2025 Q3

LATVIAN CYBERSPACE SITUATION

PERIOD: 01.07.2025. - 30.09.2025.

CERT.LV
Cyber Incident
Response Institution

Institute of Mathematics and
Computer Science University of Latvia

Ministry of Defence
Republic of Latvia

Summary

The cyber-threat level in Latvia remains consistently high, with an average of 500-700 incidents every quarter since 2022. Periods of low intensity are a thing of the past, and internet users are still exposed to constant risks.

In the third quarter of 2025, **671 cyber incidents** were recorded, which is 5% less than in the second quarter of this year, but 2% more than in the third quarter of last year, and overall, an upward trajectory can be observed. The **number of compromised devices identified** by CERT.LV continues to grow rapidly, which is 111% more than in the second quarter of this year, and 36% more than in the third quarter of last year.

Key trends and threats

- The number of compromised devices continues to grow rapidly, indicating a new phase of cyber threats – an increase in IoT and botnet activity, malware, and automated vulnerability exploitation. This signals the need to strengthen vulnerability management and perform timely updates to smart devices.

- Critical vulnerabilities in Microsoft SharePoint and WinRAR were actively exploited – at least one compromise was detected in Latvia's critical infrastructure (CI) sector. CI operators who have implemented and use CERT.SOC services are able to detect such threats much faster and eliminate them more effectively.

- Cyber threats originating in Russia remain high, especially against critical infrastructure and OT systems (energy, water, heating); DDoS attacks from the Russia-linked group NoName057(16) and botnets have been observed.

- Encrypting ransomware, which is becoming increasingly adept at circumventing defence mechanisms, continues to threaten organisations, with three cases registered by CERT.LV. Institutions need to strengthen their backup, recovery, and incident response capabilities.

- Supply-chain attack risks continue to rise, underscoring the need for more proactive security audits, stricter cybersecurity requirements in procurement, and ongoing reminders about the importance of timely software updates. The introduction of the new "minimum cybersecurity requirements" regulation is a positive step that will help raise the overall cybersecurity maturity across organisations.

- Social engineering and fraud campaigns are reaching new levels of intensity: paid Google ads are being used to spread fraudulent websites offering fake investment schemes; there has been an increase in SMS and email phishing campaigns impersonating government agencies (particularly CSDD, VID EDS, DPD) and well-known public figures. A new dimension of threat – the ClickFix mechanism, which uses CAPTCHA checks to get users to unknowingly activate harmful actions. 2FA, DNS firewalls, timely updates, and employee training reduce risks and the impact of incidents.

Attacks are becoming hybrid, exploiting both technological and human vulnerabilities. Resilience is critical; rapid, coordinated action is essential to limit the impact of an attack – timely vulnerability remediation, telemetry data, and response capabilities can significantly reduce the potential consequences.

These trends confirm the need to continue strengthening Latvia's preparedness for a wide range of threats by applying multi-layered cyber defence – DNS firewalls, support in resolving cyber incidents and Security Operations Centre (SOC) services, threat hunting and security testing, as well as user education and training provided by the CERT.LV team.

Contents

1. Cybersecurity threats: statistics and trends

Dynamics of cyber incidents and compromised devices

In the third quarter of 2025, **671 cyber incidents** were recorded, which is **5% less** than in the second quarter and **2% more** than in the third quarter of last year. Fluctuations in the number of cyber incidents are observed, but overall, the trend is upward.

The number of incidents has stabilised at a high level: since Q3 2022, there have been an average of 500-700 incidents, indicating a persistently high cyber-threat background and a constant workload for those responsible for cybersecurity.

The **rapid increase in the number of compromised devices identified by CERT.LV** continues, which is **111% more** than in Q2 of this year and **36% more** than in Q3 of last year. This indicates the greater use of botnets, malware, automated scanning, and exploitation of vulnerabilities and configuration flaws. At the same time, the increase can be explained by improvements in monitoring and detection capabilities. The increase was also influenced by the addition of data from the State Joint-Stock Company “Latvia State Radio and Television Centre” to CERT.LV telemetry data in Q2 of this year.

The number of incidents and compromised devices does not always correlate. In 2025, the number of incidents has remained at around 600-700 per quarter, while the number of compromised devices has doubled. This suggests that incidents are becoming broader in scope rather than more numerous.

