CERT.LV DARBĪBAS PĀRSKATS

C3
2024

CERT.LV
Kiberincidentu novēršanas institūcija

Latvijas Universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Kopsavilkums

Kopsavilkums 4

1. Kibertelpas drošības apdraudējumi: statistika un tendences 7

2. TOP kiberincidenti un apdraudējumi: atbalsts un ieteikumi to novēršanā 12

2.1. Krāpšana 12
2.2. Pakalpojuma pieejamība 16
2.3. Ievainojamības un konfigurācijas nepilnības 18
2.4. Ļaundabīgs kods 22
2.5. Ielaušanās mēģinājumi 24
2.6. Kompromitētas iekārtas un datu noplūdes 26

3. Kiberapdraudējumu prevencija 28

3.1. DNS ugunsmūris: aktīvā aizsardzība 28
3.2. Sensoru tīkls 29
3.3. Drošības operāciju centrs (SOC) 29
3.4. Pasākumi incidentu novēršanai 30
3.5. Koordinēta ievainojamību atklāšana (CVD) 31

4. Komunikācija ar sabiedrību 32

4.1. Apmācības un izglītojošie pasākumi 32
4.2. Sabiedrības informēšana un kiberhigiēnas veicināšana 34

5. Stratēģiskā sadarbība Latvijā 35

5.1. Atbalsts kibernoziedzības novēršanā un apkarošanā 36
5.2. Sadarbība kiberaizsardzības mācību organizēšanā 39
5.3. Izglītība un jauniešu kiberprasmju uzlabošana 40

6. Starptautiskā sadarbība 41

7. Pārskats par LIA Drošāka interneta centra ziņojumu līnijas darbību 45

8. Nākamajā ceturksnī plānotie pasākumi 46

Kopsavilkums

Ģeopolitiskie un ideoloģiskie konflikti turpina būt spēcīgs kiberuzbrukumu virzītājspēks. Kopš Krievijas iebrukuma Ukrainā, kiberapdraudējumu līmenis Latvijā ir būtiski pieaudzis. Latvijas atbalsts Ukrainai un Krievijas agresijas turpināšanās uztur augstu kiberapdraudējumu dinamiku, kas uzsver nepieciešamību pēc pastāvīgas modrības un uzlabotiem aizsardzības risinājumiem.

Salīdzinot ar šo pašu periodu pirms gada, lielākais pieaugums ir šādos apdraudējuma veidos:

- kompromitētas iekārtas (+267%),
- krāpšana (+183%),
- pakalpojuma pieejamība (+158%),
- ļaundabīgs kods (+73%).

Vēsturiski augstākais kiberapdraudējumu līmenis

405 955 apdraudētas unikālas IP adreses ir līdz šim augstākais rādītājs, kas liecina par ievērojamu kiberapdraudējumu pieaugumu un aktivitāti. 2024. gada 3. ceturksnī reģistrēto ziņojumu skaits ir pieaudzis par 4,4% salīdzinājumā ar iepriekšējo ceturksni un par 21% salīdzinājumā ar attiecīgo periodu pērn. Latvija demonstrē augstu kibernoturības līmeni.

Tomēr situācija Latvijas kibertelpā turpina saglabāties stabila. Kopumā fiksētie kiberuzbrukumi nav radījuši būtisku ietekmi uz sabiedrību, tās drošību un svarīgajiem pakalpojumiem, kas norāda uz efektīvu aizsardzības pasākumu esamību.

Ņemot vērā kiberapdraudējumu plašo spektru un nepārtraukto attīstību, efektīvākais veids to identificēšanai, novēršanai un seku mazināšanai ir labi koordinēta publiskā un privātā sektora sadarbība un proaktīva kibernoturības stiprināšana, kas Latvijā jau tiek īstenota un pilnveidota.

Kiberdrošības apdraudējumi pēc svarīguma un ietekmes

Pārskata periodā fiksēti 3 augstas nozīmes kiberuzbrukumi valsts iestādēs, taču tie neradīja paliekošas sekas uz sabiedrību. Nozīmīgi apdraudējumi ar plašu ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 0,23% jeb 926 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem. Tas ir 13 reizes vairāk nekā 2. ceturksnī un 27 reizes vairāk nekā pirms gada. Būtiski apdraudējumi ar vidēju ietekmi veido 0,61% jeb 2466 apdraudētas unikālas IP adreses. Pieaugums pret iepriekšējo ceturksni ir 2%, bet salīdzinājumā ar pagājušā gada 3. ceturksni pieaugums ir 9%.

Šādas tendences norāda, ka jāturpina pilnveidot kiberdrošības uzraudzība un prevencija, tostarp jāveicina automatizētas drošības telemetrijas apstrādes izmantošana 24/7 režīmā, lai efektīvi atbalstītu publiskā sektora tehniskos un cilvēkresursus pret pieaugošajiem kiberdraudiem.

Būtiskāko kiberapdraudējumu dinamika un tendences

Politiski motivēti pakalpojumatteices uzbrukumi: Pieaugums par 210% salīdzinājumā ar iepriekšējo ceturksni un par 158% salīdzinājumā ar pagājušā gada 3. ceturksni liecina par ievērojamu pakalpojumatteices uzbrukumu skaita un intensitātes pieaugumu. Pret Latviju tiek turpināti DDoS uzbrukumi, vēršot tos pret valsts iestādēm, IKT kritisko infrastruktūru un pakalpojumu sniedzējiem. No Krievijas puses atbalstīto kiberuzbrukumu mērķis Latvijā primāri ir mēģināt mazināt atbalstu Ukrainai un valsts drošības stiprināšanai, provocējot ideoloģisko vērtību sadursmes, kuras izraisījis ģeopolitiskās vides konflikts starp Ukrainu un Krieviju.

Sociālās inženierijas balstīti krāpniecības apmēri pieaug: CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ir palielinājies par 62% salīdzinājumā ar iepriekšējo ceturksni un par 183% salīdzinājumā ar pagājušā gada 3. ceturksni. Manipulatīvie pasākumi datu izgūšanai un integritātes kompromitēšanai kļūst arvien izsmalcinātāki. Visizplatītākās shēmas ir pikšķerēšana, smikšķerēšana, mērķēta pikšķerēšana, e-pasta sarakstes kompromitēšana, mānīšanās zvani,

kas iekļauj cilvēka balss atdarināšanu, viltus vietnes un profili sociālajos tīklos viltus loteriju un aptauju izplatīšanai u.c. Pieaug latviešu valodā veiktu krāpšanu aktivitāte. Ziņas tiek sūtītas gan valsts iestāžu, gan kurjeru un finanšu pakalpojumu sniedzēju vārdā. Nereti cilvēki tiek apkrāpti, jo neuzmanība un nepietiekama kiberhigiēnas prakse palielina krāpniecības riskus. Galalietotāji tiek aicināti ieviest divfaktoru autentifikāciju.

Ļaundabīga koda izplatība joprojām apdraud datu integritāti: Lai gan neliels samazinājums salīdzinājumā ar iepriekšējo ceturksni varētu norādīt uz efektīvākiem aizsardzības mehānismiem, kopējā tendence ir augoša. Salīdzinot ar 2023. gada 3. ceturksni, ļaundabīga koda izplatība pieaugusi par 73%, kas liecina par ilgtermiņa pieaugumu. Pikšķerēšanas e-pasta vēstulēs biežāk novēroti kaitīgi pielikumi ar .html paplašinājumu. Izspiedējvīrusu uzbrukumi uzņēmumiem kļūst arvien pārdrošāki un finansiāli graujošāki. Pārskata periodā ražošanas uzņēmums "Amber Beverages Group" piedzīvoja šifrējošā izspiedējvīrusa uzbrukumu, kura rezultātā notika uzņēmuma datu noplūde.

Pieaug iekārtu kompromitēšanas riski: Pieaugums par 267% liecina, ka pieaug kontu un tīmekļvietņu kompromitēšanas riski. Turpinās piegādes ķēžu kompromitēšanas gadījumi starpniekpakalpojumu sniedzējiem ārpus Latvijas, bet tādējādi tiek ietekmēts TV kanāla saturs Latvijā. Atkārtoti novērots gadījums, kad Krievijas vai ar to saistīta haktīvistu grupa uz dažām minūtēm aizstāja "Balticom" IPTV pārraidīto saturu ar savu video, kas slavina Krievijas imperiālismu.

Paplašinās CERT.LV pakalpojumu apjoms publiskā un privātā sektora organizācijām

No 2024. gada 1. septembra, stājoties spēkā Nacionālās kiberdrošības likumam (NKDL), kiberincidentu novēršanas institūcija CERT.LV kļūst par daļu no Nacionālā kiberdrošības centra. NKDL paplašina likuma tvērumu uz plašāku uzņēmumu loku, tādējādi palielinot CERT.LV klientu skaitu, kam jāievēro jaunās prasības, bet kas var arī saņemt CERT.LV piedāvātos pakalpojumus. Kā galvenā operacionālās kiberdrošības organizācija Latvijā CERT.LV piedāvā plašu pakalpojumu klāstu kibernoturības stiprināšanai.

DNS ugunsmūra efektivitāte: 3. ceturksnī DNS ugunsmūra lietotāji tika pasargāti no kaitīgu vietņu apmeklēšanas vairāk nekā 103 414 reizes, pārvirzot galalietotāju uz CERT.LV brīdinājuma vietni. Ar NKDL stāšanos spēkā elektronisko sakaru pakalpojumu sniedzējiem obligāti jāizmanto CERT.LV DNS ugunsmūris, kas automātiski bloķē kaitīgus interneta resursus, tā tagad centralizēti tiek pasargāti visi Latvijas interneta lietotāji.

Agrās brīdināšanas sistēmu (ABS) efektivitāte: 3. ceturksnī ABS ģenerēto brīdinājumu skaits valsts, pašvaldību un IKT kritiskās infrastruktūras iestādēs kopskaitā bija aptuveni 1,83 miljardi – tas ir par 26% vairāk nekā 2. ceturksnī. Šāda pieauguma iemesli galvenokārt bija ar plaša mēroga pikšķerēšanām un datorvīrusiem saistīti brīdinājumi.

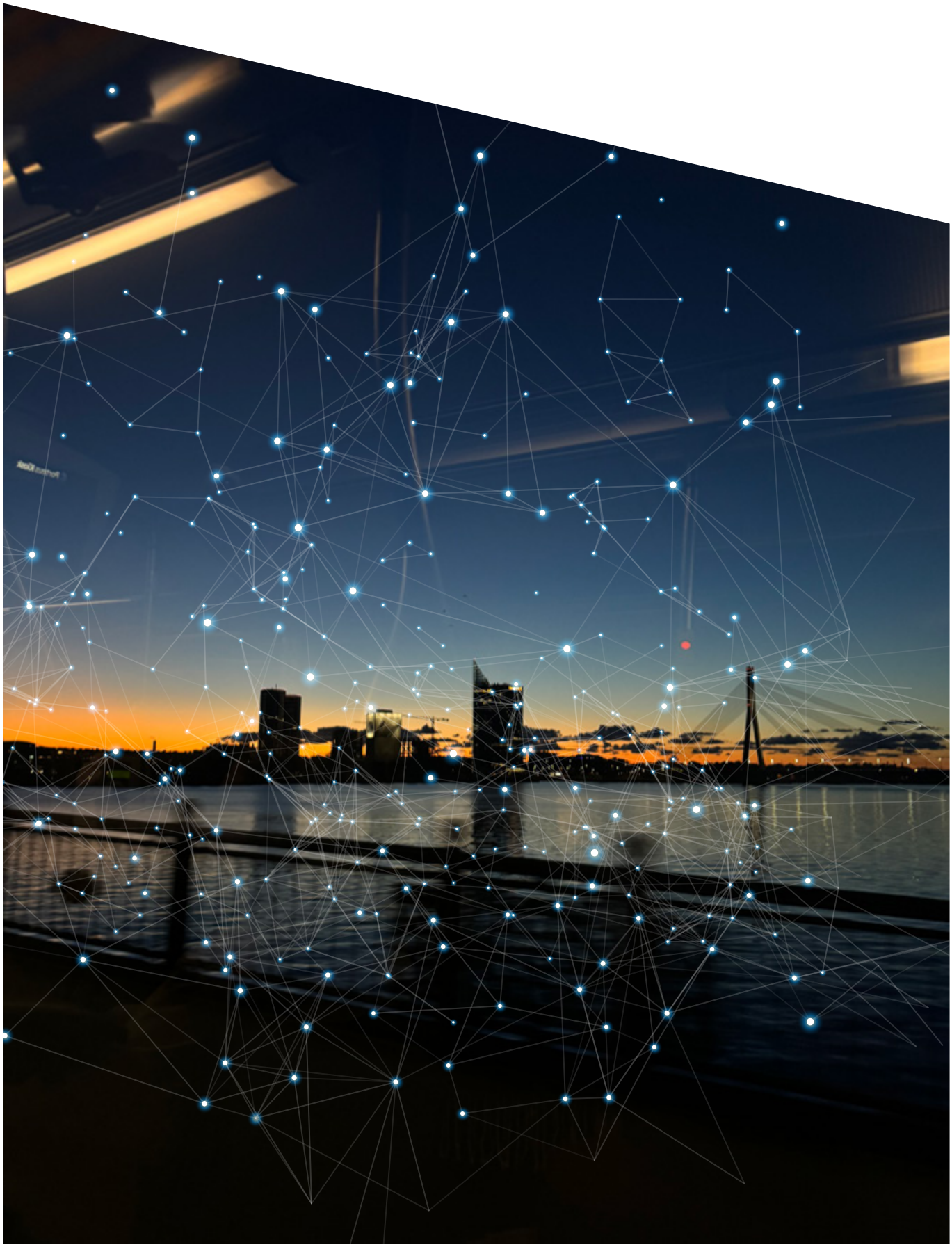
Drošības operāciju centra (SOC) attīstība: Turpinās mērķtiecīga SOC attīstība un jaunu klientu piesaiste. Pārskata perioda beigās SOC uzraudzīja 1 774 iekārtas klientu infrastruktūrā, reģistrējot vairāk nekā 46 000 drošības telemetrijas trauksmes ziņojumu, no kuriem 104 bija kritiski. Lielāko daļu veidoja zema līmeņa trauksmes ziņojumi (vairāk nekā 24 000).

Draudu medību operācijas: CERT.LV draudu medību operāciju analīze liecina, ka līdz šim veiktajās draudu medībās, aptuveni 25% jeb 8 organizāciju iekārtās tika identificēta ārvalstu APT klātbūtne, tostarp Krievijas un Ķīnas atbalstītu politiski motivētu un citu komerciāli motivētu kiberuzbrucēju klātbūtne, kas veiksmīgi neitralizēta. Atklāti arī citi būtiski apdraudējumi, kurus mērķa organizācijām, pateicoties saņemtajām atskaitēm pēc draudu medību noslēgšanās, bija iespēja novērst, pieņemot datos balstītus lēmumus.

Drošības testi: CERT.LV speciālisti, veicot 14 liela apjoma IT drošības testus, kā arī kiberapdraudējumu un pikšķerēšanas uzbrukumu simulācijas, atklāja un novērsa vairākas būtiskas ievainojamības kritiskās infrastruktūras un pakalpojumu nodrošināšanas organizācijās, kā arī trenēja šo organizāciju darbinieku kiberhigiēnas prasmes.

Koordinēta ievainojamību atklāšana (CVD): Turpinās CVD platformas attīstīšana. 3. ceturksnī drošības pētnieku skaits pieauga par 5%, ievainojamību ziņojumu skaits par 15%.

Apmācības un izglītojošie pasākumi: Pārskata periodā CERT.LV īstenoja 17 izglītojošus pasākumus kiberdrošības jomā, apmācot 7 787 dalībniekus, tā veicinot galalietotāju un organizāciju zināšanas par to, kā nodrošināt savu datu un sistēmu drošību.



1. Kibertelpas drošības apdraudējumi: statistika un tendences

Ģeopolitiskie un ideoloģiskie konflikti joprojām ir spēcīgs kiberuzbrukumu virzītājspēks. Kopš Krievijas plašā iebrukuma Ukrainā, kiberapdraudējumu līmenis Latvijā ir būtiski pieaudzis. Turpinoties Krievijas agresijai Ukrainā, kā arī turpinoties Latvijas atbalstam Ukrainai, sniedzot militāro un cita veida palīdzību, kiberapdraudējumu turpmākās attīstības dinamika saglabājas augsta, kas uzsver nepieciešamību pēc pastāvīgas modrības un uzlabotiem aizsardzības risinājumiem. Fiksētie kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību, un tas norāda uz efektīvu aizsardzības pasākumu esamību.

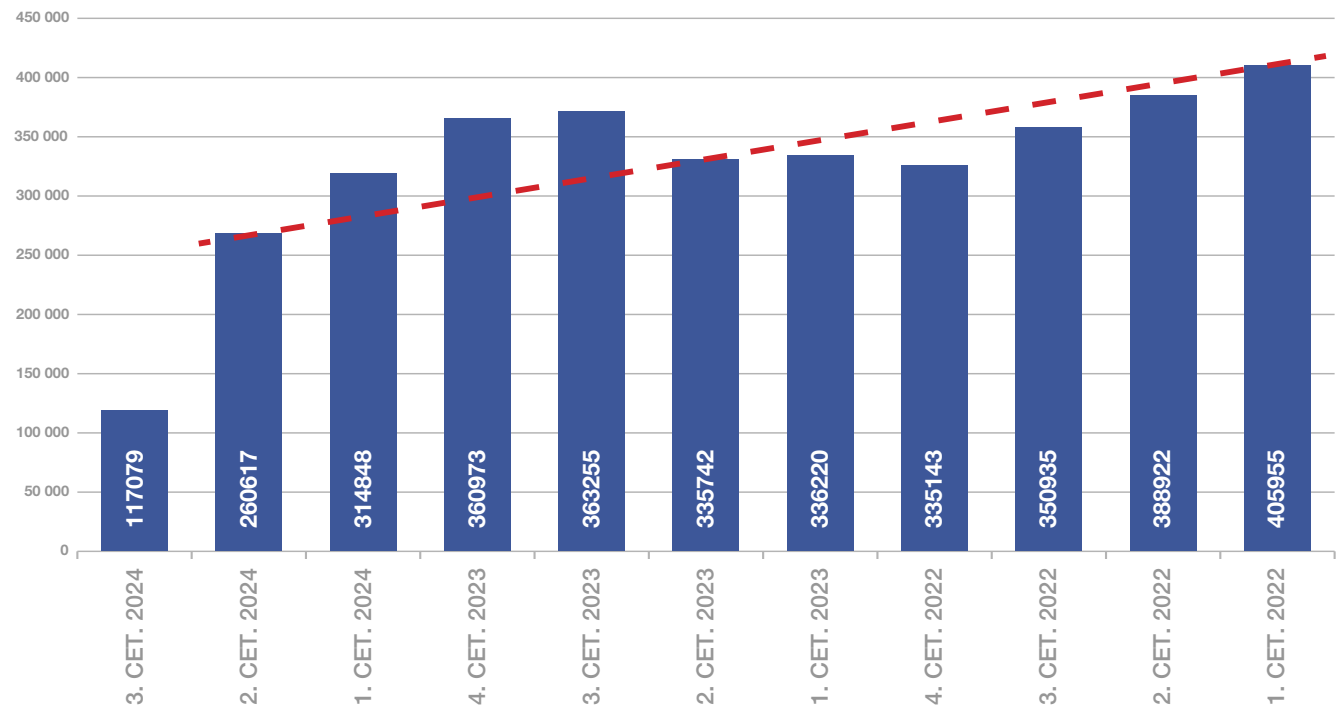
Kopš 2022. gada sākuma publiskā un privātā sektora organizācijas biežāk ziņo par incidentiem un ievainojamībām, kā arī biežāk lūdz CERT.LV atbalstu, kas liecina par pieaugošu uzticības līmeni starp publiskā un privātā sektora organizācijām.

Vēsturiski augstākais apdraudējumu līmenis

405 955 apdraudētas unikālas IP adreses ir līdz šim augstākais rādītājs, kas liecina par ievērojamu kiberapdraudējumu pieaugumu.

3. ceturksnī reģistrēto ziņojumu skaits ir pieaudzis par 4,4% salīdzinājumā ar iepriekšējo ceturksni un par 21% salīdzinājumā ar 2023. gada attiecīgo periodu, kas norāda uz pastāvīgu kiberapdraudējumu aktivitāti. Latvija demonstrē augstu kibernoturības līmeni.

