2026 C3

SITUĀCIJA LATVIJAS KIBERTELPĀ

PERIODS: 01.07.2026. - 30.09.2026.

CERT.LV
Kiberincidentu novēršanas institūcija

Latvijas Universitātes
Matemātikas un informātikas institūts

Aizsardzības ministrija

Kopsavilkums

2026. gada 3. ceturksnī Latvijas kibertelpā pieauga kiberapdraudējumu intensitāte un incidentu radītā ietekme. Uzbrucēji arvien aktīvāk izmantoja sistēmu ievainojamības, kompromitēja digitālās identitātes un izraisīja datu noplūdes. Apdraudējumu vidi raksturoja arī automatizēti uzbrukumi un sociālās inženierijas metodes. Mākslīgais intelekts (MI) ļāva uzbrucējiem ātrāk īstenot uzbrukumus un veidot pārliecinošākas krāpšanas shēmas. Vienlaikus saglabājās ģeopolitiski motivētu kiberuzbrukumu draudi.

Kiberapdraudējumu apjoms turpināja pieaugt. Pārskata periodā identificēto apdraudēto iekārtu skaits sasniedza 1,4 miljonus - par 250 % vairāk nekā 2026. gada 2. ceturksnī un par 123 % vairāk nekā attiecīgajā periodā pērn. Pieaugumu noteica gan faktiskie apdraudējumi, gan izmaiņas datu avotos. Vienlaikus pieauga CERT.LV Drošības operāciju centra (turpmāk tekstā SOC) reģistrēto trauksmju skaits, turklāt augsta līmeņa un kritisko trauksmju pieaugums bija ievērojami straujāks nekā trauksmju kopējais skaits. Šī dinamika norāda uz paaugstinātu risku informācijas sistēmu konfidencialitātei, integritātei un pieejamībai un nepieciešamību pastiprināti uzraudzīt iespējamos apdraudējumus.

CERT.LV manuāli apstrādāja 785 kiberincidentus – kas ir būtiski vairāk nekā iepriekšējā ceturksnī un pērnā gada attiecīgajā periodā. Lielais krāpšanas gadījumu īpatsvars incidentu kopskaitā apliecina, ka lietotāju kiberhigiēna un spēja atpazīt krāpšanas mēģinājumus joprojām ir būtiski kiberdrošības priekšnoteikumi.

Būtiskākie apdraudējumi bija piekļuves datu kompromitēšana, pikšķerēšana un internetā pieejamu sistēmu ievainojamību izmantošana. Turpinājās finansiāli motivētu grupējumu kiberuzbrukumi. Apjoma ziņā dominēja krāpšana, kas skāra visplašāko iedzīvotāju loku. Savukārt potenciālās ietekmes ziņā būtiskus draudus joprojām rada citu valstu atbalstītu kiberuzbrucēju grupējumi (APT). Krievija joprojām ir galvenais kiberdraudu avots Latvijai. Ar ģeopolitisko situāciju un Latvijas atbalstu Ukrainai saistītie pakalpojumatteices (DDoS) uzbrukumi un haktīvistu aktivitātes turpina pārbaudīt valsts digitālo pakalpojumu noturību. Šo faktoru kopums īpaši apdraud valsts iestādes, pašvaldības, kritisko infrastruktūru un operacionālo tehnoloģiju (turpmāk tekstā OT) vadības sistēmas.

Pārskata periodā apjomīgākais un nozīmīgākais incidents bija kiberuzbrukums VAS "Ceļu satiksmes drošības direkcija", kurā tika ietekmēti aptuveni 1,2 miljonu fizisko un 200 tūkstošu juridisko personu dati, radot datu konfidencialitātes pārkāpumu plašā mērogā. Šis un citi pēdējo mēnešu notikumi izgaismoja būtiskus trūkumus iestāžu un uzņēmumu kiberdrošības pārvaldībā, uzsverot nepieciešamību savlaicīgi identificēt un novērst sistēmu ievainojamības.

Ar Krieviju saistīti grupējumi turpināja testēt OT vidi, tostarp enerģētikas un rūpnieciskās vadības sistēmas. Latvija stiprina apsteidzošas spējas novērst apdraudējumus. CERT.LV šajā jomā jau novērsusi vairākus desmitus ievainojamību, kuru izmantošana varēja izraisīt incidentus.

Gatavojoties 15. Saeimas vēlēšanām, CERT.LV pārbaudīja vēlēšanu norisē iesaistītās informācijas sistēmas, veica draudu medības, stiprināja iesaistīto iestāžu noturību un ieviesa papildu aizsardzības pasākumus.

CERT.LV stiprināja preventīvo aizsardzību un paplašināja kiberdraudu atklāšanas spējas. DNS ugunsmūris bloķēja 4,7 miljonus pieprasījumu piekļūt krāpnieciskām vietnēm – tas ir 12 reižu vairāk nekā attiecīgajā periodā pērn. Vienlaikus CERT.LV SOC paplašināja centralizēto kiberdrošības uzraudzību un apdraudējumu atklāšanu reāllaikā. Uzraudzīto Nacionālā kiberdrošības likuma subjektu skaits palielinājās par 20 %, savukārt to gala iekārtu skaits par 25 %. Plašāks uzraudzības tvērums uzlabo iespējas savlaicīgi identificēt potenciālos apdraudējumus. Savukārt Koordinētas ievainojamību ziņošanas platformā (CVD) reģistrēti 927 ziņojumi – lielākais ziņojumu skaits kopš tās ieviešanas. Līdztekus tehnisko spēju attīstībai CERT.LV paplašināja izglītošanas darbu, kiberdrošības apmācībās sasniedzot vairāk nekā 5 600 dalībnieku.

Kopsavilkums

Kiberdraudiem kļūstot intensīvākiem un sarežģītākiem, Latvijas kibernoturībai būtiska ir savlaicīga risku apzināšana, preventīva aizsardzība un regulāra lietotāju izglītošana. Organizācijām jāpārzina savas IT sistēmas, savlaicīgi jānovērš ievainojamības, jāstiprina piekļuves kontrole un jāuzrauga izmantoto ārpakalpojumu drošība. Šo pasākumu efektivitāti nosaka koordinēta sadarbība un spēja laikus reaģēt uz apdraudējumiem.

Apvienojot testēšanu, ikdienas aizsardzību, apdraudējumu analīzi un kiberdrošības kopienas zināšanas, CERT.LV turpina stiprināt Latvijas kibernoturību. Katra savlaicīgi novērsta ievainojamība un apturēts apdraudējums padara Latviju par grūtāku mērķi kiberuzbrucējiem.

CERT.LV galvenie rādītāji 2026. gada 3. ceturksnī

785 | +17%

Manuāli apstrādāto kiberincidentu skaits 2026.-3.CET. vs 2025.-3.CET.

1,4 milj. | +123%

Identificēto apdraudēto iekārtu skaits 2026.-3.CET. vs 2025.-3.CET.

2 953 | +153%

Automatizēti identificētas un apturētas krāpnieciskas kampaņas 2026.-3.CET. vs 2026.-2.CET.

4,7milj. | +1086%

CERT.LV DNS ugunsmūra bloķētie pieprasījumi ļaunprātīgām vietnēm 2026.-3.CET. vs 2025.-3.CET.

126 | +20%

CERT.LV SOC klientu skaits (kopskaits uz 30.09.2026.)

71 243 | +25%

Gala iekārtu skaits ar CERT.LV SOC nodrošinātu redzamību (kopskaits uz 30.09.2026.)

909 | +47%

CERT.LV SOC veikta trauksmju manuālā apstrāde un lietu izveide, tostarp atklāti 19 incidenti (kopskaits uz 30.09.2026.)

Pabeigtas 6 draudu medību operācijas, un 16 – procesā

(dati par 2026.g. 3.CET)

2 657

e-pasti nosūtīti pikšķerēšanas uzbrukumu simulācijās: atvērti 55%; no tiem 38% lietotāju ievadīja datus. (dati par 2026.g. 3.CET.)

927 | +36%

CVD platformā reģistrētie ievainojamību ziņojumi (kopskaits uz 30.09.2026.)

41 | +58%

CERT.LV ekspertu īstenotās izglītojošās aktivitātes/pasākumi kiberkopienā 2026.-3.CET. vs 2025.-3.CET.

5 652 | +32%

Sasniegtās auditorijas skaits CERT.LV ekpertu īstenotās aktivitātēs/pasākumos 2026.-3.CET. vs 2025.-3.CET.

Satura rādītājs

Kopsavilkums 1

CERT.LV galvenie rādītāji 2026. gada 3. ceturksnī 3

1. Latvijas kibertelpas aina skaitļos 5

2. Draudu tendences kiberuzbrukumu veidos 8

- 2.1. Uzbrukumu vektori, draudu dinamika 8
- 2.2. Nozaru specifiskie riski 10
- 2.3. Secinājumi un ieteikumi 10

3. CERT.LV pakalpojumi: ikdienas aizsardzība, testēšana un izglītošana 12

- 3.1. DNS ugunsmūris 12
- 3.2. Apdraudējumu agrās brīdināšnas sistēma (ABS) 13
- 3.3. Drošības operāciju centrs (SOC) 13
- 3.4. IT sistēmu drošības testi un pikšķerēšanas uzbrukumu simulācijas kampaņas 17
- 3.5. Kiberdrošības draudu medību operācijas 17
- 3.6. Koordinētas ievainojamību ziņošanas platforma (CVD) 18
- 3.7. Operacionālo tehnoloģiju (OT) drošība 19
- 3.8. Izglītošana – lekcijas un dalība kiberdrošības pasākumos 20

