NATIONAL CYBER SECURITY STATUS REPORT 2019

MINISTRY OF NATIONAL DEFENCE
OF THE REPUBLIC OF LITHUANIA

National Cyber Security Status Report

2019

MINISTRY OF NATIONAL DEFENCE
OF THE REPUBLIC OF LITHUANIA

To read more - click on a corresponding title

TABLE OF CONTENTS

GLOSSARY

Critical Information Infrastructure: a communication and information system, a part thereof, or a group of communication and information systems, in which the occurrence of a cyber incident may have a significant negative impact on the national security, the economy of the country, or state and public interests.

Critical service: a service the non-provision or disruption of which would have a significant adverse effect on national security, national economy, state or public interests.

Cyber Incident: an event or activity in cyberspace that may have a negative impact on the accessibility, authenticity, integrity and confidentiality of digital information transmitted or processed on communication and information systems.

Cyber security entity: an entity which controls and/or manages information resources of the state, for example, acting as an owner and/or manager of critical information infrastructure, provider of public communication networks and/or public electronic communication services, supplier of hosting and other digital services.

Communications and information system: a network of electronic communications, information system, registry, industrial process management system and digital information stored, processed, retrieved or transmitted for the purpose of management, use, protection and maintenance of those processes.

State information resources: the totality of information managed by the institutions in the exercise of their statutory functions, that is processed by means of information technology, and of information technology tools used to process information.

ABBREVIATIONS

Botnet – A network of computers or devices of Internet of Things that can execute distributed-denial-of-service cyber attacks

CII – Critical Information Infrastructure

CIS – Communication and Information System

CMS – Content Management System

DDoS – Distributed denial-of-service attack

EU – the European Union

ICT – Information and Communication Technologies

IoT – Devices of the Internet of Things, such as smart TVs, smartphones, etc.

MoD – Ministry of National Defence of the Republic of Lithuania

NCSC – National Cyber Security Centre under the Ministry of National Defence

OS – Operating system

SIR – State Information Resources

CCST – Core Center of State Telecommunications

SW – Software

TLD – Top-level domain name system (e.g. ending in ".lt")

EDVINAS KERZA

VICE-MINISTER OF NATIONAL DEFENCE

01

INTRODUCTION

Four years in a life cycle of a state do not seem like a lot but is actually a long period of time when it comes to cyber security of our country – particularly when we evaluate where we are standing now and where we want to be in the future. Thus, we are delighted to present the fourth Lithuanian National Cyber Security Report. This is the second year since the introduction of the National Cyber Security Strategy, which consists of five key objectives. The foundations of cyber security have been laid, key decisions have been made and today we can already review the results. In Lithuania, we consider 2019 as a year of growth. We have not only improved our capabilities in response to new threats, more sophisticated attacks and newer ways to execute them, but also developed as a country which is ready to take care of its own cyber security and contribute significantly to the security in the region. We have established the Regional Centre for Cyber Security, strengthened our partnership with the United States of America, and cooperation with our reliable partners – Ukraine and Sakartvelo – we will continue our work, research and keep learning.

During the implementation of the Cyber Rapid Response Group project initiated by the EU Permanent Structured Cooperation (PESCO) in 2019, an international Rapid Response Team was created and a monitoring function was established. That being said, Lithuania continues to contribute to and support NATO's cyber defence. One of the most important decisions made this year was to establish a Secure State Data Transmission Network, which means both greater resilience and security of the country. More importantly, we have already had an opportunity to test these decisions and new policies in practice.

We have not only thought about the most efficient ways to undertake cyber incident management, but have also expanded our research efforts. Some studies, such as those on *Yandex.Taxi* and *FaceApp* mobile applications and communication devices, are already known to the public, and the results are included in this report. In this way, we contribute to the security of of Lithuanian citizens and also share information with partners in other countries. In cooperation with the team of *Create Lithuania*, we have started developing a cyber security guide for small and medium-sized enterprises.

This year, special attention was paid to new hybrid threats, disinformation campaigns and security of elections. This required concentrated efforts of the Strategic Communication Department of the Lithuanian Armed Forces and the National Cyber Security Centre. Although the nature and scale of these threats grew in 2019, we became even stronger at deterring these new challenges. This report is a detailed picture of cyber security status in Lithuania and illustrates why and how 2019 was a year of major decisions that strengthened our cyber security. The report also aims to show that cyber threats are critical not only to the state institutions and businesses, but also to every citizen of Lithuania. The National Cyber Security Centre under the Ministry of National Defence will continue to actively develop its capabilities and responsibilities in a way that will ensure the security of critical services, increasing citizens' awareness and building a safer Lithuania. And if this report inspires at least one person to take care of cyber security in her or his own immediate environment, the cyber space of Lithuania as well as the entire Europe will become more secure.

Edvinas Kerza
Vice-Minister of National Defence

02

SUMMARY

SUMMARY

In 2019, the cyber security environment in Lithuania and the world remained dynamic. Cyber incidents and information attacks have always been in the focus of the media as well as specialised cyber security forums and expert blogs. In 2019, Lithuania was actively engaged in international cooperation, establishing the Regional Cyber Security Centre as a platform for international and operational cyber security cooperation. Several important milestones were achieved: cooperation agreements with Sakartvelo and Ukraine were signed, financial support for a new generation sensor project was received from the United States and further discussions on the development of the Regional Cyber Security Centre were held.

Lithuanian cyber security specialists actively participated in cyber security exercises. The representatives of the National Cyber Security Centre (hereinafter – the NCSC) took the second place in the *Cyber Shield 2019* exercise at the end of 2019. Over 800 professionals from more than 100 public and private sector organisations took part in the event. New cyber security research was carried out on mobile applications and network routers available in the Lithuanian market. The research indicated that users' personal data from devices and gadgets is often sent to third countries where the European Union's General Data Protection Regulation does not apply. Moreover, software could gain access to excess data, services and information, which is not usually necessary for the software's functionality.

The NCSC took preventive actions to ensure cyber security during Lithuania's parliamentary and presidential elections: established a temporary centre of operations, which registered and blocked over 900 malicious IP addresses.

Lithuania's increasing cyber defence capabilities and maturity have also led to a better identification of cyber threats. In 2019, 3 241 cyber incidents that required direct involvement of professionals were identified in Lithuania. In order to harmonize cyber classification among different international and national partners of Lithuania, a new classification has been introduced, which separates cyber incidents from cyber events. In terms of incident types, the number of service disruption incidents and malware detected by technical means (sensors) in the infrastructure of critical service providers has decreased (by 12% compared to 2018). However, the amount of malicious software detected in the national defence sector has increased (49%). Meanwhile, the energy sector is showing a decreasing trend in malware. A significant incident was also registered in 2019 when malicious data encrypting code was detected in the information systems of *UAB Kauno vandenys*. As a result, there was a risk that the water supply provided by the operational technology network in Kaunas would be affected. The cyber incident was contained, but this situation is worrying because the entities controlling technological networks remain attractive targets for cyber attacks. A detailed classification of cyber incidents, information on Lithuanian IP cyber events and malware trends suggest that the impact and scale of cyber incidents in Lithuania is still underestimated.

Another major cyber security issue remains to be vulnerable websites. The results of web scanning activities have revealed that 56 400 of 118 00 websites with top level ".lt" had content management systems. The analysis has shown that 62% of them use outdated content management system software whose vulnerabilities have been already published and thus available for further exploitation. In addition, 37% of all websites have an open control panel access; therefore, adversaries can attempt to break in by automatically generated logins and passwords. Nevertheless, a positive trend in the public sector has been identified – the number of secure governmental websites increased by 11%. However, some websites are still not validated as information systems. Moreover, they are lacking responsible information security officers and are still not sufficiently addressed by site administrators in terms of cyber security. Statistically, the websites of municipal authorities, ministries and their subordinate bodies remain the most vulnerable ones in the public sector. While it can be claimed that the cyber security status of websites in the public sector is, in fact, improving, but the overall risks to these websites remain significant. To address these common website security issues, the NCSC published a free website vulnerability detection tool[1], which has been successfully used by more than 120 entities last year. In 2019, significant progress was made in the implementation of cyber security requirements. It was noted that 80% of cyber security requirements specified in the laws of Lithuania had been implemented by critical information infrastructure owners. Additionally, the NCSC has started to perform on site audits and penetration tests. These practices allowed to identify organizational and technical deficiencies and define specific actions to be taken in order to address the risks. From the administrative perspective, entities have a tendency to formally implement requirements without paying sufficient attention to practical solutions on cyber security issues. Compliance discrepancies continue to be encountered in the public sector (self-declared implementation of national cyber security requirements in this sector accounted for 22% in 2019). This issue should be partially addressed by the so-called centralised cyber security "umbrella" – a secure infrastructure provided by the Core Centre of State Telecommunications for over 400 public sector organisations.

In 2019, there was an increase in hybrid incidents, which consisted of cyber and information elements, aimed at hacking, distribution of malicious software and fake news. According to the Strategic Communication Department of the Lithuanian Armed Forces, a total of 2 890 cases of disinformation campaigns against Lithuania were identified in 2019, a quarter of them aiming at the Lithuanian constitutional foundations. The number of such harmful activities increased by 15% over the last year. Over the recent years, the media which is biased against Lithuania mainly targeted Lithuanian statehood, independence and democracy institutes.

[1] https://site-check.cert.lt/

Back to contents

03

INCREASING CYBER SECURITY RESILIENCE

Creating cyber security environment

After significant organisational changes in 2018 and legislative changes in 2019, cyber security in Lithuania has been strengthened and developed even further through the implementation of the Law on Cyber Security and various other governmental and non-governmental initiatives in the field of cyber security. As part of its cyber security policy, the Lithuanian MoD has developed a number of significant cyber security legal acts aimed at strengthening the overall cyber security ecosystem and helping to protect against cyber threats.

In 2019, to ensure implementation of the objectives set in the National Cyber Security Strategy, the MoD prepared a 3-year Institutional Action Plan (hereinafter – the Plan) to implement the National Cyber Security Strategy. Measures were determined for the implementation of the goals of the Strategy, appropriations to be allocated for those goals were specified, indicators which evaluate the fulfilment of measures, goals and tasks during the relevant period were created. Although most of the planned measures are implemented by the coordinator of the Plan – the MoD and its subordinate units – other ministries, various state institutions, agencies and their subordinate institutions are contributing with their own knowledge and competence. It is expected that the public sector interest, adequate allocation of funds, a clear role of responsibility and a continuous monitoring of the implementation and evaluation of the Plan will allow to successfully achieve the objectives of the Strategy.

In 2019, legal acts necessary for the implementation of the Law on the Management of State Information Resources, enabling the operation of the Secure State Data Communication Network (hereinafter – Secure Network) were passed to provide secure electronic communications services to the network users and to determine technical requirements that must be observed during the establishment and operation of state data centres.

Following technical requirements of the National Data Centres, approved by order of the Minister of National Defence of 18 November 2019, a list of premises regarded as national data centres will be drawn up and approved in 2020.

As of 2019, in order to ensure the management of the Secure Network, on 1 July 2019 the state enterprise Infostruktūra was transformed into the budgetary institution Core Center of State Telecommunications, which is entrusted with implementation of new functions that are vital to the state. The Secure Network is independent of any public communication networks and can operate in times of crisis or war. Lithuanian institutions included in the list of users of the Secure Network must use the Secure Network as the only provider of electronic communications services and as the only means for institutions to connect to public electronic communications networks. Currently, 463 state and municipal institutions, state enterprises and public institutions that meet at least one of the criteria specified in Article 432 (2) of the Law on State Information Resource Management of the Republic of Lithuania are included in the list of users.

The MoD is also responsible for drafting and periodic updates the list of Critical Information Infrastructures and their owners. Experts in the state institutions and other individuals responsible for identification of Critical Information Infrastructures were introduced to the key changes to the Critical Information Infrastructure Identification Methodology (hereinafter – the Methodology), which were enforced in the beginning of 2019. According to the requirements of the updated Methodology, in 2019 responsible authorities collected and analysed features and criticalities of multiple objects and organisations; in the end, they prepared a new list of Lithuania's most Critical Information Infrastructures.

In 2019, the MoD continued its initiatives in the field of cyber security with a special focus on public-private and international cooperation, and effective implementation of various EU recommendations.

In order to strengthen public-private cooperation on cyber security in Lithuania and provide an opportunity for the citizens to cooperate in the identification and elimination of security vulnerabilities by working together with the cyber security entities whose ICT security vulnerabilities were identified, the analysis of responsible practices in the identification of ICT security vulnerabilities was conducted in 2019. Proposals were also submitted for necessary legislative changes.

In order to create broader opportunities for international cooperation in the field of cyber security, the experts of Lithuania's MoD actively participated in various international meetings and working groups, increased bilateral cooperation with competent cyber security authorities of Sakartvelo and Ukraine, and strengthened close cooperation with the United States. In 2019, work began on the establishment of the Regional Cyber Security Centre as an international operational platform for cyber security. During the same year, cooperation agreements were signed with Sakartvelo and Ukraine, the US financial support for the next generation sensor project of the NCSC was received, discussions on further US support for the development of the Regional Cyber Security Centre's infrastructure continued and coordination commenced with the above countries regarding proposals on operational priorities of the Regional Cyber Security Centre for 2020–2021. In 2021, as planned, the Regional Cyber Security Centre should conduct joint research projects, organise cyber security exercises and proceed to identify and share valuable information on the latest cyber threats.

In 2019, the MoD continued to successfully lead the EU's Permanent Structured Cooperation (hereinafter – PESCO) project "Cyber Rapid Response Groups and Mutual Assistance in Cyber Security" (hereinafter – the Project). One of the most important achievements of 2019 was a completion of the preparatory phase for the signing of the Project's Memorandum of Understanding. The Project's Management Rules and the Methodology were prepared, development of cyber rapid response group operating procedures was tested during the Amber Mist 2019 cyber security exercise, activities funded in accordance with the CEF Telecom Grant Agreement were carried out, and actions of the participating Member States and private sector were coordinated in order to receive funding from the European Defence Fund.

