2025. gada 1. ceturksnis Latvijas kibertelpā

Periods: 01.01.2025. – 31.03.2025.

CERT.LV
Kiberincidentu novēršanas institūcija

2025. gada 1. ceturksnis Latvijas kibertelpā

KOPSAVILKUMS

2025. gada pirmajos mēnešos kiberdraudu ainava Latvijā un citviet pasaulē turpina attīstīties ar pieaugošu intensitāti, sarežģītību un stratēģisku virzību. Kiberoperācijas vairs nav tikai vienreizēji uzbrukumi vai peļņas gūšanas mēģinājumi - tie kļūst arvien mērķtiecīgāki, noturīgāki un saskaņoti ar plašākiem ģeopolitiskiem un ekonomiskiem mērķiem.

Turpinoties pret Latviju vērstiem plaša mēroga kiberuzbrukumiem, apdraudējuma līmenis saglabājas augsts kopš 2022. gada Krievijas pilna mēroga iebrukuma Ukrainā. Krievijas agresijas apdraudējuma fonā 2025. gada sākums skaidri apliecina Latvijas kibernoturību un spēju efektīvi aizsargāt mūsu kibertelpu.

Kiberspiegošanas un finansiāli motivēti uzbrukumi galvenokārt ir vērsti pret nozīmīgām iestādēm un organizācijām finanšu, tiesībaizsardzības, izglītības, veselības aprūpes un telekomunikāciju sektoros, kā arī pret valsts un pašvaldību iestādēm un kritisko infrastruktūru. Šo uzbrukumu nolūks ir izgūt sensitīvus datus, destabilizēt darbību, vājināt sabiedrības uzticību un radīt stratēģisku spiedienu.

Ņemot vērā iespējamos Krievijas agresīvos plānus un retoriku ES un Baltijas virzienā, paredzams, ka arī turpmākā apdraudējumu attīstības dinamika saglabāsies augsta. Interese par Latvijas infrastruktūru nav mazinājusies arī no Ķīnas un Baltkrievijas atbalstītiem kiberuzbrucējiem.

Pārskata periodā kiberincidentu skaits (631) ir audzis par 11% salīdzinājumā ar iepriekšējo ceturksni, bet ir par 11% mazāks nekā 2024. gada 1. ceturksnī.

Automātiski apstrādāto un izsūtīto brīdinājumu apjoms (284 029) ir augsts, bet gada griezumā stabils.

Kiberapdraudējumu intensitāte saglabājas augsta un novērotās tendences prasa turpmākus uzlabojumus preventīvajos drošības pasākumos un reaģēšanas efektivitātē.

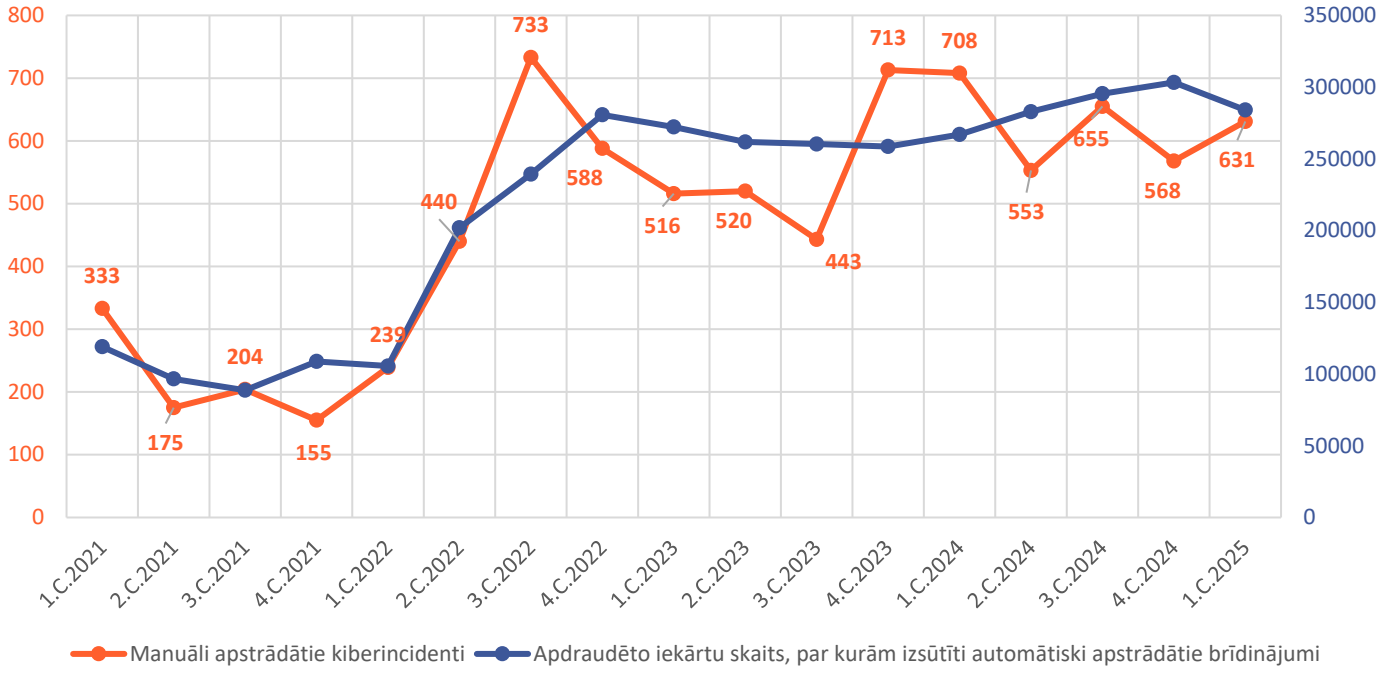
Pārskata periodā izplatītākie TOP 5 apdraudējuma veidi un kiberincidentu skaits

1. Kibertelpas drošības apdraudējumi: statistika un tendences

Latvijas kibertelpā augsta kiberapdraudējumu intensitāte vērojama kopš 2022. gada Krievijas pilna mēroga iebrukuma Ukrainā, un, paredzams, ka arī turpmākās attīstības dinamika saglabāsies augsta.