4. Pārskats par LIA Drošāka interneta centra ZL darbību 21



1. Latvijas kibertelpas aina skaitļos

Draudu intensitāte Latvijas kibertelpā

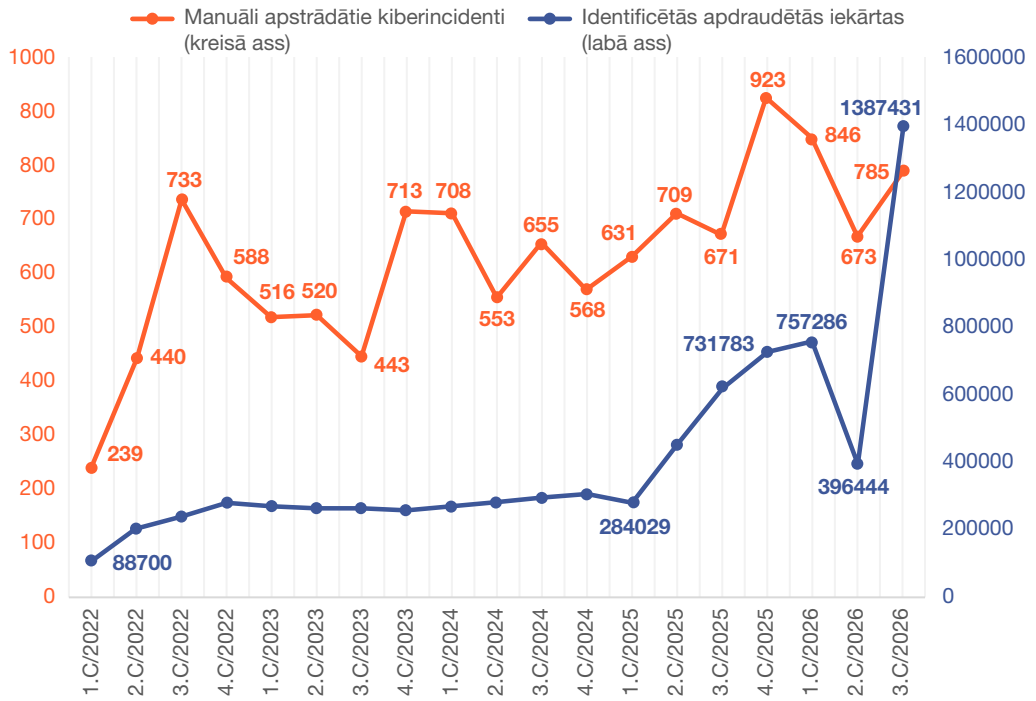
2026. gada 3. ceturksnī Latvijas kibertelpā CERT.LV identificēto apdraudēto iekārtu skaits sasniedza 1 387 431 – par 250 % vairāk nekā 2. ceturksnī un par 123 % vairāk nekā pirms gada.

Pārskata periodā statistikas pieaugumu noteica gan potenciāli apdraudēto iekārtu skaita palielināšanās, gan jaunu datu avotu (*feed*) izmantošana, kas paplašina identificējamo iekārtu loku. Pieaugumu daļēji ietekmēja Microsoft DCU CTIP *Infected feed* datu plūsmas atjaunošana pēc īslaicīga pārtraukuma 2. ceturksnī. Līdz ar to apdraudēto iekārtu skaita pieaugums atspoguļo gan faktiskos apdraudējumus, gan izmaiņas datu avotos.

Apdraudējuma līmeni palielina plaši izplatītas ievainojamības populārās tīkla iekārtās, publiski pieejami pārvaldības servisi, novecojušas programmatūras versijas un kavēta drošības atjauninājumu uzstādīšana, kā arī kiberuzbrucēju aktīvāka automatizēta skenēšana ievainojamu sistēmu meklēšanai.

Mākslīgā intelekta (MI) rīki būtiski paātrina uzbrukumu automatizāciju. Ievainojamību izmantošanas rīki nereti kļūst pieejami drīz pēc informācijas par ievainojamības vai programmatūras ielāpu publiskošanas, tādēļ organizācijām jāspēj ievainojamības novērst arvien īsākā laikā.

Pārskata periodā CERT.LV SOC reģistrēto augsta līmeņa un kritisko drošības trauksmju skaits pieauga ievērojami straujāk nekā kopējais trauksmju apjoms. Šī dinamika norāda uz paaugstinātu risku informācijas sistēmu konfidencialitātei, integritātei un pieejamībai, kā arī nepieciešamību pievērst pastiprinātu uzmanību iespējamiem apdraudējumiem.



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

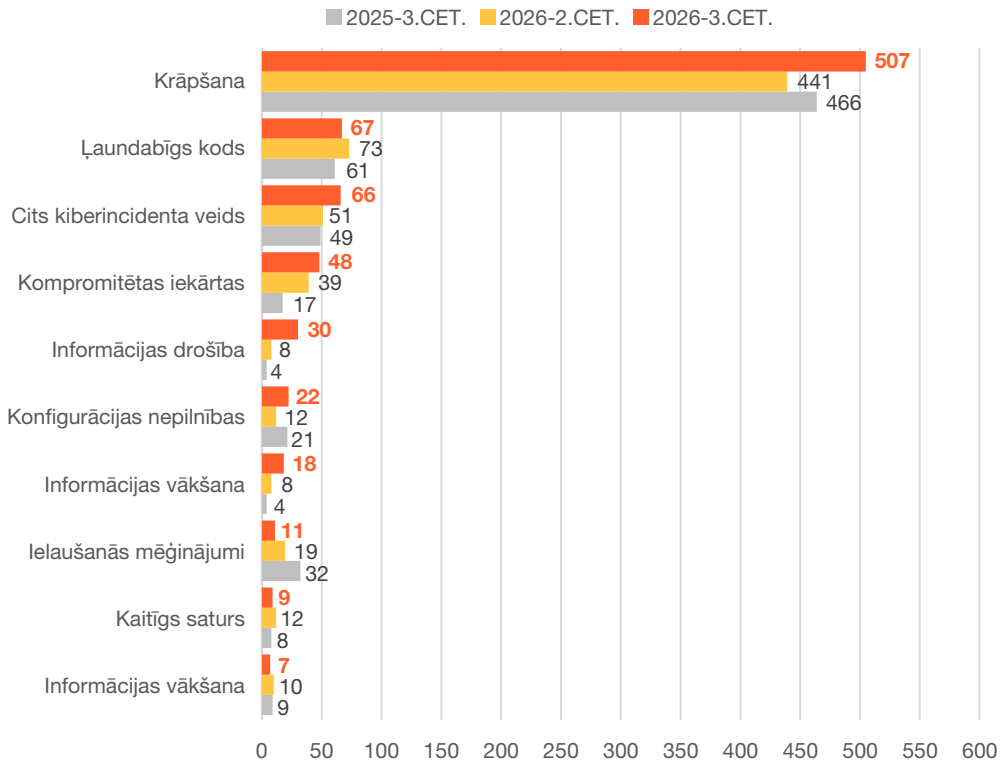
2026. gada 3. ceturksnī Latvijas kibertelpā kopumā reģistrēti 785 manuāli apstrādāti kiberincidenti – par 16,6 % vairāk nekā 2. ceturksnī un par 17 % vairāk nekā pērn attiecīgajā periodā.

Reģistrēto kiberincidentu skaits ir trešais lielākais radītājs līdz šim. Šī dinamika norāda, ka lietotāju kiberhigiēna un spēja atpazīt krāpšanas mēģinājumus joprojām ir būtiski kiberdrošības priekšnoteikumi.

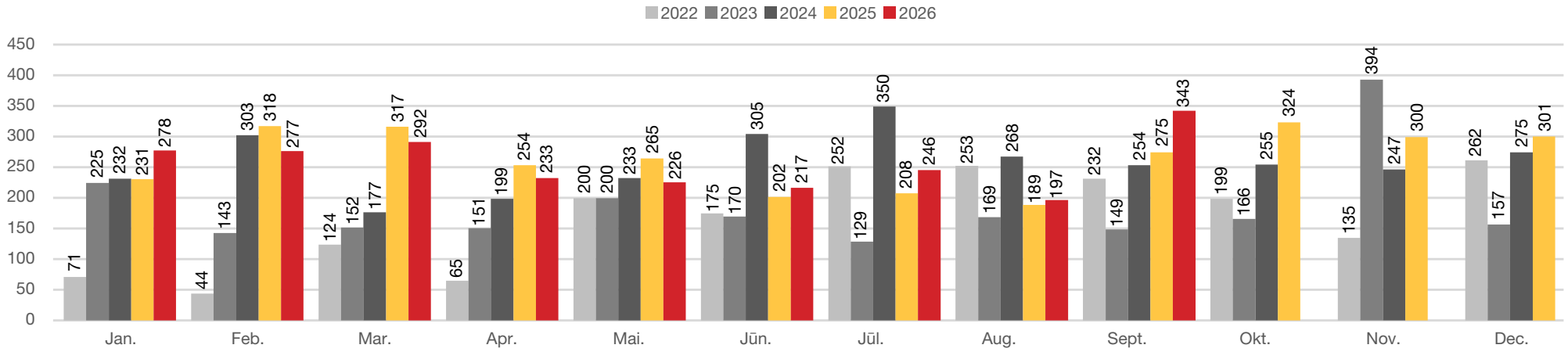
Šā gada pirmajos deviņos mēnešos CERT.LV DNS ugunsmūris vidēji mēnesī bloķēja 1,08 miljonus lietotāju veiktu pieprasījumu ļaunprātīgām vietnēm. Septembrī bloķēto pieprasījumu skaits sasniedza rekordu – aptuveni 1,7 miljonus. Šie dati apliecina DNS ugunsmūra nozīmi lietotāju aizsardzībā, preventīvi identificējot un bloķējot piekļuvi ļaunprātīgām vietnēm.

Vienlaikus CERT.LV apsteidzoši identificēja un novērsa 2 953 aktīvas krāpnieciskas kampaņas - par 153% vairāk nekā iepriekšējā ceturksnī – pirms tās masveidā sasniedza lietotājus un radīja finansiālus zaudējumus, apliecinot automatizētas aizsardzības pieaugošu nozīmi.

"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.



3. attēls. Kiberincidentu veidu dinamika



2. attēls. Kiberincidentu dinamika pa mēnešiem

Identificētās apdraudētās iekārtas

Krāpšana dominē, veidojot gandrīz 2/3 no CERT.LV reģistrētajiem incidentiem. To skaits pieauga par 15 % salīdzinājumā ar iepriekšējo ceturksni un par 9 % salīdzinājumā ar attiecīgo periodu pērn.

Informācijas drošības incidentiem bija straujākais relatīvais pieaugums – par 275 % salīdzinājumā ar iepriekšējo ceturksni un par 650 % salīdzinājumā ar attiecīgo periodu pērn.

Kompromitētu iekārtu skaits pieauga par 23 % salīdzinājumā ar iepriekšējo ceturksni un par 182 % salīdzinājumā ar attiecīgo periodu pērn.

