

2025  
C4

SITUĀCIJA LATVIJAS KIBERTELPĀ  
PERIODS: 01.10.2025. - 31.12.2025.



# Kopsavilkums

Kiberapdraudējumu līmenis Latvijā saglabājas **augsts ar noturīgu augšupejošu tendenci**. Kopš Krievijas pilna mēroga iebrukuma Ukrainā **kiberincidentu** skaits Latvijas kibertelpā ir **seškārtšojies** – 2025. gada 4. ceturksnī fiksēts vēsturiski augstākais CERT.LV manuāli apstrādātu kiberincidentu skaits (923), savukārt **apdraudēto iekārtu skaits ir pieaudzis astoņkārtīgi**, pārskata periodā **sasniedzot rekordaugstu līmeni** (731 783).

Uzbrukumi ir gan finansiāli, gan politiski motivēti, un arī ģeopolitiskie faktori turpina būt nozīmīgs draudu katalizators. Pieaug ne tikai uzbrukumu intensitāte un sarežģītība, bet arī uzbrucēju spēja pielāgoties, un tas savukārt veicina atbilstošu aizsardzības tehnoloģisko risinājumu attīstību, pieprasījumu pēc datos balstītiem pakalpojumiem un reakcijas spēju stiprināšanu publiskajā un privātajā sektorā.

2025. gada 4. ceturksnī Latvijas kibertelpā **krāpšana ir dominējošais** kiberincidentu pieauguma virzītājspēks, radot būtiskus un pieaugošus finanšu riskus iedzīvotājiem un organizācijām. Pastiprinās sociālā inženierija ar efektīvu mākslīgā intelekta rīku un automatizācijas pielietojumu, kas paātrina identitātes zādzības un kontu kompromitēšanu.

CERT.LV proaktīvi monitorē krāpšanas kampaņas un atzinīgi vērtē iedzīvotāju iesaisti krāpniecisku tīmekļvietņu identificēšanā un ziņošanā. Saņemtie ziņojumi tiek apkopoti, un kaitnieciskie domēna vārdi tiek ievietoti DNS ugunsmūrī. Pārskata periodā **DNS ugunsmūris pasargāja lietotājus no ļaunprātīgu vietņu apmeklēšanas 1,03 milj. reizes**, kas liecina par **rekordaugstu krāpšanas kampaņu intensitāti**.

Vienlaikus krāpšanas radītā kaitējuma pieaugums valstī, īpaši ārpus banku maksājumu kanāliem, norāda uz **kritisku nepieciešamību stiprināt sabiedrības digitālo prātību un noturību**, kā arī elektronisko sakaru operatoru lomu telefonkrāpšanas gadījumu novēršanā.

**Ievainojamību ekspluatācija un straujš kompromitētu iekārtu skaita pieaugums** liecina par botu tīklu, inficētu gala iekārtu un vājas konfigurācijas eskalāciju, palielinot risku turpmākiem mērķētiem uzbrukumiem.

**Būtiskus riskus rada pakalpojumatteices (DDoS) uzbrukumi**, kas vērsti pret valsts iestādēm, informācijas un komunikācijas tehnoloģiju (turpmāk – IKT) kritisko infrastruktūru un pakalpojumu sniedzējiem. Krievijas atbalstošo haktīvistu kiberdraudu aktivitāšu Latvijā primārie mērķi ir mazināt Latvijas atbalstu Ukrainai. Līdz šim fiksētie incidenti nav radījuši būtisku vai paliekošu ietekmi uz sabiedrības pamatfunkcijām, kas norāda uz esošo aizsardzības pasākumu efektivitāti.

Saglabājas **kiberspiegošanas draudi**, kas potenciāli varētu būt saistāmi ar Krieviju. Interese par Latvijas IKT kritisko infrastruktūru nav mazinājusies arī no Ķīnas un Baltkrievijas atbalstītiem kiberuzbrucējiem. **Pieaug netiešie riski, kas saistīti ar piegādes ķēdēm** un ārpakalpojumu sniedzēju izmantošanu kā biežāko “**apvedceļu**” uz **mērķa infrastruktūru**.

Lai gan Latvijas kibedrošības regulējums kopumā kļūst strukturētāks, **kiberdraudu automatizācija un pieaugošais kiberuzbrukumu temps arvien vairāk izaicina organizāciju spēju savlaicīgi identificēt uzbrukumus**. Ātrāka un efektīvāka kiberapdraudējumu atklāšana tiek panākta, apvienojot kibertelpas situācijas 24/7 monitorēšanu, Drošības operāciju centra (turpmāk – SOC) nodrošināto uzraudzību, proaktīvas draudu medības un mērķtiecīgu cilvēkfaktora un piegādes ķēdes drošības stiprināšanu.

# Satura rādītājs

<b>Kopsavilkums</b>	<b>1</b>
<b>1. Kibertelpas drošības apdraudējumi: statistika un tendences</b>	<b>3</b>
<b>2. Izplatītākie kiberaudraudējumi un būtiskākie notikumi pārskata periodā</b>	<b>5</b>
Kiberdraudu struktūras analīze pēc incidentu veidiem	5
TOP 6 kvantitatīvi lielākie kiberaudraudējuma veidi pārskata periodā	6
Ietekmes novērtējums	7
TOP 10 jaunatūras	8
Galvenie secinājumi	9
<b>3. CERT.LV pakalpojumi: uzraudzība, aizsardzība un testēšana</b>	<b>9</b>
DNS ugunsmūris	10
Sensoru tīkls	10
Drošības operāciju centrs (SOC)	11
Kiberdrošības draudu medību operācijas	13
IT sistēmu drošības testi, pikšķerēšanas uzbrukumu simulācijas	14
Koordinēta ievainojamību atklāšana (CVD)	15
<b>4. Kiberdrošības stiprināšana ar visu sabiedrību aptverošiem pasākumiem</b>	<b>16</b>



# 1. Kibertelpas drošības apdraudējumi: statistika un tendences

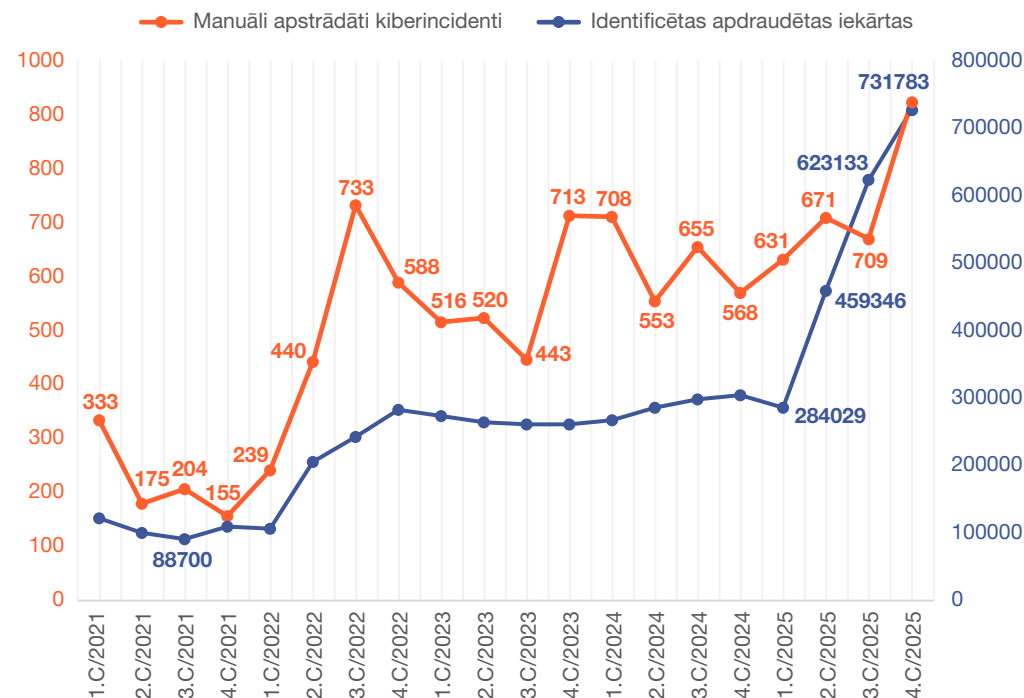
## Kiberincidentu un apdraudēto iekārtu dinamika

2025. gada 4. cet. Latvijā fiksēts **vēsturiski augstākais manuāli apstrādāto kiberincidentu<sup>1</sup> skaits – 923** incidenti, kas nozīmē **+62%** pieaugumu salīdzinājumā ar 2024. gada 4. cet. un **+38%** pieaugumu pret 2025. gada 3. cet.

