# 2025
# C2

## SITUĀCIJA LATVIJAS KIBERTELPĀ

**PERIODS: 01.04.2025.- 30.06.2025.**

CERT.LV
Kiberincidentu novēršanas institūcija

Latvijas Universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

# Kopsavilkums

2025. gada 2. ceturksnī Latvijas kibertelpā bija vērojams būtisks kiberapdraudējumu un ievainojamību pieaugums, liecinot par jau ilgākā laika posmā nostiprinātām tendencēm. 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.

Pārskata periodā Latvijā reģistrēts būtisks **kiberincidentu skaita pieaugums** – 709 gadījumi (+ 12% pret š.g. 1.cet., +28% pret 2024. gada 2.cet.). Lielākoties pieaugums ir saistīts ar cilvēkfaktoru, pieaugošo digitālo atkarību un ierīču ievainojamību, un pieaugošo ģeneratīvā mākslīgā intelekta (MI) modeļu izmantošanu ļaunprātīgos nolūkos.

Būtiski **palielinājies identificētu apdraudētu iekārtu skaits** – 459 346 (+62% gan pret š.g. 1.cet., gan pret 2024. gada 2.cet.), kas norāda uz automatizētu skenēšanas un ievainojamību izmantošanas pieaugumu, vienlaikus pieaugums skaidrojams ar apjomīgu datu avotu pievienošanu CERT.LV telemetrijas datiem.

## TOP 5 kvantitatīvi lielākie kiberapdraudējuma veidi pārskata periodā:

| Apdraudējuma veids: incidentu skaits | Izmaiņas pret 2025. g. 1. cet. | Izmaiņas pret 2024. g. 2. cet. |
|---|---|---|
| **Krāpniecība: 460** | +15% | +46% |
| **Ļaundabīgs kods: 45** | +12% | +7% |
| **Ielaušanās mēģinājumi: 31** | -56% | -33% |
| **Kompromitētas iekārtas: 25** | -24% | -32% |
| **Pakalpojuma pieejamības traucējumi: 21** | 0% | +250% |

Krāpniecības straujš pieaugums apliecina nemainīgi augstu krāpniecisko kampaņu aktivitāti pret iedzīvotājiem, izmantojot valsts iestāžu un atpazīstamu uzņēmumu identitāti. Jauni uzbrukumu vektori: viedtelevizori, balss imitācija, dubultā izspiešana. Pieaugusi biznesa e-pastu kompromitēšana (BEC) un šifrējošo izspiedējvīrusu aktivitāte. Notikušas globāla mēroga piekļuves datu noplūdes (Google, Facebook, Apple u.c.), kas palielina kiberuzbrukumu iespējamību arī Latvijā.

DDoS uzbrukumi saglabājās intensīvi un sezonāli saasināti, īpaši ap svētkiem un politiski nozīmīgu notikumu laikā, taču tie lielākoties tiek atvairīti automatizēti. Līdztekus ne vēlēšanu laikā, ne pirms un pēc tām Latvijas kibertelpā netika konstatēti kiberincidenti vai kiberapdraudējumi, kas liecinātu par ārējiem mēģinājumiem ietekmēt notiekošās vēlēšanas. Tas, savukārt, norāda uz CERT.LV īstenoto preventīvo kiberdrošības pasākumu efektivitāti.

Latvijas kibertelpā pastiprinās kiberuzbrukumu intensitāte un sarežģītība ar augstu risku iedzīvotājiem, uzņēmumiem un iestādēm. Kiberuzbrukumi tiešā un netiešā veidā ietekmē iedzīvotāju finanšu resursus, un šī ietekme kļūst aizvien jūtamāka. Šāda negatīva tendence var ietekmēt sabiedrības uzticības līmeni digitālajiem pakalpojumiem.

Lai stiprinātu valsts kibernoturību, nepieciešams pastiprināt sabiedrības izglītošanu un kiberhigiēnu, uzlabot organizāciju tehniskās aizsardzības spējas, veicināt MI tehnoloģiju un datu telemetrijas izmantošanu aizsardzībā. Tādi CERT.LV pakalpojumi kā Drošības operāciju centrs, draudu medības, drošības testi, apmācības ir stratēģiski būtiski draudu mazināšanai un svarīgi valsts kiberdrošības noturības stiprināšanai. Lai nepieļautu "viegla mērķa" statusu, Latvijai jādemonstrē noturība un stratēģiskā modrība, kas balstīta uz savlaicīgu draudu identificēšanu un rīcībspēju.