Ielaušanās mēģinājumu skaits samazinājies attiecīgi par 42 % salīdzinājumā ar iepriekšējo ceturksni un par 66 % salīdzinājumā ar attiecīgo periodu pērn.

Pieejamības traucējumi veido 0,9 % no kopējā incidentu skaita. To nelielais īpatsvars var liecināt par DDoS aizsardzības pasākumu efektivitāti.

Izplatītākie ļaunatūru tipi

- **Datu zādzības ļaunatūras**
- **Botu tīklu ļaunatūras**
- **Attālinātās kontroles trojāni datu izgūšanai un infrastruktūras kompromitēšanai**

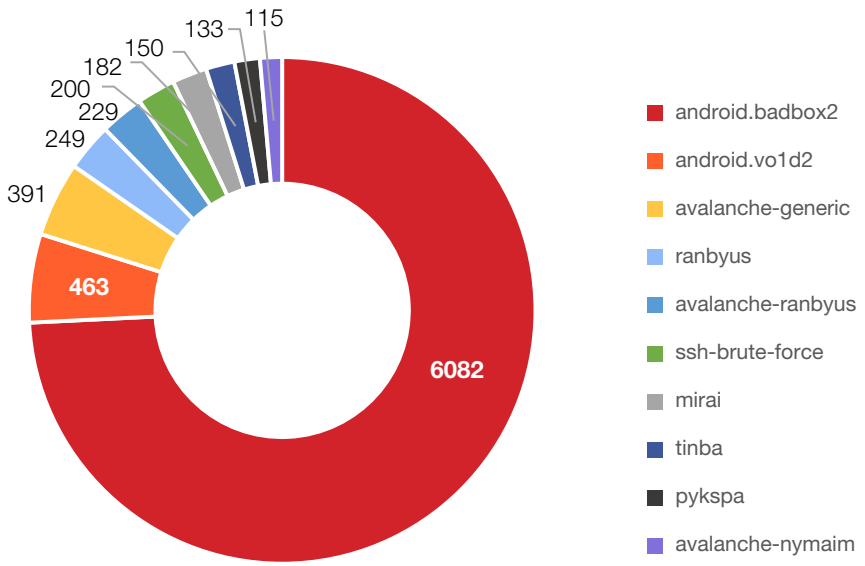
Datu zādzības ļaunatūras (*infostealears*) iegūst piekļuves datus no tīmekļa pārlūkiem vai nešifrētiem failiem. Tās izplata ar ļaunprātīgiem pārlūku paplašinājumiem vai pikšķerēšanas e-pasta vēstulei pievienotiem izpildfailiem.

TOP 10 ļaunatūras

2026. gada 3. ceturksnī biežāk konstatēto ļaunatūru izplatība liecina par masveidīgiem, automatizētiem un ilgstošiem apdraudējumiem. Jau vairākus ceturkšņus dominē ļaunatūra “Android.badbox2”, lai gan pārskata periodā tās izplatība salīdzinājumā ar iepriekšējo ceturksni samazinājusies par 4 %.

“Android.badbox2” apdraud Android ierīces, iesaistot tās botu tīklā. Galvenie riski ir piekļuves datu zādzība, inficētu ierīču attālināta kontrole un izmantošana turpmākos kiberuzbrukumos. Savukārt lietotāji un organizācijas var nezināt, ka viņu ierīces ir iesaistītas botu tīkla darbībā.

Pārējās desmit izplatītāko ļaunatūru sarakstā iekļautās ļaunatūras veido mazāku daļu, tomēr atspoguļo uzbrukumu veidu daudzveidību un rada papildu riskus ierīču drošībai.



4. attēls. TOP 10 ļaunatūras (skaits; 2026-3.CET.)

2. Draudu tendences kiberuzbrukumu veidos

2.1. Uzbrukumu vektori, draudu dinamika

Pārskata periodā iezīmējas piecas savstarpēji saistītas tendences, kas raksturo gan izmantotās uzbrukumu metodes, gan incidentu pieaugošo ietekmi uz organizācijām un iedzīvotājiem.

1. Datu noplūžu ietekme pieaug



Pārskata periodā VAS "Ceļu satiksmes drošības direkcija" (CSDD) piedzīvoja liela mēroga kiberincidentu, kurā tika skarti aptuveni 1,2 miljonu fizisko un 200 tūkstošu juridisko personu dati. Incidents apliecina, ka līdzās pakalpojumu pieejamības traucējumiem būtisks Latvijas kiberdrošības risks ir arī datu konfidencialitātes apdraudējums.

CSDD datu noplūdi veicināja nepilnības kiberdrošības pārvaldībā, tostarp nepilnīga drošības pārbaužu aptvere, nepietiekama tīkla aizsardzība, nepilnības programmatūras izstrādē, kā arī daudzfaktoru autentifikācijas (turpmāk tekstā MFA) trūkums. CERT.LV palīdzēja apturēt kiberuzbrukumu, veica tehnisko izmeklēšanu, analizēja noplūdušos datus un identificēja uzbrukumā izmantotos piekļuves kanālus.

CERT.LV brīdina, ka incidenta radītās sekas var būt ilgstošas, pat ja pats incidents jau ir novērsts. Uzbrucēji noplūdušos datus var izmantot personalizētai krāpšanai, identitātes ļaunprātīgai izmantošanai un sociālās inženierijas kampaņām. Plaša mēroga datu noplūdes var arī mazināt sabiedrības uzticēšanos digitālajiem pakalpojumiem.

Iedzīvotājiem jābūt īpaši piesardzīgiem, saņemot personalizētus zvanus, īsziņas un e-pastus. Papildu aizsardzībai jāizmanto MFA, kā arī ieteicams izmantot CERT.LV DNS ugunsmūri un tā mobilo lietotni, kas bloķē identificētās krāpnieciskās vietnes un zvanus. Organizācijām jāstiprina piekļuves kontrole, jāievieš MFA, jāuzrauga žurnālfaili, sistemātiski jāpārvalda programmatūras versijas un ievainojamības.

2. Publiski pieejamu sistēmu ievainojamības - būtisks sākotnējās piekļuves risks



Uzbrucēji arvien aktīvāk meklē internetā pieejamas, nepietiekami aizsargātas sistēmas. Šī tendence bija īpaši izteikta pārskata periodā. Īpaši apdraudētas ir VPN vārtejas, ugunsmūri, maršrutētāji, tīmekļa un pārvaldības servisi, e-pasta sistēmas un attālās piekļuves risinājumi (RDP). To kompromitēšana ļauj uzbrucējiem iekļūt dziļāk organizācijas infrastruktūrā, piekļūt datiem un traucēt pakalpojumu pieejamību.

Pārskata periodā reģistrētais kiberincidents Patērētāju tiesību aizsardzības centra (PTAC) pārziņā esošajā informācijas sistēmā **uzskatāmi parādīja riskus, ko rada novecojušas satura vadības sistēmas un savlaicīgi nenovērstas ievainojamības**. Izmantojot šīs internetā pieejamās sistēmas ievainojamību, uzbrucējs ieguva 697 komersantu pārstāvju un 34 PTAC amatpersonu kontaktinformāciju.

Pieaug arī ievainojamību automatizēta meklēšana un masveida izmantošana. Šo risku ilustrē incidents LMT grupas uzņēmumā "TSC", kas par uzbrukuma mērķi kļuva nevis apzinātas izvēles rezultātā, bet gan tāpēc, ka uzbrucējs ar automatizētiem rīkiem meklēja ievainojamas sistēmas. Tas nozīmē, ka **par mērķi var kļūt jebkura nepietiekami aizsargāta, internetā pieejama sistēma** neatkarīgi no organizācijas lieluma vai nozares.

3. Digitālā identitāte kļūst par būtisku drošības perimetru



Pieaug uzbrukumi lietotāju kontiem un to piekļuves datiem – parolēm, piekļuves un API atslēgām, sesiju marķieriem, servisa kontiem un citiem autentifikācijas datiem.

Uzbrucēji izmanto zagtus piekļuves datus, MFA apiešanas paņēmienus un nepietiekami aizsargātus servisa un API kontus, lai sistēmās darbotos kā leģitīmi lietotāji. Risku pastiprina nepilnīga piekļuves tiesību pārvaldība, nedroša sensitīvu datu

glabāšana koda repozitorijos, nepietiekama programmatūras un koda versiju kontroles sistēmu aizsardzība, kā arī nepārbaudīta MI ģenerēta koda izmantošana. Līdzās tīkla un gala iekārtu aizsardzībai arvien nozīmīgāka kļūst sistemātiska digitālo identitāšu un piekļuves tiesību pārvaldība.

4. Krāpšana saglabā līderpozīciju, sociālā inženierija pastiprina pikšķerēšanas risku



Krāpšana joprojām ir izplatītākais kiberincidentu veids Latvijā. Krāpšanas kampaņas norisinās nepārtraukti un plašā mērogā, apvienojot dažādas metodes un saziņas kanālus. Šī pieeja ļauj sasniegt plašu auditoriju un pielāgot krāpšanas scenārijus dažādām situācijām.

Pārskata periodā krāpnieki centās maldināt iedzīvotājus, izliekoties par uzticamu institūciju, uzņēmumu un digitālo pakalpojumu sniedzēju pārstāvjiem. Izmantojot lietotāju uzticēšanos un radot steidzamības sajūtu, viņi centās iegūt autentifikācijas kodus, internetbankas piekļuves datus, personas datus un maksājumu karšu informāciju. Krāpšanas kampaņās aktīvi tika izmantotas e-pasta vēstules, īsziņas, tālruņa zvani, viltotas tīmekļvietnes un reklāmas platformas. Dominēja CSDD tematika un e-pasta piekļuves datu pikšķerēšana.



5. attēls. Izplatītākās sociālās inženierijas un pikšķerēšanas kampaņas (procentuālā daļa no kopskaita; 2026-3.CET.)

Būtisku apdraudējumu radīja arī datu zādzības ļaunatūra, viltus programmatūras atjauninājumi un ļaunprātīgi pārlūku paplašinājumi. Uzbrukumos plaši izmantoja sociālo inženieriju, mudinot lietotājus pašiem veikt krāpniekiem vajadzīgās darbības. Vairāk nekā puse CERT.LV SOC reģistrēto incidentu bija saistīti ar "ClickFix" uzbrukumiem, kuros lietotājus maldināja ar viltus "CAPTCHA" pārbaudēm kompromitētās tīmekļvietnēs.