Pieaugošā uzbrukumu intensitāte, sarežģītība un nerimstoša kiberuzbrucēju izdoma mudina ikvienu organizāciju likt tam pretī atbilstošus tehnoloģiskos risinājumus, un tas savukārt sekmē tehnisko spēju attīstību, pieprasījumu pēc datos balstītiem kiberdrošības pakalpojumiem, kā arī stiprina publiskā un privātā sektora reakcijas spējas. Drošības operāciju centra pakalpojumi un regulāri IT sistēmu drošības kļūst par ierastu praksi. Izaicinājumi veicina nozīmīgus pavērsienus mūsu kiberdrošības stiprināšanā, nepieļaujot, ka Latvija varētu tikt uztverta kā viegls mērķis.

Reaģējot uz arvien pieaugošo kiberapdraudējumu apjomu un sarežģītību, no 2025. gada 1. janvāra esam pilnveidojuši statistikas apkopošanas pieeju – turpmāk tiek uzskaitīti unikālie kiberincidenti, nevis apdraudētās unikālās IP adreses. Šī pieeja precīzāk atspoguļo apdraudējumu apjomu un ietekmi; datu salīdzināmība ar vēsturiskajiem datiem ir saglabāta.

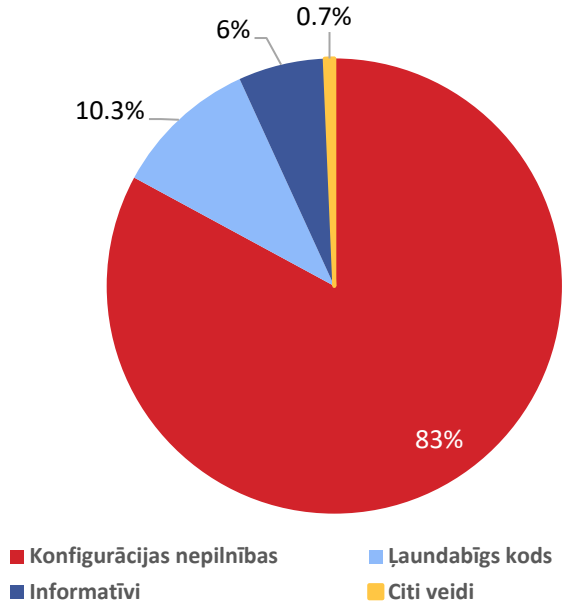


1. attēls. Kiberincidentu un iekārtu apdraudējuma līknes dinamika (skaits ceturkšņu dalījumā; 2021-2025)

Automātiski apstrādāto brīdinājumu apjoms ir augsts, bet stabils

2025. gada 1. ceturksnī automātiski apstrādāto brīdinājumu [1] skaits sasniedza 284 029, kas ir par 6% mazāk salīdzinājumā ar iepriekšējo ceturksni, bet par 6% vairāk nekā 2024. gada 1. ceturksnī. Tas nozīmē, ka apjoms saglabājas stabils gada griezumā, un apdraudējumu identifikācija un brīdinājumu izsūtīšana uzlabojas.

Kvantitatīvi lielāko daļu (83%) automātiski apstrādāto brīdinājumu veido konfigurācijas nepilnības, un saglabājās tajā pašā līmenī arī gada griezumā.



2. attēls. Automātiski apstrādātie brīdinājumi par apdraudējumiem (procentuālā daļa no kopējā skaita 2025. gada 1. ceturksnī)

Tas norāda uz sistēmu un tīkla drošības vājajiem punktiem, kas galvenokārt rodas cilvēcisku kļūdu vai nepietiekamu drošības standartu dēļ, piemēram,

- atstājot neaizsargātus servisu portus,
- izmantojot nešifrētu datu pārraidi,
- praktizējot vāju piekļuves kontroli,
- nenodrošinot iekārtu un to uzturēto servisu pienācīgu versiju kontroli.