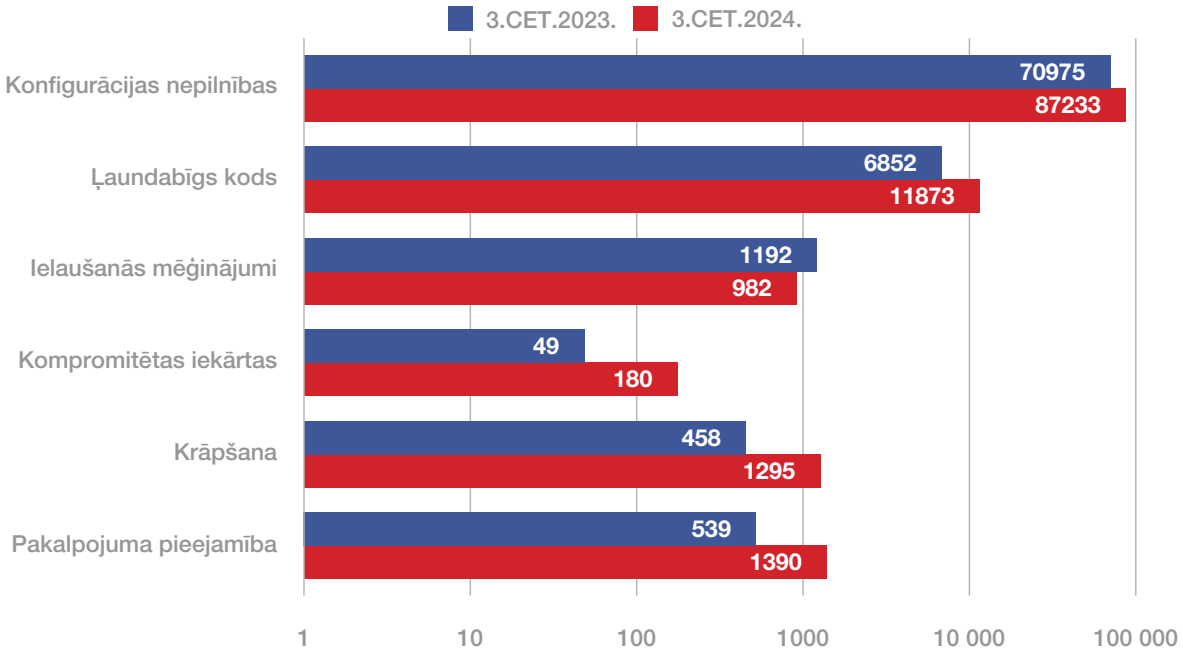
Apdraudējumu sadalījums pa ceturkšņiem



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

Kā redzams 2. attēlā, 2024. gada 3. ceturksnī izplatītākie apdraudējuma veidi: konfigurācijas nepilnības, ļaundabīgs kods, pakalpojuma pieejamība un krāpšana.

Apdraudējumu sadalījums pa ceturkšņiem



2. attēls. Apdraudēto unikālo IP adrešu skaita salīdzinājums 2023. un 2024. gada 3. ceturksnī pēc apdraudējuma veida.

*Grafikā nav iekļautas IP adreses ar apdraudējumu veidu "Cits", "Informācijas drošība", "Kaitīgs saturs", "Informācijas vākšana".

Salīdzinot ar šo pašu periodu pirms gada, pārskata periodā samazinājies ir tikai ielaušanās mēģinājumu skaits, savukārt lielākais pieaugums ir šādos apdraudējuma veidos:

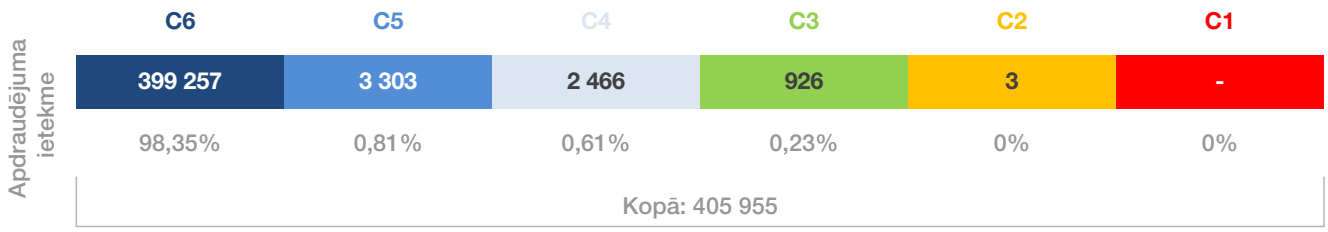
- kompromitētas iekārtas (+267%),
- krāpšana (+183%),
- pakalpojuma pieejamība (+158%),
- ļaundabīgs kods (+73%).

Apdraudētās unikālās IP adreses pēc svarīguma un ietekmes

Pilnvērtīgākam kiberdrošības situācijas novērtējumam CERT.LV izmanto Apvienotās Karalistes Nacionālā kiberdrošības centra izstrādāto apdraudējumu matricas metodoloģiju. Apdraudējumi tiek klasificēti no zemākās (C6) līdz augstākajai (C1) kategorijai, balstoties uz trim kritērijiem:

- **skartās iestādes/uzņēmuma/gala lietotāja nozīmīgumu,**
- **apdraudējuma ietekmes plašumu un**
- **radītajām sekām.**

Šie trīs kritēriji nosaka to, kāda svarīguma kategorija attiecīgajam apdraudējumam tiek piešķirta (C6-C1). Apvienojot visus faktorus un izmantojot krāsas, apdraudējumi iedalīti 6 kategorijās:

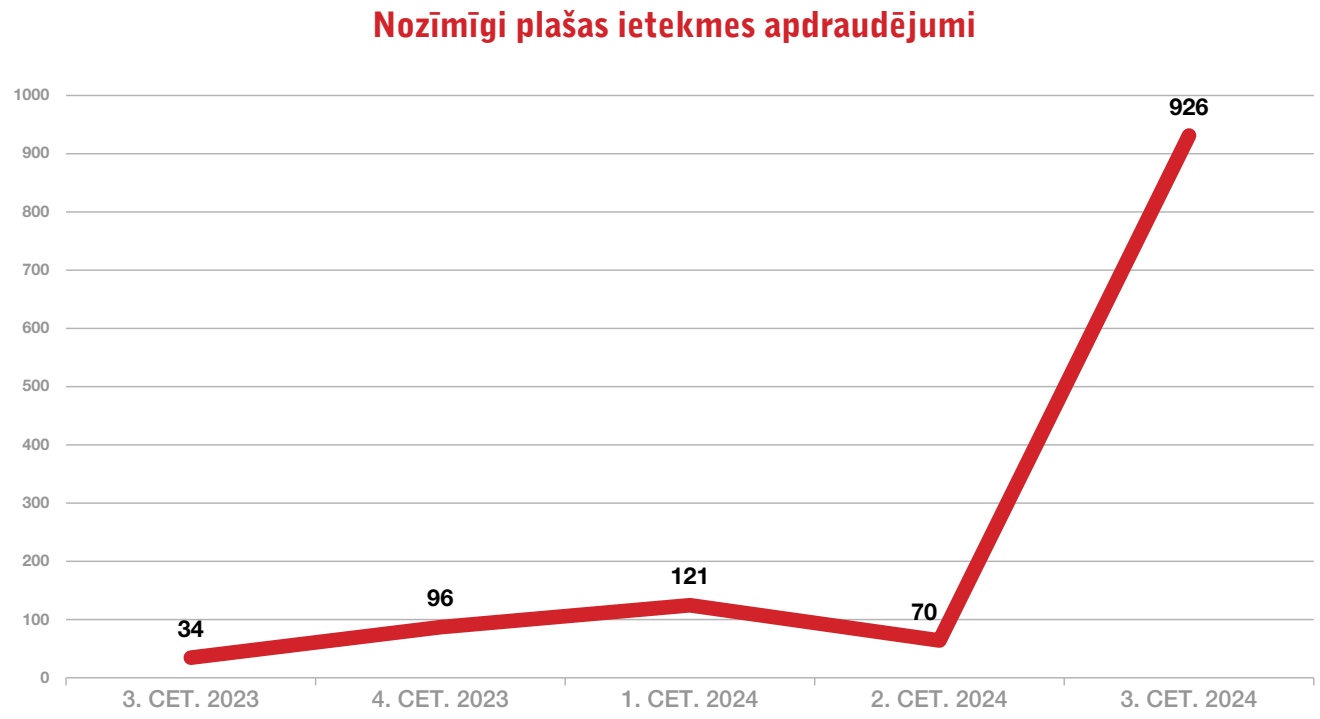


3. attēls. 3. ceturksnī apdraudēto unikālo IP adrešu sadalījums kategorijās pēc apdraudējuma ietekmes

Pārskata periodā C1 kategorijas jeb nacionāla līmeņa apdraudējumi nav fiksēti.

C2 kategorijā, kas ietver augstas nozīmes apdraudējumus, tika reģistrētas 3 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem. Tas ir vairāk nekā pagājušajā ceturksnī un pērn tajā pašā periodā. Locky un Cryptolocker ļaunatūras reģistrētas kāda elektronisko sakaru komersanta klientu tīklā, taču tas nav radījis būtisku vai paliekošu ietekmi uz sabiedrību.

C3 jeb nozīmīgi apdraudējumi ar plašu ietekmi uz komerciālo sektoru, valsts un pašvaldību iestādēm veido 0,23% jeb 926 apdraudētas unikālas IP adreses no visiem kategorizētajiem apdraudējumiem. Tas ir 13 reizes vairāk nekā šī gada 2. ceturksnī un 27 reizes vairāk nekā pirms gada (4. attēls).



4. attēls. Nozīmīgi plašas ietekmes apdraudējumi

Ievērojamais pieaugums nozīmīgu apdraudējumu kategorijā skaidri norāda uz pastiprinātu kiberaktivitāti pret Latviju, kas varētu būt saistīts ar politiskiem, ekonomiskiem vai citiem motivētiem uzbrukumiem.

DDoS uzbrukumi un sarežģītāki ielaušanās mēģinājumi pret valsts iestādēm un kapitālsabiedrībām, IKT kritisko infrastruktūru un pamatpakalpojumu sniedzējiem, tostarp finanšu, transporta, elektronisko sakaru nodrošinātājiem, liecina par mērķētiem uzbrukumiem, iespējams, vērstiem uz konkrētu sektoru destabilizēšanu, informācijas iegūšanu.

Uzbrukumu pieaugums uzsver nepieciešamību pēc pastiprinātas kiberdrošības pasākumiem, tostarp uzlabotas tīkla aizsardzības, ātrākas reaģēšanas spējas un efektīvām uzraudzības sistēmām. Fiksētie kiberuzbrukumi nav radījuši būtisku vai paliekošu ietekmi uz sabiedrību, tas norāda uz efektīvu aizsardzības pasākumu esamību, kas pastāvīgi jāuztur un jāuzlabo, lai stiprinātu kibernoturību pret nākotnes apdraudējumiem.

C4 jeb būtiski apdraudējumi ar vidēju ietekmi veido 0,61% jeb 2466 apdraudētas unikālas IP adreses. Pieaugums pret iepriekšējo ceturksni ir 2%, bet salīdzinājumā ar pagājušā gada 3. ceturksni pieaugums ir 9%. Lielākā daļa apdraudējumu reģistrēti valsts un pašvaldību iestādēs, IKT kritiskajā infrastruktūrā un pakalpojumu sniedzēju, tostarp elektronisko sakaru, veselības aprūpes, izglītības un enerģētikas jomas organizāciju, iekārtās un sistēmās. Izplatītākie apdraudējumi: konfigurācijas nepilnības, pakalpojumatteices uzbrukumi un krāpšanas mēģinājumi.

C5 jeb mēreni apdraudējumi ar nelielu ietekmi veido 0,81% jeb 3 303 apdraudētas unikālas IP adreses. Pieaugums pret iepriekšējo ceturksni ir 4%, bet salīdzinājumā ar 2023. gada 3. ceturksni ir par 16% vairāk.

Kiberapdraudējumi reģistrēti dažādu organizāciju, tostarp finanšu, transporta, elektronisko sakaru un enerģētikas jomas organizāciju, iekārtās un sistēmās. Izplatītākie apdraudējumi – DDoS uzbrukumi, krāpšanas mēģinājumi, ielaušanās mēģinājumi un konfigurācijas nepilnības – norāda uz daudzveidīgiem uzbrukuma veidiem. Sociālās inženierijas uzbrukumi galvenokārt vērsti uz plašu sabiedrību, digitālo infrastruktūru, valsts pārvaldi un finanšu sektoru, kas akcentē nepieciešamību turpināt pastiprinātas apmācības kiberdrošības jomā.

Lielākais īpatsvars (98%) apdraudējumu ietilpst maznozīmīgu apdraudējumu kopā C6, kas ir saistīti ar individuālu lietotāju iekārtām vai plaši izplatītiem ikdienišķiem, automatizētiem uzbrukumu mēģinājumiem uzņēmumiem vai valsts un pašvaldību iestādēm. Vairumā gadījumu, par kuriem ziņots CERT.LV, to ietekme ir neliela vai tās nav.

Būtiskākie kiberincidenti un kiberapdraudējumi, kas izgaismo 2024. gada 3. ceturksnī novērotās tendences un sniedz ieteikumus kiberdraudu mazināšanai, aplūkoti šīs atskaites 2. nodaļā.

Galvenās tendences un secinājumi

Pārskata periodā CERT.LV speciālisti, veicot 14 liela apjoma IT drošības testus, kā arī kiberapdraudējumu un pikšķerēšanas uzbrukumu simulācijas, atklāja un novērsa vairākas būtiskas ievainojamības IKT kritiskās infrastruktūras un pakalpojumu nodrošināšanas organizācijās, kā arī trenēja šo organizāciju darbinieku kiberhigiēnas prasmes.

CERT.LV draudu medību operāciju analīze liecina, ka līdz šim veiktajās operācijās, aptuveni 25% jeb 8 organizāciju iekārtās tika identificēta ārvalstu APT klātbūtne, tostarp Krievijas un Ķīnas sponsorētu politiski motivētu un citu komerciāli motivētu kiberuzbrucēju klātbūtne, kas veiksmīgi neitralizēta. Atklāti arī citi būtiski apdraudējumi, kurus mērķa organizācijām, pateicoties saņemtajām atskaitēm pēc draudu medību noslēgšanās, bija iespēja novērst, pieņemot datos balstītus lēmumus.

Latvija turpina sastapties ar augstu Krievijas un to atbalstošo haktīvistu radīto kiberapdraudējumu. Pret Latviju tiek turpināti DDoS uzbrukumi, vēršot tos pret valsts iestādēm, IKT kritisko infrastruktūru un pakalpojumu sniedzējiem. No Krievijas puses atbalstīto kiberuzbrukumu aktivitātes (it īpaši GRU īstenotas) Latvijā primāri mēģina mazināt atbalstu Ukrainai un valsts drošības stiprināšanai, provocējot ideoloģisko vērtību sadursmes, kuras izraisījis ģeopolitiskās vides konflikts starp Ukrainu un Krieviju.

Turpinās piegādes ķēžu kompromitēšanas gadījumi starpniekpakalpojumu sniedzējiem ārpus Latvijas, bet tādējādi tiek ietekmēts TV kanāla saturs Latvijā. Atkārtoti novērots gadījums, kad Krievijas vai ar to saistīta haktīvistu grupa uz dažām minūtēm aizstāja “Balticom” IPTV pārraidīto saturu ar savu video, kas slavina Krievijas imperiālismu.

Novērota izspiedējvīrusu pastiprināta aktivizēšanās - uzbrukumi uzņēmumiem kļūst arvien pārdrošāki un finansiāli graujošāki. Pārskata periodā ražošanas uzņēmums “Amber Beverages Group” piedzīvoja šifrējošā izspiedējvīrusa uzbrukumu, kas rezultējās uzņēmuma datu noplūdē. Pieaug draudi kiberdrošībai un datu integritātei.

Ar datiem saistītie kiberapdraudējumi visvairāk vērsti pret tām nozarēm, kurās glabājas fizisko personu informācija (valsts pārvalde, digitālā infrastruktūra, finanses un uzņēmējdarbības pakalpojumi). Jāuzsver kiberapdraudējumu motivācijas daudzveidība, sākot ar finansiāliem stimuliem un beidzot ar ideoloģiskiem mērķiem.

Lai gan sociālās inženierijas paņēmienus bieži izmanto, lai iegūtu sākotnējo piekļuvi, tos izmanto arī vēlākajos uzbrukuma posmos. Nozīmīgi piemēri ir biznesa e-pasta kompromitēšana, pikšķerēšanas e-pasta vēstules, krāpšanas ar telefonzvaniem vai sociālo tīklu kanālos, izliekoties par citu personu, viltus tīmekļvietnes, izmantojot uzticamu organizāciju zīmolus u.c.

Latvijā kibernoturības līmenis joprojām ir atšķirīgs starp dažādām organizācijām un sektoriem, taču kopumā novērojama pastiprināta interese par kibernoturības uzlabošanu, kā arī par savu IKT resursu stiprināšanu.

No 2024. gada 1. septembra, stājoties spēkā Nacionālās kiberdrošības likumam (NKDL), kiberincidentu novēršanas institūcija CERT.LV kļūst par daļu no Nacionālā kiberdrošības centra. NKDL paplašina likuma tvērumu uz plašāku uzņēmumu loku, tādējādi palielinot CERT.LV klientu skaitu, kam jāievēro jaunās prasības, bet kas var arī saņemt CERT.LV piedāvātos pakalpojumus. Kā galvenā operacionālās kiberdrošības organizācija Latvijā CERT.LV piedāvā plašu pakalpojumu klāstu kibernoturības stiprināšanai.

CERT.LV EKSPERTU KOMENTĀRS

Līdzšinējie kiberuzbrukumi nav spējuši būtiski ietekmēt Latvijas sabiedrību. Tomēr kiberdrošības kopiena nedrīkst atslābt. Ņemot vērā kiberapdraudējumu plašo spektru un nepārtraukto attīstību, efektīvākais veids apdraudējumu identificēšanai, novēršanai un seku mazināšanai ir publiskā un privātā sektora sadarbība un kibernoturības stiprināšana, kas Latvijā jau tiek īstenota un pilnveidota.

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

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

CERT.LV uztur un regulāri aktualizē informāciju par kiberdrošības apdraudējumiem, sniedz valsts un privātajām organizācijām, kā arī fiziskām personām atbalstu kiberdrošības jomā, ja incidentā iesaistīta Latvijas IP adrese vai .lv domēns.

2024. gada 3. ceturksnī tika turpināta ziņošana par incidentiem, aktīva sadarbība un informācijas apmaiņa ar kiberdrošības kopienu, kas ir būtiski efektīvas kiberdrošības priekšnoteikumi, lai stiprinātu Latvijas kiberdrošību un noturību.

Tendences īsumā:

- Uz sociālo inženieriju balstīti kiberuzbrukuma vektori datu izgūšanai un integritātes kompromitēšanai: pikšķerēšana, smikšķerēšana, mērķēta pikšķerēšana, e-pasta sarakstes kompromitēšana, mānīšanās zvani, kas iekļauj cilvēka balss atdarināšanu, viltus vietnes un profili sociālajos tīklos viltus loteriju un aptauju izplatīšanai – tostarp pieaug latviešu valodā veiktu krāpšanu aktivitāte.
- Ģeopolitiskās vides konflikti joprojām ir spēcīgs DDoS kiberuzbrukumu virzītājspēks.
- Pieaugu iekārtu kompromitēšanas riski, lielāka uzmanība piegādes ķēžu ievainojamībām.
- Ļaundabīga koda izplatība joprojām apdraud datu integritāti, lietotāju datu zadzēji un ļaunprātīgas programmatūras, kas izzog personas datus, kļūst arvien sarežģītākas un rada nopietnas bažas, pastiprinās serveru šifrēšana izspiešanas nolūkos.

Būtiskākie kiberincidenti un kiberapdraudējumi, kas izgaismo 3. ceturksnī novērotās tendences, plašāk aplūkoti turpinājumā šīs nodaļas 2.1. - 2.6. apakšsadaļās.

