latvijas Pasts" tēla izmantošanu viltus vietnes kampaņās	1 650
Par *AgenTesla* ļaunatūru	530
Par *Balada* ļaunatūru, kas bija atrodama inficētās tīmekļa vietnēs	396
Par *Rasberry Robin* vīrusa aktivitāti	101

CERT.LV piedāvā iespēju iestādēm un uzņēmumiem, kas paši uztur savus DNS rekursīvos serverus, izmantot CERT.LV uzturētās DNS RPZ (Response Policy Zone), kas satur CERT.LV identificēto bīstamo resursu sarakstus.

Papildus CERT.LV uztur arī atsevišķu DNS RPZ zonu ar katras kompetentās iestādes veidoto sarakstu, kurā iekļauti resursi, kam, atbilstoši normatīvajiem aktiem Latvijā, jāierobežo piekļuve elektronisko sakaru tīklos.

CERT.LV sadarbojas ar šo sarakstu veidotājiem, tai skaitā, pirms informācijas atjaunošanas pārbauda resursu pieraksta pareizību un unificē resursu sarakstus.

Ar RPZ zonu sarakstu var iepazīties šeit:
https://cert.lv/lv/elektronisko-sakaru-komersantiem/sadarbiba-ar-cert-lv#dnsrpz

IETEIKUMI DROŠĪBAI

CERT.LV aicina ikvienu vienmēr rūpīgi pārliecināties par e-pasta vēstules vai īsziņas sūtītāja un tā vēstulē vai īsziņā pievienotās saites patiesumu. Lai pasargātos no krāpniecisku vietņu apmeklēšanas, ikvienam lietotājam ieteicams izmantot aktīvo aizsardzību – DNS ugunsmūri. CERT.LV aicina pārsūtīt saņemtos e-pastus par krāpnieku aktivitātēm un ļaundabīgām vietnēm uz **cert@cert.lv**, kā arī informēt Valsts policiju (**https://www.vp.gov.lv/lv/ka-zinot-policijai**).

3.2. Sensoru tīkls

IT drošības apdraudējumu agrās brīdināšanas sistēma ir CERT.LV nodrošināts pakalpojums, kas veic datu plūsmas anomāliju analīzi un kiberuzbrukumu pazīmju identificēšanu pakalpojuma saņēmēja infrastruktūrā.

CERT.LV pakalpojums ietver:

- nepārtrauktu datu plūsmas anomāliju analīzi un ļaunprogrammatūras aktivitāšu atpazīšanu;
- brīdinājumu nosūtīšanu pakalpojumu saņēmējam par konstatētajiem augstas prioritātes kiberapdraudējumiem;
- regulāru CERT.LV aktuālo kiberapdraudējumu indikatoru atjaunošanu;
- pakalpojuma saņēmēju konsultēšanu un atbalstu.

Sensoru tīkls – agrās brīdināšanas sistēma (ABS) iestādēm, kurās tas ir uzstādīts, ļauj laicīgi pamanīt un atpazīt radušos apdraudējumus, kā arī savlaicīgi reaģēt uz tiem, papildus nodrošinot daudzpusīgāku priekšstatu par apdraudējumu spektru valsts un pašvaldību iestādēs. Plašāk: **https://cert.lv/lv/pakalpojumi#6-informacijas-tehnologiju-drosibas-apdraudejumu-agras-bridinasanas-sistema**

CERT.LV turpina ABS sistēmas uzturēšanu un paplašināšanu. Uz pārskata perioda beigām par ABS pakalpojuma saņemšanu noslēgti un spēkā esoši ir 79 līgumi (2. ceturksnī klāt nākuši 3 jauni līgumi) un darbojās 83 sensori (atsevišķās iestādēs darbojas vairāki sensori). Tāpat tika pilnveidota un atjaunināta sensoru programmnodrošinājuma darbība.

Ik mēnesi ABS fiksē vidēji 6 000 augstas prioritātes (ar augstu bīstamības potenciālu) incidentus valsts, pašvaldību un IKT kritiskās infrastruktūras iestādēs. 2. ceturksnī ABS ģenerēto brīdinājumu skaits kopskaitā bija aptuveni 1,45 miljardi, kas ir gandrīz divas reizes vairāk nekā 1. ceturksnī. Šāda strauja un iespaidīga pieauguma iemesls galvenokārt bija plaša mēroga pikšķerēšanas kampaņas, it īpaši, uzdodoties par Valsts ieņēmumu dienestu, pārskata periodā tika pārspēti visi iepriekšējie brīdinājumu skaita rekordi.

Pārskata periodā ABS visvairāk identificētie *apdraudējumi*

Apdraudējumi	Aprīlis	Maijs	Jūnijs
Ar datorvīrusiem saistīti brīdinājumi	31 440	20 446	15 135
Krāpšanas brīdinājumi	6 652	7 595	1 413
Ar pikšķerēšanu saistīti brīdinājumi	3 176	8 487	3 767
Ar potenciāli ļaunprātīgām vietnēm saistīti brīdinājumi	11 986	7 891	11 072
Ar robottīklu, krāpšanām, vīrusu indikatoriem saistīti brīdinājumi	17 963	30 556	7 667

CERT.LV aicina organizācijas, prioritāri valsts un pašvaldību iestādes, IKT kritiskās infrastruktūras uzturētājus un pamatpakalpojumu sniedzējus, rakstīt uz cert@cert.lv par vēlmi izmantot IT drošības apdraudējumu agrās brīdināšanas sistēmas pakalpojumu un gatavību slēgt līgumu.

3.3. Pasākumi incidentu novēršanai

Pārskata periodā valsts un pašvaldību iestāžu atbildīgajiem par IT drošību, kā arī pamatpakalpojumu sniedzējiem, digitālo pakalpojumu sniedzējiem un IKT kritiskās infrastruktūras pārstāvjiem e-pasta vēstulēs tika izsūtīti vairāki paziņojumi/brīdinājumi ar aicinājumu nekavējoties veikt programmatūras atjaunināšanu.

Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta CERT.LV tīmekļa vietnē cert.lv, kā arī sociālo tīklu "X" (@certlv) un "Facebook" (@cert.lv) kontos. Tāpat "MatterMost" saziņas platformā notiek regulāra informācijas apmaiņa starp CERT.LV, atbildīgajiem par IT drošību un citiem kiberdrošības kopienas locekļiem.

Būtiskākie brīdinājumi pārskata periodā:

- **10. aprīlī:** brīdinājums par 7 kritiskām un ļoti nopietnām ievainojamībām "Fortinet" ražotajās iekārtās. Nopietnākās ievainojamības ļauj veikt attālināto koda izpildi (RCE), nesankcionēti dzēst datnes, patvaļīgi izpildīt OS komandas.
- **12. aprīlī:** brīdinājums par ievainojamību, kas saistīta ar komandu ievadīšanu un var tikt izmantota "Palo Alto Networks" piedāvātajās "VPN-GlobalProtect" vārtejās.
- **23. maijā:** brīdinājums par 3 ievainojamībām "Veeam Backup Enterprise Manager" iekārtās. Nopietnākā ievainojamība ļauj neautentificētiem uzbrucējiem apiet autentifikāciju un iegūt piekļuvi tīmekļa saskarnei kā jebkuram autorizētam sistēmas lietotājam.
- **3. jūnijā:** brīdinājumi par augsta riska ievainojamību "Check Point Security" iekārtās, kas tiek izmantota uzbrukumos, lai iegūtu attālinātu piekļuvi ugunsmūriem un mēģinātu ielauzties uzņēmumu infrastruktūrā.

3.4. Koordinēta ievainojamību atklāšana (CVD)

CERT.LV turpināja darbu pie koordinētas ievainojamību atklāšanas ziņojumu reģistrēšanas platformas cvd.cert.lv (CVD) attīstības un popularizēšanas, pildot koordinētas ievainojamību atklāšanas procesa koordinētāja un vidutāja, kā arī platformas izstrādātāja, uzturētāja un pārziņa lomu.

CVD platformā, kas darbību uzsākta 2023. gadā, ir publicēta informācija par iestādēm, kuras brīvprātīgi iesaistījušās koordinētas ievainojamību atklāšanas procesā un noteikušas resursus, uz kuriem ievainojamību ziņošana attiecināma.

Koordinēta ievainojamību atklāšanas platforma cvd.cert.lv (CVD) nodrošina iespēju pētniekam reģistrēt ziņojumu par novēroto ievainojamību, kā arī visiem iesaistītajiem (iestādei, pētniekam un CERT.LV) iepazīties ar iesniegto informāciju, savā starpā sazināties un sekot līdzi ievainojamību novēršanas gaitai.

Plašāk: **https://cvd.cert.lv/**

Platformā tiek reģistrēti ievainojamību ziņojumi un notiek ar to apstrādi saistītā komunikācija starp iesaistītajām pusēm. Šāda ziņošanas prakse dod iespēju CERT.LV savlaicīgi uzzināt par ievainojamībām un pilnvērtīgi koordinēt ievainojamību izpēti un to novēršanu, tā efektīvāk organizēt pasākumus Latvijas kibertelpas aizsardzībai.

CERT.LV veiktais darbs pie CVD platformas darbības attīstības jau ir devis pozitīvus rezultātus. 2. ceturksnis CVD platformā ir bijis īpaši ražīgs: Drošības pētnieku skaits pieauga par 57%, uz konkrētām iestāžu programmām reģistrēto ievainojamību skaits pieauga gandrīz pieckārtīgi, savukārt reģistrēto ziņojumu skaits par CERT.LV klientūras ievainojamībām pieauga gandrīz trīskārtīgi.

