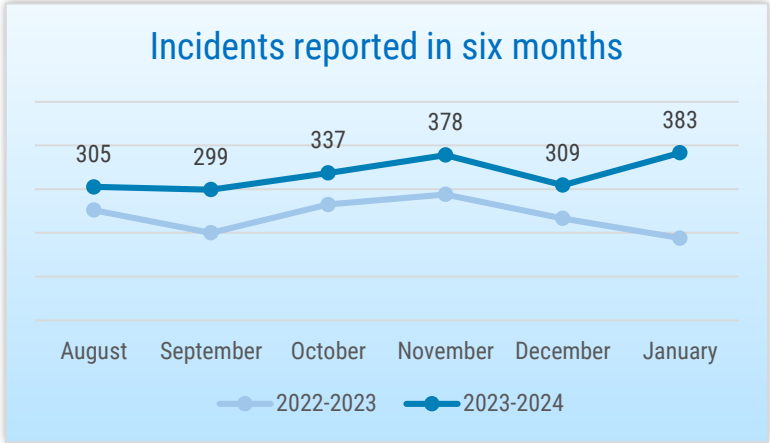
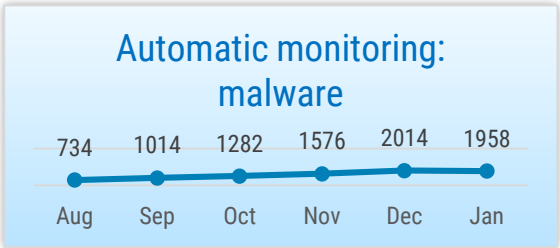
RIIGI INFOSÜSTEEMI AMET

SITUATION IN CYBERSPACE JANUARY 2024

- In January, we recorded **383 incidents with an impact**, which is the highest indicator for the last six months.
- In January, the family allowance and parental benefit payments of some individuals were transferred to **outdated bank accounts**. A company in Tallinn was hit by a **ransomware attack**.
- We organised a **cyber training** for ICT teachers, carried out an **information day** on the cyber defence of critical infrastructure, and renewed the **E-ITS portal** and the Estonian information security standard.
- Cyber attacks related to military activities continued. **Tietoevry's** data centre in Sweden was subject to a ransomware attack. **Microsoft** fell under 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

In January, we registered 17 denial-of-service attacks with an impact. On 2 January, there was a DDoS attack against the Tax and Customs Board's website emta.ee, on 3 January against the National Library's website rara.ee, and on 7 January against the err.ee news portal of the Estonian Public Broadcasting. There were short-term disruptions in the work of all three websites. On 12 January, a group engaging in denial-of-service attacks declared several Estonian websites and services as targets: tallinn.ee, evr.ee, pilet.ee, mnt.ee, nasdaqbaltic.com, app.energia.ee, nordica.ee, and the name servers of the RMIT and the state network. Attacks against the name servers and Nordica's website caused disruptions, while other attempts failed to have an impact. The group mentioned Estonia's support of Ukraine as the incentive for the attacks. On 22 January, the name servers of RIA and SMIT fell under denial-of-service attacks. Both services were disrupted due to the attack: several websites managed by SMIT and RIA opened slower than usual or displayed an error message while users were waiting.

The Social Insurance Board transferred January's family allowance and parental benefit payments of some individuals to their outdated bank accounts. The error affected about 1,400 people who had changed their account number for receiving allowances or benefits. The error was partly caused by a human mistake as well as a system error. The Social Insurance Board notified the persons affected who received their benefits later than normal, and the Data Protection Inspectorate.

On 18 January, a company operating in Tallinn fell victim to a ransomware attack. During the attack, the data on the company's server was encrypted, including documents as well as a financial software database. Based on preliminary information, a weakly protected Remote Desktop Protocol (RDP) was used for the attack.

Facebook Marketplace scams, which have been used by fraudsters for money-making for quite some time, continued in January. The scheme is normally as follows: the fraudster contacts a person selling an item on Facebook and claims to be interested in buying it. They then find an excuse why they cannot pick up the goods in person and ask to use a courier service. The seller is then asked to pay a delivery fee or insure the parcel to verify the transaction and is lead to a phishing page to enter their bank account details. The scam victim normally loses a few hundred euros, but at the end of last year, we saw a case where the losses exceeded 10,000 euros.