2.1. Krāpšana

Krāpniecības apmēri uzņem apgriezienus.

2024. gada 3. ceturksnī CERT.LV reģistrēto apdraudēto unikālo IP adrešu skaits ir palielinājies par 62% salīdzinājumā ar iepriekšējo ceturksni un par 183% salīdzinājumā ar pagājušā gada 3. ceturksni.

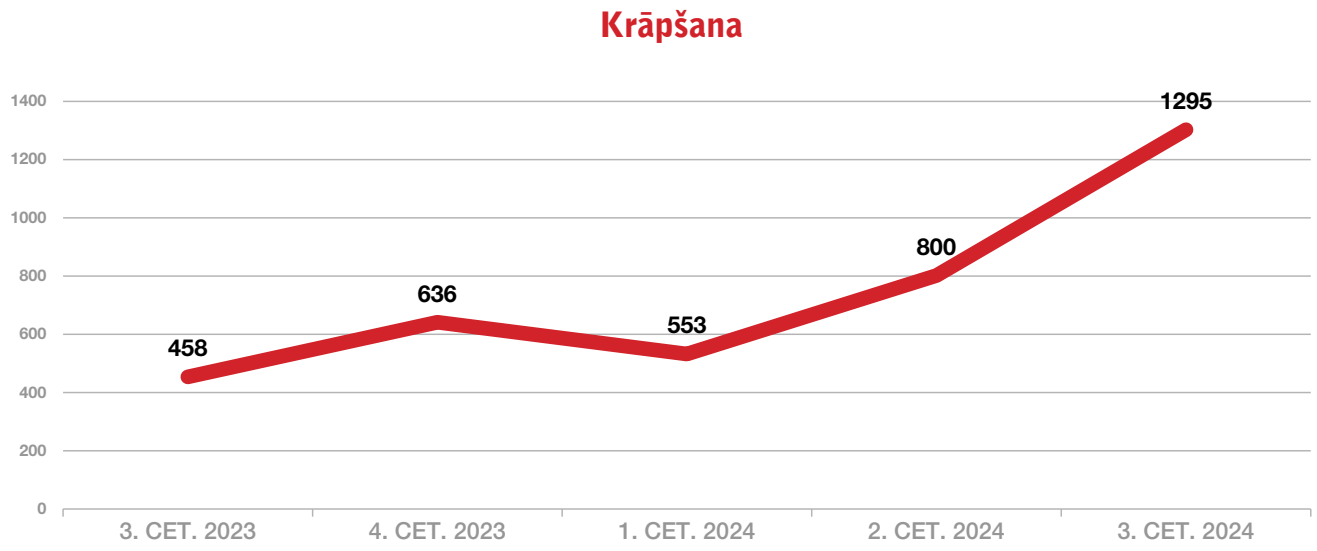
Tas norāda uz pastiprinātu kiberaktivitāti un lielāku risku interneta lietotājiem. Lai mazinātu risku, ir svarīgi turpināt izglītot sabiedrību un veicināt labu kiberhigiēnas praksi.

Uz sociālo inženieriju balstīti kiberuzbrukuma vektori

Šajā pārskata periodā pastiprinājās uz sociālo inženieriju balstīti kiberuzbrukuma vektori datu izgūšanai un integritātes kompromitēšanai. Sociālās inženierijas kampaņas dažādos veidos joprojām ir būtisks kiberapdraudējums, izmantojot tādus vektorus kā pikšķerēšanu, smikšķerēšanu, mērķētu pikšķerēšanu, e-pasta sarakstes kompromitēšanu, mānīšanās zvanus, kas iekļauj cilvēka balss atdarināšanu, zīmolu viltošanu u.c.

Sociālā inženierija ietver plašu darbību klāstu, kuru mērķis ir izmantot cilvēka kļūdas vai cilvēka uzvedību, lai iegūtu piekļuvi informācijai vai pakalpojumiem. Tā izmanto dažādus manipulācijas veidus, lai piespiestu upurus nodot personas datus vai sensitīvu un slepenu informāciju. Lietotājus var pierunāt atvērt dokumentus, ļaunprātīgas saites vai e-pastus, apmeklēt krāpnieciskas tīmekļa vietnes vai piešķirt piekļuvi sistēmām vai pakalpojumiem. Lai gan izmantotajās viltībās

un trikos var ļaunprātīgi izmantot tehnoloģijas, taču, lai tehnoloģijas būtu veiksmīgas, ļoti liela to daļa aizvien ir atkarīgas no cilvēciskā faktora.



5. attēls. Apdraudēto unikālo IP adrešu skaits

Sociālās inženierijas mērķa izvēles varianti:

- gadījuma izvēle,
- mērķēts uzbrukums, veicot priekšizpēti (“Google” paplašinātā meklēšana, publiski pieejamie dati, uzņēmumu tīmekļvietnes, “Linkedin” profili u.c.),
- daļēji automatizēts, balstoties uz noplūdušiem datiem vai vāju uzņēmuma/personas datu drošību.

Pikšķerēšana un smikšķerēšana

Pikšķerēšanas mērķis ir maldināt adresātus, lai tie atklātu savus datus, piemēram, paroles. Uzbrucēji izmanto maldinošus e-pasta ziņojumus, saites uz vietnēm, kas šķiet likumīgas, u.tml.

Pārskata periodā intensīvākā krāpniecisku īsziņu izsūtīšana jeb smikšķerēšana tika novērota sūtījumu piegādes uzņēmumu vārdā (“DPD”, “FedEX”, VAS “Latvijas Pasts” u.c.). Tāpat krāpnieki uzdevās par policijas, valsts iestāžu, mobilo sakaru operatora pārstāvjiem vai bankas darbiniekiem, lai izkrāptu personas un autentifikācijas datus. Turpinājās nodokļu atmaksas pikšķerēšanas uzbrukumi, viltus darba piedāvājumi, viltus rēķinu izsūtīšana. Ievērojami pieauga “Microsoft 365” piekļuves datu izkrāpšanas mēģinājumu skaits.

Masīvs pikšķerēšanas e-pasta vēstuļu vilnis tika novērots AS “SEB banka” vārdā. Krāpnieki, mudinot atjaunināt konta informāciju, centās iegūt potenciālā upura internetbankas piekļuves datus un pēc tam izkrāpt naudu. Kā jaunums novērota pikšķerēšana ar “Viada” vārdu, kur e-pasta vēstulē pievienotā ļaunprātīgā saitē potenciālo upuri aicināja “aplūkot” naudas pārvedumu.

Kā ierasts, jūlijs un augusts, kad sākas ceļojumu sezona, ir pļaujas laiks datu zagļiem un krāpniekiem – tie uzdevās par populārām naktsmītņu izīrēšanas vietnēm (booking.com, airbnb.com u.c.), mēģinot piekļūt lietotāju datiem.

Maskējoties aiz kurjerpasta "FedEX" vārda, jūlijā masveidā tika sūtītas e-pasta vēstules latgaliešu valodā. Tas varētu būt skaidrojams ar to, ka jūnijā tulkošanas rīks "Google Translate" tika paplašināts ar 110 jaunām valodām, tostarp latgaliešu. Iedzīvotāji tiek mudināti saglabāt modrību un brīdināt gados vecākus cilvēkus, lai viņi nekristu par upuri šādiem krāpniekiem.

Viltotas tīmekļvietnes un profili sociālajos tīklos

Viltotas tīmekļvietnes vai profili sociālajos tīklos, kas sola neiedomājamas atlaides vai aicina aizpildīt aptaujas, lai vāktu personu datus, ar krāpnieciskām saitēm aizvien pievilina neuzmanīgus lietotājus.

Teju katru dienu parādās jaunas viltus tīmekļvietnes, kas sola neiedomājamas atlaides vai pasakainas iespējas investīcijām, izmantojot pārdomātas pikšķerēšanas taktikas. Viltus ziņojumu un tīmekļa vietņu atšķiršana no īstām kļūst arvien sarežģītāka.

Augustā un septembrī īpaši brutālas bija krāpnieku "medības" sociālajos tīklos, ar 150 eiro balvu pievilinot upuri aizpildīt viltus aptauju it kā AS "SEB banka" vārdā. Viltus anketā ievadītā informācija tiek izmantota upura uzrunāšanai krāpšanas shēmās turpmāk. Tāpat "iekrist" krāpnieku rokās varēja, piedaloties neīstās loterijās, kas imitēja, piemēram, "Philips", "RD Electronics" un citus zīmolus, lai saņemtu kāroto lietu "pa lēto". Krāpnieki izplatīja viltus ziņas par labdarības izpārdošanu, novirzot upuri uz norēķinu karšu datu pikšķerēšanas formu.

Fiksēti vairāki krāpnieciski gadījumi, kur, izmantojot viltus tīmekļvietnes, kas šķietami atgādina "Omniva" vai "DPD" vietnes, krāpnieki mēģināja izkrāpt norēķinu karšu datus no personām, kas ievieto savas preces pārdošanai interneta vidē.

Mērķēta pikšķerēšana

Mērķēta pikšķerēšana ir līdzīga pikšķerēšanai, taču, lai izskatītos vēl pārliecinošāk, uzbrucēji pielāgo ziņojumus, pamatojoties uz konkrētu informāciju par organizāciju vai personu. Nereti krāpnieki izmanto brīvi pieejamās informācijas vākšanu (OSINT), lai iepazītu savu mērķi.

Savukārt uzņēmumi cieš no krāpnieku metodēm, kas īpaši mērķētas uz grāmatvežiem ar piekļuvi uzņēmuma kontiem un pilnvarām veikt maksājumus, un šī tendence kļūst arvien spēcīgāka. Nereti uzņēmumam e-pasta vēstules pielikumā krāpnieki iemāna viltotus rēķinus. Izliekoties par augstākā līmeņa vadītājiem, krāpnieki liek grāmatvežiem veikt steidzamus maksājumus. Novēroti mēģinājumi izkrāpt Smart-ID PIN kodus, kas dod piekļuvi uzņēmuma kontiem. Blēži bieži uzdodas par policijas, bankas darbiniekiem, zvanot vai sūtot īsziņas un e-pasta vēstules, imitējot it kā "slepenu operāciju", kurā grāmatvedim "jāglābj" uzņēmuma nauda.

Mānīšanās zvani, kas iekļauj cilvēka balss atdarināšanu

Pārskata periodā fiksēti krāpniecības gadījumi, kas iekļauj cilvēka balss atdarināšanu, izmantojot mākslīgā intelekta rīkus. Telefonkrāpnieki zvana no nezināmiem numuriem, atdarinot zvana saņēmējam pazīstama cilvēka balsi, un lūdz steidzamu finansiālu palīdzību. Šādi zvani tā saņēmējam rada maldīgu iespaidu, ka grūtībās ir nonācis tuvs cilvēks,

kas palielina iespēju kļūt par telefonkrāpnieka upuri. Tāpat turpinās personas datu izzagšanas mēģinājumi, izmantojot zvanītāja ID viltošanu.

CERT.LV novērojumi rāda, ka mākslīgā intelekta rīki spēj veikt zvanus latviešu valodā un, iespējams, nodrošināt tulkošanu reāllaikā.

Saņemti ziņojumi par jaunu telefonkrāpnieku shēmu

Iedzīvotāji saņem zvanus it kā no Smart-ID darbiniekiem, turklāt sākotnējā zvana veikšanā bieži tiek izmantots robots – automātiskais atbildētājs, kurš zvana saņēmēju informē, ka uz jaunas ierīces tiek uzstādīts viņa Smart-ID konts. Ja zvana saņēmējs neesot šo darbību veicis, tālāk tiek aicināts nospiest taustiņu "1", lai sazinātos ar operatoru. Izpildot šīs darbības, zvana saņēmējs šķietami tiek savienots ar Smart-ID operatoru, kas patiesībā ir krāpnieks. Sarunai tiek pieaicināti it kā policijas un bankas darbinieki, kuri palīdzēšot "novērst" radušos apdraudējumu. Šādi iegūstot uzticību, krāpnieks aicina potenciālo upuri izpaust personas datus, piemēram, internetbankas pieejas datus vai kartes datus, PIN kodu, vai izmaksāt skaidru naudu un nodot to kurjeriem u.c.

Neuzmanība un nepietiekama kiberhigiēna palielina krāpniecības riskus

Joprojām izaicinājums ir neuzmanība un nepietiekama kiberhigiēna gala lietotāju līmenī. Jāsaprot, ka pat viens lietotāja klikšķis var nodarīt milzīgu kaitējumu ne tikai pašas personas datu drošībai, bet arī darbinieka darba vietai. Elementāras kiberhigiēnas nepārzināšana vai neievērošana ir viens no iemesliem, kāpēc tik daudzi Latvijas iedzīvotāji ir pakļauti krāpniecības riskiem kibervidē.

CERT.LV mudina iedzīvotājus un organizācijas izmantot DNS ugunsmūri. CERT.LV operatīvi ievieto krāpniecisku aktivitāšu indikatorus DNS ugunsmūrī, lai tā lietotājus pasargātu no krāpniecisku vai ļaundabīgu vietņu apmeklēšanas, tādējādi novēršot lietotāju piekļūšanu bīstamiem resursiem un tos pārvirzot uz brīdinājuma vietni.

Iestāžu (prioritāri valsts un pašvaldību) darbinieku digitālās drošības un pratības uzlabošanai CERT.LV piedāvā pikšķerēšanas uzbrukumu simulācijas pakalpojumu. Ar tā palīdzību organizācijas var simulēt pielāgotus un reālus pikšķerēšanas uzbrukumus, lai apmācītu darbiniekus un veicinātu spējas identificēt, atpazīt un novērst kiberapdraudējumus. Tas palīdz stiprināt organizāciju aizsardzību pret sociālās inženierijas uzbrukumiem, tā mazinot cilvēciskā faktora riskus. CERT.LV aicina rakstīt uz cert@cert.lv un informēt par vēlmi saņemt pakalpojumu.

CERT.LV EKSPERTU KOMENTĀRS

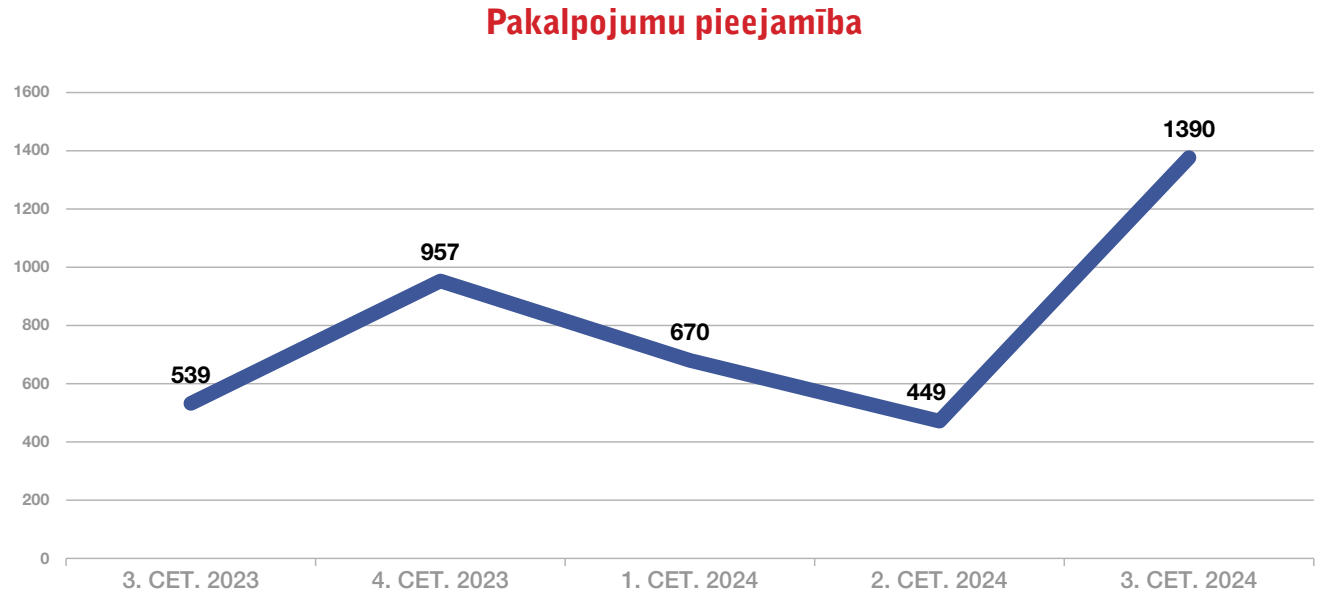
Krāpšanas taktikas ir izsmalcinātas, taču preventīvie pasākumi pavisam vienkārši – jāsāk ar drošu paroļu pārvaldnieku, divfaktoru autentifikāciju (2FA), regulāriem atjauninājumiem un DNS ugunsmūri. Turklāt vienmēr ar piesardzību izturēsimies pret aizdomīgiem zvaniem, e-pasta vēstulēm un ziņojumiem. Domāsim kritiski par katru pieprasījumu dalīties ar savu personīgo informāciju. Būsim modri un izturēsimies atbildīgi pret digitālo drošību un savām darbībām tiešsaistē!

10 IETEIKUMI DROŠĪBAI

1. Pārbaudīt avotus un datu precizitāti, kritiski izvērtējot saņemtās ziņas patiesumu un sūtītāja e-pasta adresi un saturu, rūpīgi pievērst uzmanību valodas kļūdām un stilam.
2. Regulāri un savlaicīgi atjaunināt viedierīču un iekārtu operētājsistēmas un lietotnes.
3. Neievadīt informāciju uznirstošajos logos un neklikšķināt uz saitēm tajos.
4. Neklikšķināt uz saites, ja nav pārliecības, ka saite ved uz vietni, kas saistīta ar uzticamu vēstules sūtītāju! Šaubu gadījumā zvanīt uz organizācijas oficiālo tālruni un pārbaudīt.
5. Papildu aizsardzībai izmantot divu faktoru 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 (*AnyDesk, TeamViewer, HopToDesk, AeroAdmin* u.c.).
8. Veikt DMARC un SPF pārbaudes ienākošā e-pasta vēstulēm, lai ierobežotu viltoto vēstuļu saņemšanu. Plašāk: https://cert.lv/lv/2020/05/e-pastu-drosiba-aizsardziba-pret-izejoso-e-pastu-viltosanu
9. Izmantot CERT.LV un NIC.LV nodrošināto bezmaksas aktīvo aizsardzības pakalpojumu – https://dnsmuris.lv/, lai pasargātu sevi un darbiniekus no krāpniecisku vietņu apmeklēšanas.
10. Ziņot par krāpnieku aktivitātēm un ļaundabīgām vietnēm, pārsūtot kaitīgās e-pasta vēstules uz cert@cert.lv, tādējādi pasargājot citus DNS ugunsmūra lietotājus.

2.2. Pakalpojuma pieejamība

Statistika nav iepriecinoša. Pakalpojumatteices kiberuzbrukumu skaita pieaugums par 158% salīdzinājumā ar pagājušā gada 3. ceturksni un vairāk nekā trīskārtīgs (+210%) pieaugums salīdzinājumā ar iepriekšējo ceturksni liecina par ievērojamu uzbrukumu skaita un intensitātes pieaugumu.



6. attēls. Apdraudēto unikālo IP adrešu skaits

Ir svarīgi turpināt izglītot organizāciju atbildīgos par IT drošību par pieejamām efektīvām aizsardzības stratēģijām un rīkiem, kā arī turpināt stiprināt aizsardzības pasākumus.

Pārskata periodā Latvijā novēroti apjomīgi kiberuzbrukumi pret atsevišķiem resursiem valsts un privātajā sektorā nolūkā negatīvi ietekmēt pakalpojuma pieejamību, iespējams, politisku un ideoloģisku motīvu dēļ. Ievērojams skaits kiberuzbrukumu tika vērsti uz digitālo infrastruktūru un elektronisko sakaru komersantiem, kā arī transporta un finanšu nozares aktīviem, tomēr būtiska ietekme nav konstatēta.

Haktīvistu aktivitātes, ko arvien vairāk virza notiekošie ģeopolitiskie konflikti, ir kļuvušas par dinamisku elementu kiberdraudu ainavā. Karš Ukrainā turpina katalizēt haktīvistu aktivitātes pieaugumu. Uzbrukumi bieži ir atriebība, kuru mērķis ir traucēt pakalpojumu sniegšanai un nosūtīt politiskus paziņojumus. Daļa kiberuzbrukumu nāk no prokrieviski noskaņotām haktivistu grupām, piemēram, “REvil”, “KillNet” un “Anonymous Sudan”.