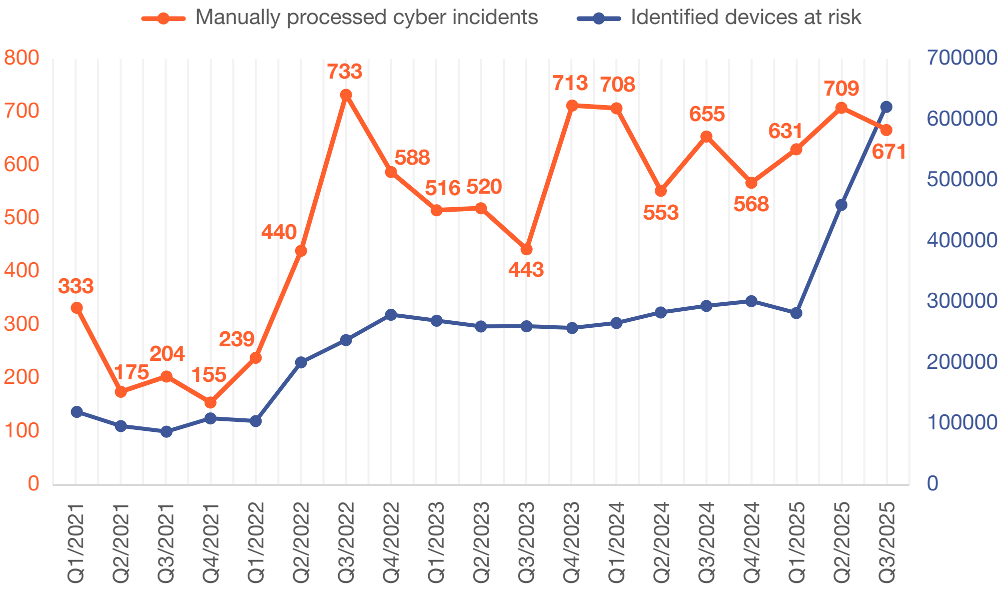


Figure 1. Number of devices exposed to cyber incidents and identified, by quarter

On a monthly basis (July–September), the number of cyber incidents has been relatively stable overall, but a significant increase was observed in September – from 189 incidents in August to 275 in September, which is approximately 45% more. This dynamic indicates a seasonal resumption of activity after the summer months and the possible start of a new wave of attacks. Compared to previous years, the number of cyber incidents in Q3 has shown a slight upward trend, which may indicate both an increase in the intensity of attacks and improved identification and reporting practices.

[1] Events that threatened data processed or the availability, authenticity, integrity, or confidentiality of services offered by or accessible through network and information systems.

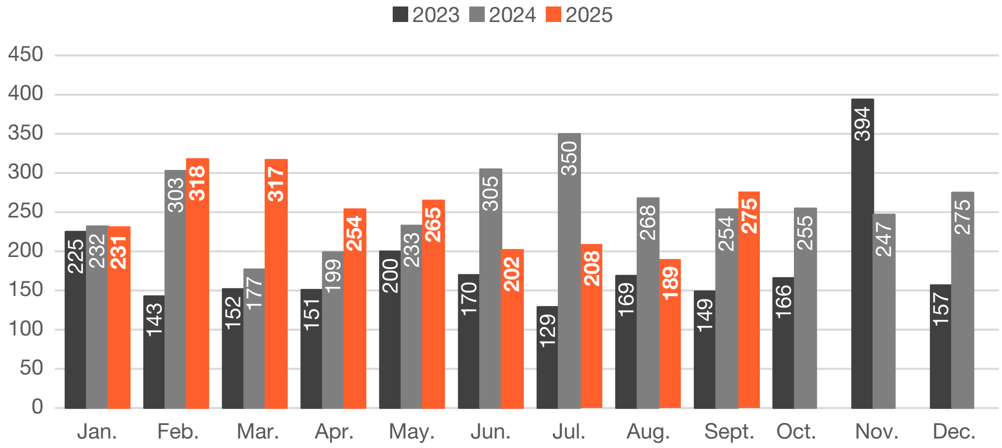
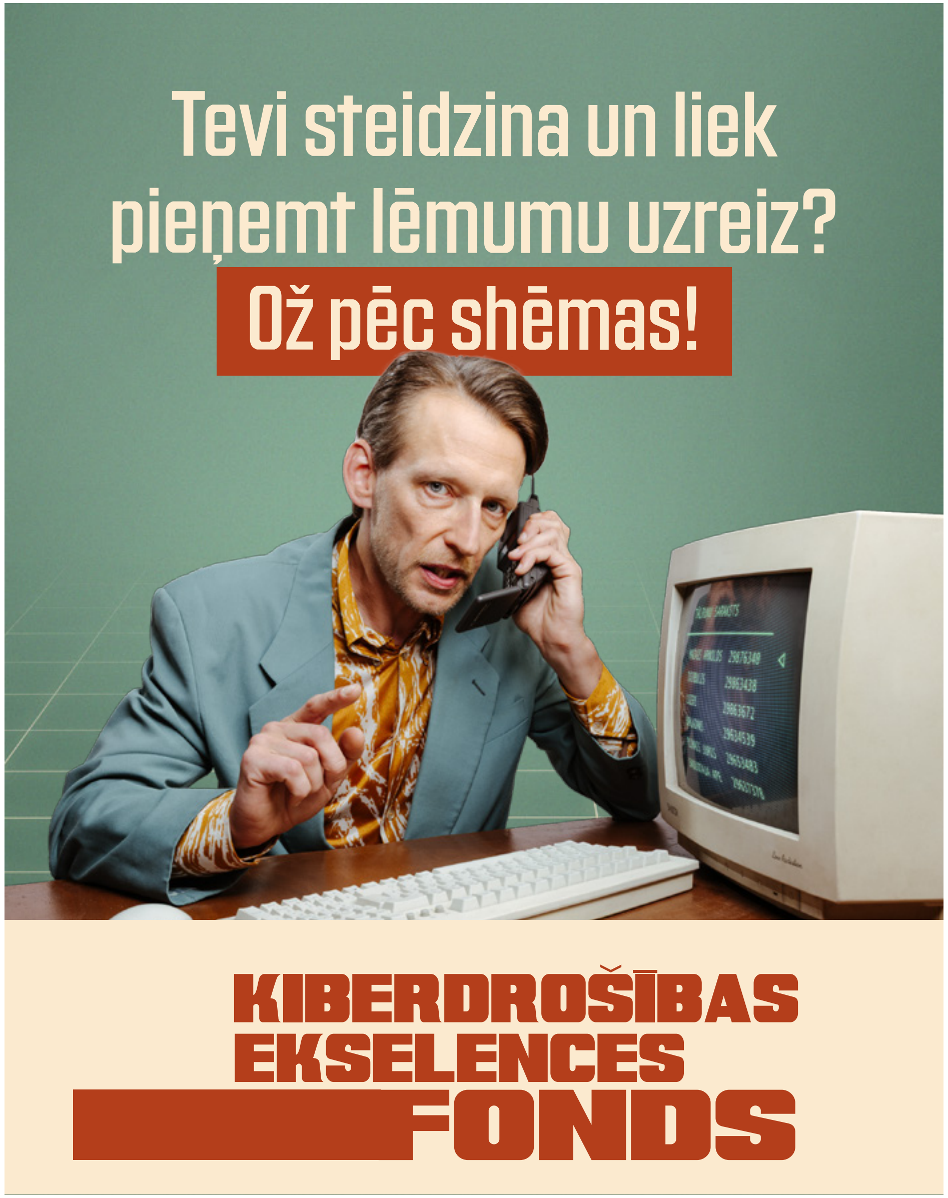