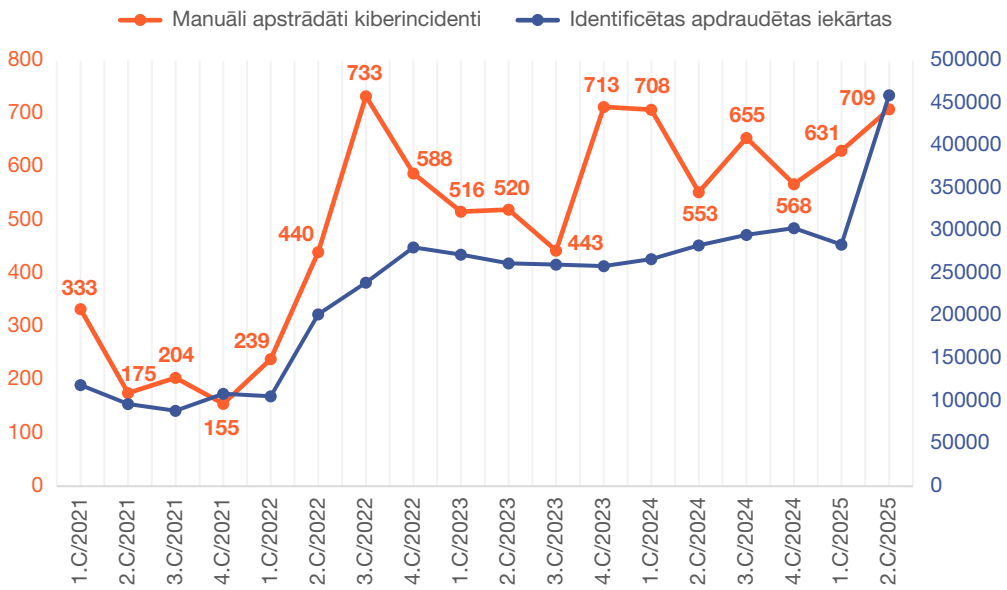
**Lepojamies ar Latvijas panākumiem – jau 3. gadu pēc kārtas Latvijas komanda iekļuvusi pasaules labāko pieciniekā NATO vērienīgākajās "Locked Shields" mācībās, šogad izcīnot 4. vietu. Īpašs panākums – 1. vieta kiberdrošības un starptautisko tiesību disciplīnā, apliecinot: arī maza valsts var būt nozīmīgs spēlētājs globālajā kibertelpā.**

# 1. Kibertelpas drošības apdraudējumi: statistika un tendences

2025. gada 2. ceturksnī, salīdzinot ar laika periodu pirms Krievijas iebrukuma Ukrainā 2022. gadā, pret Latviju vērsto kiberapdraudējumu intensitāte ir palielinājusies. Pieaug gan apdraudējumu daudzveidība, gan to tehniskā un psiholoģiskā sarežģītība.

Kopš 2025. gada sākuma Latvijas kibertelpā vērojams **straujš manuāli apstrādāto kiberincidentu skaita pieaugums**. Pīķis – 733 kiberincidenti, bija 2022. gada 3. ceturksnī, ar atkārtotu kāpumu 2023. gada 3.-4. ceturksnī un atkal 2025. gada 2. ceturksnī – reģistrēti **709 kiberincidenti**[1], kas ir **par 12% vairāk** salīdzinājumā ar iepriekšējo ceturksni un **par 28% vairāk** nekā pērn 2. ceturksnī. Pieaugums korelē ar globālo kiberapdraudējumu eskalāciju, pieaugošu digitālo atkarību sabiedrībā un cilvēkfaktoru. Būtisku lomu spēlē MI attīstība, kas atvieglo un paātrina krāpniecības, ielaušanās un automatizētu uzbrukumu veikšanu.

CERT.LV **identificētu apdraudētu iekārtu skaits** (459 346) pieauga par **62% salīdzinājumā** gan ar š.g. 1. ceturksni, gan ar pagājušā gada 2. ceturksni. Šī dinamika norāda uz automatizētu skenēšanas un ievainojamību izmantošanas pieaugumu. Kvantitatīvi lielāko daļu jeb 93% veido konfigurācijas nepilnības. Tas norāda uz sistēmu un tīkla drošības vājajiem punktiem, kas galvenokārt rodas cilvēkfaktora un nepietiekamu drošības standartu dēļ. Pieaugums ir skaidrojams arī ar to, ka 2. ceturksnī CERT.LV telemetrijas datiem pievienoti klāt papildu datu avoti.



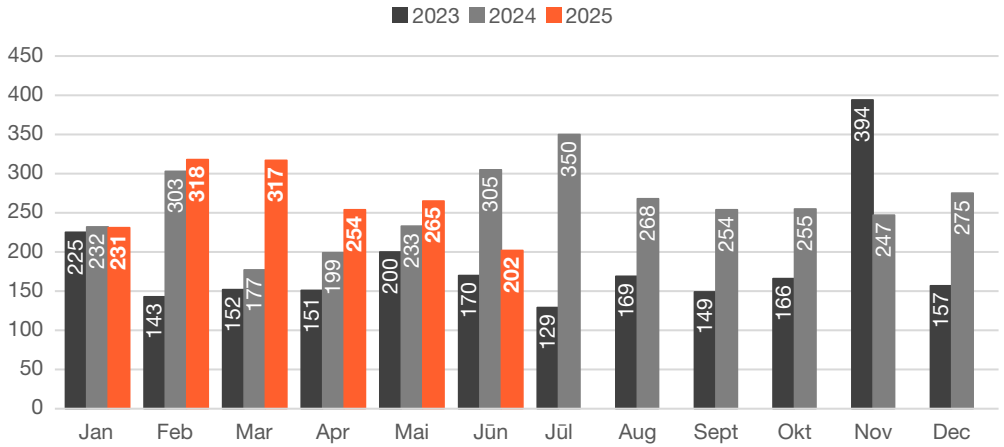

**1. attēls. Kiberincidentu un identificētu apdraudētu iekārtu skaits ceturkšņu dalījumā**

## Galvenie riski:

- **Pieaug krāpniecības mēģinājumi, it īpaši pikšķerēšanas kampaņas**, pret iedzīvotājiem valsts iestāžu nosaukuma aizsegā.
- **Cilvēkfaktors kā galvenā ievainojamība** (piemēram, 2FA neizmantošana, pikšķerēšanas saišu atvēršana) – būtisks vājais posms gan sabiedrībā kopumā, gan organizācijās, kas var ietekmēt kiberdrošības situāciju.
- **Uzņēmumus arvien biežāk apdraud šifrējošā izspiedējvīrusa uzbrukumi un biznesa e-pasta kompromitēšana (BEC)**, radot finansiālus zaudējumus un draudus reputācijai.

