2026 Q2

LATVIAN CYBERSPACE SITUATION

PERIOD: 01.04.2026-30.06.2026

CERT.LV
Cyber Incident Response Institution

Institute of Mathematics and Computer Science University of Latvia

Ministry of Defence Republic of Latvia

Summary

Cyberspace situation assessment

The cybersecurity threat level in Latvia remains high, and the intensity of cyber threats continues to increase over the long term. This is driven by the geopolitical situation, the increasingly widespread exploitation of vulnerabilities and the use of artificial intelligence in cyber attacks, and users' uncritical reliance on digital tools. These factors require continued systematic cyber risk management and the consistent strengthening of organisations' comprehensive cyber resilience.

In Q2 2026, **673 manually processed cyber incidents** were recorded, which is 20% fewer than in the previous quarter and 5% fewer than in the corresponding period last year. The **number of identified compromised devices also decreased to 396 444**, which is 48% fewer than in the previous quarter and 14% fewer than a year ago. However, both indicators **remain significantly above the 2022-2024 average**, indicating that the **cybersecurity threat level remains high**.

Main threats

The main initial compromise methods continue to be the exploitation of vulnerabilities in information systems accessible via public networks and phishing attacks targeting corporate network users. The risk remains elevated for organisations with outdated or insufficiently maintained websites, unpatched content management systems, and their plugins.

Ransomware attacks and data breaches continue to have the most significant impact on organisations. This is demonstrated by the large-scale cyber attack on the IT infrastructure of JSC Latvijas valsts meži (LVM) during the reporting period, where an unremedied vulnerability in a publicly accessible system became the entry point for a broader attack. This case clearly demonstrated that even a single critical vulnerability can significantly affect an organisation's business continuity, cause system disruptions, create a risk of data breaches, and require critical IT systems to be shut down.

At the same time, the risks posed by social engineering, identity compromise and information-stealing malware are increasing. Denial-of-service, or DDoS cyber attacks remain an effective instrument of geopolitical pressure and a persistent threat.

Fraud remains the quantitatively dominant type of cyber incident and primarily affects residents. Data compiled by the Finance Latvia Association for the first six months of 2026 also show that customers of Latvia's largest banks lose an average of around EUR 1.3 million to fraud each month. Therefore, alongside technical security measures, it is essential to continue strengthening public awareness and resilience against social engineering attacks, particularly phishing.

Russia remains the main source of cyber threats to Latvia. The activities of Russia-backed cyber attackers and hacktivists, including in response to Latvia's expressed support for Ukraine, are likely to continue.

Given the current nature of the threats, organisations should prioritise strengthening vulnerability management, continuous cybersecurity monitoring (SOC/EDR/XDR/SIEM), the use of multi-factor authentication, backup management, supply chain security, and regular user training, while periodically testing incident response and business continuity plans.

CERT.LV performance results

At the same time, growing threats are driving the development of cybersecurity capabilities. They increase demand for data-driven services to improve the ability to identify and mitigate threats in a timely manner.

In the first six months of 2026, the preventive work of the CERT.LV Cyber Incident Response Team and the active protection provided by the DNS firewall **prevented more than 5 million attempts to access malicious websites** – 6.5 times more than in the corresponding period last year. A record high of 1.1 million was reached in June.

Summary

By improving automated threat detection methods, in Q2 CERT.LV **proactively identified and prevented 1166 active fraud campaigns** – 900 more than in the previous quarter – before they reached users on a large scale and caused losses.

During the reporting period, **18 IT system security tests were conducted, identifying 31 vulnerabilities**, including critical and high-impact vulnerabilities, which were remediated before they could be exploited in cyber attacks.

Organisations' endpoint-level visibility is increasing through the implementation of CERT.LV Security Operations Centre (SOC) services in accordance with national regulations. **Visibility was provided across a total of 57 021 endpoints**, enabling threats to be identified and mitigated in a timely manner and resilience to be strengthened systematically.

Continuing cybersecurity training and public education efforts, **8632 participants were trained at 95 events during the reporting period** – 34% and 19% more, respectively, than in the corresponding period last year.

Internationally, Latvia's role in the European cyber incident response team cooperation community was strengthened by the **TF-CSIRT meeting in Riga**, which brought together more than 150 industry experts. The forum **focused on current cyber threats and challenges in Latvia**. This is particularly important at a time when cyber incidents are becoming increasingly complex and closer cooperation between organisations and countries is critically important.

To strengthen and improve institutional cooperation and preparedness to respond to large-scale cyber incidents, **the Cyber Europe exercise assessed the Latvian transport sector's ability** to respond to complex cybersecurity incidents in a coordinated manner.

The eighth **Threat Hunting Operation organised by CERT.LV, with an expanded presence, demonstrates growing operational maturity** and reinforces it as an internationally recognised model of civil-military cooperation.

The Latvian-Singaporean joint team's **1st place finish in the international cyber defence exercise Locked Shields 2026** demonstrates the high professional competence of Latvia's cybersecurity specialists and their ability to respond effectively to complex cyber incidents. It also strengthens the cooperation model between public administration, the military sector, and technology companies.

Main conclusions

Although the number of cyber incidents and identified compromised devices decreased during the reporting period, the cybersecurity threat level in Latvia remains high, and the threat intensity continues to increase over the long term. The greatest risks to organisations are posed by vulnerabilities that are not remediated in a timely manner, identity compromise and social engineering attacks, which often serve as the starting point for broader incidents.

At the same time, organisations' endpoint-level visibility continues to increase through the implementation of the CERT.LV SOC, DNS firewall, and other data-driven cybersecurity services, enabling cyber incidents to be prevented, detected, analysed, and contained in a timely manner, or responded to and resolved.

In the future, organisational resilience will increasingly depend on effective cybersecurity risk management, continuous cybersecurity monitoring (SOC/EDR/XDR/SIEM), the use of multi-factor authentication, backup management, supply chain security, and regular user training, while incident response and business continuity plans are tested regularly.

Key indicators

673 (-5%)

Manually processed cyber incidents
Q2 2026 vs Q2 2025

~369K (-7%)

Number of identified compromised devices
Q2 2026 vs Q2 2025

441 (-4%)

Fraud – quantitatively dominant incident type
Q2 2026 vs Q2 2025

73 (+56%)

Compromised devices – fastest growth
Q2 2026 vs Q2 2025

~2,5M (754%)

Attempts to access malicious websites prevented by the CERT.LV DNS firewall
Q2 2026 vs Q2 2025

1 166 (+900)

Fraud campaigns proactively identified and prevented before reaching users
Q2 2026 vs Q2 2025

105 (an increase of 13 in Q2)

Total number of institutions (NCL subjects) using the CERT.LV SOC service
Total data as at the end of Q2 2026

57 021 (an increase of 32% in Q2)

Visibility of organisational endpoints provided through the CERT.LV SOC service
Total data as at the end of Q2 2026

185 (an increase of 19 in Q2)

Total number of registered security researchers on the CVD platform
Total data as at the end of Q2 2026

683 (an increase of 142 in Q2)

Total number of vulnerability reports registered on the CVD platform
Total data as at the end of Q2 2026

95 (+34%)

Cybersecurity awareness activities/events conducted by CERT.LV experts Q2 2026 vs Q2 2025

8 632 (+19%)

Audience reached through CERT.LV expert activities/events
Q2 2026 vs Q2 2025

Contents

1. Cybersecurity threats: statistics and trends

The cybersecurity threat level in Latvia remains high, and the intensity of cyber threats continues to increase over the long term. This is driven by the geopolitical situation, the increasingly widespread exploitation of vulnerabilities and the use of artificial intelligence in cyber attacks, and users' uncritical reliance on digital tools. These factors require continued systematic cyber risk management and the consistent strengthening of organisations' comprehensive cyber resilience.