Activities of the Estonian Information System Authority

We organised a cybersecurity training for ICT teachers. On 4–5 January, the R&D Coordination Department of RIA led the cybersecurity training 'Hands-on Hacking Essentials' for the teachers of ICT specialties in vocational schools. The training was carried out by Clarified Security and its purpose was to raise the level of knowledge and skills of the teachers to integrate the topics of cybersecurity with more awareness when teaching ICT specialties. Feedback from participants was very positive and a lot of new knowledge was acquired.

On 18 January, we organised an information day for the cyber defence of critical infrastructure, the target group of which includes representatives of establishments providing and organising vital and essential services in Estonia. The range of topics was varied: we spoke about the situation in cyberspace, the legal space, as well as the management of cyber crises in Estonia. In addition, presentations were made by the providers of several vitals services. The information day had over 100 participants from state agencies as well as companies.

Several security vulnerabilities became apparent this month. The persons concerned were notified by the CERT-EE team. For example, in mid-January, we notified all establishments and companies who are using vulnerable GitLab versions based on our monitoring data. We advise to always take these kinds of notifications seriously and to react quickly by updating software. Unfortunately, we often see cyber attacks that have succeeded precisely via unpatched software.

We renewed the E-ITS portal and completed the 2023 version of the Estonian information security standard. The E-ITS is a collection of requirements and best practices that helps to raise the level of information security in both the public and private sectors.

On 25 January, we organised another RIA CyberMeetUp event, which had three speakers this time. Tanel Sepp, Director General for the Digital and Cyber Diplomacy Department at the Ministry of Foreign Affairs, spoke about the Tallinn Mechanism, which aims to amplify the cyber support of donor countries to Ukraine in the civilian domain. Edgars Milgravis, Regional Sales Manager of the Baltics at Palo Alto Networks, gave an overview of the threats of the cyber world during the previous and the current year. Finally, Vjatšeslav Antipenko, Junior Research Fellow at the University of Tartu, spoke about the management of IoT (Internet of Things) projects and their links to research in the field of cybersecurity.

International situation

Cyber attacks stemming from military activities also continued in January. According to the Security Service of Ukraine (SBU), Russian state-sponsored cyber groups have hacked several surveillance cameras located on residential buildings in Kyiv. The viewing angles of two cameras were recently altered and used to monitor the work of Ukrainian air defence and critical infrastructure facilities and for more efficient aiming during the missile and drone strikes against Kyiv on 2 January.

At the end of January, a data centre located in Kyiv fell under a cyber attack affecting several state companies offering vital services: the oil and gas company Naftogaz, the national postal service provider Ukrposhta, the transport security authority DSBT and the national railway company Ukrzaliznytsia. Due to the attack, services were disrupted, websites were down, and Ukrzaliznytsia had to stop the online sale of train tickets. The group behind the attack is unknown, however groups of Russian background are suspected.

The airport in Beirut was hit by a cyber attack which compromised the Flight Information Display System, displaying messages against Hezbollah and Iran and accusing them of dragging Lebanon into a full-scale military conflict with Israel. The attack also disrupted the Baggage Handling System.

Companies were hit by cyber attacks of significant impact this month. On 19 January, the software and digital service company Tietoevry, or more precisely its data centre located in Sweden, was hit by a ransomware attack. Tietoevry is one of the largest IT-companies in the Northern and Baltic countries with more than 24,000 employees worldwide, of which about a thousand work in the Baltic states, including Estonia. According to the company, the impact of the attack was limited, but caused service disruptions for several Swedish customers. For example, Sweden's largest movie theatre chain Filmstaden was unable to sell tickets online; several other companies experienced similar problems, and the recovery of services is still underway.

Microsoft announced that it discovered traces of a cyber attack in its system on 12 January. The attack is thought to be organised by a group with links to the Russian foreign intelligence. The attackers are said to have succeeded in compromising one inactive account in November 2023, using it to infiltrate the mailboxes of some of the employees, including members of the management. The hackers managed to steal documents and emails and their initial interest appeared to be information regarding themselves and their analysis by Microsoft.