Uz pārskata perioda beigām platformā bija reģistrēti:

- Drošības pētnieki – 66 (kopš iepriekšējā ceturkšņa beigām skaits pieauga par 24);
- Aktīvas iestāžu programmas – 10 (skaits pieauga par 3);

Uz pārskata perioda beigām platformā reģistrēti 82 ievainojamību ziņojumi, tostarp:

- CERT.LV klientūras ievainojamības – 44 (skaits pieauga par 28);
- Uz konkrētām iestāžu programmām reģistrētās ievainojamības – 38 (pieauga par 30).

CVD platformas attīstība

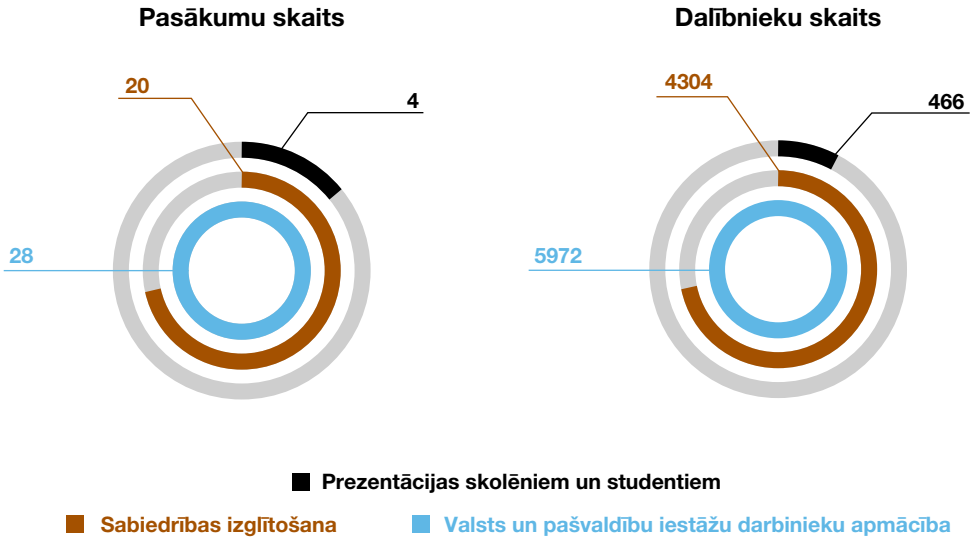
Turpinās darbs pie CVD platformas attīstības, ieviešot pētnieku reitingu un profila informācijas pārvaldīšanas iespēju. Lai nodrošinātu efektīvāku ziņojumu apstrādi, CERT.LV aicina platformā reģistrēties visas iesaistītās puses, tādējādi paātrinot informācijas apmaiņu un padarot caurspīdīgāku saziņu ievainojamības izpētes un novēršanas laikā.

4. Komunikācija ar sabiedrību

4.1. Apmācības un izglītojošie pasākumi

Pārskata periodā CERT.LV komanda veica aktīvu darbu sabiedrības izglītošanā, gan organizējot, gan piedaloties dažādos tematiskos semināros, informējot par aktualitātēm kiberdrošības jomā, kā arī veicinot kiberhigiēnas labo praksi.

2024. gada 2. ceturksnī CERT.LV īstenoja 52 izglītojošus pasākumus par IT drošību un aktualitātēm, apmācot kopskaitā 10 742 dalībniekus visā Latvijā.



9. attēls. Izglītojošo pasākumu un apmācīto personu skaits 2024. gada 2. ceturksnī

CERT.LV kiberdrošības eksperti piedalījās "Digitālā nedēļa 2024" pasākumos, kas norisinājās no 13. līdz 18. maijam. Šīs nedēļas ietvaros dažādu pasākumu formātos visā Latvijā uzņēmumi un iedzīvotāji tika aicināti attīstīt savas digitālās prasmes biznesam un nodarbinātībai, aktīvāk izmantojot digitālās tehnoloģijas un pakalpojumus.

16. maijs tematiski tika veltīts tieši digitālās drošības jautājumiem, kur visas dienas garumā norisinājās dažādi ar šo tēmu saistīti informatīvie un izglītojošies pasākumi un aktivitātes.CERT.LV sadarbībā ar Latvijas Valsts radio un televīzijas centru (LVRTC), NIC.LV un Finanšu nozares asociāciju šajā dienā organizēja vebināru "Kiberdroša uzņēmuma anatomija digitālajā vidē", kas bija orientēts uz mazajiem un vidējiem uzņēmumiem.

Arī Eiropas Parlamenta vēlēšanu ietvaros CERT.LV īstenoja izglītojošus pasākumus Latvijā, lai iepazīstinātu vēlēšanu komisiju un iecirkņu komisiju darbiniekus ar kiberdrošības riskiem, kas saistīti ar vēlēšanu norisi un kiberhigiēnas pamatiem.

Lepojamies!

Izcilu sniegumu Latvija demonstrēja NATO organizētajās pasaulē lielākajās starptautiskajās kiberaizsardzības mācībās "Locked Shields 2024". Šogad aprīlī Latvijas apvienotā komanda, tostarp CERT.LV kiberdrošības speciālisti, izcīnīja godpilno 1. vietu. Latvija piedalījās mācībās kopā ar NATO Komunikācijas un informācijas aģentūras komandu (NCIRC), veidojot vairāk nekā 220 cilvēku lielu ekspertu komandu, no kuriem aptuveni 200 bija Latvijas pārstāvji. Komandas vadību uzņēmās Latvijas Republikas Zemessardzes Kiberaizsardzības vienība.

NATO organizēto mācību gaitā vairāk nekā 4000 dalībnieku no 40 valstīm apvienoja spēkus simulētā vidē, lai aizsargātu iedomātas virtuālas valsts infrastruktūru. Redzot sasniegtos rezultātus, CERT.LV komanda var lepoties ar izciliem kiberdrošības profesionāļiem!

Aizsardzības ministrijas GODA RAKSTS tika pasniegts CERT.LV komandai par izciliem sasniegumiem NATO kiberaizsardzības mācībās "Locked Shields 2024", to saņēma CERT.LV vadītāja Baiba Kaškina.

Pateicības rakstus par veiksmīgu sadarbību un ieguldījumu Latvijas kibertelpas drošības un Latvijas valsts aizsardzības spēju stiprināšanā saņēma CERT.LV darbinieki: Agnese Kriķe, Gints Neimanis, Kārlis Svilans un Rūdolfs Ķelle.

Galda izspēles mācības par kiberdrošības incidentu izmeklēšanu

CERT.LV turpina savai klientūrai nodrošināt praktisko kiberincidenta izmeklēšanas izspēli, kur dalībniekiem tiek sniegta unikāla iespēja iejusties kiberdetektīvu lomā un interaktīvā veidā pētīt un analizēt kiberuzbrukuma gaitu starptautiskā uzņēmumā. Viens no izspēles centrālajiem uzdevumiem ir noskaidrot vainīgo, kurš ir atbildīgs par kiberuzbrukumu, kā arī pārrunāt tā sekas. Pārskata periodā CERT.LV organizēja interaktīvas mācības četrās organizācijās, kurās CERT.LV speciālistu vadībā tika izspēlēta kiberdrošības incidentu spēle:

6. aprīlī – Biedrībā "She Can Do IT";

10. aprīlī – Zemessardzes 4. brigādei;

12. aprīlī – Zemgales reģiona kompetenču attīstības centrā;

13. jūnijā – ALTUM.

Kopskaitā no visām organizācijām spēlēs piedalījās 119 dalībnieki. Kiberdrošības incidentu izmeklēšanas spēli sagatavojusi Eiropas Savienības Kiberdrošības aģentūra ENISA, lai veicinātu izpratni par kiberdrošību jomas nespeciālistiem, savukārt latviešu valodā to tulkojusi un pielāgojusi CERT.LV komanda Dainas Ozoliņas vadībā.

CERT.LV organizētās interaktīvās mācības Zemgales reģiona kompetenču attīstības centrā

Būtiskāko pasākumu apskats pārskata periodā

4. aprīlī CERT.LV piedalījās "Ēnu dienas" pasākumā un uzņēma ēnotājus, lai iepazīstinātu jauniešus ar kiberdrošības sfēru un veicinātu interesi par kiberdrošības speciālista profesiju.

4. aprīlī NEPL pasākumā ar prezentāciju "Mākslīgais intelekts un digitālā drošība" uzstājās CERT.LV eksperts Egīls Stūrmanis.

6. aprīlī kiberdrošības seminārā "No draudiem līdz izmeklēšanai", ko organizē "She Can Do IT" sadarbībā ar CERT.LV, ar pieredzes stāstiem dalījās CERT.LV ekspertes Daina Ozoliņa un Dana Ludviga.

CERT.LV "Ēnu dienas" pasākuma dalībnieki

8. aprīlī studentu korporācijas IMERIA rīkotajā viesu vakarā ar prezentāciju "Kiberdrošības aktualitātes, draudi un risinājumi" piedalījās CERT.LV eksperte Dana Ludviga.

11. aprīlī "Baltic Security Conference" paneļdiskusijā "Mākslīgā intelekta ietekme uz drošību" diskutēja CERT.LV eksperts Jānis Džeriņš. Papildus šajā konferencē CERT.LV tika pārstāvēta ar stendu, kur plašākai sabiedrībai bija iespēja iepazīties ar CERT.LV piedāvāto pakalpojumu klāstu un to sniegtajām priekšrocībām.

17. aprīlī tiešsaistes seminārā "Kiberdrošība mazajiem un vidējiem uzņēmumiem" ar vadlīnijām un praktiskiem ieteikumiem dalījās CERT.LV eksperts Mārtiņš Vecstaudžs.

19. aprīlī Jelgavas tehnoloģiju vidusskolas klātienes konferencē "Mūsdienu tehnoloģijas skolā" jauniešus uzrunāja CERT.LV eksperts Gints Mālkalnietis.