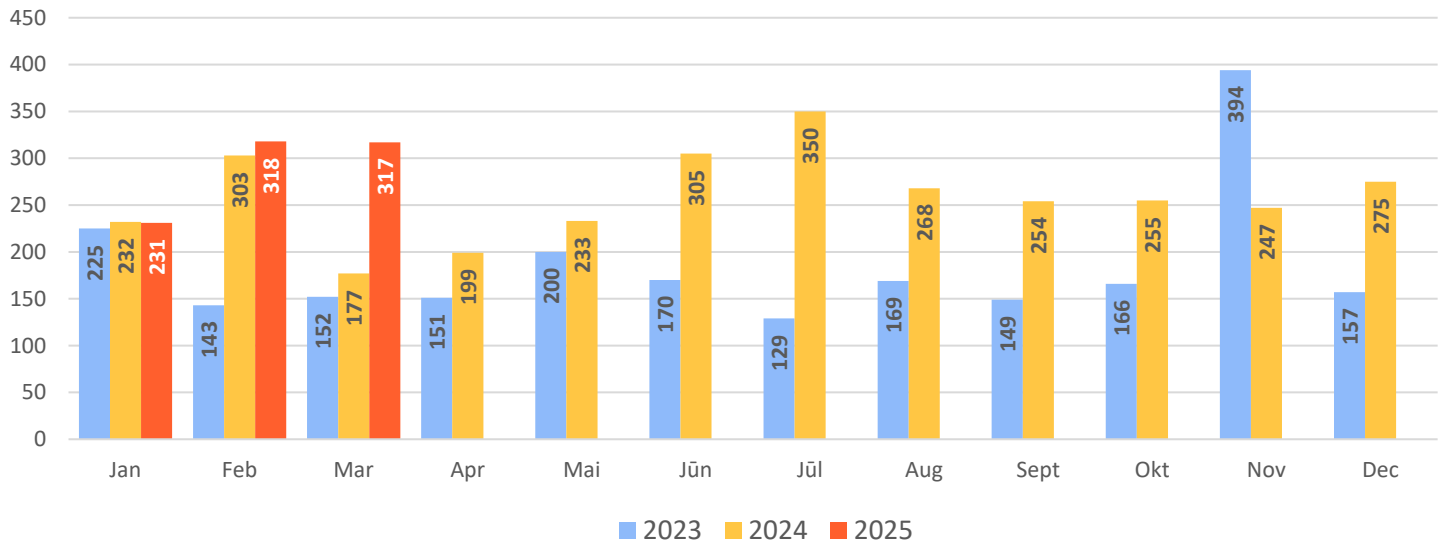
Ieteikumi ievainojamību pārvaldībai

- Regulāri veiciet visaptverošu iekārtu un sistēmu inventarizāciju pilnīgam priekšstatam par infrastruktūru, lai laikus pamanītu novecojušu vai neaizsargātu aprīkojumu.
- Samaziniet drošības riskus, nepieļaujot IT resursu lieku eksponēšanu publiskajā internetā. Nodrošiniet piekļuvi tikai caur drošiem risinājumiem, izmantojot MFA vai šifrēšanu.
- Regulāri sekojiet programmatūras izstrādātāju atjauninājumiem; nodrošinot visām sistēmām jaunākos drošības ielāpus.
- Ieviesiet centralizētu atjauninājumu pārvaldību, lai nodrošinātu nepārtrauktu uzraudzību visās organizācijas sistēmās.
- Regulāri veiciet ievainojamību skenēšanu, lai identificētu vājās vietas un samazinātu riskus no zināmām ievainojamībām.

[1] Izmatojot CERT.LV pieejamos telemetrijas datus, gala lietotājs tika informēts par iekārtas apdraudējumu, informāciju nogādājot ar interneta pakalpojumu sniedzēju starpniecību.

CERT.LV manuāli apstrādāto kiberincidentu skaits pieaug

Pārskata periodā reģistrēts 631 kiberincidents[2], kas ir par 11% vairāk salīdzinājumā ar iepriekšējo ceturksni, bet par 11% mazāk nekā pērn 1. ceturksnī. Pieaugums varētu būt saistīts ar jauniem uzbrukuma veidiem un mākslīgā intelekta (MI) attīstību, kas atvieglo un paātrina krāpšanu, ielaušanās un automatizētu uzbrukumu veikšanu. Pārskata periodā februāra mēnesī fiksēts 3. augstākais incidentu skaits pēdējo 3 gadu laikā.



3. attēls. Kiberincidentu dinamika (skaits mēnešu dalījumā; periods: 2023 - 2025)

Kiberlaikaptākļi

Ikmēneša apskats par Latvijā spilgtākajiem kiberincidentiem un apdraudējumiem TOP 5 kategorijās

Apskats vieglajā valodā: aktuālie notikumi kibertelpā, apdraudējumu analīze, kā arī noderīgi padomi, kā būt soli priekšā potenciālajiem kiberdraudiem.

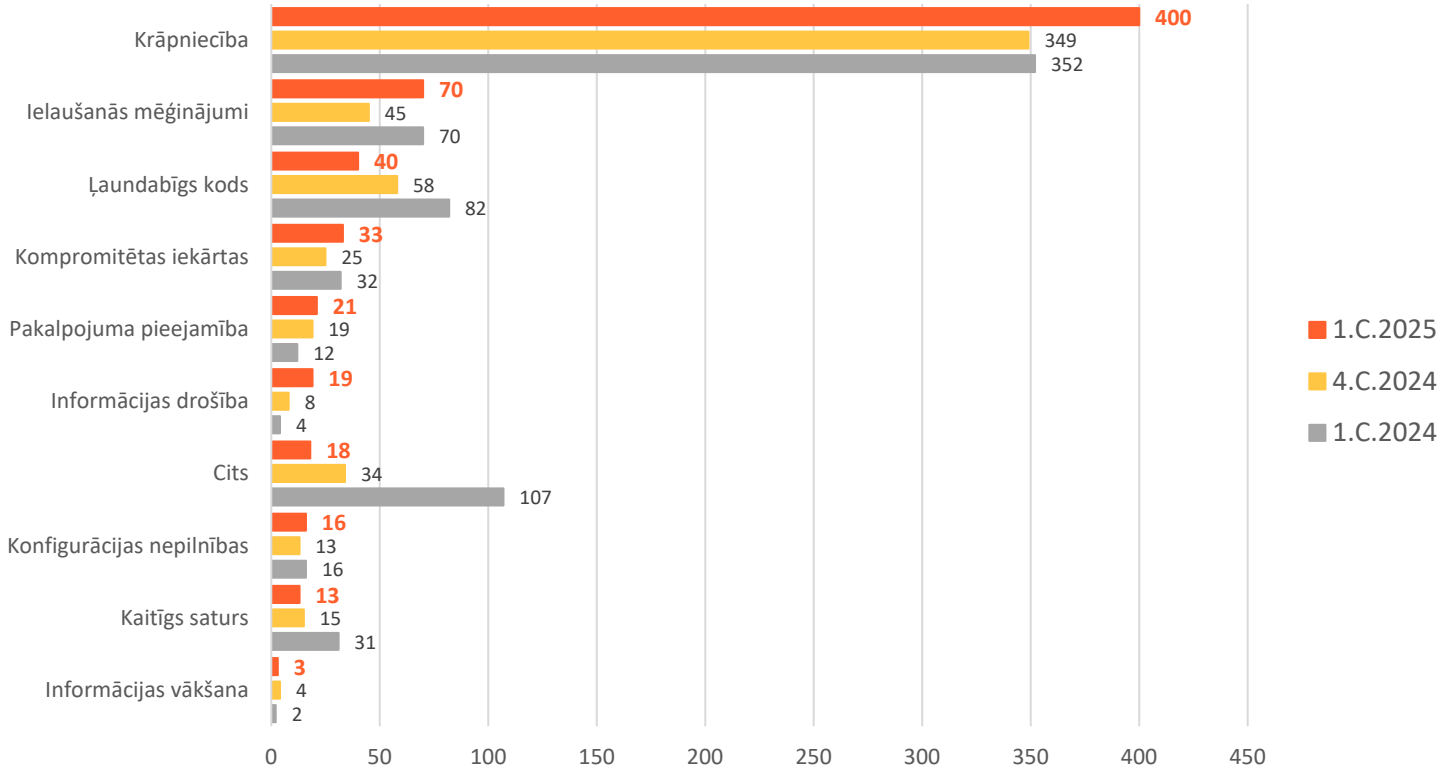
Uzziniet vairāk:

- Janvāris
- Februāris
- Marts

[2] Notikumi, kas apdraudēja apstrādātus datus vai tādu pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, kurus piedāvā tīklu un informācijas sistēmas vai kuri pieejami ar tīklu un informācijas sistēmu starpniecību.

2. Izplatītākie kiberapdraudējumi pārskata periodā: analīze un ieteikumi to novēršanā

- **Krāpšana** (400 kiberincidenti) – lielākais apdraudējums un strauji augošs.
- **Ielaušanās mēģinājumi** (70 kiberincidenti) – arvien inovatīvākas metodes un to radītie izaicinājumi nav mazinājušies gada laikā.
- **Ļaundabīgs kods** (40 kiberincidenti) – skaits samazinās, bet joprojām bīstams.
- **Kompromitētas iekārtas, pakalpojuma pieejamība un informācijas drošība** – kiberincidentu skaits aug līdz ar pieaugošu uzbrukumu intensitāti.



4. attēls. Kiberincidentu salīdzinājums pēc veida

Pakalpojuma pieejamības uzbrukumi

(+11% vs 4.C.2024 un +75% vs 1.C.2024) arvien intensīvāk tiek izmantoti, lai ietekmētu valsts mēroga resursus - TVP mājaslapas, finanšu institūciju, mobilo sakaru operatoru un atsevišķu privāto sektoru resursus.

Pārskata periodā visvairāk DDoS uzbrukumu tika vērsti pret finanšu sektoru.

Ielaušanās mēģinājumi

ar pieaugumu 56% salīdzinājumā ar iepriekšējo ceturksni norāda uz agresīvākiem uzbrukumiem pret sistēmām, taču to skaits saglabājās stabils gada griezumā. Konfigurācijas nepilnības un ievainojamības sistēmās, neatjaunināta programmatūra, vājas paroles un daudzfaktoru autentifikācijas neesamība, pikšķerēšana, iekārtu ar attālināto piekļuvi (RDP, VPN, SSH) neaizsargātība, automatizēti uzbrukumi un "botneti" ir būtiskākie drošības riski, ko izmantoja ielaušanās mēģinājumiem.

Naidīgu valstu atbalstīti un politiski motivēti kiberuzbrukumi pret Latvijas valsts iestādēm, finanšu sektoru, un kritisko infrastruktūru galvenokārt izmanto mērķētus pikšķerēšanas, ļaunatūras, DDoS uzbrukumus, infrastruktūras sabotāžu. Krievijas atbalstītas hakeru grupas ielaušanās mēģinājumus mērķē uz kritisko infrastruktūru, valsts iestādēm un lieliem uzņēmumiem. **Galvenie mērķi: izlūkošana un datu vākšana, sociālās spriedzes veicināšana, kritiskas infrastruktūras sabotāža. Interese par Latvijas IKT infrastruktūru vērojama arī no kiberuzbrucējiem, kas saistāmi ar Ķīnu un Baltkrieviju.**

Krāpšanas (+15% vs 4.C.2024 un +14% vs 1.C.2024)

gadījumu skaits turpina augt, kas norāda uz augstu apdraudējumu līmeni.

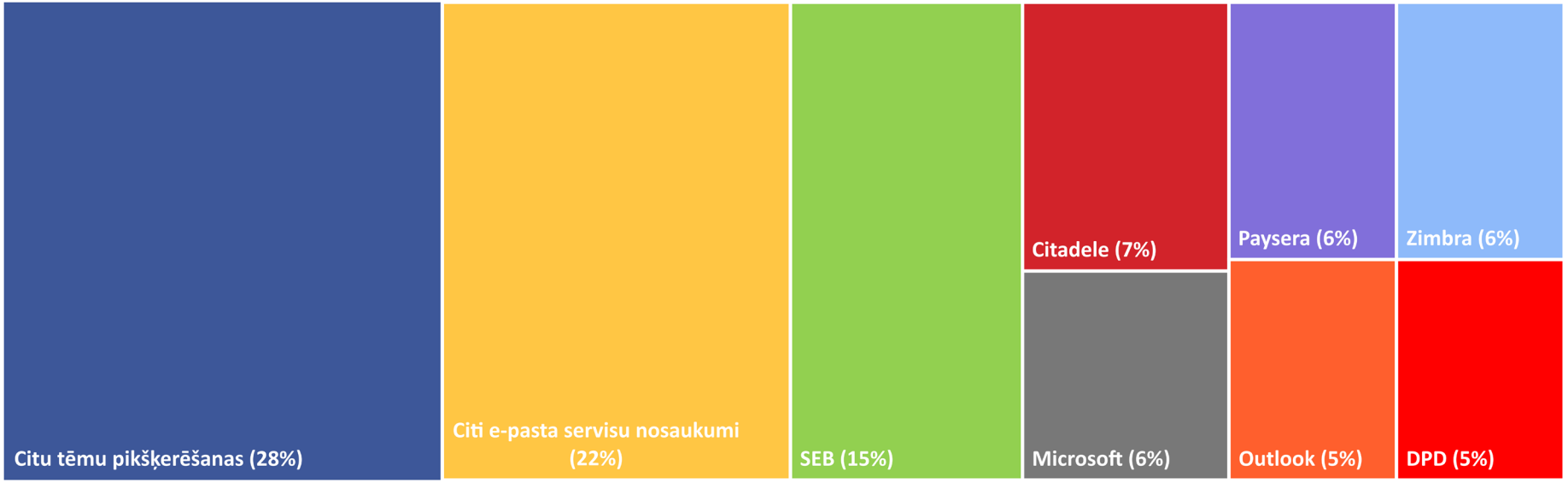
Pārskata periodā fiksētas vairākas komerciāli motivētas krāpniecības kampaņas, kuru ģenerēšanā prasmīgi izmantots MI un sociālā inženierija ar mērķi piekļūt personas datiem un informācijai.