During the implementation of the European Commission's Recommendation on a set of practical actions and measures to ensure a high level of cyber security for 5G networks across the EU, on 26 June 2019 the MoD developed a national report on the assessment of 5G infrastructure and its risks. The report describes the main threats and their sources, identifies subjects that are most vulnerable to threats, analyses the strategic aspects of the threat landscape and overviews potential vulnerabilities. On 15 July 2019, this assessment report was approved by the National Security Commission of the Government of the Republic of Lithuania. On 17 July 2019, the MoD presented the reports to the European Commission and the European Union Agency for Cyber Security (hereinafter - ENISA). With the support of the European Commission and in cooperation with ENISA, Lithuania carried out a broader risk assessment of digital ecosystem and 5G communication technologies. On 9 October 2019, the EU countries in cooperation with the European Commission and ENISA published a joint EU risk report on the use of 5G networks. It is based on the national cyber security risk assessments of all EU Member States. While cooperating with the European Commission, Lithuania will have to assess the impact of the EU recommendations before 1 October 2020, in order to determine whether further actions are necessary.

In 2019, actions were taken to provide resources needed for the development of the state's cyber defence capabilities, and relevant documentation was prepared in order to establish responsibilities and functions of the MoD-related institutions in the development of the state's cyber defence capabilities. In order to ensure interoperability of the Lithuanian Armed Forces (hereinafter – the LAF) with civilian institutions, a part of military personnel of the LAF was integrated into the National Cyber Security Centre in order to share their knowledge and experience in ensuring cyber security in the information systems managed by national defence system during peace and war.

Increasing resilience to cyber threats

In order to ensure cyber security of 2019 municipal, presidential and the European Parliament's elections in Lithuania, the NCSC was actively involved and cooperated with the Central Electoral Commission of the Republic of Lithuania and its contractors, responsible for the Central Electoral Commission Information system (hereinafter – the CECIS) hosting and maintenance, identifying risks and implementing proportionate measures. For a proactive response to cyber incidents in the context of the aforementioned elections in 2019, the NCSC set up a special operations centre and established an active relationship with organisations in other countries to ensure timely international response to any potential cyber incidents. The activities of the operations centre were based on the risks identified by the NCSC, which involved management of the CECIS cyber risks with regards to confidentiality, authenticity, integrity and availability (Fig. 1).

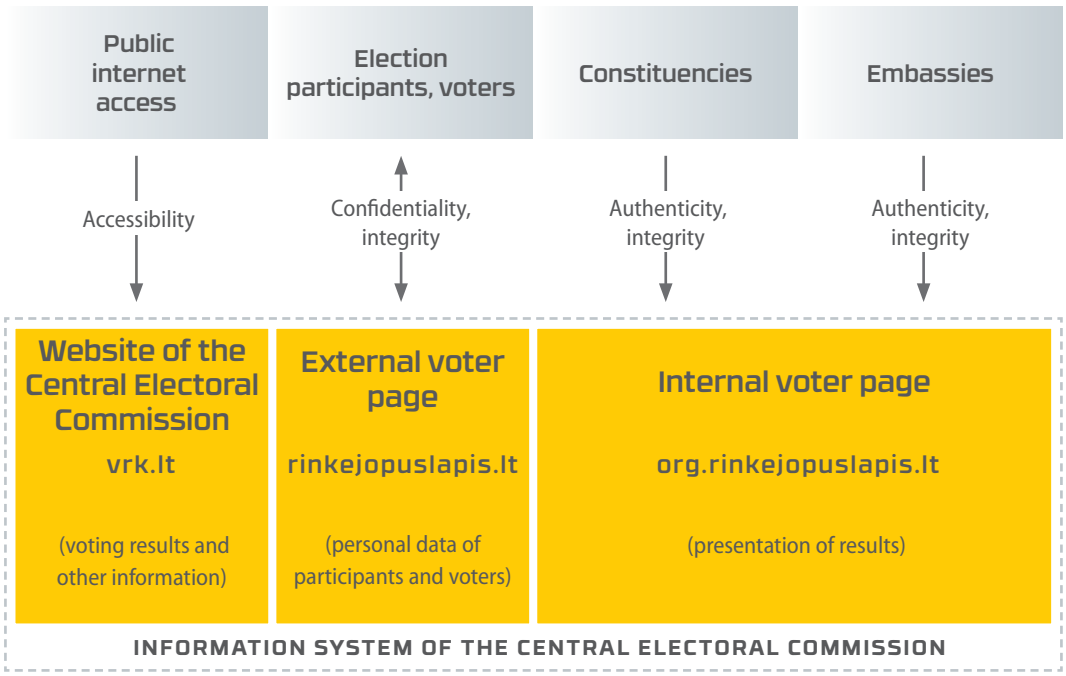

Fig. 1. Simplified risk management priority model for CECIS.

Additionally, during the election period, the NCSC continuously monitored accessibility of voter websites and its content integrity. During the work of the operations centre, the NCSC specialists blocked IP addresses that were suspicious – most IP addresses were already identified during the European Parliament's and the presidential elections, in total accounting for more than 900 IP addresses (Fig. 2).

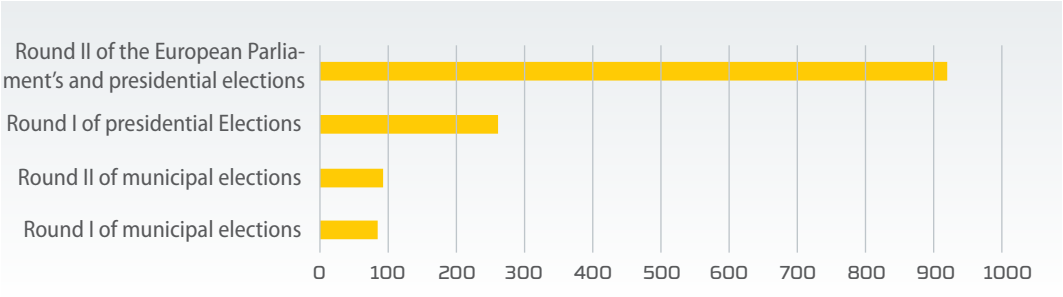

Fig. 2. IP addresses blocked during the elections in 2019.

Having observed that the servers of election commission members are not centrally managed and supervised, the NCSC concluded that, due to this, the integrity of election results can be affected or the possibility to communicate election results in a timely manner can be disrupted. For this reason, the specialists of the NCSC Innovation and Training Division prepared an operating system KAMOS-VRKS, which is specifically designed for elections. The operating model of this operating system is as follows: an OS is run from a CD with minimum drivers and software installed. Additionally, the NCSC carried out educational activities – conducted training for election workers and the representatives of political parties.

In order to further strengthen the capabilities of cyber defence in 2019, participation was increased in international cyber security exercises. *Locked Shields 2019* was one of the biggest international exercises. It was mainly focused on cooperation between experts and decision-makers, while the technical level was integrated into one strategic level. *The Blue OLEx 2019* exercise was mainly focused on cooperation between the EU institutions and the Member States in managing cyber security crises at the operational level. The international cyber security exercise *Amber Mist 2019* organised by the Lithuanian Armed Forces was intended for defensive cyber operations: assessment of hostile acts in cyberspace, identification of cyber threats, prevention of potential cyber attacks and elimination of their possible effects. Participants of this exercise were public and private sector organisations, allies and partners of the Lithuanian Armed Forces and NATO and the Cyber Rapid Response Force team, which is developed by the Lithuania-initiated EU Permanent Structured Cooperation (PESCO) project. The team, which is supervised by Lithuania, will begin its rotation on 1 January 2020. The international exercise *Cyber Shield 2019*, held at the end of the year, was aimed at strengthening cooperation among countries and response to the most common cyber incidents in critical information infrastructure, governmental institutions and public organisations – in this exercise, the specialists of the NCSC took the second place[2].

More than 800 professionals from over 100 public and private sector organisations participated in the biggest national exercise organised in Lithuania – *Cyber Shield 2019* – which was held at the end of 2019. The exercise was based on the model of NATO's cyber defence exercise *Cyber Coalition 2019*, i.e. under real-world conditions, using all available technical capacities, personnel and procedures, entities attempted to mitigate cyber incidents in their organisations and tested internal cyber incident management plans as well as the ability of personnel to detect, manage and analyse cyber incidents. The majority of the participants (90 %) said that the exercise was useful as they had an opportunity to check the internal procedures and gain new knowledge and expertise on cyber threats. The NCSC plans to further develop the exercise's concept under this model, invite increasingly different organisations and differentiate exercise scenarios by sectors.

[2] https://www.nksc.lt/naujienos/lietuviai_lipo_ant_pakilos_tarptautinesecyber_shie.html

Moment of cyber security exercise "Amber Mist". Photo by the Ministry of National Defence.

In 2019, the NCSC successfully implemented the telecommunication sector project "Tools and Capacity Building for the Improvement of Cyberspace Monitoring, Analysis and Threat Detection in Lithuania and the EU" co-financed by the Connecting Europe Facility (CEF). The aim of the project is to strengthen the capacity of the NCSC to effectively coordinate and manage cyber incidents and threats, enhance staff competences, ensure closer international and national cooperation and exchange information on threats.

Part of the project consisted of high-level international refresher training for the specialists of the NCSC. The project increased Lithuania's level of preparedness for cyber incidents, initiated the emergence of new security measures, enabled provision of wider and more effective cyber security services at the national level and made it possible to participate in joint European cooperation programmes and information exchange platforms.

During the project, according to the NCSC know-how, a platform was created for visualisation of the infrastructure of public internet networks, monitoring of access to infrastructure elements and detection of threats. The platform is based on data collected from public sources using routing (BGP) and other related network protocols. The system is based on the Lithuanian model but can be adapted by other countries and is available free of charge to all EU national CERT units. In this way, security professionals can monitor the topology of their publicly accessible national network and related security events.

During the project, special equipment for security assessment and malicious code analysis was acquired. A specialised malware code analysis system evaluates files and websites, detects various types of attacks and is also able to analyse the network traffic and the downloaded or created files. Using this tool,

a continuous check of all Lithuanian web pages that are registered with top-level ".lt" domain is carried out, and the providers of hosting services for these websites are notified if any malicious activity is found. Each month, the tool analyses more than 100 000 websites in Lithuania.

The incident management platform, which is widely used worldwide by cyber security teams, is another system acquired during the project. The platform facilitates standard incident processing processes, shortens their processing time and significantly increases the overall effectiveness of incident management. For this reason, the NCSC specialists may spend more time on preventive work, extensive analysis of sophisticated incidents and threat hunting.

Another new service for the Lithuanian public developed during the project was a tool that is designed to assess the security of websites. The tool is publicly available, and its users can check their own websites for known vulnerabilities[3]. Following an automated security audit, a website manager receives a report on specific problems and recommendations on how to improve the security status of one's own website.

One more new element is the central monitoring environment. It is a technical solution (a video screen), which allows system monitoring in real time. The system is used in the daily work of analysts and has been extremely useful during elections of recent years when threat indicators sent from many different systems had to be monitored in one place.

Funding from the European Union also made it possible to acquire high-level competence development services for the NCSC staff. During the training appreciated by security experts worldwide, the staff had the opportunity to deepen their knowledge and skills in different areas of cyber security. This allowed them to expand their competences and capabilities, in addition to creating the conditions for more competent and deeper investigations of cyber security incidents, ensuring higher level of preparedness and increasing cyber security resilience at the national level.

[3] https://site-check.cert.lt/

04

THE BIGGEST CYBER SECURITY CHALLENGES IN 2019

Statistics of cyber incidents

- In 2019, the NCSC registered 3 241 cyber incidents – three times more compared to 2018.
- Cyber incidents in Lithuanian IP range are mostly related to cyber threats of communication and information systems and malware (Table 2).
- Users and organisations are still unable to assess or do not assess the real impact of cyber incidents.

Having considered the list of criteria for cyber incidents as amended by the Law of the Republic of Lithuania on Cyber Security, as well as the increasing need to synchronise cyber incident classification with the EU Cyber Security Agency and other cyber incident management teams from partner countries, the NCSC has changed its methodology for identification of identifying cyber incidents and has made it compatible with common EU practices.

According to the Lithuanian Law on Cyber Security, a cyber incident is described as an event or act which may or already has a negative impact on communication and information systems and/or transmission of information. By early 2019, cyber incidents were counted based on both the number of processed automated notifications and cyber incidents that had to be handled manually by specialists. The National Cyber Incident Management Plan classifies incidents not only by their attributes but also by their potential impact.

Considering the increasing need to classify incidents by their impact, from 2019 it was nationally agreed to treat cyber incidents as the ones that require manual evaluation of the NCSC specialists. In the process, the impact of each cyber incident has to be evaluated and thus assigned to the appropriate incident category (Fig. 3). From now on, cyber activities which are processed by automated means and programs are separated and treated as cyber events.

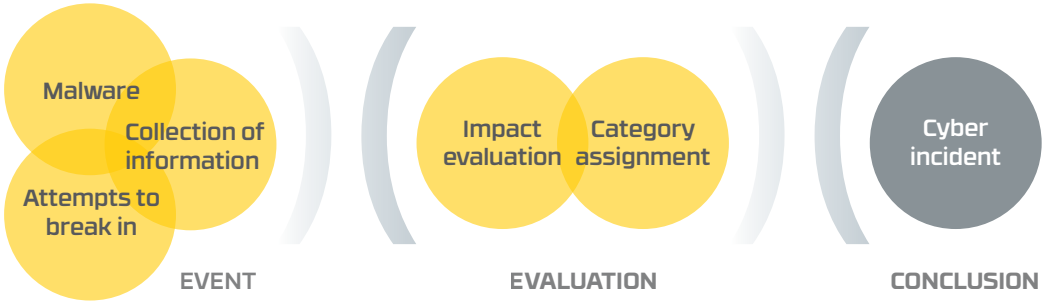

Fig. 3. Cyber incident evaluation process.

