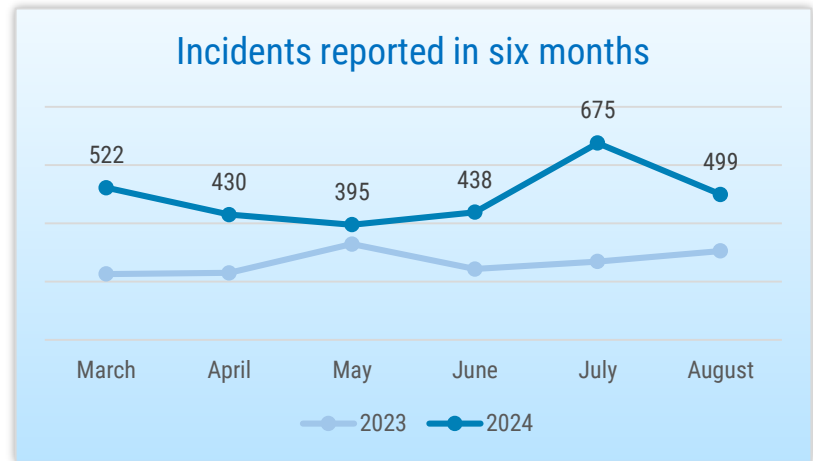




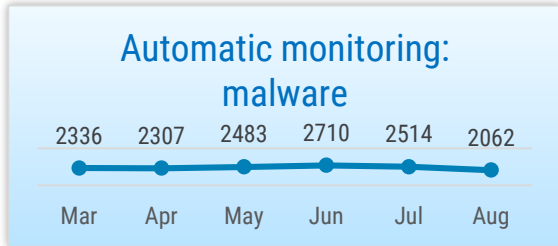
SITUATION IN CYBERSPACE

AUGUST 2024

- In August, we recorded **499 incidents with an impact**, which is slightly above the average for the last six months.
- In August, we recorded **two ransomware attacks** and saw a massive spread of phishing messages sent posing as Omniva.
- We organised an international cyber camp for girls, called **CyberWizards**. We were guests on **“Olukorrast digiriigis” podcast** to discuss the importance and current state of cybersecurity in Estonia.
- Trump’s campaign team announced that their **internal communication network was breached**. Ukrainian experts discovered a **malware campaign targeted at Ukrainian government agencies**.



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 August, we witnessed several service disruptions yet again. On 6 August between 5.25 p.m. and 6.15 p.m., there were interferences in the operation of Apollo, the online information system of the police, and PIKO, an information system of the border control. The border guards were unable to use the system because X-tee queries were not forwarded. The incident was caused by an interruption in the work of a hardware security module. On the same day, there were issues with sending messages in the online environment of the commercial register. During the incident, users of the commercial register were unable to submit applications for the first-time entries and changes to the register, where they needed to confirm their email addresses. The issue was caused by an error in an email software that was rectified by 8.02 p.m. on 6 August. On 24 August, from 3.59 a.m. until 10.30 a.m., websites managed by the Information

Technology Centre of the Ministry of Finance (RMIT) were experiencing disruptions. The malfunction, caused by a configuration error in a domain name server of the RMIT, affected 67 different websites.

On 15 August, CERT-EE was informed that the central management system of the end-user devices of the Transport Administration was compromised and an attacker had managed to gain access with administrative privileges. The Transport Administration, its partners, and CERT-EE conducted an analysis, which indicated that the attacker used a vulnerability in Fortinet software (CVE-2023-48788), disclosed in March.

In August, we also recorded two ransomware attacks. On 16 August, a ransomware attack against the Järva County Vocational Training Centre took place, as a result of which all of its servers were encrypted.

On 17 August, ransomware was used for encrypting data in a server of a South Estonian retail company. Because the attackers managed to gain access to the back-up server as well, the back-up copy was deleted. Due to the attack, the operation of the company came to a standstill.

This month also brought along a massive spread of phishing messages sent posing as Omniva. The content of the messages differed, but most of them stated that a parcel could not be delivered due to an incorrect address and asked the recipient to update their information. Some of the messages requested the payment of shipping costs or customs fees. A suspicious link was included in all messages, taking the user to a phishing page. We would like to remind everyone once again that postal companies do not send such messages or ask users to enter their data at unknown links.