Kopš Krievijas uzsāktā kara Ukrainā, kiberincidentu skaits Latvijas kibertelpā ir seškārtšojies, un novērojama noturīga augšupejoša tendence. Tas norāda uz palielinātu manuālās analīzes slodzi gan CERT.LV kiberincidentu reaģēšanas un SOC komandu darbā, gan incidentu apstrādes ekosistēmai kopumā.

Vienlaikus tas korelē ar krasu **identificēto apdraudēto iekārtu skaita vēsturiski augstāko pieaugumu** – kopš 2022. gada apdraudējumu skaits astoņkārtšojies. 2025. gads iezīmē kvantitatīvu lūzuma punktu, kur kiberincidentu apjoms vairs nepieaug lineāri, bet lēciens augšup notiek strauji, 4. cet. sasniedzot **731 783**, kas nozīmē **+141%** pieaugumu salīdzinājumā ar 2024. gada 4. cet. un **+17%** pieaugumu pret 2025. gada 3. cet.

Tas liecina par pieaugošu automatizētu botu tīklu uzbrukumiem un automatizētu skenēšanas, ievainojamību un konfigurācijas nepilnību izmantošanas pieaugumu, kā arī uzsver nepieciešamību prioritizēt proaktīvu kibernetdrošības pieeju – agrīnu apdraudējumu atklāšanu un kapacitātes stiprināšanu, lai mazinātu incidentu eskalācijas un ietekmes risku.



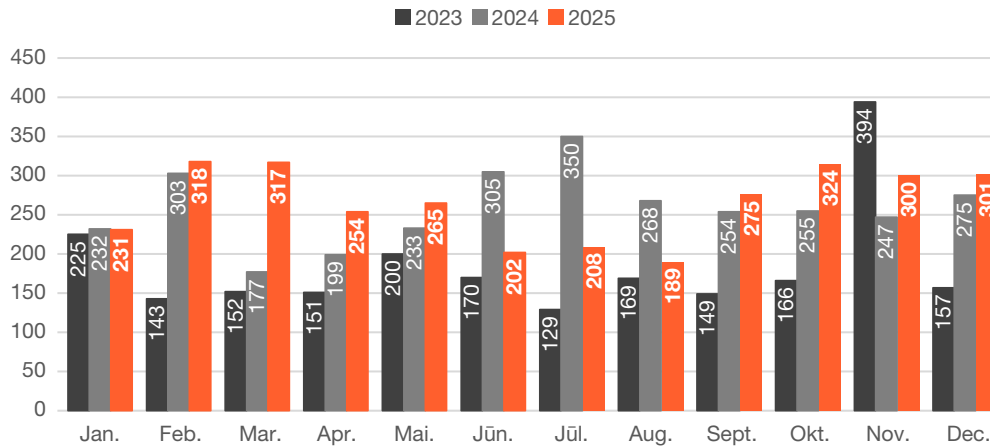
1. attēls. Kiberincidentu un identificētu apdraudētu iekārtu dinamika (skaits ceturkšņu dalījumā; 2021.-2025. gads)

Uzbrukumu klāsts ir plašs un ietver:

- ▶ citu valstu atbalstītu grupējumu darbības;
- ▶ finansiāli motivētus kibernetuzbrukumus;

Ir vairāki pozitīvi piemēri ar incidentiem, kas varēja notikt, bet nenotika, jo savlaicīgi veicot ielaušanās testus, CERT.LV komanda agrīni atklāja un novērsa ievainojamības, tādējādi novēršot būtisku kiberincidentu risku.

<sup>1</sup> 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. attēls. Kiberincidentu dinamika (skaits mēnešu dalījumā)

Pārskata periodā mēnešu dalījumā manuāli apstrādāto kiberincidentu skaits kopumā ir bijis salīdzinoši stabils un augsts, kas ir raksturīgi gada nogalei un svētku sezonai, kad atlaižu un "īpašo piedāvājumu" kļūst vairāk, un līdz ar to aktivizējas arī krāpnieki. Tas nozīmē paaugstinātu apdraudējumu un prasa īpašu modrību.

CERT.LV kiberincidentu reaģēšanas un SOC komandas ik dienu demonstrē augstu gatavību un spēju reaģēt uz dažādiem kiberdrošības izaicinājumiem, sniedzot nepieciešamo atbalstu organizācijām un privātpersonām.

Nacionālā kiberdrošības likuma (turpmāk – NKDL) subjekti, kas izmanto CERT.LV pakalpojumus, tostarp ir ieviesuši SOC pakalpojumus, apdraudējumus spēj ātrāk atklāt un efektīvāk novērst.

### Ieteikumi organizāciju IKT drošībai

- ▶ Regulāri veikt visaptverošu iekārtu un sistēmu inventarizāciju pilnīgam priekšstatam par infrastruktūru, lai savlaicīgi pamanītu un novērstu riskus, ko rada novecojis vai neaizsargāts aprīkojums.
- ▶ Nepieļaut IT resursu lieku eksponēšanu publiskajā internetā, piekļuvi nodrošināt tikai caur drošiem risinājumiem, izmantojot daudzfaktoru autentifikācijas risinājumus (MFA / 2FA) vai šifrēšanu.
- ▶ Regulāri sekot programmatūras izstrādātāju atjauninājumiem, savlaicīgi uzstādot visām sistēmām jaunākos pieejamos drošības ielāpus.
- ▶ Ieviest centralizētu atjauninājumu pārvaldību, nodrošinot nepārtrauktu uzraudzību visās sistēmās.
- ▶ Regulāri veikt ievainojamību skenēšanu, lai identificētu vājās vietas un samazinātu riskus no zināmām ievainojamībām.

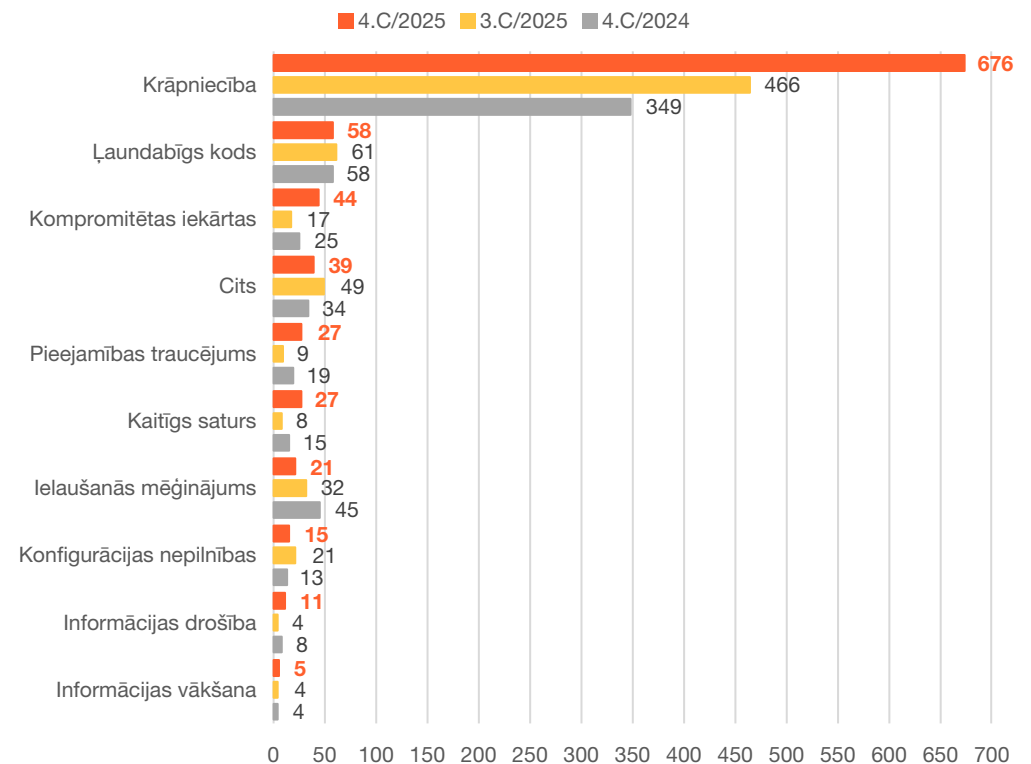
**"Kiberlaikapstākļu" vērotājiem CERT.LV piedāvā ikmēneša pārskatu vienkāršā valodā par būtiskākajiem un spilgtākajiem kiberincidentiem un apdraudējumiem Latvijas kibertelpā TOP 5 kategorijās. Pārskats pieejams tīmekļvietnē CERT.LV OKTOBRIS | NOVEMBRIS | DECEMBRIS**

## 2. Izplatītākie kiberapdraudējumi un būtiskākie notikumi pārskata periodā

### Kiberdraudu struktūras analīze pēc incidentu veidiem

Vairumā kiberincidentu veidos novērojams pieaugums pret 2024. gadu, savukārt salīdzinājumā ar 2025. gada 3. cet. aina ir nevienmērīga – daļa risku pieaug, daļa samazinās.