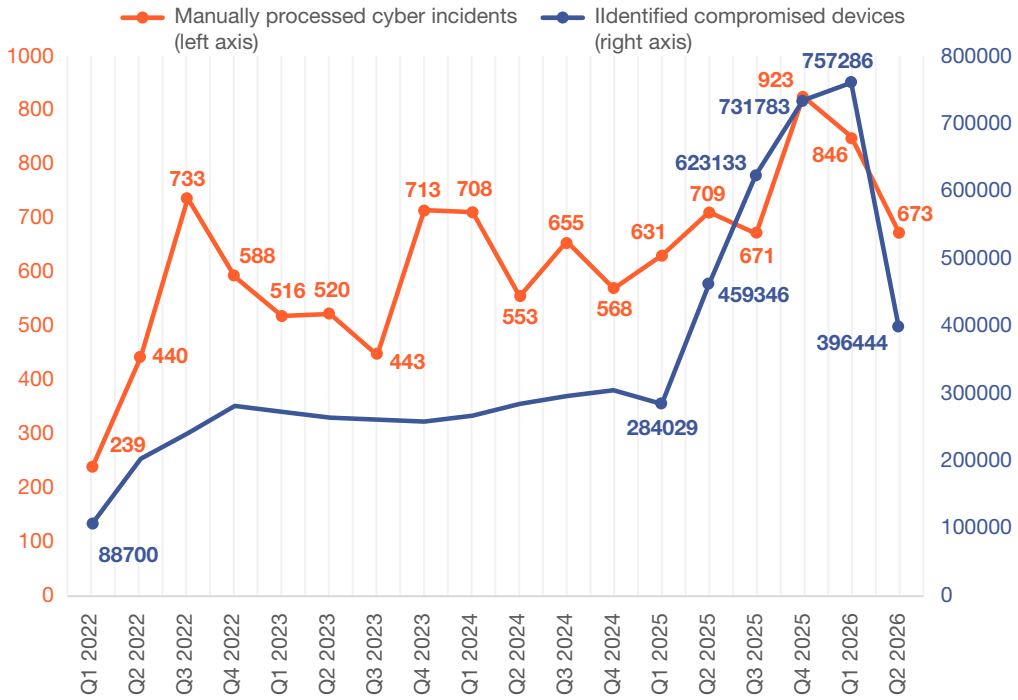

Figure 1. Dynamics of cyber incidents and identified compromised devices (number)

Manually processed cyber incidents

In Q2 2026, **673 manually processed cyber incidents** were recorded in Latvia, which is **20%** fewer than in Q1 2026 and **5%** fewer than in the corresponding period last year.

The number of cyber incidents[1] decreased for the second consecutive quarter, most likely due to the implementation of more effective threat detection and prevention mechanisms. By improving automated threat detection methods, in Q2 **CERT.LV proactively identified and prevented 1166 active fraud campaigns – 900 more than in Q1 – before they reached users on a large scale and caused losses**.

In addition, CERT.LV proactively monitors and blocks identified fraud campaigns, promptly adding their indicators to the DNS firewall. Public involvement also plays an important role. Reports from residents help to promptly identify new fraud campaigns and protect other users in a timely manner. **In the first six months of 2026, the CERT.LV DNS firewall prevented more than 5 million attempts to access malicious websites, which is 6.5 times more than in the corresponding period last year**.

However, the number of cyber incidents remains high and exceeds the 2022–2024 average. Since Russia's full-scale invasion of Ukraine in 2022, the number of cyber incidents recorded in Latvian cyberspace has increased sixfold. The long-term trend remains upward, with the intensity of cyber threats continuing to increase.

1 **Cybersecurity incident** (hereinafter – cyber incident) – an event that threatens processed data or the availability, authenticity, integrity, or confidentiality of services offered by or accessible through network and information systems.

Identified compromised devices

Although the **number of compromised devices identified** by CERT.LV **decreased significantly** in Q2 2026 (by **48%** compared with the previous quarter and by **14%** compared with the corresponding period last year), the **396 444** identified compromised devices indicate that the cyber threat level remains high.

This trend is partly explained by changes in the availability of data sources, as one of the previously used sources no longer provides information on potentially infected devices in Latvia.

Several near-cyber incidents were also prevented[2]. CERT.LV identified and remediated vulnerabilities in 76 industrial control systems, preventing their exploitation in potential attacks.

A positive trend is the gradual increase in the number of organisations using CERT.LV Security Operations Centre (SOC) services in accordance with the requirements of the National Cybersecurity Law (NCL). This expands the number and visibility of monitored endpoints, improves the ability to identify cyber threats in a timely manner, and strengthens the overall cyber resilience of both organisations and the country.

Overall, it can be concluded that despite the decrease in the number of cyber incidents and identified compromised devices, the figures remain significantly above the 2022–2024 average, and the cyber threat level remains high. At the same time, the data indicate that the security measures implemented by organisations, including the use of SOC services, are producing positive results; it is therefore important to continue systematic cyber risk management and consistently strengthen organisations' comprehensive cyber resilience.

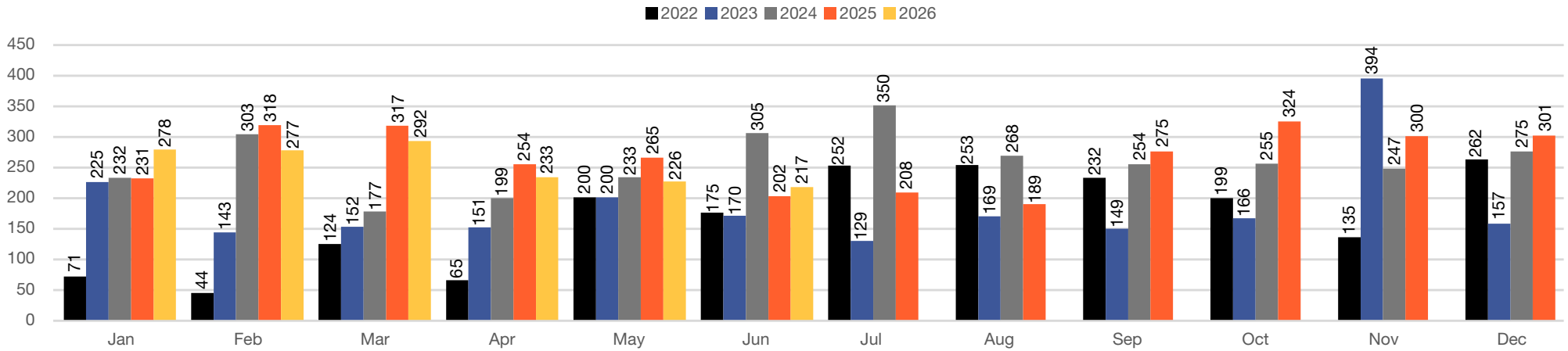

Figure 2. Cyber incident trends (monthly breakdown)

2 **Near cyber incident** – an event that could have threatened processed data or the availability, authenticity, integrity, or confidentiality of services offered by or accessible through network and information systems, but the full execution of which was successfully prevented or did not materialise.

For cyber weather observers, a monthly report on the most significant cyber incidents and threats in Latvian cyberspace, organised into TOP 5 categories, is available in the News section of the CERT.LV website – https://cert.lv/lv/zinas/kiberlaikapstakli.

2. Top reporting-period cyber threats and key events

Cyber incident types with the highest volumes

During the reporting period, a positive trend was observed, with decreases in common incident types (fraud, intrusion attempts, and availability disruptions); however, the proportion of compromised devices increased, while incidents caused by malicious code continued to account for a significant share.

- **Fraud continues to account for by far the largest share of all manually processed cyber incidents**; however, during the reporting period, the number fell to **441** incidents, 21% fewer than in Q1 and 4% fewer than a year ago. At the same time, this is still 6 times more than any other type of incident.
- **The number of malicious code incidents remained unchanged compared with Q1, but increased by 60% year on year.** Malware has become a consistently used attack tool. The proportion of automated attacks is increasing. Among the most frequently observed malware, information-stealing malware (ClickFix), remote access trojans (RATs), and ransomware variants predominated.
- **Compromised devices were the only incident category to increase during the reporting period** – by 18% compared with Q1 and by 56% year on year. However, this indicator is also based on the external threat intelligence feeds used and may therefore be affected by changes in the coverage or detection methodology of those sources. Consequently, the observed increase is explained not only by an actual rise in the number of compromised devices, but also by the potential impact of the data sources.
- **Intrusion attempts decreased by almost half.** This indicates more effective attack blocking, active DNS firewall protection, and the operation of IDS/IPS[3], as required by Latvia's cybersecurity regulations. This is a positive trend, but it does not yet mean that the overall risk has decreased.
- **The risks associated with configuration deficiencies remain high** – although there was a 33% **decrease compared with Q1, the number of incidents doubled year on year**. This continues to indicate inadequate configuration management and non-compliance with security policies.
- **The decrease in availability disruptions (DDoS)** (-67% compared with Q1) **indicates effective defence mechanisms and strong infrastructure resilience**. The multi-layered defence mechanisms used have successfully mitigated the impact of DDoS attacks, meaning that in most cases, residents do not even notice these attacks in their daily lives. However, this does not reduce the risk – these attacks remain a persistent threat, particularly in the context of the current geopolitical situation.