Figure 2. Cyber incident trends (monthly breakdown)

During the reporting period, CERT.LV experts **educated 4291 participants in 26 cybersecurity events**, improving the knowledge and skills of both individual users and organisations in ensuring data and system security.

On 8 September, the Ministry of Defence and CERT.LV launched the cybersecurity campaign “Sniff out the scheme!” (“Ož pēc shēmas!”), which aims to strengthen public cybersecurity and resilience to threats, while educating people about cyber hygiene and digital fraud schemes.

The effectiveness of the measures taken and their impact on overall cybersecurity depend directly on the willingness of all parties involved to comply with them, with everyone taking responsibility for their digital assets and organisations investing resources in cybersecurity. Effective cyber threat prevention requires the synergistic and coordinated involvement of all available resources, institutions, and organisations.



CERT.LV offers a monthly plain-language report of the critical events in Latvian cyberspace through the top-5 categories, for those interested in the “cyber weather”. The latest cyberspace events, threat analysis, and useful tips for the reporting period: JULY | AUGUST | SEPTEMBER

2. Top reporting-period cyber threats and key events

TOP 5 quantitatively largest types of cyber threats:

Type of threat	Number of cyber incidents Q3 2025	Change relative to Q2 2025	Change relative to Q3 2024
Fraud	**466**	+1%	+14%
Malicious code	**61**	+36%	+61%
Intrusion attempts	**32**	+3%	-44%
Configuration deficiencies	**21**	+250%	+40%
Compromised devices	**17**	-32%	-43%

Analysis of cyber threat structures by incident type

- **Fraud remains the dominant threat**, showing steady growth and maintaining its position as the largest category of incidents.
- **Incidents involving configuration deficiencies are increasing significantly**. Continuous monitoring, and effective and timely vulnerability management (provided by CERT.LV SOC services) can mitigate this trend.
- **The use of malware is increasing**, showing a gradual upward trend, which signals the increasingly active use of malicious software. Companies and institutions are increasingly threatened by encrypting ransomware attacks and business email compromise, causing financial losses and reputational damage.
- **Incidents of service availability disruption** are decreasing, indicating that investments in protection and coordination against DDoS attacks are paying off, but this trend needs to be consolidated in the long term.

