

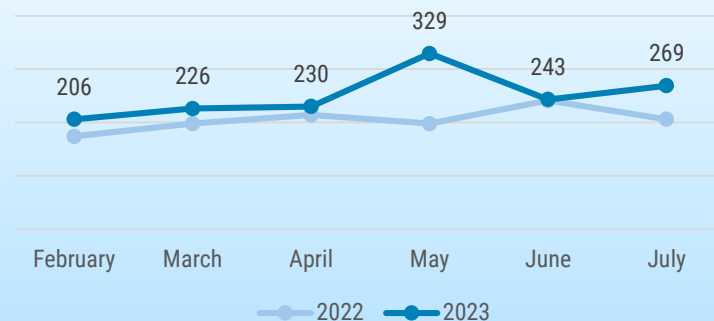


SITUATION IN CYBERSPACE

JULY 2023

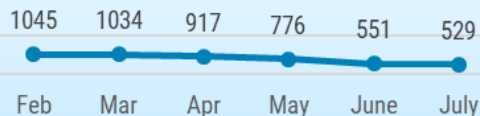
- In July, we **recorded 269 incidents with an impact**, which is slightly above the average for the last six months.
- Denial-of-service attacks continued. Over the past few months, we have seen a large number of **fake ads and scams on Facebook Marketplace**.
- In July, we ran a **cyber-awareness campaign** calling on people to be more aware of their habitual behaviour.
- In addition, **Kuku Radio launched a 10-part series called Ohtlik klikk** (A Dangerous Click) on cyber security.
- The **NATO summit in mid-July provoked cyber attacks**. At the end of the month, **Kenya was hit by a barrage of denial-of-service attacks**.

Incidents reported in six months



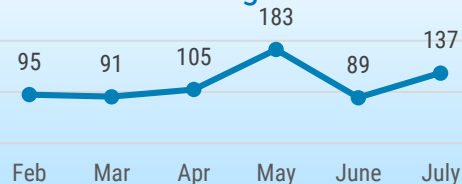
Incidents reported to CERT-EE that had an impact on the confidentiality, integrity, or availability of data or information systems.

Automatic monitoring:
malware



Devices in Estonian cyberspace infected with malware detected by automatic monitoring. CERT-EE notifies network owners of infections.

Phishing sites



Phishing sites still account for the largest proportion of incidents recorded by CERT-EE.



Situation in Estonian cyberspace

There were more service interruptions in July than in previous months.

On 1 July, between 2.16 a.m. and 12.17 p.m., the SiGa (Signature Gateway) signature service was down. This affected all clients of SiGa, including the Health and Welfare Information Systems Centre (TEHIK) and the Centre of Registers and Information Systems (RIK). The reason for the interruption was an expired TLS certificate, and after renewing the certificate, the service was restored. On 4 July, a broken Telia fibre-optic cable caused a 9-hour outage in Harku rural municipality.

The number of denial-of-service attacks has been stable in recent months.

On 7 and 8 July, denial-of-service attacks were carried out against the domain name servers of the Ministry of Foreign Affairs. These attacks passed without any significant impact, the websites were only down briefly. On 11 July, a DDoS attack was

launched against the sais.ee information system, which is used to submit applications for admission to universities, institutions of professional higher education, institutions of vocational education, and some upper secondary schools. As a result of the attack, the service was disrupted for about an hour. On 12 July, the domain name servers of the Information System Authority were hit by a denial-of-service attack and were down for a few minutes. On 15 July, ccdcoe.org, the website of the NATO Cooperative Cyber Defence Centre of Excellence, was attacked, but the attack had no effect.

At the beginning of the month, a healthcare institution alerted us of a cyber-attack.

As a result of the incident, data relating to day-to-day operations and administrative activities was lost from the file server. Fortunately, the institution had working backups and all data was restored.

This case is a perfect example of how important it is to make regular backups and how much extra work it can prevent.

Over the past few months, we have noticed fake ads on Facebook Marketplace offering various products at 10–20 times below market price.

The adverts are in incorrect Estonian and contain suspicious web links. In addition, schemes where the fraudster claims to be interested in the goods but does not have time to come and collect them in person and wants to send a courier are still attempted. If the seller agrees in good faith, the scammer will send a link, pretending to be from a courier company, asking the seller to confirm the delivery. This confirmation requires you to enter your bank card details, which will enable the fraudsters to make off with a few hundred euros. We advise you to be very careful on Facebook Marketplace as well as in other similar environments.



