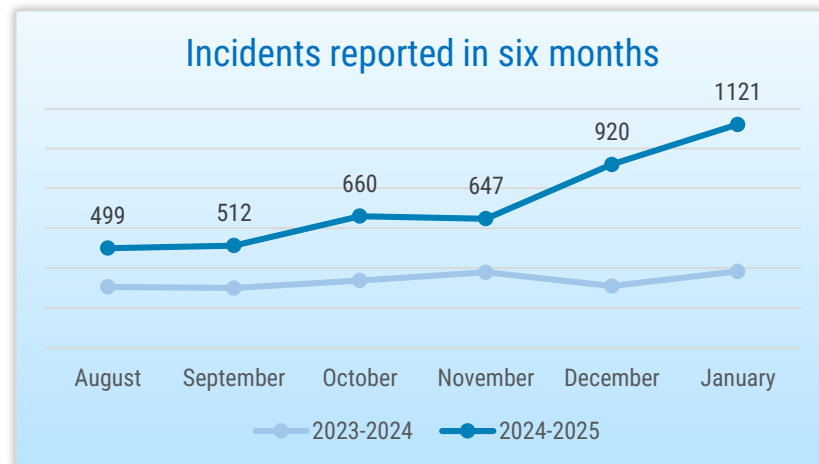




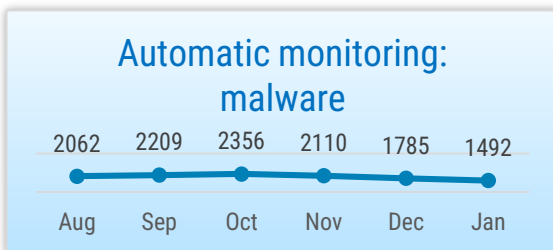
SITUATION IN CYBERSPACE

JANUARY 2025

- In January, **we recorded 1,121 incidents with an impact**, which is the highest indicator in the last six months.
- The devices of two public agencies were compromised through an **Ivanti vulnerability**. In January, emails and messages were circulating, purporting to be sent on behalf of the Tax and Customs Board.
- We published the **Cyber Security Yearbook**. In the RIA blog, we wrote about several widely used **software with support ending this year**. New episodes of the **series IT-vaatlik (IT-conscious)** were broadcast on ETV.
- A border control system at **German airports** has been hit by a major IT outage. The Italian Data Protection Authority has blocked the use of the **Chinese-made DeepSeek** artificial intelligence application in Italy.



Incidents reported to CERT-EE that had an impact on the confidentiality, integrity, or availability of data or information systems.



Devices in Estonian cyberspace infected with malware detected by automatic monitoring. CERT-EE notifies network owners of infections.



Phishing sites still account for the largest proportion of incidents recorded by CERT-EE.



Situation in Estonian cyberspace

In January, a number of essential services were once again disrupted.

On 2 January, between 1.30 p.m. and 3.58 p.m., an interruption occurred in the automatic border control system, the ABC gates, at the Narva and Saatsje border crossing points and at Tallinn Airport. The interruption was caused by the expiration of a certificate. On 8 January, between 11.18 a.m. and 1.15 p.m., messages in the SIRENE (Supplementary Information Request at the National Entry) system, used by the Police and Border Guard Board for information exchange, could not be modified or saved due to a configuration error.

On the evening of 3 January and the morning of 4 January, a denial-of-service attack hit a commercial bank operating in Estonia. There were short disruptions in the operation of its internet bank due to the attack.

In the beginning of January, it was discovered that the VPN devices of two

public agencies using the Ivanti Connect Secure software had been compromised. The attack exploited a critical vulnerability disclosed on 8 January, known as CVE-2025-0282, which allows to launch a malicious code in the system of the victim. One of the signs of a device being compromised is the interruption of the transmission of system logs. Unfortunately, vulnerabilities in Ivanti have been used for gaining access to the devices of Estonian state authorities in the past as well. At this point, it is worth reminding the reader that unpatched vulnerabilities are one of the main vectors for a successful attack.

This month saw the continuation of denial-of-service attacks against the name servers of various institutions.

The name servers of CERT-EE, the Information System Authority, EENet.ee, and the Ministry of Foreign Affairs were targeted.

As a result of defensive measures, the attacks had no effect.

In January, emails and messages seemingly sent by the Tax and Customs Board were circulating, claiming that people were entitled to an annual tax refund.