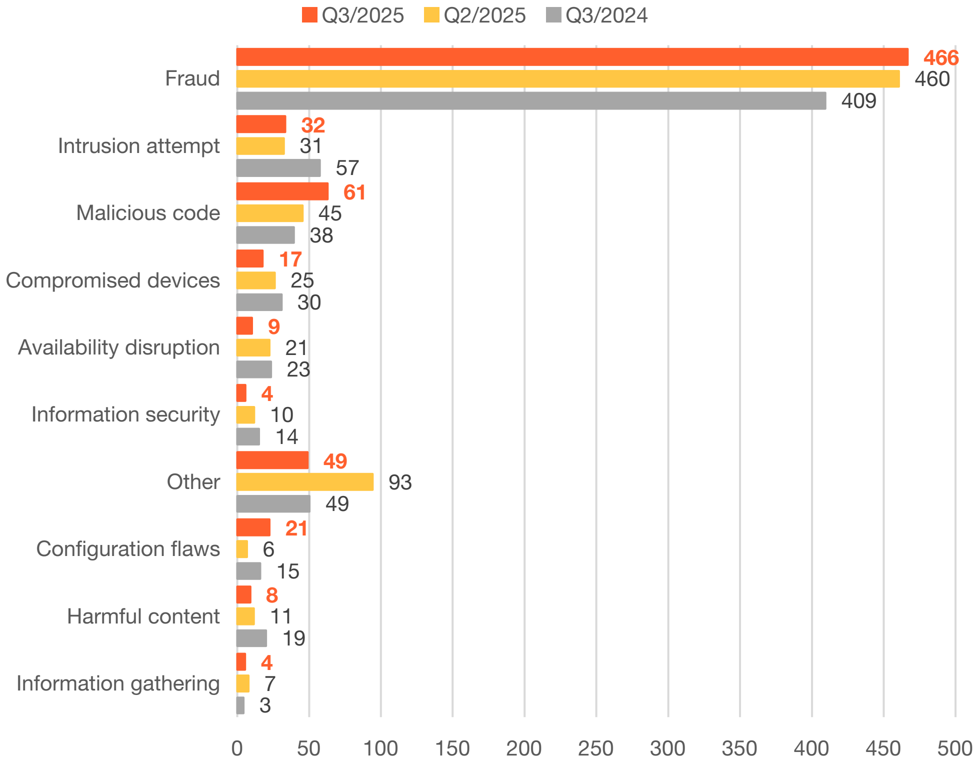


Figure 3. Quantitative comparison of cyber incident type

- **Social engineering as the main point of entry for attacks**

  Classic phishing continues, using the names of well-known organisations. Fraudsters also use misleading advertisements, imitating Latvian media websites or profiles of well-known public figures to spread and promote the credibility of fraudulent investment offers, as well as to spread fake news.

  Fraudsters used search engines (such as Google) to redirect users to a fake website that looks similar to the eParaksts.lv or E-veselība portals.

Fraud campaigns continue with fake e-mails and text messages – the highest phishing activity has been observed under the guise of CSDD, VID EDS, Facebook, or Microsoft. The financial losses incurred by individuals who fall victim to fraudsters range from a few hundred to several thousand euros.

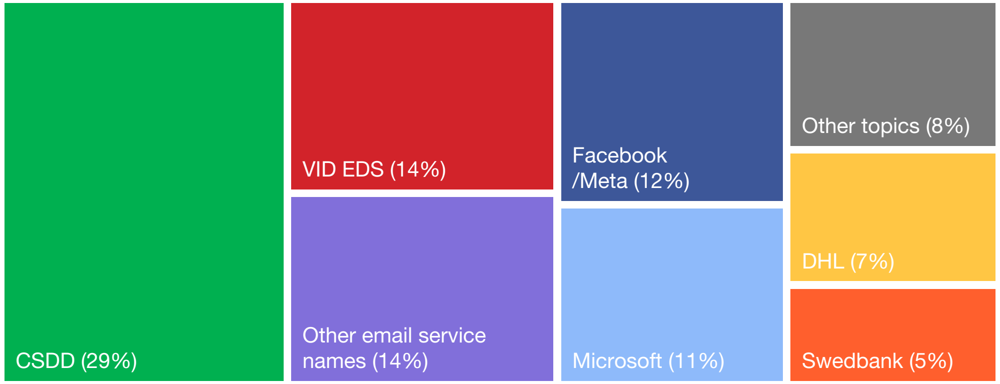


Figure 4. Top phishing campaigns assuming names of well-known organisations (as a share of total phishing reports processed by CERT.LV in Q3 2025)

CERT.LV welcomes the involvement of citizens who identify and forward fraudulent emails and websites to cert@cert.lv, as well as forwarding fraudulent SMS/WhatsApp messages to 232 304 44.

The messages received are compiled, and the malicious domain names are added to an active protection tool – a DNS firewall – to restrict access from Latvian internet users and reduce potential damage. The DNS firewall and its mobile app are available free of charge to all Latvian residents.
Read more: www.dnsmuris.lv

▸ The spread of fake CAPTCHA (ClickFix) malware continues to grow

Since the summer, there has been an increase in the number of reports of compromised websites where visitors are shown fake CAPTCHA security windows asking them to confirm that they are not robots.

This method, also known as ClickFix, is a social engineering technique that exploits users' trust in CAPTCHA checks by imitating a legitimate security process. The goal of the attack is to get the user to follow instructions that, without their knowledge, lead to the execution of active code on their computer and the download of malware. The malware is most often designed to extract authentication data. In September, two reports were received about the spread of this particular malware.

In both cases, CERT.LV contacted the website owners and advised them on how to restore the secure operation of the websites; they have now been repaired.

▸ Active exploitation of critical vulnerabilities

During the reporting period, malicious browser extensions that spy on users were discovered, as well as the exploitation of a WinRAR zero-day vulnerability (CVE-2025-8088), which allows an attacker to remotely execute code or establish persistent access.

A critical Microsoft SharePoint vulnerability (CVE-2025-53770) was also actively exploited, including at least one compromise in Latvia's critical infrastructure sector.

CERT.LV was actively involved in the investigation of the cyber incident, and the analysis showed that the attackers did not go beyond the initial access, and no lateral movement across related systems was detected.
The increasingly rapid response and identification of compromised systems is the result of the development of CERT.LV's capabilities and security operations services.

▸ The spread of malware on mobile and IoT devices – important for both individuals and organisations

During the reporting period, android.badbox2 dominated malware distribution (82% of all cases registered by CERT.LV), indicating very significant and targeted activity in the Android device segment. Its widespread distribution indicates mass infection campaigns, possibly using unofficial app installations or fake updates. This malware is a mobile botnet variant that can infect devices by placing advertisements, stealing data, and remotely controlling the device. The main risks are private data leaks, compromise of infected devices, and use in cyberattacks (DDoS, spam, etc.).

