Executive summary of the public audit report

THE CYBER SECURITY ENVIRONMENT IN LITHUANIA

9 December 2015, No. VA-P-90-4-16

Full audit report in Lithuanian is available on the website of the National Audit Office
: www.vkontrole.lt

DEFINITIONS AND ABBREVIATIONS

Definitions used[1]:

Electronic information: data, documents and information managed in an information system.

Electronic information security: ensuring the confidentiality (the electronic information can only be disclosed to authorised persons), integrity (the electronic information cannot be accidentally or unlawfully changed or destroyed) and accessibility (the electronic information can be managed when necessary) of electronic information.

Critical information infrastructure: an electronic communications network or part thereof, an information system or part thereof, a group of information systems or industrial process control systems or part thereof, irrespective of whether the proprietor of the information is a private or public administration entity, where an incident that occurs causes or may cause grave damage to national security, the national economy or social well-being.

Cyber space: an environment in which electronic information is created using individual computers or other information and communications devices and/or transferred through an electronic network to other connected computers or other information and communications devices.

Cyber incident: an event, act or omission which gives rise or may give rise to unauthorized access to an information system or electronic communications network, the disruption or change of the operation (including takeover of control) of an information system or electronic communications network, the destruction, damage, deletion or the change of electronic information, the removal or limiting of the possibility to use electronic information and which also gives rise or may give rise to the appropriation, publication, dissemination or any other use of non-public electronic information by persons unauthorized to do so.

Cyber security: the entirety of the legal, information dissemination, organisational and technical measures used to prevent, detect, analyse and react to cyber incidents, and to restore the regular operation of electronic communications networks, information systems, industrial process control systems if such an incident were to occur.

In this audit report, **cyber security** is viewed in a broader sense than in the Law on Cyber Security, and includes certain elements (security of electronic information, application, network, internet and other information infrastructure) covered by the standards of the International Organization for Standardization (ISO)[2] and the recommendations of the North Atlantic Treaty Organization's (NATO) Cooperative Cyber Defence Centre of Excellence[3].

[1] The terms used in this document are defined by the Law of the Republic of Lithuania on Cyber Security, 11/12/2014, No. XII-1428, Art. 2, the Law of the Republic of Lithuania on the Management of Public Information Resources, 15/12/2011, No. XI-1807, Art. 2. and Resolution No. 716 of the Lithuanian Government of 24/07/2013 approved in the Description of General Security Requirements for Electronic Information, p. 4.

[2] ISO/IEC 27032:2012 Information technology — Security techniques — Guidelines for cybersecurity.

[3] NATO Cooperative Cyber Defence Centre of Excellence National Cyber Security Framework Manual 2012.

Abbreviations:

CERT: National Electronic Communications Network and Information Security Incidents Investigation Service (Computer Emergency Response Team)

ES (EU): European Union.

IRD: Information Technology and Communications Department under the Ministry of the Interior.

IVPK: Information Society Development Committee under the Ministry of Transport and Communications.

KAM: Ministry of National Defence.

KSĮ: Law on Cyber Security.

KS taryba: Cyber Security Council.

LRS: Seimas of the Republic of Lithuania.

LRV: Government of the Republic of Lithuania.

NATO: North Atlantic Treaty Organization.

NKSC: National Cyber Security Centre.

PAGD: Fire and Rescue Department under the Ministry of the Interior.

PD: Police Department under the Ministry of the Interior.

RRT: Communications Regulatory Authority

SM: Ministry of Transport and Communications.

SVDPT: Secure State Data Communication Network

VDAI: State Data Protection Inspectorate

VIIV taryba: Council for the Management of Public Information Resources

VRM: Ministry of the Interior.

SUMMARY

In 2006, the Government of the Republic of Lithuania established[4] that the current regulation of electronic information security (cyber security) is insufficient, and thus resolved to draft a law on the security of electronic communications networks, approving the Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019 in 2011[5]. However, the programme is not being effectively implemented and the aforementioned law was never passed.

Up to 2015, development in the field of cyber security was based on legal acts that did not clearly define the institutions responsible for shaping and implementing cyber security policy, the duties and responsibilities of the parties involved in cyber security, or organisational and technical requirements for cyber security and measures for ensuring cyber security.

At the end of 2014, essential changes were made to cyber security regulation: the Law on Cyber Security[6] was passed, detailing how to set up, manage and control the national cyber security system and defining cyber security terms and other related concepts. Once the law came into effect (in 2015), the Ministry of National Defence was granted authorisation to shape cyber security policy as well as to set up, control and coordinate the implementation of this policy, and a National Cyber Security Centre [7] was established within the Cyber Security and Telecommunications Service under the Ministry of National Defence, along with a newly set-up Cyber Security Council[8].