1 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.

- **Mērķēti DDoS uzbrukumi pret būtisku un svarīgu pakalpojumu infrastruktūru** attiecīgajai sezonalitātei un sabiedrībai aktuālo norišu vai ģeopolitisku notikumu kontekstā. 2. ceturksnī novērots būtisks pieaugums (250%), kas daļēji skaidrojams ar papildu datu avotu pievienošanu CERT.LV telemetrijai, vienlaikus uzbrukumu skaits un intensitāte norāda uz mērķtiecīgiem centieniem, turpinot DDoS izmantošanu kā līdzekli ideoloģiska protesta paušanai vai sabiedrības uzticības mazināšanai valsts digitālajiem pakalpojumiem.
- **Pieaugoša MI loma kiberapdraudējumos un dezinformācijā.** Būtiska tendence – Krievijas kiberoperācijās strauji pieaug MI izmantošanas apjoms, turklāt MI radītā satura atpazīšana kļūst arvien grūtāka. Ņemot vērā Krievijas konfrontējošo ārpolitiku, pēdējos gados īstenotas informatīvas ietekmes kampaņas un operācijas, pieaug risks, ka MI tehnoloģijas var tikt izmantotas, lai mērķtiecīgi ietekmētu sabiedrisko domu Latvijā vai veiktu sarežģītākus kiberuzbrukumus.
- **Ievainojamību, tostarp lietu interneta (IoT), un automatizācijas izmantošana kļūst arvien aktīvāka.** Apdraudējumi skar publisko un privāto sektoru.



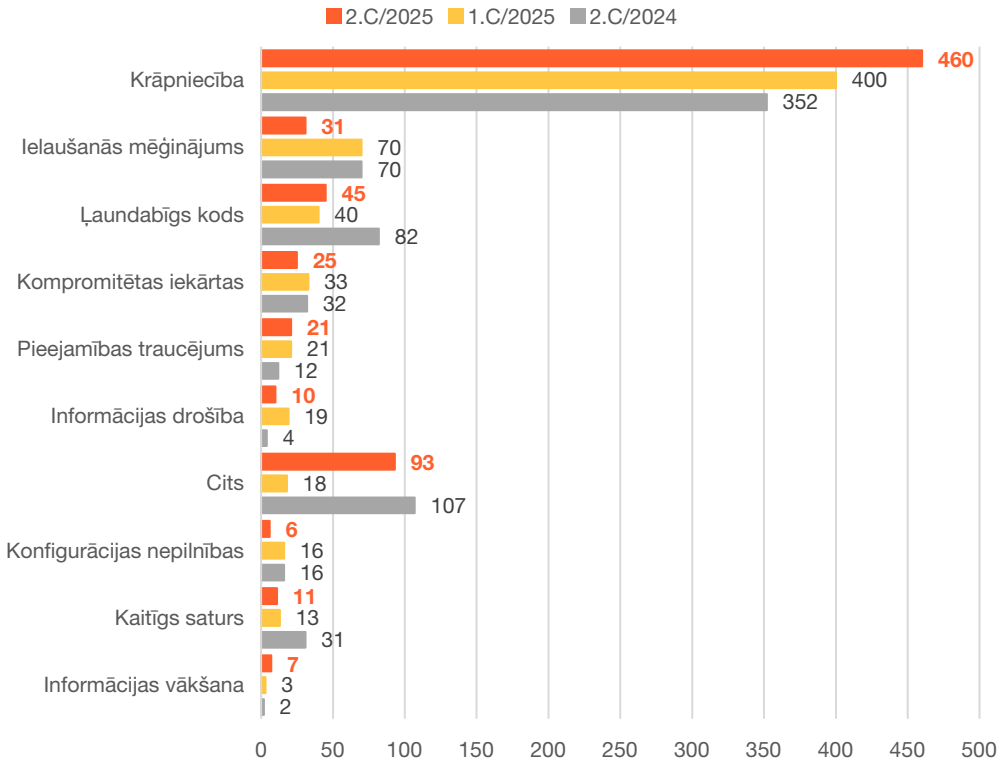

**2. attēls. Kiberincidentu dinamika (skaits mēnešu dalījumā)**

Ik mēnesi pret Latviju vērsto kiberapdraudējumu intensitāte ir augsta, taču stabila, saglabājot ierasti augsto līmeni. Tiem raksturīga spēja pielāgoties un izmantot dažādām auditorijām aktuālus tematus lielāka efekta sasniegšanai. Spilgtākie kiberapdraudējumi TOP 5 kategorijās izgaismoti ikmēneša apskatā **"Kiberlaikaptākļi"**.