The second most significant threat is Mirai (7%), which is still active and is used to attack unprotected IoT devices (routers, video cameras, etc.). The main risks are DDoS attacks and infrastructure overload.

The remaining malware accounts for a small proportion but shows a diverse combination of attack vectors and increases the risk of compromise.

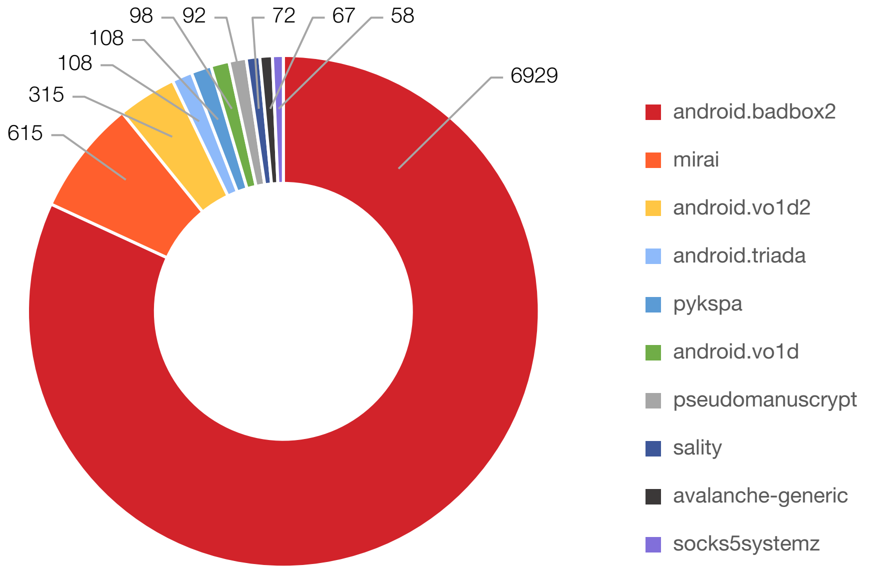


Figure 5. Top 10 malware in Q3 2025, by number

Recommended action:
The security of mobile devices is a matter of national security, as strategic and intelligence information can be obtained from compromised devices. To mitigate the risks of spyware, it is important to:

- **update devices by enabling automatic updates;**
- **practice good cybersecurity hygiene: do not click on suspicious links, enable two-factor authentication, and avoid untrustworthy apps.**

- **Ransomware and supply chain incidents**

During the reporting period, CERT.LV registered reports from three Latvian organisations that suffered attacks by encrypting ransomware (two private companies and the Culture Information Systems Centre). Attackers have become more organised, adapting their tactics to corporate defence mechanisms, while companies need to improve their defences and ability to quickly resume operations after an incident.

A large-scale ransomware attack against Collins Aerospace caused disruptions at major airports in Europe; travellers, including those from Latvia, faced longer waiting times at check-in and boarding, as well as delayed flights. Riga Airport uses different automated check-in and boarding systems, and there was no direct impact as a result of this incident.

The attackers were able to affect many operators at the same time by targeting a single centralised supplier and service; analysis of the incident shows target the common vulnerabilities of service providers rather than individual airports, achieving a wider impact.

This proves that supply chain attacks are being used more and more frequently.

Recommended action:

- **conduct supplier security audits;**
- **impose stricter requirements in procurement;**
- **regularly check that the software used is updated and patches are installed.**

Key cyber threat trends and recommended steps

Trends	Latvian cyberspace situation and recommended steps
Supply chain compromise	Security, risks and management options for using third-party services. The entry into force of the Cabinet Regulation "Minimum Cybersecurity Requirements" (on 2 July 2025) is a positive step that will improve the overall level of cybersecurity, including ensuring the security of supply chains.
The human factor, outdated IT systems	The EU support programme promoting the transformation of corporate cybersecurity to strengthen capacity should be continued; centralised vulnerability management should be strengthened, and regular training for employees and IT security tests should be carried out.
Digital surveillance and increased risk of privacy loss	The chat app MAX, introduced in Russia, which is in fact a tool developed by the Kremlin for digital control, censorship, and surveillance of society, can also be downloaded and used in Latvia. The use of such an app poses a serious risk, as it can be used to pass on intelligence about Latvian citizens. ChatControl may pose a threat to the privacy of mobile device users, as it would provide law enforcement agencies with legal access to encrypted data. Experts point to the risks that it cannot be technically implemented without checking all content.
Targeted attacks using IoT data	IoT devices are becoming increasingly popular, but if unprotected, they can be used for malicious purposes. The implementation of IoT security standards and user awareness of the risks should be promoted.
The rise of hybrid threats	Due to geopolitical tensions, Latvia is a direct target for hybrid attacks (DDoS, disinformation, sabotage). During the reporting period, Russian hackers affected hydroelectric power plants in Poland and Norway. Such incidents highlight the need to strengthen the security of systems and operational technology (OT). To promote the security of industrial automation and control systems, CERT.LV offers security tests to energy, transport, water, and other infrastructure operators, and develops sensors for OT systems.
Malicious use of AI	Fake news content created with AI tools makes manipulation more difficult to detect. It is necessary to strengthen public media literacy and cooperation between the government and the media.

