2026 C1

SITUĀCIJA LATVIJAS KIBERTELPĀ

PERIODS:
01.01.2026. - 31.03.2026.

CERT.LV
Kiberincidentu novēršanas institūcija

Latvijas Universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Kopsavilkums

2026. gada 1. ceturksnī kiberdrošības apdraudējums Latvijā **saglabājas augsts, kas prasa turpināt mērķtiecīgus pasākumus risku mazināšanai un noturības stiprināšanai**. Kopš Krievijas pilna mēroga iebrukuma Ukrainā 2022. gadā līdz šim reģistrēto kiberincidentu skaits Latvijas kibertelpā ir pieaudzis seškārtīgi, savukārt identificēto apdraudēto iekārtu skaits – astoņkārtīgi.

Manuāli tika apstrādāti **846 kiberincidenti** – skaits samazinājās pret iepriekšējo ceturksni par 8%, un vienlaikus ir otrs augstākais līdz šim reģistrētais rādītājs.

Identificēto apdraudēto iekārtus skaits sasniedza 757 286, kas ir augstākais rādītājs līdz šim. Kvantitatīvi lielāko daļu no tām veido konfigurācijas nepilnības, norādot uz sistēmu un tīkla drošības vājajiem punktiem, kas galvenokārt rodas cilvēkfaktora un nepietiekamu drošības standartu dēļ. Vienlaikus tas atspoguļo ne tikai faktisku apdraudējuma pieaugumu, bet arī **organizāciju kiberdrošības spēju pieaugumu attiecībā uz redzamību gala iekārtu līmenī**, ko nodrošina CERT.LV Drošības operāciju centra (SOC) pakalpojuma ieviešana un paplašināta atbilstība nacionālajam regulējumam. Tas ļauj agrīnāk atklāt, analizēt un novērst kiberriskus, un sistemātiski stiprināt kopējo noturību.

Lielākā daļa novēroto kiberuzbrukumu **neradīja būtiskas vai ilgstoši jūtamas sekas**. Tas lielā mērā skaidrojams ar preventīvi veiktajiem kiberaizsardzības pasākumiem un kopējo Latvijas kibertelpas noturību.

CERT.LV DNS ugunsmūris **bloķēja piekļuvi ļaunprātīgām vietnēm vairāk nekā 2,5 miljonus reižu** – tas ir par 139% vairāk nekā iepriekšējā ceturksnī un par 416% vairāk nekā attiecīgajā periodā pērn. Kiberincidentu skaita samazinājums skaidrojams arī ar apdraudējumu atklāšanas mehānismu attīstību. CERT.LV, turpinot attīstīt automatizētās atklāšanas spējas, apsteidzoši identificēja un bloķēja 266 krāpnieciskas kampaņas, tostarp novērsa vairākus gandrīz notikušus kiberincidentus.

Latvijas kibertelpa piedzīvoja pilnu spektru dažāda veida kiberuzbrukumu; kvantitatīvi lielākie bija krāpšana un ļaunprātīgs kods. Savukārt kā pastāvīgs operacionālais risks pakalpojumu atteices uzbrukumi (DDoS) pret Latvijas valsts un pašvaldību institūcijām un nozīmīgiem pakalpojumu sniedzējiem kļuvuši par nepārtrauktu slodzes un noturības testu.

Dominējošie draudi bija pikšķerēšana, informācijas zagšanas ļaunatūra, viltus programmatūras atjauninājumi un ļaunprātīgi pārlūka paplašinājumi, kas ļauj apiet tradicionālos aizsardzības mehānismus. Galvenie riski bija saistīti ar autentifikācijas datu zādzību un nesankcionētu piekļuvi.

Uzbrukumi kļūst arvien automatizētāki un balstīti uz sociālo inženieriju, nevis tikai uz tehniskām ievainojamībām – to pastiprina mākslīgā intelekta lietojuma iespēju paplašināšanās, kas paātrina krāpniecības, ielaušanās un automatizētu uzbrukumu veikšanu. Lielākais izaicinājums nav viens izolēts drauds, bet gan vairāku risku vienlaicīga iestāšanās.

Būtiska daļa kiberincidentu bija finansiāli motivēti uzbrukumi. Valstiski atbalstītu grupējumu aktivitātes joprojām ir ar mainīgu intensitāti, tostarp saistībā ar ģeopolitisko kontekstu. Krievija turpina būt galvenais drošības drauds, ņemot vērā Latvijas atbalstu Ukrainai karā pret Krievijas agresiju.

Nopietnas bažas joprojām rada apdraudējums no Latvijai naidīgo valstu puses ar mērķi iegūt kontroli un veikt destruktīvas darbības kritiskās infrastruktūras operatoru sistēmās, lai ietekmētu vai pat pārtrauktu būtisku un svarīgu pakalpojumu sniegšanu. Lai mazinātu šādas ietekmes iespējas un padarītu Latviju par grūtāku mērķi, CERT.LV turpina darbu pie operacionālo tehnoloģiju aktivitāšu virzieniem, nodrošinot plašāku redzamību un draudu identifikāciju, drošības testu veikšanu un koordinētu reaģēšanu uz incidentiem.

Pieaugošā uzbrukumu intensitāte, arvien inovatīvākas uzbrukumu metodes un ģeopolitiski motivēti incidenti **skaidri apliecina kiberdrošības izšķirošo nozīmi**. CERT.LV sniegtie pakalpojumi, tostarp SOC uzraudzība, draudu medības un regulāri drošības testi, būtiski stiprina Latvijas kibernoturību. Vienlaikus, nodrošinot regulāras apmācības un stiprinot lietotāju zināšanas kiberdrošības jomā, pārskata periodā **65** pasākumos CERT.LV eksperti izglītoja **13 309** dalībniekus.

Turpinoties pārskata periodā novērotajām tendencēm, prioritāri jāstiprina gala ierīču drošība, resursu kapacitāte, lietotāju apmācība un piegādes ķēžu kontrole, vienlaikus pastāvīgi uzlabojot reaģēšanas spējas un darbības nepārtrauktību atbilstoši normatīvajām prasībām.

Galvenie rādītāji

846 (+34%)

Manuāli apstrādātie kiberincidenti
2026.-1.CET. vs 2025-1.CET.

~754K (+167%)

Identificēto apdraudēto iekārtu skaits
2026.-1.CET. vs 2025-1.CET.

556 (+39%)

Krāpšana – dominējošais incidentu veids
2026.-1.CET. vs 2025-1.CET.

73 (+82%)

Ļaundabīgs kods - straujākais kāpums
2026.-1.CET. vs 2025-1.CET.

~2,5M (416%)

Tik reižu CERT.LV DNS ugunsmūra uzturētie saraksti bloķēja piekļuvi ļaunprātīgām vietnēm
2026.-1.CET. vs 2025-1.CET.

>84K (+9K)

DNS ugunsmūra mobilā lietotne lejupielādēta Android un IOS ierīcēs
Dati uz 2026.-1.CET. beigām

92 (+37)

Iestāžu (NKDL subjektu) skaits kopumā, kas izmanto CERT.LV SOC pakalpojumu
Dati uz 2026.-1.CET. beigām

43 037 (+3%)

Gala iekārtu skaits ar CERT.LV SOC pakalpojuma ietvarā nodrošinātu redzamību
Dati uz 2026.-1.CET. beigām

166 (+18)

CVD platformā kopumā reģistrēti drošības pētnieki
Dati uz 2026.-1.CET. beigām

541 (+107)

CVD platformā kopumā reģistrēti ievainojamību ziņojumi
Dati uz 2026.-1.CET. beigām

65 (+32)

CERT.LV ekspertu īstenotās izglītojošās aktivitātes/pasākumi kiberdrošības jomā
2026.-1.CET. vs 2025-1.CET.