Kiberuzbrucēji turpina vērsties pret NATO sabiedrotajām valstīm, lai traucētu IKT infrastruktūras darbību Ukrainas atbalstītājiem. Šī tendence nav mazinājusies un, visticamāk, turpināsies.

Šī gada jūlijā Latvijas valsts prezidenta Edgara Rinkēviča paziņojums medijiem no NATO samita Vašingtonā par Rietumu ieroču piegādēm Ukrainai izraisīja plašu diskusiju haktīvistu grupās “Telegram” kanālā. 12. jūlijā tika veikti plaši piekļuves atteices uzbrukumi elektronisko sakaru komersantiem. Pieprasījumu skaits bija pat 200 reižu lielāks nekā parasti, izraisot īslaicīgus traucējumus mājaslapu darbībā. Kiberuzbrukumi tika novērsti, galvenokārt izmantojot ģeobloķēšanu.

Pārskata periodā augusta otrajā pusē valsts mērogā tika novēroti intensīvi un pielāgoti DDoS uzbrukumi valsts sektora un transporta nozares interneta resursiem, kā arī atsevišķiem resursiem privātajā sektorā. Uzbrukumu rezultātā daļai resursu bija novērojami darbības traucējumi – lēndarbība vai atsevišķos gadījumos – periodiska nepieejamība. Kopumā uzbrukumi vērtējami kā apjomīgi. No VAS “Latvijas Valsts radio un televīzijas centrs” iegūtā informācija liecina, ka uzbrucēji profilēja vietņu veiktspēju un pielāgoja uzbrukumu parametrus, tēmējot uz noteiktām lapu funkcionalitātēm. Uzbrucēji dinamiski adaptējās un aktivizēja jaunus uzbrukuma avotus. Uzbrukumi ar dažādiem mērķiem un intensitāti turpinājās nedēļas garumā. To iemesls ir sasaistāms ar Latvijas palīdzības paketi Ukrainai, kas tika apstiprināta 13. augustā – 30 aprīkotu transportlīdzekļu nodošanu Ukrainai.

No Krievijas puses atbalstīto kiberuzbrukumu mērķis Latvijā primāri ir mēģināt mazināt atbalstu Ukrainai un valsts drošības stiprināšanai, provocējot ideoloģisko vērtību sadursmes, kuras izraisījis ģeopolitiskās vides konflikts starp Ukrainu un Krieviju. Politiski un ideoloģiski motivēti DDoS uzbrukumi, ko veic Krievijas atbalstīti haktīvistu grupējumi ar mērķi radīt sabiedrībā paniku un graut uzticību valsts iestādēm, viļņveidīgi notiek kopš 2022. gada sākuma. Visticamāk, ka Latvija, kā arī Lietuva, Igaunija, Ziemeļvalstu reģions un Polija turpinās būt Krievijas kiberoperāciju ilgtermiņa mērķi.

Kopumā situācija Latvijas kibertelpā joprojām saglabājas stabila, CERT.LV sadarbībā ar partneriem turpina aktīvi uzraudzīt kibertelpas drošību, un ir pastiprināta aizsardzība ar centralizēto DDoS aizsardzības risinājumu. CERT.LV uzsver nepieciešamību sistēmu uzturētājiem būt modriem un proaktīviem, mērķtiecīgi strādājot pie kiberdrošības pārvaldības un noturībspējas stiprināšanas, jo nav sagaidāms, ka kiberuzbrukumu mēģinājumi samazināsies.

Lai saņemtu atbalstu DDoS incidenta izmeklēšanā, seku novēršanā un prevencijas plānošanā, CERT.LV aicina zvanīt uz 67085888 vai rakstīt uz cert@cert.lv

IETEIKUMI DROŠĪBAI

1. Apzināt publiskos 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. Izstrādāt un notestēt rīcības plānu, kā rīkoties uzbrukuma laikā:
   - pieslēgt DDoS aizsardzību, ko nodrošina interneta pakalpojumu sniedzējs. Latvijā DDoS aizsardzības pakalpojumus piedāvā Aizsardzības ministrija sadarbībā ar VAS "Latvijas Valsts radio un televīzijas centrs", SIA "TET" un citi pakalpojumu sniedzēji;
   - pēc pieprasījuma interneta pakalpojumu sniedzējs var izfiltrēt/ierobežot lieko datu plūsmu automātiski vai manuāli;
   - migrēt atsevišķas svarīgākās sistēmas aiz DDoS aizsardzības uz mākoņpakalpojumu satura piegādes tīkliem (*Content Delivery Network*), piemēram, "Cloudflare", "Microsoft Azure", "Google", "AWS";
   - filtrēt piekļuvi resursam pēc ģeolokācijas, atstājot piekļuvi svarīgākajiem klientiem vai tikai Latvijas IP adrešu diapazoniem.

Pilns saraksts ar ieteikumiem DDoS ietekmes mazināšanai ir pieejams CERT.LV tīmekļvietnē: https://cert.lv/lv/2022/08/ieteikumi-ddos-ietekmes-mazinasanai

2.3. Ievainojamības un konfigurācijas nepilnības

Ievainojamība – IKT vai to pakalpojumu vājums, uzņēmība pret tehniskām problēmām vai nepilnība, kas var tikt izmantota kiberapdraudējumam.

CERT.LV regulāri veic visaptverošu monitoringu, pētot ievainojamību (CVE) ainavu, kas ir sasaistāma ar eksponētiem servisiem/iekārtām.

CVE (*Common Vulnerabilities and Exposures*) ir standartizēta sistēma, kas paredzēta dažādu programmatūras un aparatūras produktu drošības ievainojamību identificēšanai un nosaukšanai. Tā katrai ievainojamībai piešķir unikālu identifikatoru, padarot vienkāršāku dažādu sistēmu un datubāzu ievainojamību izsekošanu un atsauci uz tām.

3. ceturksnī CERT.LV proaktīvi izplatīja brīdinājumus lietotājiem par 16 jaunatklātām kritiskām CVE ievainojamībām (jūlijā – 3, augustā – 8, septembrī – 5), sniedzot koordinētus norādījumus par atjauninājumiem un to uzstādīšanu.

Atbilstoši FIRST CVSS metodoloģijai, ievainojamības, kuru vērtējums ir diapazonā no 9.0 līdz 10, ir kritiskākās ievainojamības, kas norāda, ka tām ir augsts izmantošanas potenciāls, un tās rada ievērojamus riskus sistēmām un datiem. Daudzas ir saistītas ar tīmekļa ievainojamībām, kas bieži vien ir galvenais mērķis uzbrucējiem, kuri meklē nesankcionētu piekļuvi.

Pastāvīga tendence ir ievainojamību izmantošana tīmekļa pārvaldības sistēmās, ugunsmūros, VPN un maršrutētājos. Nepareizi konfigurēti pakalpojumi joprojām rada ievērojamus riskus.

Lai mazinātu kritisko ievainojamību radītos riskus, organizācijām stingri jāapsver iespēja ieguldīt drošā programmatūras izstrādes praksē un pieņemt attiecīgas stratēģijas.

Svarīgi ir nekavējoties labot ievainojamības, kas novērtētas kā "augstas" vai "kritiskas". Šī prakse ir būtiska, lai aizsargātu organizāciju no iespējamiem uzbrukumiem. Daudzos gadījumos ievainojamības, kas ietilpst šajās kategorijās, var būt pieejamāks ieejas punkts uzbrucējiem, kuri vēlas uzlauzt sistēmas un piekļūt datiem. Šādi uzbrukumi var radīt finansiālus zaudējumus, kaitēt organizācijas reputācijai vai pat izraisīt sodus. Tomēr nevajadzētu ignorēt ievainojamības ar zemāku vērtējumu, jo tās bieži kalpo kā balsts vēlākos kiberuzbrukuma posmos.

Izaicinājumus var radīt arī kļūdains programmatūras atjauninājums, kā tas notika šā gada 19. jūlijā, kad daudzi lietotāji visā pasaulē saskārās ar operētājsistēmas "Windows" problēmām. To izraisīja kļūdains "CrowdStrike" antivīrusa programmas atjauninājums, kas izsita no ierindas vairāk nekā 8,5 miljonus datoru. IT traucējumi visā pasaulē ietekmēja lidostas, dzelzceļa satiksmi un veselības aprūpes nozari, viesnīcas, medijus, bankas un daudzas citas organizācijas. Latvijā "CrowdStrike" programmatūra nav plaši izmantota, tāpēc ietekme bija minimāla. CERT.LV eksperti iesaka vienmēr pārbaudīt atjauninājumus pirms to uzstādīšanas.

Ņemot vērā ievainojamību lielo skaitu un izaicinājumus, ar kuriem saskaras produktu izstrādātāji un lietotāji, ļoti ticams, ka ievainojamību izmantošana arī turpmāk būs viens no galvenajiem piekļuves punktiem gan valstu atbalstītiem grupējumiem, gan kibernoziedzniekiem, lai iefiltrētos sistēmās un nozagtu vērtīgus datus. Šī tendence akcentē, ka efektīva un prioritāra ievainojamību lāpīšana varētu novērst lielu skaitu incidentu vai vismaz padarīt tos ievērojami grūtāk izpildāmus.

CERT.LV brīdinājumi par kritiskām ievainojamībām 2024. gada 3. ceturksnī

CVE	Ietekmētie produkti	Apraksts
CVE-2024-6387	*OpenSSH*	2. jūlijs – Kritiska ievainojamība, kas kibertelpā tiek dēvēta arī par RegreSSHion. Izmantojot šo ievainojamību, uzbrucējs neautentificējoties var veikt attālinātu koda izpildi ar augstākajām sistēmas (*root*) privilēģijām.
CVE-2024-3596	*Blast-RADIUS*	10. jūlijs – Kritiska ievainojamība RADIUS protokolā, kuru izmantojot uzbrucējs var piekļūt mērķa organizācijas tīkla iekārtām un servisiem, nezinot lietotāju piekļuves datus un, iespējams, pat apiet vairāku faktoru autentifikāciju.
CVE-2024-6385	*GitLab Community, Enterprise versijas*	11. jūlijs – Identificētas vairākas nopietnas ievainojamības, bīstamākā un jaunākā no tām ir CVE-2024-6385, kuru uzbrucēji var izmantot, lai izpildītu neautorizētus automatizētus uzdevumus kā cits lietotājs.
CVE-2024-42008 **CVE-2024-42009** **CVE-2024-42010**	*Roundcube Webmail programmatūra*	8. augusts – Būtiskas ievainojamības, kas sniedz uzbrucējam iespēju, nosūtot speciāli izveidotu e-pasta vēstuli, izpildīt attālināto JavaScript kodu webmail lietotāja tīmekļa pārlūkā un neautorizēti iegūt pieeju e-pasta saturam, lietotāja parolēm, kontaktiem, kā arī neautorizēti izsūtīt e-pasta vēstules.
CVE-2024-38077	*Windows serveri*	9. augusts – Kritiska ievainojamība Windows serveru programmatūrā, kas sniedz uzbrucējam iespēju veikt attālinātu koda izpildi, pilnībā pārņemot Windows serveri. Attālinātai koda izpildei uzbrucējam nav nepieciešama autorizācija sistēmā vai darbības no lietotāju puses (0-click).
CVE-2024-22116	*Zabbix programmatūra*	13. augusts – Atklāta kritiska attālinātās koda izpildes (RCE) ievainojamība, kas ļauj autentificētam ierobežotas piekļuves administratoram veikt attālinātu koda izpildi.
CVE-2024-38063	*Windows sistēmas*	14. augusts – Kritiska ievainojamība, kas ļauj veikt attālinātu koda izpildi bez autorizācijas, izmantojot IPv6 paketes.
CVE-2024-2961	*Linux GLIBC funkcija iconv*	20. augusts – Atrasti jauni veidi, ka iepriekš (maijā) atklāto ievainojamību izmantot, lai panāktu attālinātu komandu izpildi Roundcube programmatūrā.

CVE	Ietekmētie produkti	Apraksts
CVE-2024-42815	*TP-Link maršrutētāji*	30. augusts – Kritiska attālinātā koda izpildes ievainojamība (CVSS 9.8*) TP-Link RE365 sērijas maršrutētājos. Veiksmīga uzbrukuma rezultātā attālināti iespējams izpildīt patvaļīgas komandas un potenciāli pārņemt iekārtu savā kontrolē.
CVE-2024-7261	*Zyxel*	4. septembris – Kritiska komandu injekcijas ievainojamība (CVSS 9.8*) vairākās ražotāja Zyxel AP un Security Router iekārtās, kas ļauj neautentificētam uzbrucējam patvaļīgi izpildīt operētājsistēmas komandas, kā rezultātā iespējams attālināti piekļūt iekārtai vai manipulēt ar sistēmas failiem un resursiem, apdraudot ierīces drošību.
CVE-2024-2169	*Webmin un Virtualmin*	5. septembris – Kritiska ievainojamība Webmin un Virtualmin vadības paneļos, to var izmantot ļaunprātīgi uzbrucēji, lai izraisītu nebeidzamu pakalpojuma atteices uzbrukumu.
CVE-2024-38812 **CVE-2024-38813**	*VMware vCenter Server, Cloud Foundation*	18. septembris – Ievainojamības sniedz uzbrucējam iespēju veikt attālinātu koda izpildi un eskalēt tiesības līdz root lietotājam, tādējādi pārņemot ievainojamo sistēmu.
CVE-2024-45519	*Zimbra Collaboration*	23. septembris – Ievainojamība dod iespēju uzbrucējam attālināti izpildīt uz sistēmas ļaundabīgu kodu, izmantojot postjournal servisu. Ievainojamībai ir pieejams POC (proof of concept), tāpēc ir sagaidāms, ka tā tiks aktīvi izmantota uzbrukumos kibertelpā.

*CVSS ir nozares standarta datorsistēmu drošības ievainojamību nopietnības novērtēšanas metodoloģija, palīdzot organizācijām noteikt prioritāti, kuras ievainojamības novērst vispirms.

Kiberuzbrucēji vispirms ķeras pie visvieglākajiem mērķiem, tāpēc neatlieciet drošības atjauninājumus. CERT.LV aicina sekot līdzi izstrādātāju norādījumiem un nevilcinoties atjaunināt programmatūras un operētājsistēmas uz jaunāko pieejamo versiju. Ar visiem aktuālajiem brīdinājumiem var iepazīties tīmekļa vietnē www.cert.lv.

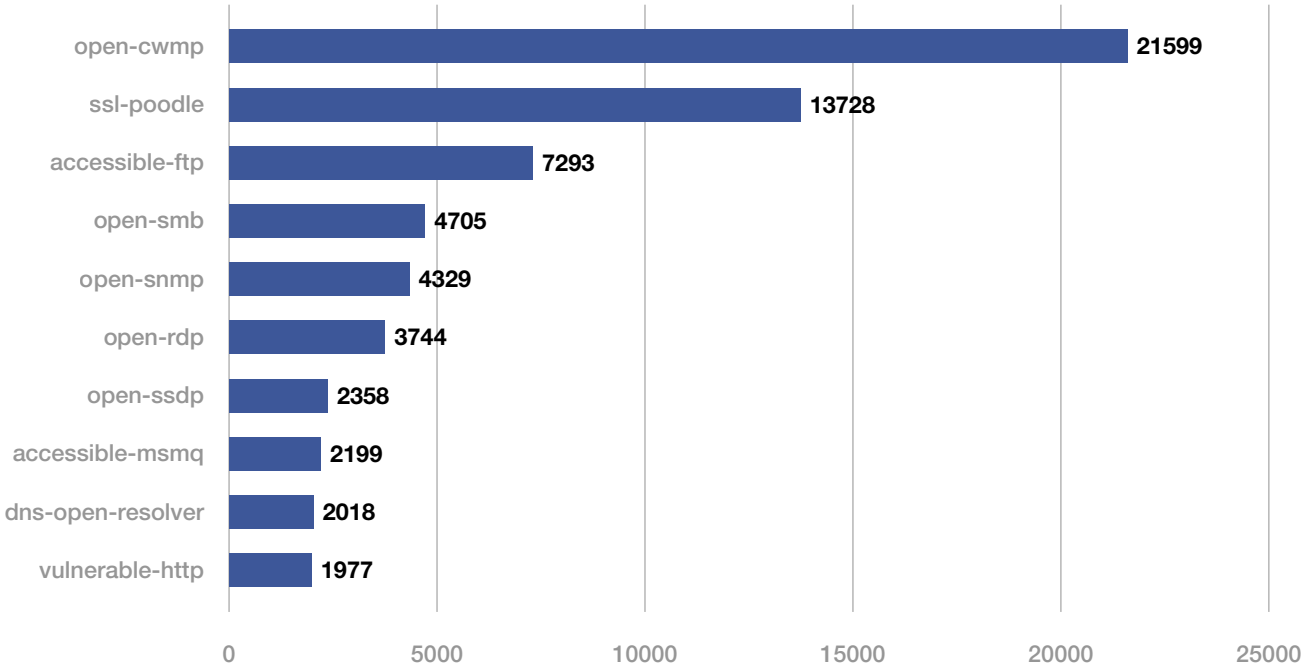
Top 10 konfigurācijas nepilnības 2024. gada 3. ceturksnī

Konfigurācijas nepilnības aizvien veido lielāko daļu no visiem CERT.LV reģistrētajiem apdraudējuma veidiem Latvijas kibertelpā. Turklāt to skaits turpina pieaugt, uzrādot augšupejošu tendenci un sasniedzot augstāko rādītāju pēdējo divu gadu laikā – 87 233 apdraudētas unikālas IP adreses.

Joprojām lielākā daļa kiberuzbrukumu tiek veikti, izmantojot publiski zināmas ievainojamības, tāpēc savlaicīga konfigurācijas nepilnību apzināšana un ievainojamību lāpīšana var būtiski uzlabot kiberdrošības situāciju.

2024. gada 3. ceturksnī konfigurācijas nepilnību TOP 10 saraksta augšgalā līderis 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.

Konfigurācijas nepilnību TOP 10



7. attēls. Top 10 Konfigurācijas nepilnības 2024. gada 3. ceturksnī

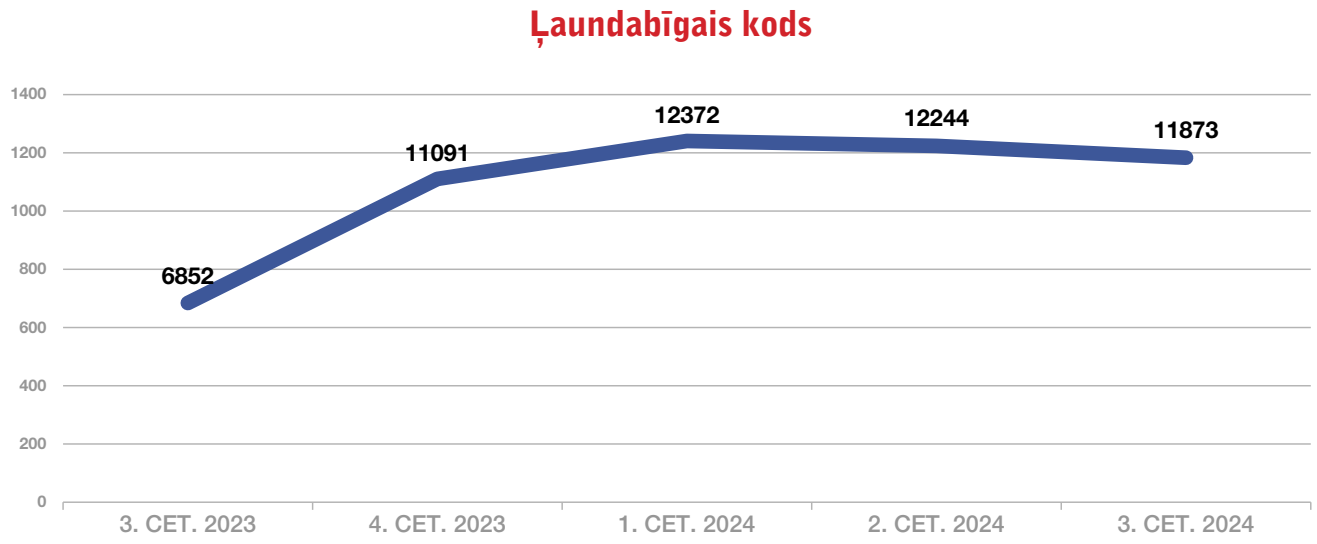
IETEIKUMI DROŠĪBAI

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

Apdraudēto unikālo IP adrešu skaits Latvijas kibertelpā joprojām saglabājas augsts. Lai gan ir neliels samazinājums salīdzinājumā ar iepriekšējo ceturksni, 73 % pieaugums salīdzinājumā ar 2023. gada 3. ceturksni liecina par ilgtermiņa pieaugumu ļaundabīga koda izplatībā.