26. aprīlī tiešsaistes seminārā "Kiberhigiēnas pamati publiskās pārvaldes darbiniekiem" kā lektors uzstājās CERT.LV eksperts Mārtiņš Vecstaudžs.

26. aprīlī iniciatīvas "Women4Cyber Latvia" viena gada jubilejas pasākumā paneļdiskusijā "Pieredzes stāsti" CERT.LV kiberdrošības analītiķe Dace Bulte stāstīja par savu karjeras ceļu, iedvesmojot sievietes uzdrošināties pieņemt jaunus izaicinājumus, iesaistīties un turpināt profesionālo attīstību kiberdrošības jomā. "Women4Cyber" mērķis ir veidot stipru kiberdrošības kopienu, pulcējot gan speciālistes, kuras jau darbojas kiberdrošības jomā, gan tās, kuras vēlas iesaistīties nozarē, iedrošinot un izglītojot.

8. maijā tiešsaistes seminārā "Kiberhigiēna ārstniecības iestādēs" ar vadlīnijām un praktiskiem ieteikumiem dalījās CERT.LV eksperts Mārtiņš Vecstaudžs.

8. maijā Rīgas domes iedzīvotāju informēšanas kampaņas un semināru cikla par civilo aizsardzību "Rīgas civilās aizsardzības plāns – pārzini un līdzdarbojies!" ietvaros, CERT.LV eksperts Gints Mālkalnietis dalījās ar CERT.LV novērojumiem un praktiskiem ieteikumiem pasākumā "Informācijas saņemšana un dezinformācijas riski – ieteicamā rīcība, kas pasargā".

10. maijā Alūksnē CERT.LV vadītājas vietnieks Varis Teivāns piedalījās reģionālajā seminārā par visaptverošu valsts aizsardzību, kura mērķis bija informēt par Latvijas aizsardzībai un drošībai aktuāliem tematiem. V. Teivāns semināra dalībniekus informēja par aktuālajiem kiberdrošības izaicinājumiem un apdraudējumiem reģionā. Tāpat ar aizsardzības nozares pārstāvjiem un semināra dalībniekiem tika pārrunāta sabiedrības loma valsts aizsardzības un kiberdrošības stiprināšanā.

10. maijā CVK darbinieku apmācībās "Kiberhigiēna -2024" uzstājās un ar praktiskiem ieteikumiem dalījās CERT.LV eksperts Egīls Stūrmanis.

16. maijā "Digitālās drošības diena" pasākumā, kas tika veltīts kiberdrošības jautājumiem, CERT.LV sadarbībā ar LVRTC, NIC.LV un Finanšu nozares asociāciju organizēja tiešsaistes semināru "Kiberdroša uzņēmuma anatomija digitālajā vidē" uzņēmējiem. Šajā seminārā uzņēmumiem kodolīgu ieskatu par drošas mājaslapas "ABC" sniedza CERT.LV eksperte Dana Ludviga. Savukārt, kā pasargāt no uzbrucējiem uzņēmuma sociālo tīklu kontus, ar praktisku

pieredzi un padomiem dalījās CERT.LV Sabiedrisko attiecību un komunikācijas grupas vadītāja Līga Besere. Semināra ieraksts šeit: **https://www.youtube.com/watch?v=tbXgKoCAqSI&t=6442s**

16. maijā #digiTuvi StarFM rubrika | #7 sērijā – "Esi soli priekšā krāpniekiem ar DNS ugunsmūri!" piedalījās CERT.LV eksperte Dana Ludviga un stāstīja par aktīvās aizsardzības rīku DNS ugunsmūris. Raidījumā klausītāji varēja uzzināt no kāda veida kiberapdraudējumiem tas pasargā ne tikai individuālus lietotājus, bet arī organizācijas, un kā tas strādā, ar ko tas atšķiras no citiem ugunsmūriem, un visbeidzot – kā to aktivizēt.
Raidījuma ieraksts pieejams šeit: **https://www.youtube.com/watch?v=S3mOJrFD16w**

30. maijā #digiTuvi StarFM rubrika | #9 sērijā – "Nepieciešamās zināšanas un prasmes karjerai kiberdrošībā" piedalījās CERT.LV vadītājas vietnieks Varis Teivāns. Viņš stāstīja par nepieciešamajām zināšanām un prasmēm, lai attīstītu karjeru tieši kiberdrošības jomā, un kādām īpašībām jāpiemīt labam kiberdrošības speciālistam, kā arī dalījās pieredzē par savu personīgo karjeras ceļu kiberdrošības jomā.
Raidījuma ieraksts pieejams šeit: **https://www.youtube.com/watch?v=IBPSLUMDz7M&t=346s**

6. jūnijā ikgadējā "Riga StratCom Dialogue" konferencē CERT.LV vadītājas vietnieks Varis Teivāns stāstīja par tehnoloģiju tendencēm un to ietekmi uz kiberdrošību Latvijā.

Ar "KiberŠahs 2024" organizēšanu saistītie darbi

Turpinās darbs pie starptautiskās kiberdrošības konferences "KiberŠahs 2024" ("CyberChess 2024") organizēšanas, kas norisināsies 1.-3. oktobrī. Konferences pirmajā dienā ir plānoti vairāki izglītojoši praktiskie semināri, savukārt otrajā un trešajā pasākuma dienā – vairākas paralēlās sesijas, kur paredzētas prezentācijas, diskusijas un praktiski demonstrējumi no pasaules līmeņa kiberdrošības ekspertiem.

4.2. Sabiedrības informēšana un kiberhigiēnas veicināšana

Pārskata periodā CERT.LV turpināja informēt sabiedrību par kiberdrošības riskiem, kiberhigiēnas veicināšanu un labo praksi, kā arī citām aktualitātēm Latvijas kibertelpā. 2. ceturksnī ar 420 publikācijām plašsaziņas līdzekļos potenciālais skatījumu skaits bija 17,54 miljoni.
Pārskata periodā mediju vislielāko interesi izraisīja aktuālā situācija Latvijas kibertelpā EP velēšanu kontekstā. Nozīmīga uzmanība tika pievērsta Latvijas apvienotās kiberdrošības komandas izcīnītajai 1. vietai lielākajās NATO kiberaizsdardzības mācībās pasaulē "Locked Shields 2024". Pastiprināta interese bija arī par piegādes ķēžu kompromitēšanas uzbrukumiem pret "TET" un "BALTICOM" TV kanāliem, kas tiek retranslēti Latvijā.
CERT.LV turpina tulkot un portālā www.esidross.lv publicēt OUCH! ikmēneša izdevumus (informācijas drošības biļetens, ko sagatavo SANS institūts).

Pārskata periodā portālā esidross.lv publicētie raksti:

- Trīs izplatītākie kiberuzbrukumu veidi, OUCH! 05/2024
- Dodaties atvaļinājumā? Vienkārši soļi kiberdrošības nodrošināšanai, OUCH! 06/2024
- Teksta ziņojumapmaiņas uzbrukumi: Smikšķerēšanas sāga OUCH! 07/2024

Ikmēneša "KiberLaikapstākļi" apskats

CERT.LV turpināja apkopot ikmēneša apskatu "KiberLaikapstākļi" par aizvadīta mēneša spilgtākajiem notikumiem kibertelpā TOP 5 kategorijās – krāpšana, ļaunatūras, ievainojamības, pakalpojuma pieejamība, ielaušanās un datu noplūde, kā arī lietu internets. Pārskati publicēti tīmekļa vietnes www.cert.lv sadaļā "Ziņas":

- **Aprīlis: https://www.cert.lv/lv/2024/05/kiberlaikapstakli-aprilis**
- **Maijs: https://cert.lv/lv/2024/06/kiberlaikapstakli-maijs#Krapsana**
- **Jūnijs: https://cert.lv/lv/2024/07/kiberlaikapstakli-2024-junijs**

5. Stratēģiskā sadarbība Latvijā

Publiskā un privātā partnerība, drošības konsultācijas, Aizsardzības ministrijas un Iekšlietu ministrijas iniciatīvas nav iespējamas bez efektīvas stratēģiskās sadarbības. Turklāt speciālistu sadarbība un viedokļu apmaiņa darba grupās palīdz mazināt riskus, uzlabot nacionālo drošību un nodrošināt būtisko un svarīgo pakalpojumu pieejamību sabiedrībai.

CERT.LV speciālisti cieši sadarbojas ar Latvijas Republikas Zemessardzes Kiberaizsardzības vienību, kas IT drošības krīzes vai apdraudējuma situācijā sadarbībā ar CERT.LV var sniegt atbalstu valstij un privātajam sektoram. Pārskata periodā svarīgākā sadarbība notika, piedaloties kiberdrošības mācību "Locked Shields 2024" plānošanā un Latvijas komandas sagatavošanā mācībām. Demonstrējot izcilu sniegumu, šogad Latvijas apvienotā komanda ieguva 1. vietu. Latvija var lepoties ar izciliem kiberdrošības profesionāļiem.

CERT.LV turpināja organizēt Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupas (DEG) sanāksmes. DEG ir brīvprātīga Informācijas tehnoloģiju un Informācijas sistēmu drošības ekspertu grupa ar mērķi veicināt IT/IS drošību, sekmēt drošības apziņas kultūru Latvijā un sniegt atbalstu CERT.LV. Sanāksmes notiek katra mēneša otrajā ceturtdienā.

CERT.LV cieši sadarbojas ar Aizsardzības ministrijas Nacionālās kiberdrošības politikas koordinācijas nodaļu un savas kompetences ietvaros aktīvi piedalījās Nacionālās kiberdrošības stratēģijas uzdevumu īstenošanā un normatīvo dokumentu izstrādes procesā.

