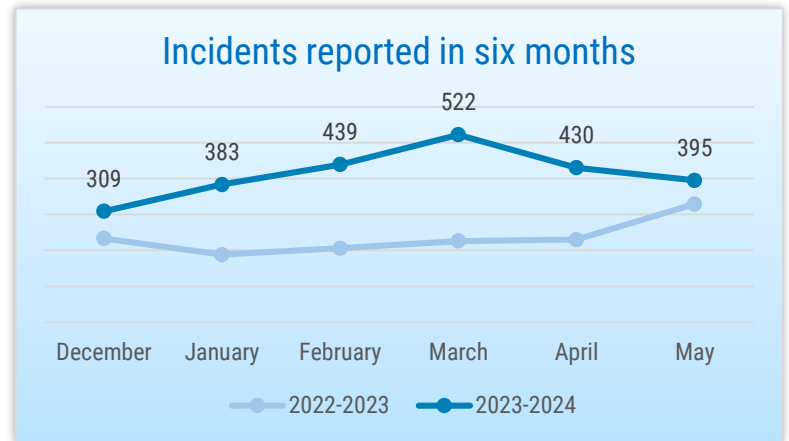




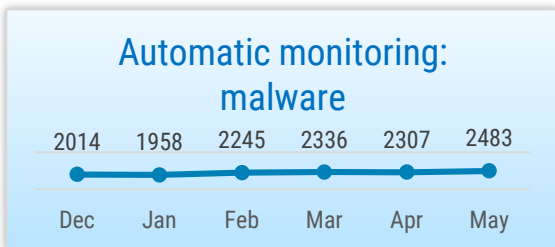
# SITUATION IN CYBERSPACE

MAY 2024

- In May, we recorded **395 incidents with an impact**, which is slightly below the average for the last six months.
- May brought along failures in the use of **authentication services** and **ticketing systems of public transportation**.
- We passed the **main audit of the Estonian Information Security Standard** successfully. We helped to ensure the **safety of online voting**.
- Cyber attacks related to **military activities continued**. The City of **Helsinki Education Division fell victim to a cyber attack**. There was a **data leak in the Ministry of Defence of the United Kingdom**.



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 May, we witnessed several failures of authentication services.

On 10 May from 2.00 p.m. to 10.30 p.m., Smart-ID registration services for minors were not available. For about an hour before noon on 14 May, there were disruptions in Smart-ID and Mobile-ID when using the services of SEB. Mobile-ID also failed for about an hour in the morning of 15 May. During the night of 18 May, another set of issues occurred when Mobile-ID services failed briefly for Tele2. CERT-EE is yet to learn about the reasons for these disruptions. On 20 May, Mobile-ID services failed for both Telia and Elisa. The Telia Mobile-ID services were disrupted from 8.01 a.m. to 9.55 a.m. due to an administrative error. On the same day from 1.07 p.m. to 1.26 p.m., Elisa's Mobile-ID services failed because of an equipment malfunction.

### There was a power cut in the Ravi Street and Magdaleena Units of East Tallinn Central Hospital in the

morning of 2 May. The hospital switched to generators, one of which failed to perform as expected, and as a result, some of the departments on Ravi Street were left without power. These facilities included a server room and the main communication node. As a consequence of the incident, the patient portal iPatsient of the East Tallinn Central Hospital was unavailable for four hours.

**There were a couple of issues with the ticket sales systems of public transportation.** On 7 May from 6.30 to 7.34 a.m., Elron's ticketing system [elron.pilet.ee](http://elron.pilet.ee) was unavailable. According to Ridango, the failure was caused by malfunctioning hardware, not an attack. The [tpilet.ee](http://tpilet.ee) website used for selling tickets for long-distance bus lines was unavailable from 2.00 to 9.07 a.m. on 25 May. The disruption was caused by a technical software error.

On 24 May from 8.13 to 10.10 p.m., **the services of the Health Insurance Fund for digital prescriptions and health insurance verification were disrupted.** They were restored after the application was restarted, but the CERT-EE team is yet to be informed about the reasons for the incident.