Nelielais samazinājums attiecībā pret iepriekšējo ceturksni varētu norādīt uz īslaicīgu uzlabojumu vai efektīvākiem aizsardzības mehānismiem, taču kopējā tendence joprojām ir augoša.



8. attēls. Apdraudēto unikālo IP adrešu skaits

TOP 5 visbiežāk pielietotās metodes sistēmu uzlaušanai un inficēšanai

- Pikšķerēšanas e-pasta vēstules;
- 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;
- Nopludināti lietotāju piekļuves dati;
- Automatizētie uzbrukumi.

Galvenie ļaunatūras tipi

- Lietotāju datu zadzēji;
- *Bot-net* jeb botu tīkli;
- Izspiedējvīrusi;
- Attālinātās kontroles trojāni datu izgūšanai vai infrastruktūras kompromitēšanai.

Sociālā inženierija, izmantojot pikšķerēšanu, mudina lietotājus lejupielādēt ļaunprātīgu programmatūru. Arī tiešsaistes reklāmās iestrādāta ļaunprātīga programmatūra paplašina uzbrukuma laukumu. Turklāt kiberuzbrucēji joprojām izmanto tādas metodes kā ar paroli aizsargāti arhīvi un maldinošas HTML pikšķerēšanas lapas. Tā saucamie *watering-hole* uzbrukumi apdraud tīmekļa vietnes, lai inficētu apmeklētājus, un piegādes ķēdes uzbrukumi ir vērsti uz sadarbības partneriem, lai iefiltrētos lielākos tīklos. Lietotāju datu zadzēji un ļaunprātīgas programmatūras, kas izzog personas datus, kļūst arvien sarežģītākas un rada nopietnas bažas - šīs tendences, visticamāk, turpināsies.

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.

Dažkārt uzbrukumi ir oportūnistiski, un to mērķis ir dati vai infrastruktūra, kam ir vislielākā ietekme uz upuru darbību. Kibernoziedznieki var vai nu zagt tieši no cietušajiem upuriem, vai pelnīt ar informāciju, kas ir nozagta no cietušajiem. Turklāt kibernoziedznieki arvien vairāk savstarpēji sadarbojas organizētās grupās, padarot tās par spēku, ar ko jārēķinās.

Pikšķerēšana joprojām ir viņu iecienītākā metode, vienlaikus uzlabojot savas stratēģijas, izmantojot sociālos medijus un populāras e-pasta mārketinga platformas. Lai apietu korporatīvo aizsardzību, kibernoziedznieki arvien vairāk pievēršas sociālajiem medijiem un saziņas platformām, piemēram, "WhatsApp" vai "LinkedIn". Personīgie konti, kas parasti ir mazāk droši nekā korporatīvie, ir īpaši neaizsargāti. Visticamāk, šī pieeja turpināsies arī turpmāk.

Ļaunatūra – Izmanto ļaunprātīgiem mērķiem – tās var būt datorvīrusi, kas domāti datora nelikumīgai attālinātai administrēšanai, klaviatūras nolasītājprogrammas paroļu zagšanai, pikšķerēšanas programmas, spiegu programmas.

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. Ievērojami pieaudzis pret uzņēmumiem vērsto kiberuzbrukumu apjoms. Kompromitēti e-pasti vai lietotņu konti tiek aktīvi izmantoti, lai tālāk izplatītu ļaunatūras.

Salīdzinājumā ar 2. ceturksni, pikšķerēšanas e-pasta vēstulēs novērots paaugstināts kaitīgo pielikumu īpatsvars ar .html paplašinājumu, tostarp arī pikšķerēšanas shēmas, kur kaitīgajā pielikumā ir instrukcijas, kas mudina lietotāju izpildīt komandas, ielīmējot tās "Windows" *run* logā.

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

Izspiedējvīrusu uzbrukumi kļūst aizvien pārdrošāki un finansiāli graujošāki

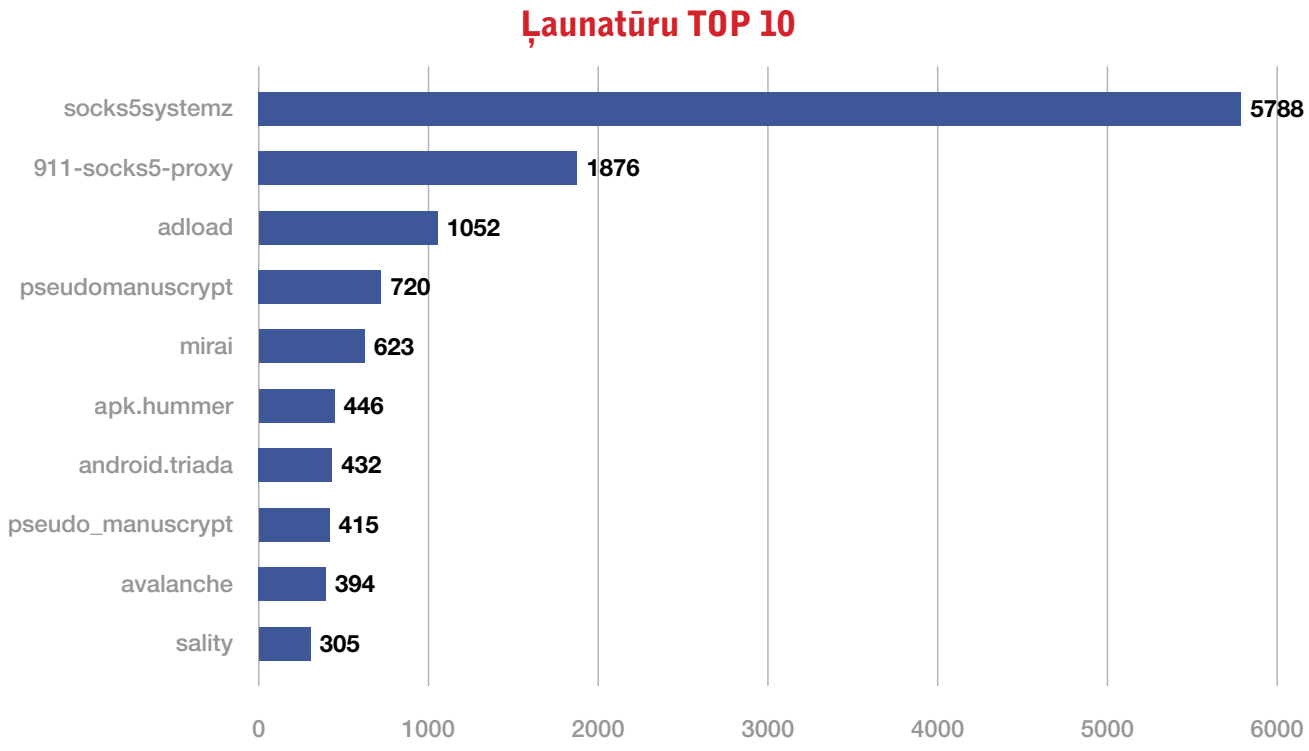
Pārskata periodā viens no lielākajiem Latvijas pārtikas ražošanas uzņēmumiem "Amber Beverages Group" piedzīvoja šifrējošā izspiedējvīrusa uzbrukumu, kas rezultējās uzņēmuma datu noplūdē. Par šo gadījumu Valsts policijā uzsākts kriminālprocess, CERT.LV turpina sniegt atbalstu.

Ļaunatūru TOP 10

2024. gada 3. ceturksnī ļaunatūru TOP 10 saraksta (9. attēls) 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.

Uz 2. vietu pakāpusies ļaunatūra 911-socks5-proxy, kas uz iekārtas lejupielādē kādu no šiem bezmaksas VPN rīkiem: *MaskVPN*, *DewVPN*, *PaladinVPN*, *ProxyGate*, *ShieldVPN* vai *ShineVPN*, papildus nokonfigurējot iekārtu par starpniekserveri (*proxy*). 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.

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

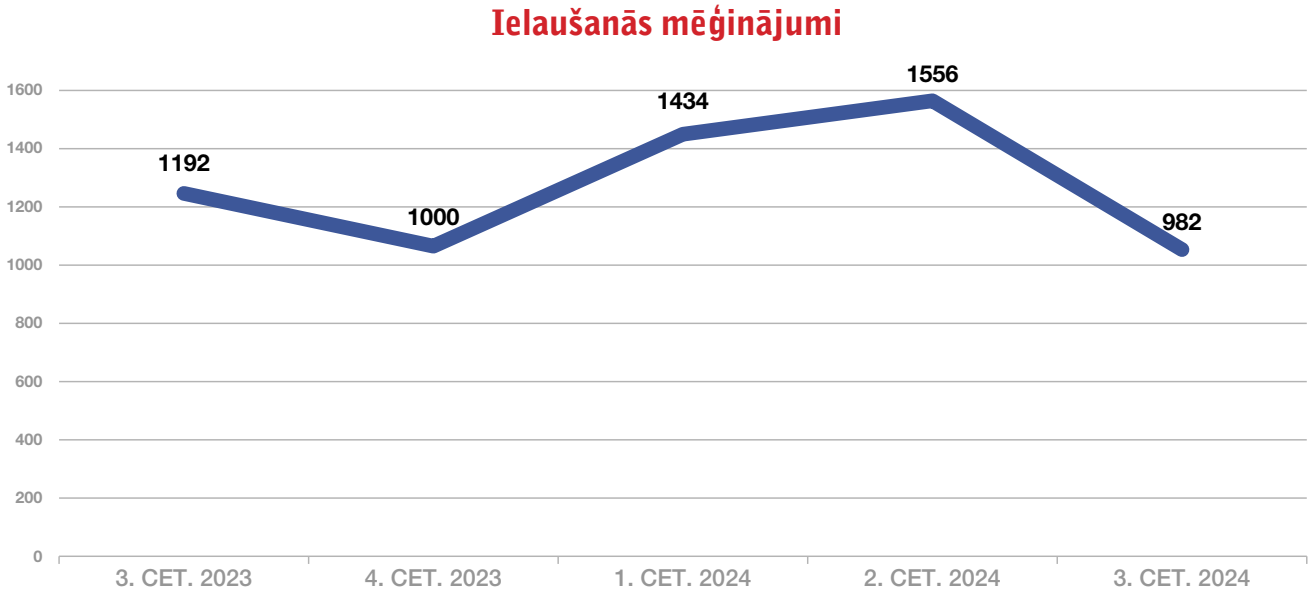


9. attēls. Apdraudēto unikālo IP adrešu skaits

CERT.LV aicina ziņot uz cert@cert.lv par kampaņveidīgām krāpnieciskām aktivitātēm un vietnēm, kas izplata vīrusus. Ļaunprātīgu kampaņu indikatori tiek operatīvi ievietoti DNS ugunsmūrī, pasargājot tā lietotājus no identificētajiem apdraudējumiem 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

2.5. Ielaušanās mēģinājumi

Pārskata periodā ielaušanās mēģinājumu skaita samazinājums par 37% salīdzinājumā ar 2. ceturksni liecina par uzlabotiem aizsardzības pasākumiem un efektīvāku reaģēšanu uz kiberapdraudējumiem. Samazinājums par 18% salīdzinājumā ar 2023. gada 2. ceturksni norāda uz ilgtermiņa uzlabojumiem kiberdrošības jomā.



10. attēls. Apdraudēto unikālo IP adrešu skaits

Lai gan iepriekšējā ceturksnī tika sasniegts augstākais rādītājs pēdējo divu gadu laikā, pašreizējais samazinājums varētu norādīt uz mainīgu apdraudējumu dinamiku un iespējamu uzbrukuma intensitātes samazināšanos.

Lielākajā daļā gadījumu tiek izmantota paroļu minēšana (*brute-force*) pret dažādiem elektronisko sakaru komersantiem, valsts un pašvaldību iestādēm, kā arī privāto sektoru.

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

Turklāt cilvēciskais faktors joprojām ir galvenais kiberdrošības risks, jo cilvēki ir viegli apmuļķojami ar, piemēram, pikšķerēšanas paņēmieniem, kas var apdraudēt citādi labi aizsargātas sistēmas.

Brutāls "mēstuļu" vilnis par viltus uzlaušanu

Augustā fiksētas apmēram 550 tūkstoši e-pasta vēstules, kas identificētas kā mēstules ar paziņojumu, ka mēstules saņēmēja operētājsistēma ir uzlauzta, visa informācija no iekārtas nokopēta uz kiberuzbrucēja serveriem un ka kiberuzbrucējam ir piekļuve upura e-pastiem, ziņojumapmaiņām, sociālajiem tīkliem, kontaktu sarakstam. Draudot sagraut upura dzīvi, kiberuzbrucējs pieprasa samaksāt 1 000 eiro (bitkoinu ekvivalentā pēc pārskaitījuma brīdī spēkā esošā valūtas kursa), lai dzēstu šo nozagto informāciju no uzbrucēja serveriem.

CERT.LV rīcībā nav informācijas, vai kāds būtu "uzķēries" un samaksājis. Tas ir krāpnieciska surogātpasta gadījums un personas dati nav tikuši izzagti.

Pikšķerēšanas e-pasta vēstules par pierakstīšanās darbību "Microsoft" kontā

Aktivizējušās "Microsoft" akreditācijas datu pikšķerēšanas, izmantojot ļaunprātīgu .html e-pasta vēstules pielikumu ar krāpniecisku pieteikšanās formu. Šīs pikšķerēšanas shēmas ir tik izsmalcinātas, ka pat visuzmanīgākais cilvēks var tikt apmānīts. Ja šādas e-pasta vēstules saņēmējs nav veicis šādu pierakstīšanos un neatpazīst minēto ierīci, visticamāk, viņa konts ir kompromitēts. CERT.LV mudina nekavējoties nomainīt kompromitēta konta paroli, izvēlēties pietiekami sarežģītu paroli, izmantojot paroļu pārvaldnieku, un uzstādīt divfaktoru autentifikāciju.
Visos gadījumos CERT.LV sniedza atbalstu un konsultācijas tālākai rīcībai.

IETEIKUMI DROŠĪBAI

1. Regulāri atjaunināt programmatūru.
2. Izmantot spēcīgas autentifikācijas metodes – ieviest divfaktoru (2FA), bet vēlams daudzfaktoru autentifikāciju (MFA) un nodrošināt stingru paroļu politiku.
3. Šifrēt sensitīvus datus gan pārsūtīšanas, gan 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 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. Apdraudēto unikālo IP adrešu skaita pieaugums par 267% salīdzinājumā ar pagājušā gada 3. ceturksni liecina par ievērojamu uzbrukumu skaita un intensitātes pieaugumu, ka tas ir redzams 2. attēlā. Uzbrukumi piegādes ķēdei joprojām ir drauds, kas tiek izmantots arī kā veids, kā nodot politisku vēstījumu.

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.

Visbiežāk sistēmu uzlaušana notiek, pielietojot šādas metodes:

- pikšķerēšanas e-pasta vēstules;
- publiski zināmas / jaunatklātas ievainojamības;
- eksponēti servisi – noklusējuma autentifikācijas piekļuves dati, paroļu uzlaušana ar pilno pārlasi, versiju ievainojamības;
- vāja paroļu pārvaldība un 2FA neesamība;
- piegādes ķēdes;
- automatizētie uzbrukumi;
- kompromitēti lietotāju sociālo tīklu konti.

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:

- 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/neeksistējoša lietotāju tiesību pārvaldība un izpildāmo failu politika.

Kompromitētas piegādes ķēdes

Līdzīgi kā aprīlī un maijā, tā arī septembrī tika ziņots par piegādes ķēžu kompromitēšanas uzbrukumu pret TV kanālu, kas tiek retranslēts Latvijā. Latvijas komunikāciju operatora "Balticom" interaktīvās televīzijas saturā 20. septembrī uz dažām minūtēm parādījies kiberuzbrucēju sagatavots videomateriāls. Sākotnējā izmeklēšana liecina, ka noticis kiberuzbrukums starpnieka pakalpojumu sniedzēja serveriem ārpus Latvijas. Pēc "Balticom" aplēsēm, iespējams, tika ietekmēti aptuveni 2% "Balticom" interaktīvās televīzijas klientu.

CERT.LV atgādina, ka šis ir jau otrais šāda veida uzbrukums tam pašam satura piegādātājam, kas ietekmēja "Balticom" saturu arī šī gada 9. maijā, un ir uzskatāms, ka atkārtoti notikusi pakalpojuma piegādes ķēdes kompromitēšana, un šis starpnieks nav ieviesis preventīvus pasākumus, tāpēc būtu jāvērtē viņa uzticamība.

Kompromitētas tīmekļvietnes

Pārskata periodā lielā skaitā tika saņemti ziņojumi par kompromitētām tīmekļvietnēm. Piemēram, septembrī kiberuzbrucēji uzlauza kāda Latvijas futbola kluba vietni un nopublicēja tajā kaitīgu saturu, tostarp Krievijas karogu un Prigožina attēlu. Tāpat septembrī, kad tika konstatēts, ka piekļuvi vairāku reģionālo mediju administratoru kontiem ieguvusi kāda kibernoziedznieku grupa, CERT.LV sazinājās ar attiecīgo reģionālo mediju administratoriem, informējot par notikušo un iesakot veikt infrastruktūras uzlabojumus, lai novērstu radušos apdraudējumu. Uzbrukuma iespējamais

mērķis varēja būt gan datu izgūšana, gan nepatiesa un izķēmota satura izvietošana, abi šie iznākumi vērtējami kā bīstami reģionālajai drošībai.

Kompromitēti konti

Pārskata periodā, it īpaši septembrī, aktivizējušās paroļu pikšķerēšanas kampaņas "DocuSign" un "Office 365" vārdā. Kiberuzbrucēji caur krāpnieciskām e-pasta vēstulēm aicina potenciālos upurus atkārtoti aktivizēt savus kontus. Ļaundaru mērķis – iegūt upuru e-pasta piekļuves datus, lai pēc tam izsūtītu jaunas krāpnieciskās e-pasta vēstules.

Visos gadījumos CERT.LV sniedza atbalstu un konsultācijas tālākai rīcībai.

IETEIKUMI DROŠĪBAI

1. **Veikt paroļu uzglabāšanu šifrētā veidā**, piemēram, izmantojot paroļu pārvaldnieku.
2. **Izmantot divu faktoru autentifikāciju visur**, kur vien tas iespējams.
3. Saņemot e-pasta vēstules 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, **regulāri monitorēt 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 ļaundabīgos 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. **Lai aizsargātu piegādes ķēdes** no potenciālajiem draudiem, **rūpīgi pārbaudīt un izvērtēt**, vai **starpniekpakalpojuma** sniedzējs uztur augstu **kiberdrošības līmeni**, kā arī turpmāk veikt regulāru uzraudzību.
10. **Izmantot efektīvu aktīvo aizsardzību – DNS ugunsmūri** (https://dnsmuris.lv/), lai pasargātu no ļaunprātīgu vietņu apmeklēšanas.
11. **Plānot un organizēt regulāras darbinieku apmācības un zināšanu pārbaudi** vismaz reizi gadā. Regulāri informēt darbiniekus par biežāk iespējamajiem kiberapdraudējumiem.
12. **Ieteicams sekot līdzi CERT.LV sociālo mediju kontiem un vietnei cert.lv**, kur atradīsiet informāciju par aktualitātēm kiberdrošības jomā.

3. Kiberapdraudējumu prevencija

3.1. DNS ugunsmūris: aktīvā aizsardzība

Latvijā regulāri notiek kampaņveidīgas krāpnieciskas 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, pasargājot tā lietotājus no identificētajiem apdraudējumiem 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.