**Kiberlaikapstākļu vērotājiem CERT.LV piedāvā ikmēneša pārskatu vienkāršā valodā par spilgtākajiem notikumiem Latvijas kibertelpā TOP 5 kategorijās. Aktuālie notikumi kibertelpā, apdraudējumu analīze un noderīgi padomi pārskata periodā: APRĪLIS | MAIJS | JŪNIJS**

# 2. Izplatītākie kiberapdraudējumi un būtiskākie notikumi pārskata periodā

2025. gada 2. ceturksnī Latvijas kibertelpā bija vērojams būtisks kiberincidentu pieaugums vairākos kiberapdraudējuma veidos, liecinot par jau ilgākā laika posmā nostiprinātām tendencēm.




**3. attēls. Kiberincidentu skaita salīdzinājums pēc veida**

**Krāpniecisko aktivitāšu un pikšķerēšanas kampaņu nemitīga klātbūtne, progresē psiholoģiskās manipulācijas kvalitāte**

Novērotas intensīvas pikšķerēšanas kampaņas, krāpniekiem uzdodoties par valsts iestādēm (it īpaši CSDD, VID), bankām (it īpaši SEB, Swedbank), pasta piegādes uzņēmumiem (it īpaši "Latvijas Pasts", "FedEx"), e-pasta servisa pakalpojumu (it īpaši Microsoft Outlook) un tehnoloģiju kompānijām (it īpaši Meta). Dominēja īsziņas par ceļu satiksmes noteikumu pārkāpumu vai neapmaksātu sodu, mēģinot izvilināt datus un izkrāpt naudu Ceļu satiksmes drošības direkcijas (CSDD) aizsegā. Valsts policijas dati rāda, ka šogad vairāk nekā 100 iedzīvotāji noticējuši viltus īsziņām CSDD vārdā – viņiem izkrāpti 174 523 eiro .

Kopumā redzams, ka krāpnieki izmanto arvien inovatīvākus risinājumus un pielāgo krāpšanas metodes attiecīgajai sezonalitātei vai sabiedrībā aktuālajām norisēm, piemēram, jūnijā tika izmantota pašvaldību vēlēšanu tematika, izsūtot īsziņas ar tekstu par "anulētu balsi".

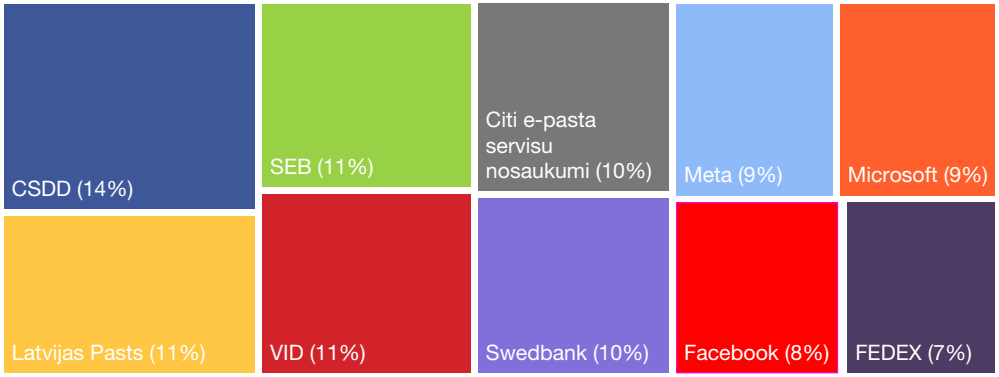
Turpinās viltus investīciju un kriptovalūtu shēmas, kas tiek reklamētas, imitējot populārus portālus (delfi.lv, diena.lv, jauns.lv). Fiksēta "dubultās" izspiešanas taktika, kur upuriem viltus "advokāts" piedāvāja "palīdzību" līdzekļu atgūšanā, tā izkrāpjot vēl vairāk naudas.

Novērotas jaunas, psiholoģiski manipulatīvas telefonkrāpšanas metodes – krāpnieki veic vairākus zvanus pēc kārtas, lai upura modrību pakāpeniski mazinātu un virzītu uz darbībām, kas var novest pie personas datu izpaušanas vai piekļuves piešķiršanas kontiem, upurim pašam to neapzinoties. Pieaug ģeneratīvā MI rīku izmantošana balss imitēšanā, lai viegli manipulētu ar cilvēku emocijām un uzticēšanos.

Novēroti gadījumi, kur krāpnieki izmantoja nejauši ģenerētus "eParaksts mobile" personas kodus / lietotāju numurus ar mērķi veikt neatļautus pirkumus interneta veikalā veikals.banknote.lv . Novērots, ka tieši svētku laikā mēdz pieaugt krāpnieku aktivitātes ar viltus paziņojumiem, piemēram par nepieciešamību atjaunot it kā beigušos "eParaksta mobile" sertifikātu vai viltus īsziņas ar saiti it kā no Valsts sociālās apdrošināšanas aģentūras e-pakalpojuma adreses.

2 Avots: https://www.vp.gov.lv/lv/jaunums/noziedznieki-ar-iszinam-csdd-varda-sogad-izkrapusi-simtiem-tukstosus-eiro

Fiksēts jauns krāpšanas vilnis, kas vērsts uz viedtelevizoriem (īpaši ar Android OS). Šajā uzbrukumā krāpnieki mērķtiecīgi maldinājuši lietotājus, liekot, piemēram, instalēt ļaunprātīgas lietotnes, kas pieprasa personas datus. Latvijā reģistrēti vairāki šādi gadījumi, kas liecina, ka šis krāpniecības veids ir guvis panākumus.