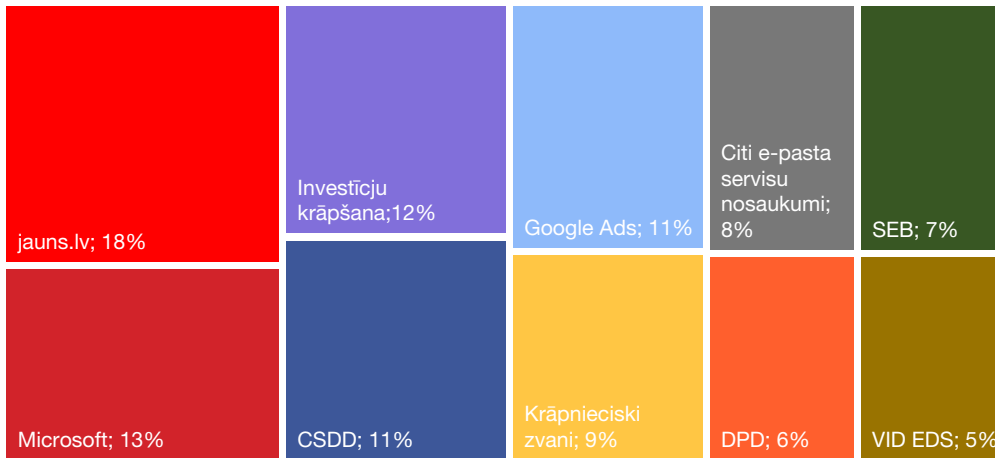
- ▶ **Dominējošais incidentu veids ir krāpšana, kas veido absolūto vairākumu un nosaka kopējo pieauguma dinamiku.** Tendences norāda uz masveidīgu sociālās inženierijas un mākslīgā intelekta (MI) rīku izmantošanu automatizēšanai un satura izveidei.
- ▶ **Tehniskie uzbrukumi** (ielaušanās, ļaunatūras) absolūtos skaitļos pārsvarā stagnē, vienlaikus tehniskajā līmenī iezīmējās **jaunas, bīstamas sociālās inženierijas un ļaunprogrammatūru kampaņas**, īpaši “ClickFix” metodes evolūcija. Microsoft 365 vidē fiksēti incidenti, kuros uzbrucēji **spēj apiet daudzfaktoru autentifikāciju (MFA)**. Finansiāli motivēti uzbrucēji aktīvi izmanto **“Infostealer” tipa datu zādzības ļaunatūras** lietotāju autentifikācijas datu izgūšanai.
- ▶ **Gan kompromitētu iekārtu skaits, gan pieejamības traucējumi (turpmāk – DDoS) strauji aug** ceturkšņa griezumā, norādot uz pieaugošu automatizētu apdraudējuma fonu. Lielākoties DDoS uzbrukumi norit, neradot ietekmi uz pakalpojumu darbību, un tie tiek atvairīti automātiski. Aizsardzības ministrija finansē centralizētu DDoS aizsardzības pakalpojumu – valsts pārvaldes iestādēm tas pieejams bez maksas. Pakalpojuma nodrošināšana deleģēta Latvijas Valsts radio un televīzijas centram.
- ▶ CERT.LV kiberdrošības draudu medību rezultāti liecina, ka **uzbrucēji bieži izmanto ārpalpojumu sniedzējus kā sākotnējo piekļuves punktu mērķa infrastruktūrai**, kas kļūst par “tiltu” tālākam uzbrukumam. **Līdzīgas pieejas tiek izmantotas arī programmatūras ekosistēmā**, lai ievietotu ļaunatūru vai manipulētu ar programmatūru piegādes ķēdi, izmantojot uzticamus kanālus un izstrādes vidi.



3. attēls. Kiberincidentu veida un skaita salīdzinājums

## TOP 6 kvantitatīvi lielākie kiberapdraudējuma veidi pārskata periodā

Apdraudējuma veids: manuāli apstrādātu incidentu skaits 2025. gada 4. cet.	Izmaiņas pret 2025. g. 2. cet.	Izmaiņas pret 2024. g. 3. cet.	Būtiskākie secinājumi
<b>KRĀPŠANA:</b> <b>676</b>	+94%	+45%	<ul style="list-style-type: none"> <li>▶ <b>Ļoti straujš un noturīgs pieaugums</b>, kas liecina par intensīvām sociālās inženierijas kampaņām. Novērota aktīva pikšķerēšana, smikšķerēšana un telefonkrāpšana. Dominēja <b>investīciju krāpšanas</b>, izmantojot viltus tīmekļvietnes ar maldinošiem rakstiem par “izdevīgām investīciju iespējām”, kuros ļaunprātīgi izmantoja sabiedrībā atpazīstamu personu tēlus (piemēram, premjerministre u.c.), lai radītu uzticamības ilūziju.</li> </ul>
<b>ĻAUNDABĪGS KODS:</b> <b>58</b>	Bez izmaiņām	-5%	<ul style="list-style-type: none"> <li>▶ Apjoms saglabājas liels un stabils, novērojami pastāvīgi ļaunatūras riski. Iezīmējās <b>bīstama sociālās inženierijas un “ClickFix” metodes</b> (lietotājs tiek mudināts pats “salabot” it kā radušos problēmu) <b>evolūcija</b>.</li> <li>▶ <b>Datu zādzības tipa ļaunatūras</b>, kas zog paroles, sīkdatnes u.c. datus, ir viens no <b>visstraujāk augošajiem</b> kiberdraudu veidiem.</li> <li>▶ Ļaunatūru statistika labi atspoguļo problēmas saistībā ar <b>SOHO un Edge tīkla iekārtu ievainojamībām</b> – vairākas izplatītākās ļaunprogrammatūras ir tieši saistītas ar mazo rūteru un citu Edge ierīču kompromitēšanu.</li> </ul>
<b>KOMPROMITĒTAS IEKĀRTAS:</b> <b>44</b>	+76%	+159%	<ul style="list-style-type: none"> <li>▶ Ceturkšņa griezumā novērojams ļoti straujš pieaugums, kas norāda uz <b>botu tīklu paplašināšanos, inficētu gala iekārtu skaita pieaugumu un plaši izplatītām nepareizi vai vāji konfigurētām sistēmām</b>. Šāda dinamika var kalpot kā priekšnoteikums turpmākiem kiberuzbrukumiem.</li> </ul>
<b>PIEEJAMĪBAS TRAUCĒJUMI:</b> <b>27</b>	+42%	+200%	<ul style="list-style-type: none"> <li>▶ Novērojams būtisks pieaugums, it īpaši salīdzinājumā ar 2025. gada 3. cet., lai gan absolūtais skaits joprojām ir mērens.</li> <li>▶ Ne katrs pakalpojuma pārtraukums ir DDoS – atsevišķos gadījumos to izraisīja <b>konfigurācijas kļūdas</b>, kas norāda uz <b>nepieciešamību uzlabot pārbaudes procedūras</b>.</li> <li>▶ Novembrī globāli pieredzētais Cloudflare pakalpojuma pārtraukums, izraisot kaskādes efektu, ietekmēja daudzu tīmekļvietņu un digitālo servisu darbību arī Latvijā. Šis incidents skaidri parāda - <b>paļaušanās tikai uz vienu risinājumu palielina risku</b>, jo pārtraukums var izraisīt plašu pakalpojumu nepieejamību, un sākas ķēdes reakcija – tīmekļa vietnes un servisi kļūst daļēji vai pat pilnībā nepieejami.</li> </ul>
<b>KAITĪGS SATURS:</b> <b>27</b>	+80%	+238%	<ul style="list-style-type: none"> <li>▶ Straujš kāpums, lai gan absolūtais skaits joprojām ir mērens. Pieaugums lielā mērā saistāms ar krāpniecisku, ļaunprātīgu tīmekļa saturu, kas pārklājas ar krāpšanas tendencēm.</li> </ul>
<b>KONFIGURĀCIJAS NEPILNĪBAS:</b> <b>15</b>	+15%	-29%	<ul style="list-style-type: none"> <li>▶ Samazinājums ceturkšņa griezumā, iespējams, liecina par uzlabotu kiberhigiēnas praksi, tomēr riski saglabājas.</li> <li>▶ <b>Augsts risks gan gala lietotājiem</b> (7-Zip, Chromium pārlūkprogrammas, Redis u.c.), gan <b>kritiskajai infrastruktūrai</b> (FortiWeb, Ubiquiti UniFi Access, Squid u.c.).</li> <li>▶ Dominē kritiskas attālinātās koda izpildes (<b>RCE</b>) tipa ievainojamības plaši izmantotās tehnoloģijās, kas ļauj uzbrucējiem iegūt pilnu kontroli pār sistēmām.</li> <li>▶ Redzama tendence – uzbrukumos <b>tiekl kombinētas vairākas ievainojamības</b>, lai apietu aizsardzības mehānismus.</li> </ul>