According to the updated cyber incidents classification, the NCSC identified a total of 3 241 cyber incidents. Having evaluated the information on investigations of cyber crimes from the Police Department under the Ministry of the Interior, it was also recognised that institutions and organisations are still reluctant to inform the responsible agencies and report a cyber crime. According to the data from the Information Technology and Communications Department under the Ministry of the Interior, only 439 crimes related to cybers pace were recorded in 2019.[4] For this reason, it can be assumed that most attention in Lithuania is paid to prevention of cyber incidents, whereas the responsibility for malicious activities is difficult to enforce from a legal point of view.

Other information, which was processed automatically, but was not classified as a cyber incident according to its impact, was treated as a cyber event. This information mainly concerns Lithuanian IP addresses belonging to both citizens and legal entities suspected of being used in malicious activities (Table 1).[5]

Type	Quantity
Cyber threats to communication and information systems	199 828
Malware	68 562
Information gathering	37 363
Attempted hackings	2 987
CIS disruption (DoS)	355

Table 1. Cyber events related to Lithuanian IP addresses.

[4] https://www.ird.lt/lt/paslaugos/tvarkomu-valdomu-registru-ir-informaciniu-sistemu-paslaugos/nusikalstamu-veiku-ziny-binio-registro-nvzr-atviri-duomenys-paslaugos/ataskaitos-1/nusikalstamumo-ir-ikiteisminiu-tyrimu-statistika-1/view_item_datasource?id=8166&datasource=40853

[5] You can check if IP is being used in malicious activities at https://www.nksc.lt/irankiai.html

The most prominent cyber events detected in 2019 included *Azorult, Pykspa* and *Conficker* (Fig. 4), which were among the top ten examples of malware found in the Lithuania. These types of malware involved taking control of user servers and stealing user information. *Azorult*, for example, is known for thefts of login and payment card data. [6]

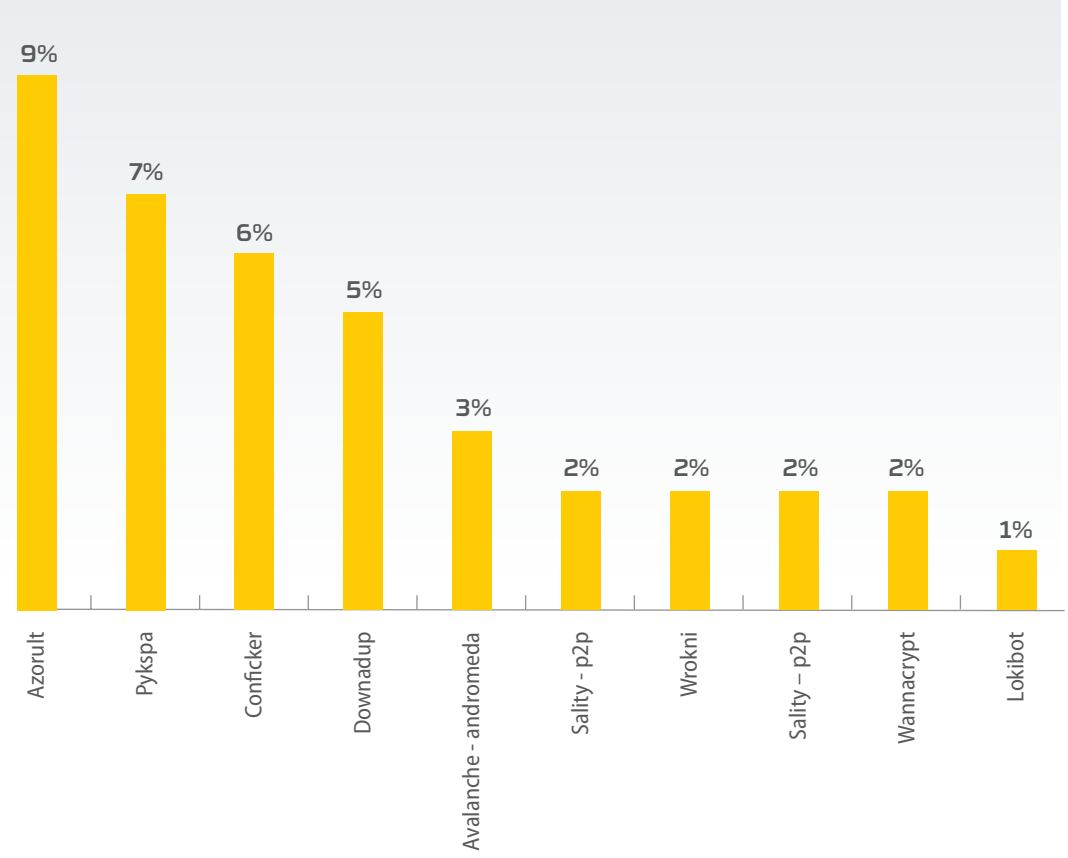

Fig. 4 Ten most widespread malware associated with Lithuanian IP addresses.

The NCSC points out that the majority of antivirus software, including freeware (as long as they are periodically updated), are able to easily detect common malware. The NCSC also periodically provides recommendations on additional methods and measures of protection.[7]

Upon assessment of information collected from third parties on CIS threats in the Lithuanian IP range, it turned out that the most popular ones were open ports. For example, data transmitted using *http* port could be easily taken over. The information provided by the NCSC partners also reveals that the use of outdated website authentication certificates is a particularly common threat in Lithuania. Such CIS threats create opportunities for hackers to carry out man-in-the middle cyber attacks by interfering to the CIS sessions.

[6] https://success.trendmicro.com/solution/000146108-AZORULT-Malware-Information

[7] https://www.nksc.lt/rekomendacijos.html

The increasing popularity of IoT highlights the risks of remotely controlled devices. Such devices often also have unencrypted remote access that adversaries can find effortlessly by using freely available tools.[8] These risks are also indirectly reflected in cyber threat statistics (e.g. *open-rdp, open-telnet*) (Fig. 5).

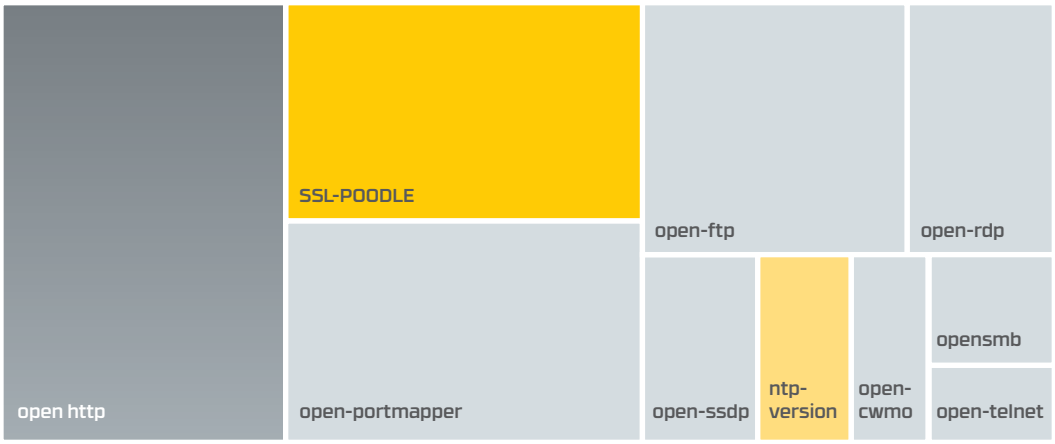

Fig. 5 The most popular cyber threats to the CIS in Lithuanian IP range.

Having reviewed the statistics of cyber incidents and events, it could be concluded that the users' cyber security awareness should be improved – for example, the most widespread malware can be detected with free antivirus software, as long as it is used properly. Furthermore, it is still difficult for different entities to assess the damage caused by the incidents. According to the official information from the State Data Protection Inspectorate and the Police Department under the Ministry of the Interior, few entities apply for retaliation against attackers.

[8] https://www.shodan.io

Proliferation of malware

- **The number of malware detected by sensors among the institutions which provide critical services was highest in the CIS of the national defence sector (49%).**
- **A declining number of malware was detected in the energy sector.**

In the context of advanced persistent threat (APT) groups, malware remains a major cyber threat. These groups are mainly linked to state actors and are politically motivated. Considering global activities of APT groups, those with close ties to governments of countries that share values different from the Western ones are most likely to be known to the cyber community. APT groups are able to use and constantly change different attack vectors during a cyber campaign. However, the key features unifying all APT groups are the precise targeting, trace hiding and the use of wide array of vulnerabilities and malware. It is increasingly apparent that APT methods are also used by criminal groups whose motives are not linked to the state actors. This trend is also indirectly linked to the increasing availability of malware. For example – the increase of malware as a service (Fig. 6). The ability to effectively exploit vulnerabilities and modify and use malware is becoming an opportunity for criminals to make profit.

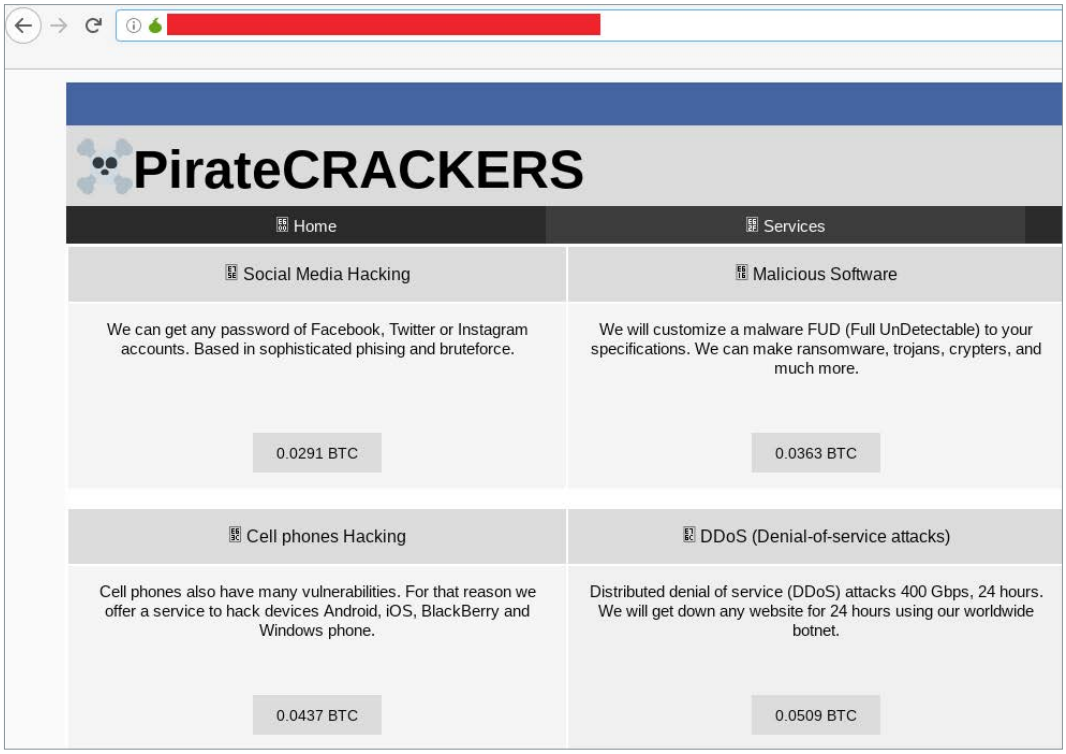

Fig. 6. Services offered by criminals on the Dark Net.

In 2019, the NCSC recorded and manually handled (with direct involvement of a specialist) 971 cases of cyber incidents that were directly related to malware. These cyber incidents have been identified through reports from cyber security entities or the use of the NCSC's technical cyber security tools (sensors) specifically tailored for this activity. Sensors are able to detect malware by using continuously updated indicators of compromise and allow entities and NCSC to block it source.

The NCSC identified a total of 413 cyber incidents related to malware (In 2018, the NCSC recorded 470 of such cases) in the CIS of critical service entities. The majority of them were registered in the national defence (49%), public administration (13%), as well as foreign affairs and security policy (12%) sectors (Fig. 7). Such statistics in the national defence sector was achieved by the increased number of the NCSC specialists working in this field, their high level of competence and the use of additional cyber security tools allowed the CERT specialists to identify cyber incidents in more detailed manner than before.

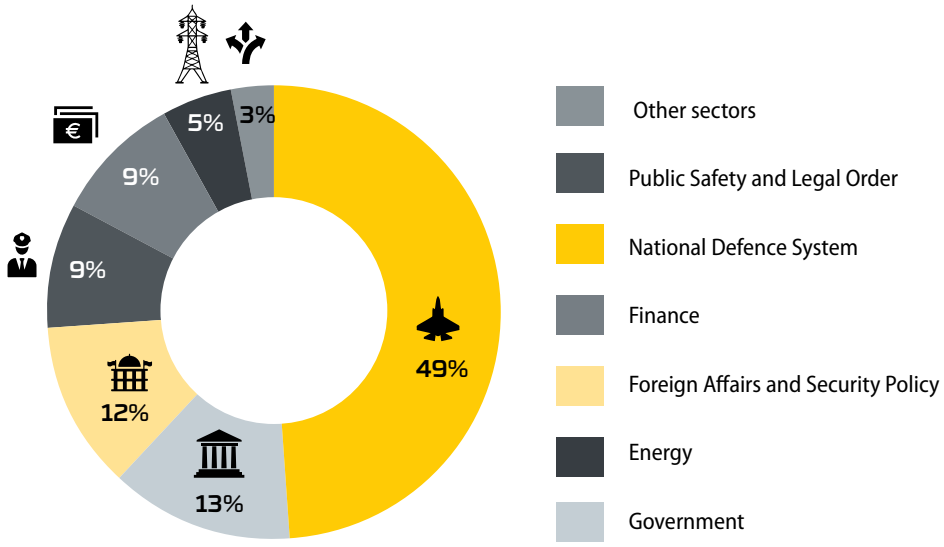

Fig. 7. Information on malware according to the critical service sectors gathered by cyber security entities and the NCSC using technical cyber security monitoring tool.