Līdz ar jaunā NKDL stāšanos spēkā 2024. gada 1. septembrī elektronisko sakaru komersantiem (ESK) ir obligāti jāizmanto CERT.LV nodrošinātais DNS ugunsmūris, kas automātiski bloķē kaitīgus un bīstamus interneta resursus. Līdz šā gada 1. septembrim daļa no ESK DNS ugunsmūri lietoja brīvprātīgi, bet tagad pasargāti tiks visi Latvijas interneta lietotāji centralizēti.

DNS ugunsmūris
Lietotāju 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 DNS ugunsmūra pakalpojuma ietvaros –

- **vairāk nekā 1 miljons apstrādāto pieprasījumu;**
- **aptuveni 103 414 reizes lietotāji pasargāti no ļaunprātīgu vietņu apmeklēšanas.**

Pēdējo divu gadu laikā pakalpojuma lietošana pieaugusi 5 reizes.

Nozīmīgākās aktīvās aizsardzības epizodes pārskata periodā

Brīdinājumi	Skaits
Par viltus elektroniskās deklarēšanas sistēmas (EDS) lapu aktivitātēm	**2 637**
Par "Latvijas Pasts" tēla izmantošanu viltus vietnes kampaņās	**1484**
Par *AgentTesla* ļaunatūru	**435**
Par Balada ļaunatūru, kas bija atrodama inficētās mājaslapās	**232**

CERT.LV piedāvā iespēju uzņēmumiem un iestādēm, 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. Ar papildu informāciju par RPZ var iepazīties šeit: https://cert.lv/lv/elektronisko-sakaru-komersantiem/sadarbiba-ar-cert-lv#dnsrpz

Par krāpnieku aktivitātēm un ļaundabīgām vietnēm CERT.LV aicina nekavējoties informēt Valsts policiju (https://www.vp.gov.lv/lv/ka-zinot-policijai), kā arī pārsūtīt kaitīgās e-pasta vēstules uz cert@cert.lv

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.

CERT.LV turpina ABS sistēmas uzturēšanu un paplašināšanu. Tāpat tika pilnveidota sensoru programmu nodrošinājuma darbība.

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

ABS ik mēnesi fiksē vidēji **6 000 augstas prioritātes** (ar augstu bīstamības potenciālu) incidentus valsts, pašvaldību un IKT kritiskās infrastruktūras iestādēs.

3. ceturksnī ABS ģenerēto brīdinājumu skaits kopskaitā bija aptuveni **1,83 miljardi**, kas ir par aptuveni **26% vairāk** nekā 2. ceturksnī.

Nozīmīgāko ABS ģenerēto brīdinājumu skaits pa CERT.LV signatūru grupām

Apdraudējumi	Jūlijs	Aug.	Sept.
Ar datorvīrusiem saistīti brīdinājumi	15 549	17 319	69 469
Ar pikšķerēšanu saistīti brīdinājumi	234 536	266 525	231 007
Ar potenciāli ļaunprātīgām vietnēm saistīti brīdinājumi	4 616	10 031	4 564
Ar robottīklu, krāpšanām, vīrusu indikatoriem saistīti brīdinājumi	1 595	2 481	867

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

3.3. Drošības operāciju centrs (SOC)

CERT.LV SOC pakalpojums centralizēti apkopo drošības telemetriju no klienta infrastruktūras, korelē notikumus klienta infrastruktūrā ar visu CERT.LV pieejamo apdraudējumu indikatoru un zināšanu kopu, lai savlaicīgi identificētu, brīdinātu, apturētu kiberapdraudējumu vai kiberincidentu un novērstu tā kaitējumu.

Drošības operāciju Centrs (SOC)
Aktīva un individuāli pielāgota kiberdrošības uzraudzība reāllaikā, lai identificētu, izmeklētu, novērstu apdraudējumus un kiberincidentus 24/7 režīmā.

Plašāk: https://cert.lv/lv/pakalpojumi

CERT.LV SOC pakalpojums piedāvā dažādas būtiskas priekšrocības, piemēram, klienta drošības telemetrijas datu apstrādi un īslaicīgu uzglabāšanu CERT.LV infrastruktūrā, Latvijas teritorijā.

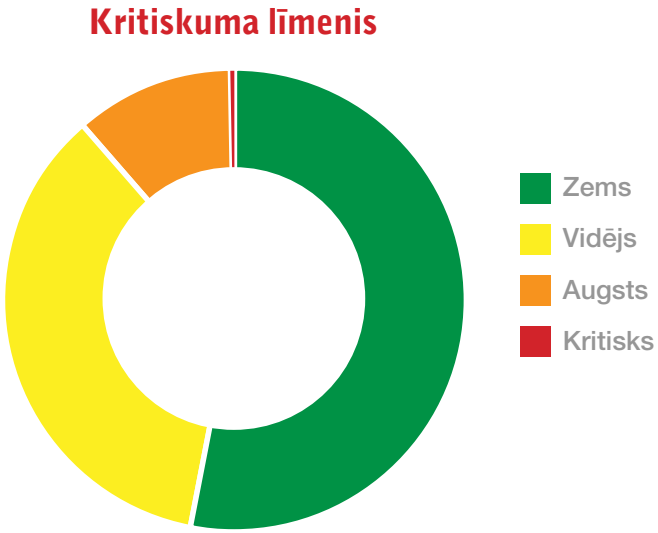
CERT.LV SOC klientiem ir nodrošināta:

- efektīva, centralizēta uzraudzība un iegūta pārredzamība 24/7 režīmā;
- operatīvi pamanīti un novērsti aktuālie kiberapdraudējumi;
- automatizēta aktīvā aizsardzība un prevencija;
- kiberincidentu izmeklēšana CERT.LV komandas vadībā;
- ērta piekļuve informācijas panelim un sekošana līdzi trauksmju ziņojumiem;
- ieteikumi un labā prakse infrastruktūras noturības stiprināšanai.

Uz pārskata beigām SOC reģistrēti drošības telemetrijas trauksmes ziņojumi vairāk nekā 46 000. Reģistrēto ziņojumu sadalījums kritiskuma līmeņos:

- Zems: **vairāk nekā 24 000**
- Vidējs: **vairāk nekā 16 000**
- Augsts: **vairāk nekā 5 000**
- Kritisks: **104**

Turpinās mērķtiecīgi uzsāktās aktivitātes CERT.LV SOC pakalpojumu attīstīšanā un jaunu klientu piesaistē, paplašinot subjektu loku atbilstoši NKDL, it īpaši veicinot sadarbību ar būtisko un svarīgo pakalpojumu sniedzējiem, lai sekmētu efektīvāku aizsardzību pret kiberdraudiem. CERT.LV aicina rakstīt uz cert@cert.lv un informēt par vēlmi izmantot SOC pakalpojumu.



11. attēls. SOC reģistrēto ziņojumu sadalījums

3.4. 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 veidā tika izsūtīti paziņojumi/brīdinājumi par 16 jaunatklātām kritiskām ievainojamībām, sniedzot koordinētus norādījumus par atjauninājumiem un mudinot tos nekavējoties veikt. Ar būtiskāko CVE ievainojamību apkopojumu un analīzi, kas atklātas 3. ceturksnī, var iepazīties šīs atskaites 2.3. sadaļā.

Informācija par jaunatklātiem apdraudējumiem un ievainojamībām tiek publicēta CERT.LV tīmekļa vietnē un 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 speciālistiem kiberdrošības kopienā.

3.5. Koordinēta ievainojamību atklāšana (CVD)

CERT.LV turpināja darbu pie CVD ziņojumu reģistrēšanas platformas cvd.cert.lv 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. Platformā tiek reģistrēti ievainojamību ziņojumi un 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, tādējādi efektīvāk organizējot pasākumus Latvijas kibertelpas aizsardzībai.

2024. gada 3. ceturksnī CVD platformā pieauga gan drošības pētnieku skaits, gan platformā reģistrēto ievainojamību ziņojumu skaits.

Turpinās darbs pie CVD pētnieku reitinga un profila informācijas pārvaldīšanas iespēju ieviešanas. 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.

Koordinēta ievainojamību atklāšana
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/

Uz pārskata perioda beigām platformā reģistrēti:

- drošības pētnieki: 69 (+3)
- aktīvas iestāžu programmas: 10
- ievainojamību ziņojumi: 94 (+12), tostarp CERT.LV klientūras ievainojamības: 50 (+6), uz konkrētām iestāžu programmām reģistrētās ievainojamības: 44 (+6)

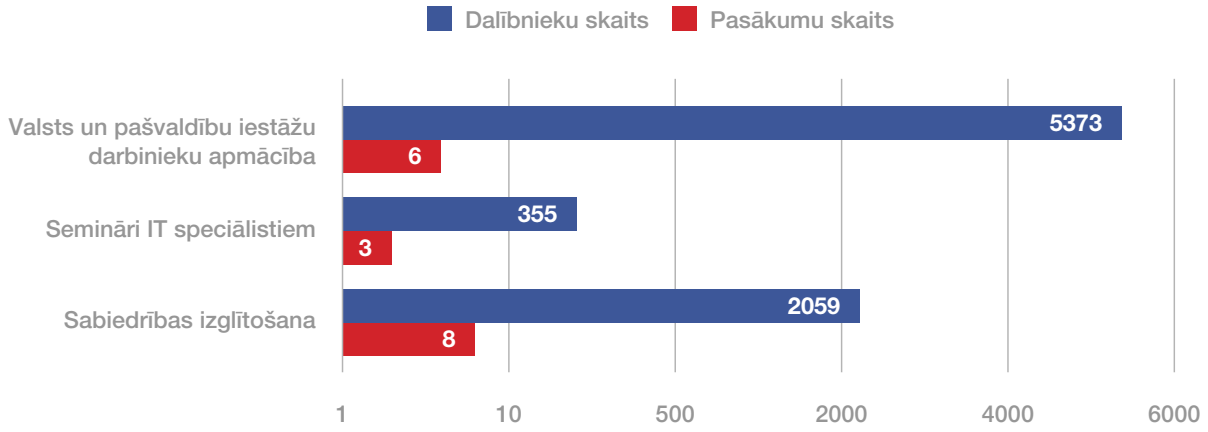
4. Komunikācija ar sabiedrību

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 3. ceturksnī CERT.LV īstenoja 17 izglītojošus pasākumus par IT drošību un aktualitātēm, apmācot kopskaitā 7 787 dalībniekus visā Latvijā.

Izglītojošo pasākumu un apmācīto personu skaits



12. attēls. Izglītojošo pasākumu un apmācīto personu skaits 2024. gada 3. ceturksnī

Jāatzīmē, ka pārskata periodā saņemts rekordliels dalībnieku pieteikumu skaits dalībai CERT.LV organizētajos tiešsaistes semināros "Kiberhigiēnas pamati publiskās pārvaldes darbiniekiem", ko vada CERT.LV kiberdrošības eksperts Mārtiņš Vecstaudžs. Tas liecina par vairākiem svarīgiem aspektiem. Pieaugoša interese liecina, ka publiskās pārvaldes darbinieki arvien vairāk apzinās kiberdrošības nozīmi un vēlas pilnveidot savas zināšanas, lai pasargātu savas organizācijas no kiberapdraudējumiem. Dalībnieku skaita pieaugums norāda arī uz uzticēšanos CERT.LV ekspertiem un to spējai nodrošināt kvalitatīvu un noderīgu apmācību semināru.

CERT.LV sniedza atbalstu Aizsardzības ministrijai informatīvo semināru organizēšanā to nozaru pārstāvjiem, kuru darbība tiek pakļauta jaunā Nacionālās kiberdrošības likuma (NDKL) regulējumam. Pārskata periodā sektorālie semināri tika organizēti telekomunikāciju un IKT, enerģētikas, ūdensapgādes, transporta, medicīnas un farmācijas, pārtikas ražošanas un vairumtirdzniecības, pasta, kurjerpakalpojumu, atkritumu apsaimniekošanas un citu nozaru, kā arī valsts pārvaldes un pašvaldību pārstāvjiem.

Praktiskās (*table top*) mācības par kiberdrošības incidentu izmeklēšanu

CERT.LV turpina savai klientūrai nodrošināt praktisku kiberincidenta izmeklēšanas izspēli, kur tās 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 trīs organizācijās:

- **12. jūlijā** – "Cyber Hack Summer School" sadarbībā ar Rīgas tehnisko universitāti
- **19. augustā** – uzņēmums "Schneider Electric"
- **17. septembrī** – NVO "LAPA"

Kopskaitā CERT.LV organizētajā kiberdrošības incidenta izmeklēšanas izspēlē un lekcijā piedalījās 33 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.

Būtiskāko pasākumu apskats pārskata periodā

6. jūlijā ikgadējā sarunu festivāla "Lampa" ietvaros Aizsardzības ministrijas organizētājā diskusijā "Vai esam gatavi kiberkaram?" ar savu redzējumu dalījās CERT.LV eksperts Kārlis Svilans.
Ieraksts: festivalslampa.lv

8. jūlijā EIT Digital Summer School "Cyber Security – Agile Methology for Developing New Solutions" ietvaros ar prezentāciju "Cybersecurity Trends, Threats and Solutions" uzstājās CERT.LV eksperte Dana Ludviga.

12. septembrī ESET organizētajā konferencē "Security Day" CERT.LV eksperte Dana Ludviga dalījās ar spilgtu stāstu par Latvijas kibertelpas noturības stiprināšanas stūrakmeņiem.

19. septembrī LVRTC organizētās "Kibernakts 2024" ietvaros ar saistošu prezentāciju "Latvijas kibertelpas noturības stiprināšanas stūrakmeņi" svarīgākos kiberdrošības izaicinājumus un risinājumus izklāstīja CERT.LV vadītāja Baiba Kaškina.
Ieraksts: lvrtc.lv/kibernakts-2024

25. septembrī tiešsaistes seminārā "Kiberhigiēna izglītības iestādēs" ar vadlīnijām un praktiskiem ieteikumiem dalījās CERT.LV eksperts Mārtiņš Vecstaudžs.

26. septembrī SIA "Tet" kiberdrošības forumā "CyberShield 2024" ar prezentāciju "Kiberkrīzes rīcības plāns: No draudiem līdz risinājumiem" uzstājās CERT.LV eksperts Kārlis Svilans.
Ieraksts: CyberShield 2024

26. septembrī SIA "Opticom" IT drošības profesionāļiem organizētās konferences "Latvijas datortīklu skola" ietvaros ar prezentāciju "Vai ir dzīve pēc NKDL stāšanās spēkā?" uzstājās CERT.LV eksperte Sanita Vītola.

26. septembrī divos tiešsaistes semināros Valsts policijas koledžai Starptautiskās profesionāļu nedēļas ietvaros ar praktiskiem kiberhigiēnas ieteikumiem dalījās CERT.LV eksperts Mārtiņš Vecstaudžs, savukārt padziļināti tehnisko prezentāciju – "Datori mums apkārt un informācijas iegūšana no tiem" – sniedza CERT.LV eksperts Gints Mālkalnietis.

27. septembrī tiešsaistes seminārā "Kiberhigiēnas pamati publiskās pārvaldes darbiniekiem" ar vadlīnijām un praktiskiem ieteikumiem dalījās CERT.LV eksperts Mārtiņš Vecstaudžs.

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.

Informācija par CERT.LV sadarbību ar medijiem

Pārskata perioda jūlija mēnesī liela mediju interese bija par globālajiem IT traucējumiem, kas saistīti ar ASV kiberdrošības uzņēmuma "CrowdStrike" radītajām problēmām. Pastiprināta interese bija par viltus "Smart-ID" e-pasta vēstulēm, Latvijas Nacionālās bibliotēkas datu centra darbības traucējumiem un par iedzīvotāju iniciatīvas vietnē manabalss.lv sākto parakstu vākšanu par mobilās lietotnes "TikTok" bloķēšanu. Tāpat uzmanību piesaistīja CERT.LV ekspertu komentāri par krāpnieku metodēm ceļojumu sezonā, kam jāpievērš uzmanība un no kā jāuzmanās.

Augustā mediju vislielāko interesi izraisīja aktuālā situācija Latvijas kibertelpā saistībā ar valsts mērogā novērotiem intensīviem pakalpojumatteices uzbrukumiem valsts sektora un transporta nozares interneta resursiem, kā arī atsevišķiem resursiem privātajā sektorā. Pastiprināta interese bija arī par krāpnieku aktivitātēm, it īpaši krāpnieciskiem zvaniem.

Kopskaitā 3. ceturksnī ar 393 publikācijām plašsaziņas līdzekļos potenciālais skatījumu skaits – 12,9 miljoni.

Ar NKDL stāšanos spēkā 1. septembrī nozīmīga uzmanība tika pievērsta izmaiņām un prasībām, ko paredz jaunais regulējums.

CERT.LV turpina tulkot un portālā www.esidross.lv publicēt "OUCH!" ikmēneša izdevumus (informācijas drošības biļetens, ko sagatavo SANS institūts). Pārskata periodā publicētie raksti:

- Teksta ziņojumapmaiņas uzbrukumi: Smikšķerēšanas sāga OUCH! 07/2024
- Sargājiet savu sirdi (un maku) no romantiskās krāpšanas OUCH! 08/2024
- Kas jāzina par drošību, baudot atpūtu?
- Iedomātās balsis: aizsardzība pret balss klonēšanas uzbrukumiem OUCH! 09/2024

Ikmēneša "KiberLaikapstākļi" apskats

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

- **Jūlijs:** https://cert.lv/lv/2024/08/kiberlaikapstakli-2024-julijs
- **Augusts:** https://cert.lv/lv/2024/09/kiberlaikapstakli-2024-augusts
- **Septembris:** https://cert.lv/lv/2024/10/kiberlaikapstakli-2024-septembris

5. Stratēģiskā sadarbība Latvijā

CERT.LV speciālisti savas kompetences ietvaros piedalās Nacionālās kiberdrošības stratēģijas uzdevumu īstenošanā un normatīvo dokumentu izstrādes procesā, cieši sadarbojoties ar Latvijas Republikas Aizsardzības ministrijas Kiberdrošības politikas departamentu.

CERT.LV piedalās Nacionālās informācijas tehnoloģiju (IT) drošības padomes darbā, kuras mērķis ir koordinēt ar IT drošību saistīto uzdevumu un pasākumu plānošanu un veikšanu.

Turpinās cieša sadarbība ar LR Zemessardzes Kiberaizsardzības vienību, kas IT drošības krīzes vai apdraudējuma situācijā sadarbībā ar CERT.LV sniedz atbalstu valsts un privātajam sektoram.

CERT.LV turpina organizēt IT un IS drošības ekspertu grupas (DEG) ikmēneša sanāksmes ar mērķi veicināt kiberdrošību, sekmēt kiberdrošības apziņas kultūru Latvijā un sniegt atbalstu CERT.LV. Sanāksmes notiek katra mēneša otrajā ceturtdienā.

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 pārskatu detalizētāk skatīt 7. nodaļā.

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 veicot Latvijas uzticamības saraksta (LV TSL – LV trust list) uzturēšanu.

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

Ieguldījums kiberdrošības rīcībpolitikas attīstībā

Lai stiprinātu kiberdrošību Latvijā un ieviestu pārskatītās Eiropas Savienības Tīklu un informācijas sistēmu drošības direktīvas (NIS2) prasības, 1. septembrī spēkā stājās Nacionālās kiberdrošības likums (NKDL).

Darbu uzsāka arī jauna institūcija – Nacionālais kiberdrošības centrs – kas darbosies kā vienotais kontaktpunkts kiberdrošības jautājumos un veiks nacionālo kiberdrošības prasību ieviešanas pārraudzību, kā arī izstrādās nacionālās kiberdrošības rīcībpolitikas iniciatīvas. Centra funkcijas īstenos Aizsardzības ministrija sadarbībā ar CERT.LV, savukārt IKT kritiskās infrastruktūras uzraudzības iestāde būs Satversmes aizsardzības birojs.

Saistībā ar NKDL ieviešanu pārskata periodā tika veikti sagatavošanās pasākumi, lai CERT.LV būtu gatava jauno uzdevumu izpildei, kad tiks uzsākta NIS2 direktīvas piemērošana un stāsies spēkā jaunais regulējums. Tiek īstenota CERT.LV iekšējās un ārējās dokumentācijas pielāgošana un citu sagatavošanās pasākumu veikšana.