From 2015, the Ministry of the Interior, which up to then had been the institution authorised to shape national policy in the area of electronic information security and cyber security, as well as to organise, coordinate and control its implementation[9], was authorised to shape policy in the field of public information resource security as much as it did not cover cyber security[10] and, along with the National Cyber Security Centre, Communications Regulatory Authority, State Data Protection Inspectorate and the Police Department, to implement cyber security policy within their respective remits[11].

Lithuanian cyber security is integrally linked to the EU Cybersecurity Strategy, the Commission's proposal for a directive concerning measures to ensure a high common level of network and information security across the Union[12] and the Digital Agenda for Europe, which is part of the

[4] Resolution No. 1211 of the Government of the Republic of Lithuania of 06/12/2006 approving the concept of the law of the Republic of Lithuania on the security of electronic communications networks and information.

[5] Resolution No. 796 of the Government of the Republic of Lithuania of 29/06/2011 approving the Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019.

[6] The Law of the Republic of Lithuania on Cyber Security , 11/12/2014. No. XII-1428.

[7] Order No. V-1321 of the Lithuanian Minister of National Defence of 29/12/2014 approving the provisions of the Cyber Security and Telecommunications Service under the Ministry of National Defence.

[8] Resolution No. 422 of the Government of the Republic of Lithuania of 23/04/2015 approving the Cyber Security Council and its regulations.

[9] Resolution No. 291 of the Government of the Republic of Lithuania of 14/03/2001 approving the regulations of the Ministry of the Interior, p. 8.6.

[10] Law of the Republic of Lithuania on the Management of Public Information Resources, 15/12/2011, No. XI-1807, (revised act, valid from 01/01/2015 with the latest amendment, passed with Law No. XII-1302 of 06/11/2014) Art. 5, p. 4.

[11] The Law of the Republic of Lithuania on Cyber Security , 11/12/2014. No. XII-1428., Art. 4, p. 2 and 3.

[12] Joint communication JOIN (2013) 1 final to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of the High Representative of the European Union for Foreign Affairs and

Europa 2020 strategy[13] and emphasises that all interested parties must make a joint effort to ensure the security and resilience of information and communications infrastructure, focusing on prevention, preparedness and information in order to develop effective and coordinated mechanisms for reacting to increasingly more complex cyber attacks and electronic crimes.

On a national scale, no exact data has been accumulated on the funds used for the implementation of cyber security and electronic information security measures. According to the assessment carried out by public auditors, over 20.9 million euros were spent on cyber security and electronic information security measures in 2011–2014, and in 2015–2020, a further 15.6 million euros from the national budget as well as EU funds and other sources of international funding are planned for this very same purpose.

The purpose of the audit was to assess whether cyber security is being ensured in Lithuania. In view of this goal, we assessed whether:

- an effective cyber security system has been set up;
- cyber security is ensured in public establishments.

During the audit, we analysed current regulation, strategic planning and management practices in the field of cyber security and electronic information security as well as the funds allocated and used in this area. We evaluated whether the cyber security and electronic information security objectives detailed in planning documents were achieved, how public establishments ensure cyber security, and whether technical and organisational measures for cyber security are being applied properly.

The audit was conducted in the Ministry of Interior and the Ministry of National Defence. We also collected data and information from the institutions operating under these ministries, other ministries, the State Chancellery, the Communications Regulatory Authority, State Data Protection Inspectorate, the State Security Department, board members of the Lithuanian Research and Education Network (LITNET), and the Information Society Development Committee under the Ministry of Transport and Communications. We also cooperated with the cyber security specialists of the INFOBALT association. During the auditing process, we carried out on-site investigations at eighteen establishments. We analysed international experience, best practices, scientific research and the information presented in public information measures related to the field being audited.

The audit covered the period from 2011 through to the first half of 2015. Data from earlier periods was used to analyse change.

We have determined that the issue of ensuring and increasing cyber security and resilience has not been effectively addressed at the national level. The focus has primarily been on reacting to and preventing incidents in cyber space, which means that traditional issues related to electronic information security (confidentiality, integrity, accessibility) have been neglected, and from 2015, not enough attention has been paid to development, legislation, improvement of organisational structure, etc. in this field.

In addition to this, the organisational and technical security measures that have been implemented in the public sector have simply not been sufficient. Public establishments do not

Security Policy of 07/02/2013 on the Cybersecurity Strategy of the European Union, and the proposal for a directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union COM(2013) 48 final.

