2025 C3

SITUĀCIJA LATVIJAS KIBERTELPĀ

PERIODS: 01.07.2025. - 30.09.2025.

CERT.LV
Kiberincidentu novēršanas institūcija

Latvijas Universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Kopsavilkums

Kiberapdraudējumu līmenis Latvijā saglabājas nemainīgi augsts – kopš 2022. gada ik ceturksni vidēji 500-700 incidenti. Zemas intensitātes periodi ir palikuši pagātnē, interneta lietotāji joprojām ir pakļauti pastāvīgiem riskiem.

2025. gada 3. ceturksnī reģistrēts **671 kiberincidents**, kas ir par 5% mazāk nekā šogad 2. ceturksnī, bet par 2% vairāk nekā pērn 3. ceturksnī, un kopumā novērojama augšupejoša trajektorija. Turpinās CERT.LV **identificēto apdraudēto iekārtu skaita straujš pieaugums**, kas ir par 111% vairāk nekā šogad 2. ceturksnī un par 36% vairāk nekā pērn 3. ceturksnī.

Galvenās tendences un draudi

- Apdraudēto iekārtu skaits turpina strauji pieaugt, liecinot par jaunu kiberdraudu posmu – pieaug *IoT* un botu tīklu, ļaunatūru un automatizētu ievainojamību izmantošanas aktivitāte. Tas signalizē par nepieciešamību stiprināt ievainojamību pārvaldību un savlaicīgi veikt atjauninājumus viedajām ierīcēm.
- Aktīvi izmantotas "Microsoft" *SharePoint* un *WinRAR* kritiskās ievainojamības – vismaz viens kompromitēšanas gadījums konstatēts Latvijas kritiskās infrastruktūras (KI) sektorā. Tie KI turētāji, kas ir ieviesuši un izmanto CERT.SOC pakalpojumus, šādus apdraudējumus spēj daudz ātrāk atklāt un efektīvāk novērst.
- Krievijas radītie kiberdraudi saglabājas augstā līmenī, īpaši pret kritisko infrastruktūru un OT sistēmām (enerģētika, ūdens, siltums); novēroti DDoS uzbrukumi no ar Krieviju saistāmā grupējuma *NoName057(16)* un botu tīkliem.
- Šifrējošie izspiedējvīrusi, arvien labāk pielāgojoties aizsardzības mehānismiem, turpina apdraudēt organizācijas, CERT.LV reģistrēti 3 gadījumi. Iestādēm jāstiprina rezerves kopēšanas, atjaunošanas un incidentu reaģēšanas spējas.
- Pieaug piegādes ķēžu uzbrukumu riski – aktīvāk jāveicina drošības auditu veikšana, jādefinē stingrākas prasības iepirkumos un pastāvīgi jāatgādina par nepieciešamību regulāri atjaunot programmatūru. "Minimālas kiberdrošības prasības" noteikumu stāšanās spēkā ir pozitīvs solis, kas uzlabos kopējo kiberdrošības līmeni.
- Sociālās inženierijas un krāpniecības kampaņas sasniedz jaunu intensitātes līmeni: izmantotas apmaksātas reklāmas "Google", lai izplatītu krāpnieciskas vietnes, kas piedāvā viltus ieguldījumu shēmas; pieaug īsziņu un e-pasta pikšķerēšanas kampaņas, uzdodoties par valsts iestādēm (īpaši CSDD, VID EDS, DPD) un sabiedrībā zināmām personām. Jauna draudu dimensija – *ClickFix* mehānisms, kas izmanto *CAPTCHA* pārbaudes, lai lietotāji neapzināti aktivizētu kaitīgas darbības. 2FA, DNS ugunsmūris, savlaicīgi veikti atjauninājumi, darbinieku apmācības mazina riskus un incidentu ietekmi.

Uzbrukumi kļūst hibrīdi – vienlaikus tiek izmantotas tehnoloģiskas un cilvēkfaktora ievainojamības. Noturība ir kritiski svarīga, tāpat ātra un koordinēta rīcība ir būtiska, lai ierobežotu uzbrukuma ietekmi – savlaicīga ievainojamību novēršana, telemetrijas dati un reaģēšanas spējas ļauj ievērojami samazināt potenciālās sekas.

Šīs tendences apliecina nepieciešamību turpināt stiprināt Latvijas gatavību visdažādākajiem apdraudējumiem, pielietojot daudzslāņainu kiberaizsardzību – DNS ugunsmūri, atbalstu kiberincidentu risināšanā un Drošības operāciju centra (SOC) pakalpojumus, draudu medības un drošības testus, lietotāju izglītošanu un apmācības, ko nodrošina CERT.LV komanda.

Satura rādītājs

1. Kibertelpas drošības apdraudējumi: statistika un tendences

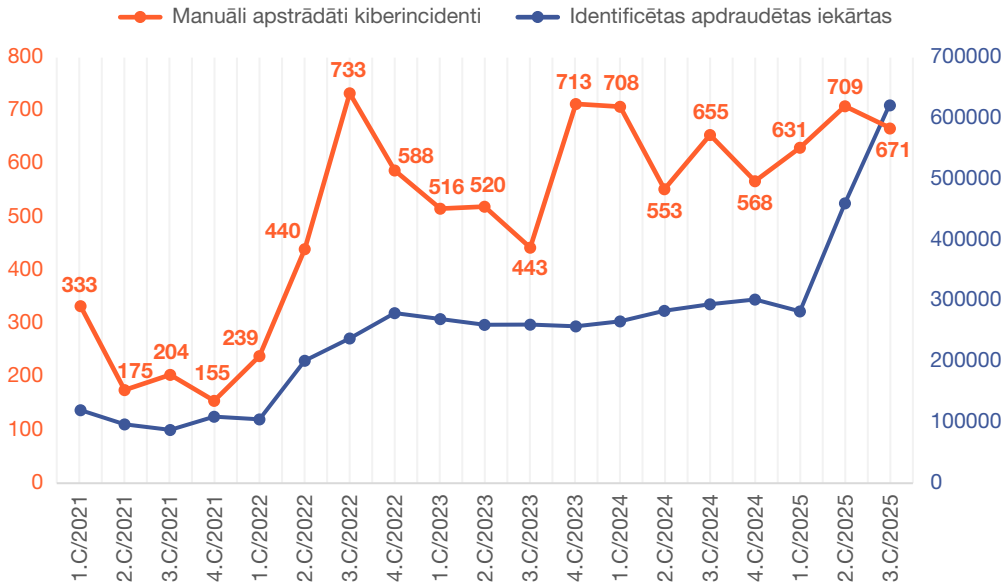
Kiberincidentu un apdraudēto iekārtu dinamika

2025. gada 3. ceturksnī – reģistrēts **671 kiberincidents**[1], kas ir **par 5% mazāk** nekā 2. ceturksnī un **par 2% vairāk** nekā pērn 3. ceturksnī. Novērojamas kiberincidentu skaita svārstības, bet kopumā – augšupejoša trajektorija.