2024. gada 1. septembrī spēkā stājās Nacionālās kiberdrošības likums

https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums

CERT.LV turpina dot vērtīgu ieguldījumu nozares politikas pamatnoteikumu sagatavošanā. Turpinās darbs pie jauno normatīvo aktu skaidrošanas un vadlīniju sagatavošanas, lai atbalstītu NKDL subjektus jauno prasību ieviešanā.

Pārskata periodā tika veikta likumprojektu/iniciatīvu izskatīšana, tostarp viens ES un 15 Latvijas līmeņa likumprojekti, kā arī organizētas sanāksmes ar Latvijas līmeņa likumprojektu virzītājiem atsevišķu problēmjautājumu vai komentāru pārrunāšanai.

Turpinās aktīva 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.

5.1. Atbalsts kibernoziedzības novēršanā un apkarošanā

5.1.1. 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. CERT.LV aktīvi veic IT drošības apdraudējumu agrās brīdināšanas sistēmu (ABS) un DNS RPZ uzstādīšanu iestādēs un uzņēmumos, lai veicinātu ātrāku IKT kritiskās infrastruktūras apdraudējumu identificēšanu un efektīvāku to novēršanu.

Pārskata periodā tika turpināts darbs pie CERT.LV pakalpojumu ietvara pilnveidošanas, gan izstrādājot jaunus risinājumus pakalpojumu sniegšanai, gan pilnveidojot ar šo pakalpojumu sniegšanu saistītās procedūras.

Jaunā NKDL subjektiem CERT.LV piedāvā plašu pakalpojumu klāstu, tostarp:

- Kiberdrošības incidentu risināšana un atbalsts 24/7 režīmā;
- Agrās brīdināšanas sistēmas;
- DNS ugunsmūris;
- Koordinēta ievainojamību atklāšana;
- Pikšķerēšanas uzbrukumu simulācijas;
- Kiberdrošības draudu medības;
- Kiberapdraudējumu simulācijas;
- CERT.LV MISP – ar ļaunatūru saistītās informācijas apmaiņas platforma;
- CERT.LV Drošības operāciju centrs (SOC);
- Industriālās automatizācijas un vadības sistēmu drošības laboratorijas pakalpojums.

Lai veicinātu industriālās automatizācijas un kontroles sistēmu drošību, CERT.LV piedāvā industriālās automatizācijas un vadības sistēmu drošības laboratorijas pakalpojumu, kas paredzēts operacionālo tehnoloģiju (OT) 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.

Pēdējos gados CERT.LV novēro arvien lielāku uzbrukumu skaitu, kuru mērķis ir kompromitēt industriālās ražošanas sistēmas. Piemēram, CERT.LV saskārās ar situāciju, kad kiberuzbrukumu piedzīvoja kāds liels lauksaimnieks. Viņa saimniecībā nebija pietiekami pasargāta graudu kaltes automatizācijas sistēma un šķietami ar Krieviju saistīti ļaundari piekļuva tai, izmainīja parametrus un graudi sāka degt. Tā kā šeit bija runa par daudzu desmitu tonnu graudu sabojāšanu, tā ir būtiska problēma ne tikai konkrētajam lauksaimniekam, bet pat nacionālā līmenī. Turklāt šāda veida riski skar arī dažāda veida enerģētikas un transporta uzņēmumus. Tāpēc CERT.LV piedāvā pakalpojumu – industriālās automatizācijas un vadības sistēmu drošības laboratoriju, lai veiktu drošības testus uz reālām ierīcēm un sniegtu atbalstu nozaru uzņēmumiem.

Saskaņā ar ASV Kiberdrošības un infrastruktūras drošības aģentūras (CISA) šogad publicēto brīdinājumu[1], OT resursi joprojām ir prokrievisko haktīvistu prioritārais mērķis. Lai gan pašreizējās darbības galvenokārt ietver nesarežģītas metodes ar ierobežotu ietekmi uz iekārtām, CISA veiktā izmeklēšana liecina, ka šiem uzbrucējiem piemīt spējas, kas varētu radīt fiziskus draudus nedrošām un nepareizi konfigurētām OT vidēm. Ņemot vērā, ka pašreizējā konfrontācijas situācija starp Krieviju un Eiropas Savienības valstīm, visticamāk, saglabāsies arī tuvākajā un vidējā termiņā, OT operatoriem ieteicams īstenot drošības paraugpraksi, piemēram, ieviest daudzfaktoru autentifikāciju OT tīklos un atvienot visas cilvēka un mašīnas saskarnes (HMI) no publiski pieejamā interneta.

CERT.LV iesaka kritiskās infrastruktūras organizācijām ieviest lietotāju uzvedības analītiku, lai automātiski atklātu uzvedības anomālijas tīklos, ierīcēs vai kontos. Uzvedības analītika ir būtiska ļaunprātīgu dalībnieku atklāšanai, kas bieži vien izmanto LOTL tehnikas. Tā sauktā "*living off the land*" (LOTL) tehnika ļauj uzbrucējam veikt ļaunprātīgas darbības, izmantojot rīkus vai programmas mērķa vidē, un izvairīties no atklāšanas. Valstu atbalstīti grupējumi, piemēram, *Volt Tyhoon*, bieži vien izmanto LOTL tehnikas informācijas vākšanai.

Izmantojot CERT.LV SOC pakalpojuma aizsardzības risinājumus, var atklāt anomālas darbības, salīdzinot notikumu žurnālus ar ikdienas darbībām. Organizācijām būtu jāapsver arī draudu medību operācijas kā proaktīvi pasākumi, lai atklātu ļaunprātīgus dalībniekus, kas izmanto LOTL tehniku.

5.1.2. Atbalsts Latvijas valsts tiesībsargājošajām iestādēm

Pārskata periodā CERT.LV sniedza atbalstu Latvijas valsts tiesībsargājošajām iestādēm izmeklēšanā, veicot padziļinātu izpēti un sagatavojot atbildes Valsts policijai par vairākiem kiberincidentiem. Būtiskākais bija augusta beigās, kad "Amber Beverages Group" – viens no lielākajiem Latvijas pārtikas ražošanas uzņēmumiem – piedzīvoja kiberuzbrukumu, kura laikā tika nošifrēta uzņēmuma IKT infrastruktūra.

Sniedzot atbalstu tiesībsargājošām iestādēm, CERT.LV speciālisti savas kompetences jomā veic ekspertīzi un sniedz komentārus par incidentos iesaistītajām IP adresēm un ar tām saistītajiem potenciālajiem apdraudējumiem, veic incidentos iesaistīto iekārtu analīzi, kā arī sniedz atzinumus pēc programmatūru izvērtējuma.

CERT.LV akcentē nepieciešamību turpināt Latvijas sabiedrības izpratnes vecināšanu par kibertelpu un kibernoziegumu riskiem tajā, lai stiprinātu sabiedrības noturību pret kiberzubrukumiem, mazinātu to ietekmi un sekmētu to novēršanu.

Īpaša uzmanība ir jāpievērš preventīvām metodēm un iniciatīvām, kas ļautu bloķēt ar noziedzīgu mērķi radītas vai noziedzīgām darbībām izmantotas interneta vietnes, turpinot pilnveidot arī iesaistīto institūciju sadarbību un atbildīgo institūciju reaģēšanas ātrumu.

5.1.3. Drošības testi

IT drošības testi

CERT.LV RedTeam, veicot 14 liela apjoma IT drošības testus, atklāja un novērsa vairākas būtiskas ievainojamības kritiskās infrastruktūras un pakalpojumu nodrošināšanas organizācijās, kā arī trenēja šo organizāciju darbinieku kiberhigiēnas prasmes.

Pārskata periodā CERT.LV RedTeam ir veikusi:

- Drošības testus – 14
- Pikšķerēšanas uzbrukumu simulēšanas kampaņas – 3
- Kiberapdraudējumu simulācijas – 1

1. https://www.cisa.gov/sites/default/files/2024-05/defending-ot-operations-against-ongoing-pro-russia-hacktivist-activity-508c.pdf

Pikšķerēšanas uzbrukumu simulācijas kampaņas

Perioda laikā tika veiktas kopskaitā 3 pikšķerēšanas uzbrukumu simulācijas kampaņas – vienai pašvaldībai un divām valsts iestādēm – kampaņas beigās visām trim iestādēm nosūtītas atskaites ar rezultātiem un ieteikumiem darbinieku izglītošanai.

CERT.LV piedāvā pikšķerēšanas uzbrukumu simulācijas pakalpojumu, lai uzlabotu iestāžu darbinieku digitālo drošību un pratību. Ar CERT.LV pakalpojuma palīdzību organizācijas var simulēt pielāgotus un reālus pikšķerēšanas uzbrukumus, lai apmācītu un veicinātu personāla spējas identificēt potenciāli riskantus uzvedības modeļus, atpazīt un novērst kiberapdraudējumus un informācijas noplūdi. Šis pakalpojums palīdzēs stiprināt organizāciju aizsardzību pret sociālās inženierijas uzbrukumiem, tādā veidā mazinot cilvēciskā faktora riskus. CERT.LV aicina rakstīt uz cert@cert.lv un informēt par vēlmi saņemt pakalpojumu.

Kiberapdraudējumu simulācija

Pārskata periodā kiberapdraudējumu simulācijas ietvaros tika identificēta viena augsta riska konfigurācijas nepilnība, kas ļāva uzbrucējiem izpildīt patvaļīgus failus uz kādas organizācijas standarta darbinieka gala iekārtas un viena vidēja riska nepilnība, kas daļēji ļāva apiet starpniekservera iestatījumus.

Tāpat drošības testi tika veikti vairākām valsts sektora sistēmām. 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.

CERT.LV piedāvā kiberuzbrucēju rīku, metožu un darbību simulāciju iestādes kiberdraudu identificēšanas spēju pārbaudei un pilnveidošanai. Pakalpojums ietver arī SOC (*Security Operations Center*) / SIEM (*Security Information and Event Management*) / EDR (*Endpoint Detection and Response*) / XDR (*Extended Detection and Response*) /MDR (*Managed Detection and Response*) spēju, procedūru, tvēruma, kvalitātes un reakcijas testus. CERT.LV aicina rakstīt uz cert@cert.lv un informēt par vēlmi saņemt pakalpojumu.

5.1.4. Kiberdrošības draudu medību operācijas

Līdz pārskata beigām kiberdrošības draudu medību operācijās analīze jau veikta:

- **vairāk nekā 140 000 gala iekārtās.**
- **kopskaitā 31 publiskā sektora iestādē un IKT kritiskās infrastruktūras uzņēmumā.**

CERT.LV ir līdere kiberdrošības draudu medību operāciju vadīšanā Eiropas Savienībā. Proaktīva kiberuzbrucēju klātbūtnes identificēšana jeb draudu medību operācijas tiek veiktas kopš 2022. gada ar mērķi identificēt kiberapdraudējumu klātbūtni Latvijai svarīgās IKT infrastruktūras sistēmās.

Aptuveni **25% jeb 8 organizāciju iekārtās tika identificēta ārvalstu APT klātbūtne** (tostarp Krievijas un Ķīnas atbalstītu politiski motivētu un citu komerciāli motivētu kiberuzbrucēju), **kas veiksmīgi neitralizēta**. Atklāti arī citi būtiski apdraudējumi, kurus mērķa organizācijām, pateicoties saņemtajām atskaitēm pēc draudu medību noslēgšanās, bija iespēja novērst, pieņemot datos balstītus lēmumus.

CERT.LV gan atsevišķi, gan kopā ar sadarbības partneru apvienoto komandu darbojas iepriekš izvēlētā informācijas sistēmu tīklā (mērķa iestādes izvēle tiek izvērtēta sadarbībā ar valsts drošības iestādēm), lai identificētu uzbrucēja klātbūtni, atklātu, uzraudzītu un analizētu ļaunprātīgas darbības, kā arī lai analizētu uzbrukumu taktiku, paņēmienus un procedūras.

Draudu medību atskaitē tiek iekļauta informācija par visiem atradumiem, kā arī tiek sniegti ieteikumi seku mazināšanai un kibernoturības stiprināšanai.

Draudu medību operācijas notiek ciešā sadarbībā ar Kanādas Bruņoto spēku kiberpavēlniecību, kas ir būtiska Latvijas kiberaizsardzības spēju kāpināšana, attīstot savas spējas un pretstāvēšanas kapacitāti, lai novērstu jebkura kiberuzbrukuma iespējamību.

Pārskata periodā tika izstrādāti teorētiskie un praktiskie materiāli šogad oktobrī gaidāmajām starptautiskajam draudu medību operāciju semināram ("Threat Hunting Workshop"), kas tiks īstenots sadarbībā ar Kanādas bruņoto spēku kiberpavēlniecību un NATO CCDCOE.

Salīdzinājumā ar citām NATO dalībvalstīm daudzās kiberdrošības jomās, it īpaši draudu medību operācijās, CERT.LV komanda pārējos apsteigusi, un sadarbības partneri labprāt no CERT.LV mācās, it īpaši jautājumos, kas skar cīņu pret inovatīviem uzbrukumiem. Tas nenozīmē, ka citi ir sliktāki, tas nozīmē, ka CERT.LV eksperti ir ļoti spējīgi un CERT.LV metodes – pietiekami efektīvas.

Kā apliecinājums tam šogad ir arī Latvijas komandas, tostarp CERT.LV ekspertu, 1. vieta lielākajās NATO kiberaizsardzības mācībās "Locked Shields 2024".

Lai efektīvi pasargātu organizāciju IKT infrastruktūru, CERT.LV piedāvā NKDL subjektiem plašu kiberdrošības pakalpojumu klāstu, tajā skaitā kiberdrošības draudu medību operācijas, kas sniedz reālistiskāko ieskatu mērķa infrastruktūrā. CERT.LV aicina rakstīt uz cert@cert.lv un informēt par vēlmi saņemt pakalpojumu.

5.2. Sadarbība kiberaizsardzības mācību organizēšanā

"Namejs 2024"

Sākot no 30. septembra līdz 4. oktobrim, CERT.LV piedalās mācībās "Namejs" Civilās aizsardzības Operacionālā vadības centra Sakaru grupas sastāvā, atbildot uz kiberincidentiem hibrīdapdraudējuma situācijā.

"Namejs"

Visaptverošas valsts aizsardzības mācības, kas ir iepriekš plānotas un visā Latvijā norisinās kopš 2014. gada.

Militāro mācību regulārai norisei ir būtiska loma, lai uzturētu un stiprinātu Nacionālo bruņoto spēku kaujas spējas, kurām pastāvīgi jābūt augstā līmenī. Bruņotajiem spēkiem vienmēr jābūt gataviem laikus un efektīvi reaģēt uz potenciāliem apdraudējumiem un garantēt Latvijas drošību. Savukārt sadarbības stiprināšana ar valsts un pašvaldību iestādēm, dažādu nozaru komersantiem un to iesaiste mācībās stiprina visaptverošas valsts aizsardzības sistēmu Latvijā.

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, darba grupas mērķis ir nodrošināt, ka kvalifikācijas ieguvēji jau mācību laikā apgūst darbam nepieciešamās zināšanas un kļūst par augsti novērtētiem speciālistiem.

CERT.LV aktīvi iesaistās Latvijas jauniešu kiberdrošības prasmju veicināšanā, gan atbalstot Nacionālā kiberdrošības izaicinājuma sacensību sagatavošanu, gan piedaloties Latvijas komandas sagatavošanā dalībai "Eiropas kiberdrošības izaicinājums 2024" (ECSC) sacensībās, kas norisināsies 2024. gadā no 8. līdz 11. oktobrim Turīnā, Itālijā.

Latvijas kiberdrošības izaicinājums jauniešiem

Latvijas komanda 2024. gadā pirmo reizi piedalīsies Eiropas kiberdrošības izaicinājuma sacensībās, un Nacionālā kiberdrošības izaicinājuma sacensības nodrošināja kandidātu atlasi Latvijas komandai.

Nacionālo atlasi organizēja Aizsardzības ministrija sadarbībā ar CERT.LV, Latvijas Universitāti un Zemessardzes Kiberaizsardzības vienību. To atbalstīja Eiropas Kiberdrošības kompetenču centra Latvijas Nacionālais koordinācijas centrs (NCC-LV) un Eiropas Kiberdrošības kompetenču centrs, savukārt līdzfinansē Eiropas Savienība (ES).

Ikgadējo pasākumu 2024. gadā organizē ES Kiberdrošības aģentūra (ENISA) sadarbībā ar Itālijas kiberdrošības aģentūru un Kiberdrošības nacionālo laboratoriju (CINI). Vairāk informācijas: https://ecsc2024.it/.

Piedaloties kiberdrošības sacensībās, jauniešiem ir iespēja pārbaudīt un pielietot praksē iegūtās zināšanas un prasmes dažādās kiberdrošības jomās, kā arī tikties un veidot ciešāku sadarbību ar citu ES dalībvalstu pārstāvjiem.

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, ES 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 turpināja dalību CSIRTs Network darba grupā "Maturity", kura rūpējas par ES dalībvalstu CSIRT komandu brieduma līmeņa paaugstināšanu.

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

- **Coordinated Vulnerability Disclosure Task Force** – norit darbs pie ES līmeņa koordinētas ievainojamību atklāšanas pieredzes un prakšu apkopošanas;
- **EU Cybersecurity Index** – turpinās darbs pie EU Cybersecurity Index platformas attīstīšanas.

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.

Lepojamies! 2024. gada maijā GOVCERT.LU eksperts veica CERT.LV Peer Review pēc SIM3 metodoloģijas, un jūlija beigās GOVCERT.LU iesniegtais Peer Review ziņojums apliecina, ka CERT.LV komanda ieguvusi augstāko jeb EXPERT vērtējumu.

CSIRT Network Situation Update sanāksmes: turpinās regulāra dalība sanāksmēs, kuru mērķis ir veikt informācijas apmaiņu par aktuālo situāciju 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.

Pārskata periodā CERT.LV piedalījās Eiropas Kiberdrošības produktu sertifikācijas grupas ECCG (European Cybersecurity Certification Group) sanāksmēs, tajā skaitā sanāksmēs, pārstāvot Latvijas intereses un sniedzot savu 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": Mācības "Cyber Europe" norisinājās no 19. līdz 20. jūnijam ar primāro auditoriju – enerģētikas sektors, sekundārajām auditorijām – valsts pārvalde un datu centri. Septembrī CERT.LV iesaistījās mācību noslēguma ziņojuma (After Action Report) sagatavošanā. Mācību izvērtēšanas sanāksme plānota 2024. gada novembrī.

“Cyber Europe” ir Eiropas kiberdrošības aģentūras ENISA lielākās organizētās kibedrošības mācības, kurās iesaistās lielākā daļa ES dalībvalstu, kā arī ES organizācijas. Mācību mērķis ir pārbaudīt un uzlabot kiberdrošības incidentu risināšanas, darbības nepārtrauktības un krīzes vadības prasmes dalībvalstīs, kā arī testēt standarta darbības procedūras (SOP). 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.

NATO CCD COE organizētās mācības “Crossed Swords 2024”: 3. ceturksnī CERT.LV piedalījās mācību “Crossed Swords 2024” plānošanas ciklā, sniedzot atbalstu organizatoriem (*White Team*) informācijas operāciju spēles scenārija izstrādē.

NATO organizētās mācības “Cyber Coalition”: 3. ceturksnī CERT.LV piedalījās mācību “Cyber Coalition” nacionālajā plānošanas konferencē, kur Nacionālie bruņotie spēki informēja par šī gada mācību scenāriju, Latvijas izvēlētajiem scenārija virzieniem un izaicinājumiem un sadarbību starp civilo un militāro jomu.

Sadarbība FIRST ietvaros

Turpinājās regulāra dalība FIRST Membership Committee (Jauno biedru uzņemšanas komitejas) sanāksmēs, lai apspriestu turpmākos noteikumus biedru uzņemšanā un piesaistīšanā, biedru kategorijas, 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 Membership Committee priekšsēdētājas pienākumus, piedalījās jauno biedru pieteikumu izskatīšanā, kā arī veicināja biedru uzņemšanas procesa pilnveidošanu.

Sadarbība TF-CSIRT ietvaros

CERT.LV ir viena no 42 Eiropas TF-CSIRT/Trusted Introducer sertificētajām komandām. Uz pārskata perioda beigām kopienā ir 526 komandas, kas apliecina CERT.LV komandas augsto brieduma un sagatavotības līmeni.