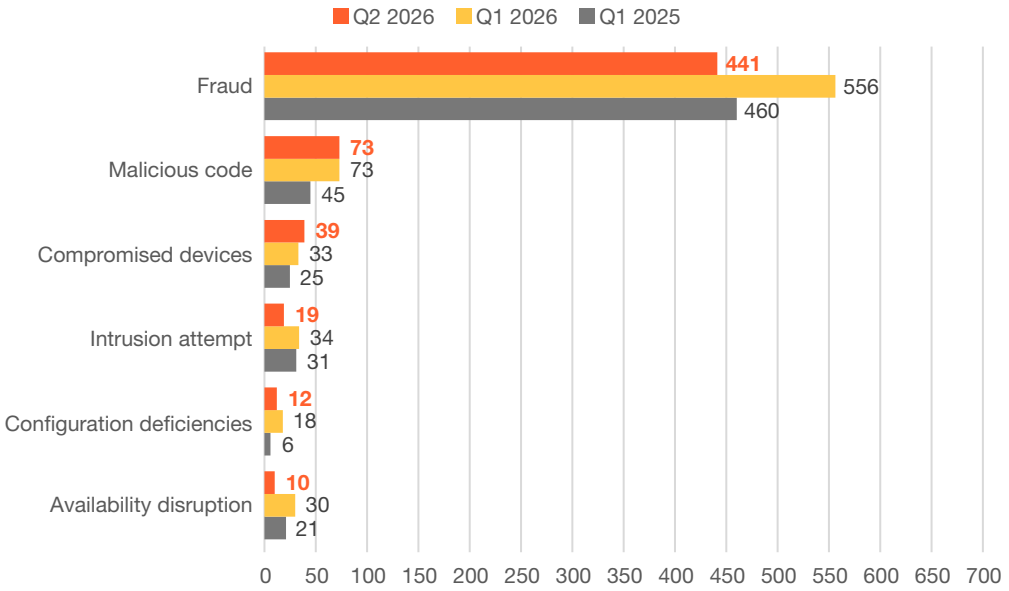

Figure 3. TOP 6 cyber incident types (number)

3 **IDS** – Intrustion Detection System;
IPS – Intrustion Prevention System.

TOP 10 malware

The most widespread malware types in Q2 2026 indicate large-scale, automated, and persistent threats. Android.badbox2 continues to dominate the TOP 10 malware list, with its prevalence increasing by 9% compared with the previous quarter.

Android.badbox2 is a mobile botnet variant capable of infecting devices, for example, by stealing credentials and remotely controlling the device. Its spread indicates significant and targeted activity on Android devices and points to mass infection campaigns using unofficial app installations or fake updates. The main risks are the interception of access credentials, compromise of infected end devices, and their use in subsequent cyber-attacks. Organisations and individual users may not even be aware that their IP address is “participating” in botnet attacks.

The remaining top malware together account for a quantitatively smaller share; however, they demonstrate a diverse combination of attack vectors and increase compromise risks.

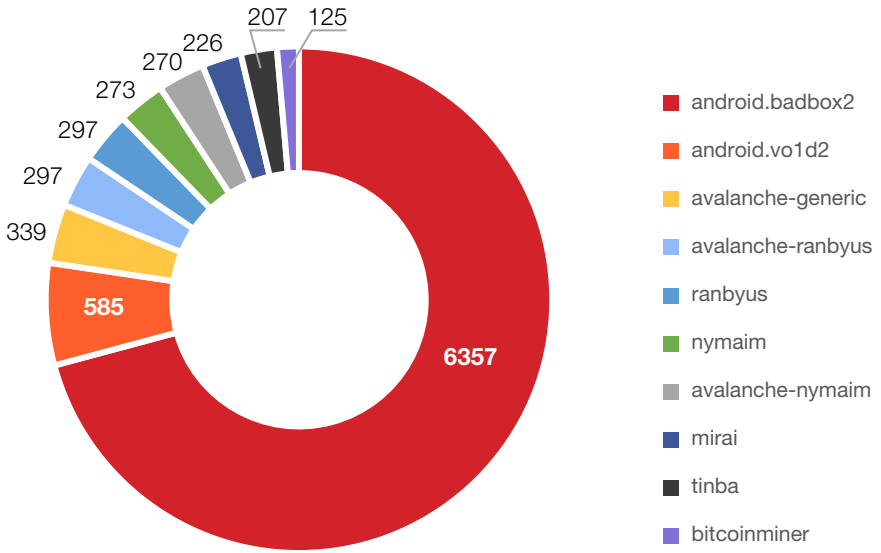

Figure 4. TOP 10 malware (number; Q2 2026)

Main trends in cyber attack types

Vulnerability management deficiencies and data breach risks are intensifying

Attacks against organisations continue to make widespread use of software vulnerabilities that have been known for several years and for which vendors have published patches. This highlights the importance of regularly updating software.

In terms of impact, the most significant threats to organisations remain encrypting ransomware attacks and data breaches, which often begin with the exploitation of vulnerabilities in publicly accessible systems. This is demonstrated by the large-scale cyber attack on the IT infrastructure of JSC Latvijas valsts meži (LVM) during the reporting period, where an unremedied vulnerability in a publicly accessible system became the entry point for a broader attack.

The LVM case clearly demonstrated that even a single critical vulnerability can have a significant impact on an organisation’s business continuity,

The most common types of malware

- **User data-stealing malware**
- **Botnets**
- **Remote control trojans for data extraction and infrastructure compromise**

“Infostealer” type data-stealing malware is used to extract access credentials from web browsers or unencrypted files. It is distributed as malicious browser extensions or executable files attached to phishing emails.

causing system disruptions, data breach risks, and the need to restrict and shut down critical IT systems.

CERT.LV has published **recommendations for improving the cyber resilience of IT infrastructure on its website**.

Vulnerabilities also continue to be exploited to gain unauthorised access to websites and redirect users to malicious websites or distribute malware. During the reporting period, several cases of .lv websites being compromised were identified, with visitors redirected to gambling websites or ClickFix schemes.

In quantitative terms, configuration deficiencies caused by human factors and inadequate security standards account for the largest share of identified compromised devices.

The success of fraud increasingly depends on the ability to influence people

Social engineering, rather than bypassing technical security solutions, is playing an increasingly important role in fraud campaigns. Attackers adapt fraud schemes to current events, popular services, and well-known brands, while the use of artificial intelligence (AI) makes fraudulent messages increasingly credible and harder to distinguish from genuine communication.

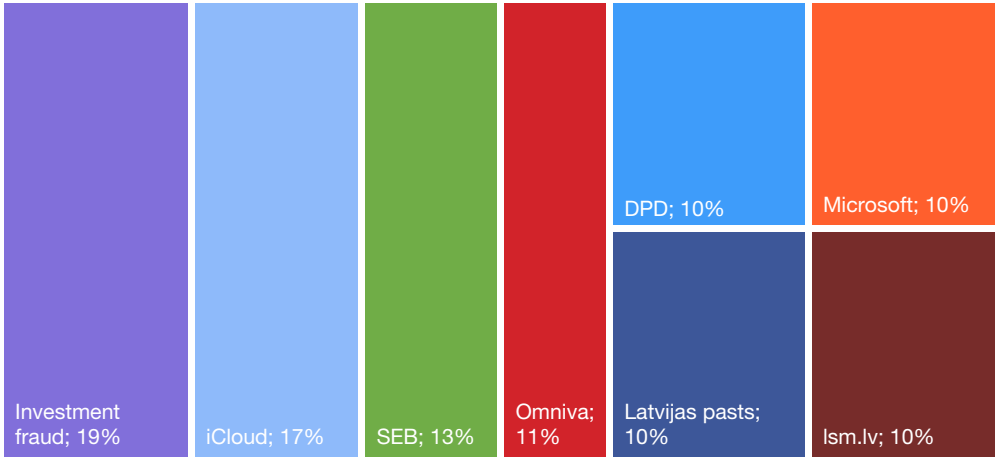

Figure 5. Most common fraud campaigns and themes (as a percentage of the total; Q2 2026)

Investment fraud campaigns continued to dominate during the reporting period, while attacks also continued to exploit the names of banks, public authorities, delivery companies, and other trusted organisations, as well as impersonating representatives of authoritative institutions, to obtain payment card details or authentication information, or induce victims to authorise fraudulent payments themselves.
At the same time, sophisticated social engineering techniques such as ClickFix, in which users are persuaded to activate malware on their own devices, are becoming increasingly common.

The impact of threats remains high. Data from the Finance Latvia Association[4] indicate that in the first **six months of 2026, customers of Latvia's largest banks lost EUR 7.83 million to fraud**, while more than EUR 11 million in attempted fraud was prevented. Fraudsters steal an average of around EUR 1.3 million per month. This indicates **that users remain the primary target of attacks and that social engineering is one of the most significant cyber threats**.