Turpinās sadarbība ar Latvijas Interneta asociāciju (LIA), kas izglīto sabiedrību par iespējamajiem riskiem un draudiem interneta vidē, veicinot drošu interneta lietošanu un nodrošinot ziņojumu līniju ziņošanai par bērnu seksuālu izmantošanu atainojošu materiālu apriti internetā. (LIA Drošāka interneta centra ziņojumu līnijas darbības pārskatu skatīt 7. nodaļā).

5.1. Kibernoziedzības novēršana un apkarošana

Sadarbība ar IKT kritiskās infrastruktūras turētājiem

Turpinās sadarbība ar IKT kritiskās infrastruktūras turētājiem, gan uzraugot situāciju kibertelpā, gan sniedzot konsultācijas un atbalstu kibernoturības stiprināšanai un dažādu sektoru sadarbības pilnveidošanai.

Pārskata periodā tika būtiski pilnveidots CERT.LV pakalpojumu ietvars, gan izstrādājot jaunus risinājumus pakalpojumu sniegšanai, gan pilnveidojot ar šo pakalpojumu sniegšanu saistītās procedūras.

IKT kritiskās infrastruktūras turētājiem CERT.LV piedāvā plašu pakalpojumu klāstu, tostarp pikšķerēšanas uzbrukumu simulācijas, kiberapdraudējuma simulācijas (ietver SOC / SIEM / EDR / XDR / MDR spēju, procedūru, tvēruma, kvalitātes un reakcijas testus), agrās brīdināšanas sistēmas, CERT.LV MISP (ar ļaunatūru saistītās informācijas apmaiņas platforma), draudu medību operācijas, kā arī CERT.LV Drošības operāciju centra (SOC) pakalpojumus.

Lai veicinātu industriālās automatizācijas un kontroles sistēmu drošību, CERT.LV piedāvā drošības laboratorijas pakalpojumu, kas paredzēta operacionālo tehnoloģiju (OT), to iekārtu, programmatūras, un lietoto komunikācijas protokolu drošības testēšanai. Sadarbībā ar Latvijas industrijas partneriem CERT.LV veic darbu pie OT drošības sensora prototipa izstrādes un testēšanas.

CERT.LV piedāvā iespēju iestādēm un uzņēmumiem izmantot CERT.LV uzturētās DNS RPZ (reakcijas politikas zonas), kas satur CERT.LV identificēto bīstamo resursu sarakstus, lai veicinātu ātrāku IKT kritiskās infrastruktūras apdraudējumu identificēšanu un efektīvāku to novēršanu. Plašāk par CERT.LV nodrošināto bezmaksas pakalpojumu klāstu: **https://cert.lv/lv/pakalpojumi**

Atbalsts Latvijas valsts tiesībsargājošajām iestādēm

CERT.LV, cieši sadarbojoties ar Centrālās vēlēšanu komisijas (CVK), Valsts kanceleju un citām vēlēšanu procesā iesaistītajām institūcijām, strādāja, lai veiktu ielaušanās testus visām sistēmām, kas iesaistītas Eiropas Parlamenta (EP) vēlēšanu norises nodrošināšanā. Pārskata periodā Latvijā netika novērots neviens incidents, kas būtu tieši saistāms ar vēlēšanu sistēmām vai vēlēšanu drošību.

CERT.LV eksperti savas kompetences ietvaros deva vērtīgu ieguldījumu darba grupās, kas saistītas ar vēlēšanu organizēšanu gan no tehnoloģiskā viedokļa, gan no drošības viedokļa. CERT.LV komanda izvērtēja gan trešo pušu veiktos vēlēšanu sistēmu drošības testus, gan arī pati veica testēšanu un sniedza ieteikumus drošības uzlabošanai.

Tika simulēta kiberuzbrucēju rīcība, mēģinot kontrolēti ielauzties sistēmās, lai pārbaudītu, vai nav atrodamas būtiskas ievainojamības, gan veikti slodzes testi, kas simulēja gan dabīgu lietotāju apmeklētību, gan arī potenciālā uzbrucēja izraisītu sistēmas pārslodzi. Testu rezultātā tika gūta pārliecība par šo sistēmu noturību. Tika veikta arī funkcionālo daļu pārbaude, lai pārliecinātos, ka tur nav loģikas kļūdu vai nav iespējamas citas neparedzamas darbības.

Kopskaitā testi tika veikti trīs sistēmām, no kurām sarežģītākās sistēmas tests tika pabeigts jau šā gada 1. ceturksnī. Savukārt atlikušo divu sistēmu testus CERT.LV pabeidza 2. ceturkšņa sākumā, un to rezultātā netika konstatēta neviena kritiska ievainojamība, kas varētu būtiski ietekmēt šo sistēmu darbību. Resursu turētājiem un izstrādātājiem tika iesniegti pārskati par testu rezultātiem un sniegtas rekomendācijas nepilnību novēršanai.

Pārskata periodā CERT.LV sadarbība ar visiem piegādātājiem ir vērtējama kā veiksmīga, visas atklātās nepilnības ir tikušas savlaicīgi novērstas.

Draudu medību operācijas

Kibertelpa ir kļuvusi par stratēģiski nozīmīgu vidi, līdzvērtīgu zemei, jūrai, gaisam un kosmosam. Pēc Krievijas pilna mēroga iebrukuma Ukrainā šī nozīme ir vēl acīmredzamāka. Proaktīvu kiberuzbrucēju klātbūtnes meklēšanu jeb draudu medību operācijas CERT.LV sadarbībā ar partnervalstīm Latvijai svarīgās infrastruktūras sistēmās veic kopš 2022. gada.

CERT.LV komanda ir līdere draudu medību operāciju organizēšanā un vadīšanā ES, sniedzot savu ieguldījumu NATO kolektīvajā aizsardzībā, veicinot starptautisko normu piemērošanu kibertelpā un veidojot uzticamu sabiedroto loku, kas spēj gan sniegt savstarpēju atbalstu kiberdraudu izvērtējumā, gan ātri apmainīties ar informāciju un labajām praksēm.

Draudu medību operāciju rezultātā izdevies būtiski stiprināt Latvijas IKT kritiskās infrastruktūras un digitālo pakalpojumu kibernoturību, turklāt vairākkārtīgi ir izdevies identificēt un veiksmīgi likvidēt citu valstu kiberoperāciju vienību klātbūtni Latvijai svarīgās infrastruktūras sistēmās.

CERT.LV draudu medības notiek ar mērķi identificēt kiberapdraudējumu klātbūtni Latvijai svarīgās IKT infrastruktūras sistēmās. Līdz pārskata beigām ir analizētas vairāk nekā 140 000 iekārtas 31 organizācijā. 25% jeb 8 organizācijās ar augstu ticamību konstatēta ārvalstu APT klātbūtne.

Gatavojoties Eiropas Parlamenta vēlēšanām jūnijā, atkārtotas draudu medības notika Centrālās vēlēšanu komisijas infrastruktūrā un citās ar vēlēšanu sistēmu saistītās infrastruktūrās, kā arī tika veikti vairāki pasākumi ar drošības testiem CERT.LV klientūras organizācijās un sniegti ieteikumi drošības uzlabošanai. Latvijā netika novērots neviens incidents, kas būtu tieši saistāms ar vēlēšanu sistēmām vai vēlēšanu drošību.

Sniedzot savu ieguldījumu NATO kolektīvajā aizsardzībā, CERT.LV turpina draudu medību operācijas ciešā sadarbībā ar Kanādas Bruņoto spēku kiberpavēlniecību, kas ir būtiska kiberaizsardzības spēju kāpināšana, attīstot savas spējas un pretstāvēšanas kapacitāti, lai novērstu jebkura kiberuzbrukuma iespējamību.

Noslēgušās mēnesi ilgas draudu medības ar paplašinātu sabiedroto klātbūtni: CERT.LV jūnija beigās noslēdza paplašinātas klātbūtnes draudu medību operāciju, kurā piedalījās Kanādas bruņoto spēku kiberpavēlniecības, Kanādas kiberdrošības centra un Latvijas bruņoto spēku pārstāvji. Paplašinātā klātbūtne spēcināja un papildināja pastāvīgi notiekošās draudu medības.

Vairākas sabiedroto nācijas (Polija, Nīderlande, Francija un ASV) apmeklēja notiekošo paplašinātās klātbūtnes operāciju, lai mācītos no Latvijas un Kanādas veiksmīgās sadarbības, un, iespējams, pārņemtu labo praksi, lai īstenotu to atbildības jomās savās valstīs.

Paplašinātās klātbūtnes operācijas laikā, vēlreiz apliecinot Latvijas un Kanādas stratēģiski svarīgo sadarbību, to apmeklēja arī vairākas augsta līmeņa amatpersonas no Kanādas – Kanādas Vēstnieks NATO D. Angell, Kanādas Aizsardzības atašejs NATO viceadmirālis Bishop, Kanādas kiberpavēlniecības komandieris flotiles admirālis Carosielli un Kanādas Bruņoto spēku pārstāvniecības Latvijā komandieris pulkvedis V. G. Kirstein.

Publicēts pirmais Latvijas kibertelpas un CERT.LV tehnisko aktivitāšu 2023. gada pārskats: CERT.LV komanda 2023. gadā par prioritāti noteica draudu medību operācijas – proaktīvas kiberuzbrucēju meklēšanas operācijas Latvijas IKT kritiskajā infrastruktūrā, lai stiprinātu valsts nacionālajai drošībai un sabiedrībai nozīmīgu pakalpojumu sniedzēju sistēmu noturību un drošību.

2023. gada pārskata mērķis – sniegt Latvijas kiberdrošības pārvaldniekiem un speciālistiem operacionāli pielietojamu informāciju, analītiķiem izmantojamu apkopojumu par aizvadītā gada notikumiem Latvijas un Ziemeļeiropas reģiona kibertelpā, kā arī kiberdrošības situācijas attīstības prognozes tuvākai nākotnei.