Īpaši izplatītas bija pikšķerēšanas, kas vērstas pret Latvijas iedzīvotājiem, izmantojot zināmu organizāciju nosaukumus.

Nākamajā 5. attēlā redzams, ka procentuāli lielākā daļa no kopējā CERT.LV apstrādāto pikšķerēšanas ziņojumu skaita bija saistīti ar SEB bankas nosaukuma izmantošanu pikšķerēšanas nolūkā.

Dažādu citu tēmu pikšķerēšana konstatēta 34 reizes, savukārt mazāk populāru tīmekļa e-pasta servisu pikšķerēšanas tēma - 27 reizes.

Krāpnieku galvenais motīvs ir peļņas gūšana, taču pieaug gadījumu skaits, kur šādi uzbrukumi veikti spiegošanas nolūkā.



5. attēls. Izplatītākās pikšķerēšanas kampaņas, izmantojot zināmu organizāciju nosaukumus

(procentuālā daļa no kopējā CERT.LV apstrādāto pikšķerēšanas ziņojumu skaita 2025. gada 1. cet.)

CERT.LV atgādina, ka valsts institūcijas un to pārstāvji e-pasta ziņojumos vai telefonsarunās nemudinās uz tūlītēju rīcību un neaicinās dalīties ar bankas konta pieejas vai maksājumu karšu datiem.

Par zvana vai ziņas leģitimitāti jāpārliecinās, apmeklējot iestādes oficiālo tīmekļa vietni un sazinoties, izmantojot tur norādīto telefona numuru.

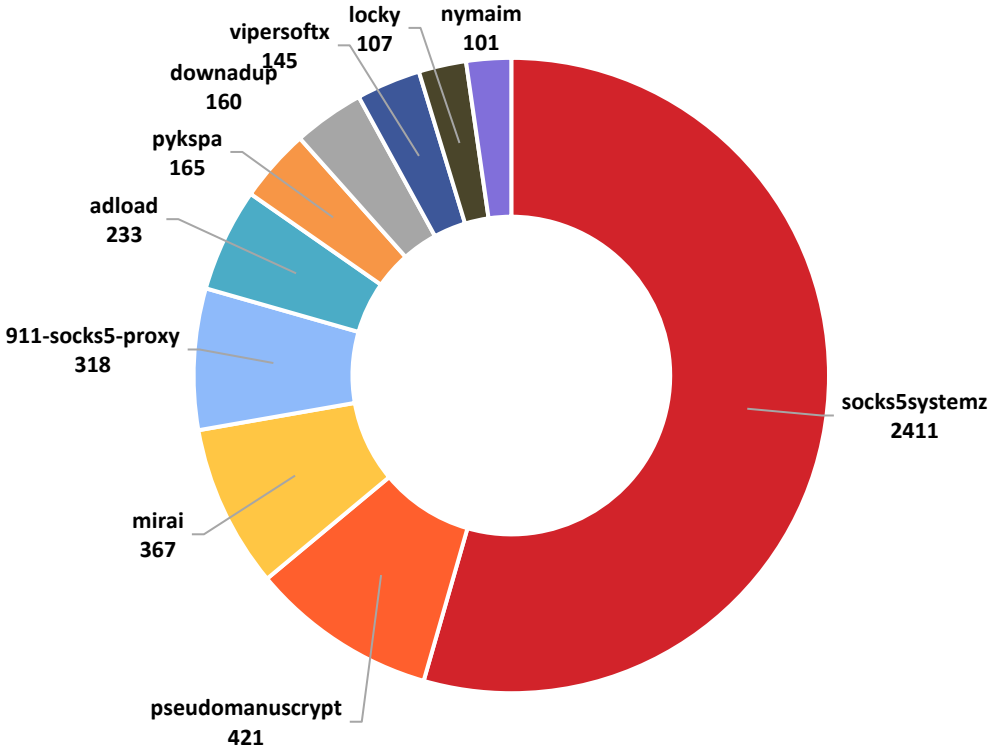
IETEIKUMI ORGANIZĀCIJĀM NODARBINĀTO APMĀCĪBAI:

- Apmācīt lietotājus aizdomīgu e-pastu atpazīšanā (viltus sūtītāji, steidzami pieprasījumi) un kā pārbaudīt e-pasta galvenes un saturu.
- Bloķēt konkrētu failu tipus e-pasta pielikumos (.exe, .js, .vbs u.c)
- Regulāri organizēt (ne retāk kā reizi gadā) darbinieku apmācības par aktuālajiem kiberriskiem un kiberdrošības labo praksi. CERT.LV piedāvā lekcijas, spēles un seminārus.
- Veikt darbinieku zināšanu pārbaudi, tostarp regulāras piešķērēšanas simulācijas kampaņas, papildinot tās ar apmācībām un reāliem pikšķerēšanas piemēriem. Iekļaut iestādes vadību pikšķerēšanas simulācijās, jo vadītāji bieži vien ir uzbrukumu mērķi.

