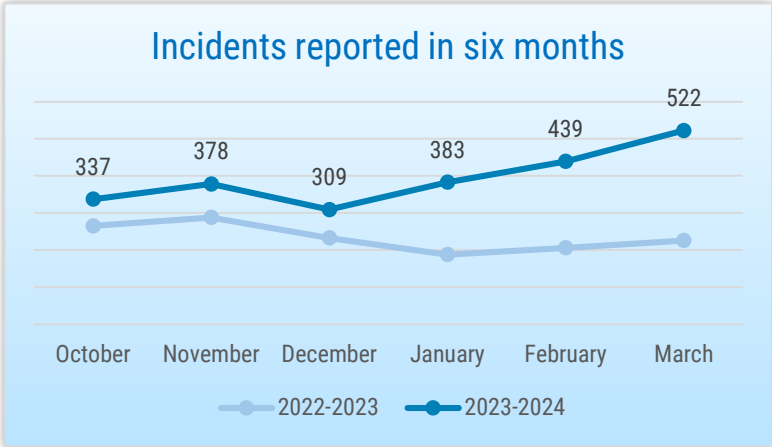
RIIGI INFOSÜSTEEMI AMET

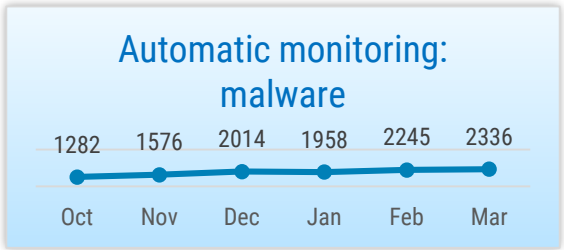
SITUATION IN CYBERSPACE

MARCH 2024

- In March, we recorded **522 incidents with an impact**, which is the highest indicator for the last six months.
- On 1 March, **cash handling company Hansab experienced a cyber incident**. On 9 March, the largest denial-of-service attack so far was carried out against Estonian public sector webpages.
- We ordered an **analysis on the cybersecurity risks of artificial intelligence and machine learning technologies** and the mitigation options thereof. We published the **English-language version of the Cyber Security Yearbook**.
- Cyberattacks related to military activities continued. **Microsoft** is still handling the consequences of the cyber incident from January. The **French unemployment** office fell under a cyberattack.



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

On 1 March, the cash handling and payment terminal provision company Hansab fell under a cyberattack. In Estonia, Hansab fulfills cash orders for ATMs for Swedbank, Luminor and LHV banks. As a result of the cyberattack, the operations of some of Hansab's IT systems were disrupted, but the services of the commercial banks remained operational. The company disconnected its systems from the external network as soon as it heard from the incident and started investigating the exact circumstances.

On 9 March, the largest denial-of-service attack so far was carried out against Estonian public sector webpages. The targeted webpages were ttja.ee, airport.ee, mkm.ee, ria.ee, riigikogu.ee, siseministeerium.ee, transpordiamet.ee, transport.tallinn.ee, eesti.ee, id.ee, estonia.ee, president.ee, emta.ee, politsei.ee, and just.ee. Nearly three billion malicious queries were made in just over four hours. The last record-breaking attack against the public sector was carried out in August 2022 with 425 million queries against the id.ee webpage. On 10 March, attacks against the CERT-EE webpages report.cert.ee and cuckoo.cert.ee followed, causing disruptions in their work over a period of a few hours.

On 18 March between 00:06 until 9:26, ID-card authentication was unavailable in the state authentication service TARA and the state SSO (single-sign-on) service. The interruption was caused by the expiration of a certificate.

The work of the eesti.ee portal was interrupted on three occasions. The malfunctions experienced in the evening of 14 March between 18:57 and 19:11 were caused by a setup error made during updates. On 21 March, some of the eesti.ee state portal services were unavailable for about two and a half hours. The interruptions were caused by an error that occurred while changing the certificates of the X-tee security servers. On 26 March, failures when logging in to the state portal were experienced over a period of 2 hours with the cause still unknown.