13 309 (+3 104)

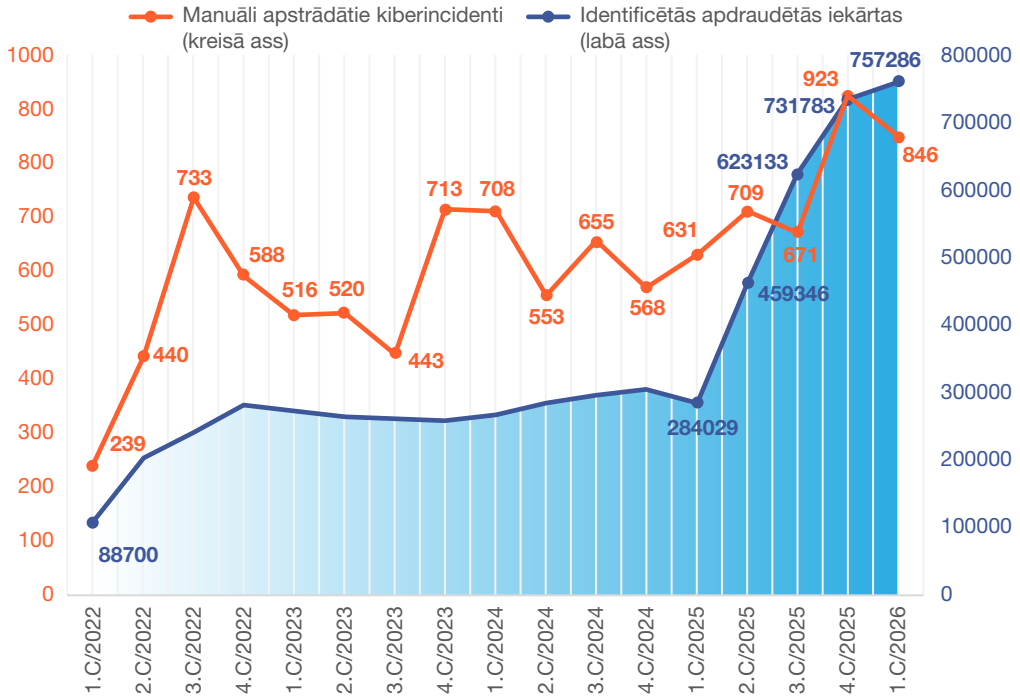
Sasniegtās auditorijas skaits CERT.LV ekpertu īstenotās aktivitātēs/pasākumos
2026.-1.CET. vs 2025-1.CET.

Satura rādītājs

1. Kibertelpas drošības apdraudējumi: statistika un tendences

Kiberincidentu un apdraudēto iekārtu dinamika

2026. gada 1. ceturksnī kiberdrošības apdraudējums Latvijā saglabājas augsts, kas liek turpināt mērķtiecīgu darbu risku mazināšanā un noturības stiprināšanā. Kopš 2022. gada Krievijas pilna mēroga iebrukuma Ukrainā Latvijas kibertelpā reģistrēto kiberincidentu[1] skaits ir pieaudzis seškārtīgi, savukārt identificēto apdraudēto iekārtu skaits – astoņkārtīgi.



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

Manuāli apstrādātie kiberincidenti

2026. gada 1. ceturksnī Latvijā reģistrēti **846 manuāli apstrādāti kiberincidenti** – tas ir otrs augstākais rādītājs līdz šim. Salīdzinājumā ar 2025. gada 1. ceturksni pieaugums ir par 34%.

Savukārt salīdzinājumā ar 2025. gada 4. ceturksni incidentu skaits samazinājās par 8%. Nozīmīgs aspekts, kas veicināja samazinājumu, ir apdraudējumu atklāšanas mehānismu efektivitātes attīstība. Pārskata periodā **apsteidzoši tika identificētas un ierobežotas vairākas krāpnieciskas kampaņas**, tostarp novērsti vairāki gandrīz notikuši kiberincidenti[2]. CERT.LV, arvien attīstot automatizētus detekcijas mehānismus (analītiskos skriptus) un DNS/domēnu reputācijas indikatorus, **apsteidzoši identificēja** un bloķēja **266 aktīvas krāpnieciskas kampaņas** (dominēja kampaņas ar CSDD un banku identitātes ļaunprātīgu izmantošanu), tādējādi efektīvi **ierobežojot to izplatību un novēršot piekļuvi gala lietotājiem**.

Kopumā Latvijas kibertelpas drošības apdraudējumu pieaugums korelē ar globālo kiberapdraudējumu eskalāciju, pieaugošu digitālo atkarību sabiedrībā un cilvēkfaktoru. Būtisku lomu spēlē mākslīgā intelekta (MI) rīku nemitīga attīstība, kas atvieglo un paātrina krāpniecības, ielaušanās un automatizētu uzbrukumu veikšanu.

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.

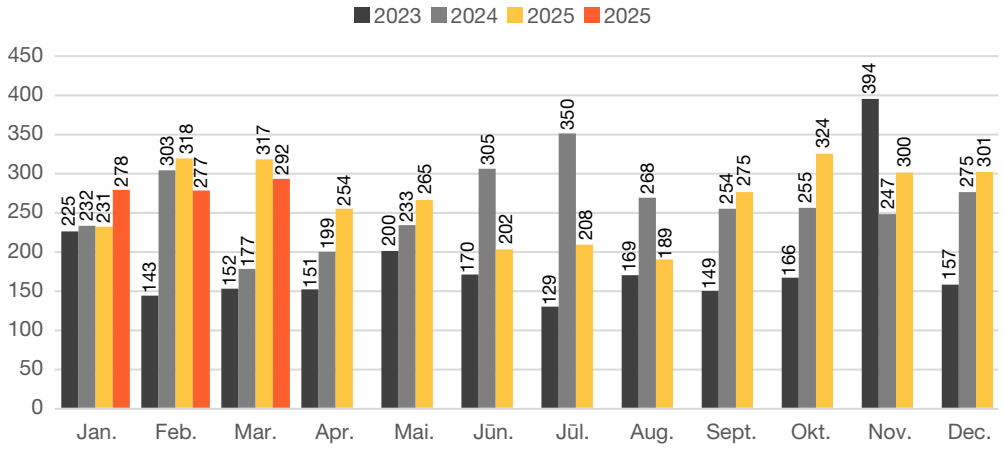
2 **Gandrīz noticis kiberincidents** – notikums, kurš būtu varējis apdraudēt apstrādātus datus vai tīklu un informācijas sistēmu piedāvāto vai ar tīklu un informācijas sistēmu starpniecību pieejamo pakalpojumu pieejamību, autentiskumu, integritāti vai konfidencialitāti, bet kura pilnīga īstenošanās tika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

Identificētās apdraudētās iekārtas

CERT.LV identificēto apdraudēto iekārtu skaits sasniedza 757 286, **kas ir augstākais rādītājs līdz šim** – par 167% vairāk nekā 2025. gada 1. ceturksnī un par 3% vairāk nekā 4. ceturksnī. Šī dinamika norāda uz automatizētu skenēšanas un ievainojamību izmantošanas pieaugumu. Kvantitatīvi lielāko daļu veido konfigurācijas nepilnības, norādot uz sistēmu un tīkla drošības vājajiem punktiem, kas galvenokārt rodas cilvēkfaktora un nepietiekamu drošības standartu dēļ.

Identificētu apdraudētu iekārtu skaita pieaugums ir skaidrojams ne tikai ar faktisku apdraudējuma pieaugumu, bet arī ar **būtiski uzlabotu redzamību gala iekārtu līmenī, ieviešot CERT.LV SOC pakalpojumu**. Vienlaikus, paplašinot klientu loku atbilstoši Nacionālajam kiberdrošības likumam (turpmāk – NKDL) noteiktajiem subjektiem[3], **ir palielināts uzraugāmo iekārtu apjoms**. Šie faktori kopumā veicina savlaicīgu apdraudējumu identificēšanu, un uzlabo organizāciju spēju nodrošināt nepārtrauktu, efektīvu aizsardzību un noturību pret kiberapdraudējumiem 24/7 režīmā.

2026. gada sākums rāda, ka laika posmā no janvāra līdz martam kiberincidentu skaits joprojām saglabājas augsts un kopumā noturīgs, norādot uz pastāvīgi augstu incidentu fonu, nevis atsevišķiem pīķiem. Tas nozīmē, ka organizācijām jāstrādā nepārtrauktas noturības režīmā, nevis jāreaģē tikai uz atsevišķiem incidentiem.