Fraud attempts impersonating booking.com are increasing

Fraud attempts impersonating booking.com are increasing, exploiting the holiday season and the relevance of travel bookings. Fraudsters use WhatsApp messages or emails to impersonate booking.com or hotel representatives and redirect users to fake links to obtain payment card details.

This trend is particularly dangerous because attackers are shifting from mass, generic phishing messages to more personalised and credible scenarios. The attacks are based on genuine user situations – upcoming travel and hotel bookings. Fraudsters exploit both a sense of urgency and a trusted international brand. For residents and organisations with frequent travel or business trips, this may result in financial losses, misuse of personal data, and disruption to travel plans.

CERT.LV has compiled **recommendations on how to protect yourself from fraudsters impersonating booking.com** on its website.

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

Account takeover attempts are increasing in messaging apps

During the reporting period, attempts to take over residents' WhatsApp and Signal accounts using social engineering techniques continued. Attackers attempt to obtain authentication details or verification codes by exploiting residents' inattention and insufficient knowledge of app security features. Account takeover may result in unauthorised access to private communications, facilitate fraud in the victim's name, and increase the risk of data breaches.

CERT.LV has compiled **recommendations on how to strengthen account security and reduce risks** on its website.

Security risks to political parties' digital resources are increasing in the context of elections

As the 15th Saeima elections approach, the risk of cyber threats and disinformation campaigns targeting political parties and their digital resources is increasing. In the digital age, political parties and their representatives may also become significant targets of cyber attacks and disinformation campaigns, particularly during preparations for elections. To reduce security risks, CERT.LV has initiated preventive measures by sending letters offering cybersecurity support to all state-funded political parties.

Artificial intelligence (AI) is playing an increasingly important role in both attacks and defence

AI is increasingly enhancing the scalability and automation of cyber attacks. Moreover, the threat is no longer limited to an attacker using AI as a tool, but may also take the form of an autonomous system conducting a continuous, adaptive campaign. Human response speed alone is no longer sufficient against such threats.

Organisations therefore have a growing need to develop AI-based cybersecurity capabilities as well. Automated data analysis and AI solutions enable cyber threats to be identified more quickly, large volumes of data to be analysed, and suspicious activities to be detected in a timely manner. Automated data processing and analysis solutions are already being used in Latvia to prevent cyber attacks. As the experience of other countries also shows, AI solutions are particularly useful for the early identification of risks and in-depth analysis of complex datasets.

Attacker motivations

- **Financially motivated cyber attackers:** main areas – ransomware, business email compromise (BEC), investment fraud, and data monetisation to generate profit or obtain other benefits.
- **Politically motivated and state-backed attackers** (APTs, or Advanced Persistent Threats): unlike financially motivated attackers, APT groups do not seek quick gains, but prolonged and undetected access to the systems of public authorities, critical infrastructure (CI), and other strategically important organisations in order to obtain information and sensitive data. **Latvia also faces an elevated risk of APT information influence operations before the 15th Saeima elections.**
- **Destructive attacks**, the objective of which is not direct financial gain, but the disruption of service availability or sabotage, using cyber attacks to raise the attacker's profile. These may take the form of DDoS attacks, attempts to gain control of CI systems, or other attacks intended to disrupt the continuity of essential services, create a sense of insecurity in society, and undermine trust in public digital services.

Regional threat context

- **Russia** remains the primary source of cyber threats. Russian hacktivist activity (often linked to and observed following public expressions of support for Ukraine in Latvia's media space) is expected to continue. The impact of these attacks is still assessed as low. The main risks are related to reputational damage to state institutions and influence on public opinion and the information space. An attack may disrupt the operation of the targeted website and the availability of the service.

- Activity of groups linked to **China** (PRC) with economic motivation (data acquisition, access to technologies); increasingly intensive attempts to spread within networks and access sensitive information.
- Occasional involvement of **Belarus**, mainly as part of Russia's "orchestrated" hybrid operations.

Targeted sectors

CERT.LV regularly identifies attempted attacks against state and municipal institutions, the financial sector, healthcare, telecommunications companies, educational institutions, and critical infrastructure (CI).

The threat to operational technology (OT), which is used to monitor and control physical processes, equipment, and infrastructure providing essential services to society, is increasing.

Russia-backed hacktivist groups also continue to conduct waves of DDoS attacks against Latvian public authorities and CI service providers. Although these attacks have not caused prolonged service disruptions, they demonstrate continued interest in Latvia's strategically important sectors.

Main conclusions and recommendations

- The cybersecurity threat level in Latvia remains high, and the long-term trend continues to be upward. This is driven by the geopolitical situation, the increasingly widespread exploitation of vulnerabilities and the use of artificial intelligence in cyber attacks, and users' uncritical reliance on digital tools. These factors require continued systematic cyber risk management and the consistent strengthening of organisations' comprehensive cyber resilience.
- Cyber attacks most commonly exploit vulnerabilities in information systems accessible via public networks or use phishing attacks targeting corporate network users. Every organisation must have a thorough and responsible understanding of its infrastructure, implementing updates and security patches in a timely manner to strengthen system resilience and ensure business continuity.
- The misuse of trust and identity compromise are growing risks, while information-stealing malware is actively used to compromise accounts and conduct further cyber attacks.
- DDoS attacks remain an effective instrument of geopolitical pressure and a persistent threat.
- Fraud remains the quantitatively dominant type of cyber incident in Latvia and primarily affects residents. Data compiled by the Finance Latvia Association for the first six months of this year also show that an average of around EUR 1.3 million is lost to fraud each month. Therefore, alongside technical security measures, it is essential to continue strengthening public awareness and resilience against social engineering attacks, particularly phishing.
- Organisations should prioritise strengthening continuous cybersecurity monitoring (SOC/EDR/XDR/SIEM), vulnerability management, the use of multi-factor authentication, backup management, supply chain security, and user training, while regularly testing incident response and business continuity plans.

3. CERT.LV services: protection and testing

3.1. DNS firewall

Campaign-based fraudulent activity regularly occurs in Latvia, including redirection to fake websites to obtain credentials for bank, email or social media accounts, as well as the distribution of malware in cyberspace.

CERT.LV proactively monitors and stops identified fraud campaigns, promptly adding campaign indicators to the DNS firewall. The DNS firewall mobile app protects users not only from fraud campaigns in cyberspace, but also from identified fraudulent calls.

In Q2 2026, the CERT.LV DNS firewall, using the lists it maintains, **prevented more than 2.5 million attempts to access malicious websites – 2% more than in the previous quarter and 754% more than in the corresponding period last yea**r (the statistics do not include data from lists maintained by other competent state authorities to restrict illegal online content).

In the first six months of this year, the CERT.LV DNS firewall prevented more than 5 million attempts to access malicious websites, which is 6.5 times more than in the corresponding period last year. In June, a record high of approximately 1.1 million was reached.

In 2026, activity remained very high in almost every month. The average monthly volume of blocked requests reached 830 thousand – indicating the persistent activity of fraud campaigns proactively identified and prevented by the CERT.LV DNS firewall.

~2.5 million – attempts by users to access malicious websites prevented in Q2
~30 min. – average response time until the identification and addition of the indicator to the DNS firewall
~88 thousand – downloads of the DNS firewall mobile app on Android and iOS devices (since 2024)
~5.2 million – DNS requests for malicious domain names in Q2

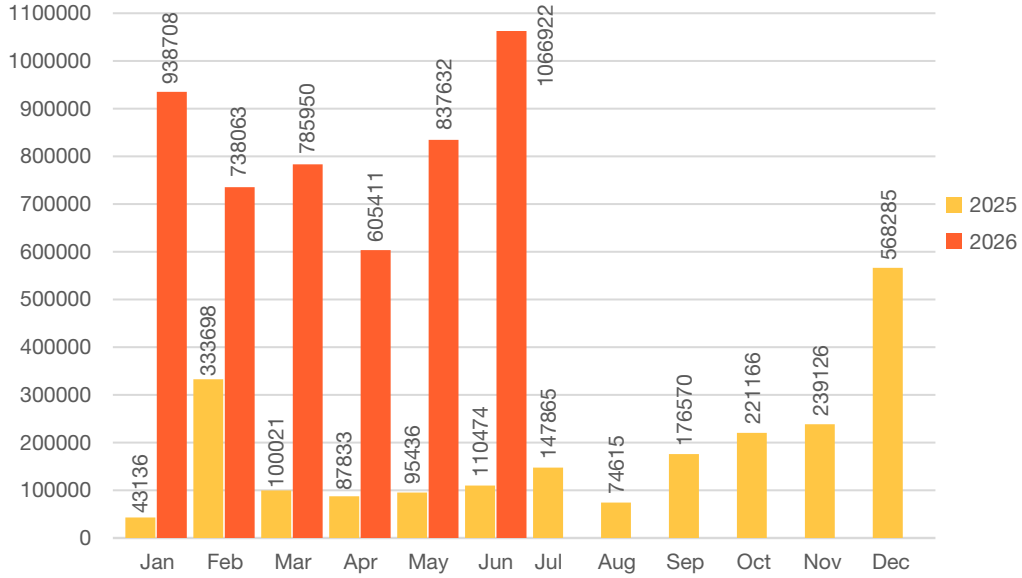

Figure 6. User requests to malicious websites prevented by CERT.LV DNS firewall lists* (*cert-shield, malware, phishing, high-risk)

Major active defence episodes during the reporting period:

- requests to a command-and-control server (C&C) used by remote access malware (RAT) were stopped;
- the use of the LSM brand in advertising campaigns for fraudulent cryptocurrency investment platforms was stopped;
- fake online casino websites were blocked.