Ieteicams izmantot CERT.LV pikšķerēšanas uzbrukumu simulācijas pakalpojumu.

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.



6. attēls. TOP 10 ļaunatūras; skaits 2025. gada 1. ceturksnī

Izplatītākie ļaunatūras tipi:

- **Lietotāju datu zadzēji**
- **Botu tīkli**
- **Izspiedējvīrusi**
- **Attālinātās kontroles *trojāni* datu izgūšanai, infrastruktūras kompromitēšanai**

Visbiežāk lietotāju datu zadzēju ļaunatūras tiek mērķētas uz nedroši 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 - šīs tendences, visticamāk, turpināsies.

***Socks5systemz* vēlreiz pierāda savu noturību kibervidē – nemainīga līdere ļaunatūru TOP 10 sarakstā jau vairākus gadus.** Tā inficē iekārtas, pārvēršot tās par pāradresācijas *proxy* jeb starpniekserveriem, savukārt ļaundari tos var 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.

Galvenās tendences un secinājumi

Manipulācijas māksla kibertelpā: sociālā inženierija un krāpniecības

- **Pikšķerēšana un personalizēti kiberuzbrukumi:** būtiski pieaug zināmu organizāciju nosaukumu un MI pielietošana, lai radītu uzticamus, uz konkrētiem mērķiem vērstus e-pastus, īsziņas un viltus tīmekļvietnes.
- **Balss klonēšana un telefonkrāpniecība:** pieaug draudi, ko rada MI izmantošana balss klonēšanai, lai pārliecinātu upurus veikt maksājumus vai izpaust sensitīvu informāciju.
- **Romantiskās un investīciju krāpšanas hibrīdi:** sociālie tīkli un MI tiek izmantoti arvien izsmalcinātāk, lai radītu viltus identitātes un investīciju platformas, izraisot būtiskus finansiālos zaudējumus romantiskiem upuriem.
- **e-pasta kontu kompromitēšana un viltus rēķini** - kompromitēti darbinieku e-pastu konti tiek izmantoti ļaunprātīgu pielikumu izplatīšanai, viltotu rēķinu sūtīšanai, radot finansiālus zaudējumus organizācijām.

Arvien intensīvāki mērķēti uzbrukumi valsts un publiskajam sektoram

- **Mērķētas pikšķerēšanas:** pret valsts un pašvaldību iestādēm tiek vērstas mērķētas pikšķerēšanas ar kaitīgiem pielikumiem. Bieži tiek izmantoti iepriekš kompromitēti e-pasta konti, lai pastiprinātu uzbrukuma ticamību.
- **Politiski motivēti kiberuzbrukumi**: valsts pārvaldes un kritiskās infrastruktūras objekti saglabājas kā augsta riska mērķi. Novērotas aktivitātes, kas saistītas ar citu valstu atbalstītiem kiberuzbrukumiem (APT).

Ļaundabīgs kods un izspiedējvīrusi – kibertelpā pieaugoša problēma

- **Izspiedējvīrusu pieaugums:** novēroti uzbrukumi, īpaši veselības aprūpes sektorā. Datu šifrēšana paralizē organizāciju darbību, uzbrucēji pieprasa izpirkuma maksu par datu atgūšanu.
- **Ļaunatūras sarežģītība:** datu zagšanai izmantotās ļaunatūras kļūst tehniski attīstītākas un grūtāk atklājamas.

Strauji augošie draudi: kompromitētas ierīces un saziņas lietotnes

- **Nepietiekami aizsargātas iekārtas:** palielinās kompromitēto iekārtu skaits, kas signalizē par trūkumiem tīkla segmentācijā un ierīču drošības politikās un procedūrās.
- **Saziņas platformu apdraudējumi:** vērojami mēģinājumi pārņemt lietotāju Signal un WhatsApp kontus, lai piekļūtu sensitīvai saziņai. Uzbrukumi tiek saistīti ar Krievijas atbalstītiem uzbrucējiem, kas pastāvīgi pilnveido taktikas.

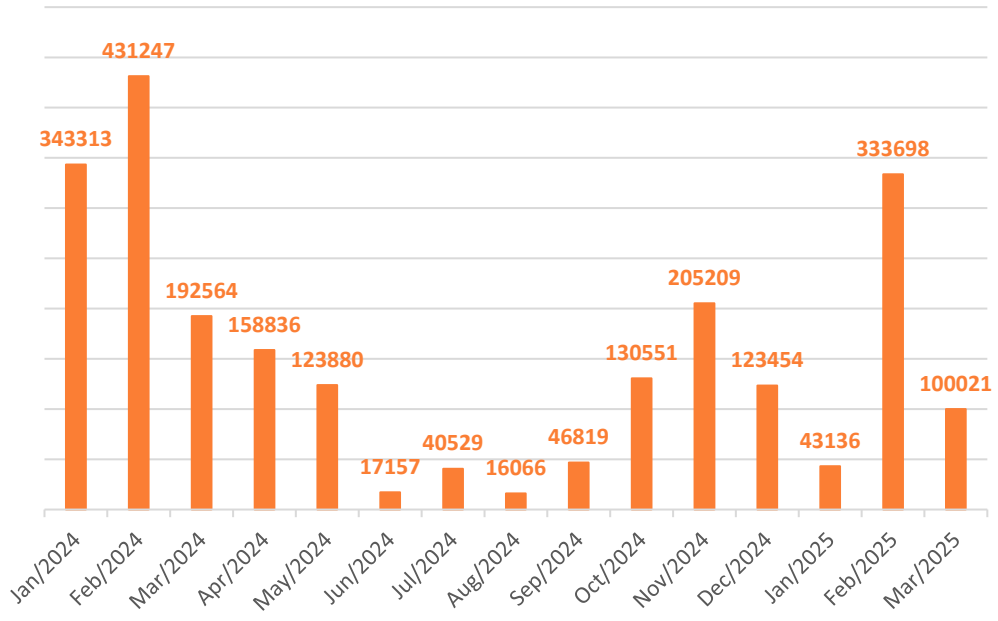
- Pieaugošie kiberuzbrukumu draudi apliecina nepieciešamību pastiprināt darbinieku kiberdrošības apmācības, īpaši attiecībā uz sociālo inženieriju un pikšķerēšanas atpazīšanu.
- Svarīgi ieviest daudzfaktoru autentifikāciju un pārskatīt piekļuves kontroles mehānismus visos sistēmas līmeņos.
- Jāstiprina tīklu segmentācija, ierīču kontrole un monitorings, īpaši attiecībā uz IoT iekārtām.

