2026 C2

SITUĀCIJA LATVIJAS KIBERTELPĀ

PERIODS:

01.04.2026. - 30.06.2026.

CERT.LV
Kiberincidentu novēršanas institūcija

Latvijas Universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Kopsavilkums

Kibertelpas situācijas novērtējums

Kibertelpas drošības apdraudējums Latvijā saglabājas augsts, un ilgtermiņā kiberdraudu intensitāte turpina pieaugt. To nosaka ģeopolitiskā situācija, arvien plašāka ievainojamību un mākslīgā intelekta izmantošana kiberuzbrukumos un lietotāju nekritiska paļaušanās uz digitālajiem rīkiem. Šie faktori prasa turpināt sistemātisku kiberrisku pārvaldību un konsekventi stiprināt organizāciju visaptverošo kibernoturību.

2026. gada 2. ceturksnī reģistrēti **673 manuāli apstrādāti kiberincidenti**, kas ir par 20% mazāk nekā iepriekšējā ceturksnī un par 5% mazāk nekā attiecīgajā periodā pērn. Arī **identificēto apdraudēto iekārtu skaits samazinājās līdz 396 444**, kas ir par 48% mazāk nekā iepriekšējā ceturksnī un par 14% mazāk nekā pirms gada. Tomēr abi rādītāji **joprojām ievērojami pārsniedz 2022.-2024. gada vidējo līmeni**, un tas liecina, ka **kiberdrošības apdraudējums saglabājas augsts**.

Galvenie draudi

Galvenie sākotnējās kompromitēšanas veidi joprojām ir publiskā tīklā pieejamu informācijas sistēmu ievainojamību izmantošana un pikšķerēšanas uzbrukumi, kas vērsti pret korporatīvā tīkla lietotājiem. Paaugstināts risks saglabājas organizācijās ar novecojušām vai nepietiekami uzturētām tīmekļvietnēm, neatjauninātām satura vadības sistēmām un to spraudņiem.

Būtiskāko ietekmi uz organizācijām turpina radīt izspiedējvīrusa uzbrukumi un datu noplūdes. To apliecina pārskata periodā notikušais liela mēroga kiberuzbrukums AS "Latvijas valsts meži" (LVM) IT infrastruktūrai, kur savlaicīgi nenovērsta publiski pieejamas sistēmas ievainojamība kļuva par ieejas punktu plašākam uzbrukumam. Šis gadījums uzskatāmi parādīja, ka pat viena kritiska ievainojamība var būtiski ietekmēt organizācijas darbības nepārtrauktību, radīt sistēmu darbības traucējumus, datu noplūdes risku un nepieciešamību apturēt kritisku IT sistēmu darbību.

Vienlaikus pieaug sociālās inženierijas, identitātes kompromitēšanas un informācijas zagšanas ļaunatūras radītie riski. Pakalpojumatteices jeb DDoS kiberuzbrukumi saglabājas kā efektīvs ģeopolitiska spiediena instruments un pastāvīgs apdraudējums.

Kvantitatīvi dominējošais kiberincidenta veids joprojām ir krāpšana, kas visvairāk skar iedzīvotājus. Arī Finanšu nozares asociācijas apkopotie 2026. gada pirmo sešu mēnešu dati rāda, ka Latvijas lielāko banku klientiem vidēji mēnesī tiek izkrāpti ap 1,3 milj. eiro. Tādēļ līdztekus tehniskajiem drošības pasākumiem būtiski turpināt stiprināt sabiedrības informētību un noturību pret sociālās inženierijas uzbrukumiem, īpaši pikšķerēšanu.

Krievija joprojām ir galvenais kiberdraudu avots Latvijai. Tās atbalstītu kiberuzbrucēju un haktīvistu aktivitāte, tostarp reaģējot uz Latvijas pausto atbalstu Ukrainai, visticamāk, saglabāsies arī turpmāk.

Ņemot vērā aktuālo draudu raksturu, organizācijām prioritāri jāstiprina ievainojamību pārvaldība, nepārtraukta kiberdrošības uzraudzība (SOC/EDR/XDR/SIEM), daudzfaktoru autentifikācijas izmantošana, rezerves kopiju pārvaldība, piegādes ķēžu drošība, regulāra lietotāju apmācība, vienlaikus periodiski testējot incidentu reaģēšanas un darbības nepārtrauktības plānus.

CERT.LV darbības rezultāti

Pieaugošie draudi vienlaikus veicina kiberdrošības spēju attīstību. Tie palielina pieprasījumu pēc datos balstītiem pakalpojumiem, lai uzlabotu spēju savlaicīgi identificēt un novērst apdraudējumus.

2026. gada pirmajos sešos mēnešos CERT.LV Kiberincidentu risināšanas komandas preventīvais darbs un DNS ugunsmūra aktīvā aizsardzība **novērsa vairāk nekā 5 milj. piekļuves mēģinājumu ļaunprātīgām vietnēm** – 6,5 reizes vairāk nekā attiecīgajā periodā pērn. Jūnijā sasniegts rekordaugsts rādītājs – 1,1 milj.

Kopsavilkums

Pilnveidojot automatizētās draudu atklāšanas metodes, CERT.LV 2. ceturksnī **apsteidzoši identificēja un novērsa 1 166 aktīvas krāpnieciskas kampaņas** – par 900 vairāk nekā iepriekšējā ceturksnī - vēl pirms tās masveidā sasniedz lietotājus un rada zaudējumus.

Pārskata periodā tika veikti **18 IT sistēmu drošības testi**, kuros **identificēta 31 ievainojamība**, tostarp kritiskas un augstas ietekmes, kas tika novērstas pirms to iespējamas izmantošanas kiberuzbrukumos.

Pieaug organizāciju redzamība gala iekārtu līmenī, ko nodrošina CERT.LV Drošības operāciju centra (SOC) pakalpojumu ieviešana atbilstoši nacionālajam regulējumam. Kopumā **nodrošināta 57 021 gala iekārtas pārskatāmība**, kas ļauj savlaicīgi identificēt un novērst apdraudējumus, sistemātiski stiprinot noturību.

Turpinot apmācības un sabiedrības izglītošanu kiberdrošības jomā, pārskata periodā **95 pasākumos tika apmācīti 8 632 dalībnieki** – attiecīgi par 34% un 19% vairāk nekā attiecīgajā periodā pērn.

Starptautiskajā arēnā Latvijas lomu Eiropas kiberdrošības incidentu reaģēšanas komandu sadarbības kopienā stiprināja **TF-CSIRT sanāksme Rīgā**, pulcējot vairāk nekā 150 nozares ekspertu. Forums **pievērsa uzmanību aktuālajiem kiberapdraudējumiem un izaicinājumiem Latvijā**. Tas ir īpaši svarīgi laikā, kad kiberincidenti kļūst arvien sarežģītāki, un ciešāka sadarbība starp organizācijām un valstīm ir kritiski nepieciešama.

Stiprinot un pilnveidojot institūciju sadarbību un gatavību reaģēt uz plaša mēroga kiberincidentiem, **"Cyber Europe" mācībās tika izvērtēta Latvijas transporta nozares spēja** koordinēti reaģēt uz sarežģītiem kiberdrošības incidentiem.

CERT.LV organizētā jau **astotā Draudu medību operācija ar paplašinātu klātbūtni apliecina pieaugošu operacionālo briedumu**, nostiprinot to kā starptautiski atzītu civilās un militārās sadarbības modeli.

Savukārt Latvijas-Singapūras apvienotās komandas izcīnītā **1. vieta starptautiskajās kiberaizsardzības mācībās "Locked Shields 2026"** apliecina Latvijas kiberdrošības speciālistu augsto profesionālo sagatavotību un spēju efektīvi reaģēt uz sarežģītiem kiberincidentiem. Tas arī stiprina valsts pārvaldes, militārā sektora un tehnoloģiju uzņēmumu sadarbības modeli.

Galvenie secinājumi

Lai gan pārskata periodā kiberincidentu un identificēto apdraudēto iekārtu skaits samazinājās, kiberdrošības apdraudējums Latvijā saglabājas augsts, un ilgtermiņā draudu intensitāte turpina pieaugt. Lielāko risku organizācijām rada savlaicīgi nenovērstas ievainojamības, identitātes kompromitēšana un sociālās inženierijas uzbrukumi, kas bieži kalpo par sākumpunktu plašākiem incidentiem.

Vienlaikus turpina pieaugt organizāciju redzamība gala iekārtu līmenī, ko nodrošina CERT.LV SOC, DNS ugunsmūra un citu datos balstītu kiberdrošības pakalpojumu ieviešana, lai varētu laikus novērst, atklāt, analizēt un ierobežot kiberincidentus vai reaģēt uz kiberincidentiem un tos pārvarēt.

Turpmāk organizāciju noturību arvien vairāk noteiks efektīva kiberdrošības risku pārvaldība, nepārtraukta kiberdrošības uzraudzība (SOC/EDR/XDR/SIEM), daudzfaktoru autentifikācijas izmantošana, rezerves kopiju pārvaldība, piegādes ķēžu drošība un regulāra lietotāju apmācība, vienlaikus regulāri testējot incidentu reaģēšanas un darbības nepārtrauktības plānus.

Galvenie rādītāji

673 (-5%)

Manuāli apstrādātie kiberincidenti
2026.-2.CET. vs 2025-2.CET.

~369K (-14%)

Identificēto apdraudēto iekārtu skaits
2026.-2.CET. vs 2025-2.CET.

441 (-4%)

Krāpšana – kvantitatīvi dominējošais incidentu veids
2026.-2.CET. vs 2025-2.CET.

73 (+56%)

Kompromitētas iekārtas – straujākais kāpums
2026.-2.CET. vs 2025-2.CET.

~2,5M (754%)

CERT.LV DNS ugunsmūra novērstie lietotāju piekļuves mēģinājumi ļaunprātīgām vietnēm
2026.-2.CET. vs 2025-2.CET.

1 166 (+900)

Apsteidzoši identificētas un novērstas krāpnieciskas kampaņas pirms tās sasniedz lietotāju
2026.-2.CET. vs 2025-2.CET.

105 (2. cet. skaits pieauga par 13)

Iestāžu (NKDL subjektu) skaits kopumā, kas izmanto CERT.LV SOC pakalpojumu
Dati kopumā uz 2026.-2.CET. beigām

57 021 (2. cet. skaits pieauga par 32%)

CERT.LV SOC pakalpojuma ietvarā nodrošinātā redzamība organizāciju gala iekārtām
Dati uz 2026.-2.CET. beigām

185 (2. cet. skaits pieauga par 19)

CVD platformā kopumā reģistrēti drošības pētnieki
Dati uz 2026.-2.CET. beigām

683 (2. cet. skaits pieauga par 142)

CVD platformā kopumā reģistrēti ievainojamību ziņojumi
Dati uz 2026.-2.CET. beigām

95 (+34%)

CERT.LV ekspertu īstenotās izglītojošās aktivitātes/pasākumi kiberdrošības jomā
2026.-2.CET. vs 2025-2.CET.

