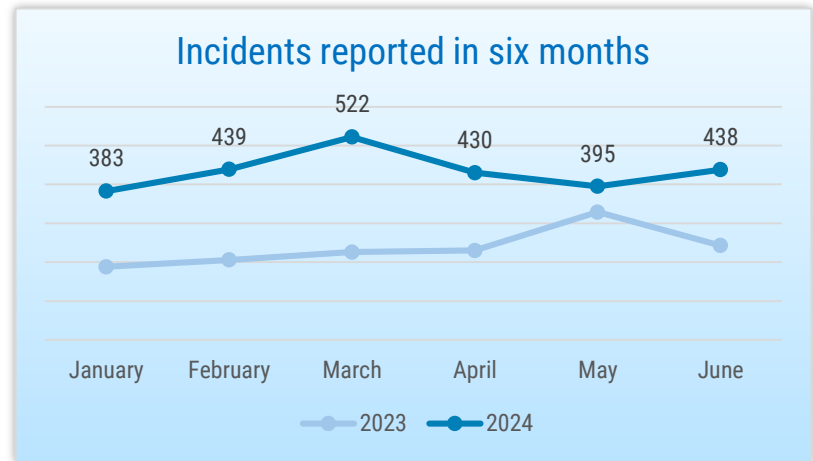




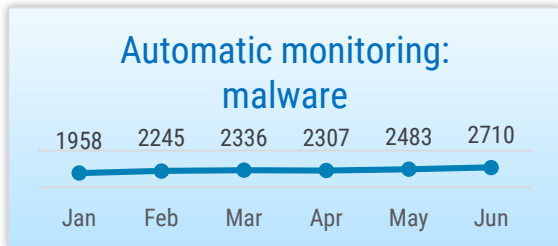
SITUATION IN CYBERSPACE

JUNE 2024

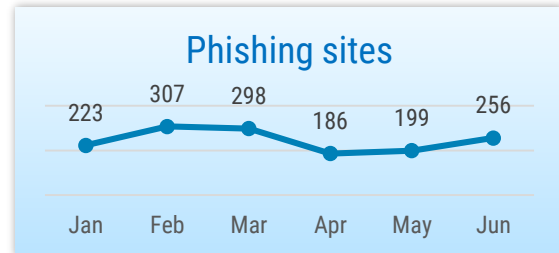
- In May, we recorded **438 incidents with an impact**, which is slightly above the average for the last six months.
- In June, there were some problems in the operation of **TEHIK services** and the use of **authentication services**. The data on the server of Tallinn Health Care College **was encrypted**.
- We helped to ensure the readiness, security, and technical support for **e-voting in the European Parliament elections**. The new, 2024 version of the Cyber test is ready.
- The data of nearly a thousand European and UK politicians were available on the **dark web**. The city of Cleveland fell victim to a **cyber attack**.



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

The situation in cyberspace was generally very calm during the European Parliament elections in Estonia from 3 June to 9 June, but unfortunately, we still experienced some technical malfunctions. On 3 June, the first day of e-voting, the users of Chrome and Firefox browsers had problems downloading the voter app from the valimised.ee website. Notably, web browsers initially considered the application file malware. In addition, at the beginning of the election period, the operating systems of visitors to the election website could not be identified, which led to some users being offered to download software designed for the wrong operating system.

In June, we saw a number of service disruptions. On 4 June, between 7.47 a.m. and 2.50 p.m., the services of TEHIK were interrupted for half a day due to a software failure of network equipment. By midday, the systems

were back up and running, but at around 1.30 p.m., they failed again. All services of TEHIK were affected, including telephones, email, websites, and information systems. Despite experiencing disruptions, ambulance brigades were still able to respond to calls and the Emergency Response Centre continued to operate without interruption.

From 10.35 p.m. on 11 June until 12.10 a.m. on 12 June, there were problems with the operation of Estonian and Lithuanian Mobile-ID. As a result, problems occurred when using Mobile-ID to log in to internet banks and other e-services and give digital signatures. On the morning of 20 June, there was a DDoS attack against the Smart-ID service, disrupting the service in all Baltic countries for nearly two hours. The attack was repeated on the morning of 21 June, causing disruptions to the Smart-ID service.

On several occasions there were failures in the information system for processing emergency notifications (SOS2). Users were unable to log in to the system and there were other service disruptions. The errors were caused by incorrect database configuration.