2. attēls. Kiberincidentu dinamika (skaits mēnešu dalījumā)

3 Būtisko pakalpojumu sniedzēji, svarīgo pakalpojumu sniedzēji un informācijas un komunikācijas tehnoloģiju kritiskās infrastruktūras īpašnieki un tiesiskie valdītāji (turpmāk visi kopā – NKDL subjekti)

"Kiberlaikapstākļu" vērotājiem CERT.LV piedāvā ikmēneša pārskatu par būtiskākajiem un spilgtākajiem kiberincidentiem un apdraudējumiem Latvijas kibertelpā TOP 5 kategorijās. Pārskats pieejams tīmekļvietnē CERT.LV sadaļā "Ziņas" (JANVĀRIS | FEBRUĀRIS | MARTS)

2. Izplatītākie kiberapdraudējumi un būtiskākie notikumi pārskata periodā

TOP 5 kvantitatīvi lielākie kiberincidentu veidi

Lielākais risks - krāpšana un ļaundabīgs kods. Uzrādot strauju pieaugumu:

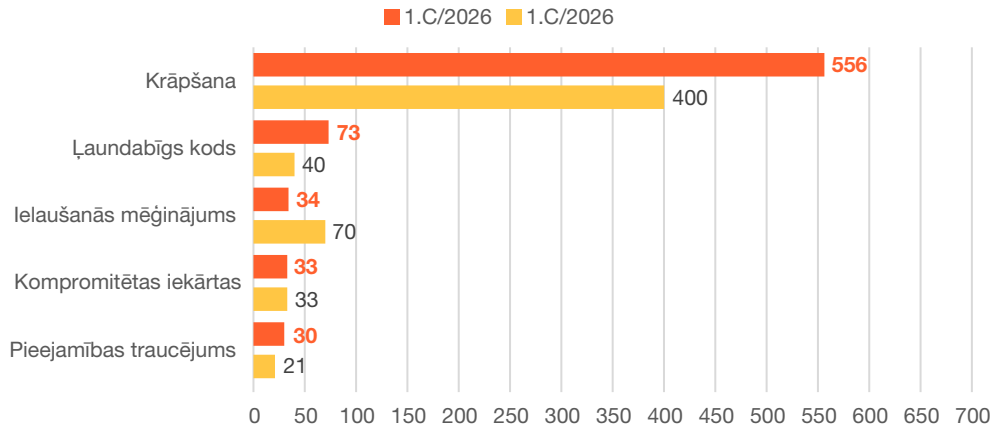
- krāpšana pieaugusi par 39% (dominējošais incidentu veids);
- ļaundabīgs kods pieaudzis par 82% (straujākais kāpums).

Kompromitētu iekārtu skaits saglabājas nemainīgs, savukārt pieejamības traucējumi pieauga par 43%, kas norāda uz pieaugošiem operacionāliem riskiem.

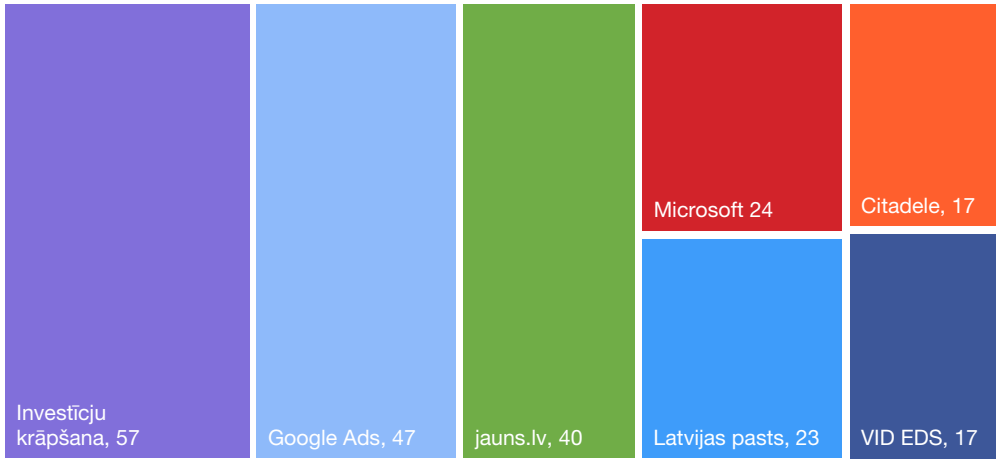
Ielaušanās mēģinājumu skaita samazinājums norāda uz uzbrukumu taktikas maiņu. Kiberapdraudējumu fokuss pāriet no tehniskiem ielaušanās mēģinājumiem uz cilvēkfaktora izmantošanu (pikšķerēšana, krāpšana) un ļaunatūru izmantošanu piekļuves datu zagšanai.

Dominē investīciju shēmas ar slavenību dziļviltojumiem un "investēšanas veiksmes stāstiem" viltus portālos; izplatīta arī ļaunprātīga Google reklāmu izmantošana, uzdošanās par autoritatīvām iestādēm.

CERT.LV veiktais sabiedriskās domas pētījums par kiberdrošības izpratni un paradumiem Latvijas sabiedrībā atklāj, ka vairāk nekā puse (66%) Latvijas iedzīvotāju ir saskārušies ar krāpnieciskām aktivitātēm digitālajā vidē. Biežākie iemesli, kāpēc "uzķērušies" uz krāpniekiem - steigas dēļ neiedziļinoties (21%), kā arī tas, ka krāpnieciskā saruna un tās saturs šķita ticams (19%).



3. attēls. TOP5 kiberincidentu veidi (skaits)



4. attēls. Izplatītākās krāpniecības kampaņas un tematika (skaits)

CERT.LV aicina ikvienu izmantot platformu kibertests.lv, kas paredzēta iedzīvotājiem un organizācijām, lai novērtētu savas pamatzināšanas kiberdrošībā un saprastu, kas būtu uzlabojams. Vienlaikus kibertests.lv var kalpot kā sagatavošanās posms pirms pikšķerēšanas testa veikšanas, sniedzot organizācijai pārskatu par jau esošo situāciju un jomām, kurās nepieciešami uzlabojumi.

TOP 10 ļaunatūras

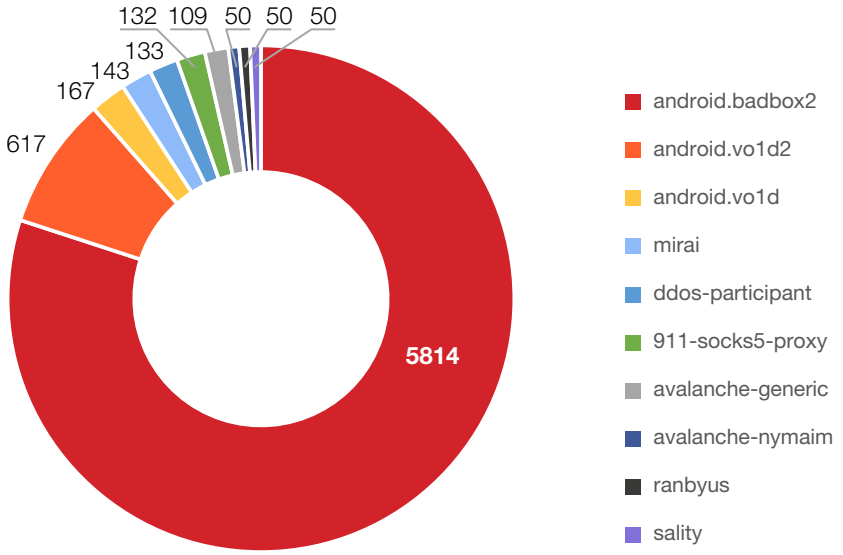
2026. gada 1. ceturksnī izplatītāko ļaunatūru tipi liecina par masveidīgiem, automatizētiem un ilgstošiem apdraudējumiem.

Ļaunatūru TOP 10 augšgalā joprojām pārliecinoši dominē ļaunatūra "Android.badbox2", tās izplatība ir pieaugusi par 58% salīdzinājumā ar iepriekšējo ceturksni.

"Android.badbox2" ir mobilais botu tīkla variants, kas spēj inficēt ierīces, veicot, piemēram, piekļuves datu zagšanu un attālinātu kontroli par ierīci. Tās izplatība norāda uz būtisku un mērķtiecīgu aktivitāti Android ierīcēs un liecina par masveida inficēšanas kampaņām, izmantojot neoficiālas lietotņu instalācijas vai viltus atjauninājumus.

Galvenie riski – piekļuves datu pārtveršana, inficētu gala ierīču kompromitēšana un izmantošana turpmākos kiberuzbrukumos. Organizācijas un individuālie lietotāji var pat nezināt, ka viņu IP adrese "piedalās" botu tīkla uzbrukumos.

