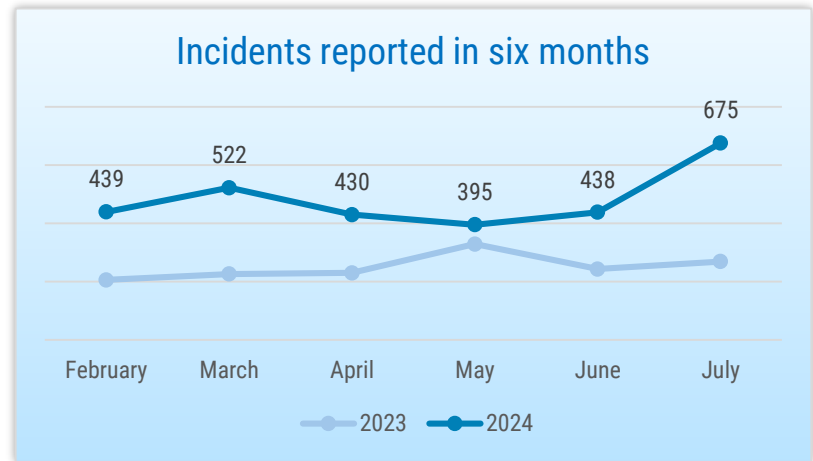




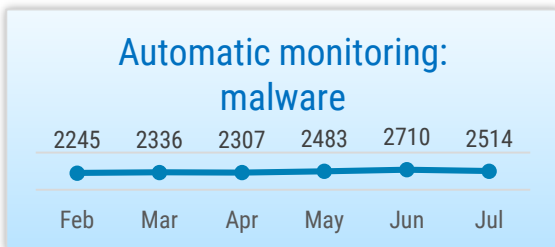
SITUATION IN CYBERSPACE

JULY 2024

- In July, we recorded **675 incidents with an impact**, which is the highest result in the last six months.
- Over half of the registered incidents were **phishing pages**, which are increasingly popular for defrauding people of money or account details.
- We supported the preparation of **the national cybersecurity strategy for 2024–2030**. We published new **materials** to help companies implement information security measures more easily.
- The UEFA Euro 2024 brought along **cyber attacks**. NATO member states are creating a new **cyber defence centre** in Belgium.



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

Elsewhere in the world, a faulty software update of CrowdStrike caused extensive malfunctions and interruptions, incapacitating 8.5 million Windows devices. Different sectors in many countries were affected – aviation, healthcare, trade, banking, and media. However, it did not cause significant disruptions in Estonia. Here, CrowdStrike Falcon Sensor is not widely used. As far as we know, it impacted one energy company and one private enterprise. In the former, internal services and customer service were interrupted for a few hours, but there was no impact on energy production. The CrowdStrike malfunction also disrupted checking into Ryanair flights at the Tallinn Airport.

In July, several disruptions occurred in the various services of the Health and Welfare Information Systems Centre. From 8.05 a.m. until 9.14 a.m. on 1 July, the digiregistratuur.ee web

page was down. The malfunction was caused by a network disruption, following which the services were not immediately restored. There were interruptions in the functioning of digital prescriptions, as well. Starting from 8.30 a.m. on 6 July, some prescription medications had incorrect discount rates and it was not possible to prescribe certain other prescription medications. The incident was caused by incorrect data and it was resolved by 2.18 p.m. on 8 July. From 2.29 p.m. until 2.47 p.m. on 10 July, the main services of the Health Insurance Fund (digital prescriptions, checking the existence of valid health insurance) were unavailable through X-tee. This was caused by a malfunction in a Java application and the functionality of the services was restored after a restart.

July also witnessed several phishing incidents. Phishing emails, seemingly sent on behalf of the police and claiming that the recipient's Smart-

ID had expired, were the most common. Emails with various subject lines were also sent pretending to be the police, claiming that the recipient of the email is subject to legal proceedings and the email constitutes a summons to a hearing. We recommend that you do not open the attachment of the email and delete the letter instead. The emails phishing for Smart-ID account details claimed that the account of the user had been suspended and they had to verify their identity to restore it. The emails were sent from a random domain that is not connected to the Smart-ID service and they contained a link directing to a phishing site.