In the other cyber security entities, the CIS of the NCSC sensors have detected 558 malware communications, as well as various preventive measures taken by the entities themselves, such as properly configured firewalls and deployment of intrusion detection or prevention systems. However, cyber incidents are becoming increasingly difficult to detect using standard tools based on rules and threat indicators. For example, a type of malware may encrypt communications, making it more difficult to detect them. For this reason, sophisticated cyber incident management requires constant threat monitoring, especially that of advanced persistent threats.

Although the value of cryptocurrencies fluctuates, their generation at the expense of other Internet users resources is still prevalent when malicious websites and botnet networks are used.

Due to the increasing availability and wider use of malware, it can be claimed that the threat, from information security perspective, is relevant to national security, business and citizens. (Table 2).

CYBER SECURITY THREAT	IMPACT ON		
	National security	Business and SIR	Residents
Proliferation of malware	✓	✓	✓

Table 2. Impact of malware threat.

Significant cyber incidents

- **Entities that manage operation technology networks in Lithuania often become targets of cyber attacks.**
- **Incidents, which consisted of cyber and disinformation campaigns, continued to be recorded.**

In 2019 a cyber attack on information systems of *UAB Kauno vandenys* was a significant incident in Lithuania. *UAB Kauno vandenys* is a water supplier based in the second largest city of Lithuania, Kaunas. During the incident, malware encrypted data in the administrative network and cloud infrastructure. It is important to note that water supply was not disrupted. Entities performing technological processes often enable VPN access through logical separation from the administrative to the technological network, thereby creating a potential cyber attack vector for specific critical services. VPN access is just one of the ways the operation technology network can be accessed from the administrative network. For this reason, it is necessary to isolate the technological processes as much as possible and to physically separate and protect the systems. The cyber attack vector of *UAB Kauno vandenys* was via internet accessible open-rdp port (Fig. 8). It is likely that a failure to manage this cyber incident in a timely manner could have affected water supply in Kaunas.

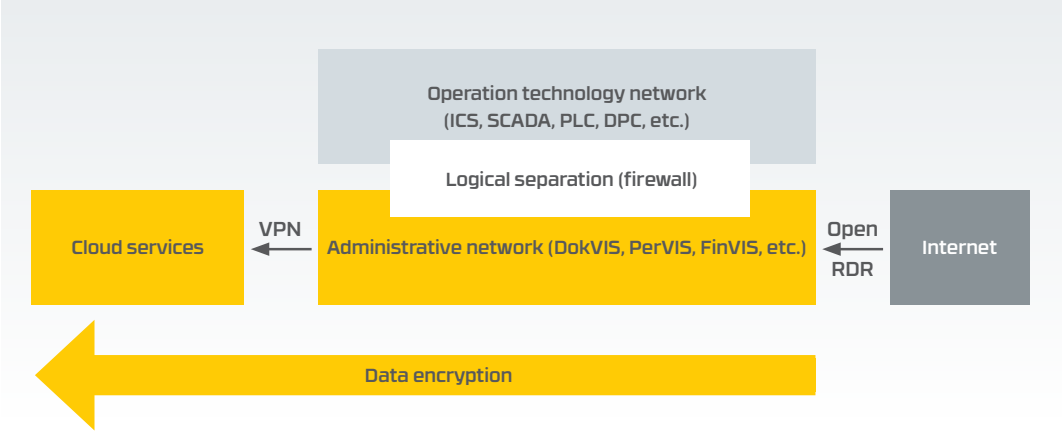

Fig. 8. A hypothetical example of data encryption during a cyber incident against an organisation, providing services within operation technology network.

Another notable cyber incident in 2019 was a cyber and information attack using news media website *kaunas.kasvyksta.lt*. The specifics of this cyber attack were identical to the one carried out on *tv3.lt* website in 2018. The initial phase of the attack was hacking into a website and creation of a backdoor connection. The original attack vector could not be identified since the affected entity failed to provide detailed log records. Having gained the access to the website, a hacker posted fake news entry and sent spoofed targeted e-mails with the malware attached. In this particular case, the cyber attack consists of hacking a website and distribution of malware via e-mail, whereas information attack is related to the spread of false information (Fig. 9). According to the NCSC, fake news were repeatedly posted through backdoor access to the website, which is *de facto* related to the website owners' lack of attention to cyber security measures, their deployment and use.

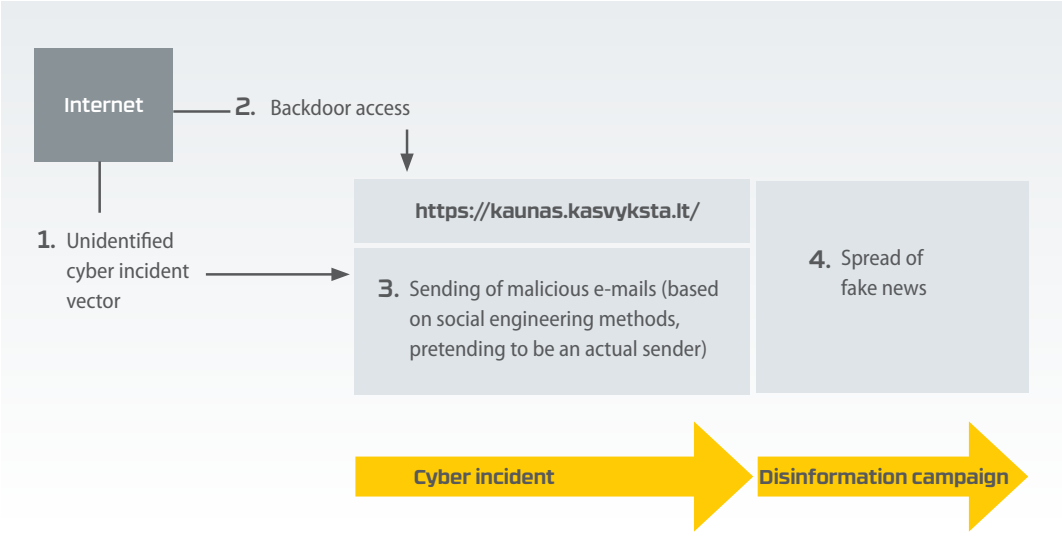

Fig. 9 Cyber incident and disinformation campaign using the website ***kaunas.kasvyksta.lt.***

Vulnerable websites

- **Statistically, the websites of municipal authorities, ministries and their subordinate bodies are the most vulnerable websites of the public sector.**
- **37% of 118 000 websites in Lithuania have an open administrator or user access to the CMS.**
- **Number of secure websites in the public sector grew by 11% in 2019.**

The use of websites vulnerabilities for cyber attacks is unfortunately still an underestimated threat. Vulnerable websites can be used for disinformation campaigns, such as fake news. Attacks based on social engineering can also be attempted in order to swindle users out of their credentials or money. In such cases, cyber attacks are carried out against websites, exploiting their vulnerabilities, installing malicious software, etc. The most common case is malicious websites with free or purchased domain names. Hackers seek to upload such websites into a high-speed infrastructure. These sites are also commonly used to conduct malicious activity based on social engineering techniques.

In 2019, cyber security organisation *Akamai* carried out a monitoring of domain names used in social engineering cyber attacks, i.e. baiting (the monitoring sample was over 2 billion websites). The monitoring detected the names of domains (ending with .com, .tk, .loan etc.) that conducted malicious activities for less than three days.[9] A short period of activity is related to the efforts of hosting providers to block such sites immediately. This kind of activity implies constant malicious efforts to seek out hosting providers that disregard recommendations from supervising authorities to shut down malicious resources. Websites related to *Akamai* investigation have also been aggressively exploited by *botnets* that are used to distribute malware and mine cryptocurrency at the expense of users. In this case, malware is not necessarily installed on the site visitors' computers – computer resources are used to process the

[9] https://www.cisco.com/c/dam/en/us/products/collateral/security/email-security/email-threat-report.pdf

code embedded in the website and thus to generate cryptocurrency. The websites of business companies, public sector organizations and the public have the biggest threat of vulnerability as the functionality of these sites directly affects the services provided and their accessibility (Table 3).

CYBER THREAT	IMPACT ON		
	National security	Business and RIS	Residents
Vulnerable websites		✓	✓

Table 3. Impact of the threat of vulnerable websites.

In 2019, the NCSC verified the security assessment of more than 118 000 websites of the Lithuanian TLD with the suffix ".lt" and more than 900 public administration entities, SIR and CII owners. Having identified 56 700 (48%) websites with known CMS, it was determined that Word Press was the most popular open source CMS in Lithuania, accounting for 34% of the total range of websites and 33% of the set of public sector websites (Table 4).

№	Content management system	Prevalence in Lithuania	Prevalence in the public sector
1	WordPress	34%	33%
2	Joomla	4%	13%
3	Fresh Media	< 1%	6%
4	Idamas	< 1%	5%
5	Drupal	< 1%	3%
6	Other	8%	2%
7	Unidentified	~ 52%	38%

Table 4. The most popular identifiable CMS in Lithuania

Of the CMS identified (56 700 from total of 118 000 Lithuanian sites), it was found that 63% of their software versions were outdated, which meant a risk that the outdated CMS would have a vulnerability that could allow a malicious attack to be carried out against a website. To make matters worse, 8 % of the identified websites' owners use CMS that are no longer supported by developers, which may result in a lack of updates and security vulnerabilities. Of all the websites in the range (118 000), nearly 44 000 (37%)

have open access from an external network to the administration and/or management of the website (Fig. 10). Vulnerable CMS and an open administrator or user access windows to the website are cyber security risks that increase the probability of hacking, site management takeover, content alteration, malicious insertion of software or unauthorised access to the organisation's internal networks.

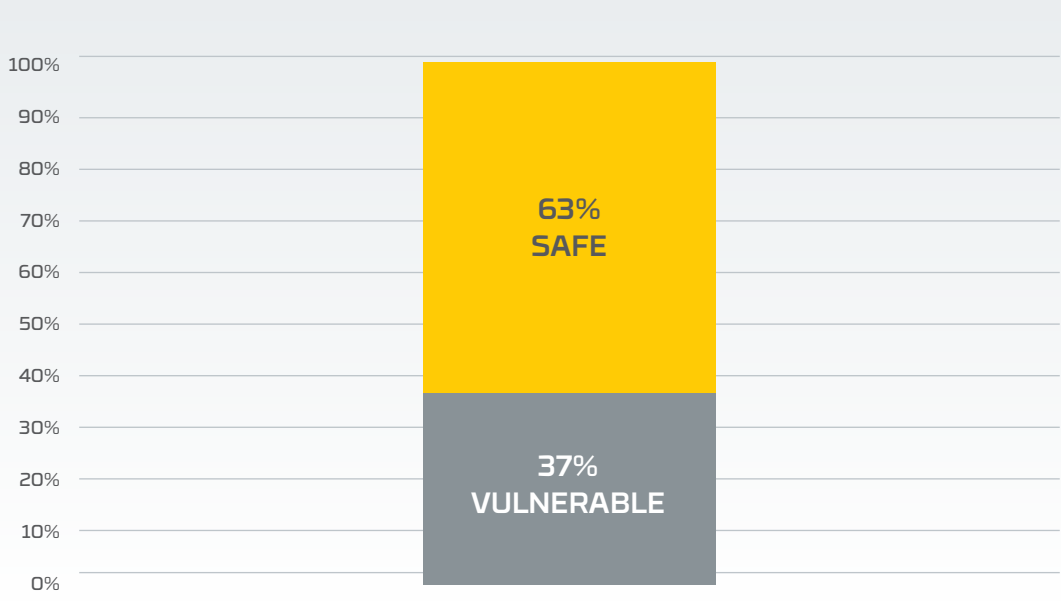

Fig. 10. Evaluation of cyber security of Lithuanian (.lt) websites based on the possibilities to access the site management (scope: 118 000 sites).

Open source CMS websites that are not updated on a regular basis are the most common target of cyber attacks. The situation is complicated further by unreliable and non-updated CMS plugins as well as open access by external network users and administrators, unencrypted communication or misuse of cryptographic tools, i.e. authentication without TLS / SSL Certificates, using SSL 3.0 and older cryptographic algorithms. According to the NCSC, public access to external website administrator window (e.g. ".lt/admin") is not restricted in almost half of the sites that have open access to CMS. In this case, especially if there is no password change policy and the number of login attempts is not limited, attackers have a possibility to carry out brute-force attacks by using the technical means and retrieving user lists.

In 2019, the NCSC also monitored vulnerabilities of public sector websites and reviewed the evaluation of cyber security of public sector websites, elaborating on the assessment in detail (Annex 1). The situation of cyber security with regards to public sector websites is getting better if compared to the previous period; however, 17 % of the sites can still be easily hacked (Fig. 11). In order to remove vulnerabilities, the NCSC directly informs the potentially vulnerable sites' administrators and coordinates the removal of high-priority vulnerabilities. Based on the analysis results, the NCSC provides recommendations to the web administrators on the most common weaknesses of the websites and information systems.