In the early morning of 4 June, a total of approximately 1.5 TB of data on the server of the Tallinn Health Care College was encrypted. The server was used to store the files of university staff and students. The incident affected more than 200 school staff, students, and other users of the file server. By 5 June, the services had been restored from a backup.

On 18 June, the Moodle server of Tallinn University of Technology was compromised. Attackers mapped the intranet and tried to gain access to computers on the intranet. The exact circumstances of the attack are still being clarified.



Activities of the Estonian Information System Authority

We helped to ensure the readiness, security, and technical support in the European Parliament elections, including e-voting. Election week took place from 3 June to 9 June and RIA was on high alert throughout the election period (orange, Charlie). This time, more than 153,000 people, or 41.5% of all voters, opted for e-voting. Technically, both e-voting and the election information system functioned without any major problems and the situation in cyberspace was very calm.

On 13 June, the last RIA CyberMeetUp event of the season took place. On this occasion, we were represented by Joosep Sander Juhanson (Information Security Expert, CERT-EE), who gave an overview of the situation in cyberspace. Master Sergeant Kristo Pals (Estonian Defence Forces) spoke about cyber military service in the Estonian Defence Forces. In addition, Rainer Ratnik (attorney-at-law, WIDEN) and

Helen Evert (insurance broker, IIZI) gave an overview of cyber insurance and its legal and practical aspects. Recordings of the June event and all previous events are available on the [website](#) of RIA.

We published a course on outsourcing (supply chain) in the Digital State Academy. The e-learning course 'Secure outsourcing with E-ITS' will help you to understand and implement best practices in outsourcing to ensure the protection of your organisation's data and the consistent quality of services. The Digital State Academy is primarily a learning platform for e-courses and digital skills in the public sector, but the training is open to all. The courses are free of charge and can be taken at a time and place of your choice.

The new, 2024 version of the Cyber test is ready. As previously, the cyber test consists of two parts: a course to

consolidate the basics and then a test to check your knowledge. In the course, we cover all of the most important topics related to cyber hygiene – password security, the spreading of malware, recognising phishing emails, using flash drives and other data media, secure remote working, and much more. This year, we have also included training videos that cover all the main topics and make the training more interesting. You can find out more about joining with Cyber test [here](#).

This year, we are organising a summer camp for girls interested in cyber security in Kehtna. The international cyber security camp CyberWizards will take place from 29 July to 3 August and is open to girls aged 13–16 who like to solve exciting problems and take on challenges. For more information on the camp, visit the [website](#) of RIA.



International situation

Cyber attacks linked to the military activities in Ukraine continued in June. CERT-UA [reported](#) that Ukrainian civil servants and members of the Defence Forces, as well as employees of defence industry companies, are being actively targeted by a malware campaign spreading through the Signal messaging application. In most cases, the malware is hidden inside a message sent to the victim with a link or file and a password to open it. When opened, it allows an attacker to take control of the device. To increase credibility, a previously compromised account on the victim's contact list may be used.

At the beginning of the month, it was revealed that the data of nearly a thousand European and UK politicians was available on the dark web. A report by technology companies Proton and Constella Intelligence reveals that the personal data of around a thousand European

and UK politicians – email addresses, dates of birth, and, in many cases, passwords – is up for sale on the dark web. British MPs have the most data available, followed by members of the European Parliament and the French Parliament. The data showed that in a number of cases, official email addresses were used to register user accounts in different environments, and in some cases, for example, in dating portals.

On 3 June, a ransomware attack hit the pathology and diagnostics provider Synnovis, which has partnerships with several major London hospitals. As a result, the work of hospitals is disrupted, with the incident mainly affecting blood transfusions and rapid blood tests. Many surgeries have had to be postponed and regular appointments cancelled. The attack is believed to have been carried out by a Russian ransomware group called Qilin.

In mid-June, the City of Cleveland reported that it had been the victim of a cyber attack and that many public services had been taken offline. Cyber attacks have disrupted American municipalities in the past, but Cleveland, with a population of 400,000, is the largest city so far to have had to temporarily shut down many services.

The United States has decided to completely ban the sale of products from the Russian cybersecurity company Kaspersky.Labs to US customers as of 20 July. The reason for the ban is the ties of Kaspersky.Labs to the Russian government and the possibility that the latter might pressure the company to share data on US clients to help plan cyber operations against the US. The current customers of Kaspersky include critical infrastructure companies and local governments of the US.