Overall, it can be concluded that the threats are becoming persistent rather than seasonal. Most of these threats target people as the primary attack target. Without the active protection provided by the CERT.LV DNS firewall, a significant proportion of users would reach phishing pages, malware download sites, and fraudulent platforms. The CERT.LV DNS firewall protects users from visiting identified fake websites by redirecting them to a secure warning page where they receive an explanation of the threat that was prevented.

3.2. Cybersecurity Early Warning System (EWS)

The Cybersecurity Early Warning System (EWS) is a service provided by CERT.LV for analysing data traffic anomalies and identifying signs of cyber attacks in the service recipient's infrastructure. CERT.LV continues to maintain and expand the EWS system.

The EWS service includes the continuous analysis of data traffic anomalies and detection of malware activity, notifications to the service recipient about identified high-priority cyber threats, regular updates of CERT.LV's current cyber threat indicators, and consultation and support for service recipients.

Detection and prevention of cyber threats and incidents

In Q2 2026, the number of alerts recorded by the EWS was approximately **982** million, **13%** more than in Q1. Moreover, an increase has been observed since the beginning of 2026. This indicates increasing cyber threat intensity and the emergence of new vulnerabilities – after publicly known vulnerabilities are disclosed, attackers often begin scanning systems and attempting to exploit them on a large scale. CERT.LV notes that potentially, any insecurely managed device exposed to the internet is at risk of attack.

The most significant threats during the reporting period:

- network requests to domains distributing malware, including ClickFix;
- network requests to domains associated with identified phishing and fraud campaigns;
- requests to domains distributing fake software by imitating the names of trusted tools.

Public involvement is also important: residents forward fraudulent emails, text messages, and website links to cert@cert.lv, or report them by calling 23230444 (WhatsApp). The reports received are compiled and malicious domain names are added to the DNS firewall to protect Latvian internet users. dnsmuris.lv and its mobile app are available free of charge to every resident and organisation in Latvia.

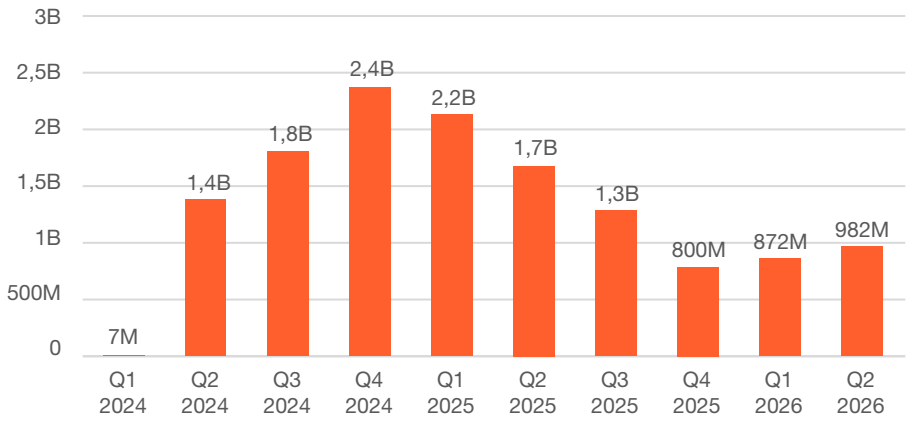

Figure 7. Quarterly dynamics of alerts recorded by the EWS (number in millions – billions; 2024-2026)

3.3. Security Operations Centre (SOC)

Implementation of the SOC service

CERT.LV continues to develop SOC services and attract new clients, expanding the client base in line with the NCL and strengthening effective protection and resilience against cyber threats.

The SOC centrally collects security telemetry from client infrastructure, correlates events, and links them with the complete set of threat indicators and knowledge available to CERT.LV. Significant added value is provided by the SOC analyst team,

which uses specialised software and available data to prevent harm in a timely manner by identifying, issuing warnings about, and stopping threats or cyber incidents.

By the end of the reporting period, the total number of SOC clients had reached **105** (an increase of **13** in Q2). Institutions and organisations from various sectors that provide essential and important services use CERT.LV SOC solutions. Compared with other sectors, ministries, and their subordinate institutions, local governments and healthcare institutions are the most highly represented.

Visibility was provided across a total of **57 021 endpoints**, including servers and workstations. The increase in Q2 2026 accounted for 32% of the total. As the scope of monitoring expands, the number of security events to be analysed and alerts generated also increases.

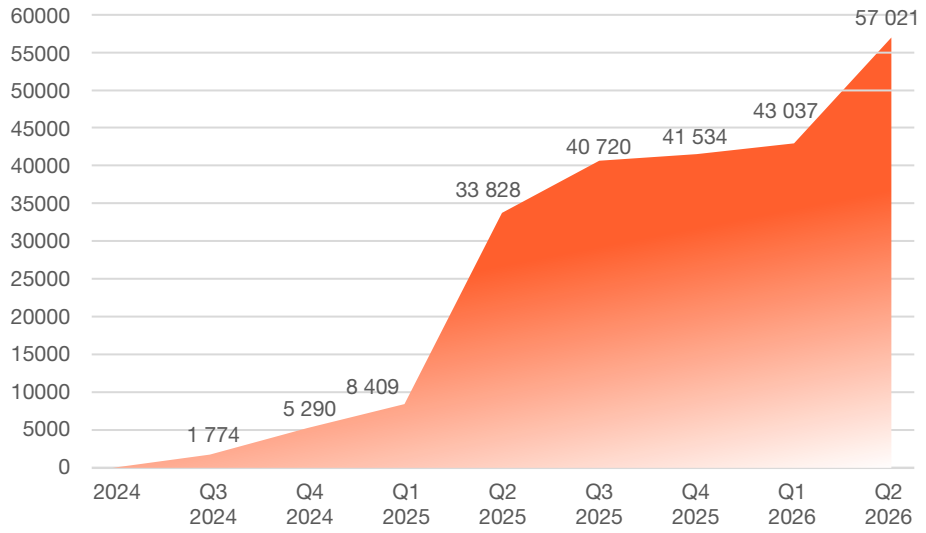

Figure 9. CERT.LV SOC visibility dynamics: number of endpoints (2024-2026)

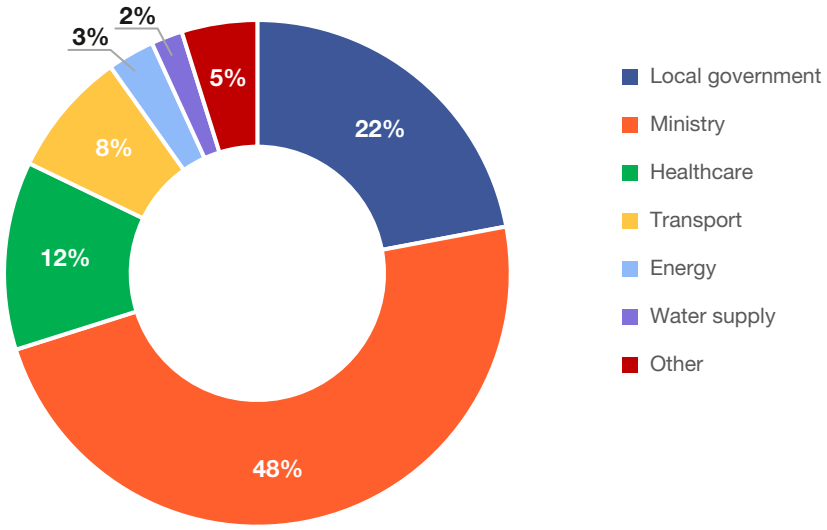

Figure 8. Distribution by institutional sector using CERT.LV SOC (%, data as at 30.06.2026)

Incidents and security alerts: threat detection and prevention

Indicators	Quantity	Change (%) compared with Q1 2026
Total number of security alerts registered within the CERT.LV SOC service in Q2 2026:	**~25 milj.**	**+4%**
Number of low-level alerts	**~6 milj.**	**+0,72%**
Number of medium-level alerts	**~18 milj.**	**-1,48%**
Number of high-level alerts	**~16 tūkst.**	**+47%**
Number of critical alerts	**~35 tūkst.**	**+116%**
Number of manually created cases	**617**	**+5,3%**
Number of false positive cases	**599**	**+5%**
Number of cyber incidents	**19**	**+27%**

During the reporting period, **approximately 25 million security alerts were registered, 4% more** than in Q1 2026. The increase in the number of security alerts primarily reflects the expansion in the number of endpoints monitored by the SOC and an improved ability to identify potential threats. At the same time, it indicates increasing attack activity in cyberspace.