**4. attēls. Izplatītākās pikšķerēšanas kampaņas, izmantojot zināmu organizāciju nosaukumus (procentuālā daļa no kopējā CERT.LV apstrādāto pikšķerēšanas ziņojumu skaita 2025. gada 2. cet.)**

### Pieaug biznesa e-pasta kompromitēšanas (BEC) gadījumu skaits

Mērķētos kiberuzbrukumos pāris uzņēmumi saņēma vairākus rēķinus ar viltotiem kontu numuriem un, veicot to apmaksu, cieta būtiskus finansiālus zaudējumus. Piekļuve, kas tika izgūta caur nopludinātiem uzņēmuma vadītāja e-pasta piekļuves datiem, izgaismo 2FA kritisko nozīmi – 2FA neizmatošana ir kritiska ievainojamība.

### Pieaug šifrējošo izspiedējvīrusu riski

Izspiedējvīrusu uzbrukumi kļūst par arvien nopietnāku draudu Latvijas uzņēmumiem, spējot pilnībā paralizēt to darbību un radīt milzīgus finansiālus zaudējumus. Turklāt Ransomware-as-a-Service (RaaS) modeļa izplatība padara šos uzbrukumus pieejamākus plašākam noziedznieku lokam. Bīstams Mallox paveida izspiedējvīruss, kas darbojas kā RaaS, skāra divus uzņēmumus lauksaimniecības nozarē. Šifrējošā izspiedējvīrusa uzbrukumu piedzīvoja arī Jelgavas tipogrāfija. Uzņēmums, kura apgrozījums ir 17 milj. gadā, bija spiests apturēt darbību, jo tā dati bija sašifrēti; iespējamie zaudējumi tiek lēsti līdz ceturtdaļai no šīs summas.

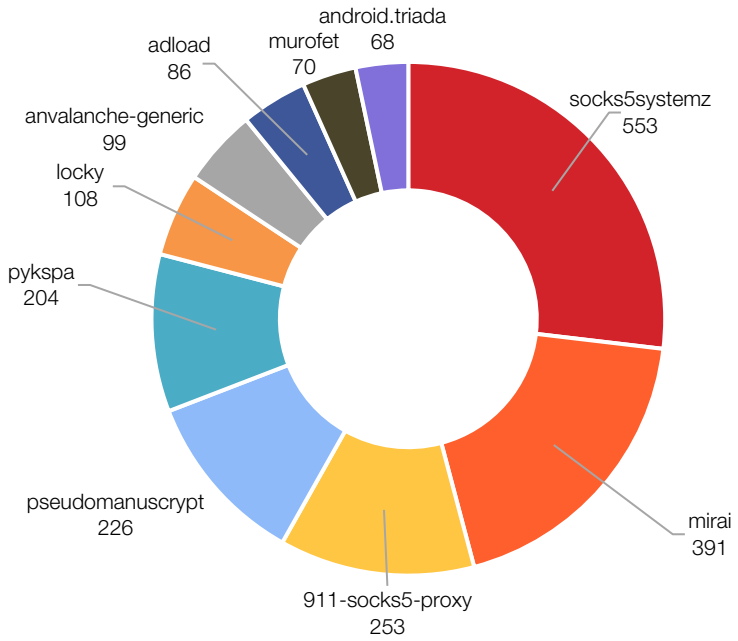
### Ģeopolitiskos notikumos balstītu DDoS uzbrukumu intensitāte saglabājas viļņveidīga

2025. gada aprīļa mēnesī novērots kiberincidents, kurā DDoS uzbrukuma dēļ uz kādu brīdi piekļuve bija traucēta politiskās partijas tīmekļvietnei un e-pasta serverim. Maija svētku brīvdienās DDoS uzbrukumu apjoms pret valsts resursiem pieauga par 40%, it īpaši intensīvi uzbrukumi tika vērsti pret finanšu nozares resursiem. Zīmīgi, ka 9. maijā tika veikts DDoS uzbrukums pret Okupācijas muzeja tīmekļvietni, kas bija nesekmīgs. Kopumā DDoS uzbrukumi nav radījuši paliekošu ietekmi, lielākā daļa DDoS uzbrukumu tiek atvairīti automatizēti.

CERT.LV, gatavojoties 7. jūnijā notikušajām Pašvaldību vēlēšanām, proaktīvi īstenoja virkni preventīvo pasākumu, uzlabojot gatavību reaģēt uz potenciālajiem kiberapdraudējumiem. Ne vēlēšanu laikā, ne pirms un pēc tām Latvijas kibertelpā netika konstatēti kiberincidenti vai kiberapdraudējumi, kas liecinātu par ārējiem mēģinājumiem ietekmēt notiekošās vēlēšanas.

### Datu zagšanai izmantotās ļaunatūras progresē un kļūst grūtāk atklājamas

Dominē ievainojamas vietnes, kas ir bāzētas uz WordPress satura vadības sistēmas un ir inficētas ar ļaunatūru. Tāpat sabiedrība aktīvi tika brīdināta par viltus CAPTCHA ļaunatūras izplatīšanos, kas paredzēta personas datu zagšanai inficētās tīmekļvietnēs – Latvijā fiksēti vairāki cietušie.