Finanšu nozares asociācijas dati liecina, ka 2026. gada pirmajos deviņos mēnešos finanšu iestādes novērsušas naudas izkrāpšanas mēģinājumus 16,6 miljonu eiro apmērā - par 73 % vairāk nekā attiecīgajā periodā pērn. Savukārt banku klientiem, pašiem apstiprinot maksājumus, izkrāpti 10 miljoni eiro - par 11 % vairāk nekā attiecīgajā periodā pērn. Novērsto krāpšanas mēģinājumu apmērs apliecina savlaicīgas klientu apkrāpšanas mēģinājumu atklāšanas nozīmi. Līdztekus finanšu un citu nozaru uzņēmumu ieviestajiem aizsardzības risinājumiem būtiska ir arī iedzīvotāju prasme atpazīt krāpšanu. Tomēr izkrāptās summas pieaugums norāda, ka risks saglabājas augsts. Jārēķinās, ka krāpnieki turpinās pielāgot savas metodes un meklēs jaunus veidus, kā izkrāpt naudu. Tāpēc ikvienam jāsaglabā modrība.

5. Ģeopolitiski motivēti draudi saglabājas



Ģeopolitiskās situācijas ietekme Latvijas kibertelpā saglabājas. Būtiskākie draudi saistīti ar valstiski atbalstītu grupējumu aktivitātēm, haktīvismu un IKT kritiskās infrastruktūras izpēti.

Ar Latvijai nedraudzīgām valstīm saistīti grupējumi (APT) turpina izlūkošanas un pikšķerēšanas aktivitātes pret valsts pārvaldi, pašvaldībām un valstij nozīmīgiem uzņēmumiem. Krievija joprojām tiek identificēta kā primārais kiberdraudu avots Latvijai un ir dominējošais valstiskais apdraudējums ar augstu eskalācijas potenciālu. Vienlaikus kiberdraudi jāvērtē plašākā hibrīddraudu kontekstā, kas ietver sabotāžas, informācijas ietekmes un IKT kritiskās infrastruktūras apdraudējuma riskus.

DDoS uzbrukumi un haktīvistu aktivitātes joprojām tiek izmatotas kā ģeopolitiskā spiediena instruments. To intensitāte var pieaugt pēc politiskiem notikumiem vai publiskiem paziņojumiem kontekstā ar Latvijas atbalstu Ukrainai.

Līdzšinējie aizsardzības pasākumi lielākoties ir ļāvuši izvairīties no ilgstošas vai būtiskas ietekmes uz pakalpojumu pieejamību, taču uzbrukumu risks saglabājas. Latvijai jāturpina stiprināt aizsardzību un gatavību dažāda veida kiberapdraudējumiem.

2.2. Nozaru specifiskie riski

Valsts pārvalde, pašvaldības un vēlēšanu infrastruktūra: paaugstināta uzmanība bija sagaidāma saistībā ar 2026. gada 3. oktobrī gaidāmajām 15. Saeimas vēlēšanām Latvijā. Pārskata periodā Latvijai nedraudzīgu valstu atbalstītas uzbrucēju grupas (APT) un organizētās noziedzības grupas turpināja izlūkošanas un pikšķerēšanas aktivitātes, vēršoties pret ministrijām, pašvaldībām un valstij nozīmīgiem uzņēmumiem.

Uzraugot kibertelpu, septembrī CERT.LV SOC pakalpojuma ietvarā tika konstatēts kiberincidents kādas pašvaldības e-pasta serverī. Veicot padziļinātu incidenta analīzi, tika novērota uzbrucēju interese par atslēgvārdiem "velesanas" un "namejs". Šāda aktivitāte norāda uz iespējamību, ka uzbrukums varētu būt politiski motivēts. Ņemot vērā, ka uzbrukums tika apturēts stadijā, kad uzbrucēji veica kompromitēta servera izzināšanu, plaša e-pastu datu noplūde nav notikusi.

Septembrī dažos Latvijas reģionos konstatēti kiberuzbrukumi pašvaldību novērošanas kamerām un ēku viedās vadības elementiem. Tajos novērojama saistība ar Krieviju. Incidentu skaits nebija liels, tomēr to nozīme ir būtiska. Uzbrucēji centušies piekļūt kamerām, mainīt attēlu, veikt digitālu vandālismu vai demonstrēt savus vēstījumus. CERT.LV šos gadījumus nesaista ar vēlēšanu norisi. Tomēr tie liecina, ka pašvaldību viedā infrastruktūra var kļūt par uzbrukuma mērķi reputācijas ietekmēšanai un sabiedrības uzticības graušanai. Tādēļ būtiska ir ne tikai vēlēšanu infrastruktūras aizsardzība, bet arī valsts un pašvaldību tīmekļvietņu, sakaru sistēmu un citu saistīto digitālo pakalpojumu nepārtraukta uzraudzība.

Enerģētika un OT vadības sistēmas: ar Krieviju saistīti APT grupējumi turpināja apzināt OT vidi, īpaši enerģētikas un rūpnieciskās vadības sistēmas. Būtisks risks ir publiski pieejamas vai nedroši konfigurētas OT pārvaldības saskarnes. To kompromitēšana var radīt ne tikai informācijas drošības, bet arī fizisko procesu traucējumu risku. Latvija stiprina apsteidzošas spējas. CERT.LV šajā jomā jau ir novērsusi vairākus desmitus ievainojamību, kuru izmantošana varēja izraisīt incidentus. Organizācijas tiek aicinātas stiprināt atbildīgāku tehnoloģiju ieviešanu un rūpīgāku ārpakalpojumu uzraudzību.

Finanšu sektors: turpinās finansiāli motivētu grupējumu kiberuzbrukumi un krāpšanas kampaņas. Pieaug krāpšanas mēģinājumu skaits, kuros izmanto MI, lai izstrādātu sarežģītākas shēmas un pārliecinošāku saturu.

2.3. Secinājumi un ieteikumi

2026. gada 3. ceturksnī Latvijas kibertelpā pieauga gan kiberapdraudējumu intensitāte, gan incidentu radītā ietekme. Kiberdrošības riskus arvien vairāk nosaka savstarpēji saistītu faktoru kopums: publiski pieejamu sistēmu ievainojamību izmantošana, datu konfidencialitātes apdraudējumi, digitālo identitāšu kompromitēšana, uzbrukumu automatizācija, sociālā inženierija un ģeopolitiski motivēti draudi. MI rīku izmantošana paātrina uzbrukumu sagatavošanu un īstenošanu.

Šo faktoru mijiedarbība palielina apdraudējuma riskus īpaši valsts iestādēm, pašvaldībām un kritiskās infrastruktūras organizācijām, tostarp to izmantotajām OT sistēmām.

Lielais krāpšanas gadījumu īpatsvars incidentu kopskaitā apliecina, ka lietotāju kiberhigiēna un spēja atpazīt krāpšanas mēģinājumus joprojām ir būtiski kiberdrošības priekšnoteikumi. Identificēto apdraudēto iekārtu skaita būtiskais pieaugums norāda uz paaugstinātu risku informācijas sistēmu konfidencialitātei, integritātei un pieejamībai.

Šīs tendences uzsver nepieciešamību stiprināt lietotāju modrību un tehniskās aizsardzības pasākumus, īpašu uzmanību pievēršot savlaicīgai sistēmu atjaunināšanai, ievainojamību novēršanai, apdraudējumu atklāšanai un reaģēšanai uz incidentiem.

Galvenie ieteikumi

Valsts iestādēm, pašvaldībām, kritiskās infrastruktūras organizācijām, kā arī būtisko un svarīgo pakalpojumu sniedzējiem prioritāri ieteicams:

Organizāciju aizsardzība

1. **Ieviest daudzfaktoru autentifikāciju (MFA)**
   Paaugstinātas drošības sistēmu lietotājiem, pamata drošības sistēmu administratoriem un lietotājiem, kuri tām piekļūst attālināti no ārējā tīkla, kā arī visām publiski eksponētām un būtiskām sistēmām.

2. **Pilnībā apzināt savus IT aktīvus**
   Īpaši uzraudzīt internetā pieejamās sistēmas.

3. **Savlaicīgi novērst ievainojamības**
   Maksimāli saīsināt atjauninājumu ieviešanas laiku.

4. **Centralizēti uzkrāt un analizēt žurnālfailus**

5. **Nodalīt administratora kontus no ikdienas lietotāju kontiem**

6. **Ātri identificēt un izolēt kompromitētas sistēmas**
   Nodrošināt šim nolūkam nepieciešamās spējas.

7. **Regulāri pārbaudīt gatavības plānus**
   incidentu reaģēšanai un darbības nepārtrauktībai.

Kritiskā infrastruktūra un OT

Segmentēt rūpnieciskās vadības sistēmas no korporatīvā IT tīkla un pastiprināti uzraudzīt ārpakalpojumu sniedzēju piekļuvi.

Vēlams slēgt piekļuvi novērošanas kameru un viedās vadības iekārtu pārvaldības rīkiem no publiskā interneta. Attālinātas vadības un uzraudzības funkcijas šajās iekārtās jāveic caur iestādes pārvaldītu VPN savienojumu.

Starptautiskā sadarbība

Turpināt informācijas un kiberdraudu izlūkošanas datu (IOC/CTI) apmaiņu ar sabiedrotajiem. Aktīvi piedalīties NATO un ES koordinētajās iniciatīvās.

Sabiedrības informēšana

Regulāri informēt par aktuālajām krāpšanas kampaņām, pikšķerēšanu un sociālās inženierijas paņēmieniem, jo šie apdraudējumi skar visplašāko iedzīvotāju loku.

3. CERT.LV pakalpojumi: ikdienas aizsardzība, testēšana un izglītošana

3.1. DNS ugunsmūris

Latvijā regulāri notiek kampaņveidīgas krāpnieciskas aktivitātes – gan novirzīšana uz viltus vietnēm lietotāja kontu piekļuves datu izkrāpšanai, gan ļaunatūru izplatīšana. CERT.LV proaktīvi monitorē un aptur identificētās krāpnieciskās kampaņas, operatīvi ievietojot kampaņu indikatorus DNS ugunsmūrī.