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



5. attēls. TOP 10 ļaunatūras (skaits)

TOP 10 tendences kiberuzbrukumu veidos

- **Strauji pieaug mērķēta pikšķerēšana, kas pielāgota konkrētam kontekstam.** Uzbrukumi notiek brīdī, kad lietotājs, piemēram, pārlūkā meklē konkrētu pakalpojumu (VID EDS, e-veselība). Pikšķerēšana kļūst par precīzu uzbrukumu lietotāja nodomam. Ļaunprātīgi izmantojot Google reklāmas, lietotājs tiek novirzīts uz viltotām tīmekļvietnēm.
- **Sociālās inženierijas tehnoloģiska evolūcija un diversifikācijas pieaugums**, tostarp viltus "CAPTCHA", kas liek lietotājam pašam instalēt ļaunatūru; viltus programmatūras atjauninājumi; uzbrukumi, kas izmanto vairākus saziņas kanālus (e-pastu, tālruni un tīmekli), lai psiholoģiski ietekmētu cilvēkus.

Izplatītākie ļaunatūru tipi

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

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

- **Ļaunprātīgi pārlūka paplašinājumi, kas maskējas kā leģitīmi rīki**, bet patiesībā veic kaitīgas darbības (ievāc paroles, sesiju sīkdatnes un citus datus).
- **Ļaunatūra lietotāju autentifikācijas datu izgūšanai un kontu kompromitēšana.** Uzbrukumu mērķis pāriet no infrastruktūras uz gala lietotāju. Dominē ļaunatūra, kas paredzēta informācijas zādzībai – tā iegūst pārlūkā saglabātās paroles un sesiju piekļuves datus. Latvijā konstatēti vairāki gadījumi, tostarp tādi, kad no tīmekļa lejupielādēti un "palaisti" izpildāmie faili. Tāpat pieaudzis pikšķerēšanas e-pastu ar ļaunprātīgiem pielikumiem skaits. Starptautiskie avoti liecina, ka 2025. gadā būtiski pieaudzis nozagto piekļuves datu apjoms nelegālajos tirgos, kas norāda uz šo datu aktīvu tirdzniecību.
- **Automatizācija uzbrukumos pieaug.** Pikšķerēšana kombinācijā ar ļaunprogrammatūru un uzbrucēju pārvaldītiem vadības un kontroles serveriem (*Command and Control / C2 servers*) ļauj uzbrukumus veikt ātri, lēti un lielā apjomā, kas padara tos grūtāk novēršamus.
- **Jauna automatizēta masveida krāpniecība ar "kluso zvanu" taktiku.** Tas ir tehniski vienkāršs, bet efektīvs sagatavošanās posms, kurā "klusie zvani" tiek izmantoti aktīvu tālruņa numuru validācijai, iezīmējot pāreju uz masveida datu vākšanu.
- **Kritiskās infrastruktūras pastāvīga "testēšana".** Novērojami plaša pārklājuma pakalpojuma atteices uzbrukumi (*carpet bombing*), kurā uzbrucēji vienlaikus ar lielu datplūsmu pārslogo ļoti plašu mērķu loku. Tas norāda uz pieaugošu automatizētu apdraudējuma fonu. Novēroti periodiski terabitu apmēra uzbrukumi telekomunikāciju nozares uzņēmumu infrastruktūrai, kas uzskatāmi par īpaši apjomīgiem un spēcīgiem.
- **Izspiedējvīrusu pieaugums rada augstu ietekmes un darbības nepārtrauktības risku.** Latvijā fiksēti vairāki gadījumi, tostarp "HardBit" incidents – mērķēts uz uzņēmuma grāmatvedības serveri.
- **Biznesa e-pasta kompromitācija (BEC) ar augstu finansiālo ietekmi.** Viens no efektīvākajiem finanšu uzbrukuma veidiem (vadītāju e-pastu kompromitēšana, viltoti rēķini/maksājumu pieprasījumi). Latvijā fiksēti reāli gadījumi ar ievērojamiem uzņēmumu finanšu zaudējumiem.
- **Saziņas platformu kompromitēšana.** Uzbrukumi pāriet uz drošām saziņas platformām (lietotnes Signal kontu pārņemšanas gadījumi). Mērķi: amatpersonas, kas Latviju pārstāv starptautiski, un žurnālisti. Tas rada augstus datu noplūdes riskus un potenciāli spiegošanai labvēlīgus apstākļus.

Uzbrucēju motivācija

- **Finansiāli motivēti kiberuzbrucēji:** galvenie virzieni – izspiedējvīrusi, BEC, investīciju krāpšana un datu monetizācija, lai tādējādi nopelnītu naudu vai gūtu citu labumu.
- **Politiski motivēti un valstiski atbalstīti uzbrucēji:** galvenie virzieni – DDoS uzbrukumi augstas nozīmes mērķiem; kiberuzbrukumi industriālām kontroles sistēmām; kontu kompromitēšanas mēģinājumi publiskām, starptautiskām personām; izlūkošana un piekļuve sensitīvai informācijai. Paaugstināts risks ar informatīvās ietekmes operācijām pirms 2026. gada Saeimas vēlēšanām.
- **Oportūnistiski kiberuzbrucēji:** fokusējas uz redzamiem mērķiem – valsts iestādes, stratēģiskas organizācijas, publiskie pakalpojumi. Izmanto DDoS kā zemas barjeras ietekmes instrumentu. Aktivitāte bieži nav tieši pierādāma, bet mērķu izvēle norāda uz stratēģisku interesi.

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 pieejamība sabiedrībai.
- 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.
- Pastāv risks, ka **Irānas** haktīvistu grupējumi varētu aktivizēties Latvijas informatīvajā telpā, ja tajā tiek pausts atbalsts Izraēlai. Līdzīga sakarība jau novērota Krievijas haktīvistu aktivitātēs, kas pastiprinās, reaģējot uz Latvijas atbalstu Ukrainai.

Mērķētās nozares

Pieaugoši riski, ko var radīt apdraudējums operacionālajām tehnoloģijām (OT), kuras tiek izmantotas fizisku procesu, iekārtu un infrastruktūras monitorēšanai un kontrolei, lai nodrošinātu sabiedrībai kritiski svarīgus pakalpojumus, tostarp **enerģētikā, ūdensapgādē un transportā**.

Kiberuzbrucēji var attālināti piekļūt industriālās kontroles sistēmām vai citām OT, lai ietekmētu pakalpojumu sniegšanu, ja šo sistēmu kiberaizsardzība netiek veikta pietiekami efektīvi un atbildīgi.

Tāpat mērķi ir valsts un pašvaldību iestādes, aizsardzības un politikas sektors, telekomunikācijas, mazumtirdzniecība un akadēmiskā vide. Riska grupā ir arī organizācijas ar plašu publisko atpazīstamību un lielu klientu bāzi.

Ietekme uz sabiedrību, organizācijām un valsti

Latvijas kibertelpai raksturīgi trīs savstarpēji pastiprinoši riski.

- **Pakalpojuma pieejamības traucēšana.** Nozīmīgu mērķu (LVRTC, "Tet", e-veselība) piemēri rāda, ka DDoS ir nevis teorētisks, bet ikdienas operacionāls risks. Latvijā redzami periodiski terabitu apjoma triecieni, tiek testētas sistēmu "robežas", vienlaikus mērķis ir arī "sodīt" par Latvijas atbalstu Ukrainai.
- **Informācijas zagšanas ļaunatūra un lietotāja kontu kompromitēšana.** Uzbrukumu mērķis pāriet no infrastruktūras uz galalietotāju. Gadījums ar Microsoft "tenant" konta kompromitēšanu, kas notika kāda novada pašvaldībā, apliecina, ka šie uzbrukumi var potenciāli radīt plašu ietekmi
- **Piegādes ķēdes un ārpakalpojumu riski.** Latvijā daļa uzņēmumu joprojām izmanto stratēģiski apšaubāmus risinājumus. Piemēram, incidents, kur uzņēmuma grāmatvedības serveris, ko izmantoja 1C noliktavas sistēmas darbībai, tika kompromitēts un inficēts ar "HardBit" izspiedējvīrusu, skaidri parādīja, ka šāda izvēle nav tikai IT jautājums, bet biznesa un nacionālās drošības jautājums. 1C grāmatvedības programmatūras izcelsmes valsts ir Krievija, un šāda produkta izvēle ir uzskatāma par stratēģisku kļūdu un potenciālu apdraudējumu.

