SUMMARY OF THE ESTONIAN INFORMATION SYSTEM'S AUTHORITY ON ENSURING CYBER SECURITY IN 2012

Cyberspace is both an ecosystem consisting of an infrastructure and services, and an environment where and through which social relationships and processes similar to those in the common physical world unfold. Cyberspace is also part of the physical world: many processes and relationships can only exist with the help of information technology and occur in cyberspace such as digital communication, information processing, the storage of information, etc. A long time has passed since information technology was the sole the domain of engineers; rather it has become an intrinsic part of our daily lives. All technology users, from CEOs to schoolchildren, must also learn to address the risks and threats associated with IT and the cyber environment.

The level of development, scope and use of cyberspace, including society's reliance on it, different between countries. Estonia belongs to the group of highly cyber-dependent countries that consider ensuring cyber security a matter of national security and societal welfare. In order to protect the cyber environment, it is necessary to understand risks, recognise threats, and deal with any potential consequences.

RIA as a provider of cyber security

Estonia has actively addressed the question of cyber security on a national level since at least 2007, with the aim of ensuring the security and availability of national institutions and vital services at all times. The National Cyber Security Strategy developed in 2008 laid out a national action programme up to 2013. In 2011, the Estonian Information System's Authority (RIA) was established as Estonia's central cyber security competence and coordination centre, and the responsibility for cyber security policy coordination was handed over from the Ministry of Defence to the Ministry of Economic Affairs and Communications in the same year. On 21 March 2013, the Government approved a proposal according to which the Estonian cyber security strategy for 2014–2017 will be drawn up.

PRINCIPLES OF CYBERSECURITY IN ESTONIA:

- whole of nation (industry, individual users)
- government role as regulator who establishes societal expectations, rules
- PPP, close coopeeration

RIA's main cyber security tasks cover:

- Executing supervision over information systems used to provide vital services[1] and over the implementation of the security measures covering the information assets related to these systems;
- Organising activities related to the Estonian state siformation system and the

[1] Vital services and providers thereof are defined in section 34 of the Emergency Act.

information security of Estonian critical information infrastructure;
- Handling security incidents that occur in Estonian computer networks.

In 2012, RIA completed the manning of its cyber security function with specialists, ensuring the fundamental competence required for performing the main tasks of the Authority and handling the critical infrastructure incidents of the cooperation network. Presently, 22 people work in positions at RIA that are directly related to providing cyber security. RIA's recent priorities encompass assembling the necessary competence to ensure security, creating and developing cooperation networks, developing specific capabilities (e.g. SCADA/ICS security) and supporting providers of vital services and critical infrastructure administrators in ensuring cyber security.

2012 passed without major incidents

By law, public sector institutions and providers of vital services are required to report major information security incidents. RIA was alerted to several incidents during the year (the Department of Supervision registered 41 significant incidents), but none of these amounted to an emergency situation. In addition to continued operation interruption incidents (for example Elion interruptions, card payment system and air traffic control system malfunctions), media attention was also drawn to the so-called "#opEstonia" case, which did not impact the functioning of critical information systems and was addressed in the course of routine, although much more intensive, work. There were some criminal attacks that could be considered serious, as their goal was to obtain access to bank accounts by phising. The RIA Department for Handling Information Security Incidents (CERT-EE) usually deals with tens of cases every day, but the required action in handling the incidents is largely limited to user advice and taking on the role of a coordinator; RIA is rarely required to provide on-the-spot technical assistance.

Ensuring security through enhanced knowledge

Over the course of the year, we organised 5 seminars, 1 conference, 1 information day and 17 trainings for a total of 684 participants from the European Union Structural Funds programme "Enhancing knowledge of the information society". In addition, RIA held an international CERT-EE symposium in Tallinn on topics dealing with the handling of cyber incidents, in which 226 people participated, including 114 from outside Estonia. RIA also organised practical security training for IT specialists, implementing and auditing Estonia's baseline IT security guidelines (ISKE), risk management training for information security managers (CISO-s), and introductory trainings for common users were organised.
RIA participated as an authority or was represented by experts at national as well as international cyber exercises, that tested procedures for resolving civil and military cyber crises. These exercises also involved providers of vital services from the private sector.

Cyber crime

The level of cyber crime greatly influences public opinion on cyber security. Any crime

related to information technology or employing IT is notionally deemed to be a cyber crime. Generally, computer crime remained at the same level as in previous years. In 2012, the Estonian national police (the Investigation Department of the Central Criminal Police of the Police and Border Guard Board) opened Division V, whose primary duties include pre-trial procedures for serious IT-related crimes and serious covert crimes, as well as participation in the all-inclusive coordination of the area.