- **Geopolitically motivated attacks**

  Both as a reaction to foreign policy statements (Latvia's victory in international drone procurement in the context of support for Ukraine) and the broader influence operations of the DDoSIA group NoName0579(16) – these threats continue. In Q3, DDoS attacks were directed against several municipal websites, transport and telecommunications infrastructure. Short-term disruptions were observed, but most resources were adequately protected, and the attacks had no impact.

  Politically or ideologically motivated DDoS attacks carried out by hacktivist groups supporting the Russian Federation's aggression with the aim of creating public resonance and undermining trust in state institutions have been occurring in waves since 2022, and it is likely that the Baltic states will continue to be a long-term target of Russian cyber operations.

  To mitigate the impact of DDoS attacks, organisations are advised to use DDoS protection services. The Ministry of Defence funds a centralised DDoS protection service, which is available to state administration institutions free of charge. The provision of this service has been delegated to LVRTC.

Main conclusions

- **Uzbrukumi kļūst hibrīdi – Attacks are becoming hybrid**, exploiting both technological and human vulnerabilities.
- **Speed is a critical factor**, both in the attackers' response and on the defence side.
- **Resilience must be multi-layered** – at the technological, operational, organisational, and human factor levels.

These trends underscore the need for CERT.LV services – DNS firewall, incident response support, SOC capabilities, threat hunting, security testing, user education and training – this strengthens the cyber resilience and preparedness of technological and human resources for future threats.

CERT.LV services: monitoring, protection and testing

CERT.LV services, including the DNS firewall, support resolving incidents, Security Operations Centre (SOC), cyber threat hunting, security testing, education and training activities for the public, as well as other services, are an essential asset for mitigating risks and building resilience to increasingly intense and sophisticated cyber threats.

DNS firewall

In Q3 2025, as part of the DNS firewall service:

- **The number of DNS requests for malicious domain names** reached almost **4.6 millio**n, which is **81% more than in Q2 and 418% more than in Q3 of last year**. The increase was likely driven by seasonal factors (such as people returning to work after summer holidays). **There was also a noticeable increase in requests to various infected WordPress pages, but in most cases, there were no actual human clicks on these pages, and they were most likely automated requests (from firewall or proxy systems) that regularly check domain reputation.**
- **All of the lists maintained by the CERT.LV DNS firewall blocked cyber attacks** that protected users from visiting malicious sites **399 050** times, which is a significant increase – **36% more than in Q2 and 74% more than in Q3 of last year. Possible reasons for the increase could be seasonal or time-related factors – a cyclical increase that may change in the next quarter**. The number of attacks defended against also has a direct correlation with the number of active fraud campaigns.
- **Since its launch, the DNS firewall app has been downloaded 65 000 times** (31.8 K on Android and 32.9 K on iOS).

To strengthen public cybersecurity and resilience against threats while simultaneously educating people about cyber hygiene and digital fraud schemes, during the reporting period, experts from CERT.LV actively gave interviews as part of the cybersecurity campaign “Sniff out the scheme!” (“Ož pēc shēmas!”) and emphasised the importance of the DNS firewall as an effective protection solution against modern cyber threats.

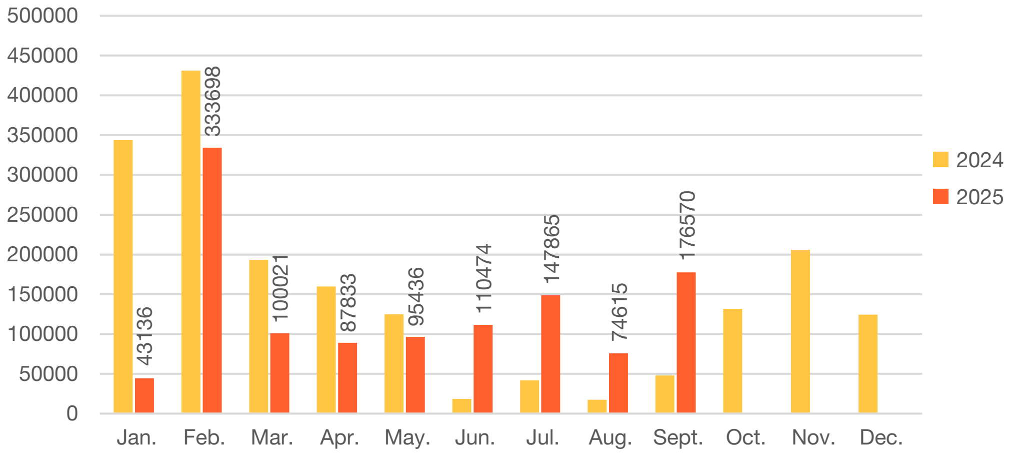


Figure 6. Cyber attacks repelled across all CERT.LV zones

Major active defence episodes during the reporting period

Warnings	Quantity
Vulnerable websites based on the WordPress content management system and infected with malware	30805
Websites that contain malicious JavaScript code and display fake pop-up windows	22026
Websites that offer fake financial services	14621
The use of the “DELFI” image in advertising campaigns for fraudulent cryptocurrency investment platforms	12316
Use of CSDD branding in fake website campaigns	9823
Use of Jauns.lv branding in fraudulent cryptocurrency investment platform advertising campaigns	7485
Use of DPD branding in fake website campaigns	2404
Use of FedEx branding in fake website campaigns	2383
Use of State Revenue Service branding in fake website campaigns	1542
Use of Latvijas Pasts image in fake website campaigns	1231

Threat early warning system (EWS)

The Cybersecurity Early Warning System (EWS) is a service provided by CERT.LV that analyses traffic anomalies and identifies signs of cyber-attacks in the service recipient's infrastructure.

