



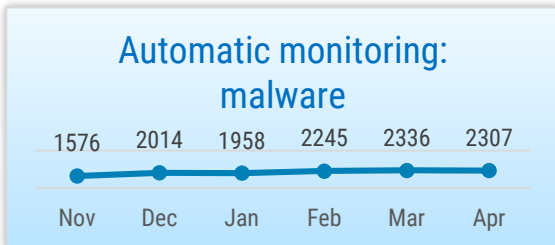
SITUATION IN CYBERSPACE

APRIL 2024

- In April, we recorded **430 incidents with an impact**, which is slightly above the average for the last six months.
- In April, failures occurred in the use of the **Examinations Information System** as well as in **digital signature provision**.
- In April, we carried out **E-ITS inclusion seminars**, where we offered practical advice to implementers of the standard. Eight startups launched in the Cyber Accelerator organised by RIA and Tehnopol.
- Cyber attacks related to **military activities continued**. The US cyber agency **CISA fell under a cyber attack**. One of the largest **platforms used by phishing scammers was closed down** as a result of international police operation.



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 April, problems with the Examinations Information System occurred on several occasions.

Entrance tests for the state upper secondary schools of Tallinn and Harju County were carried out on 6 April, but were suspended due to failures of the Examinations Information System (EIS); the test results will not be considered. According to Raivo Trummal, head of State School Management at the Ministry of Education, the failures were caused by a system overload. On 10 April, CERT-EE additionally received a notification that the personal information of 539 individuals is publicly available on the GitHub page of the Examinations Information System. These had been inserted there seven years prior and marked as test data, but were actually authentic personal data. The information has now been removed and the Education and Youth Board has said it will notify the Data Protection Inspectorate of the breach.

This month, there were also several failures in digital signature provision.

Digital signing was unavailable in the DigiDoc application from 9.53 to 10.57 a.m. on 12 April. The interruption was caused by the renewal of certificates by SK ID Solutions. From 8.32 p.m. on 15 April to 8.30 a.m. on 16 April, failures occurred with updating the DigiDoc application on Windows-operated devices. An error message was displayed to users who tried to update the application during that period and Microsoft Defender did not allow to launch the software. The incident was caused by human error: an unsigned file had been uploaded on the installer.id.ee page.

The Data Tracker – an eesti.ee state portal service that allows you to view queries related to your data – was unavailable for about 4 hours in the afternoon of 9 April. The interruption was caused by an error that occurred in the updating process.

Between 11.40 a.m. and 4.33 p.m. on 26 April, there was a **nationwide interruption in the service provision of an information system used by family physicians.** The issuing of prescriptions and certificates for sick leaves as well as registering for appointments was disrupted due to the failure. The failure was caused by a power outage in the main server of Medisoft AS.

In April, we also saw DoS attacks with impact. On 20 and 21 April, three DoS attacks occurred against ts.ee, the website of the Port of Tallinn. The attacks caused interruptions of a few minutes in the work of the website. On 24 April, from 9.13 to 9.57 a.m. and from 10.47 to 11.45 a.m., the Internet connection of the Tallinn Industrial Education Centre was out of use. The failure was caused by a cyber attack that overloaded the access channel used to provide an internet connection.



Activities of the Estonian Information System Authority

In April, we carried out yet another set of E-ITS inclusion seminars, where we give practical advice and recommendations to implementers of the Estonian Information Security Standard to simplify the understanding and implementation of the standard.

The presenters include implementers of the Estonian Information Security Standard, who share their experience in implementing the standard. If you wish to participate, keep an eye on the event [information](#) available in the E-ITS portal.

On 18 April, we organised a traditional RIA CyberMeetUp event.

This time, presentations were given by Lieutenant Colonel Urmet Tomp (NATO CCDCOE) and Dr Adrian Venables (TalTech), who gave an exclusive overview of the international cyber defence exercise Locked Shields organised by the NATO Cooperative Cyber Defence Centre of Excellence. Arne Ansper (Cybernetica AS)

introduced a conference dedicated to post-quantum cryptography and the importance of this topic. Märt Hiietamm (RIA) provided an overview of the situation in cyberspace. Both this and prior events are available on the [website](#) of RIA.

Eight startups launched in the Cyber Accelerator organised by Tehnopol and RIA.

The aim of the Cyber Accelerator is to bring new products and companies into the area of cyber security to benefit other companies as well. More information about the second round of the Cyber Accelerator and the participating companies is available [here](#).

We carried out a cybersecurity and cyber hygiene training for the library staff of Valga County.

We spoke about the safer use of computers and the internet and the scam and phishing schemes that could threaten us.

We visited the Raadio 2 show “R2 päev” to talk about the increasing number of cyber attacks.

Kaisa Vooremäe from the Analysis and Prevention Department of RIA explained which phishing and fraud schemes are spreading on the internet and how to recognise them.

Gert Auväärt, Deputy Director General of RIA, and Lauri Almann, Chairman of the Board of the Estonian Association of Information Technology and Telecommunications,

discussed the current situation in the field of cyber security, the main challenges in the public as well as private sector, and the strategic trends in the field in the podcast [Strateegia Akadeemia](#) of the Ministry of Economic Affairs and Communications. The viewers find out how the guests would grade the current situation of Estonia's cyber security and if the state and its citizens can sleep in peace.



International situation

Cyber attacks stemming from military activities also continued in April. The group Blackjack linked to the Security Service of Ukraine has allegedly [managed](#) to attack and destroy a data centre used by the Russian military industry and the energy and telecommunications sector. The data centre belonged to the cloud service provider OwenCloud.ru and is also used by Gazprom, Rosneft, Rostelecom, as well as several metallurgical companies. 300 terabytes of data was destroyed during the operation allegedly organised as a retaliation for an attack on Ukraine's data centre in January. The same group is now targeting the company Moskollector responsible for managing Moscow's sewage system, the work of which is said to be disrupted as a result.

[According to CERT-UA, a Russian hacker group carried out attacks on about 20 Ukrainian energy, water,](#)

[and heat providers in March 2024 to disrupt their information and communication systems.](#) CERT-UA reacted to the cyber attacks by removing the malware and increasing security measures.

[In January, the US cybersecurity agency CISA fell under a cyber attack,](#) during which the criminals managed to compromise two of the agency's information systems. The attack was carried out via a security vulnerability that was exploited across the world (including in Estonia) and for which a [warning](#) was issued by the agency in February. Now, in April, a CISA representative [confirmed](#) that no data theft was identified during the attacks. At the same time, the CISA also manages the Chemical Security Assessment Tool, from where the criminals might have retrieved sensitive data.

[As a result of an international police](#)

[operation where Estonia also participated,](#) one of the biggest platforms used by phishers, LabHost, was closed down with 37 suspects detained across the world. About ten of the suspects were targeting Estonia in their phishing schemes, mainly by imitating bank platforms. During an international investigation, at least 66,000 webpages used by about 10,000 criminals to embezzle data or money from victims were identified.

[A hospital in Cannes reported on 16 April that they have fallen victim to a cyber attack,](#) causing them to temporarily fall back on pen and paper and postpone nearly a third of their scheduled surgeries. Details of the attack have not been made public. The hospital notes in their announcement that a few months back, they had conducted an exercise to handle a situation like this, which is why the transfer to an extraordinary regime went quite smoothly.