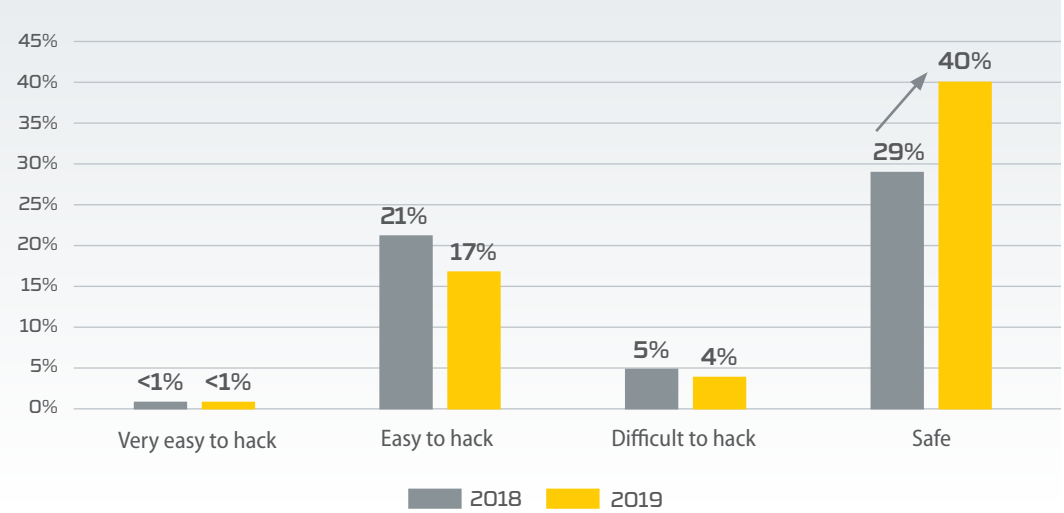

Fig. 11. Cyber security of public sector websites during the period from 2018 to 2019 based on the assessment of vulnerability per domain.

The research of the public sector websites has revealed that the closest attention should be paid to the protection of the websites of municipal authorities, ministries and their subordinate bodies (Fig. 12).

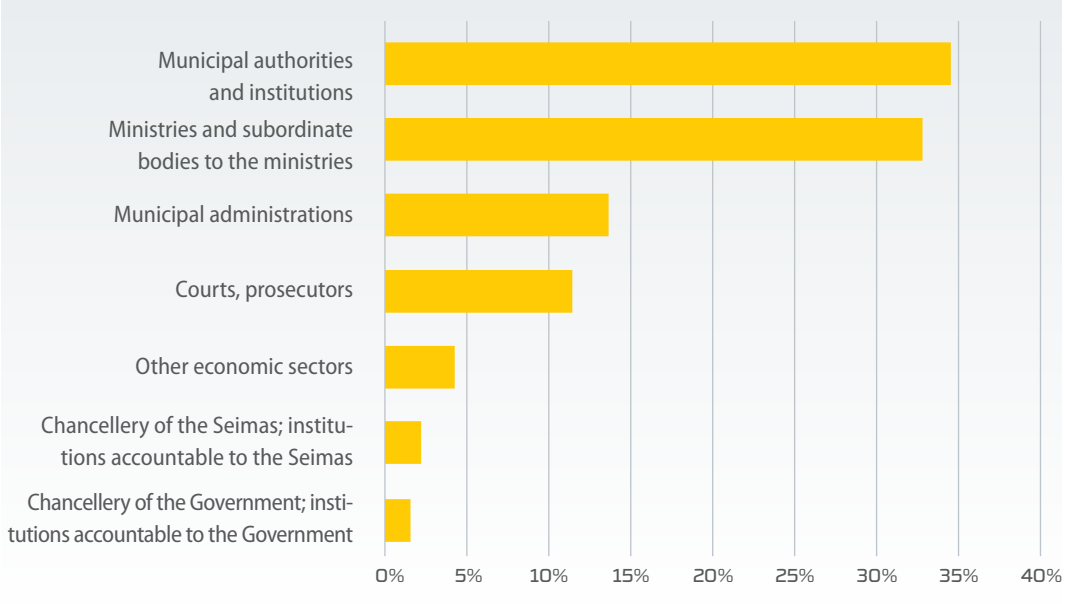

Fig. 12. General vulnerability of the websites in public sector bodies.

A tendency has been noticed that CMS developed in Lithuania are especially vulnerable to cyber attacks. Insufficient quality assurance during CMS development or programming of its components is the main reason for these vulnerabilities. The CMS of one Lithuanian manufacturer had a critical security vulnerability that allowed persons to embed additional source code into the page viewed by users (*cross-site scripting* security vulnerability). Sixty-five Lithuanian websites with this vulnerability have been detected.

Following the principle of responsible disclosure, the NCSC has informed the creator of the CMS and the web administrators of vulnerable websites and has provided instructions on how to eliminate the vulnerabilities.[10] The NCSC notes that the entities do not always purchase website support services or fail to include the contractual obligation to eliminate vulnerabilities resulting from a defect. Usually, websites are not validated as information systems, no security officers are assigned, while administrators do not pay enough attention to cyber security issues and the information published on the websites is not considered to be important. For this reason, funding is not always allocated for website updates, and sometimes the website is so old that it is not even possible to update its software to the latest version. In addition, the NCSC reports that the situation of cyber security of the websites can be checked publicly using a free of charge tool available at the website of the NCSC. During a short period in 2019, this tool was successfully used by 120 entities (Fig. 13).

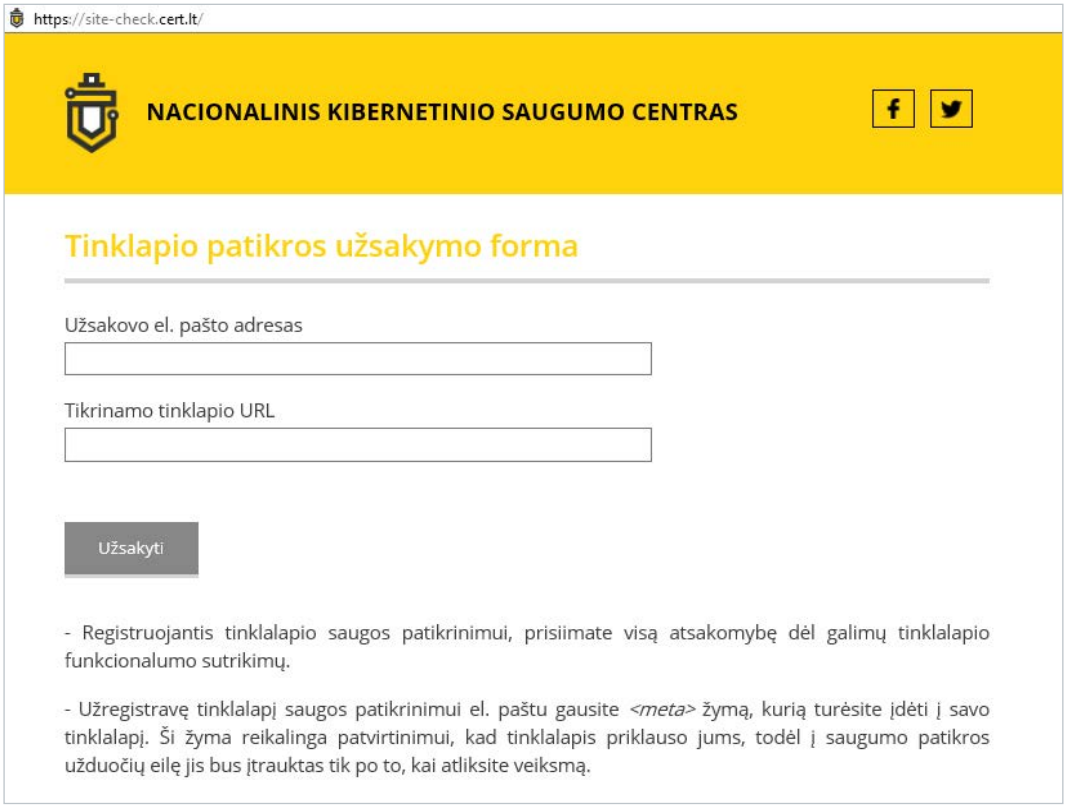

Fig. 13. A tool for checking vulnerability of the websites, available at https://site-check.cert.lt.

[10] CMS producer is not disclosed as the vulnerabilities are currently being eliminated.

Implementing cyber security requirements

In 2019, the specialists of *Create Lithuania* working at the Ministry of National Defence conducted a survey of small and medium-sized enterprises on cyber security.[11] More than 200 respondents took part in the survey. The analysis of the survey results has revealed that three out of four small and medium-sized enterprises are not ready or do not know whether they are ready to withstand cyber attacks. No less than 72% of the respondents said they did not know how to evaluate vulnerabilities and risks of cyber security. In addition, the respondents said they did not understand the consequences of cyber attacks. For this reason, cyber security entities find it difficult to implement cyber security requirements established by the Government of the Republic of Lithuania.

The monitoring of implementation of cyber security requirements has revealed that the implementation of requirements of CII owners has increased, i.e. in 2019, 80 % of CII owners had implemented cyber security requirements (Fig. 14). Unfortunately, SIR owners and administrators are still facing problems with the implementation of the said requirements.

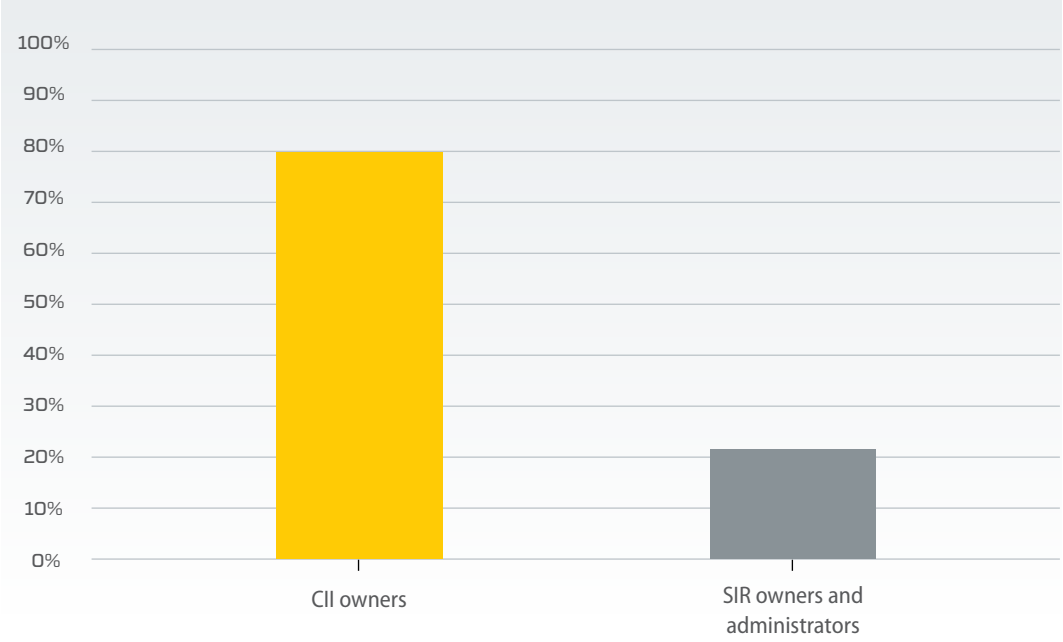

Fig. 14. Implementation of organisational and technical requirements of cyber security.

Cyber security strategy places a great emphasis on the cyber security of the owners of critical information infrastructures. In 2019, the NCSC introduced a new capability, i.e. IT audits of cyber security. Audit results lead to the conclusion that the declared implementation of cyber security requirements does not reflect the true situation of cyber security in the organisations.

[11] http://kurklt.lt/2020/01/06/apklausa-lietuvos-svv-truksta-kibernetinio-saugumo-ziniu/

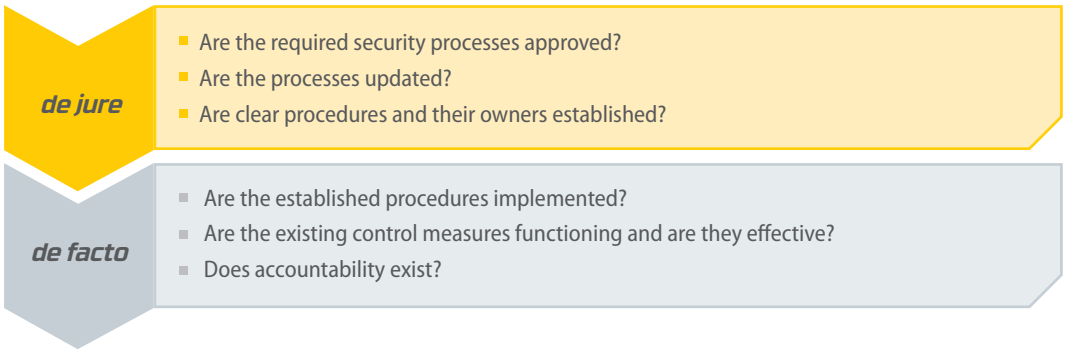

Fig. 15. The process of cyber security audit as conducted by the NCSC.

Organisations often meet or almost meet the *de jure* criterion of cyber security requirements. The inspected entities have formally defined cyber security processes and guidelines, but the descriptive part of cyber legislature is still often perceived as a bureaucratic burden. Security documents are often prepared in accordance with already outdated and invalid legal acts of the Republic of Lithuania, whereas the processes defined in the content of the documents are not assigned to the appropriate subdivisions based on their competence. During the analysis of cyber security implementation, the NCSC has also noticed a tendency that organisations tend to define the content of information and cyber security documents in the abstract, which allows them to formally justify the implementation of the requirements while skipping the regulation of the required processes.

Due to formal and abstract processes, the actual safety of an organisation is often ensured by the *ad hoc* principles, when the owners of the processes and their responsibilities are not clear. The NCSC has noticed some cases when the responsibility for the information system and its security was assigned to a particular structural unit of the organisation, but in practice, the supervision of the system was sporadically performed by one of the administrators. Physical audit has also revealed that formal compliance with organisational and technical cyber security requirements was *de facto* implemented partially, failing to ensure proportional cyber security for critical services.[12]

A lack of risk management culture is one more tendency which has been noticed by the NCSC during the audits. Organisations still do not perceive information as property and therefore fail to properly evaluate the impact of cyber attacks. For this reason, it is likely that the organisations have taken too much risk. In terms of formal cyber security regulation, audits by the NCSC detected typical shortcomings of technical control measures (Fig. 16).