Incidentu skaits stabilizējies augstā līmenī: kopš 2022. gada 3. ceturksnī vidēji 500-700 incidenti, tas norāda uz nemainīgi augstu kiberapdraudējumu fonu un pastāvīgu slodzi atbildīgajiem par kiberdrošību.

Turpinās CERT.LV **identificēto apdraudēto iekārtu skaita straujš pieaugums**, kas ir par **111% vairāk nekā** š.g. 2. ceturksnī un par **36% vairāk** nekā pērn 3. ceturksnī. Šī dinamika norāda uz botu tīklu, ļaunatūru, automatizētu skenēšanas, ievainojamību un konfigurācijas nepilnību izmantošanas pieaugumu. Vienlaikus pieaugums skaidrojams ar plašāku monitoringa un atklāšanas spēju uzlabošanos. Pieaugumu ietekmēja arī šogad 2. ceturksnī VAS "Latvijas Valsts radio un televīzijas centrs" datu pievienošana CERT.LV telemetrijas datiem.

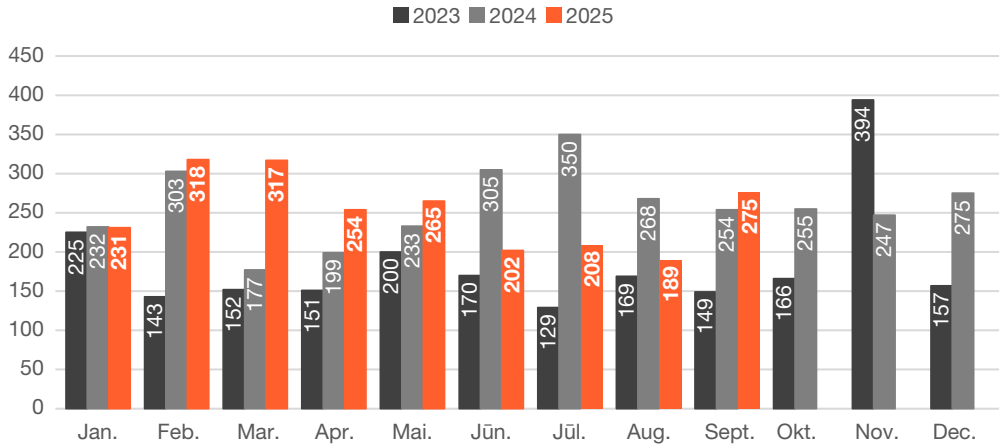
Incidentu skaits un apdraudētās iekārtas ne vienmēr korelē. 2025. gadā novērojams, ka incidentu skaits saglabājas līdzīgā līmenī (ik ceturksni ap 600-700), bet apdraudēto iekārtu skaits "uzleca" divkārši. Tas norāda, ka incidenti kļūst plašāki pēc ietekmes mēroga, nevis tikai vairāk skaita ziņā.



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

Mēnešu dalījumā (jūlijs-septembris) kiberincidentu skaits kopumā ir bijis salīdzinoši stabils, taču septembrī novērojams būtisks pieaugums – no 189 incidentiem augustā līdz 275 septembrī, kas ir aptuveni 45% vairāk. Šī dinamika norāda uz sezonālu aktivitātes atjaunošanos pēc vasaras mēnešiem un iespējamu jaunu uzbrukuma viļņa sākumu. Salīdzinot ar iepriekšējiem gadiem, 3. ceturksnī kiberincidentu skaits ir bijis ar nelielu pieauguma tendenci, kas var liecināt gan par uzbrukumu intensitātes pieaugumu, gan par uzlabotu to identificēšanas un ziņošanas praksi.

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.

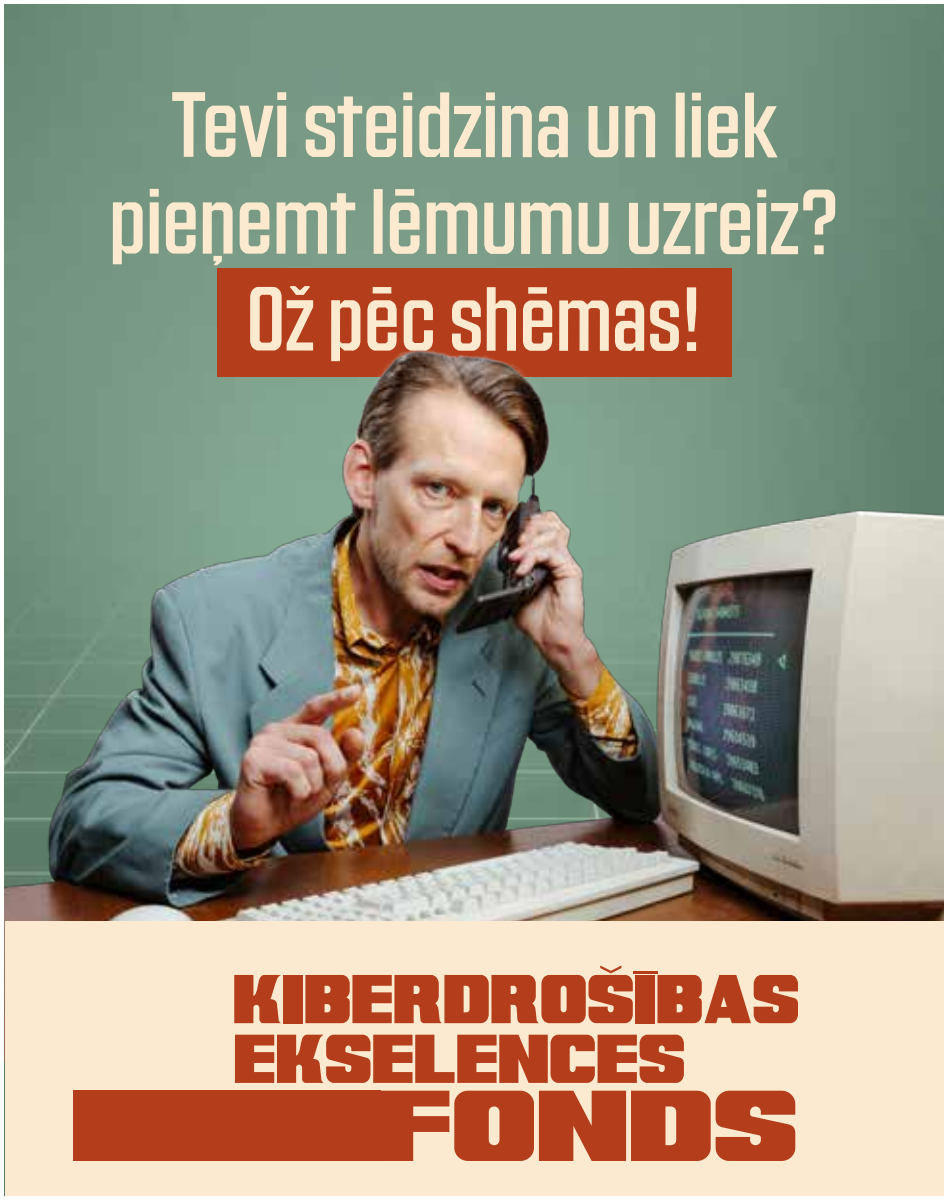


2. attēls. Kiberincidentu dinamika (skaits mēnešu dalījumā)