On 29 July, a small company in Tartu fell victim to a ransomware attack. In the course of the incident, malware encrypted files in four computers. The normal operation of the company was interrupted and an ongoing investigation is focusing on ascertaining the exact circumstances.



Activities of the Estonian Information System Authority

Until 2 September, SMEs can apply for a grant for the evaluation and upgrade of their cybersecurity to prevent damage caused by cyber attacks or technical malfunctions.

The amount of the grant is 60,000 euros and it consists of two parts: 10,000 euros for the evaluation of the cybersecurity of the company and 50,000 euros for development. For more information about applying for the cyber grant, please visit the [website](#) of Enterprise Estonia.

We notified the owners of network devices whose devices might contain the CVE-2024-6387 vulnerability of OpenSSH.

This is a vulnerability allowing unauthorised access to the system to an attacker who has managed to take advantage of it successfully. We suggested that everyone update their Open SSH server application to the most recent version, where the aforementioned vulnerability has been patched.

CERT-EE releases such statements frequently and we recommend that you take these seriously, because attackers often gain access through unpatched software.

The Ministry of Economic Affairs and Communications and the Estonian Information System Authority prepared **the Estonian national cybersecurity strategy for 2024–2030 ‘Läbivalt IT-vaatlikum Eesti’** (‘A more IT-conscious Estonia’) which sets the safety and trustworthiness of Estonian cyberspace as well as its resilience to cyber threats as its main objectives. The Estonian cybersecurity strategy maps the most recent changes in this area and describes the necessary course for adjusting to them. The cybersecurity strategy is available [here](#).

Kaisa Vooremäe, Prevention Manager at the Analysis and Prevention Department of RIA,

was a guest at the studio of Kuku Raadio to [discuss](#) threats in our cyberspace and ways to protect against them. We also reminded people how to recognise phishing pages and what a virtual private network (VPN) is.

We published new [materials](#) to help companies start implementing cybersecurity measures. The initial measures of the Estonian Information Security Standard (E-ITS) are primarily meant for companies that have not systematically addressed cybersecurity before and do not have to comply with the requirements of the Cybersecurity Act, but want to protect their business operations and customer data better. The recently completed cybersecurity guidelines help companies and organisations prevent economic and reputational damage caused by cyber attacks, data leaks, and technical issues.



International situation

The European Football Championships, which took place from 14 June until 14 July, brought along several cyberattacks. A CyberInt [report](#) revealed that the number of cyber attacks against the members of the UEFA (Union of European Football Associations) increased during the Euro 2024 and several dark web forums are offering the account details of thousands of UEFA partners and clients for sale. In addition, DDoS attacks against media channels reporting on the games were carried out. The report states that the increase in the number of cyber attacks in relation to a large sports event has become the new normal, while also predicting the same for the Olympic Games in Paris, taking place from 26 July to 11 August.

In spring, the entertainment company LiveNation/Ticketmaster was targeted with a cyber attack that allowed the criminals to steal a cloud

-based database. In July, criminals [claimed](#) that they are also in possession of the barcodes for 166,000 tickets of the ongoing Taylor Swift tour and the ticket details of several other major events (such as Formula 1, Sting concerts, etc.), demanding millions of dollars for not releasing them. Ticketmaster, in turn, assured that the barcodes of tickets are updated regularly and the stolen tickets are therefore invalid.

NATO member states are [creating a new cyber defence centre in Belgium](#). The purpose of the centre is to increase the level of security of NATO networks and to improve situational awareness as well as the protection of cyberspace in peacetime and during crises and conflicts. Military and civilian experts from NATO countries are going to be employed by the centre and it will provide information to the NATO commanders-in-chief about the vulnerabilities and threats in cyberspace.

In the middle of July, a faulty CrowdStrike update [led to global interruptions in Windows systems](#), impacting the operation of many organisations and services. This malfunction resulted in a so-called blue screen in the affected Windows workstations and servers, causing disruptions in the work of many providers of vital and important services, such as airports, hospitals, and harbours. On 30 July, a DDoS attack against Microsoft [took place](#), disrupting the work of several services (such as Outlook and Azure) for nearly ten hours.

The law enforcement agencies of the United Kingdom [closed down a platform for ordering denial-of-service attacks called DigitalStress](#). It was one of the most popular platforms for ordering denial-of-service attacks (DDoS), allowing people with low technical skills to commit cyber attacks.