#### 4. attēls. Izplatītākās krāpšanas kampaņas, izmantojot organizāciju nosaukumus (procentuālā daļa no kopējā CERT.LV apstrādāto pikšķerēšanas ziņojumu skaita 2025. gada 4. cet.)

Novērojama tendence – krāpšanas kampaņas kļūst arvien īsākas, precīzāk mērķētas un kontekstuāli pielāgotas. Tiek izmantoti zināmu organizāciju nosaukumi un procesi, un tieši par to, kas konkrētajā brīdī izklausās “ticami”.

Pārskata periodā visvairāk tika izmantotas viltotas tīmekļvietnes, atdarinot reālas vietnes, piemēram, jauns.lv, un izplatot maldinošus reklāmrakstus, kuros izmantoti sabiedrībā zināmu personu tēli, lai radītu ticamību krāpnieciskiem investīciju piedāvājumiem.

Pikšķerēšanas kampaņās aktīvi tika izmantota Google Ads sponsorēto lapu izvietošana Google meklētājā, lai novirzītu lietotājus uz krāpniecisku lapu. Piemēram, ierakstot Google meklētājā vārdu “ibanka”, kā pirmie (sponsorētie) meklēšanas rezultāti parādījās krāpnieku izveidotas viltotas lapas, kas vizuāli atgādināja SEB bankas internetbanku.

Fiksētas krāpnieciskas kampaņas valsts iestāžu vārdā (it īpaši CSDD), pieaug krāpnieciski zvani, kuros uzdodas par dažādu organizāciju pārstāvjiem, novēroti smikšķerēšanas gadījumi piegādes uzņēmumu vārdā, kā arī cita veida krāpšanas gadījumi.

## Ietekmes novērtējums

- ▶ Svētku un izpārdošanu periodos finanšu zaudējumu riskus būtiski palielina krāpnieciskas kampaņas, viltotas tīmekļvietnes, kontu kompromitēšana un lietotāju neuzmanība paaugstinātas aktivitātes un steigas apstākļos.
- ▶ Plaši izplatīta personas datu un identitātes zādzība, un lietotāju kontu kompromitēšana.
- ▶ Sabiedrības informētības un digitālās prasmes trūkumi joprojām ir būtiski.

Saskaņā ar Valsts policijas informāciju 2025. gada pirmajos 10 mēnešos iedzīvotāju zaudējumi krāpšanas rezultātā sasnieguši 17,99 milj. eiro.

**Finanšu nozares asociācijas** dati rāda informāciju – 2025. gada pirmajos 11 mēnešos finanšu krāpniekiem no Latvijas iedzīvotājiem izdevies izkrāpt 10,954 milj. eiro, kas ir par 26% mazāk nekā attiecīgajā periodā pērn. Vienlaikus bankām izdevies pasargāt iedzīvotājus no zaudējumiem 12,749 milj. eiro apmērā.

Tas norāda uz banku preventīvo pasākumu efektivitātes pieaugumu, taču vienlaikus – uz kopskaitā krāpšanas radītā kaitējuma pieaugumu valstī, īpaši ārpus banku maksājumu kanāliem. Turklāt telefonkrāpšanas gadījumos izkrāpto līdzekļu apmērs sasniedz gandrīz 5,91 milj. eiro, kas norāda uz kritisku nepieciešamību stiprināt elektronisko sakaru operatoru lomu telefonkrāpniecību novēršanā.

Valsts policijas un Finanšu nozares asociācijas sniegtā statistika atšķiras, jo Finanšu nozares asociācijas dati apkopo informāciju tikai par Latvijas finanšu tirgus dalībniekiem, savukārt Valsts policijas statistika aptver arī ārpus Latvijas finanšu institūcijām notiekošo.

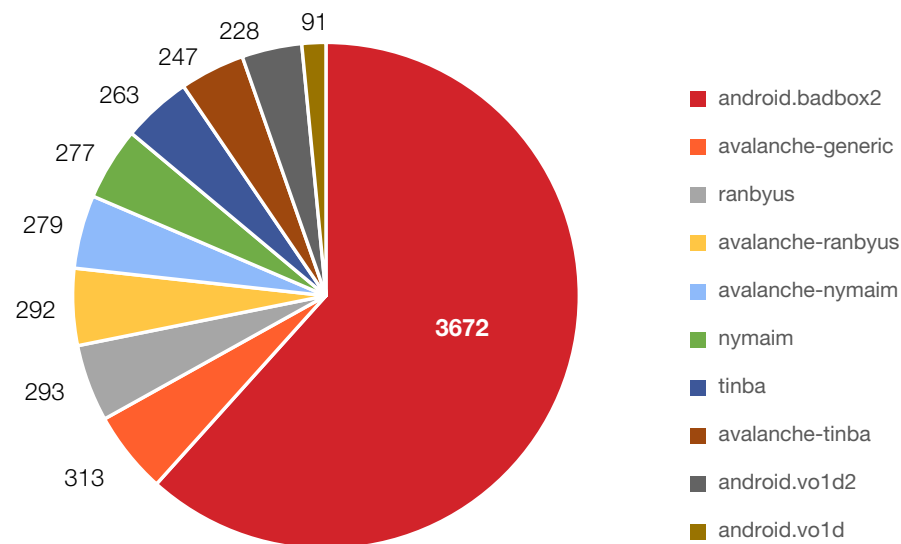
## 5 vienkārši soļi lietotāju drošībai digitālajā vidē

- ▶ Izmantot spēcīgas, unikālas paroles un visur, kur iespējams, iespējot daudzfaktoru autentifikāciju (MFA/ 2FA).
- ▶ Savlaicīgi atjaunināt operētājsistēmas, lietotnes un pārlūkprogrammas.
- ▶ Neatvērt aizdomīgas saites un pielikumus (īpaši, ja rada steidzamības sajūtu).
- ▶ Ierobežot publiskā Wi-Fi izmantošanu vai lietot VPN, pieslēdzoties sensitīviem kontiem.
- ▶ Izmantot DNS ugunsmūra mobilo lietotni.

## TOP 10 ļaunatūras

2025. gada 4. cet. izplatītāko ļaunatūru tipi liecina par masveidīgiem, automatizētiem un ilgstošiem apdraudējumiem.

- ▶ Ļaunatūru TOP 10 augšgalā pārlicinoši dominē ļaunatūra “Android. badbox2”, kas ir mobilais botu tīkla variants un spēj inficēt ierīces, veicot, piemēram, piekļuves datu zagšanu un attālinātu kontroli par ierīci. Tās izplatība norāda uz būtisku un mērķtiecīgu aktivitāti Android ierīcēs un liecina par masveida inficēšanas kampaņām, izmantojot neoficiālas lietotņu instalācijas vai viltus atjauninājumus.
- ▶ Galvenie riski – piekļuves datu pārtveršana, inficētu gala ierīču kompromitēšana un izmantošana turpmākos kiberuzbrukumos. Organizācijas un individuālie lietotāji var pat nezināt, ka viņu IP adrese “piedalās” botu tīkla uzbrukumos.
- ▶ Pārējās topa ļaunatūras kopā veido kvantitatīvi mazāku daļu, tomēr parāda daudzveidīgu uzbrukumu vektoru kombināciju un palielina kompromitēšanas riskus.