2026. gada 3. ceturksnī CERT.LV DNS ugunsmūris bloķēja 4,7 miljonus lietotāju veiktu ļaunprātīgu vietņu pieprasījumus – par 89 % vairāk nekā 2. ceturksnī un 12 reižu vairāk nekā pērnā gada attiecīgajā periodā*.

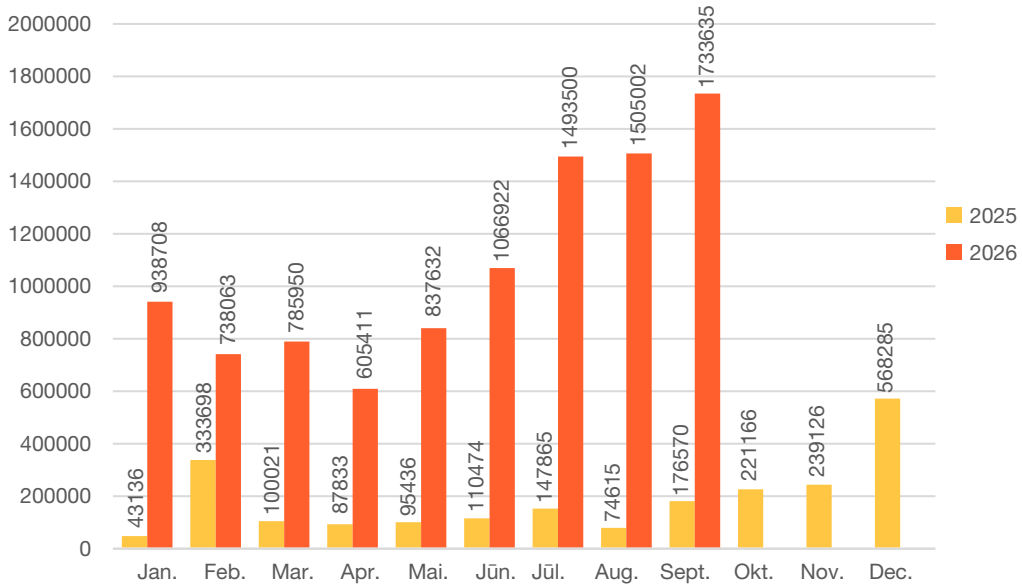
*Statistikā nav iekļauti dati par citu valsts kompetento iestāžu sarakstiem nelikumīga tiešsaistes satura ierobežošanai.

DNS ugunsmūra mobilā lietotne Android un IOS ierīcēs kopš 2024. gada kopumā lejupielādēta 91 854 reizes – pieaugums veido 4 % no kopējā apjoma. Mobilā lietotne pasargā ne tikai no krāpnieciskām kampaņām kibertelpā, bet arī identificētiem viltvāržu zvaniem.

Nozīmīgākās aktīvās aizsardzības epizodes:

- Bloķēti pieprasījumi vietnēm, kas izplatīja “ClickFix” un ”ClearFake” ļaunatūru;
- Bloķēti pieprasījumi vietnēm, kas bija iesaistītas ļaunprātīgu robottīklu darbībā un ļaunprogrammatūras izplatīšanā;
- Bloķēta piekļuve krāpnieciskām kriptovalūtu ieguldījumu platformām, kuru reklamēšanā izmantoti “LSM” un “Jauns.lv” nosaukumi un vizuālā identitāte.

Kiberapdraudējumi ir pastāvīgi un lielākoties finansiāli motivēti. CERT.LV DNS ugunsmūris efektīvi aizsargā lietotājus no pikšķerēšanas lapām, ļaunatūras lejupielādes



6. attēls. CERT.LV DNS ugunsmūra sarakstu bloķētie pieprasījumi ļaunprātīgām vietnēm

vietnēm un krāpnieciskām platformām. Mēģinot piekļūt ļaunprātīgai vietnei, kas iekļauta CERT.LV DNS ugunsmūra bloķēšanas sarakstā (*cert-shield, malware, phishing, high-risk*), lietotājs tiek novirzīts uz drošu brīdinājuma lapu.

Aizsardzību palīdz stiprināt arī iedzīvotāji, pārsūtot krāpnieciskus e-pastus uz cert@cert.lv, par īsziņām un aizdomīgām saitēm “WhatsApp” ziņojot uz numuru 23230444. CERT.LV apkopo saņemtos ziņojumus un iekļauj kaitnieciskos domēna vārdus DNS ugunsmūra bloķēšanas sarakstā. Vairāk informācijas: dnsmuris.lv

3.2. Apdraudējumu agrās brīdināšnas sistēma (ABS)

ABS pakalpojuma ieviešana

ABS ir CERT.LV nodrošināts pakalpojums datu plūsmas anomāliju analīzei un kiberuzbrukumu pazīmju identificēšanai pakalpojuma saņēmēja infrastruktūrā. ABS pakalpojums galvenokārt paredzēts Nacionālās kiberdrošības likuma (NKDL) subjektiem un kritiskās infrastruktūras organizācijām.

ABS pakalpojums ietver nepārtrauktu datu plūsmas anomāliju analīzi un ļaunprogrammatūras aktivitāšu atpazīšanu, brīdinājumu nosūtīšanu par konstatētiem augstas prioritātes kiberapdraudējumiem, regulāru CERT.LV izmantoto kiberapdraudējumu indikatoru atjaunināšanu, kā arī konsultācijas un atbalstu klientiem.

CERT.LV turpina ABS ieviešanu un uzturēšanu, paplašinot pakalpojuma saņēmēju loku atbilstoši NKDL un stiprinot to aizsardzību un noturību pret kiberapdraudējumiem.

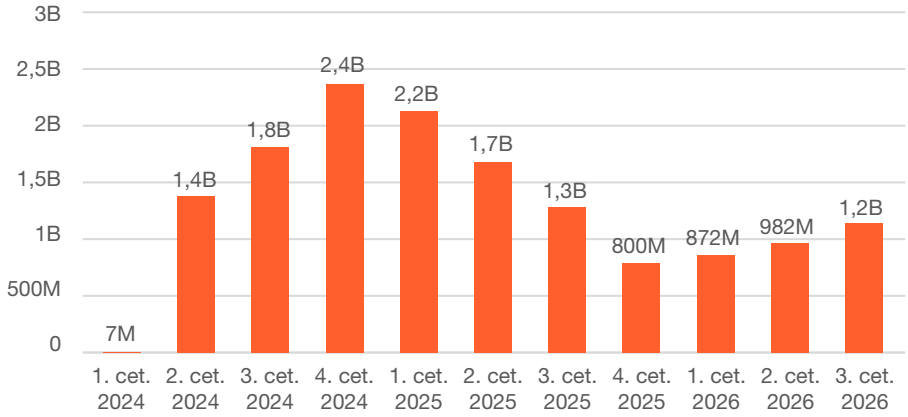
Kiberapdraudējumu un incidentu atklāšana un novēršana

2026. gada 3. ceturksnī ABS reģistrēto trauksmju skaits bija 1,2 miljardi – par 18 % vairāk nekā 2. ceturksnī.

Pārskata periodā, palielinoties pakalpojuma saņēmēju skaitam un sensoru apjomam, pieauga analizējamās datu plūsmas apjoms, kā arī darba apjoms anomāliju un ļaunprogrammatūras aktivitāšu identificēšanā, brīdinājumu nosūtīšanā un atbalsta sniegšanā.

Aktuālākie apdraudējumi pārskata periodā:

- pieprasījumi uz “ClickFix”/”ClearFake” ļaunatūru izplatošiem domēniem;
- pieprasījumi uz domēniem, kas izplata kaitnieciskus attālinātās pārvaldības rīkus (RAT);
- pieprasījumi uz domēniem, kas saistīti ar identificētām pikšķerēšanas un krāpniecības kampaņām;
- pēc ievainojamību publiskas izziņošanas uzbrucēji nereti masveidā skenē sistēmas, lai atrastu un izmantotu tajās esošās ievainojamības.



7. attēls. CERT.LV ABS reģistrēto trauksmju dinamika pa ceturkšņiem (skaits 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. 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.

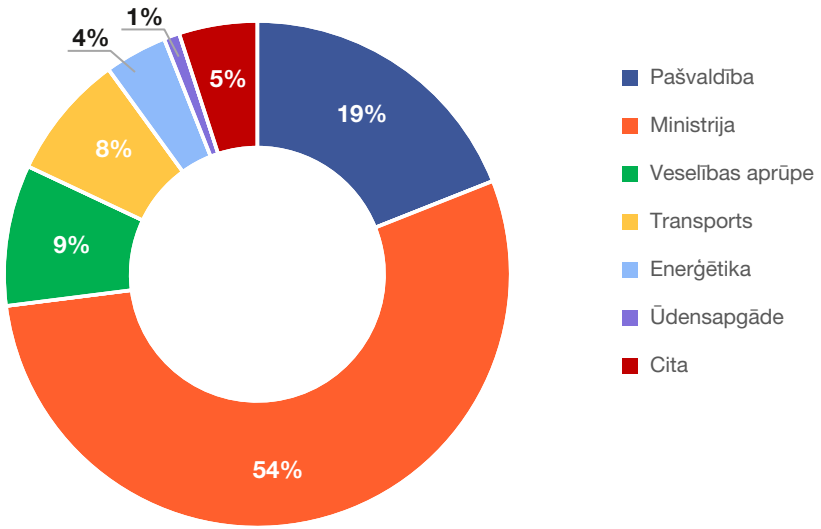
Īpaši nozīmīgs ir SOC analītiķu ieguldījums, kas, izmantojot īpašu programmnodrošinājumu un pieejamos datus, savlaicīgi novērš kaitējumu – identificē, brīdina un aptur apdraudējumu vai kiberincidentu.

Pārskata perioda beigās SOC klientu skaits sasniedza 126 – skaits pieauga par 20 %.