5. attēls. TOP 10 ļaunatūras; skaits 2025. gada 2. ceturksnī

**Pieaug ievainojamību izmantošana**

Starptautiskā kontekstā ar potenciālu ietekmi izceļas Krievijas valsts atbalstītās APT28 grupas aktivitātes, kas izmantoja XSS ievainojamības populāros e-pasta serveros (Roundcube, Zimbra u.c), lai konfidenciālu datu zagšanas nolūkā uzbruktu valsts iestāžu un aizsardzības nozares organizāciju e-pasta kontiem, galvenokārt Ukrainā un Austrumeiropā. Tās ir augsta līmeņa kiberizlūkošanas operācijas ar potenciāli nopietnām sekām nacionālajai drošībai, it īpaši saistībā ar atbalstu Ukrainai. Risks pastāv arī Latvijas organizācijām, ja netiek savlaicīgi veikti e-pasta serveru atjauninājumi.

**Plaša mēroga piekļuves datu noplūdes kiberincidents ar augstu risku arī Latvijas iedzīvotājiem, kuru dati varētu būt nopludināti**

Tīmeklī atklāta līdz šim lielākā datu noplūde, kuras rezultātā publiskoti piekļuves dati no vairāk nekā 16 miljardiem kontu tādos populāros servisos kā Google, Facebook, Apple, Telegram u.c. Šie dati var tikt izmantoti kontu uzlaušanai, krāpniecības nolūkos u.c. Liela daļa datu, iespējams, iegūta ar datu zagšanas ļaunatūru. Visdrīzāk šie dati apkopoti no daudziem avotiem ilgākā laika periodā. CERT.LV aicina ikvienu lietotāju ievērot drošības pasākumus (katram tīmekļa resursam izmantot unikālu paroli, uzstādīt 2FA visur, kur tas ir iespējams, nevērt aizdomīgas saites, veikt atjauninājumus).

**Sagaidāms būtisks IoT ierīču un automatizācijas radīto risku pieaugums**

IoT jeb ierīces ar “smadzenēm” un interneta pieslēgumu bieži vien ir vājais posms tīkla drošībā un ir viegls mērķis botu tīklu veidošanai, kas tālāk tiek izmantots plaša mēroga DDoS uzbrukumiem. Automatizēto botu datplūsmas dominance (pētījumi rāda, ka vairāk nekā 50% interneta datplūsmas ģenerē boti, no kuriem 37% ir ļaunprātīgi) signalizē par jaunu ēru kiberdrošībā, kur aizsardzības sistēmām jāspēj cīnīties ar MI radītiem

## Galvenie secinājumi.

**Latvijas kibertelpā novērots gan kvalitatīvs, gan kvantitatīvs kiberincidentu, apdraudējumu un ievainojamību pieaugums, kas ietekmē organizāciju reputāciju un darbības nepārtrauktību. Kiberuzbrukumi tiešā un netiešā veida ietekmē iedzīvotāju finanšu resursus, un šī ietekme kļūst aizvien jūtamāka, ņemot vērā tehnoloģiju izplatību ikdienā. Šāda negatīva tendence var ietekmēt sabiedrības uzticības līmeni digitālajiem pakalpojumiem.**

**Cilvēkfaktors paliek centrālais riska avots. Kritiskā domāšana, kiberhigiēna un sabiedrības izpratne joprojām nav pietiekamas, kas padara organizācijas ievainojams pret sociālās inženierijas un krāpniecības uzbrukumiem. Nepieciešams stiprināt gan organizāciju tehnisko aizsardzību, gan indivīdu kiberhigiēnu un kritisko domāšanu.**

**Vienlaikus jāstiprina sabiedrības noturība pret informācijas ietekmes operācijām un dezinformāciju. Valsts spēja laikus identificēt ietekmes operācijas un uzturēt dialogu ar sabiedrību kļūst par būtisku drošības garantu.**

**Svarīga ir reāllaika telemetrijas izmantošana, drošības testi un MI tehnoloģiju ieviešana organizāciju kiberaizsardzībā. Krievijas agresija, visticamāk, turpināsies arī kibertelpā – atturēšanas stratēģijā būtiska būs noturības demonstrēšana un preventīva rīcība, lai Latvija netiktu uztverta kā viegls mērķis.**

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

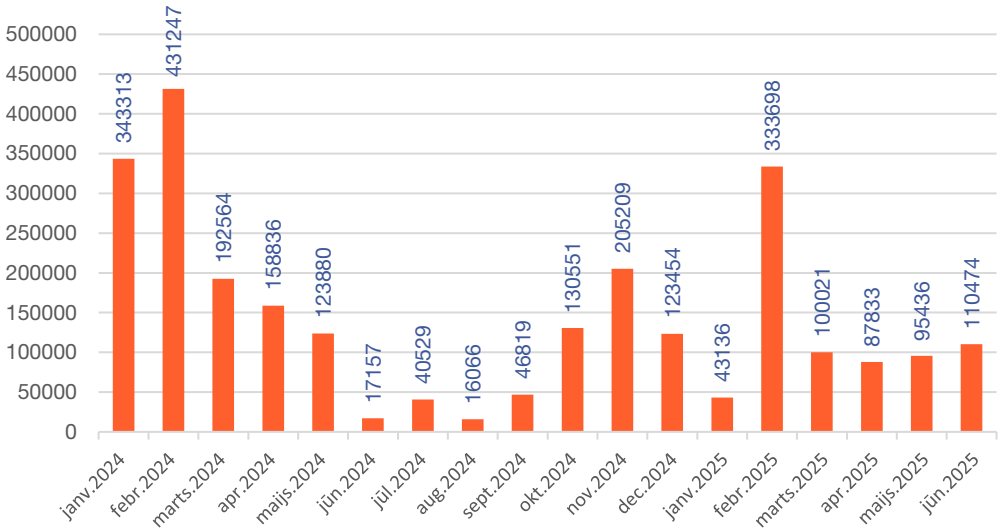
CERT.LV pakalpojumi, tostarp DNS ugunsmūris, atbalsts incidentu risināšanā, Drošības operāciju centrs (SOC), kiberdrošības draudu medības, drošības testi, sabiedrības izglītošana un apmācības u.c., ir būtisks resurss risku mazināšanai un noturības stiprināšanai pret arvien intensīviem un sarežģītiem kiberdraudiem.