Galvenie secinājumi un priekšlikumi

Kiberdrošības apdraudējums Latvijā saglabājas augsts un kļūst arvien vairāk orientēts uz lietotāju kompromitēšanu, nevis tikai infrastruktūras ievainojamībām.

DDoS uzbrukumi kļuvuši par pastāvīgu operacionālu risku, kas testē organizāciju pieejamību un noturību. Nepieciešams stiprināt darbības nepārtrauktības plānus un infrastruktūras elastību.

Dominē pikšķerēšana, informācijas zagšanas ļaunatūra, viltus programmatūras atjauninājumi un ļaunprātīgi pārlūka paplašinājumi, kas ļauj apiet tradicionālos aizsardzības mehānismus. Galvenie riski saistīti ar autentifikācijas datu zādzību un nesankcionētu piekļuvi, īpaši organizācijās ar vāju lietotāju drošības kontroli. Cilvēkfaktors un sociālā inženierija ir kļuvuši par galveno uzbrukuma virzītāju.

Lai mazinātu ietekmi, prioritāri jāstiprina gala ierīču drošība, resursu kapacitāte, lietotāju apmācība un piegādes ķēžu kontrole, vienlaikus uzlabojot reaģēšanas spējas un darbības nepārtrauktību atbilstoši normatīvajām prasībām.

Ieteikumi organizāciju IKT drošībai

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

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

3.1. DNS ugunsmūris

CERT.LV DNS ugunsmūris, izmantojot tā uzturētos sarakstus, 2026. gada 1. ceturksnī bloķēja piekļuvi ļaunprātīgām vietnēm vairāk nekā 2,5 miljonus reižu – tas ir:

- par 139% vairāk nekā iepriekšējā ceturksnī;
- par 416% vairāk nekā attiecīgajā periodā pērn.

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

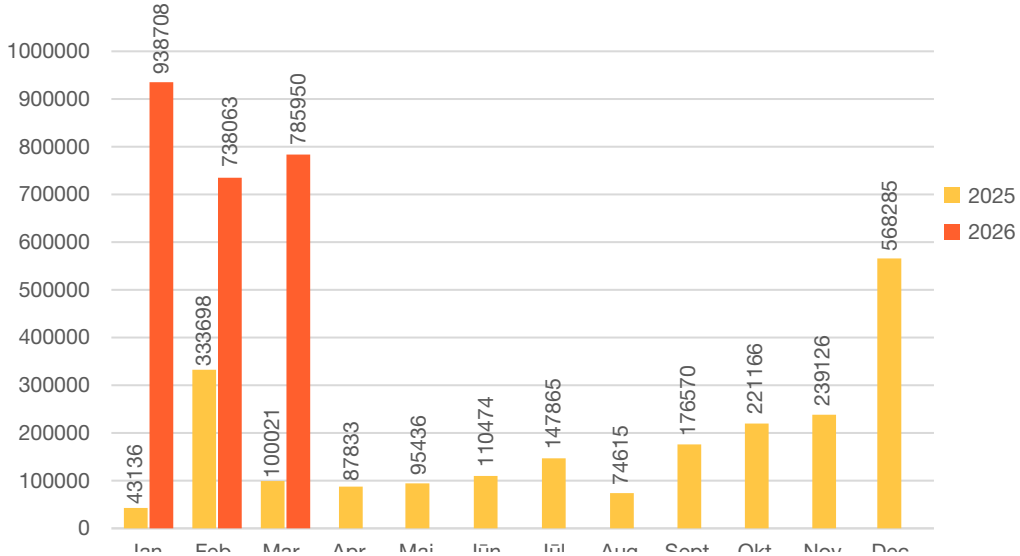
CERT.LV proaktīvi monitorē un aptur identificētās krāpnieciskās kampaņas. Nozīmīga ir arī iedzīvotāju iesaiste, kuri pārsūta krāpnieciskos e-pastus, īsziņas un tīmekļa vietņu saites uz cert@cert.lv vai ziņo pa tālruni 23230444. Saņemtie ziņojumi tiek apkopoti un pārbaudīti, kaitnieciskie domēna vārdi ievietoti DNS ugunsmūrī, lai ierobežotu piekļuvi no LV interneta lietotāju puses un samazinātu iespējamo kaitējumu.

Nozīmīgākās aktīvās aizsardzības epizodes pārskata periodā:

- "Jauns.lv", "DELFI" un "LSM" tēla izmantošana krāpniecisku kriptovalūtu investīciju platformu reklamēšanas kampaņās;
- "CSDD" un "SEB" tēla izmantošana viltus vietnes kampaņās.

DNS ugunsmūris un tā mobilā lietotne bez maksas ir pieejama ikvienam Latvijas iedzīvotājam un organizācijai. Papildu informācija par DNS ugunsmūra uzstādīšanu pieejama vietnē dnsmuris.lv.

~280K – Vidējais bloķēto ļaunprātīgo vietņu skaits mēnesī
~30min. – Vidējais reakcijas laiks līdz ļaunprātīgu vietņu identificēšanai un indikatora ievietošanai bloķēšanas sarakstā
>84K – DNS ugunsmūra mobilā lietotne lejupielādēta Android un IOS ierīcēs (kopš 2024. gada)
~5,6M – DNS pieprasījumu skaits 2026. gada 1. ceturksnī



6. attēls. CERT.LV DNS ugunsmūra uzturēto sarakstu (*cert-shield, malware, phishing, high-risk*) bloķētās ļaunprātīgās vietnes*

3.2. 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.

Pakalpojums ietver:

- nepārtrauktu datu plūsmas anomāliju analīzi un ļaunprogrammatūras aktivitāšu atpazīšanu;

* Šajā statistikā nav iekļauti dati par citu valsts kompetento iestāžu sarakstiem par nelikumīga tiešsaistes satura ierobežošanu.

- brīdinājumu nosūtīšanu pakalpojumu saņēmējam par konstatētajiem augstas prioritātes kiberapdraudējumiem;
- regulāru CERT.LV aktuālo kiberapdraudējumu indikatoru atjaunošanu;
- pakalpojuma saņēmēju konsultēšanu un atbalstu.

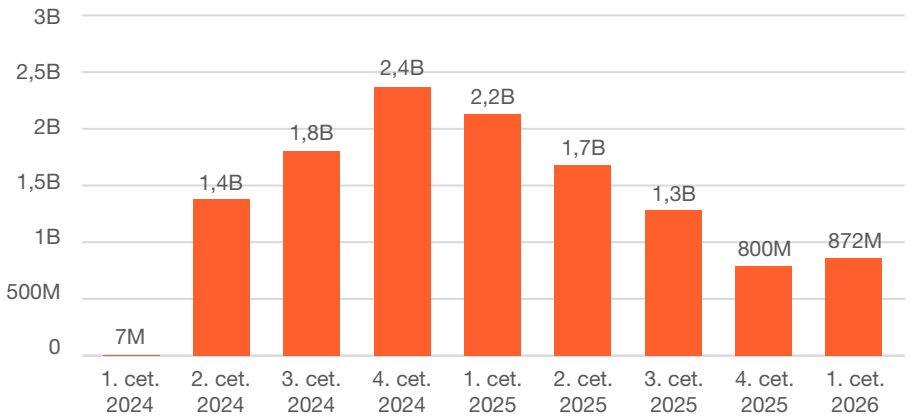
Kiberapdraudējumu un kiberincidentu atklāšana un novēršana

2026. gada 1. ceturksnī ABS reģistrēto trauksmju skaits bija aptuveni 872 miljoni – tas ir:

- par 9% vairāk nekā iepriekšējā ceturksnī;
- ~2,52 reizes mazāk nekā attiecīgajā periodā pērn.

Apjoma kritums skaidrojams ar pielietotās indikatoru kopas optimizēšanu.

Aktuālākie apdraudējumi bija saistīti gan ar tīkla pieprasījumiem uz domēniem, kas saistīti ar identificētām pikšķerēšanas kampaņām, gan ar ļaunatūrām, kas aicina lejupielādēt viltus programmatūras atjauninājumus. Konstatēti arī tīkla pieprasījumi uz identificētiem kaitīgiem uzbrucēju pārvaldītajiem vadības un kontroles serveriem.