**Phishing messages sent on behalf of courier companies are still circulating.** Lately, we have seen an increasing number of messages claiming that a parcel cannot be delivered due to missing or incorrect address details. User is then directed to a phishing page to enter their bank card details. This way, various amounts were defrauded from Estonians in May, ranging from a few dozen to several thousand euros. We recommend that you contact the courier company by phone and check whether the message is genuine if you receive such a message and have even the slightest doubt about its validity.



# Activities of the Estonian Information System Authority

**At the end of April, RIA successfully completed the main audit of the implementation of the Estonian Information Security Standard (E-ITS)**, confirming that the necessary information security measures to protect the activities of the authority have been successfully applied. E-ITS was commissioned by the Information System Authority and compiled over several years. Its implementation is obligatory to all organisations performing public services. RIA started to implement E-ITS in the spring of 2022 and the process took about 18 months prior to the audit. The application of E-ITS is an ongoing activity, similarly to ensuring information security, because the processes, assets, and cyber risks of the organisation keep transforming. In the future, we will continue introducing the completed implementation plan of information security measures to all who want to learn from our experience.

**On 16 May, another monthly RIA CyberMeetUp took place.** Peeter Marvet (Police and Border Guard Board) explained the situation in cyberspace, Talis Pähn (CR14) discussed Open Cyber Range, and Tiina Pau (RIA) talked about the CyberWizards 2024 youth summer camp. Other speakers included guests from abroad – Daniela Bularda (ECCC, Romania) presented the international aspects of supporting the development of cybersecurity, and Antonin Dufka and Jan Kvapil (Masaryk University, Czech Republic) discussed MeeSign, a threshold cryptography platform. Both this and prior events are available on the [website](#) of RIA.

**We have been preparing for a long time to ensure the readiness, security, and technical support of online voting.** European Parliament elections will take place on 9 June. Online voting started at 9.00 a.m. on 3 June and will last until 8.00 p.m. on 8 June, available around the clock. In

addition, we organised a national campaign inviting people to vote securely, which includes checking their online votes with a smart device. More information is available [here](#).

**We were invited on the podcast Olukorrast digiriigis** (Situation in the Digital State) to discuss online voting. Alo Einla, Head of the Elections Infosystems Development Department at RIA, presented the contribution of the authority to organising elections. Among other things, the topic of the security of online voting came up. In the podcast, you will learn why online voting can be trusted, the number of control layers on the system, and when we might be able to use our mobile phones to vote. Listen to the podcast [here](#).

We commissioned a study from the University of Tartu which **will help Estonian companies to implement automation in production securely**. The study is available [here](#).



# International situation

## **Cyberattacks in relation to Russian military activities continued in May.**

CERT-UA [reported](#) that attacks against smart phones and other mobile devices of Ukrainian soldiers have become more frequent, initiated by hackers associated with Russian military intelligence GRU. The attacks mimicked popular applications, such as Kropyvva, but actually contained spyware. Malware was also sent through messaging applications Signal and Telegram. Attackers responded to defensive measures quickly and looked for ways to bypass them.

**On 2 May, the city government of Helsinki [communicated](#) that a cyber attack was launched against their education division**, which suffered a massive data leak. The attackers most likely took advantage of a critical vulnerability in the management interface of a remote desktop and managed to steal large amounts of data. The precise composition of data

is still being ascertained, but the information definitely included the personal data of thousands of children and young people, including sensitive health data; it also contained the data of adults who have used continued education opportunities provided by the city during the last few years.

In the first week of May, it was [disclosed](#) that **the personal data of over 225,000 active duty members, veterans, and reservists of the UK defence forces were leaked** through a payroll software used by the UK Ministry of Defence. The data included names and bank account details. According to BBC, the payroll software was provided by Shared Services Connected Ltd, and this incident once again emphasised the need to mitigate risks related to external service providers better, particularly in the defence sector.

## **The European Police Office Europol [confirmed](#) that their EPE (Europol Platform for Experts) portal was compromised and the resulting data leak is under investigation.**

According to the attackers, they managed to retrieve documents containing classified information and intended for internal use from the Europol systems. EPE is an online platform for police officials for sharing knowledge, good practices, and non-personalised data about crime.

**A week before the European Parliament elections in Germany, a cyber attack was [launched](#) against the conservative party of Ursula von der Leyen (CDU)**. The representative of the party did not reveal any details about the attack, but confirmed that they were forced to remove some of their IT systems from the network.