High-level alerts increased by 47%, while critical alerts increased by 116%. This indicates a significant increase in the proportion of the most serious incidents. Although the number of critical alerts more than doubled, the number of cyber incidents increased by 27%, indicating that the SOC is able to effectively identify and contain threats before they escalate.

A large number of false alerts were also observed within the SOC service (an increase of 5%).

The most common causes of false alerts observed in client infrastructure:

- incomplete or outdated records of ICT resources (a lack of centralised management at the institutional or municipal level);
- endpoint configurations are not standardised;
- a list of authorised software with an enforcement mode has not been implemented;
- web browser plugins and extensions are not managed and controlled;
- the unjustified use of multiple remote access tools (such as AnyDesk and TeamViewer, including outdated versions) for user support;
- logging is not enabled, and documentation and procedures are lacking;
- the use of USB flash drives and the execution of files from them are not monitored.

False alerts result in a larger volume of low-value work for SOC analysts when reviewing events, creating a risk that a genuine attack may be missed among the false positives.

To detect incidents and threats effectively, background noise from alert notifications must be reduced.

The most common situation in a compromised environment:

- **the principle of least privilege has not been implemented**, allowing an attacker to rapidly expand access rights and move through the infrastructure;
- **network segmentation is lacking**, meaning that a compromise in one part of the network often allows unhindered lateral movement to other systems;
- **software execution restrictions have not been implemented**, allowing malicious code and unauthorised applications to be executed without significant obstacles;
- **unified IT environment management and centralised security telemetry are not** provided, making timely threat detection, correlation, and effective incident response more difficult;
- **remote administration tools are used without control, with various** administration solutions operated without centralised management, monitoring or security policies, significantly expanding the attack surface and making unauthorised access more difficult to identify.

Cases created and cyber incidents recorded within the SOC service

In Q2 2026, **617 cases were created manually** (5.3% more than in Q1 2026), while **599 cases were false positives** (5% more than in Q1 2026).

Within the SOC, **19 cyber incidents were recorded** (27% more than in Q1 2026) **across 16 different institutions**.

Within the CERT.LV SOC service in Q2 2026:

617 (+5.3%) – Manually created cases

599 (+5%) – False positive cases

19 (+27%) – Incidents recorded across 16 institutions

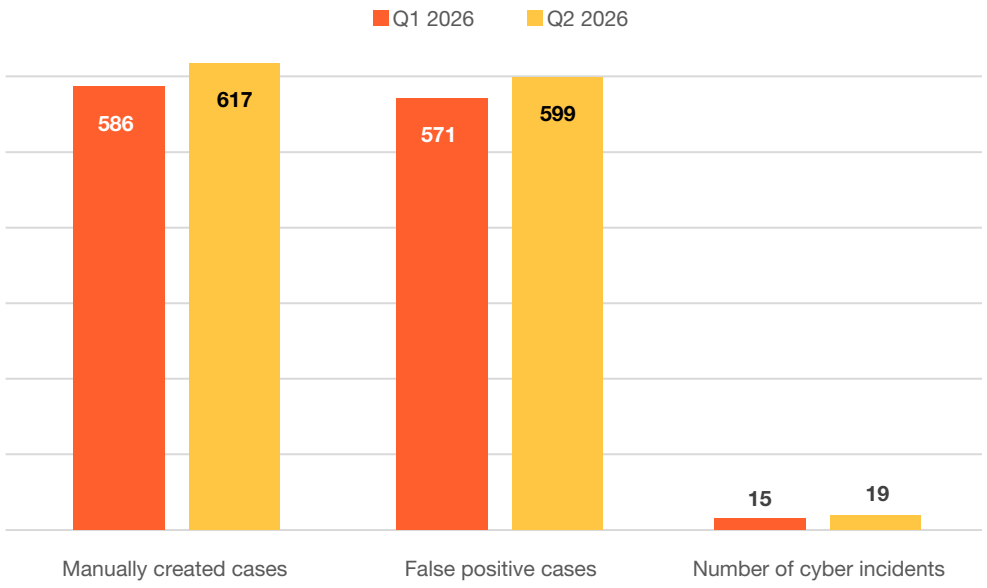

Figure 10. SOC: Structure and comparison of security events

Overview of cyber incidents recorded during the reporting period

The most extensive cyber incident involved a compromised website visited by users from three institutions, putting endpoints at risk or infecting them with malware. The **vulnerability on the compromised website** was remediated, and the infection was removed from the affected endpoints.

The largest number of alerts within the SOC service is caused by **uncontrolled unwanted software** – executable files downloaded from the internet and run by users; for example, games are often downloaded together with malware. Unwanted software that affected endpoints was identified on several occasions, and the alerts were registered as cyber incidents.

During the reporting period, several cyber incidents were recorded in which initial access occurred through **phishing emails, infected email attachments, browser plugins or fake CAPTCHA prompts; all of these**, as in previous periods, continue to pose a threat.

A cyber incident was identified on a website server. It **was compromised by exploiting a vulnerable content management system component**.

Endpoints continue to be inadvertently exposed to the internet without local protection (a local firewall), and brute-force password attacks against these endpoints remain ongoing.

Recorded incidents were mainly related to user actions and weak security practices, with the most significant risks being the human factor and insufficient access control. This indicates the need to prioritise user training, access control, and endpoint security as key protection areas.

Dominant initial access vectors:

- **phishing and malicious email attachments;**
- **browser plugins;**
- **fake CAPTCHA;**
- **unwanted software – executable files downloaded from the internet and run by users;**
- **a vulnerable website content management system;**
- **flash drives and executable files run from**

3.4. IT system security tests and phishing attack simulation campaigns

Phishing attack simulation campaigns

In Q2 2026, **3 phishing attack simulation campaigns** were conducted across three institutions. A total of **829 emails** were sent as part of these campaigns. More than half of users, or **67% of users, opened the link in the email**, and **24% of those users entered their credentials**.

The purpose of phishing attack simulation campaigns is to train and enhance the ability of organisations' employees to identify potentially risky behaviour patterns, as well as recognise and prevent cyber threats and information leakage. This helps significantly strengthen organisations' protection against social engineering attacks, thereby reducing risks related to the human factor.

IT system security tests

The purpose of security testing is to identify potential vulnerabilities, security threats, and system deficiencies in order to prevent possible cyber attacks and data leaks.

During the reporting period, CERT.LV conducted **18 IT system security tests** (8 more than in Q1). The tests **identified 31** vulnerabilities, including critical and high-impact vulnerabilities, which were remediated before they could potentially be exploited in cyber attacks.

When conducting an IT system security test, CERT.LV provides network security analysis, software vulnerability assessment, web application security assessment, IT infrastructure vulnerability assessment, as well as consultations and recommendations for improving security.