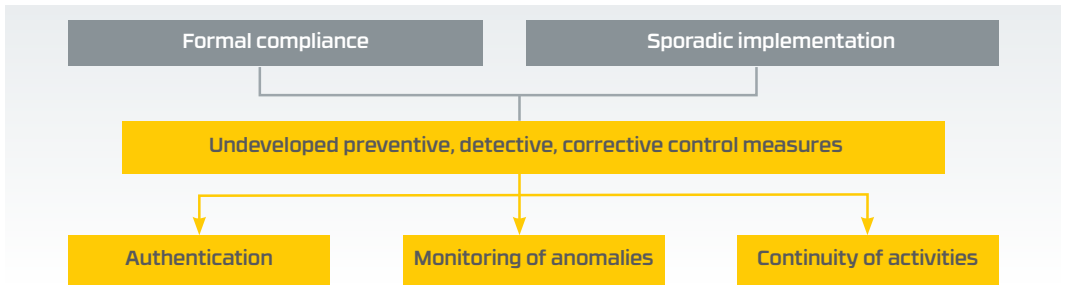

Fig. 16. Typical weaknesses of cyber security.

[12] Anonymised data shall be provided herein having considered the fact the NCSC checks by priority the owners of critical information infrastructures, the exhaustive list of which is managed in accordance with the procedure laid down by the Law on State Secrets and Official Secrets.

For example, from a preventive point of view, not enough attention is paid to the storage of login data. Authentication information is still often stored in the local servers as unencrypted files and in the systems' instruction manuals which are sometimes uploaded into public document management systems. Usually, the method for the generation of passwords for users and administrators includes only two groups (letters and numbers), while the requirement for password change is enforced every six months or is not enforced at all. There are still frequent cases when users forget to change the manufacturer's default passwords in the hardware and software. As far as detective measures are concerned, in many cases, although the operations of the users and administrators are logged in the information systems, the records are not reviewed and no anomalies are monitored, thus the restart method is typically applied in the event of malfunction of the information infrastructure or its structural element. Intrusion detection systems are still not used, while firewalls in the key servers are not enabled that could block all incoming and outgoing flows, except for those that are related to the functionality and administration of critical information infrastructure. For this reason, a huge gap has been observed between incident detection regulation and actual enforcement of the requirements (Fig. 17). Corrective measures for non-holistic cyber security implementation also cause additional risks. No backup restoration tests are made which could show whether there are any corrupted copies and if all the necessary information is stored in the copies. The software of platforms with infrastructure elements is also rarely updated.

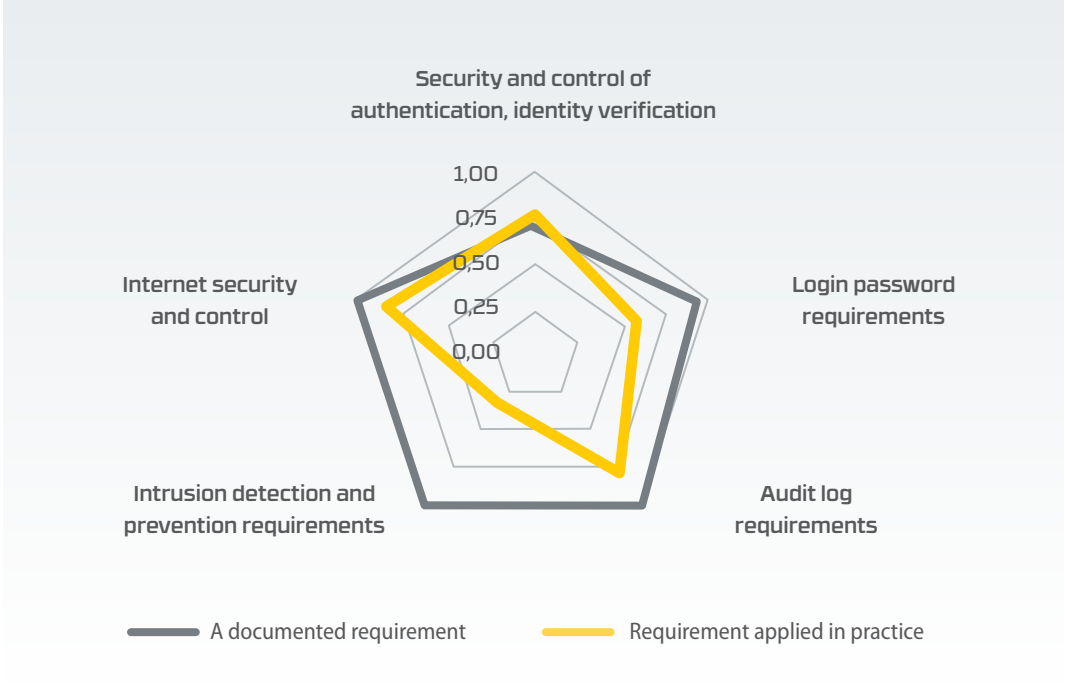

Fig. 17. Actual implementation of technical cyber security requirements in one of the organisations. 0 – not implemented, 1 – the requirement is implemented.

Credibility of service providers, hardware and software

- **Examples of unreliable software and hardware have been detected, whereas user data is sent to the countries where EU data protection requirements are not applied.**
- **Publicly distributed software and applications have clearly excessive rights to access data on the devices.**

Reliability of hardware and software is primarily related to cyber security risks. Device security vulnerabilities is one of the biggest risks. Device security vulnerabilities cause the greatest threat in the IoT environment. Manufacturers seek to create relatively cheap devices at the lowest costs; therefore, not much attention is paid to cyber security and authentication control of these devices. Due to low computing resources in these devices, encryption is also ignored. This threat is relevant at the international level. For this reason, the EU seeks to establish a common certification mechanism for devices and services.[13] According to the data at the disposal of the NCSC, in Lithuania, such gaps are mainly related to the enabled excessive services and open ports. Often, open port functionality is not necessary, and users can block this access themselves, i.e. by changing user login data of the control panel and by blocking or restricting access from external networks by limiting it to certain IP addresses only. A hacker may look for vulnerabilities in the IoT in order to execute a cyber attack, even though such activities do not require specific knowledge and tools, and publicly available tools are sufficient.[14]

Reliability of service providers is one more important aspect of hardware and software reliability (Fig. 18). This issue is multifaceted: on the one hand, it is related to the uncertain reputation of the manufacturer, while on the other hand, it is related to unauthorised changes in the manufacturing process. Sometimes it may be related to different regional or national regulations. For this reason, hardware and software

[13] https://www.enisa.europa.eu/topics/standards/certification

[14] https://www.shodan.io/

intended for certain regions may not meet specific quality assurance requirements, for example, the ones applied in the EU countries. Certification initiated at the EU should improve safe distribution (in terms of cyber security) across Europe, but so far, since there is no uniform regulation, users themselves assume risks, which sometimes increase due to the lowest cost principle. For this reason, hardware made even by reliable manufacturers, which is assembled in the untrusted countries at low prices, may pose risks of vulnerabilities, backdoor access, etc. (Fig. 18).

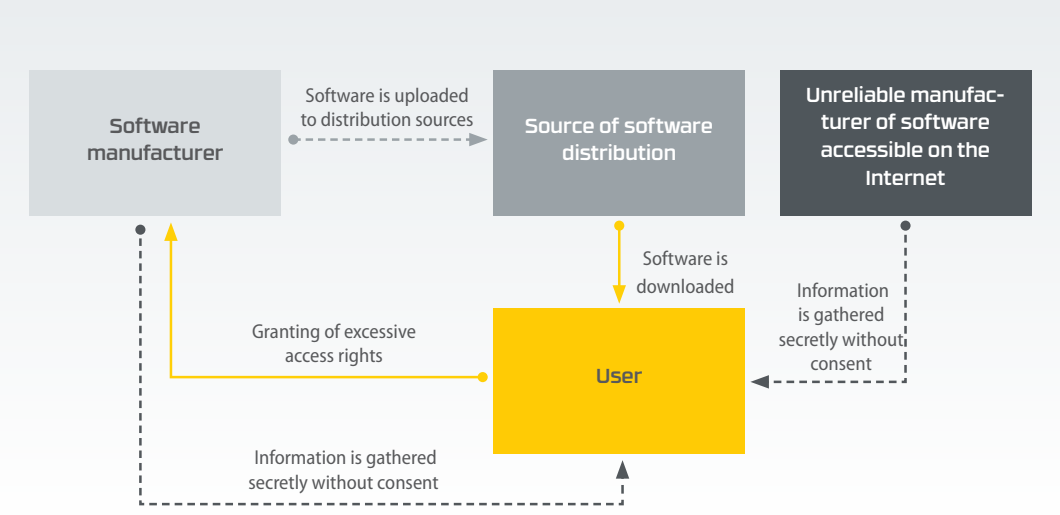

Fig. 18. Example of software and hardware reliability risks.

According to the NCSC, the issue of reliability of service providers, software and hardware is comprehensive (Table 5).

CYBER SECURITY THREAT	IMPACT ON		
	National security	Business and SIR	Residents
Reliability of service providers, software and hardware	✓	✓	✓

Table 5. Impact of the threat of devices' security vulnerabilities.

In order to ensure a safe use of hardware and software in the country, the NCSC has performed a complex assessment of cyber security of electronic services (mobile applications, software and communications and multimedia equipment) provided in Lithuania. The research was carried out in the most relevant risk areas for the users by assessing the mobile app software as well as communications (routing and switching) and multimedia equipment.

The results reflect sophisticated cyber security risks which are expressed in various forms and content services and are oriented towards interception of user data (personal, infrastructure, etc.).

The majority of software products are free of charge and therefore are used by many users in Lithuania. Software products developed in non-NATO countries have been found to have high functional completeness, but in almost all cases they pose a threat to the users of these products, i.e. they potentially collect excess information and establish multiple connections to encrypted communication channels with servers in the Eastern countries. Often, product manufacturers tend to hide the true country of origin of their products.

Results of the analysis of mobile applications

Cyber security assessment of the software of mobile applications *Yandex.Taxi, FaceApp* and *ABBYY Business Card Scanner* has been conducted recently. The findings of the analysis indicate that the applications required access rights to the mobile device and their user agreements could be interpreted too widely. Moreover, they were able to transfer data from mobile device to third countries where the provisions of the General Data Protection Regulation are not applied.

Yandex.Taxi mobile application analysis

The NCSC has assessed *Yandex.Taxi* software package which has been actively distributed in Lithuania since 26 July 2018.

During the survey, the application was found to require access to a large amount of sensitive data and access for using device functions. The application can activate the camera and microphone of the device (record user environment), use the contact list (access to phonebook, information of accounts used), control calls, establish the identity and status of the device, control short message services (ability to intercept incoming messages), modify the content stored in the memory of the smart device, see the exact location of the device (GPS), control network access (send data via the Internet, monitor and control network connections, control Wi-Fi access (Fig. 19).

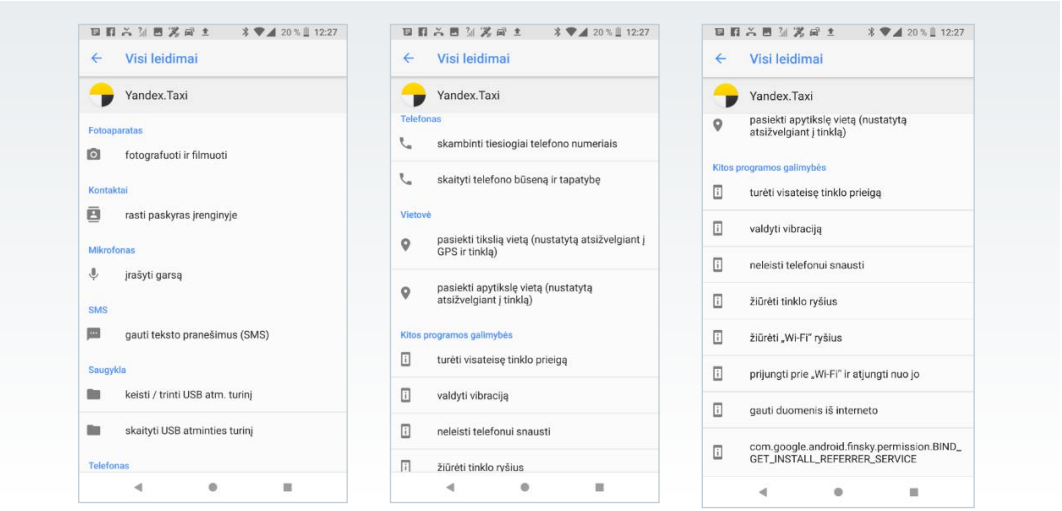

Fig. 19. Yandex.Taxi settings.

It should be noted that later versions of the application may even increase the number of required types of access in the future. In 2019, a slightly modified application was launched in Finland under the name of *Yango*. However, in spite of the required excessive access to the device's functionality, it is designed in high-quality, is properly optimised and uses encrypted channels and standard protocol ports for data transmission.

The NCSC analysis has revealed that the application had active communication with 11 unique IP addresses (10 of which belong to the Russian Federation) on a regular basis via encrypted communication channels. The data has been found to be transmitted at different time intervals.

The analysis has revealed that the application is able to communicate with addresses in different regions of the Russian Federation at various times and via encrypted communication channels (based on geolocation IP database information), regardless of whether the application is in standby or active mode. It should be noted that *Yandex. Taxi* mobile application maintains a regular connection with three addresses (Table 6).