CERT.LV continues to maintain and expand the EWS system.

In Q3 2025, the number of warnings generated by EWS was **1.3 billion**, which is 24% less than in the previous quarter and 29% less than in Q3 of last year.

The most common high-priority cyber threat alerts by CERT.LV Signature Group were related to computer viruses, phishing and potentially malicious websites, as well as to botnets, scams and virus indicators.

Every month, EWS records an average of **6000** high-priority cyber threats (incidents with high danger potential) in national and municipal-government, as well as ICT-critical infrastructure.

Security Operations Centre (SOC)

Since 2024, when the CERT.LV SOC service was launched for institutions, the active development of the CERT.LV SOC service and the attraction of new customers have continued, expanding the customer base in accordance with the NCSL to promote more effective protection and resilience against cyber threats.

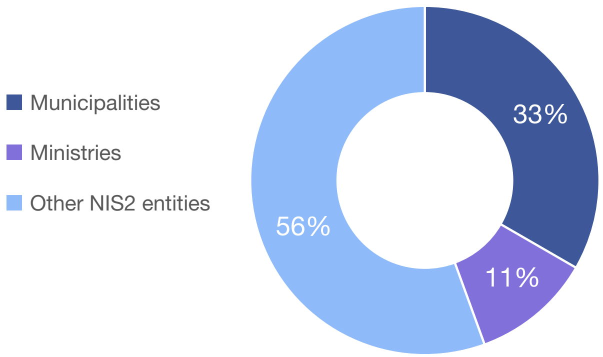


Figure 7. CERT.LV SOC customer sector structure in Q3 2025 (percentage of total)

Overview of security alert reports

- **Visibility gained over 40 720 devices**, including servers and workstations.
- The number of end devices increased by **6892 devices – an increase of approximately 20% of the total volum**e, resulting in an increase in the number of security alert reports.
- More than **15 million** security alerts were recorded, which is **43% more** than in Q2. The large increase can be explained by greater visibility in the infrastructure of new customers and the time taken to process alerts in order to investigate and suppress false positives.
- When processing security alert reports, **486 cases were created manually**.

Number of devices with visibility gained	**40 720**
Number of registered security alert reports	**15M+**
Manually created cases	**486**
False positives	**472**
Number of incidents	**14**
Low level of alert:	**4M+**
Medium level of alert	**11M+**
High level of alert:	**64K+**
Critical level of alert:	**5K+**

Figure 8. Dynamics of security alert reports in SOC customer infrastructure (data as of 30.09.2025)

The vast majority of alerts are medium and low level, which may be related to system noise, false positives, or less serious cases.

Only 0.5% of all alerts are high/critical level. The number of critical incidents (5K+) is quantitatively a relatively small percentage of the total (0.03%), but they require the most attention.

High-level alerts (64K+) place a significant burden on the SOC team. They are indicators of potentially dangerous attacks and require careful investigation.

The absolute number of critical and high-level alerts (~69 000) indicates constant serious threats.

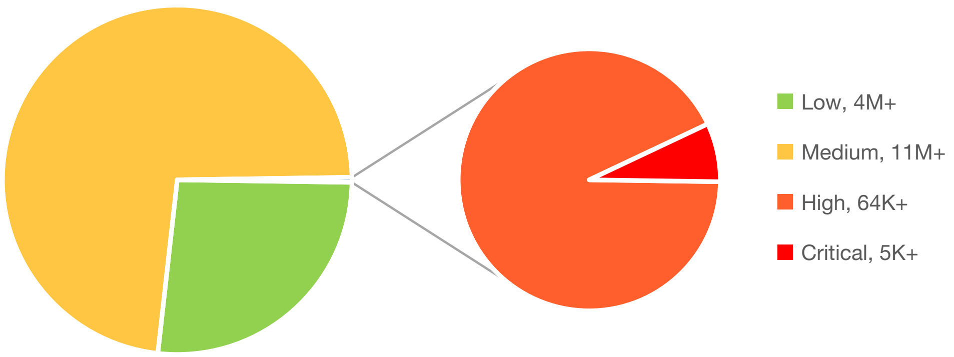


Figure 9. Security alert reports registered by CERT.LV SOC in Q3 2025.

While monitoring customer infrastructure with the SOC service provided by CERT.LV, 14 cyber incidents were registered in Q3 2025.

The most frequently detected cyber incidents and recommended actions

Cyber incidents	Risks	Recommended action
Brute-force attacks	Workstations connected to external networks, bypassing corporate security policies and devices exposed to the internet without a local firewall. This increases the vulnerability to automated attacks.	► Install local firewalls. ► Provide a VPN connection to the corporate network. ► Use strong passwords and MFA.
Use of unwanted software in a corporate environment	Unofficial activation tools, games, file-sharing software (BitTorrent), etc., may contain malware that threatens the integrity of the system and may compromise the system.	► Implement a software whitelist. ► Uninstall unauthorised apps and programs used for private purposes. ► Remove outdated or duplicate applications ► Do not use software from non-NATO/EU manufacturers. ► Do not use multiple remote access tools at the same time.
Malware that spreads via USB flash drives or fake CAPTCHAs (ClickFix)	Users are misled by fake CAPTCHAs that mimic security checks. Activating the malware allows access to login details, email correspondence, and other confidential information that can be used in future attacks.	► Prevent executable files from being launched from USB drives. ► Update your browsers regularly. ► Use browser extensions that block suspicious scripts. ► Educate staff on social engineering techniques.