Pārskata periodā CERT.LV eksperti **26 pasākumos par kiberdrošību izglītoja 4 291 dalībnieku**, pilnveidojot gan individuālu lietotāju, gan organizāciju zināšanas un prasmes datu un sistēmu drošības nodrošināšanā.

8. septembrī Aizsardzības ministrija un CERT.LV atklāja kiberdrošības kampaņu "Ož pēc shēmas!", kuras mērķis ir stiprināt sabiedrības kiberdrošību un noturību pret apdraudējumiem, vienlaikus izglītojot par kiberhigiēnu un digitālajām krāpniecības shēmām. Vietnē shemas.lv pieejama aktuālā informācija par izplatītākajām krāpniecības metodēm un praktiski padomi, kā no tām pasargāties.

Veikto pasākumu efektivitāte un ietekme uz kopējo kiberdrošību ir tieši atkarīga no visu iesaistīto vēlmes tos ievērot, ikvienam uzņemoties atbildību par saviem digitālajiem aktīviem un organizācijām investējot resursus kiberdrošībā. Efektīva kiberapdraudējumu novēršana prasa visu pieejamo resursu, institūciju un organizāciju sinerģisku un koordinētu iesaisti.



"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: JŪLIJS | AUGUSTS | SEPTEMBRIS

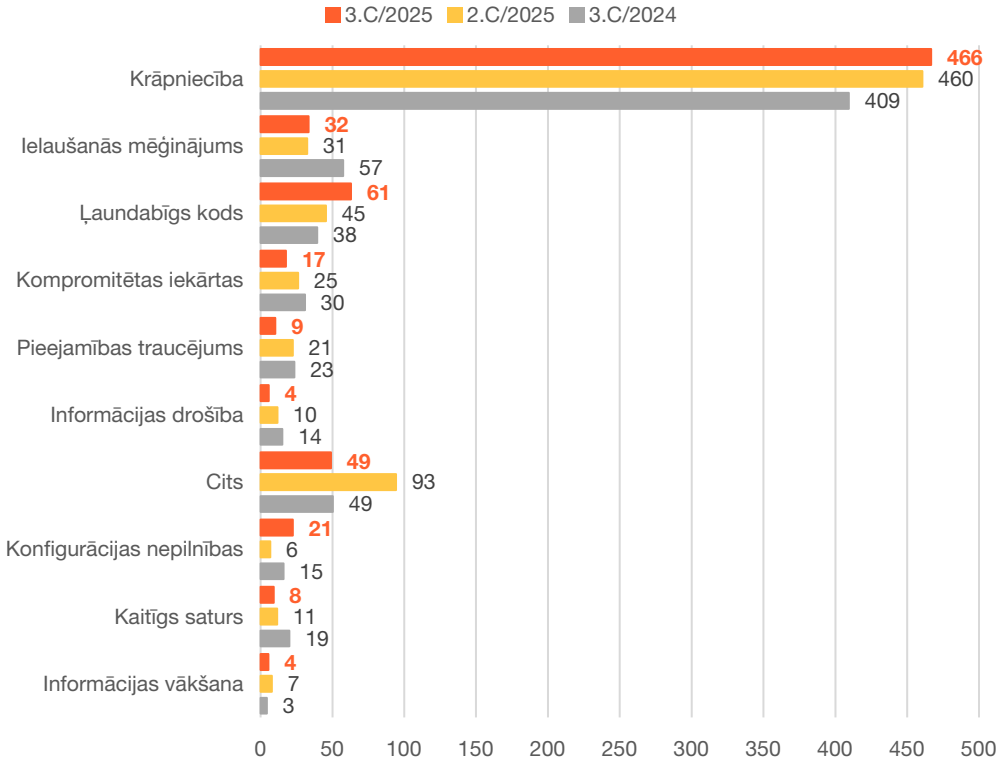
2. Izplatītākie kiberapdraudējumi un būtiskākie notikumi pārskata periodā

TOP 5 kvantitatīvi lielākie kiberapdraudējuma veidi pārskata periodā:

Apdraudējuma veids	Kiberincidentu skaits 2025. gada 3. cet.	Izmaiņas pret 2025. g. 2. cet.	Izmaiņas pret 2024. g. 3. cet.
Krāpniecība	**466**	+1%	+14%
Ļaundabīgs kods	**61**	+36%	+61%
Ielaušanās mēģinājumi	**32**	+3%	-44%
Konfigurācijas nepilnības	**21**	+250%	+40%
Kompromitētas iekārtas	**17**	-32%	-43%

Kiberdraudu struktūras analīze pēc incidentu veidiem

- **Krāpšana saglabājas kā dominējošais drauds**, rādot stabilu pieaugumu un noturīgu pozīciju kā lielākā incidentu kategorija.
- **Būtiski palielinās konfigurācijas nepilnību incidenti**. Nepārtraukta uzraudzība (monitorings), efektīva un savlaicīga ievainojamību pārvaldība (ko nodrošina CERT.LV SOC pakalpojumi) var šo tendenci mazināt.
- **Pieaug ļaunprogramatūras izmantošana**, demonstrējot pakāpenisku augšupeju, kas signalizē par arvien aktīvāku ļaunatūras pielietojumu. Uzņēmumus un iestādes arvien biežāk apdraud šifrējošā izspiedējvīrusa uzbrukumi un biznesa e-pasta kompromitēšana, radot finansiālus zaudējumus un draudus reputācijai.
- **Samazinās pakalpojuma pieejamības traucējumu gadījumi**, kas liecina, ka ieguldījumi aizsardzībā un koordinācijā pret DDoS uzbrukumiem dod rezultātus, bet šī tendence jānostiprina ilgtermiņā.



