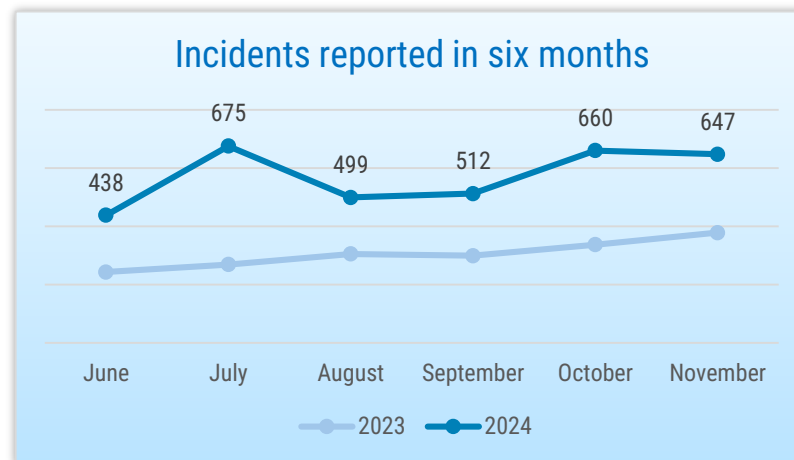




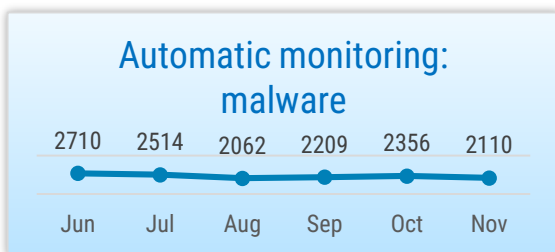
SITUATION IN CYBERSPACE

NOVEMBER 2024

- In November, **we recorded 647 incidents with an impact**, which is a higher indicator than the average of the last six months.
- In November, **a dental clinic was hit by a ransomware attack** and **four businesses fell victim to invoice fraud**.
- We organised a **cyber security urban camp** for the Home Daughters and started a series of **E-ITS workshops**. In the RIA blog, we wrote about using AI applications in writing attack codes and shopping securely in online shops.
- **A cyber attack** was carried out against the information systems of **courts in Washington**, as well as **South Korean government** and private sector websites.



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 November, we again recorded a number of incidents affecting essential services. On 1 November, a dental clinic was hit by a ransomware attack used to encrypt the data on the server. The clinic did not have a working backup, meaning the data could not be restored. The CERT-EE team carried out an analysis and found that the attack originated via an open remote desktop (RDP) connection with a password that was too easy to guess. In light of the incident, we recommend reviewing both the remote desktop protocol access and password policies in your company to avoid a similar situation.

From 3–5 November, there were failures in the Pärnu Hospital information system used for data exchange (e.g. transmission of X-ray images). The failures were caused by a module; restarting it temporarily helped stabilise the system, but the error soon recurred. A fix had to be made to the software to resolve the incident.

On 17 November, the website of the Consumer and Technical Regulatory Authority ttja.ee was hit by a denial-of-service attack. As a side effect, there were outages for seven minutes on a total of eighteen state agency websites managed by the Information Technology Centre, including those of the Ministry of the Interior, the Ministry of Climate, the Tax and Customs Board, CERT-EE, and the Labour Inspectorate. CERT-EE and RIA name servers were actively attacked in both October and November, but these attacks generally had no impact.

On 22 November, between 10.16 and 10.56 a.m., the ID-card signing and authentication services failed due to a failure in the validity confirmation service provided by SK ID Solutions, which allows real-time queries on the status of certificates. The outage was caused by a configuration error made during maintenance.

In November, we recorded four

successful cases of invoices fraud. In total, Estonian companies lost nearly 300,000 euros in the four incidents. Invoice fraud means that an invoice (where only the bank account number has been changed) is sent to an institution company on behalf of its partner. By this time, the fraudsters will have been monitoring communications between the two parties for some time and will intervene at the appropriate moment by sending the invoice. Often, this does not raise concerns and the invoice is automatically paid. The fraud usually comes to light when the partner starts to enquire why they have not been paid yet. In the first case this month, the fraudsters had been monitoring the communications for some time. In the second, an invoice with the changed account number was simply sent to the general e-mail address of the company. Read the [RIA blog](#) for suggestions on what to do to avoid becoming a victim of invoice fraud.