Cybersecurity threat hunting operations

At the end of the reporting period, the analysed cybersecurity threat hunting operations since 2022 totalled:

- **more than 162 000 end devices** (the number of end devices **increased by 2000** in Q3);
- **almost 40 public** sector institutions providing essential and important services, and ICT critical infrastructure companies;
- the presence of foreign APTs was identified in the equipment of approximately **20%** of organisations.

IT system security tests and phishing attack simulation campaigns

In Q3 2025, CERT.LV conducted **four IT system security tests**, during which a total of more than **10 vulnerabilities with varying levels of risk were identified**.

CERT.LV also conducted a cyberattack simulation for one of Latvia's critical infrastructure service providers, during which several critical vulnerabilities were identified and eliminated that would have allowed attackers to completely take over the company's IT systems, and managed critical infrastructure.

During the reporting period, CERT.LV conducted a total of **four phishing attack simulation** campaigns to train and promote the ability of organisation employees to identify potentially risky behaviour patterns, as well as recognise and prevent cyber threats and information leaks. Total campaign audience: **1541 persons**.

Coordinated vulnerability detection (CVD)

The CVD reporting practices facilitate the earlier discovery of vulnerabilities, helping coordinate their investigation and elimination, while achieving better efficiency in organising security measures.

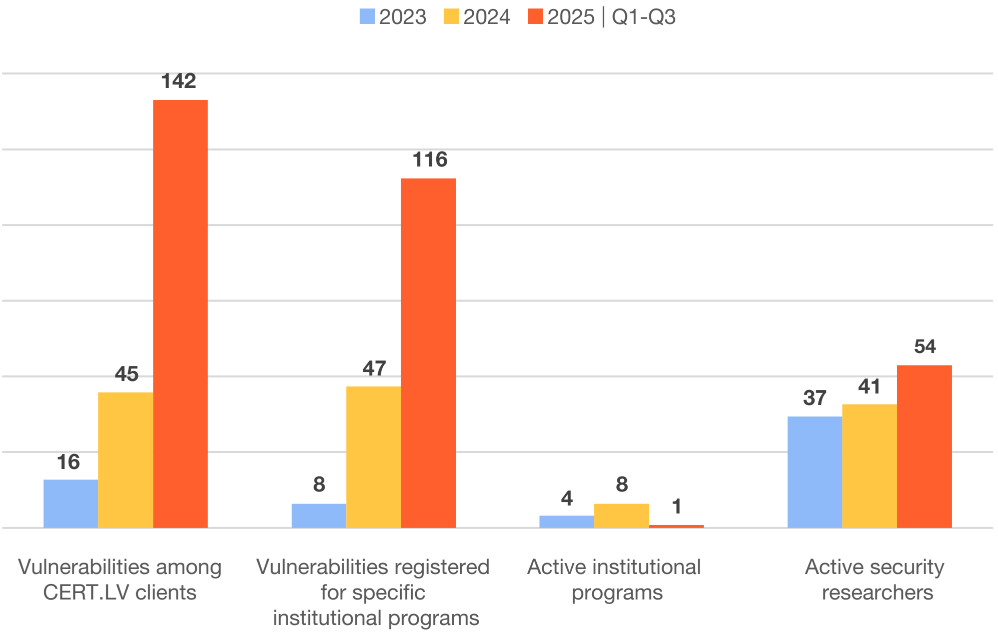


Figure 10. CVD platform: Number of vulnerability reports in Latvia

As of the end of the reporting period (30.09.2025), the CVD platform has registered a total of:

- Security researchers: **132 assets** (Q3 +18)
- New institution programmes: **13**
- Vulnerability reports: **372** (Q3 +159), including:
  - ✓ Vulnerabilities among CERT.LV clients: **203** (Q3 +100)
  - ✓ Vulnerabilities reported on specific institutional software: **171** (Q3 +59)

CERT.LV offers a broad range of cybersecurity services that effectively protect the ICT infrastructure of organisations and bolster their cyber resilience.
Protect and secure your cyberspace today with the expertise and advice of CERT.LV: https://cert.lv/lv/pakalpojumi
If you would like to receive a CERT.LV service, please write to us at cert@cert.lv

CERT.LV's mission is to promote cybersecurity in Latvia.

The main tasks of CERT.LV are to maintain and update information on cybersecurity threats, provide support to state institutions in the field of cybersecurity, assist in resolving cybersecurity incidents for any natural or legal person if the incident involves a Latvian IP address or a .LV domain, as well as to organise informational and educational events for government employees, IT security professionals, and other interested parties.

The report includes publicly available information and does not contain any restricted information. This report is for information only.

Contact CERT.LV:

Phone: +371 67085888

E-pasts: cert@cert.lv

Tīmekļa vietne: cert.lv

Follow CERT.LV news on:

@cert.lv