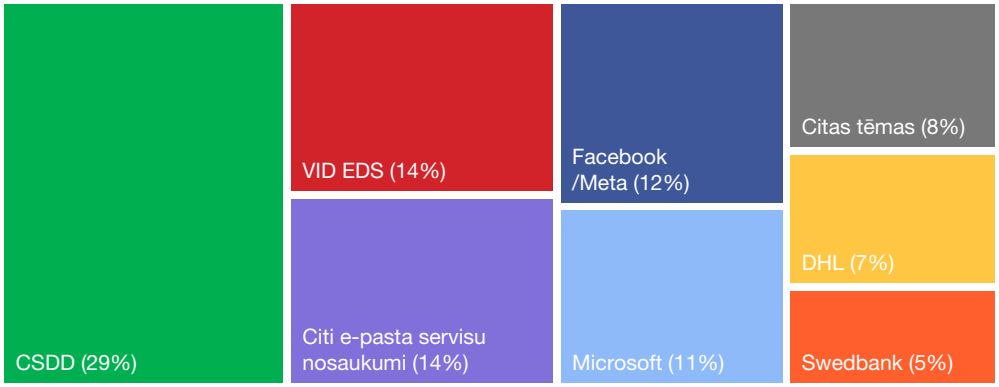
3. attēls. Kiberincidentu skaita salīdzinājums pēc veida

- **Sociālā inženierija kā galvenais uzbrukuma ieejas punkts**

  Turpinās klasiskā pikšķerēšana, izmantojot zināmu organizāciju vārdus. Tāpat krāpnieki izmanto maldinošas reklāmas, atdarinot Latvijas mediju vietnes vai sabiedrībā zināmu cilvēku profilus, lai izplatītu un veicinātu ticamību krāpnieciskiem investīciju piedāvājumiem, kā arī izplatītu viltus ziņas.

  Krāpnieki izmantoja meklētājprogrammas (piemēram, “Google”), lai novirzītu lietotājus uz viltus vietni, kas izskatās līdzīgas portālam “eParaksts.lv” vai “E-veselība”.

Turpinās krāpniecības kampaņas ar viltus e-pasta vēstulēm un īsziņām – vislielākā pikšķerēšanas aktivitāte novērota CSDD, VID EDS, "Facebook" vai "Microsoft" vārda aizsegā. Krāpnieku slazdos nonākušai personai finanšu zaudējumu apmērs svārstās no dažiem simtiem līdz pat vairākiem tūkstošiem eiro.



4. attēls. Izplatītākās pikšķerēšanas kampaņas, izmantojot zināmu organizāciju nosaukumus (procentuālā daļa no kopējā CERT.LV apstrādāto pikšķerēšanas ziņojumu skaita 2025. gada 3. cet.)

CERT.LV atzinīgi vērtē iedzīvotāju iesaisti, kuri identificē un pārsūta gan krāpnieciskus e-pastus un tīmekļa vietnes uz e-pastu cert@cert.lv, gan pārsūta krāpnieciskas īsziņas SMS/WhatsApp uz tālr. 232 304 44.

Saņemtie ziņojumi tiek apkopoti, un kaitnieciskie domēna vārdi ievietoti aktīvās aizsardzības rīkā – DNS ugunsmūrī, lai ierobežotu piekļuvi no Latvijas interneta lietotāju puses un samazinātu iespējamo kaitējumu. DNS ugunsmūris un tā mobilā lietotne bez maksas ir pieejama ikvienam Latvijas iedzīvotājam. Plašāk: www.dnsmuris.lv

- **Turpina pieaugt viltus CAPTCHA (*ClikFix*) ļaunatūras izplatība**

  Jau kopš vasaras pieaudzis ziņojumu skaits par kompromitētām tīmekļa vietnēm, kurās apmeklētājiem tiek rādīti viltus drošības *CAPTCHA* logi, ar aicinājumu apstiprināt, ka lietotājs nav robots.

  Šī metode, pazīstama arī kā *ClikFix*, ir sociālās inženierijas paņēmiens, kas izmanto lietotāju uzticību *CAPTCHA* pārbaudēm, imitējot leģitīmu drošības procesu. Uzbrukuma mērķis ir panākt, lai lietotājs seko norādēm, kas – pašam to neapzinoties – noved pie aktīvā koda izpildes datorā un ļaunprogrammatūras lejupielādes. Ļaunatūra visbiežāk paredzēta autentifikācijas datu izgūšanai. Septembra mēnesī saņemti divi ziņojumi par konkrētās ļaunatūras izplatību.

  Abos gadījumos CERT.LV sazinājās ar mājaslapu īpašniekiem un ieteica, kā atjaunot drošu mājaslapas darbību; tagad tās ir salabotas.

- **Aktīva kritisku ievainojamību izmantošana**

  Pārskata periodā atklāti ļaunprātīgi pārlūku paplašinājumi, kas izspiego lietotājus, kā arī *WinRAR* "nulles" dienas ievainojamības (CVE-2025-8088) izmantošana, kas ļauj uzbrucējam attālināti izpildīt kodu vai izvietot pastāvīgu piekļuvi.

  Tāpat aktīvi tika izmantota kritiskā "Microsoft" ***SharePoint*** ievainojamība (CVE-2025-53770), tostarp vismaz viens kompromitēšanas gadījums Latvijas kritiskās infrastruktūras sektorā.

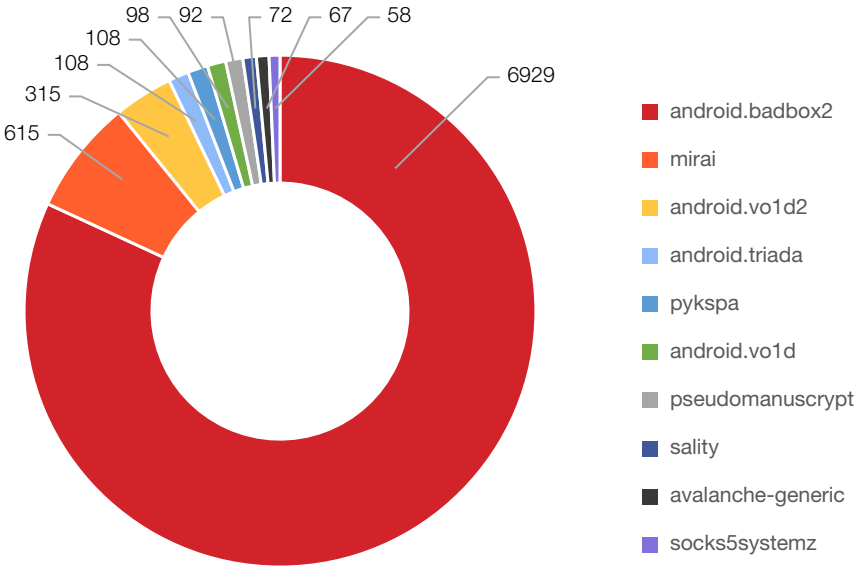
  CERT.LV aktīvi iesaistījās kiberincidenta izmeklēšanā, un veiktā analīze rādīja, ka uzbrucēji nav tikuši tālāk par sākotnējo piekļuvi, pārvietošanās laterāli pa saistītajām sistēmām netika konstatēta. Arvien ātrāka reakcija un kompromitēto sistēmu identificēšana ir CERT.LV spēju un drošības operāciju pakalpojumu attīstības rezultāts.