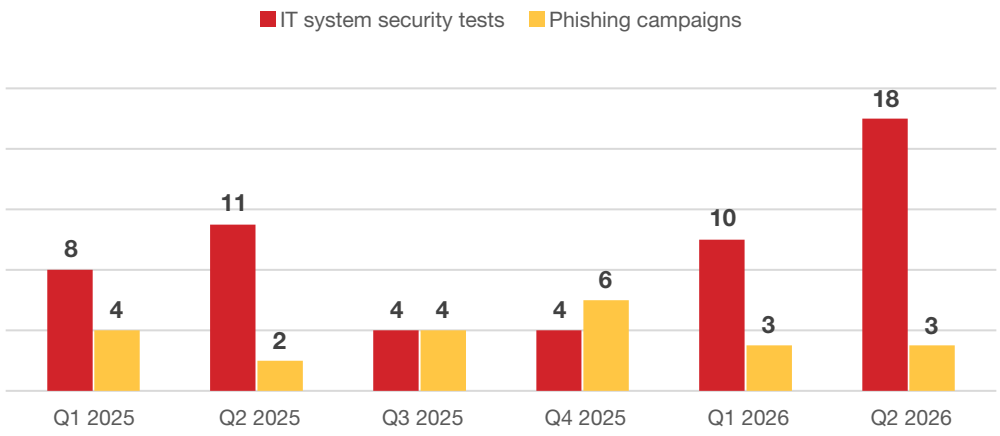

Figure 11. IT system security tests and phishing attack simulation campaigns (number)

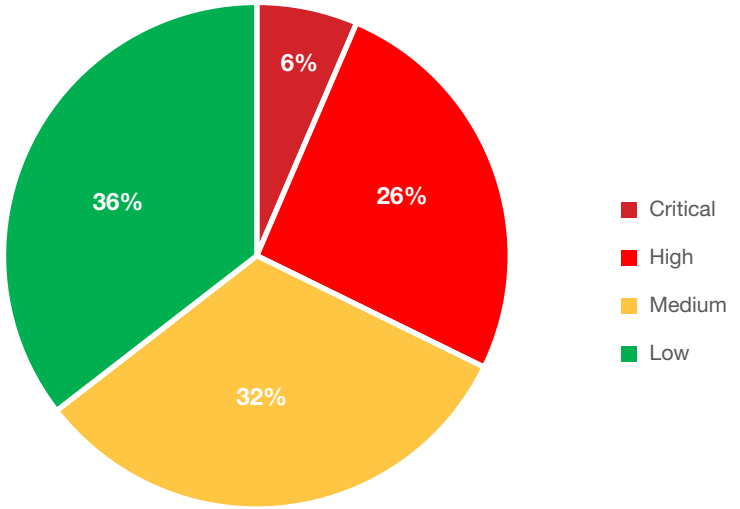

Figure 12. Q2 Potential impact of vulnerabilities identified in IT system tests (% of the total – 31)

3.5. Cybersecurity threat hunting operations

Cybersecurity threat hunting is a proactive process in which CERT.LV cybersecurity experts search Latvian ICT systems for signs of potential threats or unauthorised activity in order to identify risks and mitigate potential threats in a timely manner. Since CERT.LV launched cybersecurity threat hunting in 2022, threat analysis has been conducted in the infrastructure of more than 40 NCL subjects and ICT critical infrastructure organisations.

During the reporting period, analysis of endpoints identified several security deficiencies, including insecure software and device configurations and the use of outdated components exposed to security vulnerabilities, increasing the risk of potential cyber incidents.

The eighth Threat Hunting Operation with an expanded presence demonstrates operational maturity

In May 2026, CERT.LV completed its eighth three-week Threat Hunting Operation with an expanded presence, in cooperation with the Canadian Armed Forces Cyber Command and allies from Ireland, Norway, Poland, and the United Kingdom. 30 technical experts participated in the operation, strengthening the security of the digital infrastructure of Latvian state and public institutions.

The operation demonstrated the growing maturity of Latvia's threat hunting approach and reinforced it as an internationally recognised cooperation model combining civil and military capabilities. Its primary significance lies in the timely identification of signs of threats, the strengthening of cyber resilience, and the consolidation of Latvia's role in developing a practical threat hunting methodology. The main conclusion is that continued investment is required in threat hunting capacity, institutions' technical preparedness, a shared methodology, and cooperation with allies.

"This operation gave international partners an opportunity to learn about our threat hunting methodology and apply it to their own needs where appropriate. At the same time, it strengthened international cooperation by promoting coordinated action, the exchange of experience, and mutual support in the face of cyber threats," said CERT.LV Deputy Head Varis Teivāns.

3.6. Coordinated Vulnerability Disclosure Platform (CVD)

The CERT.LV Coordinated Vulnerability Disclosure (CVD) Platform is intended to facilitate cooperation between state and municipal institutions and cybersecurity researchers, and to improve the security of ICT resources.

Using the CVD platform, an institution can register information on all ICT resources it uses for which it wishes to receive reports on identified vulnerabilities. The platform provides a transparent and user-friendly interface where all received reports can be viewed, and communication with researchers and other involved parties can be maintained. Responsible disclosure helps to remediate vulnerabilities before they are exploited, reducing risks for both organisations and users.

By the end of Q2 2026, the CVD platform had registered a total of:

- **185 security researchers** (an increase of 19 in Q2);
- **18 active institutional programmes** (4 new programmes);
- **683 vulnerability reports** (an increase of 142 in Q2), including:
  - ✓ **492** CERT.LV client vulnerability reports (an increase of 137 in Q2);
  - ✓ **191** vulnerabilities reported under specific institutional programmes (an increase of 5 in Q2).

View active institutional programmes on the CVD platform: **cvd.cert.lv**

To test the vulnerabilities of resources exposed to external networks, CERT.LV invites organisations to create and manage their own programme on the cvd.cert.lv platform. Security researchers are also invited to use the CVD platform to report vulnerabilities discovered in the resources of public authorities and Latvia-registered companies securely and in a coordinated manner, facilitating faster remediation.

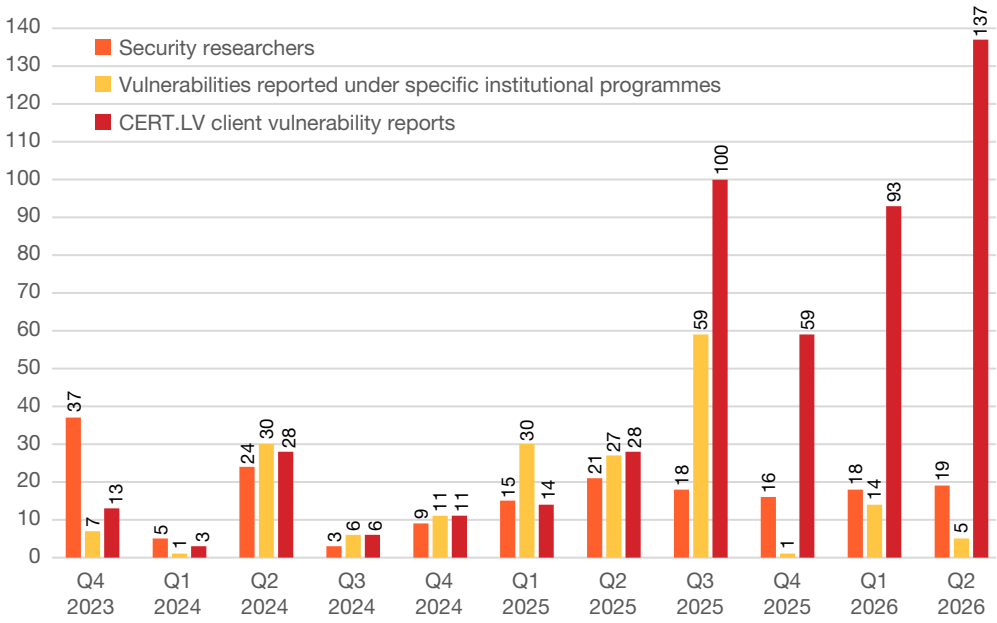

Figure 13. CVD: Number of security researchers and vulnerability reports

3.7. Operational Technology (OT) Security

Activities

CERT.LV has established cooperation with operators in Latvia's energy, water supply, district heating, and transport sectors, and has concluded operational technology (OT) security service agreements. OT system security is strengthened in three main areas: **system monitoring and anomaly identification; security testing; and incident response.**

- **As part of system monitoring**, CERT.LV has installed five OT network traffic monitoring sensors, and active preparations are under way to expand the sensor network. Alongside the monitoring of communications within internal OT networks, Latvian IP address ranges are monitored continuously to identify publicly exposed systems, determine their potential vulnerabilities, and coordinate access restrictions and remediation.
- **As part of security testing for OT system components**, various smart and industrial control devices are tested to identify potential vulnerabilities or supply chain weaknesses that could enable manufacturers or external attackers to gain unauthorised control of these devices and the systems as a whole. Initial checks are carried out on equipment originating from China. Over the past year, such equipment has included remotely controllable smart devices (e.g., smart meters and mobile communication modems) and electric vehicle charging stations.
- **Broader cooperation has been established** with Nordic and Baltic (NB8) cybersecurity authorities.

Threats, incidents, impact

Early identification of potential risks and vulnerabilities, proactive action, and the mitigation of their impact are carried out. **The overall resilience of Latvia's operational technology and related systems against cyber attacks is assessed as satisfactory, with the steady improvement trend continuing.** As a result of regular activities, private or small-scale OT systems accessible from the internet are identified, and operators are informed and engaged in cooperation to reduce or eliminate the potential impact.