Pārskatā ir ietverti praktiski ieteikumi kiberapdraudējumu prevencijai, kurus CERT.LV aicina nekavējoties īstenot, lai paaugstinātu kiberdrošības līmeni un efektīvāk aizsargātu savas organizācijas IKT infrastruktūru.

CERT.LV aicina iepazīties ar 2023. gada pārskatu plašāk:
https://cert.lv/lv/2024/06/latvijas-kiberdrosibas-un-cert-lv-tehnisko-aktivitasu-2023-gada-parskats

Izcils sniegums starptautiskajās kiberdrošības mācībās: Pārskata periodā izcilu sniegumu Latvija demonstrējusi starptautiskajās kiberdrošības mācībās – šogad Latvijas apvienotā komanda, kurā savu ieguldījumu deva arī CERT.LV speciālisti, ieguva 1. vietu lielākajās kiberaizsardzības mācībās pasaulē "Locked Shields 2024". Tas apliecina to, ka ir izveidots spēcīgs profesionāls pamats, lai efektīvi turpinātu pilnveidot un attīstīt Latvijas kiberdrošības infrastruktūru un ekspertīzi.

CERT.LV sadarbība kiberdrošības jomā

- Saistībā ar Nacionālās kiberdrošības likuma (NKDL) ieviešanu, kura mērķis ir stiprināt kiberdrošību Latvijā un ieviest pārskatītās Eiropas Savienības Tīklu un informācijas sistēmu drošības direktīvas (NIS2) prasības vienādi augsta kiberdrošības līmeņa panākšanai visā Eiropas Savienībā (ES), tika veikti sagatavošanās pasākumi, lai CERT.LV ir gatava jauno uzdevumu izpildei, kad tiks uzsākta NIS2 direktīvas piemērošana un stāsies spēkā NKDL. CERT.LV

2024. gada 20. jūnijā Saeima pieņēma Nacionālās kiberdrošības likumu. Šis likums attiecas uz būtisko un svarīgo pakalpojumu sniedzējiem, kā arī informācijas un komunikācijas tehnoloģiju kritisko infrastruktūru, un tajā ir noteikti kritēriji, pēc kuriem tiek definēta publiskā un privātā sektora organizācijas piederība kādai no minētajām grupām.
Plašāk: **https://cert.lv/lv/2024/06/saeima-pienem-nacionalas-kiberdrosibas-likumu**

piedalās nozares politikas pamatnoteikumu sagatavošanā. Sekmējot Kiberdrošības pārvaldes reformas mērķu sasniegšanu, CERT.LV turpina darbu pie jauno normatīvo aktu skaidrošanas un vadlīniju sagatavošanas, lai atbalstītu NKDL subjektus jauno prasību ieviešanā.

- Pārskata periodā tika veikta likumprojektu / iniciatīvu izskatīšana, tostarp ES un Latvijas līmeņa likumprojekti, kā arī organizētas sanāksmes ar Latvijas līmeņa likumprojektu virzītājiem atsevišķu problēmjautājumu vai komentāru pārrunāšanai.
- Aktīva iesaiste CVK Vēlēšanu darba grupā, sniedzot rekomendācijas drošai vēlēšanu sistēmu izstrādei un uzturēšanai. CERT.LV eksperti regulāri piedalījās Vēlēšanu IT darba grupas un starpinstitūciju darba grupas sanāksmēs. CERT.LV sniedza savu redzējumu CVK par IT riskiem saistībā ar EP 2024. gada vēlēšanu nodrošināšanu, izvērtēja trešo pušu veiktos vēlēšanu sistēmu drošības testus, kā arī pati veica testēšanu un sniedza rekomendācijas drošības uzlabošanai. CERT.LV īstenoja arī izglītojošus pasākumus, lai iepazīstinātu vēlēšanu komisiju un iecirkņu komisiju darbiniekus ar kiberdrošības riskiem, kas saistīti ar vēlēšanu norisi un kiberhigiēnas pamatiem.
- Sadarbībā ar Aizsardzības ministriju CERT.LV apkopoja un izplatīja informatīvo materiālu **"ABC ceļvedis"** kiberdrošības veicināšanai iestāžu vadītājiem, kur sniegti padomi par to, kā mazināt potenciālos riskus un apzināt potenciālos draudus, ar ko iestādes un uzņēmumi varētu saskarties kibertelpā.
- Sadarbībā ar Aizsardzības ministriju CERT.LV, primāri fokusējoties uz kiberdrošības aspektiem, izstrādāja informatīvo materiālu iedzīvotājiem un rokasgrāmatu pašvaldībām **"Kā rīkoties kara gadījumā"**.
- Iesaiste Nacionālā koordinācijas centra vadītajā Starpinstitucionālajā darba grupā, kuras mērķis – veicināt informācijas apmaiņu starp valsts pārvaldes iestādēm un organizācijām par aktivitātēm un pasākumiem dažādās kiberdrošības jomās, lai sekmētu efektivitāti un sadarbību.
- 3. aprīlī CERT.LV vizītē uzņēma Moldovas Republikas Aizsardzības ministru Anatoliju Nosatiju (Anatolie Nosatîi), lai pārrunātu kiberdrošības jautājumus abās valstīs un iespējamo sadarbību kiberdraudu apzināšanā, informācijas apmaiņā un citos aspektos.

CERT.LV vadītāja Baiba Kaškina un LR Aizsardzības ministrijas pārstāvis Edgars Kiukucāns tiekas ar Moldovas Republikas Aizsardzības ministru un citiem delegācijas pārstāvjiem.

5.2. CERT.LV atbalsts DDUK sekretariāta darbā

Pārskata periodā CERT.LV turpināja aktīvi iesaistīties Digitālās drošības uzraudzības komitejas (DDUK) darbā, tās ietvaros sniedzot atbalstu kvalificētu elektroniskās identifikācijas pakalpojumu sniedzēju un uzticamu sertifikācijas pakalpojumu sniedzēju uzraudzībā, kā arī veic Latvijas uzticamības saraksta (LV TSL – LV trust list) uzturēšanu.

Turpinās CERT.LV eksperte iesaiste topošās eIDAS 2.0 regulas projekta izskatīšanā, kā arī tā ietekmes uz DDUK plānotajiem darbiem novērtēšanā, tostarp iesaistoties digitālās identitātes maka ieviešanas darba grupas sanāksmēs.

5.3. Izglītība un jauniešu kiberprasmju uzlabošana

CERT.LV piedalās Saldus tehnikuma organizētajā darba grupā kvalifikācijas "Kiberdrošības tehniķis" standarta izstrādei, daloties ar savu pieredzi un sniedzot plašāku redzējumu par speciālistiem nepieciešamajām zināšanām, iemaņām un prasmēm, lai nodrošinātu, ka kvalifikācijas ieguvēji jau mācību laikā apgūst darbam nepieciešamās zināšanas un kļūst par augsti novērtētiem speciālistiem.

Latvijas kiberdrošības izaicinājums jauniešiem

Sadarbībā ar Aizsardzības ministrijas ES kiberdrošības jautājumu nodaļu, CERT.LV deva savu ieguldījumu, strādājot pie Eiropas mēroga kiberdrošības sacensību jauniešiem "Eiropas kiberdrošības izaicinājums 2024" (ECSC) nacionālās atlases nodrošināšanai nepieciešamās infrastruktūras un uzdevumu kopas sagatavošanas darbiem. 2024. gadā sacensības tika rīkotas pirmo reizi.

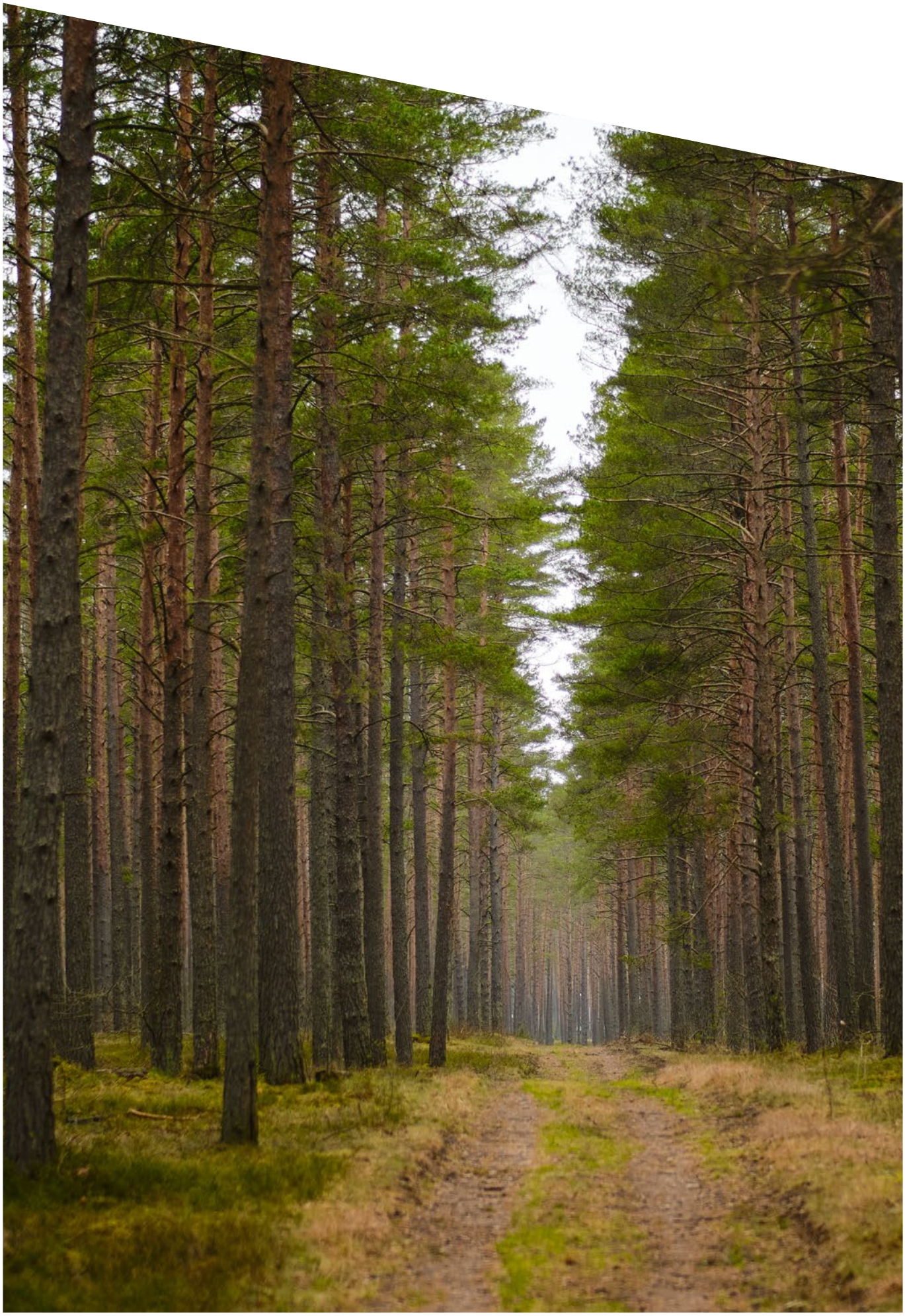
Latvijas kiberdrošības izaicinājumu organizēja Aizsardzības ministrija sadarbībā ar CERT.LV, Latvijas Universitāti un Zemessardzes Kiberaizsardzības vienību. Izaicinājumu atbalsta Eiropas Kiberdrošības kompetenču centra Latvijas Nacionālais koordinācijas centrs (NCC-LV) un Eiropas Kiberdrošības kompetenču centrs, un to līdzfinansē ES.