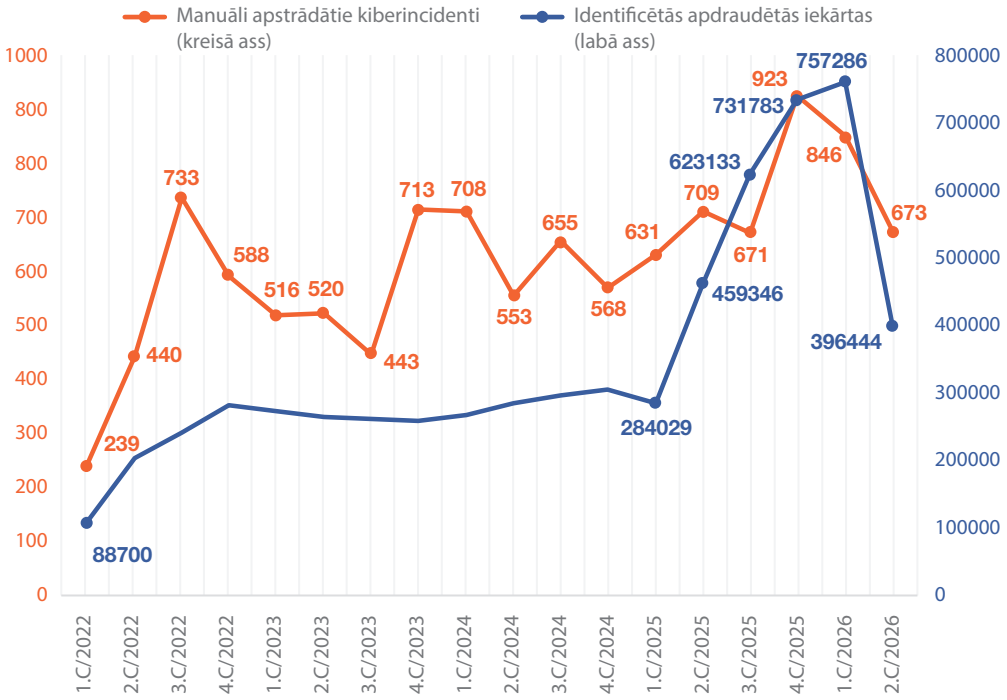
8 632 (+19%)

Sasniegtās auditorijas skaits CERT.LV ekpertu īstenotās aktivitātēs/pasākumos
2026.-2.CET. vs 2025-2.CET.

Satura rādītājs

1. Kibertelpas drošības apdraudējumi: statistika un tendences

Kibertelpas drošības apdraudējums Latvijā saglabājas augsts, un ilgtermiņā kiberdraudu intensitāte turpina pieaugt. To nosaka ģeopolitiskā situācija, arvien plašāka ievainojamību un mākslīgā intelekta izmantošana kiberuzbrukumos un lietotāju nekritiska paļaušanās uz digitālajiem rīkiem. Šie faktori prasa turpināt sistemātisku kiberrisku pārvaldību un konsekventi stiprināt organizāciju visaptverošo kibernoturību.



1. attēls. Kiberincidentu un identificēto apdraudēto iekārtu dinamika (skaits)

Manuāli apstrādātie kiberincidenti

2026. gada 2. ceturksnī Latvijā reģistrēti **673 manuāli apstrādāti kiberincidenti**, kas ir par **20%** mazāk nekā 2026. gada 1. ceturksnī un par 5% mazāk nekā attiecīgajā periodā pērn.

Kiberincidentu skaits samazinājās jau otro ceturksni pēc kārtas, un to, visdrīzāk, veicinājusi efektīvāku apdraudējumu atklāšanas un novēršanas mehānismu ieviešana. Uzlabojot automatizētās draudu atklāšanas metodes, 2. ceturksnī **CERT.LV apsteidzoši identificēja un novērsa 1 166 aktīvas krāpnieciskas kampaņas – par 900 vairāk nekā 1. ceturksnī – vēl pirms tās masveidā sasniedz lietotājus un rada zaudējumus**.

Papildus tam CERT.LV proaktīvi monitorē un bloķē identificētās krāpnieciskās kampaņas, operatīvi pievienojot to indikatorus DNS ugunsmūrim. Būtiska nozīme ir arī sabiedrības iesaistei. Iedzīvotāju ziņojumi palīdz operatīvi identificēt jaunas krāpniecības kampaņas un savlaicīgi pasargāt citus lietotājus. **2026. gada pirmajos sešos mēnešos CERT.LV DNS ugunsmūris ir novērsis vairāk nekā 5 milj. piekļuves mēģinājumu ļaunprātīgām tīmekļvietnēm, kas ir 6,5 reizes vairāk nekā attiecīgajā periodā pērn**.

Tomēr kiberincidentu skaits joprojām saglabājas augsts un pārsniedz 2022-2024. gada vidējo līmeni. Kopš 2022. gada Krievijas pilna mēroga iebrukuma Ukrainā Latvijas kibertelpā reģistrēto kiberincidentu skaits ir pieaudzis seškārtīgi. Ilgtermiņa tendence - joprojām ir augšupejoša, kiberdraudu intensitāte turpina pieaugt.

1 **Kiberdrošības incidents** (turpmāk — kiberincidents) — notikums, kas apdraud 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.

Identificētās apdraudētās iekārtas

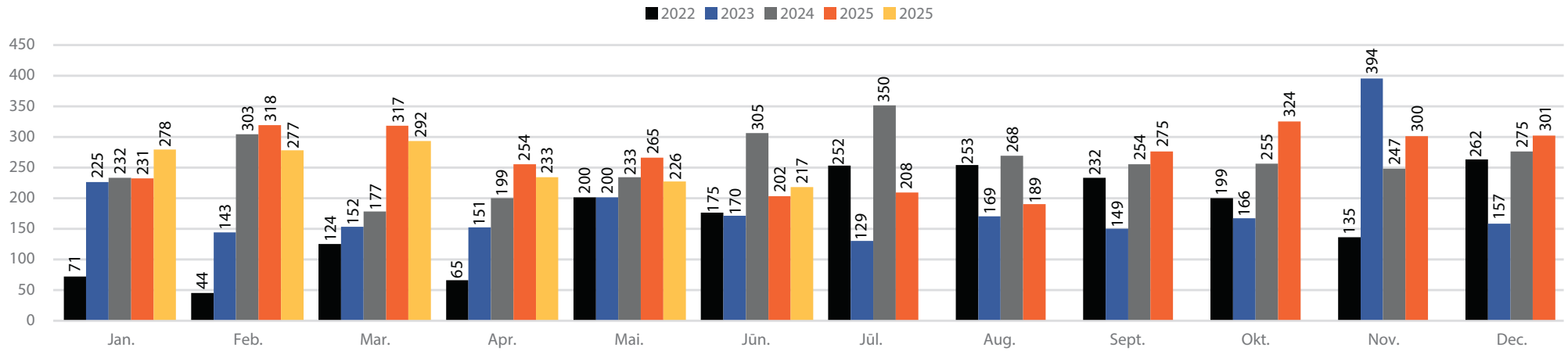
Lai gan 2026. gada 2. ceturksnī CERT.LV **identificēto apdraudēto iekārtu skaits būtiski samazinājās** (par **48%** salīdzinājumā ar iepriekšējo ceturksni un par **14%** salīdzinājumā ar attiecīgo periodu pērn), identificētās **396 444** apdraudētās iekārtas liecina, ka kiberdraudu līmenis joprojām ir augsts.

Šī dinamika daļēji skaidrojama ar izmaiņām datu avotu pieejamībā, jo viens no iepriekš izmantotajiem avotiem vairs nenodrošina informāciju par potenciāli inficētām iekārtām Latvijā.

Tāpat novērsti vairāki gandrīz notikuši kiberincidenti. CERT.LV identificēja un novērsa ievainojamas 76 industriālās kontroles sistēmās, nepieļaujot to izmantošanu potenciālos uzbrukumos.

Pozitīva tendence ir pakāpenisks to organizāciju skaita pieaugums, kuras izmanto CERT.LV Drošības operāciju centra (SOC) pakalpojumus atbilstoši Nacionālā kiberdrošības likuma (NKDL) prasībām. Tas paplašina monitorējamo gala iekārtu apjomu un redzamību, uzlabo kiberapdraudējumu savlaicīgas identificēšanas iespējas un stiprina gan organizāciju, gan valsts kopējo kibernoturību.

Kopumā secināms - neraugoties uz kiberincidentu un identificēto apdraudēto iekārtu skaita samazināšanos, to skaits joprojām ir ievērojami lielāks nekā 2022.-2024. gada vidējais līmenis, un kiberdraudu līmenis joprojām saglabājas augsts. Vienlaikus dati liecina, ka kopumā organizāciju īstenotie drošības pasākumi, tostarp SOC pakalpojuma izmantošana, sniedz pozitīvus rezultātus, tādēļ svarīgi turpināt sistemātisku kiberrisku pārvaldību un konsekventi stiprināt organizāciju visaptverošo kibernoturību.



2. attēls. Kiberincidentu dinamika (skaits mēnešu dalījumā)

2 **Gandrīz noticis kiberincidents** – notikums, kurš būtu varējis apdraudēt apstrādātus datus vai tīklu un informācijas sistēmu piedāvāto vai ar tīklu un informācijas sistēmu starpniecību pieejamo pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, bet kura pilnīga īstenošanās tika sekmīgi novērsta vai kurš neīstenojās.

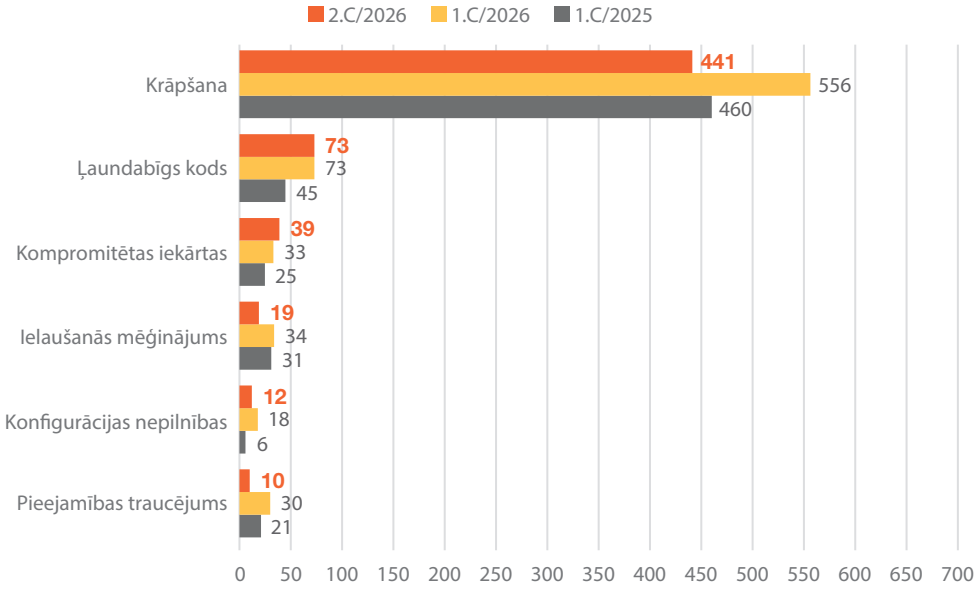
"Kiberlaikapstākļu" vērotājiem tīmekļvietnē CERT.LV sadaļā "Ziņas" pieejams ikmēneša pārskats TOP 5 kategorijās par būtiskākajiem kiberincidentiem un apdraudējumiem Latvijas kibertelpā – https://cert.lv/lv/zinas/kiberlaikapstakli.

2. Izplatītākie kiberapdraudējumi un būtiskākie notikumi pārskata periodā

Kvantitatīvi lielākie kiberincidentu veidi

Pārskata periodā vērojama pozitīva dinamika, samazinoties skaitam ierastajos incidentu veidos (krāpšana, ielaušanās mēģinājums un pieejamības traucējums), taču vienlaikus pieaug kompromitētu iekārtu īpatsvars, kā arī saglabājas būtisks ļaundabīgā koda izraisīto incidentu īpatsvars.