- **Mobilo un IoT ierīču ļaunatūru izplatība – būtisks gan privātpersonām, gan organizācijām**

  Pārskata periodā ļaunatūru izplatībā dominē *android.badbox2* (82% no visiem CERT.LV reģistrētajiem gadījumiem), kas norāda uz ļoti būtisku un mērķtiecīgu aktivitāti "Android" ierīču segmentā. Tās plašā izplatība liecina par masveida inficēšanas kampaņām, iespējams, izmantojot neoficiālas lietotņu instalācijas vai viltus atjauninājumus. Šī ļaunatūra ir mobilais botu tīkla variants, kas spēj inficēt ierīces, veicot reklāmu izvietošanu, datu zagšanu un attālinātu kontroli par ierīci. Galvenais riski – privāto datu noplūde, inficēto ierīču kompromitēšana un izmantošana kiberuzbrukumos (DDoS, *spam* u.c.).

Otrs nozīmīgākais drauds ir *Mirai* (7%), kas joprojām ir aktīva un tiek izmantota uzbrukumiem neaizsargātām IoT ierīcēm (rūteri, videokameras u.c.). Galvenie riski – DDoS uzbrukumi un infrastruktūras pārslogošana.

Pārējās ļaunatūras kopā veido nelielu daļu, tomēr parāda daudzveidīgu uzbrukumu vektoru kombināciju un palielina kompromitēšanas riskus.



5. attēls. TOP 10 ļaunatūras; skaits 2025. gada 3. ceturksnī

Ieteicamā rīcība:
Mobilo ierīču drošība ir valsts drošības jautājums, jo no kompromitētas ierīces var iegūt stratēģisku un izlūkinformāciju.
Lai mazinātu spiegprogrammatūras riskus, svarīgi:

- **atjaunot ierīces, ieslēdzot automātiskos atjauninājumus;**
- **ievērot kiberdrošības higiēnu: neklikšķināt uz aizdomīgām saitēm, aktivizēt divu faktoru autentifikāciju un izvairīties no neuzticamām lietotnēm.**

- **Izspiedējvīrusu un piegādes ķēžu incidenti**

Pārskata periodā CERT.LV reģistrēja 3 Latvijas organizāciju ziņojumus, kuras cieta šifrējoša izspiedējvīrusa uzbrukumā (2 privātie uzņēmumi un Kultūras informācijas sistēmu centrs). Uzbrucēji kļuvuši organizētāki, to taktikas pielāgojas uzņēmumu aizsardzības mehānismiem, savukārt uzņēmumiem jāuzlabo aizsardzības pasākumi un spēja ātri atjaunot darbību pēc incidenta.

Vērienīgs izspiedējvīrusa uzbrukums pret *Collins Aerospace* radīja traucējumus lielākajās lidostās Eiropā; ceļotāji, tostarp no Latvijas, saskārās ar ilgāku gaidīšanas laiku pie reģistrācijas un iekāpšanas, un kavētiem reisiem. Rīgas lidostā tiek izmantotas citas automatizētās reģistrācijas un iekāpšanas sistēmas, un tiešas ietekmes tieši šī incidenta rezultātā nebija.

Uzbrucēji varēja ietekmēt daudzus operatorus vienlaikus, izmantojot vienu centralizētu piegādātāju un pakalpojumu; incidenta analīze liecina, ka kiberuzbrukumi mērķēti uz pakalpojumu sniedzēju kopīgajām vājajām vietām, nevis uz katru lidostu atsevišķi, panākot efektu plašākā amplitūdā.

Tas pierāda, ka piegādes ķēžu uzbrukumi tiek izmantoti arvien biežāk.

Ieteicamā rīcība:

- **veikt piegādātāju drošības auditus;**
- **paredzēt stingrākas prasības jau iepirkumos;**
- **regulāri pārbaudīt vai lietotā programmatūra tiek atjaunota un ielāpi uzstādīti.**

Būtiskāko kiberdraudu tendences un ieteicamie soļi

Tendences	Situācija Latvijas kibertelpā un ieteicamie soļi
Piegādes ķēžu kompromitēšana	Trešo pušu servisu izmantošanas drošība, riski un pārvaldīšanas iespējas. MK noteikumu "Minimālas kiberdrošības prasības" stāšanās spēkā (2025. gada 2. jūlijā) ir pozitīvs solis, kas uzlabos kopējo kiberdrošības līmeni, tostarp lai nodrošinātu piegādes ķēžu drošību.
Cilvēkfaktors, novecojušas IT sistēmas	Jāturpina ES atbalsta programma, kas veicina uzņēmumu kiberdrošības pārveidi kapacitātes stiprināšanai; jāstiprina centralizēta ievainojamību pārvaldība, jāveic regulāras apmācības darbiniekiem un IT drošības testi.
Digitālā novērošana un privātuma zuduma risku pieaugums	Krievijā ieviestā tērzēšanas lietotne *MAX*, kas faktiski ir kremļa izstrādāts instruments sabiedrības digitālai kontrolei, cenzūrai un uzraudzībai, var tikt lejupielādēta un lietota arī Latvijā. Šādas lietotnes izmantošana rada nopietnu risku, jo var tikt nodota izlūkinformācija par Latvijas iedzīvotājiem. Mobilo ierīču lietotāju privātuma apdraudējumu, iespējams, var radīt *ChatControl*, kas tiesībaizsardzības iestādēm nodrošinātu likumīgu piekļuvi šifrētiem datiem. Eksperti norāda uz riskiem, ka to nevar tehniski ieviest, neliekot pārbaudīt visu saturu.
Mērķēti uzbrukumi, izmantojot IoT datus	IoT ierīces kļūst arvien populārākas, bet neaizsargātas tās var tikt izmantotas ļaunprātīgiem nolūkiem. Jāveicina IoT drošības standartu ieviešana un lietotāju informēšana par riskiem.
Hibrīddraudu pieaugums	Ģeopolitiskās spriedzes dēļ Latvija ir tiešs hibrīduzbrukumu mērķis (DDoS, dezinformācija, sabotāža). Pārskata periodā Krievijas hakeri ietekmēja hidroelektrostacijas Polijā un Norvēģijā. Šādi incidenti akcentē nepieciešamību stiprināt sistēmu un operacionālo tehnoloģiju (OT) drošību. Veicinot industriālās automatizācijas un kontroles sistēmu drošību, CERT.LV piedāvā enerģētikas, transporta, ūdens u.c. infrastruktūras turētājiem drošības testus, izstrādā sensorus OT sistēmām .
MI ļaunprātīga izmantošana	Viltus ziņu saturs, kas veidots ar MI rīkiem, padara manipulācijas grūtāk atpazīstamas. Jāstiprina sabiedrības medijpratība, kā arī sadarbība starp valdību un medijiem.