Activities of the Estonian Information System Authority

In mid-November, the Harju, Rapla, and Tallinn Home Daughters gathered for a cyber security urban camp to acquaint themselves with the work of cyber security experts and ethical hacking and learn how to protect themselves from cyber threats. The camp started with cyber hygiene and gradually moved on to more technical issues. Among other things, the camp focused on secure passwords, file metadata and the capabilities of the testing tool FlipperZero, and network scanning. Participants also got to hack into the administrator's view of an unsecured website. This was the fourth urban camp organised in cooperation between RIA and the Home Daughters.

We wrote in the RIA [blog](#) about how hackers have started using artificial intelligence (AI) applications to write attack codes. This provides more and more opportunities for technically inferior hackers, who can now use clever queries to create malware suitable for attacks.

It has been discovered that the attacks on Estonian boiler plants and pumping stations in late 2023 were also carried out using codes generated by artificial intelligence.

With Black Friday and the festive season approaching, we shared some advice on how to shop safely and avoid falling victim to fraud in our [blog](#). When shopping, customers should pay attention to the content of the online shop and, if necessary, look into its background. They should also be careful when using payment systems and sharing their data. Check out our [blog](#) to read about invoice frauds and suggestions on how not to fall victim to a similar scheme.

New episodes of the series *IT-vaatlik* were broadcast on ETV in November. Topics covered included cyber criminals, fraud calls, data backup, and online shopping. All episodes can be viewed on the website of the [ERR Archives](#).

Another RIA CyberMeetUp took place on 14 November. Watch it [here](#). This year, the event took place in cooperation with the Estonian-Czech joint project [CHESS Cyber-Security Excellence Hub](#). The next CyberMeetUp will take place on 11 December.

On 21 November, the first session of a series of workshops for local governments, their administrations, and state educational institutions on the practical application of the Estonian Information Security Standard (E-ITS) took place. The first workshop was aimed at the heads of the institutions. The next three sessions will introduce the mapping of business processes and assets, the development of an implementation plan (including modelling of modules and measures), and the preparation of documents to be created. The series will involve 60 institutions, over 180 participants, and 15 speakers from RIA. For more information on RIA events, check out our [website](#).



International situation

At the beginning of November, a [cyberattack](#) was carried out against the information systems of courts in Washington, leaving them partially disrupted. Additionally, several websites and services were inaccessible. Hearings also had to be postponed in some court buildings. Information on who may have been behind the attack has not been made public but according to a spokesman for the courts, there is no reason to believe it was a targeted attack.

The FBI and CISA investigation [confirms](#) that in the course of the attacks carried out against several US telecoms companies that came to light in the autumn, hackers with a Chinese background managed to gain access to the devices of some US government officials and top politicians, steal data from them, and intercept conversations. The hackers are also said to have stolen information related to US law enforcement operations. According to a [joint statement](#) by CISA

and the FBI, this is part of a broad cyber intelligence campaign by Chinese state-sponsored hackers.

South Korea reported intense waves of denial-of-service attacks against government-related websites and the private sector in November. Behind the attacks are pro-Kremlin hacktivists and their actions are motivated by the decision of South Korea to monitor the involvement of North Korean units in the war in Ukraine. According to South Korean information, more than 10,000 North Korean fighters have been sent to Ukraine to fight for Russia, and they are also taking part in military operations in Kursk. According to the Office of the President of South Korea, Russian hacktivists have attacked South Korean websites in the past, but this has become much more intense with developments in Ukraine.

Hackers in France managed to compromise the MediBoard software account and steal the health data of

patients at least one hospital. Softway Medical Group, the company that provides MediBoard, acknowledged the compromise, but confirmed that it was not related to a software security vulnerability or a configuration error, but most likely to an abuse of account privileges. The incident came to light after hackers put up for sale the database of one hospital (nearly 760,000 patients) and claimed to have access to patient health data, treatment invoices, and booking systems of several other hospitals via the MediBoard platform.

At the end of the month, a cyber attack was carried out against a foundation that runs several hospitals in the UK, forcing the cancellation of scheduled admissions and procedures. Part of the IT systems were removed from the network and the hospitals switched to using paper and pens to manage the incident. Emergency services remained operational.