- **Krāpšana joprojām veido pārliecinoši lielāko daļu no visiem manuāli apstrādātajiem kiberincidentiem**, taču pārskata periodā novērojams kritums līdz **441** incidentam jeb par 21% mazāk nekā 1. ceturksnī un par 4% mazāk nekā pirms gada. Vienlaikus tas joprojām ir 6 reizes vairāk nekā jebkurš cits incidenta veids.
- **Ļaundabīga koda incidentu skaits salīdzinājumā ar 1. ceturksni nav mainījies, taču gada griezumā pieaudzis par 60%**. Ļaunatūra ir kļuvusi par stabilu uzbrukuma instrumentu. Novērojams automatizētu uzbrukumu īpatsvara pieaugums. Starp biežāk novērotajām ļaunatūrām dominēja informācijas zagšanas ļaunatūra ("ClickFix"), attālinātās piekļuves (RAT) un izspiedējvīrusu paveidi.
- **Kompromitētas iekārtas ir vienīgā incidentu kategorija, kuru skaits pārskata periodā pieauga** – par 18% salīdzinājumā ar 1. ceturksni un par 56% gada laikā. Taču šis rādītājs balstās arī uz izmantotajiem ārējiem draudu informācijas avotiem (threat intelligence feeds), tādēļ to var ietekmēt arī izmaiņas šo avotu pārklājumā vai detekcijas metodikā. Līdz ar to novērotais pieaugums ir skaidrojams ne tikai ar faktisku kompromitēto iekārtu skaita palielināšanos, bet arī ņemot vērā iespējamo datu avotu ietekmi.
- **Ielaušanās mēģinājumi samazinājušies gandrīz uz pusi**. Tas norāda uz efektīvāku uzbrukumu bloķēšanu, aktīvu DNS ugunsmūra aizsardzību un IDS/IPS darbību, kā to paredz Latvijas kiberdrošības regulējums. Tā ir pozitīva tendence, taču tā vēl nenozīmē kopēja riska samazināšanos.
- **Konfigurācijas nepilnību riski saglabājas augsti** – lai gan pret 1. ceturksni ir kritums par 33%, **gada laikā incidentu skaits ir dubultojies**. Tas joprojām norāda uz nepietiekamu konfigurācijas pārvaldību un drošības politiku neatbilstību.
- **Pieejamības traucējumu (DDoS) samazinājums** (-67% pret 1. ceturksni) **norāda uz efektīviem aizsardzības mehānismiem un labu infrastruktūras noturību**. Izmantotie vairākslāņu aizsardzības mehānismi ir ļāvuši sekmīgi mazināt DDoS uzbrukumu ietekmi, tādēļ lielākajā daļā gadījumu iedzīvotāji šos uzbrukumus ikdienā pat nepamana. Tomēr tas nemazina risku – šie uzbrukumi saglabājas kā pastāvīgs apdraudējums, īpaši pašreizējās ģeopolitiskās situācijas kontekstā.



3. attēls. TOP 6 kiberincidentu veidi (skaits)

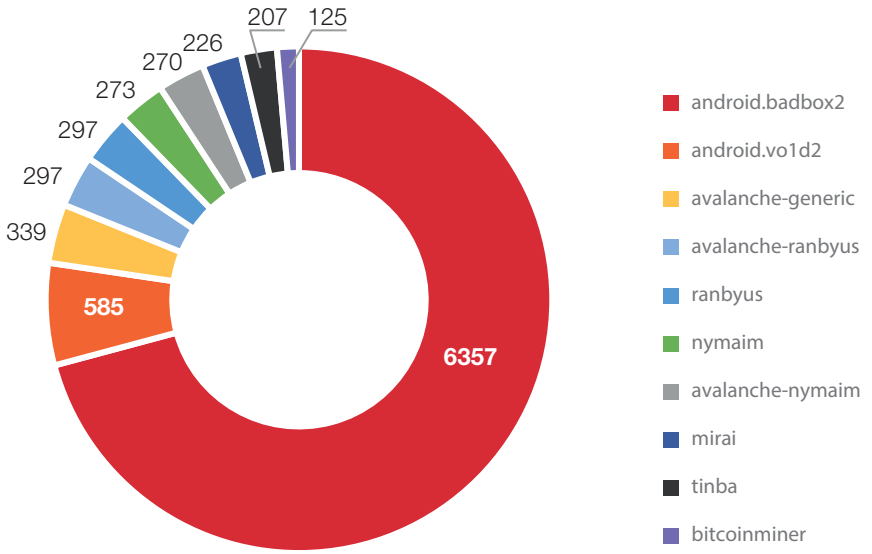
3 **IDS (Intrustion Detection System)** – ielaušanās atklāšanas sistēma;
IPS (Intrustion Prevention System) – ielaušanās novēršanas sistēma.

TOP 10 ļaunatūras

2026. gada 2. ceturksnī izplatītāko ļaunatūru tipi liecina par masveidīgiem, automatizētiem un ilgstošiem apdraudējumiem. Ļaunatūru TOP 10 augšgalā joprojām pārliecinoši dominē ļaunatūra "Android.badbox2", tās izplatība ir pieaugusi par 9% salīdzinājumā ar iepriekšējo ceturksni.

"Android.badbox2" ir mobilais botu tīkla variants, kas spēj inficēt ierīces, veicot, piemēram, piekļuves datu zagšanu un attālinātu kontroli pār 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.



4. attēls. TOP 10 ļaunatūras (skaits; 2. CET.)

Galvenās tendences kiberuzbrukumu veidos

Padziļinās ievainojamību pārvaldības nepilnības un datu noplūdes riski

Uzbrukumos organizācijām joprojām plaši tiek izmantotas jau vairākus gadus zināmas programmatūras ievainojamības, kurām ražotāji ir publicējuši ielāpus. Tas uzsver regulāras programmatūras atjaunināšanas nozīmi.

No ietekmes viedokļa būtiskākais drauds organizācijām saglabājas šifrējošā izspiedējvīrusa uzbrukumi un datu noplūdes, kuru sākotnējais posms nereti ir publiski pieejamu sistēmu ievainojamību izmantošana. To apliecina arī pārskata periodā notikušais liela mēroga kiberuzbrukums AS "Latvijas valsts meži" (LVM) IT infrastruktūrai, kur savlaicīgi nenovērsta publiski pieejamas sistēmas ievainojamība kļuva par ieejas punktu plašākam uzbrukumam.

LVM gadījums uzskatāmi parādīja, ka pat viena kritiska ievainojamība var radīt būtisku ietekmi uz organizācijas darbības nepārtrauktību, izraisot

Izplatītākie ļaunatūru tipi

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

***"Infostealer"* 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, kas pievienots pikšķerēšanas e-pasta vēstulei.**

sistēmu darbības traucējumus, datu noplūdes riskus un nepieciešamību ierobežot un apturēt kritisku IT sistēmu darbību.

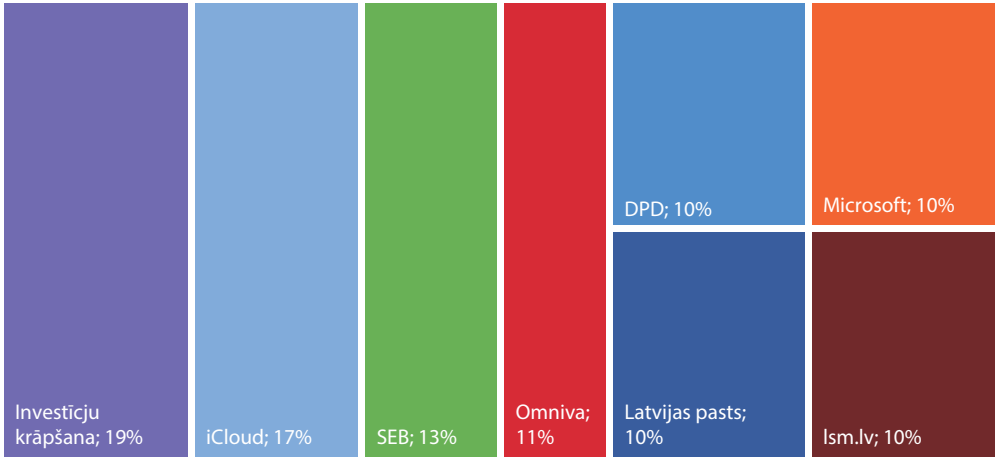
CERT.LV vietnē publicētas **rekomendācijas IT infrastruktūras kiberdrošības noturības uzlabošanai**.

Tāpat turpinās ievainojamību izmantošana, lai iegūtu neatļautu piekļuvi vietnēm un novirzītu lietotājus uz kaitīgām vietnēm vai izplatītu ļaunatūru. Pārskata periodā konstatēti vairāki .lv vietņu kompromitēšanas gadījumi, kad apmeklētāji tika pārsūtīti uz azartspēļu vietnēm vai "ClickFix" shēmām.

Kvantitatīvi lielāko daļu no identificētajām apdraudētajām iekārtām veido konfigurācijas nepilnības, kas rodas cilvēkfaktora un nepietiekamu drošības standartu dēļ.

Krāpšanas panākumus arvien vairāk nosaka spēja ietekmēt cilvēku

Krāpšanas kampaņās arvien lielāka nozīme ir sociālajai inženierijai, nevis tehnisko drošības risinājumu apiešanai. Uzbrucēji pielāgo krāpniecības shēmas aktuāliem notikumiem, populāriem pakalpojumiem un sabiedrībā zināmiem zīmoliem, savukārt mākslīgā intelekta (MI) izmantošana padara krāpnieciskos ziņojumus arvien ticamākus un grūtāk atšķiramus no īstas saziņas.



5. attēls. Izplatītāko krāpniecības kampaņu tematika (% daļa no kopējā skaita; 2026-2.CET.)

Pārskata periodā joprojām dominēja investīciju krāpšanas kampaņas, kā arī turpinās uzbrukumi, kuros tiek izmantoti gan banku, valsts iestāžu, piegādes uzņēmumu un citu uzticamu organizāciju vārdi, gan uzdošanās par autoritatīvu institūciju pārstāvjiem, lai izvilinātu maksājumu karšu datus, autentifikācijas informāciju vai panāktu, ka cietušais pats apstiprina krāpniecisku maksājumu. Vienlaikus arvien izplatītāki kļūst izsmalcināti sociālās inženierijas paņēmieni, piemēram, "ClickFix", kuros lietotājs tiek pārliecināts pats aktivizēt ļaunatūru savā ierīcē.

Draudu ietekme saglabājas augsta. Finanšu nozares asociācijas dati[4] liecina, ka 2026. gada pirmajos **sešos mēnešos Latvijas lielāko banku klientiem izkrāpti 7,83 milj. eiro**, bet novērsto krāpšanas gadījumu apmērs pārsniedza 11 miljonus eiro. Krāpnieki vidēji mēnesī izkrāpj ap 1,3 milj. eiro. Tas norāda, ka l**ietotājs joprojām ir galvenais uzbrukumu mērķis un sociālā inženierija – viens no būtiskākajiem kiberdraudiem**.

Aktivizējas krāpšanas mēģinājumi booking.com vārdā

Pieaug krāpšanas mēģinājumi booking.com vārdā, izmantojot atvaļinājumu sezonu un ceļojumu rezervāciju aktualitāti. Krāpnieki ar "WhatsApp" ziņām vai e-pastiem uzdodas par booking.com vai viesnīcu pārstāvjiem un novirza lietotājus uz viltus saitēm, lai izvilinātu maksājumu karšu datus.

Šī tendence ir īpaši bīstama, jo uzbrucēji pāriet no masveida, vispārīgām pikšķerēšanas ziņām uz personalizētākiem un ticamākiem scenārijiem. Uzbrukumi balstās uz reālām lietotāju situācijām – gaidāmiem ceļojumiem un viesnīcu rezervācijām. Krāpnieki izmanto gan steidzamības sajūtu, gan uzticamu starptautisku zīmolu. Iedzīvotājiem un organizācijām ar aktīvu ceļojumu vai komandējumu plūsmu tas var radīt finanšu zaudējumus, personas datu ļaunprātīgu izmantošanu, kā arī ceļojumu plānu traucējumu riskus.