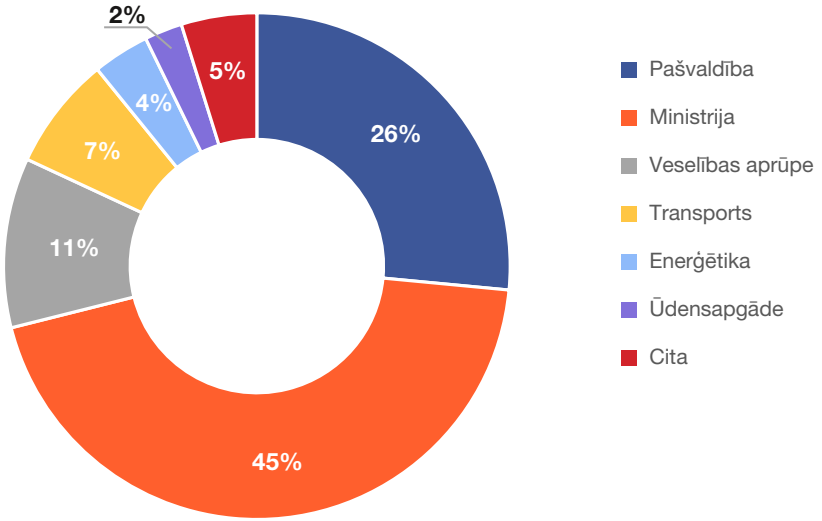
7. attēls. ABS reģistrēto trauksmju skaits pa ceturkšņiem (milj. - miljrd.)

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.

CERT.LV SOC pakalpojums centralizēti apkopo drošības telemetriju no klienta infrastruktūras, korelē notikumus klienta infrastruktūrā ar visu CERT.LV pieejamo apdraudējumu indikatoru un zināšanu kopu, lai savlaicīgi identificētu, brīdinātu, apturētu kiberapdraudējumu vai kiberincidentu un tā kaitējumu.

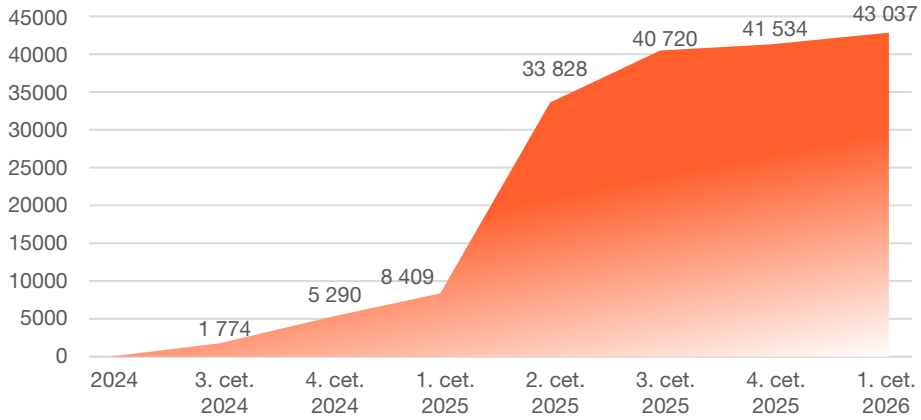


8. attēls. Sadalījums ar iestāžu sektoriem, kas izmanto CERT.LV SOC

CERT.LV SOC pakalpojumu uz 2026. gada 1. ceturkšņa beigām kopskaitā izmanto: **92 NKDL subjekti** (pieaugums par 37).

CERT.LV SOC klientu skaita pieaugumu daļēji ietekmēja arī atšķirības statistikas metodoloģijā – uzskaite tiek veikta pēc institūciju reģistrācijas numura, tādējādi ne tikai resora līmenī, bet arī padotības iestādes tiek skaitītas atsevišķi, ja tām ir savs reģistrācijas numurs, un tās ir reģistrētas Nacionālā kiberdrošības centrā kā subjekti.

Kopskaitā **iegūta redzamība pār 43 037 gala iekārtām**, tostarp serveriem un darbstacijām. Pārskata periodā pieaugums veido 3,6% no kopēja apjoma, līdz ar to palielinājies arī drošības trauksmes ziņojumu skaits.



9. attēls. CERT.LV SOC redzamības dinamika: gala iekārtu skaits

Drošības trauksmes ziņojumu dinamika CERT.LV SOC klientu infrastruktūrā

Rādītāji	Skaits	Skaita izmaiņas pret 2025. gada 4.cet.
CERT.LV SOC pakalpojuma ietvarā kopumā reģistrēto drošības trauksmju ziņojumu skaits 2026. gada 1. ceturksnī:	**~24 milj.**	**+4%**
Zems trauksmes līmenis	**~6 milj.**	**-11%**
Vidējs trauksmes līmenis	**~18 milj.**	**+8%**
Augsts trauksmes līmenis	**~11 tūkst.**	**-86%**
Kritisks trauksmes līmenis	**~16 tūkst.**	**-70%**
Manuāli izveidotas lietas	**586**	**+13%**
Viltus pozitīvās lietas	**571**	**+12%**
Kiberincidentu skaits	**15**	**+88%**

Pārskata periodā **reģistrēti aptuveni 24 miljoni drošības trauksmes ziņojumu**, kas ir **par 4% vairāk** nekā 2025. gada 4. ceturksnī. Pieaugums galvenokārt skaidrojams ar iegūtu plašāku redzamību jauno klientu infrastruktūrā.

Lielākā daļa trauksmju bija vidēja līmeņa (~74% no kopēja apjoma), un to skaits pieauga par 8% salīdzinājumā ar 2025. gada 4. ceturksni. Savukārt zema līmeņa trauksmes (~25% no kopējā apjoma), kas pārsvarā saistītas ar sistēmu troksni un viltus pozitīviem gadījumiem, samazinājās par 11%.

Kopumā novērojama kvalitātes uzlabošanas trauksmju apstrādē, samazinot maznozīmīgu notikumu īpatsvaru.

Augsta un kritiska līmeņa trauksmju absolūtais skaits (~27 tūkst.) samazinājās gandrīz pieckārtīgi salīdzinājumā ar 2025. gada 4. ceturksni (~133 tūkst.).

Augsta un kritiska līmeņa trauksmes liecina par iespējamiem bīstamiem uzbrukumiem un prasa rūpīgu izvērtēšanu, īpašu uzmanību pievēršot kritiskā līmeņa trauksmēm.

Trauksmju skaita samazinājumu ietekmēja klientu vidē ieviesto drošības pasākumu efektivitāte, kā arī viltus pozitīvo gadījumu identificēšana. Samazinātais trauksmju apjoms ļauj agrīnāk identificēt reālos riskus un veicina sistemātisku kiberdrošības noturības stiprināšanu.

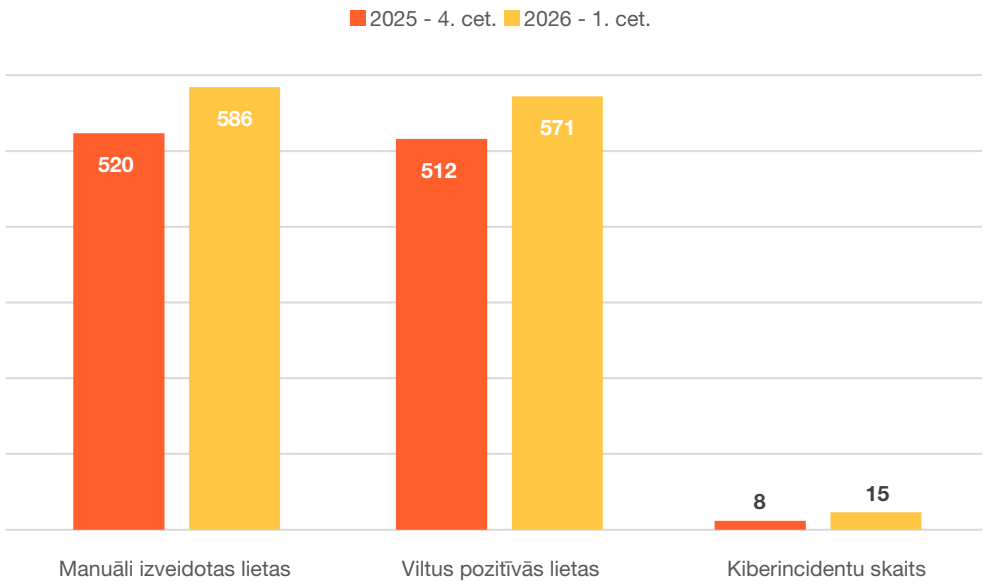
SOC pakalpojuma ietvarā izveidotās lietas un fiksētie kiberincidenti

CERT.LV SOC pakalpojuma ietvarā 2026. gada 1. ceturksnī:

586 (+66) – Manuāli izveidotas lietas

571 (+59) – Viltus pozitīvās lietas

15 (+7) – Fiksētie incidenti 13 dažādās iestādēs



10. attēls. Drošības notikumu struktūra un skaita salīdzinājums

Pārskata periodā fiksēto kiberincidentu pārskats

Plašākais incidents tika konstatēts vienlaikus četrās iestādēs, kura laikā tika identificētas aizdomīgas aktivitātes, liecinot par iespējamu iekārtu inficēšanos ar ļaunatūru pikšķerēšanas rezultātā. Kopumā tika skartas 6 iekārtas, kurām bija pieejama redzamība SOC pakalpojuma ietvaros.