[13] COM (2010) 245: Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe. P. 2.3.

pay enough attention to ensuring cyber security in their activity, and the recently passed Law on Cyber Security does not resolve all of the risks related to cyber security. This law will prove to be as effective as its accompanying legislation, the practical experience of the establishments that implement it and their ability to manage cyber security and electronic information security as well as to choose effective measures for ensuring that requirements are met and addressing issues related to the competence of specialists in the field. If these shortcomings are not dealt with, this could harm not only administrative and public services as well as information, but also every citizen, the country's reputation and confidence in new technology.

In order to improve the quality of cyber security regulation and to resolve existing planning and financing problems, we have proposed that the Government establish general strategic goals for cyber security and electronic information security as well as the measures necessary to implement them, and consolidate the management of electronic information security. An institution should also be selected for coordinating the development of and unifying requirements for this area and setting criteria and priorities for the allocation and use of funds.

To the Ministry of National Defence and the Ministry of the Interior, we have recommended reviewing and unifying existing requirements for cyber security and electronic information security, approving needed regulations and methodological documents and planning for measures for consulting and informing the entities that are responsible for ensuring cyber security and electronic information security about pertinent issues in the field.

The following public audit conclusions and recommendations were drawn upon the assessment of the audit findings.

CONCLUSIONS

1. In Lithuania, the areas of cyber security and electronic information security are governed by separate laws, however, implementing them is not an easy task, and the general public security level in these areas has so far not seen significant improvement because:

   1.1. The Programme for the Development of Electronic Information Security (Cyber Security) for 2011–2019, which was expected to achieve the most results in the field, is being implemented ineffectively (as of September 2015, the overall implementation of programme goals reached 21%). Not all of the links between cyber security and electronic information security planning documents have been addressed, and measures established in planning documents are not being implemented on time (subsection 1.1, pages 11-14);

   1.2. legal acts regulating cyber security have not been drafted on time, no solution has been found for the revision and harmonization of requirements for the area of cyber security and other areas related to information security (subsection 1.2, pages 15-17);

   1.3. the cyber security management system that took effect in 2015 has not created sustainable management conditions for the areas concerned: there are partial overlaps in the activity of public establishments, it is unclear which parts of forming and implementing cyber security and electronic information security policy fall within the purview of certain institutions (subsection 1.3, pages 18-19);

   1.4. the allocation and use of funds for cyber security and electronic information security (15.6 million euros planned for 2015–2020) is implemented without the Ministry of National Defence and the Ministry of the Interior setting priorities and criteria or having

data about the factual state of the cyber security and electronic information security in specific institutions, the funds that have already been used (20.9 million euros in 2011-2014) or their impact (subsection 1.4, pages 19-22).

2. The implementation of technical and organisational measures for cyber security and electronic information security in the public sector is insufficient, and establishments are not properly prepared to react to potential cyber threats because the audited institutions:

   2.1. apply, on average, only 25% of the recommended organisational measures for this area; the principal shortcomings are linked to creating security management systems, managing incidents, ensuring operational continuity, improving the competence of personnel and external collaboration;

   2.2. adequately implement only 39% of the recommended technical measures and continue to be vulnerable due to the inadequate setting of security configurations and management of electronic communications networks as well as mobile and other technologies (subsection 2, pages 23-26).

RECOMMENDATIONS

To the Government of the Republic of Lithuania:

1. In order to ensure cyber security and increase its resilience as well as to improve existing planning, legal regulation and financial management, the following actions should be taken:

   1.1. set general strategic goals for the field of cyber security and electronic information security and the measures necessary to achieve them (Conclusion 1.1);

   1.2. assign an establishment that would be responsible for coordinating the development of and unifying requirements for this area on a national scale (Conclusion 1.2);

   1.3. consolidate the management of electronic information security (conclusions 1.3 and 2);

   1.4. establish priorities, criteria and a monitoring and control mechanism for allocating and using funds for cyber security and electronic information security at the national level (Conclusion 1.4).

To the Ministry of National Defence and the Ministry of the Interior:

2. In order to improve the quality and effectiveness of cyber security regulation, reduce the administrative burden on establishments implementing these requirements or monitoring their implementation, the following actions should be taken:

   2.1. revise existing cyber security and electronic information security requirements, ensure their compatibility and/or approve missing regulations and methodological documents (conclusions 1.2 and 2);

   2.2. ensure that relevant establishments can receive consulting and information on issues related to cyber security and electronic information security (creating a management system, managing incidents, ensuring operational continuity, developing the competence of personnel, external collaboration, setting security configurations, network security, managing mobile technologies and other technologies), (Conclusion 2).

Measures and time frames for the implementation of the recommendations are presented in Annex 1.