This incident was special because the recipients were directed to open the link via a QR code. As QR code scanners often open the link automatically and do not show the user a preview of the domain, the user may not realise that it is a suspicious link. A [guide](#) (in Estonian) prepared by the Tax and Customs Board on how to spot scam emails and messages is also available. As far as we know, the scam was not successful and people realised that the email was suspicious. Unfortunately, the same cannot be said about the ongoing campaign of phishing emails sent posing as LHV Pank, asking for an urgent update of customer details. We can see that people are still falling victim to the phishing emails sent posing as LHV.



Activities of the Estonian Information System Authority

We published our Cyber Security Yearbook, where we discuss all the important events that happened in cyberspace last year. For example, the yearbook explains that there were 6,515 cyber incidents with an impact in Estonia last year – around twice as many as in 2023. Almost two thirds of them were various types of phishing attempts, but the number of cases of fraud, for example, also increased. In addition to what is happening in Estonia, we also took a look at what is happening around the world, including Chinese ambitions in cyberspace.

In 2025, vendor support, including security upgrades, will end for a number of key software products. The end of official support for Microsoft Windows 10 Enterprise, Education, Home, and Pro on 14 October 2025 will have the biggest impact on individuals, businesses, and institutions. We wrote in the RIA [blog](#) (in Estonian) about a number of widely used programs that will end support this year.

We also blog regularly each week about the most important security vulnerabilities. Vulnerabilities in software are a favourite target for attackers for gaining primary access to the systems of an organisation. We encourage you to read our [blog posts](#) on vulnerabilities every week.

In both December and January, ETV aired new episodes of the TV series IT-vaatlik. In the episodes, we discussed topics such as keeping children safe online, account hijacking, the safe use of social media and smartphones, falling victim to scams, and cyber incidents and scams common in Estonia. All episodes can be viewed on the website of the [ERR Archives](#).

Another CyberMeetUp took place on 16 January. You can watch it [here](#). This time, presentations were given by Jürgen Erm (NEVERHACK Estonia), Raimundas Matulevičius (University of Tartu), Rain Ottis (TalTech),

Triin Toimetaja (PwC), and Johannes Kadak (ECSC Estonia). The first CyberMeetUp of the year set a new attendance record with 70 people attending and many listening online. The next event will take place on 13 February.

We published an article on investment fraud in the IT-vaatlik prevention portal. As the number of different types of investment scams has recently increased significantly in Estonia, it is important to recognise and be aware of them. According to the Police and Border Guard Board, Estonians lost more than 4.8 million euros in investment scams alone in 2024. Investment fraud offers the victim a seemingly excellent investment opportunity, promising a low-risk or risk-free investment and a guaranteed return. Check out the typical signs of a scam and a specific example in the IT-vaatlik [portal](#).



International situation

On 3 January, an extensive disruption hit the IT systems of the border control at German airports, causing long queues in non-Schengen border crossings. At several major airports, border queues were at least two hours long and some passengers were kept on board of planes for extended periods to avoid overcrowding the airports. The reason for the IT outage is unknown.

The UK domain registry Nominet reported a cyber incident discovered in early January, in which attackers exploited a zero-day vulnerability in the Ivanti VPN software. This security flaw has been exploited since mid-December and the attacks are generally attributed to threat actors linked to the Chinese government. Nominet manages over 11 million .uk domain names, and until last September, it ran the Protective Domain Name Service (PDNS) for the National Cyber Security Centre of the UK.

A volunteer hacker group called the Ukrainian Cyber Alliance hacked into the network of Nodex, a Russian telecom, stealing data and destroying systems. Nodex confirmed in a social media post on the same day that it had been the victim of a devastating cyber attack and was trying to restore its systems from backups. NetBlocks, an organisation that monitors network data, detected that the services for landline and mobile phones were both disrupted in the Nodex network. Roskomnadzor, a Russian telecom watchdog, also confirmed widespread outages in communication systems, mainly in the Moscow region, but did not name a specific network operator or the cause of the outages.

In the second half of January, a law came into force in the US, banning the use of the TikTok app for all users until it is separated from ByteDance, a Chinese company. TikTok stopped working and could not be downloaded from app stores. The ban lasted only

about 14 hours, however, because President Trump wrote on his social media platform the very next morning that he was going to suspend the law and give TikTok a 90-day extension to find a local buyer so that 170 million Americans could continue using the popular app.

The Italian data protection authority Garante blocked the use of the Chinese-made DeepSeek artificial intelligence application in Italy. Garante justifies the decision by saying that it did not receive adequate answers from the company as to what kind of personal data is collected from Italian users through the app and under which regulation, and whether this data is stored in China. DeepSeek-related companies Hangzhou DeepSeek AI and Beijing DeepSeek AI are said to have responded to the inquiry that they do not operate in Italy and are therefore not subject to EU law.