Activities of the Estonian Information System Authority

In July, we ran a cyber awareness campaign to draw attention to the threats that lurk in cyberspace in Estonia, which can leave our businesses and people without vital data, accounts, and money. As part of the campaign, we invited people to be more aware of their habitual behaviour and to test their knowledge on the [IT-vaatlik \(Be IT-conscious\)](#) website. Engaging and practical instructional videos will explain how to protect yourself from common cyber threats, and you can test your knowledge by taking a 12-question quiz. In addition, Ohtlik klikk (A Dangerous Click), a 10-part series on cybersecurity, was launched on 3 July and will air every Monday on Kuku Radio. The aim of the series is to inform about the dangers and concerns in cyberspace and about the personal responsibility in preventing and dealing with the consequences of cyber incidents. The radio broadcasts can be listened to [here](#).

The second quarterly assessment of this year shows that phishing messages and emails continue to account for a large proportion of incidents. In addition, we wrote about online shops with outdated software, supply chain attacks, and the Cyber test. You can read the assessment [here](#).

In a DigiPRO Geenius [article](#), Märt Hiieamm, Head of the Analysis and Prevention Department of RIA, and Marju Hendre, Chief Analyst in the same department, talk about the dangers lurking in the cyber world, the most common ways Estonians are deceived, and tips to protect yourself from such threats. In addition, we also talked about the Cyber test created by RIA and the public test on the 'IT-vaatlik' website.

On 10–11 July, representatives of 19 Member States of the EU and of 148 institutions/businesses gathered in

Paris to kick-start pilot projects for the future EU-wide digital identity application (EUDI Wallet). Estonia, coordinated by RIA, is participating in the development of the technical solution for testing the digital driving licence. Read more on the project [website](#).

We started six new supervisory procedures. The aim of the supervision is to verify compliance with cyber security requirements from the point of view of the implementation of organisational, physical, and IT security measures. We assess the adequacy of the security measures in place to prevent, report, and respond to cyber incidents. In addition, we issued two precepts and closed two proceedings. The main reasons for issuing the precepts were shortcomings in the organisation and security architecture of cross-organisational information security.



International situation

Cyber-attacks related to military activities continued. At the beginning of the month, the [website and mobile applications of RZD](#), the Russian national railway company, were down due to a cyber attack. This meant that train passengers could only buy tickets at the train station and RZD had to add ticket kiosks at stations. The online services of the company were unavailable for at least six hours, with some disruptions lasting longer. Responsibility for the cyber attack was claimed by the IT Army of Ukraine.

In mid-July, a NATO summit was held in Lithuania, which provoked a series of cyber attacks. Hackers took down several websites related to tourism and transport. For example, stops.lt, which allows people to plan their journey, was targeted. The Russian attackers also managed to take over the airwaves of a local radio station and the music channel of a shopping mall, both of which replaced

the music with pro-Russian propaganda urging against giving arms to Ukraine. In both cases, an online music streaming platform [was compromised](#) as a third party. According to the Lithuanian cyber centre, the incidents were quickly detected and the broadcasts of disinformation were stopped. The cyber centre also confirmed denial-of-service attacks and advised Vilnius residents in general to be vigilant.

[Nagoya Port](#), one of the largest and busiest ports in Japan, was hit by a ransomware attack, which shut down the port for at least a few days. A large amount of Japan's trade passes through the port of Nagoya, including, for example, exports of Toyota cars. The attack was carried out by a criminal cyber group operating in Russia called LockBit, which demands a ransom from the port.

[At the end of July, Kenya was also fighting off a huge cyber-attack.](#)

According to the authorities, a local government portal used for more than 5,000 government services was attacked. The hacker group Anonymous Sudan has claimed responsibility for the attack.

[In the UK, a cyber-attack on software company Ortivus disrupted the work of ambulances](#), forcing affected ambulances to operate with pen and paper. The treatment of patients and the work of the ambulance service continued, but by working manually instead of using electronic systems.

[Businesses were also hit by cyber attacks.](#) For example, the [Taiwanese chipmaker TSMC](#), whose customers include Apple, confirmed that their data was stolen in the aftermath of a cyber-attack. Responsibility for the attack has been claimed by the ransomware group LockBit, which now demands 70 million dollars for non-disclosure.