## DNS ugunsmūris

2025. gada 2. ceturksnī kopskaitā DNS ugunsmūra pakalpojuma ietvaros:

- **Kaitīgo domēna vārdu DNS pieprasījumu skaits** sasniedza 2 532 552, kas ir par 255% vairāk salīdzinājumā ar 1. ceturksni un par 219% vairāk nekā pērn 2. ceturksnī. Izteikti redzams, ka notikuši pieprasījumi gan uz SEB, Swedbank, gan uz dažādām inficētām WordPress lapām ļoti lielā daudzumā, tomēr vairumā gadījumu reāla cilvēku klikšķināšana uz šīm lapām praktiski neuzrādās, un tie, visticamāk, ir bijuši automatizēti pieprasījumi, piemēram, no Firewall vai proxy sistēmām, kas regulāri pārbauda domēnu reputāciju.

- **Visu CERT.LV zonu atvairītie kiberuzbrukumi pasargāja lietotājus** no ļaunprātīgu vietņu apmeklēšanas 293 743 reizes, kas ir par 38% mazāk salīdzinājumā ar 1. ceturksni un par 2% mazāk nekā pērn 2. ceturksnī. Iespējamie samazinājuma iemesli varētu būt sezonālie vai laika perioda faktori – ciklisks kritums, kas var mainīties nākamajā ceturksnī. Atvairījumu skaitu tiešā veidā ietekmē arī aktīvo krāpniecības kampaņu skaits.




**6. attēls. Visu CERT.LV zonu atvairītie kiberuzbrukumi**

## Nozīmīgākās aktīvās aizsardzības epizodes pārskata periodā

| Brīdinājumi | Skaits |
|---|---|
| Ievainojamas vietnes, kas ir bāzētas uz WordPress satura vadības sistēmu un ir inficētas ar ļaunatūru. | **24 874** |
| Viltus internetveikali, kas izmanto atpazīstamu zīmolu nosaukumus. | **23 357** |
| Azartspēļu reklamēšana ar inficētu vietņu palīdzību. | **8 115** |
| "Jauns.lv" tēla izmantošana krāpniecisku kriptovalūtu investīciju platformu reklamēšanas kampaņās. | **6 207** |
| "Latvijas Pasts" tēla izmantošana viltus vietnes kampaņās. | **6 120** |
| "DELFI" tēla izmantošana krāpniecisku kriptovalūtu investīciju platformu reklamēšanas kampaņās. | **4 284** |
| "Valsts ieņēmumu dienests" tēla izmantošana viltus vietnes kampaņās. | **2 249** |
| Krāpnieciskas ātro kredītu vietnes | **1 875** |
| "DIENA" tēla izmantošana krāpniecisku kriptovalūtu investīciju platformu reklamēšanas kampaņās. | **1 727** |
| "CSDD" tēla izmantošana viltus vietnes kampaņās. | **1 522** |

## Apdraudējumu agrās brīdināšanas sistēma

Informācijas tehnoloģiju drošības apdraudējumu agrās brīdināšanas sistēma (ABS) ir CERT.LV nodrošināts pakalpojums, kas veic datu plūsmas anomāliju analīzi un kiberuzbrukumu pazīmju identificēšanu pakalpojuma saņēmēja infrastruktūrā. Uz pārskata perioda beigām ABS ģenerēto brīdinājumu skaits bija aptuveni **1,7 miljardi**.

Izplatītākie augstas prioritātes kiberapdraudējumu brīdinājumi pa CERT.LV signatūru grupām bija ar datorvīrusiem, pikšķerēšanu un potenciāli ļaunprātīgām vietnēm saistīti brīdinājumi, kā arī ar robottīklu, krāpšanām un vīrusu indikatoriem saistīti brīdinājumi.

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

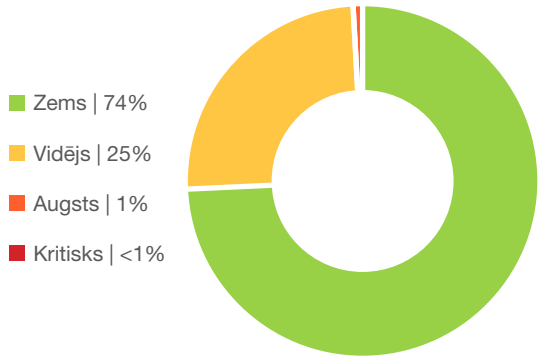
## Drošības operāciju centrs (SOC)

Kopš 2024. gada, kad tika uzsākta CERT.LV SOC pakalpojuma sniegšana iestādēm, uz 2025. gada 2. ceturkšņa beigām ir iegūta **redzamība kopskaitā pār 33 828 iekārtām** (serveriem un darbstacijām). 2. ceturksnī gala iekārtu skaits pieauga par **25 419 – pieaugums veido aptuveni 75% no kopējā apjoma**, līdz ar to palielinājies arī drošības trauksmes ziņojumu skaits.