Activities of the Estonian Information System Authority

Between 29 July and 3 August, we organised the CyberWizard international cyber camp for girls, which took place for the second time this year. The goal of the camp is to promote cybersecurity as an exciting career option among girls, because currently, only about a fifth of the workforce are female in this sector. 95 girls between the ages of 13 and 16 participated in the camp, half of whom were from Estonia and the rest from abroad – Latvia, Lithuania, the Czech Republic, Poland, Italy, Hungary, France, Ukraine, and Cyprus. In addition to the staff of RIA, cybersecurity experts from Clarified Security, Telia, SEB Pank, and the Police and Border Guard Board shared their experiences with the girls.

Märt Hiietamm, the Head of the Analysis and Prevention Department of the Information System Authority, and Irina Klementi, the Acting Head of the National Cybersecurity Department and the Head of Cyber Risk

Management of the Ministry of Economic Affairs and Communications, were invited to the podcast *Olukorrast digiriigis to discuss the importance and current state of cybersecurity in Estonia*. Due to changes in security situation, the new national cybersecurity strategy that was approved in June focuses primarily on improving the resilience of our digital state. Both guests of the podcast considered the attitude among the public the biggest issue in this domain. The Cybersecurity Strategy 2024–2030 is available [here](#).

We published educational videos created during a study on AI and the security of machine learning technology, available [here](#). The study and the videos are useful for all Estonian organisations and companies that are planning to adopt AI.

In July, we concluded the development of the e-state app, and in the autumn, we are going to start

testing the application publicly. The e-state app is a presentation layer for mobile devices, complementing the Eesti.ee state portal and allowing to find all essential government services in the same environment. In autumn, all who are interested can test the Eesti.ee mobile application. A tester is able to use services provided through the mobile app and share feedback about the user-friendliness of the services.

On 27 and 29 August, information days for the heads of educational establishments took place. During the event, we talked about data protection, requirements for information security, and monitoring compliance. The Cybersecurity Act that took effect in 2022 established information security requirements for educational institutions, meaning that various establishments must create a system for the management of information security to protect their services, assets, and data



International situation

According to the [campaign team of Donald Trump, a presidential candidate in the US, their internal communication network was breached](#). A representative of the team blamed Iran for the cyberattack, but no concrete proof has been presented so far. Nevertheless, the representative of the campaign team referred to a recent Microsoft [analysis](#) describing several operations for meddling in the elections, which are linked to various Iranian cyber groups. According to the analysis, Iran used a hacked email account to send messages to a high-level official working for the campaign in June. Politico, a US publication, confirmed that they received documents related to the Trump campaign from an anonymous email account.

[In June, Ukrainian experts discovered a malware campaign targeting](#) Ukrainian government agencies and attempting to infect them

with a backdoor-type malware. As far as is known, over a hundred devices were infected. Victims received an email sent posing as the Security Service of Ukraine (SBU), demanding that the user forward certain documents, and containing a link to an archive with a .zip extension. When clicking on the link, malware was initiated in the computer, allowing to take control of the device remotely.

[National Public Data, a data brokerage company operating in Florida in the US and providing services for background checks, admitted](#) to a large data leak as a result of a cyber attack that took place months ago. According to the media, the leak might potentially affect nearly all Americans – allegedly, the leaked database contained 2.9 billion lines of data, including names, social security numbers, addresses, and email addresses. Although the criminals initially attempted to sell the data, they later published the database for free.

[Halliburton, one of the largest oil processors in the world, fell victim to a cyber attack](#), disrupting the operations of the company. The exact circumstances and impact of the attack are currently unknown, but some experts have hinted at a possible ransomware attack. Large oil companies have been victims of high-impact cyber attacks in the past as well: in 2021, Colonial Pipeline was hit by a ransomware attack, leading to fuel shortages in parts of the US.

[Microchip Technology, a semiconductor manufacturer from the US, announced that production processes were disrupted in several of its factories due to a cyber attack](#). Suspicious network traffic was discovered on 17 August, after which some of the systems had to be isolated from the network, leading to interruptions in the operation of some of its factories.