Sertifikācija notiek, izmantojot SIM3 standartu un TI/TF-CSIRT noteiktus parametru līmeņus. SIM3 tiek izmantots arī NIS direktīvas CERTu tīklā *Self-Assesment* un *Peer Review*. atbilstoši ENISA metodoloģijai.

Lepojamies! CERT.LV ir augstākā līmeņa TF-CSIRT Trusted Introducer sertificēta IT drošības incidentu novēršanas komanda.

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.

TF-CSIRT/Trusted Introducer (TI)) ir Eiropas reģiona CERTu organizācija, kas apvieno incidentu reaģēšanas komandas no visiem sektoriem. 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 2016. gada.

Sertifikācija notiek, ja institūcijas vērtējamie parametri sasniedz nepieciešamo minimālo novērtējumu, kuru apstiprina ārējs auditors. Veiksmīga sertifikācija apliecina komandas profesionalitāti un procesu sakārtotību. Sertifikāts tiek izsniegts uz 3 gadiem, pēc tam ir jāveic sertifikācijas uzturēšanas atkārtots audits.

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

No 25. līdz 27. septembrim Prāgā, Čehijā norisinājās 72. TF-CSIRT sanāksme, kuras ietvaros uzstājās CERT.LV eksperti - Dana Ludviga ar prezentāciju "The Rise and Impact of DNS Firewall in Latvia – From Idea to Mandatory Measure" un Egils Stūrmanis ar prezentāciju "Twelve Years Experience of Cybersecurity Awareness Raising in Latvia".

CERT.LV eksperti Egils Stūrmanis un Dana Ludviga 72. TF-CSIRT sanāksmē

Dalība citos starptautiskos pasākumos kiberdrošības jomā

9. jūlijā Ņujorkā, ASV Apvienoto Nāciju organizācijā CERT.LV vadītāja Baiba Kaškina pārstāvēja Latviju tematiskajā diskusijā par noturības stiprināšanu kibertelpā, ko organizēja Latvijas pastāvīgā pārstāvniecība ANO sadarbībā ar Bahreinas un Kolumbijas pārstāvniecībām, kā arī ar ANO domnīcu UNIDIR. Pasākumu atklāja LR Aizsardzības ministrijas valsts sekretāra vietnieks – politikas direktors Rolands Heniņš.

CERT.LV eksperti Egils Stūrmanis un Dana Ludviga 72. TF-CSIRT sanāksmē

No 22. līdz 23. augustam Arhusā, Dānijā "Nordic-Baltic CyberSkills Think Tank" darba grupas sanāksmēs piedalījās gan Aizsardzības ministrijas, gan CERT.LV pārstāves. CERT.LV eksperte Sanita Vītola piedalījās diskusijās un pastāstīja par Latvijas iniciatīvām kiberdrošības izglītības pilnveidošanā. Vairāk informācijas: https://cyberbridgeforum.com/

No 12. līdz 13. septembrim Tallinā, Igaunijā konferencē "Nordic Baltic Security Summit" paneļdiskusijā "The Role of Education and Social Awareness in Building Resilient Cyber Security" CERT.LV vadītāja Baiba Kaškina dalījās ar CERT.LV redzējumu par stratēģijām un labākajām praksēm kibernoturības stiprināšanai.

CERT.LV vadītāja B. Kaškina "Nordic Baltic Security Summit" paneļdiskusijā

19. septembrī Atēnās, Grieķijā norisinājās ENISA organizētā konference "Threathunt 2030". Tajā piedalījās arī CERT.LV pārstāvji. Konferences laikā tika pārrunāti nākotnes kiberdrošības apdraudējumi un kā Eiropas Savienība un dalībvalstis vislabāk var paredzēt, identificēt, novērst un reaģēt uz nākotnes kiberdrošības izaicinājumiem.

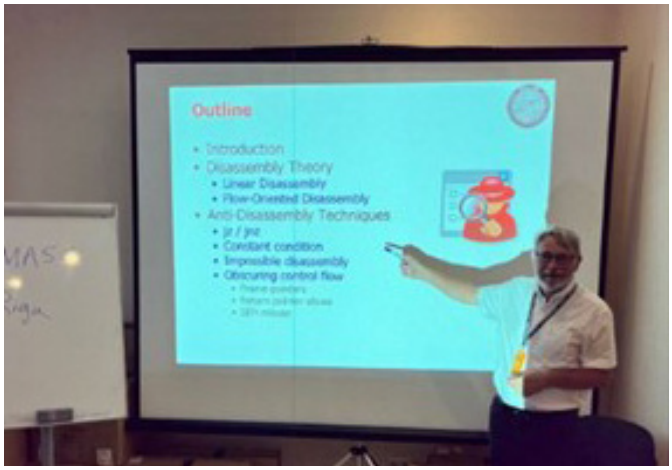
No 23. līdz 24. septembrim Budapeštā, Ungārijā 24. CSIRT Network sanāksmē attālināti piedalījās CERT.LV pārstāvji, lai nodrošinātu sekmīgu informācijas apmaiņu un ciešāku sadarbību ar ES kiberincidentu novēršanas komandām.

No 23. līdz 27. septembrim Seulā, Dienvidkorejā Korejas CERT organizētajā kiberdrošības pasākumā piedalījās CERT.LV eksperte Daina Ozoliņa. Pasākuma mērķis bija sapulcināt kiberincidentu novēršanas institūciju darbiniekus no Āzijas-Klusā okeāna reģiona, Eiropas un Amerikas. Tā programmā bija iekļauts TRANSITS-I kurss par kiberdrošības organizatoriskajiem, operacionālajiem, juridiskajiem un tehniskajiem aspektiem, kurā liels uzsvars bija uz dažādu valstu un reģionu pieredzi un diskusijām, kurās D. Ozoliņa prezentēja CERT.LV iniciatīvas – kopā ar Kanādas kolēģiem veiktās draudu medības, DNS ugunsmūri, CVD platformu, kā arī dalību starptautiskajās mācībās. Tāpat D. Ozoliņa piedalījās arī praktiskajās (*table top*) mācībās par izspiedējvīrusa uzbrukumu (incidenta risināšana, koordinācija un komunikācija).

CERT.LV turpina piedalīties Ziemeļvalstu un Baltijas valstu drošības operāciju centra (Nordic-Baltic SOC) izveides koordinācijas darbā.

Latvijā norisinās augsta līmeņa mācību kurss kiberdošības speciālistiem

Augustā veiksmīgi norisinājās 2 nedēļu ilgas apmācības par ļaunprogrammatūru analīzi – "Malware Analysis Short Course", kuras vadīja Kanādas Karaliskā militārā koledža (Canada Royal Military College) sadarbībā ar CERT.LV. Kursa dalībnieki guva gan teorētiskas zināšanas, gan praktisku pieredzi un svarīgas prasmes, kas noderēs ikdienas darbā cīņai pret kiberapdraudējumiem, tā stiprinot valsts kopējo kibertelpas aizsardzību. Mācības vērtējamas kā vērtīgs solis Latvijas un Kanādas kopējā sadarbībā.



Kanādas Karaliskās Militārās Koledžas mācību kursa dalībnieki

7. Pārskats par LIA Drošāka interneta centra ziņojumu līnijas darbību

Latvijas Interneta asociācijas (LIA) Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.07.2024. līdz 30.09.2024. ir saņēmusi un izvērtējusi 350 ziņojumus. No tiem 83 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 18 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 23 ziņojumos konstatēta personas goda un cieņas aizskaršana, 15 ziņojumi saņemti par naida runu un 1 ziņojumā konstatēti vardarbīgi materiāli.
Par finanšu krāpšanas mēģinājumiem internetā saņemti 132 ziņojumi, 22 ziņojumu saturs nav bijis pretlikumīgs, 56 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.
Valsts policijai nosūtīts 41 ziņojums par naida runu un bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 13 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 31 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 27 ziņojumu saturs ir dzēsts no publiskas aprites internetā, un 4 ziņojumi atrodas dzēšanas procesā sadarbībā ar INHOPE un Valsts policiju.

Pārskats par saņemtajiem ziņojumiem no 01.07.2024. līdz 30.09.2024.

Ziņojumi	Jūl-24	Aug-24	Sep-24	Q3
Erotisks/ pornogrāfisks saturs bez izvietotiem brīdinājumiem	11	2	5	**18**
Pedofilija/ mazgadīgo prostitūcija/ bērnu seksuālu izmantošanu saturoši materiāli	39	25	19	**83**
Vardarbīga rakstura materiāli	0	0	1	**1**
Cieņas/ goda aizskaršana	11	5	7	**23**
Naida kurināšana/ rasisms	5	6	4	**15**
Finanšu krāpniecība	82	26	24	**132**
Konsultācijas/ padomi	22	19	15	**56**
Citi	2	9	11	**22**
KOPĀ:	**172**	**92**	**86**	**350**

Ziņojumi nosūtīti Valsts policijai	19	15	7	**41**
Ziņojumi nosūtīti INHOPE asociācijai	10	2	1	**13**
Kopā nosūtīti izskatīšanai	**29**	**17**	**8**	**54**

8. Nākamajā ceturksnī plānotie pasākumi

Svarīgākie virzieni un pasākumi 2024. gada 4. ceturksnī NKDL un NIS2 ieviešana

Ar Nacionālās kiberdrošības likuma (NDKL) stāšanos spēkā tiek ieviestas pārskatītās ES Tīklu un informācijas sistēmu drošības direktīvas (NIS2) prasības.
Likumā noteiktas izmaiņas kiberdrošības pārvaldības modelī – darbu uzsākusi jauna institūcija – Nacionālais kiberdrošības centrs (NKC). Centra funkcijas īstenos Aizsardzības ministrija sadarbībā ar CERT.LV.
IKT kritiskās infrastruktūras uzraudzības iestāde būs Satversmes aizsardzības birojs.

Stiprinot kiberdrošību Latvijā, CERT.LV turpina aktīvi uzraudzīt kibertelpu, risināt un koordinēt incidentus, nodrošināt plašu kiberdrošības pakalpojumu klāstu, informēt un izglītot sabiedrību, veicinot stratēģisku sadarbību valsts un starptautiskā mērogā.

Atbilstoši NKDL kiberdrošības prasību ievērošana ir attiecināma uz plašāku uzņēmumu loku, līdz ar to būtiski palielinās CERT.LV klientūras skaits un paplašinās CERT.LV nodrošināto pakalpojumu apjoms publiskā un privātā sektora organizācijām.

Lai arī virkne NKDL saistīto noteikumu vēl tiek izstrādāti, darbs infrastruktūras drošības stiprināšanā nedrīkst apstāties. CERT.LV turpina attīstīt savas un klientūras spējas, nodrošinot ātru un efektīvu reaģēšanu uz kiberdrošības incidentiem, kibertelpas situācijas uzraudzību un draudu analīzi, kā arī aktīvās aizsardzības un Drošības operāciju centra pakalpojumus. Tuvākā gada laikā ļoti būtiska CERT.LV iesaiste paredzama, izglītojot un atbalstot jaunos NKDL subjektus likuma un saistīto noteikumu prasību ieviešanā, kā arī kiberdrošības pārvaldības procesu izvērtēšanā un pilnveidošanā.

Pakalpojumu attīstība

Īstenojot mērķi - būt par galveno operacionālo kiberdrošības organizāciju Latvijā – CERT.LV turpinās paplašināt un nostiprināt savu pakalpojumu klāstu, vienlaikus palielinot to kapacitāti. Primāri fokusējoties uz valsts un pašvaldību iestādēm un IKT kritiskās infrastruktūras uzturētājiem, aktīvāk tiks veicināts CERT.LV pakalpojumu pielietojums valsts sektorā.

Turpinot nodrošināt DNS ugunsmūra pakalpojumu ikvienam iedzīvotajam un organizācijai Latvijā, paredzams, ka tuvāko mēnešu laikā DNS ugunsmūra lietotājiem tiks piedāvātas mobilās lietotnes. Tās nodrošinās aktīvo aizsardzību pret kiberdrošības apdraudējumiem Android un Apple iOS iekārtās un ļaus bloķēt arī krāpnieku zvanus.

Draudu medību operācijas

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

Lai padarītu Latviju par maksimāli neparocīgu mērķi kiberuzbrucējiem, CERT.LV komanda turpinās stiprināt savu līderību kiberdraudu medību operāciju organizēšanā, izmantojot jaunākās metodes, rīkus un labākās prakses draudu identificēšanai un novēršanai.

Turpināsies kiberdrošības draudu medību operācijas gan saviem spēkiem, gan ciešā sadarbībā ar Kanādas Bruņoto spēku kiberpavēlniecību. Tās primāri vērstas Latvijai nozīmīgu IKT sistēmu noturības stiprināšanai, un sekundāri kopīgais darbs sniedz ieguldījumu NATO kolektīvajā aizsardzībā.

No 21. līdz 25. oktobrim Rīgā norisināsies divi secīgi kiberspēju attīstīšanai un stiprināšanai veltīti semināri:

- No 21. līdz 23. oktobrim notiks pirmais starptautiskais CERT.LV un Kanādas bruņoto spēku kiberpavēlniecības organizētais Draudu medību seminārs: "Threat Hunt Workshop". Semināra norisi atbalsta arī Aizsardzības ministrija un NATO CCDCOE.
- No 24. līdz 25. oktobrim notiks ASV Eiropas Kiberpavēlniecības EUCOM organizēts seminārs par kiberdraudu izlūkošanu: "Cyber Threat Intelligenge".

Kiberdrošības mācības

Oktobra sākumā turpināsies dalība mācībās "NAMEJS", kurās būs iekļauta arī reaģēšana uz kiberdrošības incidentiem. Savukārt novembrī CERT.LV piedalīsies ENISA organizēto mācību "Cyber Europe" izvērtēšanas sanāksmē, kas būs apvienota ar 2026. gada mācību sākotnējo plānošanas sanāksmi.

Tāpat CERT.LV atbalstīs NATO CCDCOE mācību "Crossed Swords 2024 " plānošanu un izspēli šā gada decembrī organizatoru komandā (*White Team*), kā arī mācību "Locked Shields 2025" jauno plānošanas ciklu.

Plānots, ka CERT.LV piedalīsies arī NATO organizēto mācību "Cyber Coalition" izspēlē šā gada decembrī kā mācību auditorija, reaģējot uz kiberapdraudējumu veselības sektorā.

Kiberšahs 2024 konference

No 1. līdz 3. oktobrim jau 11. reizi Rīgā norisināsies nozīmīgākā kiberdrošības konference Baltijā – "KiberŠahs 2024" ("CyberChess 2024"), lai pārrunātu un dalītos pieredzē par stratēģiski politiskiem un dziļi tehniskiem izaicinājumiem, kā arī par inovāciju un nākotnes jautājumiem. Oktobris tradicionāli Eiropā tiek atzīmēts kā kiberdrošības mēnesis, un šīs konferences norise mēneša pašā sākumā iezīmē simbolisku startu plašākai diskusijai par kiberdrošības nozīmīgumu mūsdienu sabiedrībā. Konferenci organizē CERT.LV, LR Aizsardzības ministrija un Nacionālais kiberdrošības centrs sadarbībā ar ISACA Latvijas nodaļu un LU MII.

Pulcējot vairāk nekā 500 kiberdrošības jomas profesionāļus no teju 20 valstīm, vairāk nekā 50 lektori, tajā skaitā arī runātāji no CERT.LV, 3 dienu garumā dalīsies ar saviem pētījumiem un pieredzes stāstiem ar kiberdrošību saistītās jomās, īpaši pievēršot uzmanību cīņai ar pastāvošajiem draudiem.

Konferences atklāšanā dalībniekus līdztekus ar LR Aizsardzības ministru un Nacionālās Kiberdrošības centra ģenerāldirektoru uzrunās arī CERT.LV vadītāja Baiba Kaškina. Konferences galvenās skatuves - stratēģiski politiskās sesijas moderators būs pieredzējis moderators Oskars Priede, savukārt abas paralēlsesijas un tajās notiekošās paneļdiskusijas vadīs CERT.LV kiberdrošības profesionāļi Dana Ludviga un Dr. Bernhards Blumbergs. Ar saistošu prezentāciju svarīgākos kiberdrošības izaicinājumus un risinājumus, īpaši pievēršoties pieredzei par paveiktajām draudu medībām, izklāstīs CERT.LV vadītājas vietnieks Varis Teivāns. Praktisko semināru konferences pirmajā dienā par DNS ugunsmūra izstrādi un pielietojumu vadīs CERT.LV kiberdrošības eksperts un Incidentu risināšanas nodaļas vadītājs Armīns Palms. Plašāka informācija par pasākumu: https://cyberchess.lv/

Citi izglītojošie pasākumi kiberdrošības jomā

Decembrī CERT.LV plāno organizēt ikgadējo kiberdrošības semināru "Esi drošs" valsts un pašvaldību iestāžu atbildīgajiem par IT drošību, kā arī citiem interesentiem kiberkopienā.

Plānota dalība arī citos kiberkopienas pasākumos:

- **9. oktobrī "SEB CFO Forum 2024"** uzņēmumu vadītāju un finanšu direktoru foruma ietvaros paneļdiskusijā dalīsies pieredzē CERT.LV vadītāja Baiba Kaškina.
- **18. oktobrī konferencē "Mākslīgais intelekts un drošība digitalizācijā"**, ko organizē Valmieras attīstības aģentūra sadarbībā ar Vidzemes plānošanas reģionu, ar savu ekspertīzi dalīsies arī CERT.LV profesionāļi.

- **17. oktobrī "EPALE kopienas konferencē 2024"** CERT.LV eksperte Dana Ludviga piedalīsies ar prezentāciju – "Kiberdrošības Kods: Latvijas kibertelpas draudi, ekspertu izaicinājumi un mans ceļš".
- **No 22. līdz 23. oktobrim ALTUM pasākumā** CERT.LV ekspertes Dana Ludviga un Daina Ozoliņa vadīs kiberdrošības incidenta izmeklēšanas spēli. Pasākuma ietvaros Dana Ludviga vadīs arī lekciju "Kiberdrošības aktualitātes – draudi un risinājumi".
- **5. novembrī Latvijas bankā** CERT.LV ekspertes Dana Ludviga un Daina Ozoliņa vadīs kiberdrošības incidenta izmeklēšanas spēli. Pasākuma ietvaros Dana Ludviga vadīs arī lekciju "Kiberdrošības aktualitātes – draudi un risinājumi".

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 un semināros.

- **No 8. līdz 11. oktobrim Turīnā, Itālijā "Eiropas kiberdrošības izaicinājums 2024"** (ECSC) sacensībās CERT.LV eksperts Rihards Kauliņš darbosies Latvijas komandā kā dalībnieks, savukārt CERT.LV eksperts Mārtiņš Vecstaudžs atbalstīs komandu gan sagatavošanas darbos, gan sacensību laikā, piedaloties sacensību komiteju darbā.
- **10. oktobrī Briselē, Beļģijā CERT.EU konferencē "Tales From the Real World"** CERT.LV eksperts Kārlis Svilans uzstāsies ar prezentāciju "Defending From the Beast in the East – CERT.LVs Approach to Multinational Threat Hunting".
- **No 15. līdz 16. oktobrim Tirānā, Albānijā, un no 24. līdz 25. oktobrim Belgradā, Serbijā, ES atbalstītā "Cyber Balkans"** projekta ietvaros notiks divu dienu semināri kiberdrošības profesionāļiem. Tajos CERT.LV kiberdrošības eksperts un Incidentu risināšanas nodaļas vadītājs Armīns Palms dalīsies pieredzē ar CERT.LV praksi kiberdrošības incidentu risināšanā.
- **No 15. līdz 18. oktobrim Tokijā, Japānā** "CEATEC 2024 – Toward Society 5.0" konferences ietvaros tematiskajā panelī "AI for All" ar virzienu par kiberdrošības savstarpējo mijiedarbību ar AI/ML runās CERT.LV kiberdrošības profesionālis Dr. Bernhards Blumbergs. CEATEC ir pasaulē lielākā elektronikas un tehnoloģiju izstāde ar ļoti lielu starptautisko uzmanību un redzamību (https://www.ceatec.com/en/).
- **1. novembrī Tartu, Igaunijā** notiks konference "Cybercation - Nordic-Baltic Educators' Forum", kurā plānota arī CERT.LV eksperta dalība un uzstāšanās ar prezentāciju.

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
Kiberincidentu novēršanas institūcija