A continuous threat from states unfriendly to Latvia is expected, aiming to gain control and carry out destructive actions in critical infrastructure operator systems. To mitigate such risks and make Latvia a more difficult target, CERT.LV will continue work on OT activity areas, ensuring broader visibility and threat identification, the execution of security tests, and coordinated incident response.

4. Strengthening cybersecurity through society-wide measures

Continuing to improve the cybersecurity knowledge and skills of individual users and organisations, CERT.LV experts reached a total audience of **8632 people** through **95 events** in Q2 2026. This represents 34% more events and 19% more participants than in the corresponding period last year.

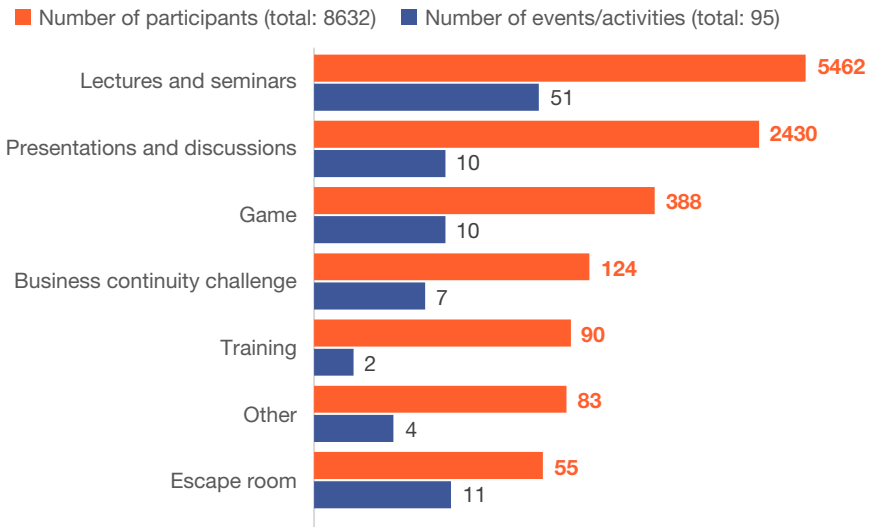

Figure 14. Type of educational method vs audience reached (number; Q2 2026)

CERT.LV offers the opportunity to improve your cybersecurity knowledge at any time using Kibertests.lv. It is a free platform where, in just a few minutes, you can test your knowledge of the most common cybersecurity risks and receive practical recommendations on how to stay safer in your daily life.

Kibertests.lv is suitable for both individuals and organizations. Individuals can take the tests anonymously and receive immediate results, while companies can assess their employees' knowledge levels and obtain aggregated results to help plan targeted cybersecurity training.

For more information about the lectures, training games, and educational events offered by CERT.LV, see the Services section of the cert.lv website.

5. International cooperation

European cybersecurity experts analyse the latest cyber threats and share experience at the TF-CSIRT meeting in Riga

From 11 to 13 May 2026, Riga hosted the 77th annual TF-CSIRT meeting – a forum at which more than 150 experts from European cyber incident response teams analysed the latest cyber incidents, attacker tactics, and response practices. Participants discussed critical infrastructure protection, vulnerability management, the opportunities and risks of artificial intelligence, and crisis communication in cyberspace. CERT.LV presented Latvia's experience in industrial technology security, preventing commercial attacks and cooperation among Security Operations Centre (SOC) experts.

The event strengthened Latvia's involvement in the European cybersecurity cooperation network and drew international attention to the challenges currently affecting Latvia and the region.

"The TF-CSIRT meeting in Riga was an important opportunity not only to strengthen international cooperation in cybersecurity, but also to demonstrate the competence and experience of Latvian experts to the European community. Such meetings are particularly important at a time when cybersecurity incidents are becoming increasingly complex and closer cooperation between organisations and countries is critically important," said CERT.LV Head Baiba Kaškina.

CERT.LV has been a member of TF-CSIRT since 2007 and, since 2016, one of the TF-CSIRT/Trusted Introducer certified teams in Europe. The TF-CSIRT meeting and forum were organised with EU financial support under the CERT.LV-SOC-LV project. The meeting was organised by TF-CSIRT in cooperation with CERT.LV, the Ministry of Defence, the National Cybersecurity Centre, the ISACA Latvia Chapter, the Institute of Mathematics and Computer Science of the University of Latvia, and Censys. The meeting is co-funded by the European Union (as part of the CERT.LV-SOC-LV project; https://cert.lv/en/about-us/international-projects; project ID: 101249230)

In picture: CERT.LV representative and TF-CSIRT Steering Committee member Dana Ludviga and CERT.LV Head Baiba Kaškina

"CERT.LV is actively involved in coordinating the TF-CSIRT community's strategic initiatives, while also highlighting the cybersecurity challenges most relevant to our region. This makes it possible to draw European experts' attention to current threats in Latvia and, through international cooperation, to strengthen the security of Latvia's cyberspace," said CERT.LV representative and TF-CSIRT Steering Committee member Dana Ludviga.

Latvia-Singapore joint team wins 1st place in the Locked Shields 2026 cyber defence exercise

In April 2026, the joint Latvian-Singaporean team won 1st place in the international cyber defence exercise Locked Shields 2026, which involved approximately 4000 participants from 41 countries. The joint Latvian-Singaporean team comprised approximately 230 participants, around 140 of whom represented Latvia.

CERT.LV experts participated in the exercise as part of the joint Latvian-Singaporean team, performing tasks in the technical, media, strategic communication, and legal teams.

The result demonstrates the high level of preparedness of Latvia's cybersecurity experts, and their ability to operate within an international team and respond effectively to complex cyber incident scenarios in practice.

Participation strengthened CERT.LV's experience in testing procedures, technical cooperation, incident management, and the international exchange of experience. The achievement reinforces Latvia's reputation as a strong cybersecurity partner and demonstrates the effectiveness of the cooperation model between the state, the military sector, and technology companies.

The Locked Shields 2026 exercise is organised by the Tallinn-based NATO Cooperative Cyber Defence Centre of Excellence (NATO CCDCOE) in cooperation with Alliance member states, partner countries, and technology companies.

Photo: NATO CCDCOE

Transport sector improves crisis management in the Cyber Europe 2026 cybersecurity exercise

On 10-11 June 2026, the European Union Agency for Cybersecurity (ENISA) held the Europe-wide Cyber Europe 2026 cybersecurity exercise, in which Latvian transport sector and public administration institutions participated in a coordinated crisis management and incident response simulation. The purpose of the exercise was to test and improve the ability to identify, analyse, and manage cybersecurity incidents, and to strengthen cooperation at the national and international levels.

The exercise focused on transport sector resilience, incident management, information flows, and coordinated action in situations that may affect service continuity.

6. Overview of the activities of the LIA Safer Internet Centre Report Line

From 01.04.2026 to 30.06.2026, the Latvian Internet Association Safer Internet Centre Reporting Line (RL) received and assessed 457 reports. Of these, 286 reports concerned child sexual abuse material; 36 cases involved pornography displayed without an age restriction warning; 16 reports concerned defamation; 3 reports concerned hate speech; and 4 reports concerned violent material. The Reporting Line received 43 reports of attempted financial fraud online; the content of 49 reports was not illegal; and in 20 cases, reporters were advised on how to resolve the issue.

82 reports concerning child sexual abuse material hosted on servers in Latvia were forwarded to the State Police. A total of 206 reports concerning child sexual abuse material located outside Latvia were entered into the INHOPE Association database and submitted to the reporting line in the relevant INHOPE country for further action to remove the illegal content from public access.

During the reporting period, of the 82 reports concerning child sexual abuse material hosted in Latvia, the content of 80 reports was removed from public access online, while 2 reports remained in the removal process.

Overview of reports received from 01.04.2026 to 30.06.2026

Reports	Apr-26	Mai-26	Jun-26	Q2
Erotic/pornographic content without displayed warnings	17	7	12	36
Paedophilia / prostitution of minors / child sexual abuse material	29	172	85	286
Violent content	2	1	1	4
Defamation / insult	10	4	2	16
Incitement to hatred / racism	2	1	0	3
Financial fraud	15	13	15	43
Consultations / advice	7	6	7	20
Other	13	22	14	49
TOTAL:	95	226	136	457

Reports sent to the State Police	1	70	11	82
Reports sent to the INHOPE association	22	99	85	206
TOTAL SENT FOR REVIEW:	23	169	96	288

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-mail: cert@cert.lv

Website: www.cert.lv

Follow CERT.LV news on:

@cert.lv