5. attēls. TOP 10 ļaunatūras; skaits 2025. gada 4. ceturksnī

## Izplatītākie ļaunatūru tipi

- ▶ Lietotāju datu zādzības ļaunatūras
- ▶ Botu tīkli
- ▶ Attālinātās kontroles trojāni datu izgūšanai un infrastruktūras kompromitēšanai

“Infostealear” tipa datu zādzības ļaunatūra tiek izmantota piekļuves datu izgūšanai no tīmekļa pārlūka vai nešifrētiem failiem. Tā tiek izplatīta kā ļaundabīgs tīmekļa pārlūka spraudnis vai kā izpildfails, pievienots pie pikšķerēšanas e-pasta vēstules.

## Citu valstu atbalstīti kibernetu uzbrukumi

<p><b>Krievija</b></p>	<ul style="list-style-type: none"> <li>▶ Krievijas atbalstītie uzbrukumi (APT – Advanced Persistent Threat) paplašina savu darbību un īsteno kibernetu operācijas plašāk nekā iepriekš, taču kopējā uzbrukumu kvalitāte ir pazeminājusies, kas norāda uz uzbrukēju profesionalitātes kritumu, bet vienlaikus – uz pieaugošu mērogu un apjomu, ar kādu tiek mēģināts ietekmēt kibertelpu.</li> <li>▶ Krievija ir joprojām galvenais reģiona apdraudējuma avots, kas savieno tehniskus uzbrukumus ar informatīvo ietekmēšanu, turklāt jebkurš līdzeklis, kas var nodarīt kaitējumu, tiek uzskatīts par pieņemamu un pielietojamu.</li> </ul>
<p><b>Baltkrievija</b></p>	<ul style="list-style-type: none"> <li>▶ Mazāk nozīmīgs spēlētājs, pārsvarā iesaistās epizodiskās kampaņās, visticamāk, Krievijas “orķestrētās”.</li> <li>▶ Aktivitātes vairāk saistītas ar informatīvās telpas ietekmēšanu un retāk – ar tehniski izsmalcinātām kibernetu operācijām.</li> </ul>
<p><b>Ķīna (ĶTR)</b></p>	<ul style="list-style-type: none"> <li>▶ Ar ĶTR saistāmie grupējumi Latvijā novērojami arvien biežāk.</li> <li>▶ Ja iepriekš tie pārsvarā izmantoja ievainojamības Edge tīkla iekārtās (VPN vārtejas, uguns mūris u.c.), lai iegūtu sākotnējo piekļuvi, tagad vērojama mērķtiecīgāka un agresīvāka izplatīšanās tīklos.</li> </ul>

Rietumvalstis, tostarp Latvija, saskaras ar sabotāžas mēģinājumiem pret to kritiskās infrastruktūras objektiem. Krievija un Baltkrievija **kā ieročus pret rietumvalstīm izmanto operacionālās tehnoloģijas (OT)** – enerģētikas, ūdens, siltumapgādes infrastruktūru, kā arī **dronus un citas bezpilota platformas**, lai destabilizētu sabiedrisko un ekonomisko vidi.

Lai gan visbiežāk kibernetu uzbrukumu veicēji ir kibernetu uzbrukuma speciālisti, arī valstiski atbalstītas grupas turpina mērķēt uz stratēģiski svarīgām nozarēm, **galvenokārt spiegošanas, bet nereti arī finansiāla labuma dēļ.**

APT uzbrukumi tiek veikti pēc noteiktām shēmām, un arvien biežāk ir iespējams tos paredzēt un **atbilstoši reaģēt, attīstot atturēšanas spējas, padarot Latviju par uzbrukējam neparocīgāku mērķi.**

## Galvenie secinājumi

Ģeopolitiskie un ideoloģiskie konflikti joprojām ir spēcīgs kibernetu uzbrukumu katalizators. Pieaugoša kibernetu uzbrukumu aktivitāte un arvien plašāka spektra kibernetu apdraudējumi, ko pastiprina MI rīku izmantošana un automatizācija, ir veicinājusi kibernetu incidentu skaita pieaugumu arī Latvijā, īpaši krāpšanas, kompromitētu iekārtu un automatizētu uzbrukumu kategorijās.

Līdz šim fiksētie incidenti nav radījuši būtisku vai paliekošu ietekmi uz sabiedrības pamatfunkcijām, kas norāda uz esošo aizsardzības pasākumu efektivitāti. Vienlaikus krāpšanas radītā kaitējuma pieaugums valstī, īpaši ārpus banku maksājumu kanāliem, norāda uz kritisku nepieciešamību stiprināt sabiedrības digitālo pratību un noturību. Ir būtiski arī stiprināt elektronisko sakaru operatoru lomu telefona zvanu krāpšanas gadījumu novēršanā.

Neraugoties uz salīdzinoši spēcīgu normatīvo regulējumu, pieejamām tehnoloģijām un valsts atbalstu aizsardzības spēju stiprināšanai, apdraudējumu risks saglabājas augsts.

Individuālā līmenī jāveicina daudzfaktoru autentifikācijas izmantošana (MFA/ 2FA) un izpratne par kibernetu higiēnas nozīmi, kas var būtiski samazināt krāpniecības, personas datu noplūdes un kontu kompromitēšanas riskus.

Organizāciju ilgtspējīgu noturību var nodrošināt tikai ar daudzslāņainu pieeju, kur kibernetu drošība ir integrēta organizāciju vadības stratēģiskajos lēmumos, ikdienas operacionālajā darbībā un lietotāju uzvedībā, apvienojot tehnoloģiskos risinājumus, SOC 24/7 uzraudzību, regulāru testēšanu un mērķtiecīgu darbinieku apmācību. Tas palīdz būtiski samazināt gan kibernetu incidentu iespējamību, gan to ietekmi uz darbības nepārtrauktību, sensitīviem datiem, reputāciju un finanšu stabilitāti.

### 3. CERT.LV pakalpojumi: uzraudzība, aizsardzība un testēšana

CERT.LV pakalpojumi, tostarp DNS ugunsmūris, atbalsts incidentu risināšanā, SOC 24/7 uzraudzība, kibernetikas draudu medības, drošības testi, sabiedrības izglītošana un apmācības u.c., ir būtisks atbalsts risku mazināšanai un noturības stiprināšanai pret pieaugušiem kibernetikas draudiem. Savukārt Aizsardzības ministrijas izstrādātais kibernetikas regulējums nodrošina sadarbības ietvaru, kas nosaka atbildības, pienākumus un minimālās prasības NKDL subjektiem.

#### DNS ugunsmūris

**2025. gada 4. cet.** visu CERT.LV DNS ugunsmūrim uzturēto sarakstu atvairījumi pasargāja lietotājus no ļaunprātīgu vietņu apmeklēšanas **1 028 577 reizes**, kas ir ievērojams pieaugums – par **158%** vairāk nekā 2025. gada 3. cet. un par **124%** vairāk nekā pērn 4. cet. (pārskata perioda statistikā nav iekļauti dati par citu valsts kompetento iestāžu sarakstiem par nelikumīga tiešsaistes satura ierobežošanu).

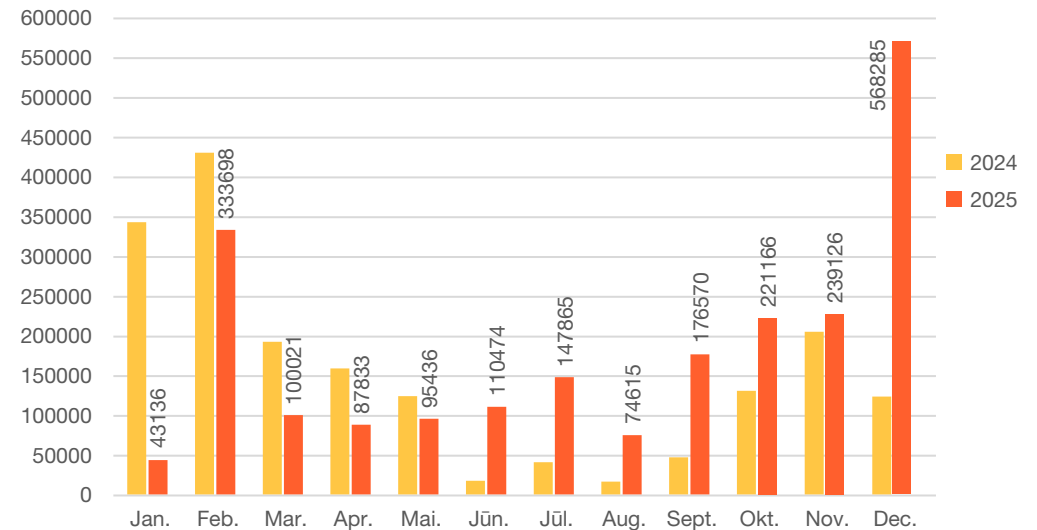
Iespējamie pieauguma iemesli ir sezonālie un kontekstuālie faktori, kā arī atvairījumu skaitu tiešā veidā ietekmē aktīvo krāpniecības kampaņu skaits.

