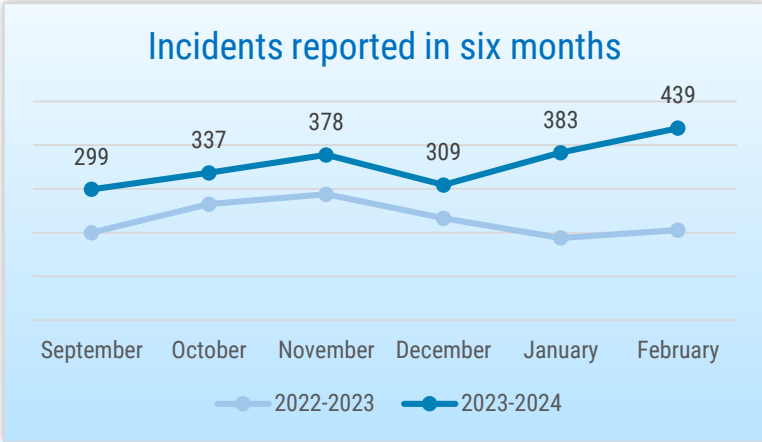
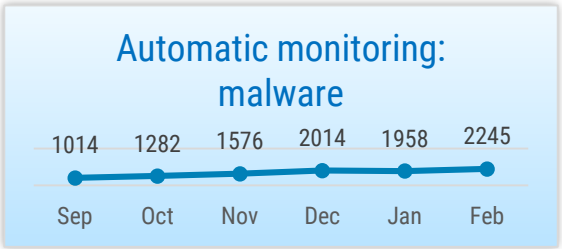
RIIGI INFOSÜSTEEMI AMET

SITUATION IN CYBERSPACE FEBRUARY 2024

- In February, we recorded **439 incidents with an impact**, which is the highest indicator for the last six months.
- In February, **numerous institutions** were affected by cyber incidents. In addition, both **phishing and malware emails** were sent on behalf of companies.
- We published the **RIA cyber security yearbook**, which summarises the most important cyber incidents of the past year and describes the situation in cyberspace.
- Cyber attacks related to military activities continued. The maker of **AnyDesk was hit by a cyber attack**. Several incidents affecting the **health sector** occurred.



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 February, numerous institutions were hit by cyber incidents.

On 2 February, one public authority reported that their VPN servers had been compromised. The attack, which started in January, mapped the institution's network and may have also leaked data. By now, all affected servers have been shut down and the impact of the attack is being analysed. The Ivanti vulnerabilities were used to attack, which you can read more about here.

Another institution upgraded its file hosting software, but an error occurred and the system had to be restored from a backup copy. During the restoration process, it was discovered that the backup function had been down for some time and therefore, not all data could be restored. It is not yet clear how much of the data of the institution and its sub-institutions has disappeared.

On 10 February, it was **not possible to access many of the services of the IT and Development Centre at the Estonian Ministry of the Interior (SMIT),** including e-Police, the call recording system, and the remote working solution. The failures were caused by a fault in the SMIT firewall.

On 16 February, the income tax return page of the Tax and Customs Board at tuludeklaratsioon.emta.ee was unavailable for about half an hour. The outage coincided with the period for filing income tax returns and was caused by a disk overload on the web server.

On the night of 22 February, SK ID Solutions carried out routine maintenance. During this process, an error occurred and for almost ten hours, the validation service responded with 'INVALID' when checking the validity of an institution's certificates (digital stamps, authentication and encryption certificates).

In February, both phishing and malware emails were sent on behalf of companies. On the morning of 23 February, letters in faulty Estonian started arriving in many people's mailboxes, calling for the renewal of domain names. The emails were seemingly sent from Zone Media OÜ, included a fake link, and attempted to obtain usernames and passwords. The emails were sent by random domains, which made it possible to tell that they were not legitimate.

At the same time, emails sent on behalf of Tallink were also circulating, with a Trojan-type malware-infected file attached. Once again, the letter was sent from a random domain and claimed to have a subscription attached. Such emails should be forwarded to the CERT-EE for investigation and then deleted. It is very important to take note of the address from which the message was sent and, in the case of an unknown sender, never open the attachment.