Sacensības norisinājās trīs kārtās no 8. marta līdz 8. maijam un pulcēja 469 jauniešus vecumā no 14 līdz 24 gadiem no 100 dažādām izglītības iestādēm. Piedaloties sacensībās, jauniešiem bija iespēja pārbaudīt un pielietot praksē iegūtās zināšanas un prasmes kiberdrošības vai kiberaizsardzības jomās.

5. maijā Aizsardzības ministrijas valsts sekretāra vietnieks Rolands Heniņš un CERT.LV vadītāja Baiba Kaškina pasniedza apbalvojumus 84 talantīgākajiem Latvijas jauniešiem par sasniegumiem valsts mēroga kiberdrošības sacensībās "Nacionālais kiberdrošības izaicinājums".

Sacensību dalībniekiem ar lielāko punktu skaitu kopvērtējumā būs iespēja kļūt par daļu no Latvijas nacionālās izlases dalībai starptautiskās kiberdrošības sacensībās "Eiropas kiberdrošības izaicinājums", kas norisināsies 2024. gadā no 8. līdz 11. oktobrim Turīnā, Itālijā.

"Nacionālais kiberdrošības izaicinājums" apbalvošanas ceremonijas dalībnieki



6. Starptautiskā sadarbība

CERT.LV turpina pārstāvēt Latvijas intereses un stiprināt sadarbību ar citu valstu kiberdrošības incidentu novēršanas vienībām un starptautiskām organizācijām. Pārskata periodā CERT.LV darbinieki sniedza savu redzējumu un ieguldījumu dažādās darba grupās, daloties ar pieredzi un labo praksi, sniedzot konsultācijas un atbalstu, kā arī uzstājās ar prezentācijām starptautiskās konferencēs un semināros. Turpinājās arī darbinieku jaunu prasmju apgūšana un kvalifikācijas celšana, piedaloties starptautiskās mācībās.

Sadarbība ar CSIRTs tīklu, ENISA, Eiropas Savienības institūcijām un NATO

CERT.LV regulāri piedalās NIS (Tīklu un informācijas drošības) direktīvas *CSIRTs Network* (CSIRT tīkls) sadarbības tīkla sanāksmēs. *CSIRTs Network* darbu koordinē ENISA – ES Kiberdrošības aģentūra, kas sniedz ieguldījumu ES politikā kiberdrošības jomā.

Pārskata periodā CERT.LV piedalījās *CSIRTs Network* darba grupā *Maturity*, kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.

CSIRTs tīkls (CSIRTs Network) – Eiropas Savienības (ES) dalībvalstu kiberdrošības incidentu novēršanas institūciju tīkls nodrošina sadarbību starp kiberdrošības incidentu novēršanas vienībām ES. Sanāksmes notiek 3 reizes gadā, tās organizē konkrētajā brīdī ES Padomes prezidējošā valsts sadarbībā ar ENISA. Reizi gadā sanāksme notiek arī apvienotās sesijās kopā ar NIS direktīvas Sadarbības grupu un *CyCLONe*.

22. maijā Gentā, Beļģijā norisinājās *CSIRT Network* sanāksmē, kurā piedalījās CERT.LV pārstāvji, tostarp Kiberdrošības eksperts Aleksejs Veremejenko dalījās ar Latvijas pieredzes stāstu pie "Graphoscope" izstrādes, attīstīšanas un pilnveidošanas. "Graphoscope" kalpos analītiķiem kā noderīgs rīks, lai korelētu datus no dažādiem datu avotiem un parādītu tos vizuālā formā.

CERT.LV speciālisti turpina aktīvi līdzdarboties ENISA organizētajās darba grupās:

- ***Coordinated Vulnerability Disclosure (CVD) Task Force*** – norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas politikas vadlīniju veidošanas;
- ***EU Cybersecurity Index*** – tiek izstrādāta kiberdrošības indeksa vērtības aprēķina metodoloģija dalībvalstu kiberdrošības novērtēšanai; turpinās darbs pie *EU Cybersecurity Index* platformas attīstīšanas;
- ***CSIRT Services Framework*** – tika turpināts darbs, izstrādājot vienotu ietvaru CERT komandu dalībnieku lomām, kompetencēm un prasmēm. Pārskata periodā tika veikta CERT komandu tipu noteikšanas metodoloģijas izstrāde, kas sekmētu veicamajiem uzdevumiem nepieciešamo lomu un kompetenču identificēšanu.

***CSIRT Network Situation Update* sanāksmes:** pārskata periodā turpinājās regulāra dalība sanāksmēs, kuru mērķis ir veikt informācijas apmaiņu par aktuālo kibertelpā starp CSIRT tīkla biedriem.

Eiropas Komisijas EHDS (*European Health Data Space*) regulas darba grupa: CERT.LV speciālisti sniedza savu ieguldījumu darba grupā, kuras mērķis ir veicināt pacientu elektronisko datu pieejamību un iesaistīto pušu sadarbību Eiropas līmenī. Pārskata periodā darba grupa izvērtēja regulas saikni ar Mākslīgā intelekta aktu, Datu pārvaldības aktu un Vispārīgo datu aizsardzības regulu.

Regulāra CERT.LV ekspertu dalība Eiropas Kiberdrošības produktu sertifikācijas grupas ECCG *(European Cybersecurity Certification Group)* sanāksmēs, tajā skaitā sanāksmēs, pārstāvot Latvijas intereses un sniedzot CERT.LV redzējumu par problemātiskiem jautājumiem, kas skar ES mākoņpakalpojumu sertificēšanas shēmas (EUCS) tālāku virzību ES valstīs, kā arī par citiem IKT produktu kiberdrošības sertifikācijas ieviešanas jautājumiem ES valstīs.

ENISA organizētās mācības "Cyber Europe 2024": Šogad lielākās Eiropas kibermācības tiek rīkotas jau septīto reizi! Pārskata periodā mācības norisinājās no 19. līdz 20. jūnijam, risinot enerģētikas nozares noturības jautājumus

un izaicinot tūkstošiem dalībnieku, kas cieši saistīti ar kiberdrošību. Mācību dalībniekiem šogad bija jāreaģē gan uz tehniskiem izaicinājumiem (piemēram, tika analizēti tīkla faili, ļaunatūras, pikšķerēšanas e-pasti), gan ar krīzes vadības un sabiedrisko attiecību aspektiem.

"Cyber Europe" mācības, ko vada ENISA un organizē sadarbībā ar CERT.LV un daudziem citiem ES dalībniekiem, ir izveidotas, lai pārbaudītu mūsu gatavību pret kiberdraudiem daudzās nozarēs. Izmantojot aizraujošus scenārijus, ko iedvesmojuši reāli notikumi, kurus pilnībā izstrādājuši Eiropas kiberdrošības eksperti, šīs mācības ir reāla iespēja dalībniekiem risināt sarežģītas uzņēmējdarbības nepārtrauktības un krīzes vadības situācijas.

NATO CCDCoE organizētās mācības un konferences: Pārskata periodā CERT.LV piedalījās mācību "Locked Shields 2024" plānošanas ciklā, sniedzot atbalstu organizatoriem (*White Team*) stratēģiskās komunikācijas un mediju spēles incidentu rakstīšanā, spēles vides *Info Range* sagatavošanā, mācību izspēlē un izvērtēšanā. "Locked Shields" ir lielākās NATO kiberaizsardzības mācībās, kurās 2024. gadā piedalījās vairāki tūkstoši dalībnieku no vairāk nekā 40 valstīm.

CERT.LV eksperti piedalījās arī mācību galvenajā izspēlē apvienotajā Latvijas un NATO Komunikācijas un informācijas aģentūras komandā (NCIRC) laikā no 22. līdz 26. aprīlim, pildot uzdevumus gan tehniskajā komandā, īpaši draudu medību un situācijas izvērtēšanas jomā, gan stratēģiskās komunikācijas un juridiskajās komandās; Latvijas apvienotā komanda šogad mācībās ieguva 1. vietu.