Visās skartajās vidēs tika izmantota ESET antivīrusu programmatūra, kas konkrētajā gadījumā nespēja novērst ļaunatūras izpildi. Skartās iekārtas tika izolētas, sazinoties ar attiecīgo iestāžu kontaktpersonām. Notikums tika nodots turpmākai izmeklēšanai un ietekmes novērtēšanai.

Incidenta izmeklēšanas procesā tika konstatēta vēl viena inficēta iekārta citā iestādē, kuras drošības telemetrijas dati SOC pakalpojuma ietvarā nebija pieejami. Ņemot vērā incidenta mērogu un potenciālo ietekmi, klientiem tika izsūtīti brīdinājumi, kā arī publicēts informatīvs paziņojums sociālajos medijos.

Citi konstatētie incidenti galvenokārt bija saistīti ar nevēlamas vai nekontrolētas programmatūras lejupielādi un palaišanu, informācijas zagšanas ļaunatūru un paroļu pilno pārlasi (brute-force attack), kā arī ar neaizsargātu gala iekārtu netīšu eksponēšanu internetā, potenciāli pakļaujot tās riskam.

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.

CERT.LV SOC pakalpojums veicina savlaicīgu apdraudējumu identificēšanu un reaģēšanu, uzlabo organizāciju spēju nodrošināt nepārtrauktu, efektīvu aizsardzību un noturību pret kiberapdraudējumiem 24/7 režīmā.

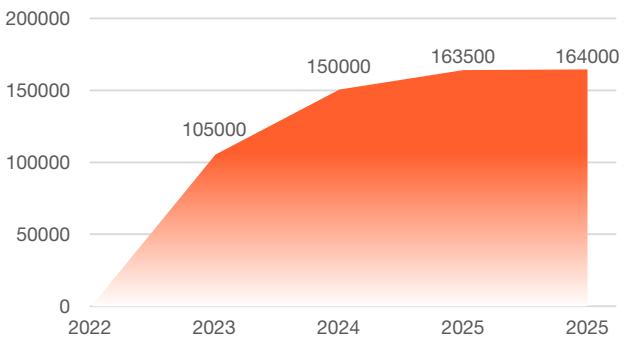
Dominējošie sākotnējās piekļuves vektori:

- **pikšķerēšana un ļaunprātīgi e-pastu pielikumi;**
- **pārlūku spraudņi;**
- **viltus "CAPTCHA";**
- **no tīmekļa lejupielādēti un palaisti izpildāmie faili;**
- **zibatmiņas, palaisti izpildāmie faili.**

3.4. Kiberdrošības draudu medību operācijas

Kopš 2022. gada, kad tika uzsāktas kiberdrošības draudu medības, uz 2026. gada 1. ceturkšņa beigām kopumā draudu medību operācijas tika veiktas **164 000 gala iekārtās** vairāk nekā 42 NKDL subjektu, tostarp IKT kritiskās infrastruktūras organizācijās.

Iegūtie dati liecina, ka APT klātbūtne iekārtās tika identificēta aptuveni 20% no visām draudu medību operācijās analizētajām organizācijām.



11. attēls. Draudu medībās analizēto iekārtu apjoma dinamika

Divpusējās stratēģiskās sadarbības

Latvija – Kanāda

Turpinās CERT.LV stratēģiskā partnerība ar Kanādas Bruņoto spēku kiberpavēlniecību draudu medību operāciju organizēšanā.

24.-27. martā Rīgā notika CERT.LV un Kanādas Bruņoto spēku kiberpavēlniecības organizētais jau ceturtais **Draudu medību apmācību kurss** par kiberdraudu meklēšanu, kuru vadīja Kanādas un Latvijas kiberdrošības speciālisti. Tas pulcēja 37 dalībniekus no 14 valstīm, lai stiprinātu viņu spējas rīkoties proaktīvi un savlaicīgi identificēt kiberdraudus vēl pirms to īstenošanās. Draudu medību apmācību kurss tika īstenots ar Eiropas Savienības (ES) finansiālu atbalstu projekta CERT.LV-SOC-LV ietvarā.

Foto: Amy Langlois

Latvija – Ukraina

Turpinās stratēģiskā partnerība ar Ukrainas kiberdrošības institūcijām, abpusēji attīstot kiberaizsardzības spējas, nodrošinot IKT infrastruktūru ar atbilstošu kiberaizsardzības līmeni un integrējot Ukrainas cīņā pret Krieviju gūto pieredzi. Plašāk: Latvija un Ukraina paraksta nodoma vēstuli par sadarbību reģionāla kiberdrošības centra izveidē Ukrainā.

Foto: Aizsardzības ministrija

19. februārī Ukrainā, Kijevā, pasākumā Kyiv International Cyber Resilience Forum 2026 CERT.LV eksperts Mārtiņš Savickis vadīja vienas dienas Draudu medību semināru foruma apmeklētājiem un uzstājās ar prezentāciju "Threat Hunting in Latvia: Proactive Defense of Critical Infrastructure" par draudu medībām un to rezultātiem Latvijā. Forumu jau otro gadu pēc kārtas finansiāli un saturiski atbalstīja Aizsardzības ministrija un CERT.LV. Plašāk: **Noslēdzies Latvijas atbalstītais Kijivas starptautiskais kibernoturības forums**.

3.5. IT sistēmu drošības testi un pikšķerēšanas uzbrukumu simulācijas kampaņas

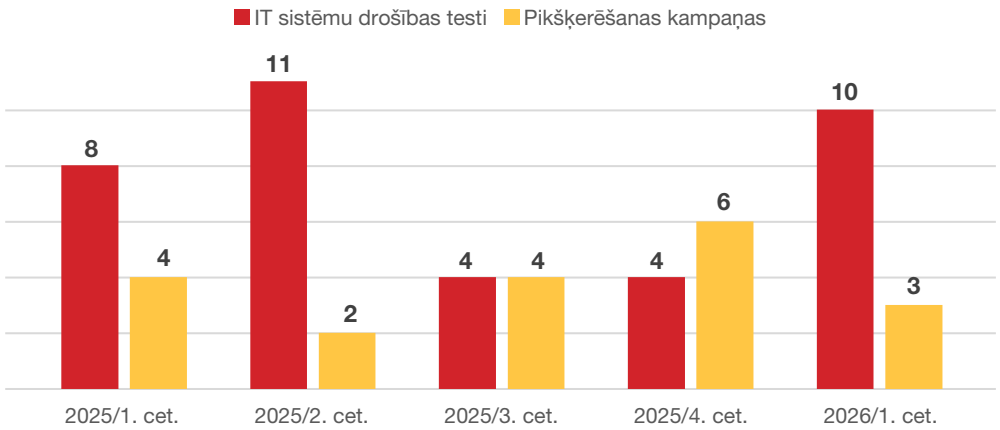
IT sistēmu drošības testi

CERT.LV 2026. gada 1. ceturksnī veica **10** IT sistēmu drošības testus, kuru gaitā identificētas kopskaitā **22** ievainojamības, tostarp **7** no tām būtiskas , kas, pateicoties veiktajiem drošības testiem, jau ir novērstas.

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

CERT.LV nodrošina:

- tīkla drošības analīzi;
- programmatūras ievainojamību novērtējumu;
- web lietotņu drošības novērtējumu;
- IT infrastruktūras ievainojamību novērtēšanu;
- konsultācijas un ieteikumus par drošības uzlabošanu.