- **Ģeopolitiski motivēti uzbrukumi**

  Gan kā reakcija uz ārpolitiskiem paziņojumiem (Latvijas uzvara starptautiskā dronu iepirkumā kontekstā ar atbalstu Ukrainai), gan plašākas "DDoSIA" grupējuma NoName0579(16) ietekmes operācijas – šie draudi turpinās. 3. ceturksnī DDoS uzbrukumi tika vērsti pret vairākām pašvaldību tīmekļvietnēm, transporta un telekomunikācijas infrastruktūru. Tika novēroti īslaicīgi darbības traucējumi, bet lielākā daļa resursu bija pienācīgi pasargāti, un uzbrukumi ietekmi neradīja.

  Politiski jeb ideoloģiski motivēti DDoS uzbrukumi, ko veic Krievijas Federācijas agresiju atbalstoši haktīvistu grupējumi ar mērķi radīt sabiedrībā rezonansi un graut uzticību valsts iestādēm, viļņveidīgi notiek jau kopš 2022. gada, un ticams, ka Baltijas jūras valstis turpinās būt Krievijas kiberoperāciju ilgtermiņa mērķi.

  Lai mazinātu DDoS uzbrukumu ietekmi, organizācijām ieteicams izmantot DDoS aizsardzības pakalpojumus. Aizsardzības ministrija finansē centralizētu DDoS aizsardzības pakalpojumu – Valsts pārvaldes iestādēm tas pieejams bez maksas. Pakalpojuma nodrošināšana deleģēta LVRTC.

Galvenie secinājumi

- **Uzbrukumi kļūst hibrīdi** – tie vienlaikus izmanto gan tehnoloģiskas, gan cilvēkfaktora ievainojamības.
- **Ātrums ir kritisks faktors** – gan uzbrucēju reakcijā, gan aizsardzības pusē.
- **Noturība jāveido daudzslāņaina** – tehnoloģiskā, operacionālā, organizatoriskā un cilvēkfaktora līmenī.

Šīs tendences uzsver nepieciešamību pēc CERT.LV pakalpojumiem – DNS ugunsmūris, atbalsts incidentu risināšanā, SOC spējas, draudu medības, drošības testi, lietotāju izglītošana un apmācības – tas stiprina tehnoloģisko un cilvēcisko resursu kibernoturību un gatavību nākotnes draudiem.

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

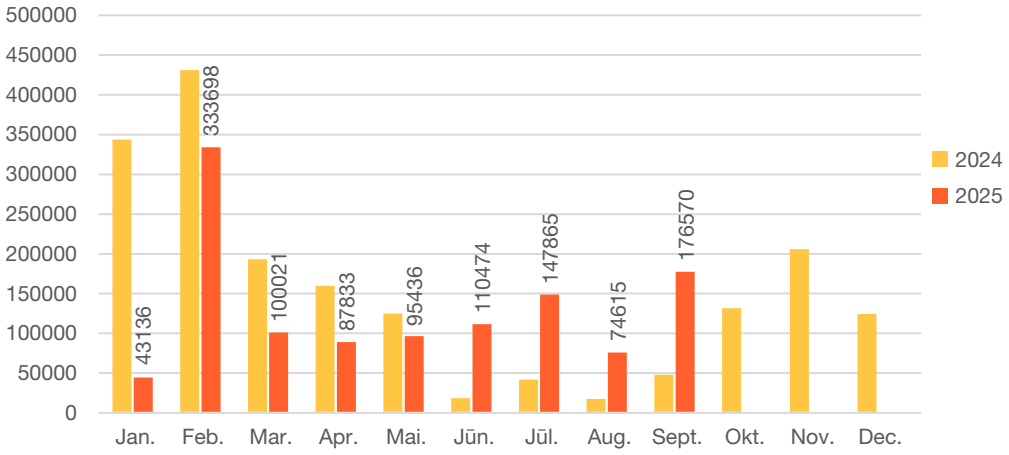
CERT.LV pakalpojumi, tostarp DNS ugunsmūris, atbalsts incidentu risināšanā, Drošības operāciju centrs (SOC), kiberdrošības draudu medības, drošības testi, sabiedrības izglītošana un apmācības u.c., ir būtisks resurss risku mazināšanai un noturības stiprināšanai pret arvien intensīviem un sarežģītiem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

DNS ugunsmūris

2025. gada 3. ceturksnī kopskaitā DNS ugunsmūra pakalpojuma ietvaros:

- **Kaitīgo domēna vārdu DNS pieprasījumu skaits** sasniedza gandrīz **4,6 miljonus**, kas ir **par 81% vairāk salīdzinājumā ar 2. ceturksni un par 418% vairāk nekā pērn 3. ceturksnī**. Pieaugumu, iespējams, izraisīja sezonālie faktori (piemēram, iedzīvotāju atgriešanās darbos pēc vasaras atvaļinājumiem). Izteikti redzams, ka notikuši pieprasījumi arī uz dažādām inficētām "WordPress" lapām ļoti lielā daudzumā, tomēr vairumā gadījumu reāla cilvēku klikšķināšana uz šīm lapām neuzrādās, un tie, visticamāk, ir bijuši automatizēti pieprasījumi (no firewall vai proxy sistēmām), kas pārbauda regulāri domēnu reputāciju.
- **Visu CERT.LV DNS ugunsmūrim uzturēto sarakstu atvairītie kiberuzbrukumi** pasargāja lietotājus no ļaunprātīgu vietņu apmeklēšanas **399 050** reizes, kas ir ievērojams pieaugums – **par 36% vairāk nekā 2. ceturksni un par 74% vairāk nekā pērn 3. ceturksnī**. Iespējamie pieauguma iemesli varētu būt sezonālie vai laika perioda faktori – ciklisks pieaugums, kas var mainīties nākamajā ceturksnī. Atvairījumu skaitu tiešā veidā ietekmē arī aktīvo krāpniecības kampaņu skaits.
- **Kopš ieviešanas DNS ugunsmūra lietotne** lejupielādēta **65 tūkst.** (31,8K Android un 32,9K iOS) ierīcēs.