CERT.LV proaktīvi monitorē un savlaicīgi aptur krāpnieciskās kampaņas, un vienlaikus atzinīgi vērtē iedzīvotāju iesaisti, kuri identificē un pārsūta krāpnieciskus e-pastus un tīmekļa vietnes uz cert@cert.lv. Saņemtie ziņojumi tiek apkopoti, un kaitnieciskie domēna vārdi ievietoti DNS ugunsmūrī, lai ierobežotu piekļuvi no LV interneta lietotāju puses un samazinātu iespējamo kaitējumu.

#### Sensoru tīkls

Kibernetikas apdraudējumu agrās brīdināšanas sistēma (ABS) ir CERT.LV nodrošināts pakalpojums, kas veic datu plūsmas anomāliju analīzi un kibernetikas draudumu pazīmju identificēšanu pakalpojuma saņēmēja infrastruktūrā. CERT.LV turpina ABS sistēmas uzturēšanu un paplašināšanu.

2025. gada 4. cet. ABS ģenerēto brīdinājumu skaits bija aptuveni 800 milj., kas ir mazāk nekā iepriekšējā ceturksnī. Apjoma kritums skaidrojams ar pielietotās indikatoru kopas optimizēšanu.



6. attēls. Visu CERT.LV DNS ugunsmūra uzturēto sarakstu atvairījumi, kas pasargāja lietotājus no ļaunprātīgu vietņu apmeklēšanas

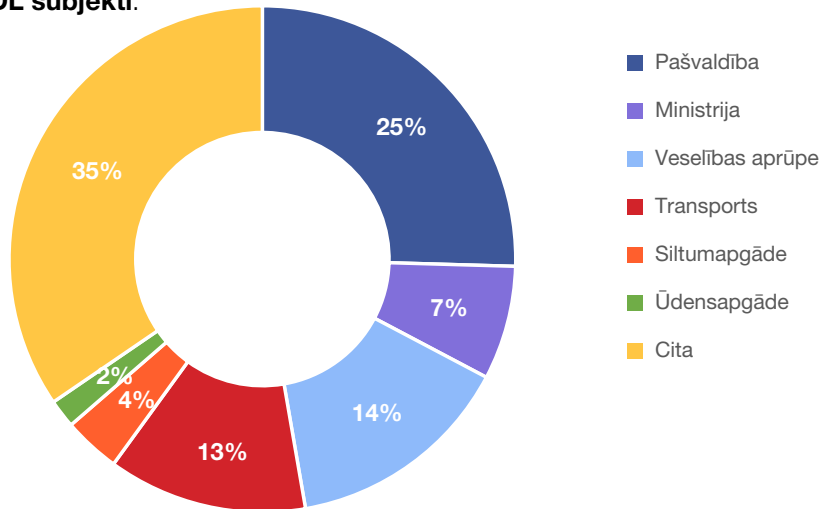
ABS vidēji ik mēnesi fiksē **6 000** augstas prioritātes kibernetikas draudumus (incidentus ar augstu bīstamības potenciālu) valsts, pašvaldību un IKT kritiskās infrastruktūras organizācijās.

**> 2,2 milj.** – CERT.LV DNS ugunsmūra uzturēto sarakstu atvairījumu skaits 2025. gadā (pieaugums +20% salīdzinājumā ar 2024. gadu)  
**~75 tūkst.** – DNS ugunsmūra mobilā lietotne lejupielādēta Android un iOS ierīcēs kopskaitā (kopš 2024. gada, kad lietotne tika ieviesta)  
**~30 min.** – Vidējais reakcijas laiks līdz identificēšanai un indikatora ievietošanai bloķēšanas sarakstā  
**~13,1 milj.** – Kaitīgo domēna vārdu DNS pieprasījumi 2025. gadā kopskaitā

## Drošības operāciju centrs (SOC)

Turpinās CERT.LV SOC pakalpojumu attīstīšana un jaunu klientu piesaiste, paplašinot klientu loku atbilstoši NKDL un sekmējot efektīvāku 24/7 aizsardzību un noturību pret kibernetiskajiem draudumiem.

Uz pārskata perioda beigām (31.12.2025.) **CERT.LV SOC pakalpojumus izmanto 55 NKDL subjekti.**



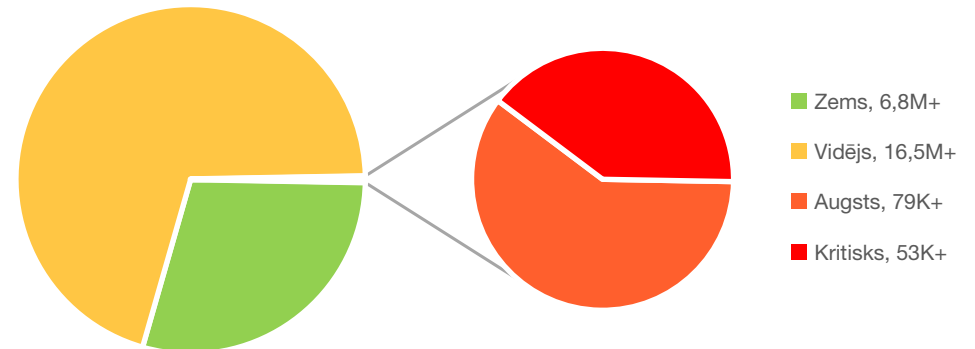
7. attēls. Procentuāls sadalījums ar iestāžu sektoriem, kas izmanto CERT.LV SOC pakalpojumu

### Drošības trauksmes ziņojumu dinamika CERT.LV SOC klientu infrastruktūrā

	Kopskaits
Trauksmes ziņojumu skaits	<b>23M+</b>
Manuāli izveidotas lietas	<b>689</b>
Viltus pozitīvas lietas	<b>521</b>
Incidentu skaits	<b>8</b>
Zems trauksmes līmenis	<b>6,8M+</b>
Vidējs trauksmes līmenis	<b>16,5M+</b>
Augsts trauksmes līmenis	<b>79k+</b>
Kritisks trauksmes līmenis	<b>53k+</b>

### Drošības trauksmes ziņojumu dinamika kopskatā




- **Iegūta redzamība kopskaitā pār 41 534 gala iekārtām**, tostarp serveriem un darbstacijām. 2025. gada 4. cet. iegūta redzamība pār 814 gala iekārtām (pieaugums +2% no kopējā apjoma), līdz ar to palielinājies arī drošības trauksmes ziņojumu skaits.
- **Vairāk nekā 23 milj. drošības trauksmes ziņojumu** – 2025. gada 4. cet. pieaugums +57% pret 2025. gada 3. cet.. Pieaugums skaidrojams ar iegūtu plašāku redzamību jauno klientu infrastruktūrā un nepieciešamo laiku trauksmes ziņojumu apstrādei, lai izmeklētu un noklusinātu viltus pozitīvās trauksmes.
- **689 manuāli izveidotas lietas** – 2025. gada 4. cet. pieaugums +40% pret 3. cet., apstrādājot drošības trauksmes ziņojumus.
- **681 viltus pozitīva lieta.**



8. attēls. Trauksmes ziņojumu līmenis 2025. gada 4. cet.

Pārliecinoši lielākā daļa jeb **70% trauksmju ir vidēja līmeņa**, bet 29% ir zema līmeņa trauksmju, kas saistītas ar sistēmu troksni, viltus pozitīviem, konfigurācijas nepilnībām vai mazāk nopietniem gadījumiem.