12. attēls. IT sistēmu testi un pikšķerēšanas uzbrukumu simulācijas

Pikšķerēšanas uzbrukumu simulācijas kampaņas

Pārskata periodā veiktas **3 pikšķerēšanas uzbrukumu simulācijas kampaņas**, lai apmācītu un veicinātu organizāciju darbinieku spējas identificēt potenciāli riskantus uzvedības modeļus, atpazīt un novērst kiberapdraudējumus un informācijas noplūdi. Šo kampaņu ietvarā tika nosūtītas **912 e-pasta vēstules**.

Pikšķerēšanas uzbrukumu simulācijas palīdz būtiski stiprināt organizāciju aizsardzību pret sociālās inženierijas uzbrukumiem, tādā veidā mazinot cilvēciskā faktora riskus.

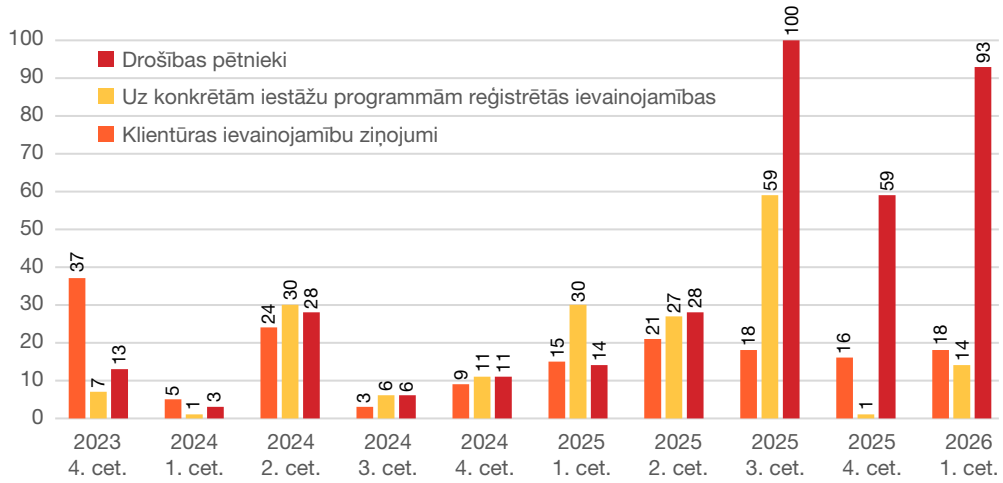
3.6. Ievainojamību ziņošanas platforma (CVD)

CVD platforma 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.

CVD platformā 2026. gada 1. ceturkšņa beigās kopumā reģistrēti:

- **166 drošības pētnieki** (skaits pieauga par 18);
- **14 aktīvas iestāžu programmas** (jaunpienācējs – Valsts i eņēmumu dienests);
- **541 ievainojamību ziņojums** (pieaugums par 107), tostarp:
  - ✓ **355** CERT.LV klientūras ievainojamības (pieaugums par 93);
  - ✓ **186** uz konkrētām iestāžu programmām reģistrētās ievainojamības (pieaugums par 14).

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



13. attēls. CVD: Drošības pētnieku un ievainojamību ziņojumu pieauguma tendences

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 (turpmāk OT) drošības pakalpojumu līgumus.

OT sistēmu drošības veicināšana notiek trijos galvenajos virzienos: **sistēmu uzraudzība un anomāliju identifikācija, drošības testu veikšana, incidentu risināšana**.

- Sistēmu uzraudzības ietvaros CERT.LV ir uzstādījusi piecus OT tīkla datu plūsmas uzraudzības sensorus, kā arī notiek aktīvi sagatavošanās darbi to paplašināšanai. Paralēli iekšējo OT tīklu komunikāciju monitorēšanai, tiek veiktas darbības nepārtrauktai Latvijas IP adresācijas tīklu uzraudzībai ar mērķi identificēt publiski eksponētas sistēmas, apzināties 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 sistēmu noturībā pret kiberuzbrukumiem ir vērtējama kā atbilstoša ar nemainīgu tendenci pilnveidoties. 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

Veicinot izpratni un stiprinot lietotāju, tostarp organizāciju darbinieku zināšanas un prasmes kiberdrošības jomā, CERT.LV eksperti 2026. gada 1. ceturksnī kopumā **65** pasākumos un aktivitātēs izglītoja **13 309** dalībniekus. Tas ir attiecīgi par 32 pasākumiem un 3 104 dalībniekiem vairāk nekā tajā pašā periodā pērn.

CERT.LV 2026. gada 1. ceturksnī:

- organizēja vebināru IT speciālistiem **"Efektīva Windows ugunsmūra pārvaldība"**, kura laikā CERT.LV eksperti skaidroja, kā pareizi konfigurēt Windows ugunsmūri korporatīvajā vidē, izmantojot grupu politikas (GPO), lai efektīvi aizsargātu gala iekārtas arī ārpus organizācijas tīkla un mazinātu kiberdrošības riskus. Slaidi no vebināra pieejami tīmekļvietnē **cert.lv**;
- organizēja IT drošības semināru **"Esi drošs!"** kopumā (klātienē un tiešsaistē) pulcējot vairāk nekā 500 dalībniekus. Seminārs norisinājās "Digitālā nedēļa Latvijā 2026" ietvaros, tajā tika aplūkoti praktiski un aktuāli jautājumi, kas saistīti ar NKDL subjektu reģistrāciju, rīcību kiberdrošības incidenta gadījumā, kā arī sniegts ieskats draudu medību norisē, uzņēmuma darbinieku pikšķerēšanas testos, 2025. gadā biežāk novērotajos "kiberlaikapstākļos", kā arī ievainojamību atklāšanas procesos. Ieraksts un slaidi no semināra pieejami tīmekļvietnē **cert.lv**;
- rīkoja tālākizglītības semināru pedagogiem , kas notika sadarbībā ar LIKTA "Digitālā nedēļa Latvijā 2026" ietvaros. Pasākuma mērķis bija pārrunāt aktuālo kiberdrošības jomā, kā arī izspēlēt un sagatavot dalībniekus kiberizmeklēšanas spēles "Atrodi hakeri Livonijas vidusskolā" vadīšanai pamatskolas vecāko klašu un vidusskolas skolēniem.

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

5. Pārskats par LIA Drošāka interneta centra ZL darbību

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.01.2026. līdz 31.03.2026. ir saņēmusi un izvērtējusi **340** ziņojumus. No tiem **101** ziņojuma saturā ir konstatēti bērnu seksuālu izmantošanu atainojoši materiāli, **14** gadījumos konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, **19** ziņojumos konstatēta personas goda un cieņas aizskaršana, **4** ziņojumi saņemti par naida runu un **5** ziņojumos konstatēti vardarbīgi materiāli. Par finanšu krāpšanas mēģinājumiem internetā saņemti **48** ziņojumi, **117** ziņojumu saturs nav bijis pretlikumīgs, **32** gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti **22** ziņojumi par naida runu un bērnu seksuālu izmantošanu atainojošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. **62** ziņojumi par bērnu seksuālu izmantošanu atainojošiem 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 **22** ziņojumiem par bērnu seksuālu izmantošanu atainojošiem materiāliem **20** ziņojumu saturs ir dzēsts no publiskas aprites internetā un **2** ziņojumi atrodas dzēšanas procesā.

Drošības trauksmes ziņojumu dinamika CERT.LV SOC klientu infrastruktūrā

Ziņojumi	Jan-26	Feb-26	Mar-26	1. cet.
Erotisks/pornogrāfisks saturs bez izvietotiem brīdinājumiem	6	3	5	14
Pedofilija/mazgadīgo prostitūcija/ bērnu seksuālu izmantošanu saturoši materiāli	40	27	34	101
Vardarbīga rakstura materiāli	1	3	1	5
Cieņas/goda aizskaršana	7	10	2	19
Naida kurināšana/rasisms	0	1	3	4
Finanšu krāpšana	20	9	19	48
Konsultācijas/padomi	10	11	11	32
Citi	38	49	30	117
KOPĀ:	122	113	105	340

Ziņojumi nosūtīti Valsts policijai	9	3	10	22
Ziņojumi nosūtīti INHOPE asociācijai	22	21	22	65
KOPĀ NOSŪTĪTI IZSKATĪŠANAI:	31	24	32	87

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