Lai stiprinātu sabiedrības kiberdrošību un noturību pret apdraudējumiem un vienlaikus izglītotu par kiberhigiēnu un digitālajām krāpniecības shēmām, pārskata periodā kiberdrošības kampaņas "Už pēc shēmas!" CERT.LV eksperti aktīvi sniedza intervijas un uzsvēra DNS ugunsmūra nozīmi kā efektīvu aizsardzības risinājumu pret mūsdienu kiberapdraudējumiem.



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	**30805**
Vietnes, kurās ievietots kaitīgs Javascript kods un izvada viltus uznirstošos logus	**22026**
Vietnes, kas piedāvā viltus finanšu pakalpojumus	**14621**
"DELFI" tēla izmantošana krāpniecisku kriptovalūtu investīciju platformu reklamēšanas kampaņās	**12316**
"CSDD" tēla izmantošana viltus vietnes kampaņās	**9823**
"jauns.lv" tēla izmantošana krāpniecisku kriptovalūtu investīciju platformu reklamēšanas kampaņās	**7485**
"DPD" tēla izmantošana viltus vietnes kampaņās	**2404**
"FedEx" tēla izmantošana viltus vietnes kampaņās	**2383**
"Valsts ieņēmumu dienests" tēla izmantošana viltus vietnes kampaņās	**1542**
"Latvijas Pasts" tēla izmantošana viltus vietnes kampaņās	**1231**

Apdraudējumu agrās brīdināšanas sistēma (ABS)

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

CERT.LV turpina ABS sistēmas uzturēšanu un paplašināšanu.

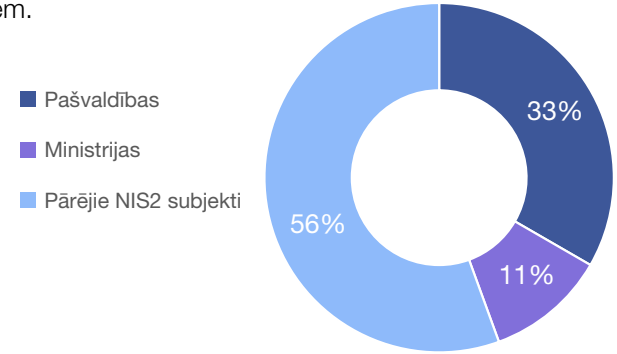
2025. gada 3. ceturksnī ABS ģenerēto brīdinājumu skaits bija **1,3 miljardi**, kas ir par 24% mazāk nekā iepriekšējā ceturksnī un par 29% mazāk nekā pērn 3. ceturksnī.

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, turpinās CERT.LV SOC pakalpojuma aktīva attīstīšana un jaunu klientu piesaiste, paplašinot klientu loku atbilstoši NKDL, lai sekmētu efektīvāku aizsardzību un noturību pret kiberapdraudējumiem.



7. attēls. CERT.LV SOC klientu sektoru struktūra 2025. gada 3. ceturksnī (procentuālā daļa no kopējā skaita)

Drošības trauksmes ziņojumu dinamika kopskatā

- **Iegūta redzamība pār 40 720 iekārtām**, tostarp serveriem un darbstacijām.
- Gala iekārtu skaits pieauga par **6 892 iekārtām – pieaugums veido aptuveni 20% no kopēja apjoma**, līdz ar to palielinājies arī drošības trauksmes ziņojumu skaits.
- Reģistrēti vairāk nekā **15 miljoni** drošības trauksmes ziņojumu, kas ir **par 43% vairāk** nekā 2. cet. Lielais pieaugums skaidrojams ar iegūtu plašāku redzamību jauno klientu infrastruktūrā un laiku trauksmes ziņojumu apstrādei, lai izmeklētu un noklusinātu viltus pozitīvās trauksmes.
- Apstrādājot drošības trauksmes ziņojumus, **manuāli izveidotas 486 lietas**.

Iekārtu skaits ar iegūtu redzamību	**40 720**
Reģistrēto drošības trauksmes ziņojumu skaits	**15M+**
Manuāli izveidotas lietas	**486**
Viltus pozitīvie	**472**
Incidentu skaits	**14**
Zems trauksmes līmenis:	**4M+**
Vidējs trauksmes līmenis:	**11M+**
Augsts trauksmes līmenis:	**64K+**
Kritisks trauksmes līmenis:	**5K+**

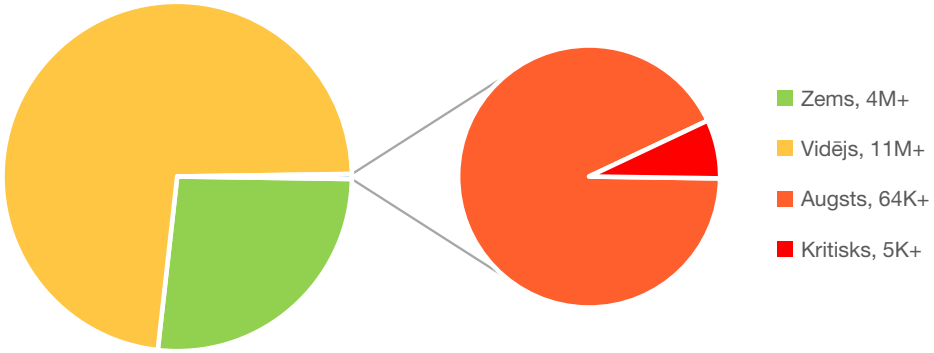
8. attēls. Drošības trauksmes ziņojumu dinamika SOC klientu infrastruktūrā (dati uz 30.09.2025.)

Pārliecinoši lielākā daļa trauksmju ir vidējā un zemā līmeņa, kas var būt saistītas ar sistēmu troksni, viltus pozitīviem vai mazāk nopietniem gadījumiem.

Tikai 0.5% no visām trauksmēm ir augsta/kritiska līmeņa. Kritisko incidentu skaits (5K+) kvantitatīvi ir salīdzinoši niecīgs procents no kopēja apjoma (0.03%), taču tieši tie prasa vislielāko uzmanību.

Augsta līmeņa trauksmes (64K+) veido nozīmīgu slodzi SOC komandai. Tās ir indikatori potenciāli bīstamiem uzbrukumiem un prasa rūpīgu pārbaudi.

Kritiska un augsta līmeņa trauksmju absolūtais skaits (~69 tūkst.) norāda uz pastāvīgiem nopietniem apdraudējumiem.