The Police and Border Guard Board assesses the major factors impacting police work in fighting cyber crime in 2012 as follows:

- Trojan wars (conflicts between virus producers from Russia and USA and China) for financial means continued. The wars have become more commercial.
- Cybercriminals continued to seek sales channels for stolen information.
- Developing fraud, which has continued to become a service and is being offered as a service.
- Disengaging cybercriminals from the net forced them to advance further (man-in-the-browser (MITB), i.e. attempt to steal information directly from a browser).
- Increase in hacking.
- Fast information exchange facilitated the apprehension of criminal groups and botnet operators (i.e. malware users that direct and coordinate attacks).
- Different teenage cyber abuse cases reached the scale of Child Grooming (a child is enticed to take naked pictures of himself/herself and then money is extorted with a threat that otherwise the pictures will be posted in e.g. Facebook).
- Apprehended distributors of child pornography consider their immoral activities as normal.

The Police and Border Guard Board considers these trends likely to continue in 2013.

Security measures and supervision

During the past year, RIA prepared and presented proposals to ministries for amending and changing regulations governing cyber security and its supervision, including proposals to change the Public Information Act, Emergency Act, Electronic Communications Act and State Secrets and Classified Information of Foreign States Act. RIA also prepared several implementing regulations that were adopted by the Government.

The most important changes worth highlighting concern a regulation enacting stricter information security measures for state authorities that comes into force in 2013 and requires all state authorities to appoint a senior information security official (CISO). This official will be responsible for information security and ensuring security requirements for electronic systems relevant for the functioning of vital services. This regulation took a significant amount of time to prepare. Of particular note is that private companies providing vital services have expressed their positive interest in clear regulations and requirements for security measures adopted at a government level. Such regulations would in their view add clarity their understanding society's expectations toward private companies and transparently enable them to carry social responsibility.

RIA's initial step in exercising its supervisory authority over the implementation of security measures in state authorities required us to assess our own situation. RIA was established based on the former Estonian Informatics Centre; therefore, RIA continues to provide IT-services to state authorities and organises the functioning of the national base infrastructure. Our self-assessment revealed several shortcomings in systems administered by RIA, which has helped in assessing similar shortcomings in other authorities. RIA next mapped and assessed the implementation of security measures and ISKE in state authorities. The situation is not completely satisfactory: four out of eleven ministries admit that there are deficiencies in the implementation of ISKE in their area of administration and that the application of these security measures is still in its initial stage.

Internet security of machines

The widespread use of automatic control systems, robotics and integrated smart technologies has increased the risks that a cyber attack could have direct kinetic effects that might in a worst-case scenario result in interruptions to vital services. RIA has reacted with further cyber security measures. The introduction of smart meters in Eesti Energia and the security problems of various remote and automatic control systems are among the instances that have motivated us to direct more resources into ensuring the security of the ICS/SCADA systems necessary for providing vital services. In 2012, RIA organised several penetration tests in cooperation with the providers of vital services during which the security of the information systems of vital services was tested. The resulting information enabled the companies to improve and change their security policies.

International cooperation

The successful implementation of cyber security requires effective daily international cooperation in handling incidents and developing security measures. In 2012, we enhanced our communication with state authorities and research institutions in the US, France, Germany and other countries. Cooperation with the BSI (*Bundesamt für Sicherheit in der Informationstechnik)* in Germany, from where the ISKE security framework used in the Estonian state authorities originates, and with Idaho National Laboratory in the US concerning the security of ICS/SCADA systems, merits mentioning. RIA representatives actively participated in the work of professional organisations and international working groups and contributed to the training of foreign partners.

Internal cooperation

RIA is active with the public and private sector through working parties and various commissions. The Critical Information Infrastructure Protection Commission, the CERT-EE network and monthly coordination meetings with other state authorities are worth mentioning here. RIA works actively with the Data Protection Inspectorate, Technical Surveillance Authority, Defence Forces and security authorities, as well as the Estonian Defence League's Cyber Unit.

Summary

2012 was a peaceful year in Estonian cyberspace and gave us time to plan our activities and learn from others. In 2013, the projects initiated by RIA must give us the technical awareness capabilities to detect risks to the state information system. Stricter supervision should help increase Estonia's overall readiness to tackle threats. Close cooperation with the private sector, especially with the providers of vital services and security companies, should enhance the competitiveness and sustainability of Estonian companies.

A secure cyberspace for all!

Toomas Vaks
Director of Cyber Security, RIA

In preparing this summary, data from the Estonian Information System's Authority and the Police and Border Guard Board were used.