Commercial name: Yandex. Taxi

Systematic name: **ru.yandex.taxi**

No		City	Hostname	Data is transmitted via the application in standby mode	Data is transmitted via the application in the active mode
1	ACTIVE NETWORK CONNECTIONS	Moscow	*.yandex.net	Yes	Yes
2		Moscow	*.yandex.net	Yes	No
3		Moscow	*.yandex.net	Yes	No
4		New Jersey	*.linode.com	Yes	Yes
5		Yekaterinburg	*.yandex.net	Yes	Yes
6		Moscow	*.yandex.ru	No	Yes
7		Yekaterinburg	*.yandex.ru	No	Yes
8		Yekaterinburg	*.yandex.net	No	Yes
9		Yekaterinburg	*.yandex.net	No	Yes
10		Moscow	*.yandex.net	No	Yes
11		Moscow	*.yandex.ru	No	Yes

Table 6. Analysis of software package network traffic (Note: IP addresses are known to the NCSC).

ABBYY Business Card Scanner mobile application analysis

Mobile application *ABBYY Business Card Scanner* is designed for virtualisation of business cards.

A business card captured on a mobile device is analysed and digitised by the application, i.e. the name, surname and institution being represented as well as other data on the card is extracted. It should be noted that extraction and digitisation of data based on photo material is a relatively complex procedure (Fig. 20).

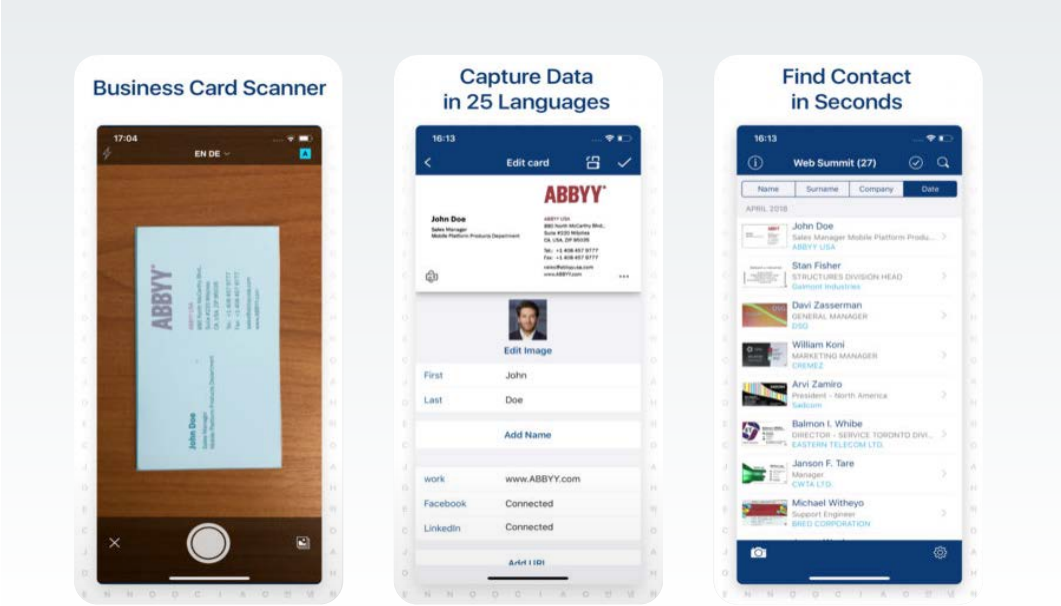

Fig. 20. ***ABBY Business Card Scanner*** mobile application.

Apple's App Store, i.e. a platform for downloading apps, specifies the following information: the seller of the application is *ABBY USA Software House Inc.*, the headquarters is in Milpitas, California and the Chief Executive Officer, CEO, is Ulf Persson (Fig. 21).

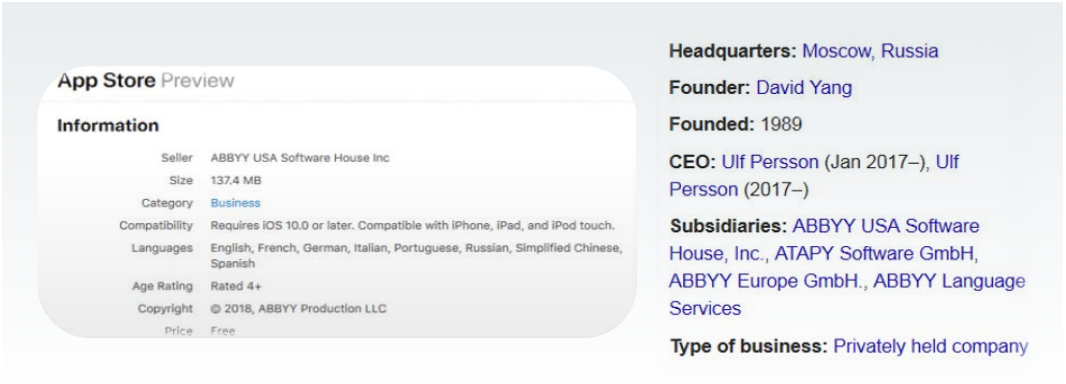

Fig. 21. Information describing the producer ***ABBYY.***

The analysis of app traffic decomposition has revealed that *ABBYY Business Card Scanner* connects to 61 servers located in Germany, Poland, Sweden, Ireland, the USA and Russia. It can be said that *ABBYY* has consistently avoided to reveal the origins of the company by indicating the USA as the country of its commercial development.

According to the assessment of threats to national security conducted by the State Security Department of Lithuania and the Second Investigation Department under the Ministry of Defence in 2018, "Russian intelligence and security services have legal powers and technical possibilities to gain access to data from Russian and foreign citizens using Russian electronic communication platforms". The assessment of threats also states the following: "<...> the risk of personal data leakage to Russian intelligence and security services applies to all Lithuanian citizens using Russian social networks and e-mail services, such as *odnoklasniki, mail.ru, yandex*, etc."

FaceApp mobile application analysis

Mobile application *FaceApp* is a photo transformation program created by the Russian software developer *OOO Wireless Lab*. The application allows users to graphically modify the features of faces captured in photos by using specialised filters, i.e. to make a person captured older or younger, add a smile or change gender-specific facial features. According to the terms of use of *FaceApp*, only individuals aged 18 or older can use the application (if the application is used by individuals aged 13 or older, parents or guardians assume responsibility for its use).

Applications in Android (*FaceApp* version 3.4.8, size 12.45 MB) and iOS (*FaceApp* version 3.4.7, size 153.1 MB) platforms have been analysed. When the application is installed on a mobile device, an alert is displayed stating that the selected photos will be remotely processed on the mobile application developer's servers. If the user disagrees with the provided terms, the application displays a window stating that it cannot function and prompts the user to agree to remotely process his/her photos. Based on the application access requirements and the level of data access to the device, it can be assumed that the access requirements are intended to ensure functionality of the mobile application, are not excessive and are an integral part of the application for a proper performance. It should be noted that the user who downloads and installs the *FaceApp app* agrees with the conditions specified in the terms of use. Otherwise, there is no possibility to use the services: „<...> By accessing the *FaceApp* website or by downloading *FaceApp's* mobile application, you agree to these Terms. If you do not agree to these Terms, including the mandatory arbitration provision and class action waiver in Section 15, do not access or use our Services <…>".

The terms of use indicate that the user has to grant *FaceApp* free-of-charge access to the data available in the application environment, i.e. to permit *FaceApp* to use the data, reproduce it, modify, adapt, publish, translate, create derivative works, distribute and use it publicly in all available known formats and channels (also the ones which will be created in the future): "<...> You grant FaceApp a perpetual, irrevocable, nonexclusive, royalty-free, worldwide, fully-paid, transferable sub-licensable license to use, reproduce,

modify, adapt, publish, translate, create derivative works from, distribute, publicly perform and display your User Content and any name, username or likeness provided in connection with your User Content in all media formats and channels now known or later developed, without compensation to you <...>".

It is noted at the same time that the user agrees to allow *FaceApp* to commercialise the data used in the mobile app: "...> By using the Services, you agree that the User Content may be used for commercial purposes. You further acknowledge that *FaceApp's* use of the User Content for commercial purposes will not result in any injury to you or to any person you authorised to act on its behalf <...>".

Mobile devices were found to undergo partial actual data (photo) modification procedures (compression and partial processing), and this partially processed information is sent to a remote server for final processing. Photos of the users are modified in the servers, the majority of which are registered in the United States of America (the application running on the iOS platform made connections with 2 servers registered in Ireland). Data from the server is downloaded and compiled on a mobile device, which is then displayed to the user.

The analysis has revealed that the application running on the *Android* platform sends on average 560 kB of data to the server and receives 360 kB of data; meanwhile, the application running on the iOS platform sends an average of 1.1 MB of data and receives 176 KB of data. These differences in data exchange sizes are believed to be due to different data compression mechanisms used on the Android and iOS platforms.

The biggest concern is the application usage rules, which require the user to agree to provide *Faceapp* with free-of-charge access to data available in the application environment, i.e. to allow *FaceApp* to use it, reproduce, modify, adapt, publish, translate, create derivative works, distribute and use publicly in all known available formats and channels (also the ones which will be created in the future). Considering the fact that the application was developed by the Russian software manufacturer *ООО Вайрелез Лаб*, these requirements increase the impression of a disproportion between the service profile of the application and the cost of user's personal data.

Routing and switching equipment analysis

The NCSC has also performed the assessment of cyber security of communication equipment for sale in Lithuania; this assessment was published on 10 June 2019. This analysis provides the results of the assessment of *D-Link* routers and switches for households and small businesses. The price range for the analysed equipment varies from EUR 20 to EUR 200.

Network equipment manufacturer *D-Link Corporation (D-Link Systems, Inc.)* is a Taiwan-based corporation that has owned its *D-Link* trademark for 30 years. The company has 2 000 employees and supplies its products to 60 countries. Technologically, the corporation focuses on various implementations of common network solutions, which include communication switching, routing and cloud computing technologies that create large-scale and high complexity wireless and broadband network development opportuni-

ties. *D-Link* has a wide range of target groups, i.e. households, small, medium and large business sectors, communication and electronic service providers. Despite the prominence of the *D-Link* trademark, the corporation faced certain security challenges during the development of its equipment in 2014–2018. According to the information provided by the Common Vulnerabilities and Exposures (CVE), 50 vulnerabilities were identified, 31 of which were found in 2018. A noticeably growing tendency of vulnerabilities in *D-Link* products is a matter of concern and is the subject of complex research by the NCSC.

Certain products designed for households and small and medium-sized enterprises have been found to be especially closely technologically related to the Russian Federation. The products *D-Link DIR-842, D-Link DIR-853, D-Link DSL-2640U* and *D-Link DSR-250N* are indicated as supplied by D-Link Russia. The equipment is using the Russian DNS services *Yandex.DNS* and *SkyDNS*. The Domain Name System (DNS) is a system that converts a domain's names to a server's numeric IP address. Having specified the DNS server address on the router, each domain name request is sent to the specified DNS server, which provides a numeric IP address, and the router redirects the user to the server's IP address. It should be noted that the device software is updated from the servers located in Russia (Fig. 22).

Upon activation of the default *Yandex.DNS* service on *D-Link* devices, all DNS requests are sent to the servers controlled by the Russian company *Yandex*. These servers record requests from the users that make it possible to determine the IP address of the requesting user, the user's country, the time of the request and the websites the user is visiting. It is important to note that long-term tracking of the user's DNS requests and processing of monitoring results using modern data analysis and aggregation techniques enable highly accurate insights into user behaviour in the cyberspace and, sometimes, lead to identification of a person.

In addition to *Yandex.DNS* service, the *D-Link DIR-853* product also includes another DNS service, *SkyDNS*, which is a product made by Russian corporation that provides DNS and DNS filtering services for legal entities and citizens. The corporation indicates that users from over 40 countries, including Russia, Kazakhstan and Ukraine, are using its services. *SkyDNS* manages a database with records of 90 million pages derived from aggregation of DNS inquiries. Artificial intelligence is used to characterise and classify *SkyDNS* pages by training it through consumer behaviour research: *"Our research team works with bid data using such methods as continuous machine learning, AI and user behaviour analysis to enrich SkyDNS DB and ensure high quality of web categorisation"*. It should be noted that the processes of aggregating and analysing the aforementioned information and using it to solve specific challenges can only work as long as large volumes of data are secured; conversely, improper management of this data may threaten the privacy of the users.

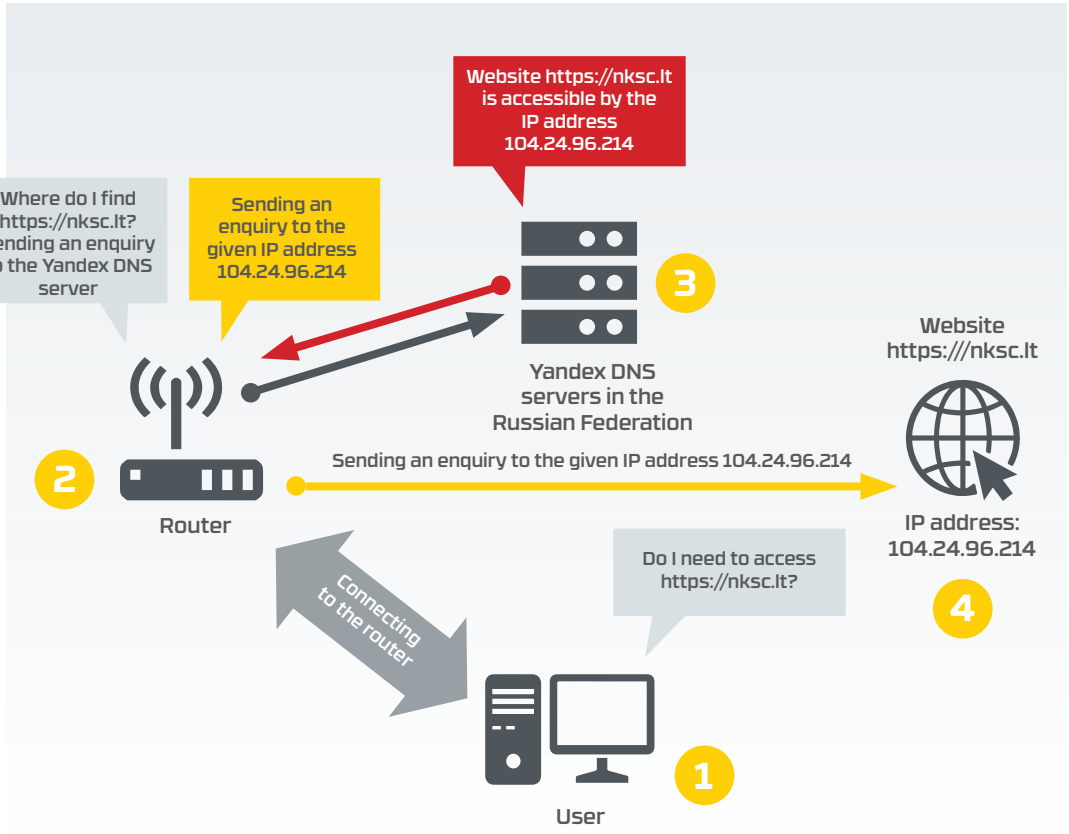

Fig. 22. Flowchart of ***Yandex.DNS*** and software update process.