CERT.LV vietnē apkopotas rekomendācijas, kā pasargāt sevi no krāpniekiem booking.com vārdā.

4 https://www.financelatvia.eu/wp-content/uploads/2026/07/FNA_krapsanas-dati_junijs_2026-2.png

Pieaug kontu pārņemšanas mēģinājumi saziņas lietotnēs

Pārskata periodā turpinājās mēģinājumi pārņemt iedzīvotāju "WhatsApp" un "Signal" kontus, izmantojot sociālās inženierijas paņēmienus. Uzbrucēji cenšas izvilināt autentifikācijas datus vai verifikācijas kodus, izmantojot iedzīvotāju neuzmanību un nepietiekamās zināšanas par lietotņu drošības funkcijām. Konta pārņemšana var radīt neatļautu piekļuvi privātai saziņai, veicināt krāpniecību cietušā vārdā un palielināt datu noplūdes risku.

CERT.LV vietnē apkopotas **rekomendācijas, kā stiprināt kontu drošību un mazināt riskus**.

Vēlēšanu kontekstā pieaug partiju digitālo resursu drošības riski

Tuvojoties 15. Saeimas vēlēšanām, pieaug kiberdraudu un dezinformācijas kampaņu risks pret politiskajām partijām un to digitālajiem resursiem. Digitālajā laikmetā arī politiskās partijas un tās pārstāvošās personas var kļūt par būtisku kiberuzbrukumu un dezinformācijas kampaņu mērķi, jo īpaši laikā, kad notiek gatavošanās vēlēšanām. Drošības risku mazināšanai CERT.LV ir ierosinājusi preventīvus pasākumus, nosūtot kiberdrošības atbalsta piedāvājuma vēstules visām valsts finansētajām politiskajām partijām.

Arvien vairāk pieaug mākslīgā intelekta (MI) nozīme gan uzbrukumos, gan aizsardzībā

MI arvien vairāk palielina kiberuzbrukumu mērogojamību un automatizāciju. Papildus tam drauds vairs nav tikai uzbrucējs, kas izmanto MI kā instrumentu, bet gan autonoma sistēma, kas veic pastāvīgu, adaptīvu kampaņu. Pret šādiem draudiem cilvēka reakcijas ātrums vien vairs nav pietiekams.

Tādēļ organizācijām pieaug nepieciešamība attīstīt arī MI balstītas kiberdrošības spējas. Automatizēta datu analīze un MI risinājumi ļauj ātrāk identificēt kiberapdraudējumus, analizēt lielus datu apjomus un savlaicīgi atklāt aizdomīgas aktivitātes. Arī Latvijā kiberuzbrukumu novēršanā jau tiek izmantoti automatizēti datu apstrādes un analīzes risinājumi. Kā liecina arī citu valstu pieredze, MI risinājumi ir īpaši noderīgi agrīnā risku identificēšanā un sarežģītu datu kopu padziļinātā analīzē.

Uzbrucēju motivācija

- **Finansiāli motivēti kiberuzbrucēji:** galvenie virzieni – izspiedējvīrusi, iejaukšanās biznesa sarakstē (BEC), investīciju krāpšana un datu monetizācija, lai nopelnītu naudu vai gūtu citu labumu.
- **Politiski motivēti un valstiski atbalstīti uzbrucēji** (APT jeb *Advanced Persistent Threats*): atšķirībā no finansiāli motivētiem uzbrucējiem, APT grupējumu mērķis nav ātrs ieguvums, bet gan ilgstoša un nepamanīta piekļuve valsts iestāžu, kritiskās infrastruktūras (KI) un citu stratēģiski nozīmīgu organizāciju sistēmām, lai iegūtu informāciju un sensitīvus datus. Tāpat **Latvijā pastāv paaugstināts risks saskarties ar APT informatīvās ietekmes operācijām pirms 2026. gada 15. Saeimas vēlēšanām**.
- Destruktīvi uzbrukumi, kuru mērķis nav tiešs finansiāls ieguvums, bet gan pakalpojuma pieejamības traucēšana vai sabotāža, izmantojot kiberuzbrukumu sava reitinga celšanai. Tie var izpausties kā DDoS uzbrukumi, mēģinājumi iegūt kontroli pār KI sistēmām vai citi uzbrukumi, kuru mērķis ir ietekmēt būtisku pakalpojumu nepārtrauktību, radīt sabiedrībā nedrošības sajūtu un vājināt uzticību valsts digitālajiem pakalpojumiem.

Reģionālais draudu konteksts

- **Krievija** saglabājas kā primārais kiberdraudu avots. Sagaidāms, ka Krievijas haktīvistu aktivitāte (bieži saistīta un novērota pēc publiskas atbalsta paušanas Ukrainai Latvijas mediju telpā) turpināsies arī turpmāk. Ietekme no šiem uzbrukumiem vēl joprojām vērtējama kā zema. Galvenie riski ir saistīti ar valsts iestāžu reputācijas graušanu, sabiedrības un informācijas telpas ietekmēšanu. Uzbrukuma rezultātā var tikt traucēta mērķa vietnes darbība un pakalpojuma pieejamība.

- Ar **Ķīnu** (ĶTR) saistītu grupējumu aktivitāte ar ekonomisku motivāciju (datu ieguve, piekļuve tehnoloģijām); jūtami intensīvāki mēģinājumi izplatīties tīklos un piekļūt sensitīvai informācijai.
- Epizodiska **Baltkrievijas** iesaiste, galvenokārt kā daļa no Krievijas "orķestrētām" hibrīdoperācijām.

Mērķētās nozares

CERT.LV regulāri identificē uzbrukumu mēģinājumus pret valsts un pašvaldību iestādēm, finanšu sektoru, veselības aprūpi, telekomunikāciju uzņēmumiem, izglītības iestādēm un kritisko infrastruktūru (KI).

Pieaug apdraudējumu risks operacionālajām tehnoloģijām (OT), kuras tiek izmantotas fizisku procesu, iekārtu un infrastruktūras monitorēšanai un kontrolei, nodrošinot sabiedrībai būtiskus pakalpojumus.

Tāpat Krievijas atbalstītie haktīvistu grupējumi turpina viļņveidīgi veikt DDoS uzbrukumus pret Latvijas valsts iestādēm un KI pakalpojumu sniedzējiem. Lai gan šie uzbrukumi nav radījuši ilgstošus pakalpojumu pārtraukumus, tie apliecina pastāvīgu interesi par Latvijas stratēģiski nozīmīgajiem sektoriem.

Galvenie secinājumi un rekomendācijas

- Kibertelpas drošības apdraudējums Latvijā saglabājas augsts, un ilgtermiņa tendence joprojām ir augšupejoša. To nosaka ģeopolitiskā situācija, arvien plašāka ievainojamību un mākslīgā intelekta izmantošana kiberuzbrukumos un lietotāju nekritiska paļaušanās uz digitālajiem rīkiem. Šie faktori prasa turpināt sistemātisku kiberrisku pārvaldību un konsekventi stiprināt organizāciju visaptverošo kibernoturību.
- Visbiežāk kiberuzbrukumi notiek, izmantojot ievainojamības publiskā tīklā pieejamās informācijas sistēmās vai ar pikšķerēšanas uzbrukumu starpniecību, kas vērsti pret korporatīvā tīkla lietotājiem. Katrai organizācijai ir rūpīgi un atbildīgi jāpārzina sava infrastruktūra, savlaicīgi ieviešot atjauninājumus un drošības ielāpus, tā stiprinot sistēmu noturību un nodrošinot nepārtrauktu darbību.
- Pieaugoši riski ir uzticības ļaunprātīga izmantošana un identitātes kompromitēšana, savukārt informācijas zagšanas ļaunatūra tiek aktīvi izmantota kontu kompromitēšanai un turpmākiem kiberuzbrukumiem.
- DDoS uzbrukumi saglabājas kā efektīvs ģeopolitiska spiediena instruments un pastāvīgs apdraudējums.
- Krāpšana joprojām ir kvantitatīvi dominējošais kiberincidentu veids Latvijā, kas visvairāk skar iedzīvotājus. Arī Finanšu nozares asociācijas apkopotie šī gada pirmo sešu mēnešu dati rāda, ka vidēji mēnesī tiek izkrāpti ap 1,3 milj. eiro. Tādēļ līdztekus tehniskajiem drošības pasākumiem būtiski turpināt stiprināt sabiedrības informētību un noturību pret sociālās inženierijas uzbrukumiem, īpaši pikšķerēšanu.
- Organizācijām prioritāri jāstiprina nepārtraukta kiberdrošības uzraudzība (SOC/EDR/XDR/SIEM), ievainojamību pārvaldība, daudzfaktoru autentifikācijas izmantošana, rezerves kopiju pārvaldība, piegādes ķēžu drošība un lietotāju apmācība, regulāri testējot incidentu reaģēšanas un darbības nepārtrauktības plānus.

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

3.1. DNS ugunsmūris

Latvijā regulāri notiek kampaņveidīgas krāpnieciskas aktivitātes – gan novirzīšana uz viltus vietnēm bankas, e-pasta vai sociālo tīklu kontu piekļuves datu izkrāpšanai, gan ļaunatūru izplatīšana kibertelpā.

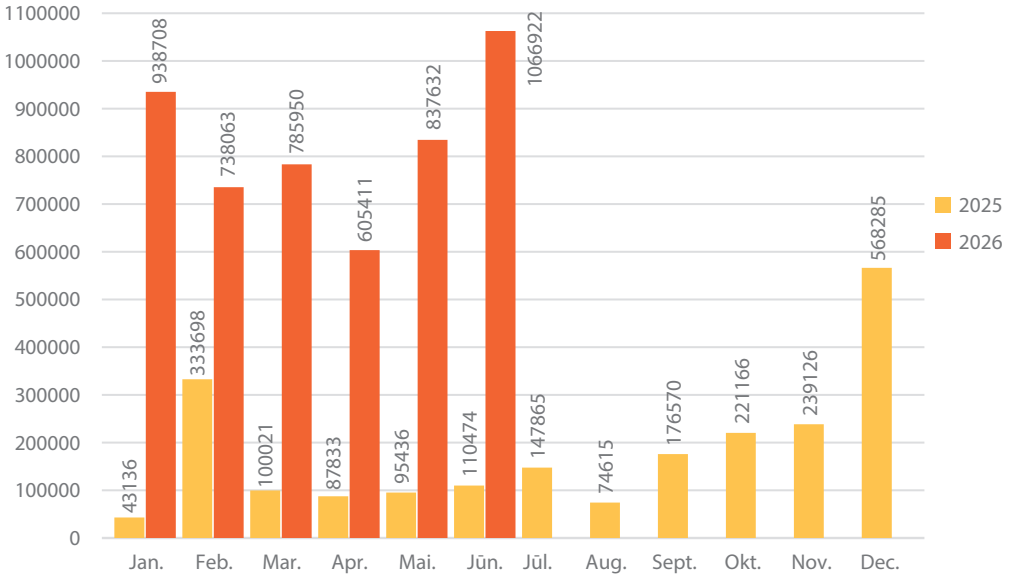
CERT.LV proaktīvi monitorē un aptur identificētās krāpnieciskās kampaņas, operatīvi ievietojot kampaņu indikatorus DNS ugunsmūrī. DNS ugunsmūra mobilā lietotne pasargā ne tikai no krāpnieciskām kampaņām kibertelpā, bet arī identificētiem viltvāržu zvaniem.

