FACTSHEET

Cyber security

"Cyber security is a field where the size of a country and its population have no importance. This is a field where Estonia clearly holds a leading role."

Kersti Kaljulaid, Former President of Estonia

Being a digital society means being exposed to cyber threats and staying aware of their existence. With solid investments in its cyber security infrastructure, Estonia has developed extensive expertise in this area, becoming one of the most recognized and valued international cyber security experts.

Ensuring cyber security has three main components: the architecture of the information systems, user awareness, and established rules with full compliance. In order to ensure information security to the providers of vital services, it is particularly important to adhere to both awareness and security requirements. Compliance is monitored by the Information System Authority (RIA).

Through numerous training programmes and media campaigns, the RIA ensures that everyone is aware of cyber security issues. Estonia guarantees cyber security above all via the architecture of the information systems and the proper training of the professionals responding to incidents.

Cyber attacks in 2007

In 2007, street riots connected to the relocation of a WW II memorial took place in Tallinn. At the same time, a coordinated campaign of cyber attacks against a number of Estonian government agencies, banks and media websites was unleashed. As a result of these DDoS attacks and web defacements, the display of Estonian internet sites experienced disruptions.

Due to the politically motivated riots in Tallinn, the cyber attacks are associated with the Russian Federation, although due to the difficulty of attribution in cyberspace, there is no direct evidence to support this claim. It was the first known large-scale cyber attack aimed at a single country. Estonia mitigated the attacks well, documented and analysed the data, and is now able to share its experiences.

Cooperative Cyber Defense Center of Excellence in Estonia

Because of Estonia's experience with the 2007 cyber attacks and their effective adoption of e-government solutions, the NATO Cooperative Cyber Defense Center of Excellence (NATO CCD COE) was founded in Tallinn in 2008.

The NATO CCD COE manages cyber security research and training. The heart of the Centre is a diverse group of experts — researchers, analysts, trainers and educators — from 20 nations. The mix of military, government and industry backgrounds means the NATO CCD COE provides a unique international 360-degree understand-ing of cyber defence. The Centre is staffed and financed by member nations and is not part of NATO's military command or force structure.

Cyber Range & Exercises

Several Estonian companies have created a vast suite of cyber ranges and exercises to train employees in all kinds of organisations to strengthen the cyber resilience.

To name one, CR14 (Cyber Range 14) was established by the Estonian Ministry of Defence on the 1st of January 2021 and is based on more than 10 years of military-grade cyber range experience in cybersecurity training, exercises, testing, validation and experimentation. CR14 is a government-owned and operated entity, which offers cybersecurity-related training and development for domestic and international; private and public sector partners:

- Estonian Cyber Range (Estonian Government and other public sector organisations)
- NATO Cyber Range (NATO member states)
- Open Cyber Range (companies, startups, the entire private sector; OCR will be also implemented on NATO innovation and startup programs)
- Classified Cyber Range

Questions & answers

How can we ensure the security of the users of e-services?

With the baseline national digital identity, which includes the national ID card and its additional tokens — mobile ID, residence card, digital ID, e-resident card. This ensures the uniformity of a person's identity on the internet, and allows for authentication and digital signing.

How is the overall cyber security of e-services ensured?

A distributed architecture of data management, where the data is maintained by the owners of the databases and X-road allows the secure exchange of information between databases and registries. The data cannot be duplicated and there is no central database, the communication between databases is encrypted and sessions leave traces with evidential value. Communication with and between state institutions takes place in a national communications network, which the Information System Authority (RIA) monitors around the clock.

For more information:
www.ria.ee/en | ccdcoe.org

Facts and figures

- → E-solutions and robust cyber security require a functioning infrastructure and organisational structures. If any link in the chain fails, there needs to be an alternative way to provide that service.
- → There have been 1.3 million ID cards issued in Estonia, 64%of which are used regularly.
- → There are over 3000 e-services available for use in the public and private sectors.
- → Estonia ranks as the 3rd most secure country on Global Cybersecurity Index (International Telecommunication Union (2020)
- → Estonia ranks 4th in the NCSI National Cyber Security Index EGA (2022)