Activities of the Estonian Information System Authority

At the beginning of the month, we published the RIA cyber security yearbook, which summarises the most important cyber incidents of the past year and describes the situation in cyberspace. We recorded 3,314 cyber incidents with an impact last year, which is 24% more than in 2022; there were record highs in both politically motivated cyber incidents and scams designed to steal money from people and businesses. In addition to the above, you can read about serious cyber incidents that affected Estonia's healthcare sector, the wave of dangerous security vulnerabilities, events in international cyberspace, and much more in the latest cyber security yearbook. The yearbook is available here.

In both January and February, critical security vulnerabilities in a number of widely used software products were disclosed. For example, the CERT-EE team alerted nearly two hundred users of Fortinet products about devices on their network that could be affected by a critical security vulnerability in FortiOS. We recommended updating the FortiOS software as soon as possible, as Fortinet devices and their vulnerabilities have often been targeted by attackers.

We visited the Lasnamäe District Administration to talk about cyber hygiene. Analysts of RIA's Analysis and Prevention Department provided an overview of internet scams, how to spot them, and how to use the internet safely. The free internet safety lectures were organised by the Lasnamäe District Administration in cooperation with the Tallinn Central Library, the Police and Border Guard Board, and RIA. The main objective of the lecture series was to raise awareness among the elderly of the various fraud and scam schemes.

On 22 February, another CyberMeetUp event took place at the Palo Alto Club in Tallinn. This time, presentations were given by cyber start-ups participating in the cyber accelerator programme. As the programme is drawing to a close, it is a good time to take stock of what has been done and what problems have been solved. In addition, Kaisa Vooremäe, Prevention Manager at RIA, spoke about the latest RIA cyber security yearbook. Recordings of this and all previous events can be viewed on the website of RIA.

Listen also to the podcast "Olukorrast digiriigis", where Märt Hiietamm, Head of the Analysis and Prevention Department of RIA, talks about the new cyber security yearbook, the situation in Estonian cyberspace, what RIA is doing to improve cyber security, and what people and companies can do to protect themselves.

International situation

War-related cyber attacks also continued in February. According to the State Service of Special Communications and Information Protection of Ukraine (SSSCIP), Russian hackers infiltrated several popular Ukrainian news portals and spread war-related misinformation through them. One of Ukraine's most widely read online publications, Ukrainska Pravda, the business newspaper Liga.net, and the news portals Apostrophe and Telegraf were affected by the attack.

On 7 February, the FBI, CISA, and the NSA, along with other members of the Five Eyes intelligence alliance, issued a warning that the Chinese state-sponsored hackers' group Volt Typhoon has been infiltrating US critical infrastructure networks, for example in the communications, energy, transport, and water sectors, for years. In some cases, access was gained at least five years ago. According to the agencies, the purpose thereof is not cyber intelligence, but pre-positioning for future destructive attacks. The agencies have also issued technical guidelines on how to protect against Volt Typhoon and other groups with a similar modus operandi.

The German company developing the popular AnyDesk remote access software reported that a recent cyber attack breached their production environment. There is also evidence of a data leak – the details of thousands of customers of AnyDesk (contact information, session information, customer IDs, etc.) have been put up for sale on the dark web. Although AnyDesk advised all customers to change their passwords and update their software following the incident, some of the data on sale on the dark web was obtained after the incident became public. AnyDesk has 170,000 customers worldwide.

Several incidents affecting the healthcare sector took place this month. A ransomware attack against a medical sector information system led to a situation in Romania where hundreds of hospitals were forced to disconnect their systems from the network. The attack used the Backmydata ransomware and demanded a ransom of 3.5 bitcoins, but the group did not disclose its name in the ransom note. The attack forced hospitals to reorganise their work, with prescriptions and medical records being written by hand.

A cyber attack disrupted the work of pharmacies across the US. Change Healthcare, a provider of software for pharmacies, was forced to shut down some of its systems following a cyber attack. This meant that many pharmacies across the US could not, for example, check whether patients had health insurance or if they were eligible for prescription drugs and benefits.