2026. gada 2. ceturksnī CERT.LV DNS ugunsmūris, izmantojot tā uzturētos sarakstus, novērsa vairāk nekā 2,5 milj. piekļuves mēģinājumu ļaunprātīgām vietnēm – tas ir par 2% vairāk nekā iepriekšējā ceturksnī un par 754% vairāk nekā attiecīgajā periodā pērn (statistikā nav iekļauti dati par citu valsts kompetento iestāžu sarakstiem nelikumīga tiešsaistes satura ierobežošanai).

Šā gada pirmajos sešos mēnešos CERT.LV DNS ugunsmūris ir novērsis vairāk nekā 5 milj. piekļuves mēģinājumu ļaunprātīgām vietnēm, kas ir 6,5 reizes vairāk nekā attiecīgajā periodā pērn. Savukārt jūnijā tika sasniegts rekordaugsts skaits – aptuveni 1,1 milj.

2026. gadā gandrīz visi mēneši saglabā ļoti augstu aktivitāti. Bloķēto pieprasījumu apjoms vidēji mēnesī sasniedz 830 tūkst. – tas liecina par krāpšanas kampaņu noturīgu aktivitāti, ko CERT.LV DNS ugunsmūris ir preventīvi identificējis un novērsis.

~2,5 milj. – novērstie lietotāju piekļuves mēģinājumi ļaunprātīgām vietnēm 2. cet.
~30 min. – vidējais reakcijas laiks līdz identificēšanai un indikatora ievietošanai DNS ugunsmūrī
~88 tūkst. – DNS ugunsmūra mobilā lietotne lejupielādēta Android un IOS ierīcēs (kopš 2024. gada)
~5,2 milj. – kaitīgo domēna vārdu DNS pieprasījumu skaits 2. cet.



6. attēls. CERT.LV DNS ugunsmūra sarakstu* novērstie lietotāju pieprasījumi uz ļaunprātīgām vietnēm (cert-shield, malware, phishing, high-risk*)**

Nozīmīgākās aktīvās aizsardzības epizodes pārskata periodā:

- apturēti pieprasījumi uz attālinātās piekļuves ļaunprogrammatūras (RAT) izmantotu komandu-kontroles serveri (C&C);
- apturēta "LSM" tēla izmantošana krāpniecisku kriptovalūtu investīciju platformu reklamēšanas kampaņās;
- bloķētas viltus tiešsaistes kazino vietnes.

Kopumā secināms - draudi kļūst pastāvīgi, nevis sezonāli. Lielākā daļa šo draudu ir vērsti uz cilvēku kā primāro uzbrukuma mērķi. Bez CERT.LV DNS ugunsmūra aktīvās aizsardzības ievērojama daļa lietotāju nonāktu pikšķerēšanas lapās, ļaunatūru lejupielādes vietnēs un krāpnieciskās platformās. CERT.LV DNS ugunsmūris pasargā lietotājus no identificēto viltus vietņu apmeklēšanas, tos pārvirzot uz drošu brīdinājuma vietni, kurā lietotājs saņem paskaidrojumu par novērsto apdraudējumu.

3.2. Apdraudējumu agrās brīdināšanas sistēma (ABS)

Kiberdrošības apdraudējumu agrās brīdināšanas sistēma (ABS) ir CERT.LV nodrošināts pakalpojums datu plūsmas anomāliju analīzei un kiberuzbrukumu pazīmju identificēšanai pakalpojuma saņēmēja infrastruktūrā. CERT.LV turpina ABS sistēmas uzturēšanu un paplašināšanu.

ABS pakalpojums ietver nepārtrauktu datu plūsmas anomāliju analīzi un ļaunprogrammatūras aktivitāšu atpazīšanu, brīdinājumu nosūtīšanu pakalpojumu saņēmējam par konstatētajiem augstas prioritātes kiberapdraudējumiem, regulāru CERT.LV aktuālo kiberapdraudējumu indikatoru atjaunošanu, kā arī pakalpojuma saņēmēju konsultēšanu un atbalstu.

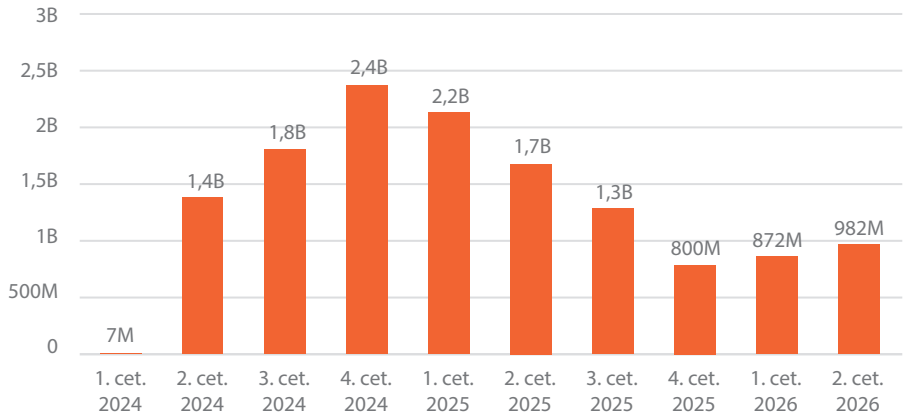
Kiberapdraudējumu un kiberincidentu atklāšana un novēršana

2026. gada 2. ceturksnī ABS reģistrēto trauksmju skaits bija aptuveni 982 miljoni, kas ir par 13% vairāk nekā 1. ceturksnī. Turklāt pieaugums novērots jau kopš 2026. gada sākuma. Tas norāda uz pieaugošu kiberapdraudējumu intensitāti un jaunu ievainojamību parādīšanos - pēc publiski zināmu ievainojamību izziņošanas uzbrucēji nereti masveidā sāk skenēt sistēmas un mēģina tās izmantot. CERT.LV norāda, ka potenciāli jebkura nedroši pārvaldīta iekārta, kas ir eksponēta internetā, ir pakļauta uzbrukuma riskam.

Aktuālākie apdraudējumi pārskata periodā:

- tīkla pieprasījumi uz ļaunatūru (tostarp arī "ClickFix") izplatošiem domēniem;
- tīkla pieprasījumi uz domēniem, kas saistīti ar identificētām pikšķerēšanas un krāpniecības kampaņām;
- pieprasījumi uz domēniem, kas izplata viltus programmatūru, atdarinot uzticamu rīku nosaukumus.

Nozīmīga ir arī iedzīvotāju iesaiste, kuri pārsūta krāpnieciskos e-pastus, īsziņas un tīmekļa vietņu saites uz cert@cert.lv vai ziņo pa tālruni 23230444 (WhatsApp). Saņemtie ziņojumi tiek apkopoti, un kaitnieciskie domēna vārdi ievietoti DNS ugunsmūrī, lai aizsargātu Latvijas interneta lietotājus. dnsmuris.lv un tā mobilā lietotne bez maksas pieejama ikvienam Latvijas iedzīvotājam un organizācijai.



7. attēls. ABS reģistrēto trauksmju dinamika pa ceturkšņiem (skaits milj. - miljrd.; 2024-2026)

3.3. Drošības operāciju centrs (SOC)

SOC pakalpojuma ieviešana

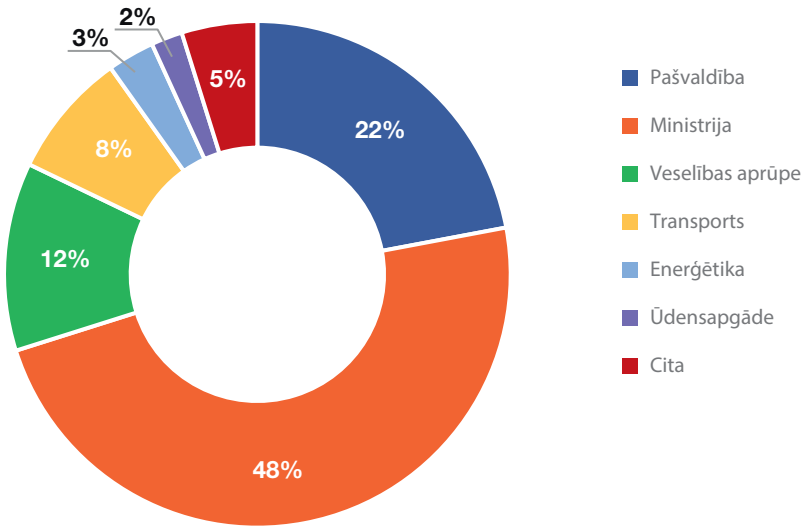
Turpinās CERT.LV SOC pakalpojuma attīstīšana un jaunu klientu piesaiste, paplašinot klientu loku atbilstoši NKDL un sekmējot efektīvāku aizsardzību un noturību pret kiberapdraudējumiem.

SOC centralizēti apkopo drošības telemetriju no klienta infrastruktūras, nosaka notikumu savstarpējās sakarības un sasaista tos ar visu CERT.LV pieejamo apdraudējumu indikatoru un zināšanu kopu. Būtisku pievienoto vērtību sniedz SOC

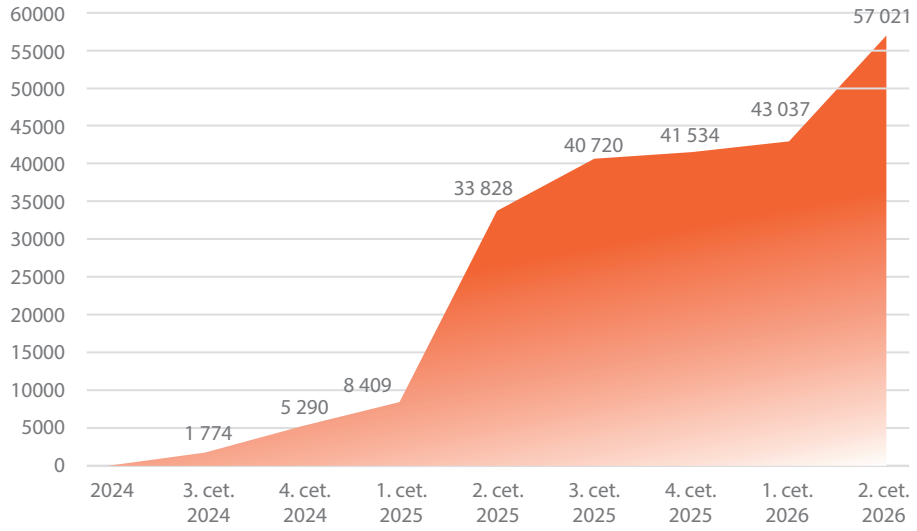
analītiķu komanda, kas, izmantojot īpašu programmnodrošinājumu un pieejamos datus, savlaicīgi novērš kaitējumu – identificē, brīdina un aptur apdraudējumu vai kiberincidentu.

Uz pārskata perioda beigām SOC klientu skaits sasniedza kopumā **105** (2. cet. skaits pieauga par **13**). Dažādu nozaru iestādes un organizācijas, kas nodrošina būtiskus un svarīgus pakalpojumus, izmanto CERT.LV SOC risinājumus. Salīdzinot ar citiem sektoriem, vairāk pārstāvētās ir ministrijas un to padotības iestādes, pašvaldības un veselības aprūpes iestādes.

Kopumā nodrošināta **57 021** gala iekārtas, tostarp serveru un darbstaciju, pārskatāmība. 2026. gada 2. cet. pieaugums veido **32%** no kopējā apjoma. Paplašinoties uzraudzības tvērumam, pieaug arī analizējamo drošības notikumu un ģenerēto trauksmju skaits.