Sadarbība FIRST ietvaros

Turpinājās regulāra dalība *FIRST Membership Committee* (Jauno biedru uzņemšanas komitejas) sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, kā arī SIM3 modeļa pielietošanu komandu sertifikācijas procesā.

FIRST ir kiberdrošības organizācija, kas apvieno CERT, CSIRT, PSIRT, SOC komandas un citus kiberdrošības profesionāļus no visas pasaules.

FIRST biedri ir no 107 valstīm.

CERT.LV vadītāja Baiba Kaškina, turpinot pildīt FIRST Jauno biedru uzņemšanas komitejas priekšsēdētājas pienākumus, piedalījās jauno biedru pieteikumu izskatīšanā, kā arī veicināja biedru uzņemšanas procesa pilnveidošanu. No 9. līdz 14. jūnijam Fukuokā, Japānā CERT.LV eksperti piedalījās 36. ikgadējajā FIRST konferencē "FIRSTCON24". Daloties pieredzē un veicinot apmaiņu ar labāko praksi Operacionālo tīklu drošības stiprināšanā, Rūdolfs Ķelle uzstājās ar prezentāciju *"From Laboratory to Grid: Advancing IACS Incident Response and Cyber Resilience"*. Savukārt CERT.LV vadītāja Baiba Kaškina uzstājās kā FIRST Jauno biedru uzņemšanas komitejas priekšsēdētāja konferences atklāšanas dienā, izskaidrojot jaunajiem dalībniekiem konferences norisi un procesus, dalības nosacījumus un citus organizatoriskos jautājumus.

Konferences ietvaros CERT.LV eksperts Bernhards Blumbergs uzstājās ar priekšlasījumu *"Distributed Web Mining Approach for Contextual Cyber Threat Intelligence Acquisition"*. Šis priekšlasījums balstīts pētījumā, ko B. Blumbergs veica Japānas starptautiskās pēcdoktorantūras stipendijas (JSPS) ietvaros.

Tāpat no 14. līdz 15. jūnijam Fukuokā, Japānā norisinājās arī Vispasaules nacionālo CERTu sanāksme, kurā CERT.LV kiberdrošības eksperti Armīns Palms un Rūdolfs Ķelle uzstājās ar prezentāciju par CERT.LV nodrošināto aktīvās aizsardzības pakalpojumu – DNS ugunsmūri, tā priekšrocībām un ieguvumiem lietotājam.

CERT.LV pārstāvji 36. ikgadējajā FIRST konferencē FIRSTCON24, Japānā

Sadarbība TF-CSIRT ietvaros

CERT.LV ir viena no 39 Eiropas TF-CSIRT/Trusted Introducer sertificētām komandām. Uz pārskata perioda beigām kopienā ir 561 komanda, kas apliecina CERT.LV komandas augsto brieduma un sagatavotības līmeni. Sertifikācijas uzturēšanai ik pēc trīs gadiem jāveic re-sertifikācijas process. 2022. gada 28. oktobrī, TF-CSIRT sanāksmē Viļņā, Lietuvā, tika paziņots, ka CERT.LV ir veiksmīgi re-sertificēta uz nākamajiem 3 gadiem (attiecīgi nākamais re-sertifikācijas process plānots 2025. gadā).

TF-CSIRT/Trusted Introducer ir Eiropas reģiona CERTu organizācija, kas apvieno incidentu reaģēšanas komandas no visiem sektoriem. Trusted Introducer (TI) serviss uztur uzticamu CERT vienību reģistru un veic vienību akreditāciju un sertifikāciju atbilstoši komandas demonstrētajam brieduma līmenim. CERT.LV ir sertificēta TI komanda kopš 01.09.2024.

Sertifikācijas pamatā ir SIM3: "Security Incident Management Maturity Model" pieeja, kas vērtē organizācijas briedumu, skatoties uz organizatoriskiem, cilvēkresursu, izmantoto tehnisko rīku un procesu parametriem un to pielietojumu kvalitatīvai organizācijas darbības nodrošināšanai, primāri vērtējot incidentu risināšanas procesa briedumu.

No 13. līdz 15. maijam Kopenhāgenā, Dānijā, norisinājās 71. ikgadējā TF-CSIRT sanāksme, kurā CERT.LV pārstāve Sanita Vītola dalījās ar Latvijas pieredzes stāstu par izveidoto Koordinētas ievainojamības ziņošanas platformu un tās panākumiem. Savukārt Kristiāna Mūze-Feldberga dalījās ar Latvijas pieredzes stāstu ikgadējās starptautiskās konferences "KiberŠahs" ("*CyberChess*") organizēšanā. Pasākuma ietvaros CERT.LV pārstāvji rīkoja CERTu Sabiedrisko attiecību speciālistu sanāksmi, kurā apsprieda krīzes komunikācijas plānu izstrādes un uzlabojumus, kas balstīti uz pēdējo gadu pieredzi, pārrunāja pieļautās kļūdas un ieguvumus, kā arī dalījās ar statistikas datiem par to, kā mainījusies sabiedrības uzvedība un kiberdrošības izpratne kopumā.

Pārskata periodā CERT.LV turpināja darbu vairākās TF-CSIRT darba grupās.

Projekta "Joint Threat Analysis Network" īstenošana

Atbilstoši līgumam ar Eiropas Komisiju Nr. INEA/CEF/ICT/A2020/2373165, kas tika apstiprināts un uzsākts 2021. gada 1. jūlijā 2020 CEF Telecom Call – Cybersecurity uzsaukumā, CERT.LV komanda pabeidza darbu pie projekta *"Joint Threat Analysis Network"* (turpmāk – JTAN projekts) īstenošanas līdz 2024. gada 30. jūnijam.

Kopējais JTAN projekta mērķis bija izveidot vienotu apdraudējumu analīzes tīklu, kas būtu atvērts Eiropas CSIRT sadarbības grupai, galveno uzmanību pievēršot tehnisko, operatīvo un stratēģisko draudu izlūkošanas informācijas apmaiņai un analīzei.

Projekta vadošais partneris ir Informācijas tehnoloģiju drošības incidentu novēršanas institūcija Polijā CERT.PL, kas darbojas institūta *Naukowa i Akademicka Sieć Komputerowa* (NASK) struktūrā. JTAN projektā piedalījās arī partneri no Austrijas, Francijas, Igaunijas, Luksemburgas, Rumānijas un Slovākijas.

Projekta ietvaros atbilstoši plānam tika pabeigti "Graphoscope" risinājuma izstrādes darbi.

Graphoscope rīks paredzēts, lai korelētu datus no dažādiem datu avotiem un parādītu tos vizuālā formā.

Galvenās "Graphoscope" priekšrocības ir šādas:

- atbalsts daudziem datu avotiem un vienkārša sistēmas uzstādīšana;
- tīmeklī bāzēta saskarne, kas nav atkarīga no iepriekš instalētām datubāzēm;
- nodrošinot elastīgus filtrus, saskarne atvieglo liela apjoma datu analīzi.

Pārskata periodā CERT.LV novirzīja papildu resursus projekta īstenošanai un veiksmīgai noslēgšanai. Notika dalība gan ikmēneša attālinātās JTAN projekta sanāksmēs, gan klātienes projekta noslēguma sanāksmē, kas notika Gentā, Beļģijā dienu pirms CSIRT Network sanāksmes.

Dalība citos dažādos starptautiskos pasākumos kiberdrošības jomā

- No 10. līdz 14. jūnijam Rennes, Francijā CERT.LV eksperte Kristīne Andersone piedalījās akadēmisko tīklu konferencē "TNC2024". K. Andersone pārstāvēja Latviju arī GEANT ģenerālajā asamblejā.
- No 20. līdz 21. jūnijam Tallinā, Igaunijā CERT.LV pārstāvji piedalījās CERT-EE organizētajā simpozijā "OctOb3rf3st 2024", kura ietvaros aktīvi iesaistījās arī CTF praktiskajās nodarbībās.
- Turpinās regulāra CERT.LV ekspertu piedalīšanās EU CyberNet projekta ikmēneša sanāksmēs. Projekta mērķis – stiprināt kiberdrošības ekspertīzi un attīstīt to ne tikai ES, bet arī ārpus tās robežām (www.eucybernet.eu). Dalība projektā sniedz iespēju CERT.LV ekspertiem iesaistīties dažādos projektos, stiprināt savas zināšanas un kapacitāti.
- CERT.LV turpina piedalīties Ziemeļvalstu un Baltijas valstu drošības operāciju centra (Nordic-Baltic SOC) izveides koordinācijas darbā.

7. Pārskats par LIA Drošāka interneta centra ziņojumu līnijas darbību

Latvijas Interneta asociācijas (LIA) Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.04.2024. līdz 30.06.2024. ir saņēmusi un izvērtējusi **11 874** ziņojumus. No tiem **11 553** ziņojuma saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, **36** gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, **21** ziņojumā konstatēta personas goda un cieņas aizskaršana, **6** ziņojumi saņemti par naida runu un **14** ziņojumos konstatēti vardarbīgi materiāli.

Par finanšu krāpšanas mēģinājumiem internetā saņemti **120** ziņojumi, **70** ziņojumu saturs nav bijis pretlikumīgs, **54** gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti **5 783** ziņojumi par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. **39** ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datubāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem **11 511** ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem visu ziņojumu saturs ir dzēsts no publiskas aprites internetā.

LIA Drošāka interneta centra ZL saņemtie ziņojumi no 01.04.2024. – 30.06.2024.