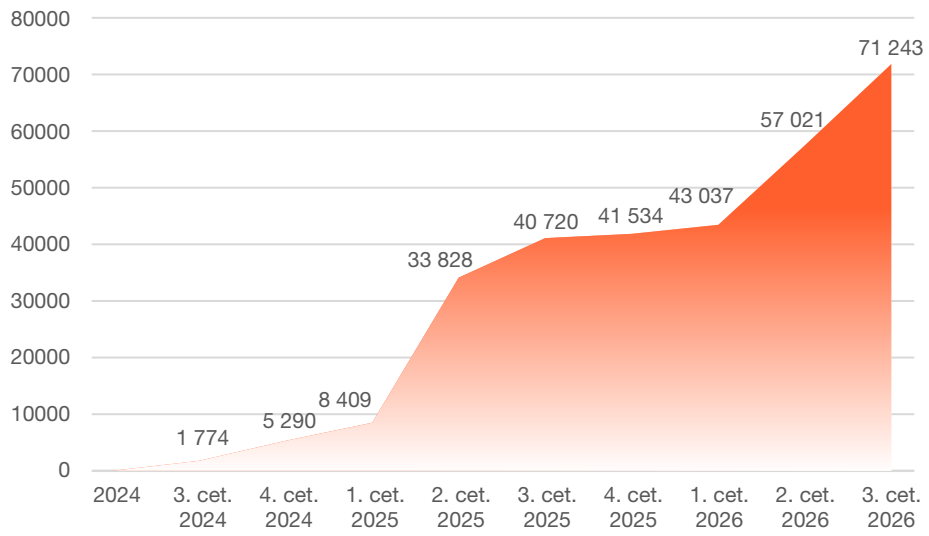
CERT.LV SOC risinājumus izmanto dažādu nozaru organizācijas, tostarp NKDL subjekti – būtisko un svarīgo pakalpojumu sniedzēji. Visplašāk pārstāvētās ir ministrijas (54 %), pašvaldības (19 %) un veselības aprūpes iestādes (9 %).

SOC redzamības dinamika

- **Kopumā nodrošināta 71 243 gala iekārtu, tostarp serveru un darbstaciju, pārskatāmība. 2026. gada 3. ceturksnī pieaugums veido 25 % no kopējā apjoma.**
- **Paplašinoties uzraudzības tvērumam, pieaug analizējamo notikumu un ģenerēto trauksmju skaits, kā arī spēja savlaicīgi identificēt apdraudējumus.**



8. attēls. Sadalījums pēc organizāciju veida/nozares, kas izmanto CERT.LV SOC (procentuālā daļa no kopējā skaita: 126)



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

Pārskata periodā reģistrētas 29 miljoni drošības trauksmes – par 16 % vairāk nekā 2026. gada 2. ceturksnī.

Drošības trauksmju skaita pieaugums primāri atspoguļo SOC uzraudzībā esošo gala iekārtu skaita paplašināšanos un uzlabotu spēju identificēt potenciālos apdraudējumus. Vienlaikus tas liecina par uzbrukumu intensitātes pieaugumu kibertelpā.

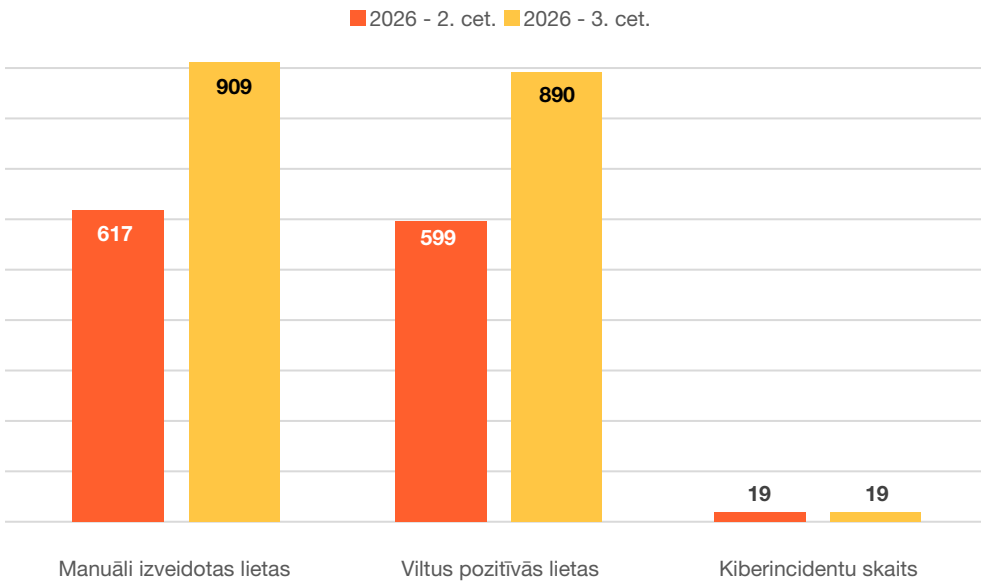
Lielāko daļu joprojām veido zema un vidēja līmeņa trauksmes, radot ļoti "trokšņainu" vidi un apgrūtinot būtiskāko trauksmju savlaicīgu noteikšanu.

Augsta līmeņa un kritiskās trauksmes kopā veido 0,3% no kopējā apjoma. Vienlaikus **augsta un kritiska līmeņa trauksmju straujais kāpums attiecīgi par 67% un 37% ir būtisks riska indikators**. Tas nozīmē, ka pārskata periodā ir palielinājies tādu notikumu īpatsvars, kuriem potenciāli ir lielāka ietekme uz konfidencialitāti, integritāti vai pieejamību. Šāds apjoms nozīmē arī būtisku operacionālo slodzi CERT.LV SOC komandai.

Incidenti un drošības trauksmes: draudu atklāšana un novēršana

Rādītāji	Skaits	Izmaiņas salīdzinājumā ar 2026. gada 2. cet. (%).
Reģistrēto drošības trauksmju ziņojumu skaits 2026. gada 3. cet. kopā:	~29M	+16%
Zema līmeņa trauksmes	~10M	+66%
Vidēja līmeņa trauksmes	~19M	+6%
Augsta līmeņa trauksmes	~27K	+67%
Kritiskas trauksmes	~47K	+37%
Manuāli izveidoto lietu skaits	909	+47%
Viltus pozitīvo lietu skaits*	890	+49%
Kiberincidentu skaits	19	0

* Viltus pozitīvs (*false positive*) kiberdrošībā ir situācija, kad drošības sistēma kļūdaini uzskata normālu darbību par incidentu vai apdraudējumu.



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

SOC pakalpojuma ietvarā izveidotās lietas un fiksētie kiberincidenti

- **2026. gada 3. ceturksnī CERT.LV SOC ietvaros manuāli tika izveidotas 909 lietas, kas ir par 47 % vairāk nekā iepriekšējā ceturksnī.**
- **Kopumā reģistrēti 19 kiberincidenti, to skaits saglabājies nemainīgs.**

Joprojām novērojams liels "viltus pozitīvo" trauksmju skaits (3. ceturksnī pieaugums par 49 %) - tas nozīmē lielāku mazefektīva darba apjomu SOC analītiķiem notikumu pārbaudē, radot risku palaist garām īstu uzbrukumu starp "viltus pozitīvajiem".

Biežākie viltus trauksmju iemesli klientu infrastruktūrā:

- Nepilnīga vai novecojusi IKT resursu uzskaite un centralizētas pārvaldības trūkums iestāžu vai novada mērogā.
- Gala iekārtu konfigurācija nav standartizēta.
- Nav izveidots atļautās programmatūras saraksts un ieviesta tā ievērošanas kontrole.
- Netiek pārvaldīti un kontrolēti tīmekļa pārlūku spraudņi un paplašinājumi.
- Lietotāju atbalstam nepamatoti tiek izmantoti vairāki attālinātās piekļuves rīki.
- Nav iespējota žurnālierakstu veidošana, trūkst dokumentācijas un procedūru.
- Netiek uzraudzīta USB zibatmiņu lietošana un kontrolēta tajās esošo failu izpilde.

SOC analītiķu slodzi palielina gan gala iekārtu un notikumu apjoma pieaugums, gan arvien sarežģītāki un augstāka riska incidenti. Vienlaikus pieaug nepieciešamība ātri izvērtēt trauksmes, noteikt prioritātes un efektīvi koordinēt rīcību ar klientiem. SOC kapacitātes stiprināšana ir būtisks priekšnosacījums, lai arī turpmāk nodrošinātu pakalpojumu kvalitāti un savlaicīgu reaģēšanu pieaugošas slodzes apstākļos.

Pārskata periodā SOC pakalpojuma ietvarā fiksēto kiberincidentu pārskats

Lielāko trauksmju skaitu izraisa nekontrolēta nevēlama programmatūra – **no tīmekļa lejupielādēti un aktivizēti izpildāmie faili**. Piemēram, no tīmekļa lejupielādēti spēļu instalācijas faili nereti satur arī ļaunatūru. Vairākos gadījumos konstatēta nevēlama programmatūra, kas ir ietekmējusi gala iekārtu darbību, tādēļ trauksmes reģistrētas kā kiberincidenti.

Pārskata periodā vairāk nekā puse reģistrēto incidentu (10) bija saistīti ar "ClickFix" uzbrukumiem, kuros lietotāji kompromitētās tīmekļvietnēs tiek maldināti ar **viltus "CAPTCHA"** pārbaudēm. Tā ir izplatīta sākotnējās piekļuves metode, kas mudina lietotāju iekopēt un izpildīt kaitīgu komandu. Iekopēto komandu izpilde atšķiras atkarībā no iestādes IT sistēmu konfigurācijas. Pēc komandas izpildes ierīcē tiek lejupielādēta ļaunatūra, kas var nozagt lietotāja piekļuves datus, instalēt papildu kaitīgas programmatūras vai veikt citas ļaunprātīgas darbības.

CERT.LV tīmekļvietnē apkopoti ieteikumi lietotājiem "ClickFix" uzbrukuma draudu mazināšanai: **https://cert.lv/lv/2025/04/viltus-captcha-var-inficet-jusu-datoru**.

Pārskata periodā reģistrēti vairāki incidenti, kuros sākotnējā piekļuve iegūta, izmantojot **pikšķerēšanas e-pastus, inficētus e-pasta pielikumus vai pārlūku spraudņus**. Šo piekļuves veidu apdraudējums saglabājas aktuāls arī turpmāk.

Savukārt trīs incidentos tika **kompromitēti klienta serveri**: divos gadījumos sākotnējā piekļuve notikusi caur **ievainojamu tīmekļa vietņu satura vadības sistēmu**, citā caur **ievainojamu e-pasta servera programmatūru**.