8. attēls. Sadalījums pa iestāžu sektoriem, kas izmanto CERT.LV SOC (%, dati uz 30.06.2026)



9. attēls. CERT.LV SOC redzamības dinamika: gala iekārtu skaits (2024-2026)

Incidenti un drošības trauksmes: draudu atklāšana un novēršana

Rādītāji	Skaits	Izmaiņas % pret 2026. gada 1. cet.
CERT.LV SOC pakalpojuma ietvarā kopumā reģistrēto drošības trauksmju skaits 2026.gada 2.cet.:	~25 milj.	+4%
Zema līmeņa trauksmju skaits	~6 milj.	+0,72%
Vidēja līmeņa trauksmju skaits	~18 milj.	-1,48%
Augsta līmeņa trauksmju skaits	~16 tūkst.	+47%
Kritisko trauksmju skaits	~35 tūkst.	+116%
Manuāli izveidoto lietu skaits	617	+5,3%
Viltus pozitīvo lietu skaits	599	+5%
Kiberincidentu skaits	19	+27%

Pārskata periodā **reģistrēti aptuveni 25 milj. drošības trauksmes ziņojumu**, kas ir **par 4% vairāk** nekā 2026. gada 1. ceturksnī. Drošības trauksmju skaita pieaugums primāri atspoguļo SOC uzraudzībā esošo gala iekārtu skaita paplašināšanos un uzlabotu spēju identificēt potenciālos apdraudējumus. Vienlaikus tas liecina par pieaugošu uzbrukumu aktivitāti kibertelpā.

Augsta līmeņa trauksmes pieaugušas par 47%, bet kritiskās – par 116%. Tas liecina par būtisku tieši nopietnāko incidentu īpatsvara pieaugumu. Lai gan kritisko trauksmju skaits vairāk nekā dubultojies, kiberincidentu skaits pieaudzis par 27%, kas liecina, ka SOC spēj efektīvi identificēt un ierobežot apdraudējumus pirms to eskalācijas.

SOC pakalpojumā novērots arī liels viltus trauksmju skaits (pieaugums +5%).

Viltus trauksmju biežākie iemesli, kas novēroti klientu infrastruktūrā:

- nepilnīga vai novecojusi IKT resursu uzskaite (trūkst centralizētas pārvaldības iestāžu / novada mērogā);
- gala iekārtu konfigurācija nav standartizēta;
- nav ieviests atļauto programmatūru saraksts ar kontroles režīmu;
- netiek pārvaldīti un kontrolēti tīmekļa pārlūku spraudņi un paplašinājumi;
- vairāku attālinātās piekļuves rīku (piemēram, “AnyDesk”, “Teamviewer”, t.sk. ar novecojušām versijām) nepamatota izmantošana lietotāju atbalstam;
- nav ieslēgta žurnālierakstu veidošana, trūkst dokumentācijas un procedūru;
- netiek uzraudzīta USB zibatmiņu lietošana un no tām izpildīto failu kontrole.

Viltus trauksmes nozīmē lielāku mazefektīva darba apjomu SOC analītiķiem notikumu pārbaudē, radot risku palaist garām īstu uzbrukumu starp “viltus pozitīvajiem”.

Lai efektīvi pamanītu incidentus un apdraudējumus, nepieciešams mazināt trauksmju paziņojumu fona troksni.

Biežāk sastopamā aina kompromitētā vidē:

- **nav ieviests mazāko nepieciešamo privilēģiju princips**, tādējādi ļaujot uzbrucējam ātri paplašināt piekļuves tiesības un pārvietoties infrastruktūrā;
- **trūkst tīkla segmentācijas**, tādēļ kompromitēšana vienā tikla daļā bieži rada iespēju netraucēti izplatīties uz citām sistēmām;
- **nav ieviesti programmatūras izpildes ierobežojumi**, kas ļauj bez būtiskiem šķēršļiem izpildīt ļaunprātīgu kodu un neautorizētas lietojumprogrammas;
- **nav nodrošināta vienota IT vides pārvaldība un centralizēta drošības telemetrija**, kas apgrūtina savlaicīgu apdraudējumu atklāšanu, korelāciju un efektīvu reaģēšanu uz incidentiem;
- **pastāv attālinātās pārvaldības vadības rīku nekontrolēta izmantošana**, kur dažādi administrēšanas risinājumi tiek lietoti bez centralizētas pārvaldības, uzraudzības un drošības politikas, būtiski palielinot uzbrukuma laukumu un apgrūtinot nesankcionētas piekļuves identificēšanu.

SOC pakalpojuma ietvaros izveidotās lietas un fiksētie kiberincidenti

2026. gada 2. ceturksnī tika **manuāli izveidotas 617 lietas** (par 5.3% vairāk nekā 2026. gada 1. cet.), savukārt **viltus pozitīvās lietas bija 599** (par 5% vairāk nekā 2026. gada 1. cet.).

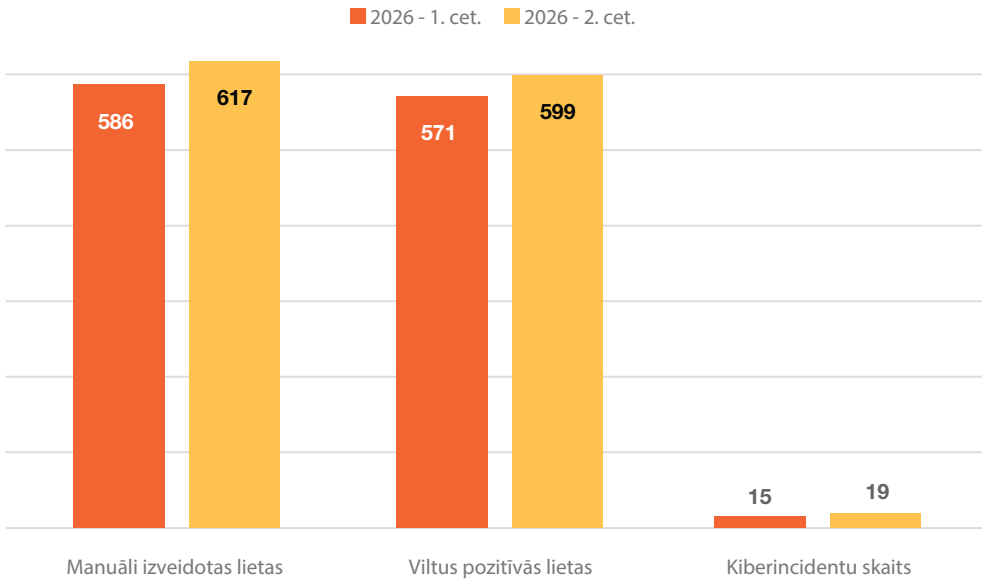
SOC ietvaros tika fiksēti 19 kiberincidenti (par 3% vairāk nekā 2026. gada 1. cet.) 16 dažādās iestādēs.

CERT.LV SOC pakalpojumu ietvarā 2026. gada 2. ceturksnī:

617 (+5.3%) – Manuāli izveidotas lietas

599 (+5%) – Viltus pozitīvās lietas

19 (+27%) – Fiksētie incidenti 16 iestādēs



10. attēls. SOC: Drošības notikumu struktūra un skaita salīdzinājums

Pārskata periodā fiksēto kiberincidentu apskats

Plašākais kiberincidents saistīts ar kādu kompromitētu tīmekļa vietni, kuru apmeklēja lietotāji no trim iestādēm, apdraudot vai inficējot ar ļaunatūru gala iekārtas. Tika novērsta **ievainojamība kompromitētajā tīmekļa vietnē**, kā arī novērsta infekcija skartajās gala iekārtās.

Lielāko trauksmju skaitu SOC pakalpojumā rada **nekontrolēta nevēlama programmatūra** – no tīmekļa lejupielādēti un aktivizēti izpildāmie faili, piemēram, spēles nereti tiek lejupielādētas kopā ar ļaunatūru. Vairākkārt konstatēta nevēlama programmatūra, kam bijusi ietekme uz gala iekārtu, un trauksmes reģistrētas kā kiberincidenti.

Pārskata periodā fiksēti vairāki kiberincidenti, kuros sākotnējā piekļuve notiksi caur **pikšķerēšanas e-pastiem, inficētiem e-pastu pielikumiem, pārlūku spraudņiem vai viltus "CAPTCHA", un tie visi**, tāpat kā iepriekšējos periodos, turpina radīt apdraudējumu.

Konstatēts kiberincidents uz tīmekļa vietnes servera. Tā **kompromitēšana notika, izmantojot ievainojamu satura vadības sistēmas komponenti**.

Turpinās **netīša gala iekārtu eksponēšana internetā** bez lokālas aizsardzības (lokālā ugunsmūra) un aktuāli paroļu pārlases uzbrukumi (*brute-force*) uz šīm gala iekārtām.

Fiksētie incidenti galvenokārt saistīti ar lietotāju rīcību un vāju drošības praksi, savukārt būtiskākie riski ir cilvēkfaktors un nepietiekama piekļuves kontrole. Tas norāda uz nepieciešamību prioritizēt lietotāju apmācību, piekļuves kontroli un gala iekārtu drošību kā būtiskus aizsardzības virzienus.

Dominējošie sākotnējās piekļuves vektori:

- **pikšķerēšana un ļaunprātīgi e-pastu pielikumi;**
- **pārlūku spraudņi;**
- **viltus "CAPTCHA";**
- **nevēlama programmatūra – no tīmekļa lejupielādēti un aktivizēti izpildāmie faili;**
- **ievainojama tīmekļvietnes vadības sistēma;**
- **zibatmiņas, aktivizēti izpildāmie faili.**

3.4. IT sistēmu drošības testi un pikšķerēšanas uzbrukumu simulācijas kampaņas

Pikšķerēšanas uzbrukumu simulācijas kampaņas

2026. gada 2. ceturksnī veiktas **3 pikšķerēšanas uzbrukumu simulācijas kampaņas** trijās iestādēs. Šo kampaņu ietvarā tika nosūtītas **829 e-pasta vēstules**. Vairāk nekā puse jeb **67 % lietotāju atvēra saiti e-pastā**, un no tiem **24% ievadīja lietotāja datus**.

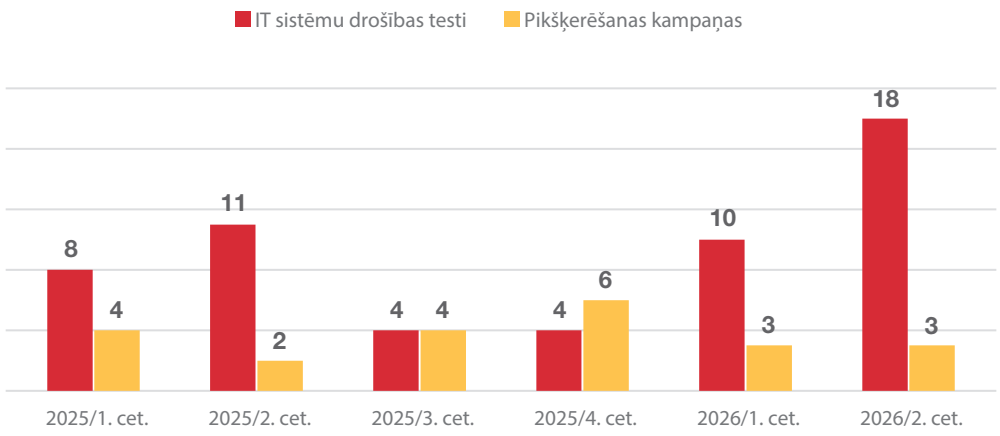
Pikšķerēšanas uzbrukumu simulācijas kampaņas mērķis ir apmācīt un veicināt organizāciju darbinieku spējas identificēt potenciāli riskantus uzvedības modeļus, atpazīt un novērst kiberapdraudējumus un informācijas noplūdi. Tas palīdz būtiski stiprināt organizāciju aizsardzību pret sociālās inženierijas uzbrukumiem, tādā veidā mazinot cilvēciskā faktora riskus.