## Pārskata periodā konstatētie kiberincidenti un ieteicamā rīcība

Kiberincidents	Sākotnējā piekļuve	Ieteicamā rīcība
<p>Paroļu pilnās pārļases uzbrukumi</p> 	<p>Darbstacijas pieslēgtas ārējam tīklam, apejot korporatīvās drošības politiku; iekārtas eksponētas internetā bez lokāla uguns mūra. Tas palielina ievainojamību pret automatizētiem uzbrukumiem.</p>	<ul style="list-style-type: none"> <li>▶ Uzstādīt lokālos uguns mūrus.</li> <li>▶ Nodrošināt VPN savienojumu ar korporatīvo tīklu.</li> <li>▶ Lietot spēcīgas, unikālas paroles un MFA.</li> </ul>
<p>Nevēlamas programmatūras lietošana korporatīvā vidē</p> 	<p>Neoficiāli aktivizācijas rīki, spēles, failu tiešās apmaiņas programmatūras (BitTorrent) u.c. var saturēt ļaunatūru, kas apdraud sistēmas integritāti un var kompromitēt sistēmu.</p>	<ul style="list-style-type: none"> <li>▶ Ieviest programmatūras "balto" sarakstu.</li> <li>▶ Atinstalēt neautorizētas lietotnes un privātām vajadzībām izmantotās programmas.</li> <li>▶ Noņemt novecojušas / dublējošas programmas.</li> <li>▶ Neizmantot programmatūru no ārpus NATO/ ES ražotājiem.</li> <li>▶ Neizmantot vairākus attālinātās piekļuves rīkus vienlaicīgi.</li> </ul>
<p>Ļaunatūra Trojāni</p> 	<p>No interneta lejupielādētas datnes</p>	<ul style="list-style-type: none"> <li>▶ Ieviest programmatūras "balto" sarakstu.</li> <li>▶ Regulāri atjaunināt pārlūkprogrammas.</li> <li>▶ Lietot pārlūka paplašinājumus, kas bloķē aizdomīgus skriptus.</li> <li>▶ Izglītēt un apmācīt darbiniekus par aktuālajiem kiberriskiem un kiberdrošību.</li> </ul>

## Aptuveni 1% no visām trauksmēm ir augsta līmeņa (vairāk nekā 79 tūkst.).

Tās veido nozīmīgu slodzi SOC komandai, jo ir indikatori potenciāli bīstamiem uzbrukumiem un prasa rūpīgu pārbaudi.

**Kritisko trauksmju skaits** (vairāk nekā 53 tūkst.) kvantitatīvi ir salīdzinoši niecīgs no kopējā apjoma, taču **prasa vislielāko uzmanību**.

Kritiska un augsta līmeņa trauksmju absolūtais skaits (vairāk nekā 133 tūkst.), salīdzinot ar 3. cet., ir **pieaudzis gandrīz četrkārtīgi**. Tas norāda uz pastāvīgiem nopietniem apdraudējumiem.

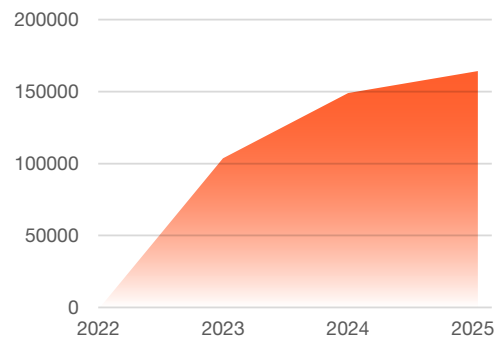
CERT.LV SOC pakalpojuma ietvaros fiksēti **8 kiberincidenti**, kuriem bijusi ietekme uz gala iekārtu vai organizācijas infrastruktūru.

Prakse rāda, ka iestādes un uzņēmumi, kas ir ieviesuši un izmanto CERT.LV SOC pakalpojumus – šādus apdraudējumus spēj daudz ātrāk atklāt un efektīvāk novērst.

## Kiberdrošības draudu medību operācijas

Kopš 2022. gada, kad tika uzsāktas kiberdrošības draudu medības, uz 2025. gada 4. cet. beigām kopskaitā draudu medību operācijās analīze ir veikta:

- ▶ **~163 500** gala iekārtās (4. cet. pieaugums ~1500);
- ▶ **Vairāk nekā 40** NKDL subjektu IKT infrastruktūrās;
- ▶ **APT klātbūtne** iekārtās identificēta aptuveni **20%** no visām analizētajām organizācijām.



9. attēls. Draudu medībās analizēto iekārtu apjoma dinamika (2022-2025)

Tas parāda, ka Latvijas organizācijas, tai skaitā, kritiskās infrastruktūras turētāji ir Krievijas mērķis, un ieviestie CERT.LV pakalpojumi kombinācijā ar vietējo un starptautisko partnerību padara Latviju par arvien neparocīgāku mērķi, jo uzbrucēju darbības tiek atklātas un novērstas ātrāk, un tā tiek panākts atturošs efekts.

## Latvija un Kanāda turpina stiprināt NATO kiberdrošības spējas



Pārskata periodā novembra sākumā Rīgā notika jau trešais četru dienu Draudu medību apmācību kurss par kiberdraudu meklēšanu, ko kopīgi vadīja Kanādas un Latvijas kiberdrošības eksperti.

Apmācību kursa mērķis – atbalstīt un spēcīnāt NATO sabiedroto spējas potenciālo draudu identificēšanā. Mācības tika organizētas sadarbībā ar Aizsardzības ministriju, CERT.LV un Kanādas Bruņoto spēku kiberpavēlniecību. Tajās piedalījās **33** pārstāvji no **11** valstīm.

## IT sistēmu drošības testi, pikšķerēšanas uzbrukumu simulācijas

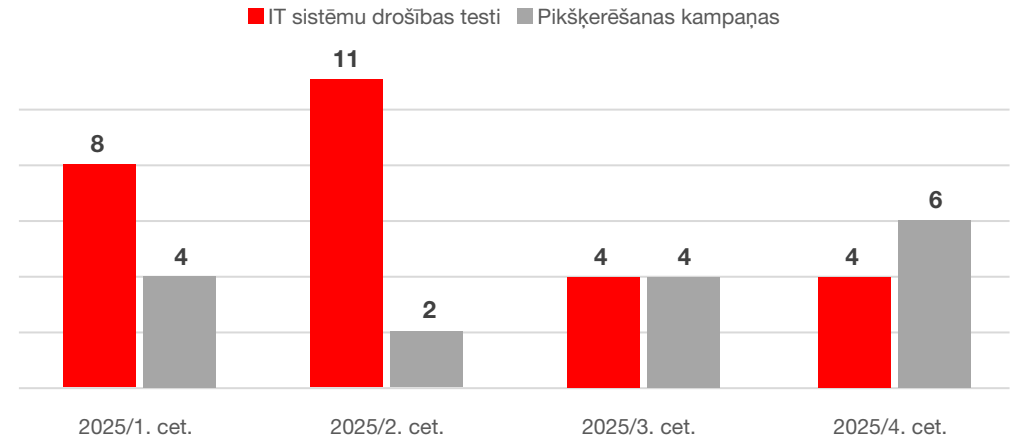
### IT sistēmu drošības testi

2025. gada 4. cet. CERT.LV komanda veica **4** IT sistēmu drošības testus, kuru gaitā identificētas kopskaitā **24** ievainojamības, tostarp **3** kritiskas un **4** augsta riska.

Drošības testu mērķis ir identificēt potenciālas ievainojamības, drošības apdraudējumus un sistēmas nepilnības, lai novērstu iespējamus kiberuzbrukumus un datu noplūdes.

### Pikšķerēšanas uzbrukumu simulācijas kampaņas

Pārskata periodā veiktas **6** pikšķerēšanas kampaņas, lai apmācītu un veicinātu organizāciju darbinieku spējas identificēt potenciāli riskantus uzvedības modeļus, atpazīt un novērst kiberapdraudējumus un informācijas noplūdi. Kopējā kampaņas auditorija: **1 800** personas.



10. attēls. CVD platforma: ievainojamību ziņojumu skaits Latvijā

## Ievainojamību ziņošanas platforma (CVD)

CVD platforma paredzēta, lai atvieglotu valsts pārvaldes un pašvaldību iestāžu sadarbību ar kibersdrošības pētniekiem un uzlabotu IKT resursu drošību.