Darbojoties sinerģijā, CERT.LV DNS ugunsmūris, SOC operācijas, draudu medības, drošības testi, pikšķerēšanas simulācijas un apmācības efektīvi stiprina organizāciju kiberaizsardzību - proaktīvi aizsargā, atklāj ievainojamības, uzlabo kiberprasmes un paaugstina gatavību apdraudējumu novēršanai.

DNS ugunsmūris

2025. gada 1. ceturksnī kopskaitā DNS ugunsmūra pakalpojuma ietvaros kaitīgo domēna vārdu DNS pieprasījumu skaits bija **713 548**. Visu CERT.LV zonu atvairītie kiberuzbrukumi pasargāja lietotājus no ļaunprātīgu vietņu apmeklēšanas **476 855** reizes, kas ir par **4% vairāk** nekā iepriekšējā ceturksnī.

CERT.LV atzinīgi vērtē iedzīvotāju iesaisti, kuri identificē un pārsūta krāpnieciskus e-pastus uz cert@cert.lv. Saņemtie ziņojumi tiek apkopoti, un kaitnieciskie domēna vārdi ievietoti aktīvās aizsardzības rīkā – DNS ugunsmūrī – kas bez maksas ir pieejams ikvienam Latvijas iedzīvotājam, turklāt ir **pieejama arī DNS ugunsmūra mobilā lietotne.**



7. attēls. Visu CERT.LV zonu atvairītie kiberuzbrukumi

Nozīmīgākās aktīvās aizsardzības epizodes pārskata periodā

Brīdinājumi	Skaits
"DELFI" tēla izmantošana krāpniecisku kriptovalūtu investīciju platformu reklamēšanas kampaņās	33 777
Viltus veikali, kas pārdod medicīniskus pakalpojumus un preces	22 126
AgentTesla ļaunatūra	4 931
"Rimi Latvia" tēla izmantošana viltus vietnes kampaņās	1 505
"Latvijas Pasts" tēla izmantošana viltus vietnes kampaņās	1 070
"DPD Latvija" tēla izmantošana viltus vietnes kampaņās	891
"Swedbank" tēla izmantošana viltus vietnes kampaņās	836
"SEB banka" tēla izmantošana viltus vietnes kampaņās	834
Krāpšanas kampaņas ar mērķi pārņemt "WhatsApp" kontu	761
"Citadele banka" tēla izmantošana viltus vietnes kampaņās	631

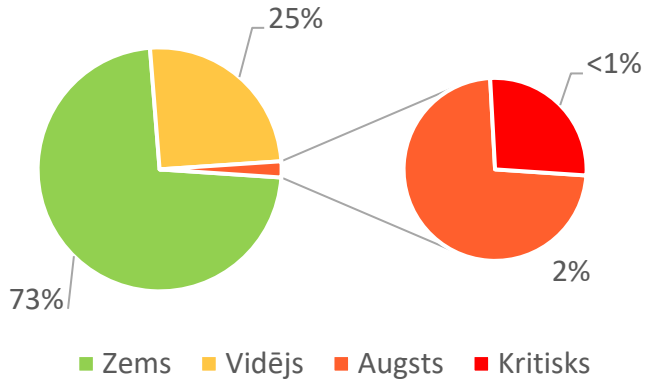
Drošības operāciju centrs (SOC)

Kopš 2024. gada, kad tika uzsākta CERT.LV SOC pakalpojuma sniegšana iestādēm, uz 2025. gada 1. ceturkšņa beigām ir iegūta **redzamība kopskaitā pār 8 409 iekārtām** (serveriem un darbstacijām).

Pārskata periodā gala iekārtu skaits ir pieaudzis par 3 119 (pieaugums par 59% pret pagājušo ceturksni), līdz ar to pieaudzis arī drošības trauksmes ziņojumu skaits (absolūtais skaits pieaudzis par vairāk nekā 851 tūkstoti).

Tika reģistrēti vairāk nekā 1,2 miljoni drošības trauksmes ziņojumu. Apstrādājot drošības trauksmes ziņojumus, **manuāli izveidota 181 lieta.** 77% gadījumu tika veikta saziņa ar klientiem, lai pieprasītu papildu informāciju, informētu par kiberapdraudējumu vai kiberincidentu.

Konstatēti 4 kiberincidenti. Visos gadījumos konstatēta ļaunatūra, kuras mērķis ir informācijas zagšana darbinieku darbstacijās. Nav konstatēta tālāka ļaunatūras ietekme infrastruktūrā.



8. attēls. SOC reģistrētie drošības trauksmes ziņojumi 2025. gada 1. ceturksnī (procentuālā daļa kritiskuma līmeņu dalījumā)

Kiberdrošības draudu medību operācijas

No 2022. gada līdz 2025. gada 1. ceturkšņa beigām kiberdrošības **draudu medību operācijās analīze ir veikta 155 000 gala iekārtās** (pārskata periodā +5 000) dažādās publiskā sektora iestādēs un IKT kritiskās infrastruktūras uzņēmumos. Veicot pārbaudes, **~20%** gadījumu infrastruktūrā tika konstatēta citu valstu atbalstītu uzbrucēju klātbūtne (APT), kas lielākoties saistīti ar Krieviju un veic plaša spektra kiberoperācijas. Novērota arī ar Ķīnu saistītu grupējumu aktivitāte.