Ziņojumi	Apr-24	Maj-24	Jun-24	Q2
Erotisks/ pornogrāfisks saturs bez izvietotiem brīdinājumiem	0	31	5	**36**
Pedofilija/ mazgadīgo prostitūcija/ bērnu seksuālu izmantošanu saturoši materiāli	6	11 423	124	**11 553**
Vardarbīga rakstura materiāli	1	12	1	**14**
Cieņas/ goda aizskaršana	7	5	9	**21**
Naida kurināšana/ rasisms	4	1	1	**6**
Finanšu krāpniecība	49	31	40	**120**
Konsultācijas/ padomi	17	10	27	**54**
Citi	7	30	33	**70**
KOPĀ:	**91**	**11 543**	**240**	**11 874**

Ziņojumi nosūtīti Valsts policijai	1	5 695	87	**5783**
Ziņojumi nosūtīti INHOPE asociācijai	3	5	31	**39**
Kopā nosūtīti izskatīšanai	**4**	**5 700**	**118**	**5822**

8. Nākamajā ceturksnī plānotie pasākumi

Svarīgākie virzieni un pasākumi 2024. gada 3. ceturksnī

NKDL un NIS2 ieviešana: Turpinās sagatavošanās pasākumi, lai CERT.LV ir gatava sekmīgi turpināt darbu, kad 2024. gada 1. septembrī stāsies spēkā Nacionālās kiberdrošības likums (NKDL), kura mērķis ir stiprināt kiberdrošību Latvijā un ieviest pārskatītās Eiropas Savienības Tīklu un informācijas sistēmu drošības direktīvas (NIS2) prasības vienādi augsta kiberdrošības līmeņa panākšanai visā Eiropas Savienībā (ES).

Sekmējot Kiberdrošības pārvaldes reformas mērķu sasniegšanu, CERT.LV turpinās darbu pie jauno normatīvo aktu skaidrošanas, lai sniegtu atbalstu jauno prasību ieviešanā CERT.LV klientūrai, uz kuru attieksies jaunais NKDL. Tāpat tuvāko mēnešu laikā savas kompetences ietvaros CERT.LV atbalstīs Aizsardzības ministriju un citas iestādes, nodrošinot savu ekspertu piedalīšanos informatīvajos semināros par NKDL un NIS2 prasībām.

NKDL noteikts, ka no 2024. gada 1. septembra tiks izveidots Nacionālais kiberdrošības centrs, kas darbosies kā vienotais kontaktpunkts kiberdrošības jautājumos un veiks nacionālo kiberdrošības prasību ieviešanas pārraudzību, kā arī izstrādās nacionālās kiberdrošības rīcībpolitikas iniciatīvas. Nacionālā kiberdrošības centra funkcijas īstenos Aizsardzības ministrija sadarbībā ar CERT.LV. Līdz 1. septembrim plānota iekšējās un ārējās dokumentācijas pielāgošana un citu sagatavošanās pasākumu veikšana.

Pakalpojumu attīstība: CERT.LV turpinās attīstīt un popularizēt kiberdrošības pakalpojumus, tostarp, DNS ugunsmūri, pikšķerēšanas uzbrukumu simulācijas, koordinētu ievainojamību atklāšanas platformu cvd.lv, kiberaizsardzības stiprināšanai un drošības kāpināšanā gan valsts un pašvaldību iestāžu resursos, gan IKT kritiskajā infrastruktūrā. Tāpat turpinās mērķtiecīgi uzsāktās aktivitātes CERT.LV Drošības operāciju centra (SOC) attīstīšanā, it īpaši veicinot sadarbību ar būtisko un svarīgo pakalpojumu sniedzējiem.

CERT.LV turpina aktīvi uzraudzīt kibertelpu, risināt un koordinēt incidentus, informēt un izglītot sabiedrību, veicinot stratēģisku sadarbību valsts un starptautiskā mērogā.

Draudu medību operācijas: CERT.LV komandas mērķis ir turpināt stiprināt savu līderību draudu medību operāciju organizēšanā ES, veicinot stratēģisko sadarbību gan valsts, gan starptautiskā mērogā. Ciešā sadarbībā ar Kanādas Bruņoto spēku kiberpavēlniecību turpināsies draudu medību operācijas. Tās primāri vērstas Latvijai nozīmīgu IKT sistēmu noturības stiprināšanai, un sekundāri kopīgais darbs sniedz ieguldījumu NATO kolektīvajā kiberaizsardzībā.

Aizvien pieaugot Krievijas radīto kiberdraudu un kiberuzbrukumu intensitātei un apjomam Latvijas sabiedroto kibertelpā, CERT.LV kopā ar alianses partneriem turpinās veidot izpratni par radītajiem riskiem, veicināt informācijas apmaiņu un gatavību uz tiem atbilstoši reaģēt.

Tuvākajos mēnešos turpināsies gan jau iesāktās draudu medību operācijas, gan tiks uzsāktas jaunas operācijas vairāku publiskā sektora iestāžu infrastruktūrā. Tiks turpināts iesāktais plānošanas un izstrādes darbs šogad oktobrī gaidāmajām draudu medību semināram. Tas tiks īstenots sadarbībā ar Kanādas bruņoto spēku kiberpavēlniecību un NATO CCDCOE.

Apmācības un izglītojošie pasākumi: 2024. gada 3. ceturksnī galvenā uzmanība tiks pievērsta nacionālo kiberdrošības mācību “Medus Pods 2025” plānošanai, tiekoties ar konkrētiem infrastruktūras turētājiem un mācību auditoriju. Tāpat turpināsies darbs pie mācību “CYBER EUROPE” izvērtēšanas, kā arī pēc nepieciešamības tiks sniegts atbalsts mācību “NAMEJS” plānošanā un izspēlē.

Plānota dalība vairākos kiberkopienas pasākumos, tajā skaitā:

- **6. jūlijā** ikgadējā sarunu festivāla "Lampa" ietvaros Aizsardzības ministrijas organizētājā diskusijā "Vai esam gatavi kiberkaram?" piedalīsies CERT.LV eksperts Kārlis Svilans.
- **8. jūlijā** EIT Digital Summer School "Cyber Security – Agile Methology for Developing New Solutions" CERT.LV eksperte Dana Ludviga uzstāsies ar prezentāciju par būtiskākiem kiberdrošības draudiem un to izaicinājumiem "Cybersecurity Trends, Threats and Solutions". Savukārt 12. jūlijā pasākuma ietvaros CERT.LV ekspertes Dana Ludviga un Daina Ozoliņa vasaras skolas dalībniekiem vadīs kiberdrošības incidenta izmeklēšanas spēli.
- **19. septembrī** CERT.LV eksperti Dana Ludviga un Gints Mālkalnietis uzstāsies SIA "Baltijas Informācijas Tehnoloģijas" rīkotajā "Tehnoloģiju ceturtdienā" ar prezentāciju par drošas uzņēmuma IT vides izveidi un uzturēšanu.
- **23.-27. septembrī** CERT.LV eksperti uzstāsties ar prezentācijām par būtiskiem aspektiem kiberhigiēnas stiprināšanā un labās prakses ieteikumiem Valsts policijas koledžas pasākumā "Starptautiskā profesionāļu nedēļa".

Starptautiskā sadarbība: CERT.LV eksperti turpina pārstāvēt Latvijas intereses un stiprināt sadarbību ar citu valstu kiberincidentu novēršanas vienībām, starptautiskām organizācijām un partneriem Eiroatlantiskās telpas drošībai un starptautiskajai drošībai kopumā, sniedzot konsultācijas un atbalstu, kā arī mērķtiecīgi uzrunājot sabiedrību starptautiskās konferencēs.

- **9. jūlijā** Ņujorkā, ASV notiks atvērtās darba grupas (OEWG) 8. pamatsesijas papildpasākums *"Building Cyber Resilience Through Effective Governance and Stakeholder Engagement"*, kas tiek organizēts sadarbībā ar pārstāvjiem no Bahreinas, Kolumbijas, kā arī "Microsoft" un "Cisco". Šajā pasākumā CERT.LV vadītāja Baiba Kaškina dalīsies pieredzē par izaicinājumiem un iespējām, izstrādājot valsts kiberdrošības pārvaldības modeļus ar iekļaujošu pieeju ieinteresētajām pusēm, kā arī par uzticībā balstītām publiskā un privātā sektora sadarbības iniciatīvām un jaunu sadarbības projektu veidošanu. Dalīšanās pieredzē un redzējumā par risinājumiem veicinās OEWG mērķu sasniegšanu, sekmējot labu kiberdrošības pārvaldību plašākā ANO dalībvalstu lokā un veidojot noturīgāku starptautisko kiberdrošības ekosistēmu.
- **12.-13. septembrī** CERT.LV vadītāja Baiba Kaškina piedalīsies nozīmīgā konferencē "Nordic Baltic Security Summit" Tallinā, Igaunijā. Forumā tiks apspriesta izglītības un sabiedrības informētības loma kibernoturības stiprināšanā. Paneļdiskusijā *"The Role of Education and Social Awareness in Building Resilient Cyber Security"* B. Kaškina dalīsies ar CERT.LV redzējumu par stratēģijām un labākajām praksēm kibernoturības stiprināšanai.
  Plašāk: **https://cybers.eu/en/security-summit**
- **23.-24. septembrim** Budapeštā, Ungārijā norisināsies 24. CSIRT Network sanāksme, kurā, kā ierasts, plānota arī CERT.LV pārstāvība, lai nodrošinātu sekmīgu informācijas apmaiņu un ciešāku sadarbību ar ES kiberincidentu novēršanas komandām.
- **25.-27. septembrī** Prāgā, Čehijā norisināsies TF-CSIRT sanāksme, kuras ietvaros CERT.LV eksperti Dana Ludviga un Egīls Stūrmanis plāno uzstāties par jaunākajām aktualitātēm un notikumiem kiberdrošības jomā.

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, kā arī organizēt informatīvus un izglītojošus pasākumus gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan citiem interesentiem.

Saziņa ar CERT.LV:

Tālrunis: +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