On 4 April, a data leak concerning the loyalty card owners of Apotheka, Apotheka Beauty, and Pet City was disclosed. In January, a backup copy of a database storing information from the years 2014–2020 fell into the hands of offenders. About 700,000 personal identification codes, more than 400,000 e-mail addresses, nearly 60,000 home addresses and about 30,000 phone numbers of Apotheka, Apotheka Beauty and PetCity loyalty card owners were leaked. Data of about 43 million purchases also leaked with information about acquired OTC medicines and other pharmaceutical products such as band-aids or analgesics visible. The offenders did not gain access to data concerning purchased prescription drugs.

Activities of the Estonian Information System Authority

In an interview to the Geenius portal, the head of CERT-EE Veiko Raasuke described the situation in Estonian cyberspace and the tasks his team handles on a daily basis. Defence measures developed by the Information System Authority and the future plans for CERT were also discussed. Among other things, Veikko advises on how to act in case of a ransomware attack and acknowledges that attacks are becoming more specifically targeted. The interview also covers a programme that pays ethical hackers for discovering and reporting security weaknesses in Estonia's digital state.

The RIA Cybersecurity Yearbook published in February has now been translated into English and is available here.

The Research and Development Coordination Department of RIA ordered an analysis on the cybersecurity risks of artificial intelligence and machine learning technologies and the mitigation options thereof which offers a summary of the different AI/ML models and proposes cybersecurity risks to look out for. The analysis is intended for everyone who plan to use artificial intelligence and machine learning technologies. The analysis of Cybernetica AS describes the current situation with AI systems and their distribution models as well as the associated risks and the mitigation measures thereof. Among other things, the analysis provides companies with an overview of the regulatory environment of the field of artificial intelligence applicable in 2024, including the initiatives and propositions of the European Union.

On 21 March, there was another RIA CyberMeetUp event. Aleksi Rantaniemi from the National Cyber Security Centre Finland (NCSC-FI) gave an overview of the cyber threats that Finland faces. A broader view of the threats and the situation in the region was provided by Juha Remes, chairman of the board of the North European Cybersecurity Cluster (NECC). The section "Situation in cyberspace" was covered by Brendan Dowling, Australia's Ambassador for Cyber Affairs and Critical Technology. The presentations were concluded by Hendrik Pillmann, expert-coordinator at the TAK, who introduced the results of the analysis of the risks of artificial intelligence and machine learning technologies and the mitigation options thereof prepared by Cybernetica. The presentations can be viewed on Facebook as live-streams or watched later on RIA's webpage.

We were guests at Vikerraadio's "Huvitaja" radio programme to talk about DoS attacks – what they are and how to protect your devices from being manipulated by cyber criminals.

International situation

According to the Defence Intelligence of Ukraine (GUR), their hackers gained access to the servers of the Russian Ministry of Defence and acquired sensitive information regarding their structural units and staff, the orders, instructions, and other documents used by the Russian intelligence and information regarding the encryption software and information security measures applied. Ukraine's press release has separately specified the Russian Deputy Minister of Defence, Timur Vadimovich Ivanov, whose documents were also accessed and who is said to have played a significant part in the success of the operation.

The German Ministry of Defence was forced to confirm that the conversation between the head of the German Air Force Operations and other high-ranking officers regarding assistance to Ukraine published full-length in Russian media in early March is legitimate. The Germans failed to use a secure communication channel, but opted for the Cisco WebEx platform instead and the recording was forwarded to the media by Russian intelligence. As the German officers also discussed the British and French arms supply to Ukraine and the support offered to Ukrainians on site, The United Kingdom and France were also disturbed by the leak scandal.

The hacking group APT29 linked to Russian Foreign Intelligence Service is targeting political parties in Germany. This shift in focus is significant because so far, embassies have been the main targets. Phishing emails are sent to political party representatives in order to compromise their systems with WineLoader malware, enabling hackers to gain remote access.

Microsoft is still handling the consequences of the cyber incident from January. The post published on 8 March indicates that the attack is more serious than originally thought and is still active. A hacker group is said to have also accessed Microsoft's source code repository, internal systems, and some e-mail exchanges between Microsoft and its clients, which is why some of the company's clients may also be under threat.

The French unemployment office France Travail announced in mid-March that it has fallen victim to a cyberattack and a resulting data theft in February. Up to 43 million people, which is more than two thirds of the population of France, may be impacted by the data theft. Names, social security numbers, and addresses have been leaked. The actual capacity and details of the attack are still being investigated and it is currently unknown if it was a ransomware attack.