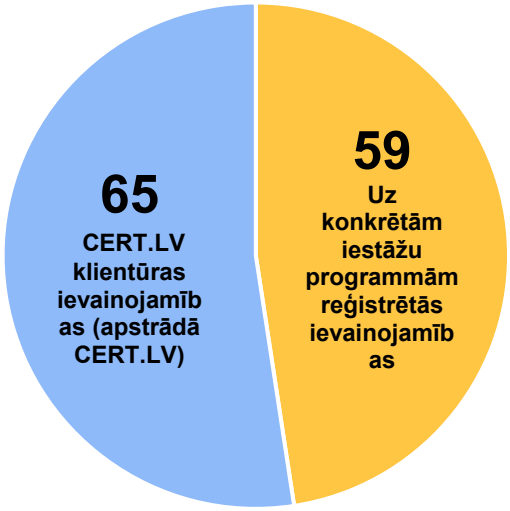
Latvijas un Kanādas kiberdrošības partnerība turpinās: pilnveidots Draudu medību apmācību kurss, kurās dalījāmies pieredzē ar kiberdrošības profesionāļiem no vairāk nekā 25 NATO dalībvalstīm. Dalībniekiem bija iespējas stiprināt savas draudu medību spējas un paplašināt zināšanas par jaunākajām kiberaizsardzības stratēģijām. Apmācību veiksmīga īstenošana ne tikai stiprināja iesaistīto organizāciju kiberdrošības noturību, bet arī noteica jaunu virzienu nākotnes sadarbības iniciatīvām un starptautiskām kiberdrošības apmācībām.

IT sistēmu drošības testi un pikšķerēšanas uzbrukumu simulācijas

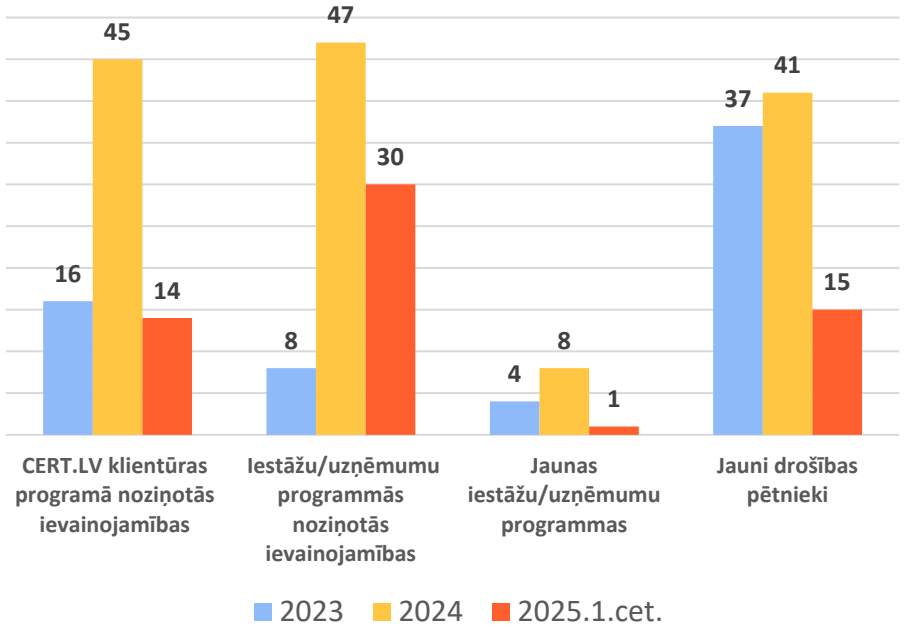
2025. gada 1. ceturksnī CERT.LV Kiberdrošības testēšanas grupa veica **8** IT sistēmu drošības testus dažādās publiskā sektora iestādēs un IKT kritiskās infrastruktūras organizācijās, kā arī veica **4** pikšķerēšanas uzbrukumu simulācijas kampaņas, veicinot un stiprinot personāla aizsardzību pret sociālās inženierijas uzbrukumiem un mazinot cilvēciskā faktora riskus. Papildu tam CERT.LV veica arī vairākas ārpus kārtas drošības pārbaudes publiskā sektora tīmekļvietnēm. Kopskaitā drošības testos tika identificētas **32** ievainojamības, no kurām kritiskas - **3**, augsta riska – **5**. Pateicoties testiem, tās tika proaktīvi novērtas.

Koordinēta ievainojamību atklāšana (CVD)

CVD ziņošanas prakse palīdz savlaicīgāk uzzināt par ievainojamībām, koordinēt ievainojamību izpēti un to novēršanu, un efektīvāk organizēt pasākumus aizsardzībai. 2025. gada 1. ceturksnī CVD platformā Drošības pētnieku skaits pieauga par **15**, kas ir par **67%** vairāk nekā iepriekšējā ceturksnī. Laika posmā no 2024. gada marta līdz 2025. gada martam reģistrēti **124 ievainojamību ziņojumi**, pārskata periodā skaits pieauga par **44**.



9. attēls. 124 ievainojamību ziņojumi; periods: 01.03.2024 - 01.03.2025.



10. attēls. CVD platforma: Ievainojamību ziņojumu skaits Latvijā

Organizāciju IKT infrastruktūras efektīvai aizsardzībai un kibernoturības stiprināšanai CERT.LV piedāvā plašu kiberdrošības pakalpojumu klāstu.
Aizsargājiet un stipriniet savu kibertelpu jau šodien, izmantojot CERT.LV ekspertīzi un ieteikumus: **https://cert.lv/lv/pakalpojumi**
Par vēlmi saņemt CERT.LV pakalpojumu aicinām rakstīt uz **cert@cert.lv**