IT sistēmu drošības testi

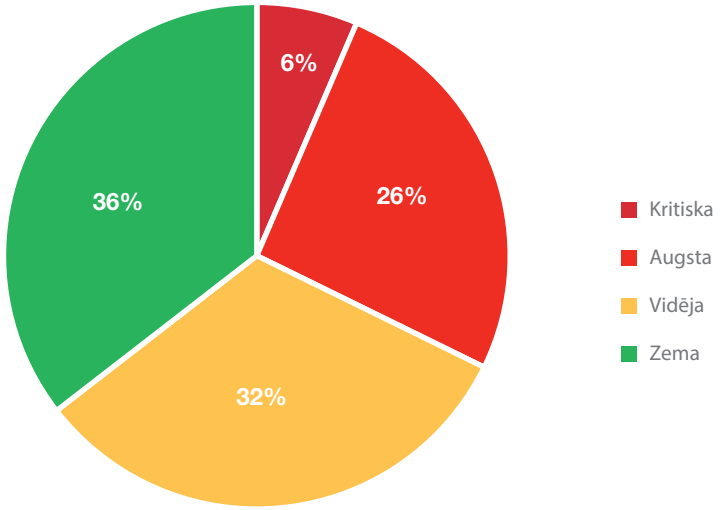
Drošības testu mērķis ir identificēt potenciālas ievainojamības, drošības apdraudējumus un sistēmas nepilnības, lai novērstu iespējamos kiberuzbrukumus un datu noplūdes.

Pārskata periodā CERT.LV veica **18 IT sistēmu drošības testus** (par 8 vairāk nekā 1. cet.). Testu gaitā tika **identificēta 31 ievainojamība**, tostarp kritiskas un augstas ietekmes, kas tika novērstas pirms to iespējamās izmantošanas kiberuzbrukumos.

Veicot IT sistēmu drošības testu, CERT.LV nodrošina tīkla drošības analīzi, programmatūras ievainojamību novērtējumu, *web* lietotņu drošības novērtējumu, IT infrastruktūras ievainojamību novērtēšanu, kā arī konsultācijas un ieteikumus par drošības uzlabošanu.



11. attēls. IT sistēmu testi un pikšķerēšanas uzbrukumu simulācijas kampaņas (skaits)



12. attēls. 2. cet. IT sistēmu testos atklāto ievainojamību potenciālā ietekme (% daļa no kopējā skaita - 31)

3.5. Kiberdrošības draudu medību operācijas

Kiberdrošības draudu medības ir proaktīvs process, kura laikā CERT.LV kiberdrošības eksperti meklē iespējamu apdraudējumu vai nesankcionētu darbību pazīmes Latvijas IKT sistēmās, lai identificētu riskus un savlaicīgi novērstu potenciālos apdraudējumus. Kopš 2022. gada, kad CERT.LV uzsāka kiberdrošības draudu medības, kopumā draudu analīze ir veikta vairāk nekā 40 NKDL subjektu un IKT kritiskās infrastruktūras organizāciju infrastruktūrā.

Pārskata periodā, analizējot gala iekārtas, konstatēti vairāki drošības nepilnību aspekti, tostarp nedroša programmatūru un iekārtu konfigurācija, kā arī novecojušu, drošības ievainojamībām pakļautu komponentu izmantošana, kas palielina potenciālo kiberincidentu risku.

Astotās Draudu medības ar paplašinātu klātbūtni apliecina operacionālo briedumu

2026. gada maijā CERT.LV noslēdza astoto trīs nedēļu Draudu medību operāciju ar paplašinātu klātbūtni sadarbībā ar Kanādas Bruņoto spēku Kiberpavēlniecību un sabiedrotajiem no Īrijas, Norvēģijas, Polijas un Apvienotās Karalistes. Operācijā piedalījās 30 tehniskie eksperti, stiprinot Latvijas valsts un publisko institūciju digitālās infrastruktūras drošību.

Operācija apliecināja Latvijas draudu medību pieejas augošo briedumu un nostiprināja to kā starptautiski atzītu sadarbības modeli, kurā apvienotas civilās un militārās spējas. Tās galvenā nozīme ir savlaicīga apdraudējumu pazīmju identificēšana, kiberdrošības noturības stiprināšana un Latvijas lomas nostiprināšana praktiskas draudu medību metodikas attīstībā. Būtiskākais secinājums – jāturpina ieguldīt draudu medību kapacitātē, institūciju tehniskajā gatavībā, kopīgā metodikā un sadarbībā ar sabiedrotajiem.

"Šī operācija deva starptautiskajiem partneriem iespēju iepazīt mūsu draudu medību metodiku un pēc nepieciešamības pielietot to savām vajadzībām. Tā vienlaikus stiprināja starpvalstu sadarbību, veicinot koordinētu rīcību, pieredzes apmaiņu un savstarpēju atbalstu kiberdraudu situācijā," norāda CERT.LV vadītājas vietnieks Varis Teivāns.

3.6. Koordinētas ievainojamību ziņošanas platforma (CVD)

CERT.LV koordinētas ievainojamību ziņošanas platforma CVD paredzēta, lai atvieglotu valsts pārvaldes un pašvaldību iestāžu sadarbību ar kiberdrošības pētniekiem un uzlabotu IKT resursu drošību.

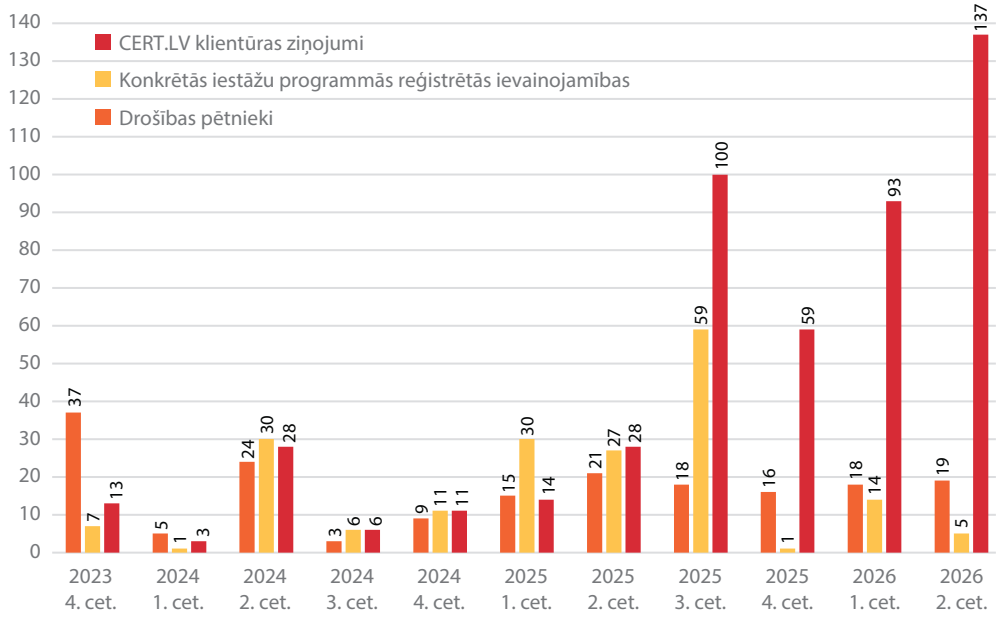
CVD platformā iestāde var reģistrēt informāciju par visiem tās izmantotajiem IKT resursiem, par kuriem tā vēlas saņemt ziņojumus par atklātajām ievainojamībām. Platforma nodrošina pārredzamu un ērtu saskarni, kurā iespējams apskatīt visus saņemtos ziņojumus, kā arī uzturēt saziņu ar pētniekiem un citām iesaistītajām pusēm. Atbildīga ziņošana palīdz novērst ievainojamības pirms to ļaunprātīgas izmantošanas, samazinot riskus gan organizācijām, gan lietotājiem.

CVD platformā 2026. gada 2. ceturkšņa beigās kopumā reģistrēti:

- **185 drošības pētnieki** (2. cet. skaits pieauga par 19)
- **18 aktīvas iestāžu programmas** (nākušas klāt 4);
- **683 ievainojamību ziņojumi** (2. cet. skaits pieauga par 142), tostarp:
  - ✓ CERT.LV klientūras ievainojamības – **492** (2. cet. skaits pieauga par 137);
  - ✓ konkrētās iestāžu programmās reģistrētās ievainojamības – **191** (2. cet. skaits pieauga par 5).

Aktīvās iestāžu programmas skatīt vietnē: **cvd.cert.lv**.

Ārējā tīklā eksponēto resursu ievainojamību testēšanai CERT.LV aicina organizācijas izveidot un pārvaldīt savas organizācijas programmu platformā cvd.cert.lv, kā arī aicina drošības pētniekus izmantot CVD platformu, lai drošā un koordinētā veidā ziņotu par atklātām ievainojamībām valsts pārvaldes iestāžu un Latvijā reģistrētu uzņēmumu resursos, tā veicinot ātrāku to novēršanu.



13. attēls. CVD: Drošības pētnieku un ievainojamību ziņojumu skaits

3.7. Operacionālo tehnoloģiju (OT) drošība

Aktivitātes

CERT.LV ir izveidojusi sadarbību ar Latvijas enerģētikas, ūdensapgādes, siltumapgādes un transporta sektora operatoriem un noslēgusi operacionālo tehnoloģiju (OT) drošības pakalpojumu līgumus. OT sistēmu drošības veicināšana notiek trijos galvenajos virzienos: **sistēmu uzraudzība un anomāliju identifikācija, drošības testu veikšana un incidentu risināšana.**

- **Sistēmu uzraudzības ietvaros** CERT.LV ir uzstādījusi piecus OT tīkla datu plūsmas uzraudzības sensorus, kā arī notiek aktīvi sagatavošanās darbi sensoru tīkla paplašināšanā. Paralēli iekšējo OT tīklu komunikāciju monitorēšanai, tiek veiktas darbības nepārtrauktai Latvijas IP adresācijas tīklu uzraudzībai ar mērķi identificēt publiski eksponētas sistēmas, apzināt to iespējamās ievainojamības un veikt to koordinētu piekļuves ierobežošanu un nepilnību novēršanu.
- **OT sistēmu komponenšu drošības testu ietvaros** tiek realizētas darbības dažādu viedo un industriālās vadības ierīču drošības pārbaudēs, lai atklātu potenciālas ievainojamības vai piegādes ķēžu nepilnības, kuras var pieļaut šo iekārtu un kopējo sistēmu nesankcionētu vadību no ražotāju vai ārējo uzbrucēju puses. Sākotnējās pārbaudes tiek veiktas iekārtām, kuru izcelsmes valsts ir Ķīna. Pēdējā gada laikā šīs iekārtas sevī iekļauj attālināti vadāmās viedās ierīces (piemēram, viedie skaitītāji un mobilo sakaru modemi) un elektroauto uzlādes stacijas.
- **Nodibināta plašāka sadarbība** ar Ziemeļvalstu un Baltijas valstu (NB8) kiberdrošības iestādēm.