Biežāk sastopamā aina kompromitētā vidē:

- **Nav ieviests mazāko nepieciešamo privilēģiju princips**, tādējādi ļaujot uzbrucējam ātri paplašināt piekļuves tiesības un pārvietoties infrastruktūrā.
- **Trūkst tīkla segmentācijas**, radot situāciju, kad kompromitēšana vienā tīkla daļā rada iespēju netraucēti izplatīties uz citām sistēmām.
- **Nav ieviesti programmatūras izpildes ierobežojumi**, tādējādi ļaujot bez būtiskiem šķēršļiem izpildīt ļaunprātīgu kodu un neautorizētas lietojumprogrammas.
- **Nav nodrošināta vienota IT vides pārvaldība un centralizēta drošības telemetrija**, tas, savukārt, 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.

Dominējošie sākotnējās piekļuves vektori



Viltus CAPTCHA pārbaudes



Pikšķerēšana un ļaunprātīgi e-pasta pielikumi



Pārlūku spraudņi



Nevēlama programmatūra
No tīmekļa lejupielādēti un aktivizēti izpildāmie faili



Tīmekļvietņu satura vadības sistēmas



Ievainojama e-pasta servera programmatūra

3.4. IT sistēmu drošības testi un pikšķerēšanas uzbrukumu simulācijas kampaņas

Pikšķerēšanas uzbrukumu simulācijas kampaņas

2026. gadā kopskaitā CERT.LV veica 12 pikšķerēšanas uzbrukumu simulācijas kampaņas, tostarp 3. ceturksnī veiktas 4 pikšķerēšanas uzbrukumu simulācijas kampaņas četrās iestādēs. Šo kampaņu ietvarā tika nosūtītas 2 657 e-pasta vēstules. Vairāk nekā puse jeb 55 % lietotāju atvēra saiti e-pastā, un no tiem, kas atvēra, lietotāja datus ievadīja 38 %.

Pikšķerēšanas uzbrukumu simulācijas kampaņas mērķis ir apmācīt lietotājus un veicināt darbinieku spējas identificēt potenciāli riskantus uzvedības modeļus, atpazīt un novērst kiberapdraudējumus un informācijas noplūdi.

IT sistēmu drošības testi

2026. gadā kopskaitā veikti 24 IT sistēmu drošības testi.

3. ceturksnī CERT.LV uzraudzīja vēlēšanu sistēmu drošības auditā konstatēto nepilnību novēršanu. Tika veikti arī vairāki atkārtoti testi, lai pārliecinātos, ka visas iepriekš identificētās nepilnības ir novērstas un izstrādes gaitā nav radušās jaunas.

CERT.LV pārbaudīja arī atsevišķas IT sistēmas un tīmekļvietnes, veica vēlēšanu sistēmu drošības testus un sniedza ieteikumus drošības uzlabošanai.

IT sistēmu drošības testēšanā CERT.LV analizē tīkla drošību, novērtē programmatūras un IT infrastruktūras ievainojamības, izvērtē tīmekļa lietotņu drošību, kā arī sniedz konsultācijas un ieteikumus drošības uzlabošanai.

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 50 NKDL subjektu un IKT kritiskās infrastruktūras organizācijās.

Pārskata periodā pabeigtas 6 draudu medību operācijas, savukārt 16 operāciju izpilde turpinās.

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

Latvija un Kanāda turpina stiprināt NATO kiberdrošības spējas Draudu medību mācību kursā

2026. gada 19.-23. oktobrī Rīgā notiks jau piektais pēc kārtas Draudu medību apmācību kurss par kiberdraudu meklēšanu, ko kopīgi vadīs CERT.LV un Kanādas kiberdrošības eksperti. Mācības organizē CERT.LV sadarbībā ar Latvijas Aizsardzības ministriju un Kanādas Bruņoto spēku kiberpavēlniecību.

Draudu medību apmācību kursa mērķis ir atbalstīt un spēcināt NATO sabiedroto spējas potenciālo draudu identificēšanā, pirms tie kļūst par reāliem kiberincidentiem.

3.6. Koordinētas ievainojamību ziņošanas platforma (CVD)

Ievainojamību ziņošanas platformas **cvd.cert.lv** (turpmāk – CVD platforma) darbību nodrošina CERT.LV, pildot koordinētas ievainojamību atklāšanas procesa koordinatora lomu un veicot NKDL noteiktos uzdevumus, kas nacionālajā līmenī reglamentē koordinētu ievainojamību atklāšanas un novēršanas procesu.

CVD platforma lietotājiem ir pieejama jau trīs gadus. Lai veicinātu visām iesaistītajām pusēm pieņemamu, atklātu un godīgu sadarbību, kā arī saskaņotu platformas izmantošanas kārtību un terminoloģiju ar normatīvā regulējuma izmaiņām, ir pārskatīti platformas lietošanas noteikumi un personas datu apstrādes kārtība. Izmaiņas stājās spēkā 2026. gada 1. augustā.

Platformā apstrādā ziņojumus par resursiem, kas ir Latvijas Republikā reģistrētas fiziskas vai juridiskas personas pārziņā. Šāda persona var būt NKDL subjekts, valsts vai pašvaldības institūcija, kura ir IKT resursa vai .lv domēna vārda īpašnieks, turētājs, valdītājs vai pārzinis.

CVD platformas rādītāji

2026. gada 3. ceturkšņa beigās kopumā reģistrēti*:



245

drošības pētnieki

skaits pieauga par 60



28

aktīvas iestāžu programmas

nākušas klāt 10



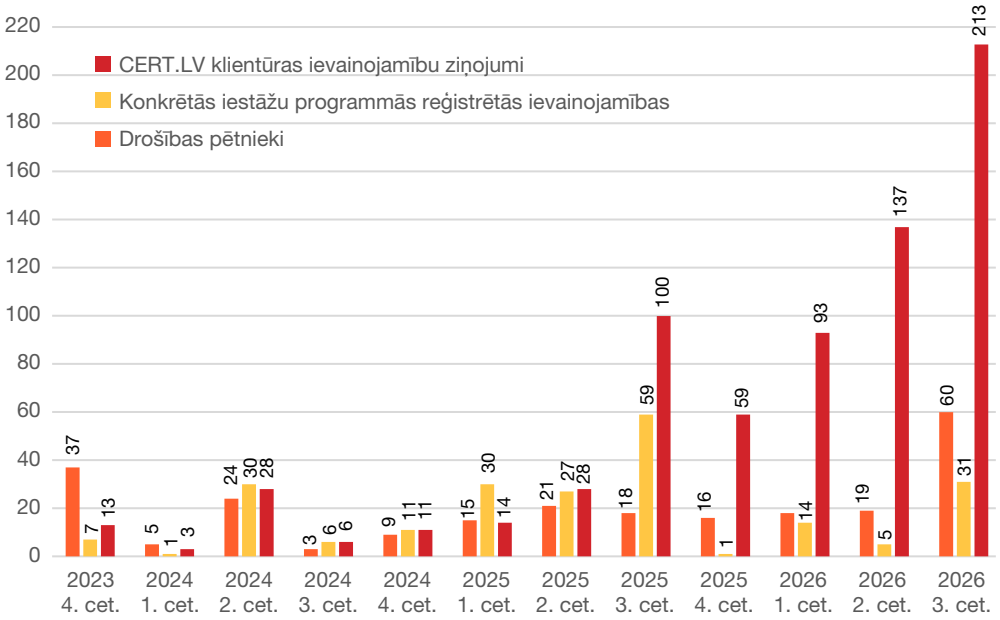
927

ievainojamību ziņojumi

skaits pieauga par 244

*Pieaugums norādīts kopš iepriekšējā ceturkšņa beigām.

Pārskata periodā platformā reģistrēts lielākais ziņojumu skaits kopš tās ieviešanas – **927** ziņojumi, tostarp CERT.LV iesniegtie ievainojamību ziņojumi – **705** (skaits pieauga par 213) un lestāžu programmās ziņotās ievainojamības – **222** (skaits pieauga par 31).



11. attēls. CVD platformas attīstības dinamika (skaits)

Aktīvās iestāžu programmas skatīt CVD platformā: **https://cvd.cert.lv/programs/all**

CERT.LV aicina organizācijas izveidot un pārvaldīt savas programmas CVD platformā, lai drošības pētnieki varētu testēt ārējā tīklā eksponēto resursu ievainojamības. Savukārt drošības pētnieki ir aicināti platformā ziņot par valsts pārvaldes iestāžu un Latvijā reģistrētu uzņēmumu resursos atklātajām ievainojamībām, veicinot to ātrāku novēršanu.

Drošības pētnieku ieguldījums ievainojamību atklāšanā palīdz stiprināt Latvijas kibertelpas drošību. Vienlaikus CERT.LV atgādina, ka ievainojamību meklēšana jāveic atbildīgi, samērīgi un ievērojot konkrētās programmas noteikumus.

Spēkā stājas Kibernoturības aktā noteiktās ziņošanas prasības ražotājiem

No 2026. gada 11. septembra saskaņā ar Eiropas Savienības (ES) Kibernoturības aktu (CRA; **https://eur-lex.europa.eu/legal-content/LV/TXT/PDF/?uri=OJ:L_202402847**) ražotājiem ir pienākums ziņot par aktīvi izmantotām ievainojamībām un nopietniem incidentiem, kas ietekmē ES tirgū pieejamo produktu ar digitāliem elementiem drošību. Ziņojumi jāiesniedz ES Kiberdrošības aģentūras (ENISA) izstrādātajā vienotajā ziņošanas platformā (SRP): **https://portal.cra-srp.enisa.europa.eu/**. Latvijā šo ziņojumu apstrādi nodrošina un turpinās veikt CERT.LV.

Informācija par ziņošanas juridiskajām prasībām, vadlīnijas ziņojumu iesniedzējiem, kā arī atbildes uz biežāk uzdotajiem jautājumiem publicētas ENISA tīmekļvietnē: **https://www.enisa.europa.eu/news/the-cra-single-reporting-platform-is-launched**.