Pārskata periodā **reģistrēti vairāk nekā 10 miljoni drošības trauksmes ziņojumu, kas ir teju 9 reizes vairāk** nekā 1. ceturksnī. SOC identificēto drošības trauksmju skaita lielais pieaugums skaidrojams galvenokārt ar iegūto plašāku redzamību jauno klientu infrastruktūrā.

Apstrādājot drošības trauksmes ziņojumus, 2. ceturksnī tika manuāli izveidotas 375 lietas. 172 reizes jeb 46% gadījumu tika veikta saziņa ar klientiem, lai pieprasītu papildu informāciju, informētu par kiberapdraudējumu vai kiberincidentu.

**Konstatēts 1 kiberincidents** – ļaunatūra *Windows* aktivizācijas rīkā, kuras mērķis ir informācijas zagšana darbinieku darbstacijās. Darbstacija pārinstalēta, un lietotāja paroles nomainītas, nav konstatēta tālāka ļaunatūras ietekme infrastruktūrā.




**7. attēls. Drošības trauksmes līmenis – SOC reģistrētie drošības trauksmes ziņojumi 2025. gada 2. cet. (procentuālā daļa no kopējā skaita)**

## Kiberdrošības draudu medību operācijas

Uz pārskata beigām kiberdrošības draudu medību operācijās kopš 2022. gada analīze ir veikta kopskaitā **160 000 gala iekārtās** gan būtisku un svarīgu pakalpojumu sniedzēju, gan valsts pārvaldes iestāžu IKT infrastruktūrā. 2025. gada 2. ceturksnī gala iekārtu skaits **pieauga par 5 000**.

Latvijas un Kanādas sadarbība kiberdrošībā turpinās, kas ir īpaši svarīgi, ņemot vērā reģiona ģeopolitisko situāciju un potenciālos draudus no trešajām valstīm. CERT.LV vadībā noslēgušās mēnesi ilgas draudu medības ar paplašinātu sabiedroto klātbūtni.

## IT sistēmu drošības testi un pikšķerēšanas uzbrukumu simulācijas kampaņas

Pārskata periodā CERT.LV veica **11 IT sistēmu drošības testus**, no kuriem 10 bija ar vēlēšanām saistītas sistēmas. Veiktas **2 pikšķerēšanas uzbrukumu simulācijas kampaņas**, stiprinot iestāžu personāla prasmes atpazīt sociālās inženierijas uzbrukumus un mazinot cilvēkfaktora riskus.

## Koordinēta ievainojamību atklāšana (CVD)

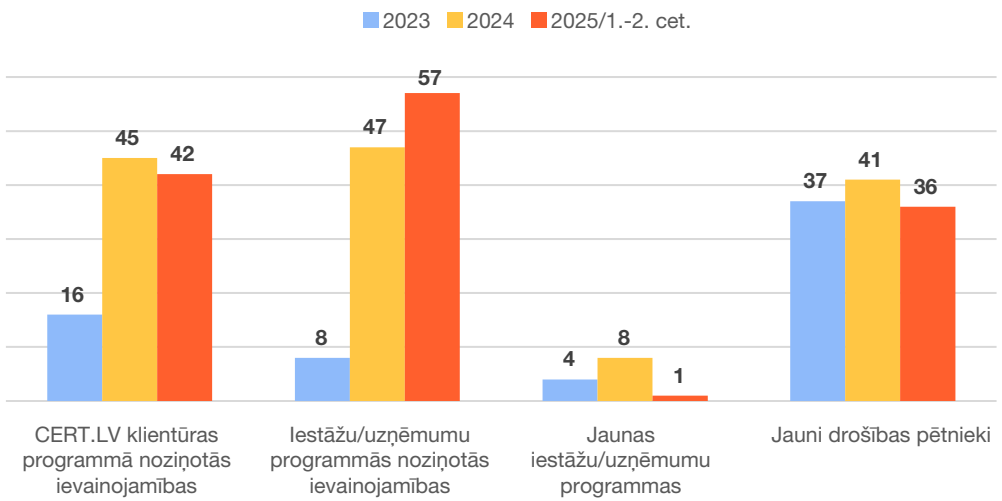
CVD ziņošanas prakse palīdz savlaicīgāk uzzināt par ievainojamībām, koordinēt ievainojamību izpēti un to novēršanu, un efektīvāk organizēt pasākumus aizsardzībai.

Uz pārskata perioda beigām (30.06.2025.) CVD platformā kopskaitā bija reģistrēti:

- Drošības pētnieki: 114 aktīvi (2. cet. skaits pieauga par 21)
- Jaunas iestāžu programmas: 13

Uz pārskata perioda beigām kopskaitā reģistrēti 215 ievainojamību ziņojumi (2. cet. skaits pieauga par 55), tostarp:

- CERT.LV klientūras ievainojamības: 103 (2. cet. skaits pieauga par 28)
- Iestāžu programmās noziņotās ievainojamības: 112 (2. cet. skaits pieauga par 27)




**8. 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**

## 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 gan valsts iestāžu darbiniekiem, gan IT drošības profesionāļiem, gan 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