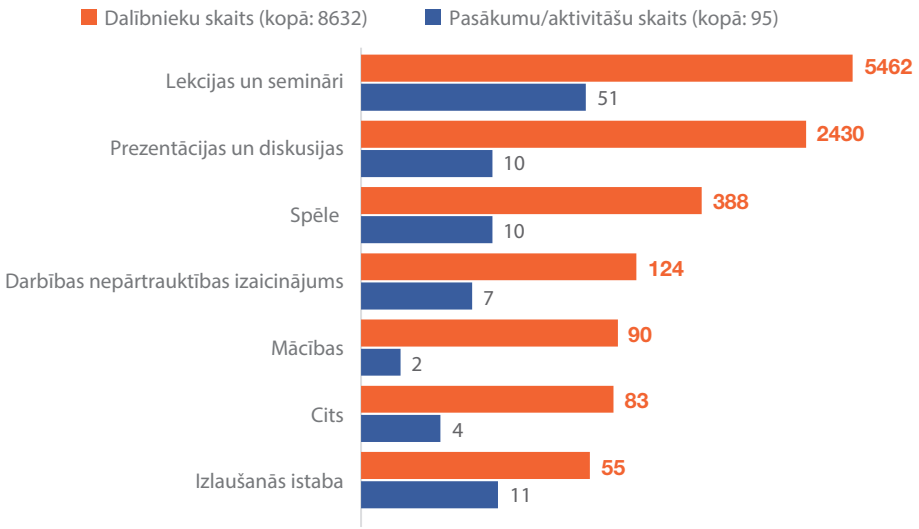
Apdraudējumi, incidenti, ietekme

Tiek veikta iespējamo risku un ievainojamību savlaicīga identificēšana, proaktīva rīcība un to ietekmes mazināšana. **Kopējā situācija Latvijas operacionālo tehnoloģiju un to sistēmu noturībā pret kiberuzbrukumiem ir vērtējama kā apmierinoša, saglabājoties nemainīgai pilnveides tendencei.** Veikto regulāro aktivitāšu rezultātā tiek identificētas privātās vai maza izmēra OT sistēmas, kuras ir pieejamas no interneta vides un tiek veikta šo operatoru informēšana un sadarbības veidošana, lai mazinātu vai novērstu iespējamo ietekmi.

Arī turpmāk sagaidāms nepārtraukts apdraudējums no Latvijai nedraudzīgo valstu puses ar mērķi iegūt kontroli un veikt destruktīvas darbības kritiskās infrastruktūras operatoru sistēmās. Lai mazinātu šādas ietekmes iespējas un padarītu Latviju par grūtāku mērķi, CERT.LV turpinās darbu pie OT aktivitāšu virzieniem, nodrošinot plašāku redzamību un draudu identifikāciju, drošības testu izpildi un koordinētu reaģēšanu uz incidentiem.

4. Kiberdrošības stiprināšana ar visu sabiedrību aptverošiem pasākumiem

Turpinot pilnveidot individuālu lietotāju un organizāciju zināšanas un prasmes kiberdrošības jomā, CERT.LV eksperti 2026. gada 2. ceturksnī **95** pasākumu ietvaros sasniedza kopumā **8 632** cilvēku lielu mērķauditoriju. Tas ir par 34% vairāk pasākumu un par 19% vairāk dalībnieku nekā attiecīgajā periodā pērn.



14. attēls. Izglītojošās metodes veids vs sasniegtā auditorija (skaits; 2026-2.cet.)

CERT.LV piedāvā pilnveidot savas kiberdrošības zināšanas jebkurā laikā, izmantojot Kibertests.lv. Tā ir bezmaksas platforma, kur dažu minūšu laikā iespējams pārbaudīt savas zināšanas par biežākajiem kiberdrošības riskiem un saņemt praktiskus ieteikumus, kā ikdienā rīkoties drošāk.

Kibertests.lv ir piemērots gan privātpersonām, gan organizācijām. Privātpersonas testus var pildīt anonīmi un uzreiz saņemt rezultātus, savukārt uzņēmumi var novērtēt darbinieku zināšanu līmeni un iegūt apkopotus rezultātus, kas palīdz plānot mērķtiecīgas kiberdrošības apmācības.

Plašāku informāciju par CERT.LV piedāvātajām lekcijām, mācību spēlēm un izglītojošiem pasākumiem skatīt CERT.LV tīmekļvietnes sadaļā "Pakalpojumi".

5. Starptautiskā sadarbība

Eiropas kiberdrošības eksperti TF-CSIRT sanāksmē Rīgā analizē jaunākos kiberapdraudējumus un dalās pieredzē

2026. gada 11.-13. maijā Rīgā notika 77. ikgadējā TF-CSIRT sanāksme – forums, kurā vairāk nekā 150 Eiropas kiberdrošības incidentu reaģēšanas komandu ekspertu analizēja jaunākos kiberincidentus, uzbrucēju taktikas un reaģēšanas praksi. Dalībnieki apsprieda kritiskās infrastruktūras aizsardzību, ievainojamību pārvaldību, mākslīgā intelekta iespējas un riskus, kā arī kibertelpas krīžu komunikāciju. CERT.LV iepazīstināja partnerus ar Latvijas pieredzi industriālo tehnoloģiju drošībā, komerciālo uzbrukumu novēršanā un Drošības operāciju centra (SOC) ekspertu sadarbībā.

Pasākums stiprināja Latvijas iesaisti Eiropas kiberdrošības sadarbības tīklā un pievērsa starptautisku uzmanību Latvijai un reģionam aktuālajiem izaicinājumiem.

"TF-CSIRT tikšanās Rīgā bija nozīmīga iespēja ne tikai stiprināt starptautisko sadarbību kiberdrošības jomā, bet arī parādīt Latvijas ekspertu kompetenci un pieredzi Eiropas kopienai. Šādas tikšanās ir īpaši svarīgas laikā, kad kiberdrošības incidenti kļūst arvien sarežģītāki un ciešāka sadarbība starp organizācijām un valstīm ir kritiski nepieciešama," norāda CERT.LV vadītāja Baiba Kaškina.

CERT.LV ir TF-CSIRT biedrs kopš 2007. gada un kopš 2016. gada – viena no TF-CSIRT/Trusted Introducer sertificētajām komandām Eiropā. TF-CSIRT sanāksmes – foruma organizācija notika ar ES finansiālu atbalstu CERT.LV-SOC-LV projekta ietvarā. Sanāksmi organizēja TF-CSIRT sadarbībā ar CERT.LV, Aizsardzības ministriju, Nacionālo kiberdrošības centru, ISACA Latvijas nodaļu, LU Matemātikas un informācijas institūtu un Censys. Sanāksmi līdzfinansē Eiropas Savienība [CERT.LV-SOC-LV projekta ietvaros] (https://www.cert.lv/lv/par-mums/starptautiskie-projekti) (projekta ID: 101249230).

Attēlā: CERT.LV pārstāve un TF-CSIRT vadības komitejas locekle Dana Ludviga un CERT.LV vadītāja Baiba Kaškina

"CERT.LV aktīvi iesaistās TF-CSIRT kopienas stratēģisko iniciatīvu koordinēšanā, aktualizējot arī mūsu reģionam nozīmīgākos kiberdrošības izaicinājumus. Tas ļauj pievērst Eiropas ekspertu uzmanību aktuālajiem apdraudējumiem Latvijā un, sadarbojoties starptautiskā līmenī, stiprināt Latvijas kibertelpas drošību," norāda CERT.LV pārstāve un TF-CSIRT vadības komitejas locekle Dana Ludviga.

Kiberaizsardzības mācībās "Locked Shields 2026" Latvijas – Singapūras apvienotā komanda izcīna 1. vietu

2026. gada aprīlī Latvijas un Singapūras apvienotā komanda izcīnīja 1. vietu starptautiskajās kiberaizsardzības mācībās "Locked Shields 2026", kurās piedalījās aptuveni 4000 dalībnieku no 41 valsts. Apvienotajā Latvijas – Singapūras komandā bija ap 230 dalībnieku, no kuriem aptuveni 140 bija pārstāvji no Latvijas.

CERT.LV eksperti piedalījās mācību izspēlē apvienotajā Latvijas un Singapūras komandā, pildot uzdevumus gan tehniskajā komandā, gan mediju, gan stratēģiskās komunikācijas un juridiskajās komandās.

Rezultāts apliecina Latvijas kiberdrošības ekspertu augsto sagatavotību, spēju darboties starptautiskā komandā un praktiski reaģēt uz sarežģītiem kiberincidentu scenārijiem.

Dalība stiprināja CERT.LV pieredzi procedūru pārbaudē, tehniskajā sadarbībā, incidentu vadībā un starptautiskās pieredzes apmaiņā. Sasniegums nostiprina Latvijas reputāciju kā spēcīgai kiberdrošības partnervalstij un apliecina valsts, militārā sektora un tehnoloģiju uzņēmumu sadarbības modeļa efektivitāti.

Mācības "Locked Shields 2026" organizē Tallinā bāzētais NATO Kiberaizsardzības izcilības centrs (NATO CCD COE) sadarbībā ar alianses dalībvalstīm, partnervalstīm un tehnoloģiju kompānijām.

Foto: NATO CCDCOE

Transporta nozare kiberdrošības mācībās "Cyber Europe 2026" pilnveido krīžu pārvaldību

2026. gada 10. – 11. jūnijā norisinājās Eiropas Savienības Kiberdrošības aģentūras (ENISA) organizētās Eiropas mēroga kiberdrošības mācības "Cyber Europe 2026", kuru ietvarā Latvijas transporta nozares un valsts pārvaldes institūcijas piedalījās koordinētā krīžu vadības un incidentu reaģēšanas simulācijā. Mācību mērķis bija pārbaudīt un pilnveidot spēju identificēt, analizēt un pārvaldīt kiberdrošības incidentus, kā arī stiprināt sadarbību nacionālā un starptautiskā līmenī.

Mācībās uzmanība tika pievērsta transporta sektora noturībai, incidentu pārvaldībai, informācijas apritei un koordinētai rīcībai situācijās, kas var ietekmēt pakalpojumu nepārtrauktību.

6. Pārskats par LIA Drošāka interneta centra ZL darbību

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.04.2026. līdz 30.06.2026. ir saņēmusi un izvērtējusi 457 ziņojumus. No tiem 286 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 36 gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 16 ziņojumos konstatēta personas goda un cieņas aizskaršana, 3 ziņojumi saņemti par naida runu un 4 ziņojumos konstatēti vardarbīgi materiāli. Par finanšu krāpšanas mēģinājumiem internetā saņemti 43 ziņojumi, 49 ziņojumu saturs nav bijis pretlikumīgs, 20 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 82 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 206 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kuru atrašanās vieta bija ārpus Latvijas, ir ievietoti INHOPE asociācijas datu bāzē un iesniegti attiecīgās INHOPE valsts ziņojumu līnijai turpmāko darbību veikšanai, lai dzēstu nelegālo saturu no publiskas aprites.

Pārskata periodā no Latvijā uzturētajiem 82 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 80 ziņojumu saturs ir dzēsts no publiskas aprites internetā un 2 ziņojumi atrodas dzēšanas procesā.

Drošības trauksmes ziņojumu dinamika CERT.LV SOC klientu infrastruktūrā

Ziņojumi	Apr-26	Mai-26	Jūn-26	2. cet.
Erotisks/ pornogrāfisks saturs bez izvietotiem brīdinājumiem	17	7	12	36
Pedofilija/ mazgadīgo prostitūcija/ bērnu seksuālu izmantošanu saturoši materiāli	29	172	85	286
Vardarbīga rakstura materiāli	2	1	1	4
Cieņas/ goda aizskaršana	10	4	2	16
Naida kurināšana/ rasisms	2	1	0	3
Finanšu krāpšana	15	13	15	43
Konsultācijas/ padomi	7	6	7	20
Citi	13	22	14	49
KOPĀ:	95	226	136	457

Ziņojumi nosūtīti Valsts policijai	1	70	11	82
Ziņojumi nosūtīti INHOPE asociācijai	22	99	85	206
KOPĀ NOSŪTĪTI IZSKATĪŠANAI:	23	169	96	288

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