3.7. Operacionālo tehnoloģiju (OT) drošība

Aktivitātes

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



Sistēmu uzraudzība un anomāliju identifikācija

CERT.LV turpina OT sistēmu datu plūsmas uzraudzības sensoru tīkla paplašināšanu. Lai efektīvāk atklātu anomālijas OT sensoru ievāktajos datos, tiek izstrādāti un izvietoti uz mašīnmācīšanos balstīti detektori. To darbību nepārtraukti pilnveido, analizējot iegūtos datus. Līdztekus iekšējo OT tīklu datplūsmas uzraudzībai nepārtraukti tiek pārraudzīta Latvijas IP adrešu telpa, lai identificētu publiski eksponētas sistēmas un to iespējamās ievainojamības. Balstoties uz iegūto informāciju, tiek koordinēta piekļuves ierobežošana šīm sistēmām un konstatēto nepilnību novēršana.



OT sistēmu drošības testi

OT sistēmu komponenšu drošības pārbaudēs tiek testētas dažādas viedās un industriālās vadības ierīces. Mērķis ir atklāt iespējamās ievainojamības un piegādes ķēžu nepilnības, kas varētu ļaut ražotājiem vai ārējiem uzbrucējiem nesankcionēti vadīt šīs ierīces vai sistēmas kopumā. Pārskata periodā tika veikti sistēmu testi, identificējot virkni uzlabojumu un pārrunājot tos ar šo sistēmu izstrādātājiem.



Starptautiskā sadarbība

Turpinās plašāka sadarbība ar Ziemeļvalstu un Baltijas valstu (NB8) kiberdrošības iestādēm. Sadarbības ietvaros notiek regulāra aktuālo kiberdraudu informācijas apmaiņa.

Apdraudējumi, incidenti, ietekme

CERT.LV turpina proaktīvi identificēt iespējamos riskus un ievainojamības, lai mazinātu to iespējamo ietekmi. **Latvijas OT sistēmu noturība pret kiberuzbrukumiem kopumā ir atbilstošā līmenī, un tai ir tendence uzlaboties.** Regulārās pārbaudēs tiek identificētas internetā pieejamas privātas vai nelielas OT sistēmas. CERT.LV informē šo sistēmu operatorus par konstatētajiem riskiem un sadarbojas ar tiem, lai mazinātu vai novērstu iespējamo kiberapdraudējumu ietekmi.

Arī turpmāk sagaidāmi pastāvīgi Latvijai nedraudzīgo valstu radīti kiberapdraudējumi, kuru mērķis ir iegūt kontroli pār kritiskās infrastruktūras operatoru sistēmām un veikt tajās destruktīvas darbības. Eiropā šādas aktivitātes īsteno ar Krieviju, Ķīnu un Irānu saistīti kiberuzbrucēji.

Pieaugot lielo valodu modeļu spējām, tos arvien plašāk izmanto automatizētai ievainojamību meklēšanai un ekspluatācijai dažādos uzbrukuma posmos, tostarp pilnas uzbrukuma ķēdes īstenošanai.

Lai mazinātu iespējamo apdraudējumu ietekmi un stiprinātu Latvijas noturību, CERT.LV turpinās pilnveidot OT sistēmu drošību, paplašinot šo sistēmu pārredzamību un draudu identificēšanas iespējas, veicot drošības testus un nodrošinot koordinētu reaģēšanu uz incidentiem.

3.8. Izglītošana – lekcijas un dalība kiberdrošības pasākumos

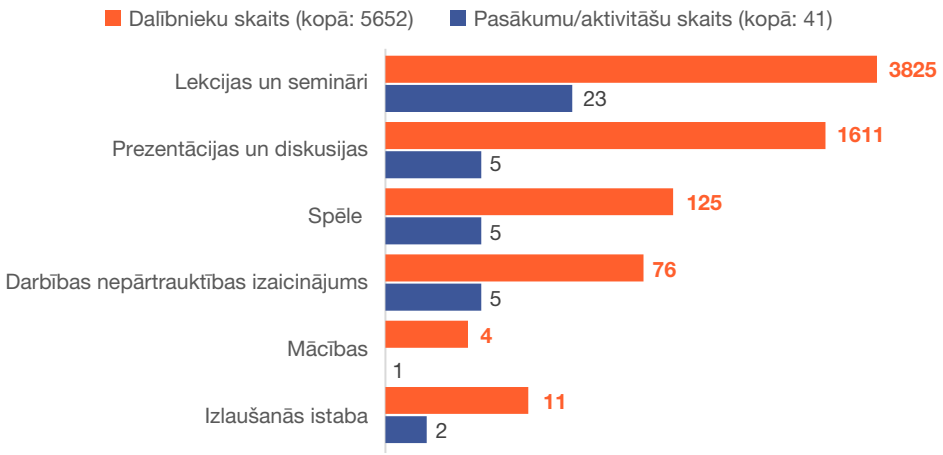
CERT.LV turpina stiprināt individuālu lietotāju un organizāciju zināšanas un prasmes kiberdrošības jomā.

2026. gada 3. ceturksnī CERT.LV eksperti 41 pasākumā sasniedza 5 652 cilvēku auditoriju. Salīdzinājumā ar 2025. gada attiecīgo periodu pasākumu skaits pieauga par 58 %, savukārt dalībnieku skaits – par 32 %.

CERT.LV ekspertu visplašāk izmantotās mācību formas bija lekcijas un semināri – gan pēc pasākumu skaita, gan sasniegtās auditorijas lieluma. Praktiskās metodes ir sarežģītāk īstenojamas lielās dalībnieku grupās, taču tās palīdz nostiprināt iegūtās zināšanas un prasmes. Mācību spēles, izaicinājumi un izlaušanās istabas ir īpaši piemērotas konkrētām mērķgrupām, piemēram, IT, drošības, vadības vai darbības nepārtrauktības komandām.

CERT.LV piedāvā ikvienam pilnveidot savas kiberdrošības zināšanas, 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.

Lai pieteiktos kiberdrošības apmācībām un citiem izglītojošiem pasākumiem, CERT.LV aicina rakstīt uz **events@cert.lv**. Plašāka informācija par piedāvātajām lekcijām, mācību spēlēm un pasākumiem pieejama CERT.LV tīmekļvietnes sadaļā **"Pakalpojumi"**.



12. attēls. Izglītošanas formāti un sasniegtā auditorija (skaits; 2026 - 3. CET.)

Kiberdrošības mēneša epicentrā – konference "CyberChess 2026"

Oktobrī, Eiropas kiberdrošības mēnesī, Rīga pulcēs Latvijas un ārvalstu kiberdrošības kopienu. 14. un 15. oktobrī notiks starptautiskā kiberdrošības konference "CyberChess 2026". Pirms tās 10.-11. oktobrī notiks CTF kiberdrošības sacensības un 13. oktobrī – praktiskie semināri. Pārskata periodā CERT.LV turpināja šo pasākumu organizēšanas darbus.

Pēc notikumiem intensīvas vasaras Latvijas kibertelpā apdraudējuma līmenis saglabājas augsts. Tādēļ konferencē galvenā uzmanība būs pievērsta aktuālajiem kiberdraudiem, praktiskai gatavībai un organizāciju noturības stiprināšanai, veicinot publiskā un privātā sektora pieredzes apmaiņu un ciešāku sadarbību ar starptautiskajiem partneriem.

Vairāk informācijas: **cyberchess.lv**. Konferenci līdzfinansē Eiropas Savienība Eiropas Kiberdrošības kompetenču centra Latvijas Nacionālā koordinācijas centra projekta (C-STRONG-NCC-LV) ietvaros.

4. Pārskats par LIA Drošāka interneta centra ZL darbību

Latvijas Interneta asociācijas Drošāka interneta centra ziņojumu līnija (ZL) laika posmā no 01.07.2026. līdz 30.09.2026. ir saņēmusi un izvērtējusi 926 ziņojumus. No tiem 332 ziņojumu saturā ir konstatēti bērnu seksuālu izmantošanu saturoši materiāli, 61 gadījumā konstatēta pornogrāfija bez izvietota brīdinājuma par vecuma ierobežojumu, 27 ziņojumos konstatēta personas goda un cieņas aizskaršana, 3 ziņojumi saņemti par naida runu un 3 ziņojumos konstatēti vardarbīgi materiāli. Par finanšu krāpšanas mēģinājumiem internetā saņemts 21 ziņojums, 460 ziņojumu saturs nav bijis pretlikumīgs, 19 gadījumos ziņotājiem tika sniegti ieteikumi problemātisko gadījumu risināšanai.

Valsts policijai nosūtīti 28 ziņojumi par bērnu seksuālu izmantošanu saturošiem materiāliem, kas tiek uzturēti uz serveriem Latvijā. 285 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 28 ziņojumiem par bērnu seksuālu izmantošanu saturošiem materiāliem 26 ziņojumu saturs ir dzēsts no publiskas aprites internetā un 2 ziņojumi atrodas dzēšanas procesā.

Pārskats par saņemtajiem ziņojumiem no 01.07.2026. līdz 30.09.2026.

Ziņojumi	Jul-26	Aug-26	Sep-26	3.cet.
Erotisks/ pornogrāfisks saturs bez izvietotiem brīdinājumiem	24	27	10	61
Pedofilija/ mazgadīgo prostitūcija/ bērnu seksuālu izmantošanu saturoši materiāli	103	68	161	332
Vardarbīga rakstura materiāli	0	1	2	3
Cieņas/ goda aizskaršana	11	4	12	27
Naida kurināšana/ rasisms	2	0	1	3
Finanšu krāpšana	11	6	4	21
Konsultācijas/ padomi	5	5	9	19
Citi	16	57	387	460
KOPĀ:	172	168	586	926

Ziņojumi nosūtīti Valsts policijai	4	15	9	28
Ziņojumi nosūtīti INHOPE asociācijai	94	43	148	285
KOPĀ NOSŪTĪTI IZSKATĪŠANAI:	98	58	157	313

CERT.LV misija ir veicināt kiberdrošību Latvijā.

CERT.LV galvenie uzdevumi ir uzturēt un aktualizēt informāciju par kiberdrošības apdraudējumiem, atbalstīt valsts institūcijas kiberdrošības jomā un sniegt atbalstu fiziskām un juridiskām personām novērst kiberincidentus, kuros iesaistīta Latvijas IP adrese vai .lv domēns. CERT.LV arī organizē 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



© CERT.LV, 2026
Pārpublicējot obligāta avota norāde.