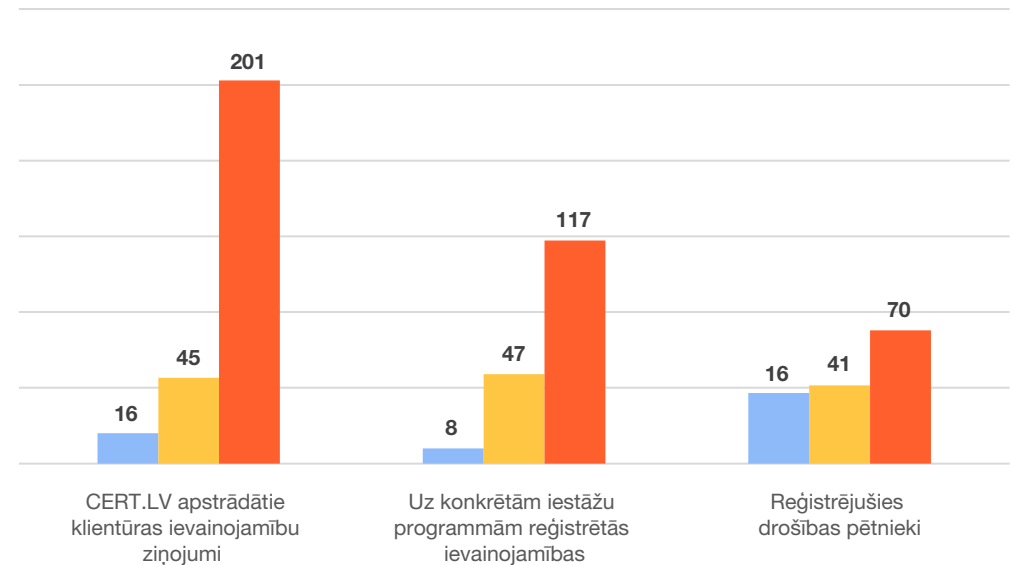
CVD platformā iestāde var reģistrēt informāciju par visiem tās izmantotajiem IKT resursiem, par kuriem tā vēlas saņemt ziņojumus par atklātajām ievainojamībām. Platforma nodrošina pārredzamu un ērtu saskarni, kurā iespējams apskatīt visus saņemtos ziņojumus, kā arī uzturēt saziņu ar pētniekiem un citām iesaistītajām pusēm.

### Uz pārskata perioda beigām (31.12.2025.) CVD platformā kopskaitā reģistrēti:

- ▶ **148** drošības pētnieki (2025. gada 4. cet. pieaugums +16)
- ▶ **434** ievainojamību ziņojumi (2025. gada 4. cet. pieaugums +60), tostarp:
  - ✓ **262** CERT.LV apstrādātie klientūras ievainojamību ziņojumi (2025. gada 4. cet. pieaugums +59)
  - ✓ **172** uz konkrētām iestāžu programmām reģistrētās ievainojamības (2025. gada 4. cet. pieaugums +1)

Aktīvās iestāžu programmas skatīt šeit: <https://cvd.cert.lv/programs/all>

■ 2023 ■ 2024 ■ 2025



11. attēls. CVD: ievainojamību ziņojumu skaits gada griezumā

Organizāciju IKT infrastruktūras efektīvai aizsardzībai un kiberneturības stiprināšanai CERT.LV piedāvā plašu kibersdrošības pakalpojumu klāstu. Aizsargājiet un stipriniet savu kibertelpu jau šodien, izmantojot CERT.LV ekspertīzi, ieteikumus un pakalpojumus. Vairāk informācijas tīmekļvietnē: [CERT.LV](https://cert.lv)

Par vēlmi saņemt CERT.LV pakalpojumu aicinām rakstīt uz [cert@cert.lv](mailto:cert@cert.lv)

## 4. Kiberdrošības stiprināšana ar visu sabiedrību aptverošiem pasākumiem

Pārskata periodā **70** pasākumos CERT.LV eksperti par kiberdrošību izglītoja **24 237** dalībnieku, stiprinot individuālu lietotāju un organizāciju zināšanas, digitālās prasmes un kiberneturību.

Praktiskas aktivitātes sabiedrības izglītošanā

- ▶ Valsts iestādēm, NKDL subjektiem un Kiberdrošības kompetenču kopienas biedriem ir nodrošināti divi jauni mācību rīki: interaktīvais materiāls **“Darbības nepārtrauktības izaicinājums”** krīžu gatavības pārbaudei un izlaušanās istaba **“Ctrl + Alt + Escape[D]”**, kas caur spēles principiem trenē riska atpazīšanu. Projekti līdzfinansēti no Eiropas Savienības programmas “Digitālā Eiropa” līdzekļiem.
- ▶ Pārskata periodā ikvienam iedzīvotājam bija iespēja novērtēt savas zināšanas Aizsardzības ministrijas un CERT.LV rīkotās sabiedrības izglītošanas kampaņas **“Ož pēc shēmas!”** ietvaros izstrādātā kiberdrošības testā, veicinot izpratni par ikdienas digitālajiem riskiem. Kampaņas laikā testu līdz galam aizpildījuši **6 025** respondenti, par kuriem ir pieejami rezultāti, savukārt uzsākuši – **8 300**.
- ▶ Publicēta platforma [kibertests.lv](http://kibertests.lv) iedzīvotāju un organizāciju kiberdrošības zināšanu pārbaudei un stiprināšanai. Tests sniedz vērtīgus ieteikumus un praktiskas vadlīnijas, kas ikdienā palīdz aizsargāt gan personīgos, gan

uzņēmuma datus, padarot digitālo vidi drošāku. Projekts līdzfinansēts no Eiropas Savienības programmas “Digitālā Eiropa” līdzekļiem.

- ▶ 9. decembrī norisinājās seminārs **“Esi drošs!”**, kopskaitā (klātienē un tiešsaistē) pulcējot 921 dalībnieku.

Veiksmīgi aizvadīts Baltijā gaidītākais kiberdrošības notikums

29.-30. oktobrī, Rīgā kiberdrošības konference **“Kiberšahs 2025”** (CyberChess 2025) pulcēja vairāk nekā **800** dalībnieku klātienē (tostarp 62 lektoros) un ar vairāk nekā **8 900** skatījumu tiešsaistē vismaz no **48** pasaules valstīm. Vienuviet tikās nozares profesionāļi, politikas veidotāji, pētnieki un industrijas pārstāvji no valsts, privātā un militārā sektora, apliecinot, ka kiberdrošība ir kopīgs uzdevums un atbildība.

Konferences ietvaros notikušajās CTF (Capture The Flag) sacensībās piedalījās vairāk nekā 200 dalībnieku no visas pasaules. Ar izciliem panākumiem izcēlās trīs Latvijas komandas, iegūstot godalgotas vietas.

“Kiberšahs 2025” konferences organizētāji: CERT.LV, Latvijas Republikas Aizsardzības ministrija un Nacionālais kiberdrošības centrs sadarbībā ar ISACA Latvijas nodaļu, Latvijas Interneta asociāciju un LU Matemātikas un informācijas institūtu.

Konferences līdzfinansējums: Eiropas Savienība Eiropas Kiberdrošības kompetenču centra Latvijas Nacionālā koordinācijas centra (NCC -LV) projekta ietvarā.



## CERT.LV misija ir veicināt kiberdrošību Latvijā.

Galvenie CERT.LV uzdevumi ir uzturēt un aktualizēt informāciju par kiberdrošības apdraudējumiem, sniegt atbalstu valsts institūcijām kiberdrošības jomā, sniegt atbalstu kiberdrošības incidentu novēršanā jebkurai fiziskai vai juridiskai personai, ja incidentā iesaistīta Latvijas IP adrese vai .LV domēns, kā arī organizēt informatīvus un izglītojošus pasākumus valsts iestāžu darbiniekiem, IT drošības profesionāļiem un citiem interesentiem.

Pārskatā iekļauta vispārpieejama informācija, neietverot ierobežotas pieejamības informāciju. Pārskatam ir tikai informatīva nozīme.

### Saziņa ar CERT.LV:

Tālrunis: +371 67085888

E-pasts: cert@cert.lv

Tīmekļa vietne: cert.lv

### Sekot CERT.LV aktualitātēm:



© CERT.LV, 2025

Pārpublicējot obligāta avota norāde.

# Ja pamani, ziņo sms/WhatsApp!

## 23230444

(krāpniecisku īsziņu un telefona numuru  
pārsūtīšanai; telefona zvani netiek apstrādāti)



## VILTUS SAITES

## KRĀPNIECISKUS TELEFONA NUMURUS

## KRĀPNIECISKAS ĪSZIŅAS