9. attēls. CERT.LV SOC reģistrētie drošības trauksmes ziņojumi 2025. gada 3. ceturksnī

Uzraugot klientu infrastruktūru ar CERT.LV nodrošināto SOC pakalpojumu, 2025. gada 3. ceturksnī tika reģistrēti 14 kiberincidenti.

Biežāk konstatētie kiberincidenti un ieteicamā rīcība

Kiberincidents	Riski	Ieteicamā rīcība
Paroļu pilnās pārlases (*brute-force*) uzbrukumi	Darbstacijas pieslēgtas ārējiem tīklam, apejot korporatīvās drošības politiku, iekārtas eksponētas internetā bez lokāla ugunsmūra. Tas palielina ievainojamību pret automatizētiem uzbrukumiem.	► Uzstādīt lokālos ugunsmūrus. ► Nodrošināt VPN savienojumu ar korporatīvo tīklu. ► Lietot spēcīgas paroles un MFA.
Nevēlamas programmatūras lietošana korporatīvā vidē	Neoficiāli aktivizācijas rīki, spēles, failu tiešās apmaiņas programmatūras (*BitTorrent*) u.c. var saturēt ļaunatūru, kas apdraud sistēmas integritāti un var kompromitē sistēmu.	► Ieviest programmatūras balto sarakstu. ► Attinstalēt neautorizētas lietotnes un privātām vajadzībām izmantotās programmas. ► Noņemt novecojušas vai dublējošas programmas ► Neizmantot programmatūru no ārpus NATO/ EU ražotājiem. ► Neizmantot vairākus attālinātās piekļuves rīkus vienlaicīgi.
Ļaunatūra, kas izplatās caur USB zibatmiņas vai viltus CAPTCHA (*ClikFix*)	Lietotāji tiek maldināti ar viltus CAPTCHA, kas imitē drošības pārbaudes. Aktivizējot ļaunatūru, tiek iegūti piekļuves dati, e-pasta sarakste u.c. konfidenciāla informācija, ko var izmantot turpmākos uzbrukumos.	► Liegt izpildāmu datņu palaišanu no USB. ► Regulāri atjaunināt pārlūkprogrammas. ► Lietot pārlūka paplašinājumus, kas bloķē aizdomīgus skriptus. ► Izglītot darbiniekus par sociālās inženierijas paņēmieniem

Kiberdrošības draudu medību operācijas

Uz pārskata beigām kiberdrošības draudu medību operācijās kopš 2022. gada analīze ir veikta kopskaitā:

- **vairāk nekā 162 000 gala iekārtās** (3.cet. gala iekārtu skaits **pieauga par 2 000**);
- **gandrīz 40 publiskā sektora** būtisku un svarīgu pakalpojumu sniedzēju iestādēs un IKT kritiskās infrastruktūras uzņēmumu infrastruktūrās;
- aptuveni **20%** organizāciju iekārtās tika identificēta ārvalstu APT klātbūtne.

IT sistēmu drošības testi un pikšķerēšanas uzbrukumu simulācijas kampaņas

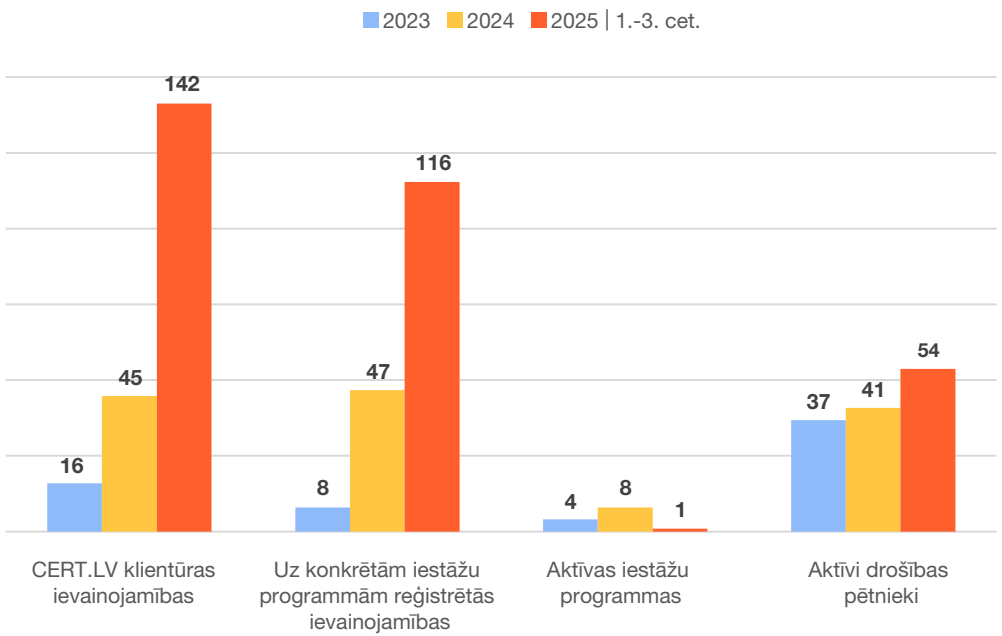
2025. gada 3. ceturksnī CERT.LV veica **4 IT sistēmu drošības testus**, kuras gaitā identificētas **kopskaitā vairāk nekā 10 ievainojamības ar dažāda riska līmeņi**.

Tāpat CERT.LV veica kiberuzbrukuma simulāciju vienam no Latvijas kritiskās infrastruktūras apkalpošanas uzņēmumiem, kuras gaitā tika identificētas un novērstas vairākas tādas kritiskas nepilnības, kas ļautu uzbrucējiem pilnībā pārņemt uzņēmuma IT sistēmas un pārvaldīto kritisko infrastruktūru.

Pārskata periodā CERT.LV veica kopskaitā **4 pikšķerēšanas uzbrukumu simulācijas** kampaņas, lai apmācītu un veicinātu organizāciju darbinieku spējas identificēt potenciāli riskantus uzvedības modeļus, atpazīt un novērst kiberapdraudējumus un informācijas noplūdi. Kopējā kampaņas auditorija: **1 541 persona**.

Koordinēta ievainojamību atklāšana (CVD)

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



10. attēls. CVD platforma: Ievainojamību ziņojumu skaits Latvijā

Uz pārskata perioda beigām (30.09.2025.) CVD platformā kopskaitā reģistrēti:

- Drošības pētnieki: **132 aktīvi** (3.cet. +18)
- Aktīvas iestāžu programmas: **13**
- Ievainojamību ziņojumi: **372** (3. cet. +159), tostarp:
  - ✓ CERT.LV klientūras ievainojamības: **203** (3.cet.+ 100)
  - ✓ Uz konkrētām Iestāžu programmām reģistrētās ievainojamības: **171** (3.cet.+59)

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