The NCSC notes that users using software pre-installed by third parties that enables the DNS function on the routers are risking that their web browsing data shall be logged and stored by third parties without any control. Users are recommended to examine the acquired software and hardware and to critically assess the content of their services.

Results of multimedia equipment analysis

The NCSC has performed security assessment of IPTV box *S-Box TX3 mini-H* (hereinafter – the box) of Radio and Television Commission of Lithuania (hereinafter – the RTC). IPTV box *S-Box TX3 mini-H* is a multimedia product distributed in Lithuania which is designed and manufactured by *Oranth*, under the Chinese trademark *Tanix*, for TV broadcasts over the Internet.

The analysis has revealed that the said box uses the 7th generation Android 7.1.2 operating system with the kernel version 3.14.29. It should be noted that the standard Android 7.1.2 OS comes with a newer kernel version 4.4, suggesting that the box uses a specialised kernel to ensure functionality of product-specific electronic elemental base. The latest Android OS is of the 9th generation; therefore, the device has a system which is two generations older than the latest version and raises doubts regarding the effectiveness of the security solutions it uses to prevent current cyber security risks.

According to the data provided by the Common Vulnerabilities and Exposures (CVE), *Android 7.1.2* has 433 vulnerabilities of varying levels. Some of these vulnerabilities enable remote control of the device. Once the control is taken over, the device can be used to initiate user network tracking processes and to participate in cyber attacks. Functionality of the graphical user interface was realised in 2016 using *Kodi 16.1*, which is no longer supported and has known software security vulnerabilities.

During the analysis, connections to 440 IP addresses in 46 countries were detected. The box attempted to connect to 5 IP addresses registered in Lithuania. Of the total range of detected IP addresses, 57 belong to legal entities registered in the Russian Federation and are as follows: 10 addresses belong to *Rostelecom*, 6 addresses to *YANDEX LLC*, 4 addresses to *JSC ER-Telecom Holding*, 3 addresses to *MnogoByte LLC*, 3 addresses to *PvimpelCom*, 3 addresses to *MnogoByte LLC*, 2 addresses to *Cronyx Plus Ltd*., 2 addresses to *2COM Co Ltd.*, 1 address to *AVK-computer Ltd.*, 2 addresses to *CDNvideo LLC*, 2 addresses to *Start LLC*, 1 address to *CJSC Rascom*, 1 address to CJSC SibTransTelecom, 1 address to CJSC TransTeleCom, 1 address to *Ddos-guard Ltd.*, 1 address to *Domain names registrar REG.RU, Ltd.,* 1 address to *Fast Link Ltd.*, 1 address to *Fly Telecom LLC*, 1 address to *Hosting Operator eServer.ru Ltd.*, 1 address to *Iskratelecom CJSC*, 1 address to *LLC GlobalTelecomStroy*, 1 address to *LLC Multiservice*, 1 address to *LLC SETEL*, 1 address to *LLC Sip nis*, 1 address to *MTS PJSC*, 1 address to *National Telecom, CJSC*, 1 address to *OAO ASVT*, 1 address to *OOO Istranet*, 1 address to *OOO Trivon Networks*, 1 address to *Pskovline Ltd.*, 1 address to *Quartz Telecom LLC*, 1 address to *RTK-Volga-Ural LLC*, 1 address to *Teleskan-Intercom Ltd*.

The survey has also found that the box tried to connect to IP addresses registered in the following countries: to 1 address in Armenia, to 5 addresses in Australia, to one address in Belarus, to 4 addresses in Belgium, to 1 address in Brazil, to 2 addresses in Bulgaria, to 10 addresses in Canada, to 1 address in Chile, to 5 addresses in China, to 5 addresses in Czech, to 2 addresses in Denmark, to 2 addresses in Finland, to 28 addresses in France, to 1 address in Sakartvelo, to 18 address in Germany, to 1 address in Greece, to 2 addresses in Honk Kong, to 5 addresses in Hungary, to 5 addresses in Ireland, to 1 address in Israel, to 4 addresses in Italy, to 4 addresses in Japan, to 1 address in Kazakhstan, to 1 address in Kuwait, to 2 addresses in Latvia, to 1 address in Malaysia, to 1 address in Morocco, to 25 address in the Netherlands, to 1 address in New Zealand, to 3 address in Norway, to 10 address in Poland, to 2 addresses in Portugal, to 1 address in Moldova, to 1 address in Romania, to 3 addresses in Slovenia, to 11 addresses in South Korea, to 3 addresses in Spain, to 6 addresses in Sweden, to 2 addresses in Switzerland, to 1 address in Taiwan, to 2 addresses in Turkey, to 18 addresses in Ukraine, to 1 address in the United Arab Emirates, to 22 addresses in the United Kingdom and to 151 addresses in the United States of America.

Some box apps use *AceStream* for content transmission. *AceStream* is based on peer-to-peer (P2P) network model where the information is exchanged directly among the users, i.e. the users send video content (or meaningful data) from one user to another, engaging in the distribution of viewable content.

It should be noted that requests sent by the box can be logged by the systems that service them, thereby identifying the user's own IP address and identifying the request-generating devices. An important aspect is that the box sends requests to the countries where the General Data Protection Regulation is not applicable. For this reason, it is difficult to ascertain the security level of the personal data of functional users that may be created (and/or involved in the infrastructure) when operating the box.

05

DISINFORMATION CAMPAIGNS

DISINFORMATION CAMPAIGNS

- **Over the last few years, the Lithuanian statehood, independence and democratic principles have become one of the most important targets of media outlets that are biased against the country.**
- **2 890 cases of informational activities biased against Lithuania have been identified; a quarter of them targeted the protection of constitutional framework.**

According to the Strategic Communication Department of the Lithuanian Armed Forces, in 2019, the level of disinformation intensity in Lithuania remained similar in terms of coverage and content to the previous year.

The main source of disinformation remained the activities conducted by the countries outside the North Atlantic Treaty Organisation (hereinafter – NATO) and the EU as well as by non-state actors that targeted the country's strategic goals and democratic institutions: Lithuania's membership in NATO and the EU, strengthening of national defence capabilities, multilateral relations, trust in state institutions, the judicial system, the country's energy autonomy, socio-economic prosperity and historical memory. In 2019, a total of 2890 cases of harmful fake information were identified in the Lithuanian cyber attacks (15% more than in 2018, on average about 241 cases monthly). More than two thirds of them were initiated and executed by third parties.

During the observation period, the number of large-scale multi-layered cyber attacks increased, i.e. attacks consisting of both cyber and information elements. These attacks featured more advanced technical and content design solutions as well as sophisticated operational capabilities. These types of attacks utilised larger amounts of informational resources as well as technological and physical capabilities. The main agent of disinformation was still the media controlled by the Kremlin regime, which published and distributed information that did not comply with the provisions of the Law on Public Information of the Republic of Lithuania.

These media outlets created the image of Lithuania as a hostile and unreliable state. They used content that promoted war and national hatred as well as elements of deception and content production that lacked transparency: falsified facts, purposefully distorted public statements, comments or press releases; additionally, video editing tools were used to falsify visual material and the identities of other individuals or institutions were exploited as a disguise. The flow of negative information correlated with significant events in foreign policy and within the country. Media outlets that were biased against Lithuania sought to exploit these events in order to build a negative image of the country in the West and incite internal conflicts within the Lithuanian society. In the field of the protection of the constitutional framework, the flow of negative information accounted for a quarter of total cases in 2019. When the verdict was due to be announced in the case of the events of January 13th, intensive disinformation activities were conducted against the Lithuanian legal system and the historical memory of the public. In the field of defence, the flow of negative information amounted to 23%: the aim was to reduce the country's confidence in the national defence policy and relations with NATO allies as well as to discredit the strengthening of the country's national defence capabilities in the region. The flow of harmful information in the defence sector intensified as Lithuania celebrated its 15th anniversary of NATO's membership in May, when the NATO military exercise *Spring Storm 2019* took place in the Baltic Sea.

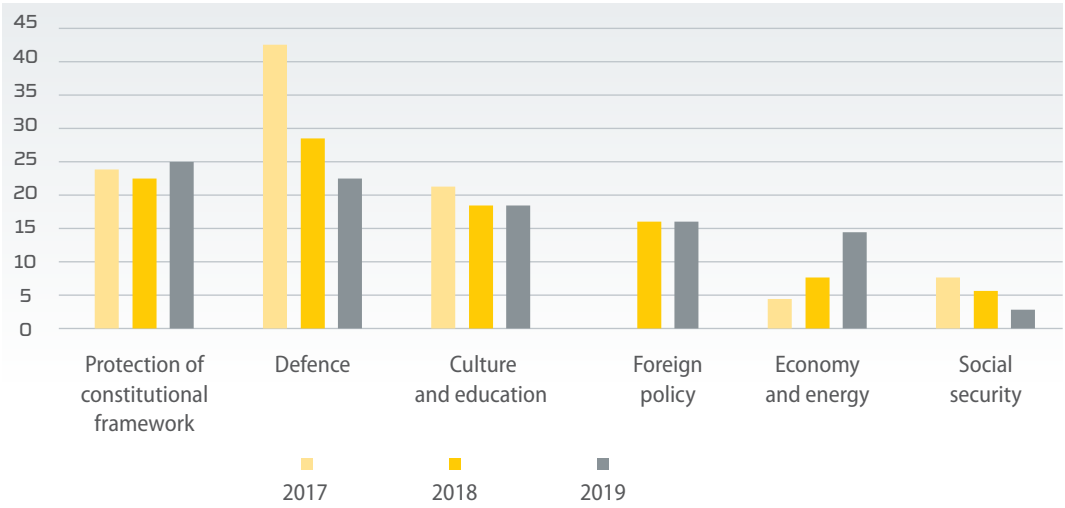

Fig. 23. Concentration of negative information in terms of strategic areas during the period from 2017 to 2019.

In the field of culture and education, a total of 522 (20%) negative information cases were identified. During discussions on the interpretation of World War II events, controversy was provoked over democracy and human rights in Lithuania, while the media outlets biased against Lithuania rushed to take advantage of it; the aim was to create the international image of Lithuania as a xenophobic, discriminatory and anti-Semitic state.

Active dissemination of information in the foreign policy sector was the result of certain national and international events: the meeting of the President of the Republic of Lithuania Gitanas Nausėda and the NATO Secretary General Jens Stoltenberg, the deployment of a battalion from the US 1st Cavalry Division in Pabradė and military exercises: *Baltic Protector 2019, Iron Wolf 2019* and *BALTOPS*.

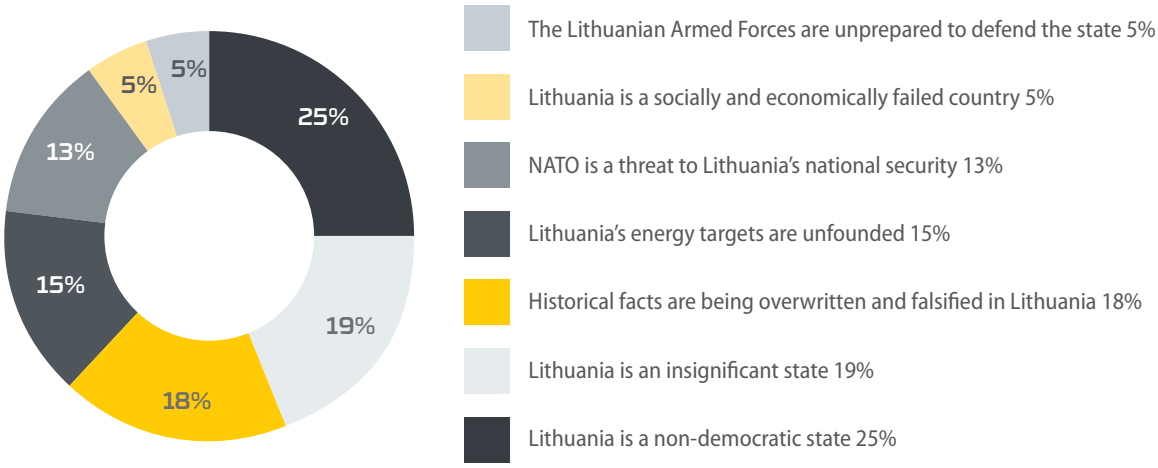

Fig. 24. Key narrative of information harmful to Lithuanian internet users in 2019.

In order to increase availability of harmful information, interested parties engaged in illegal cyber hackings into web pages by using other persons' or authorities' data and vice versa – by using provocative content that prompted Internet users to open a specific document or link; cyber practices were masked that aimed to harm the target users by trying to take over their devices or install malicious software.

One of the most prominent cyber attacks targeted a *Delfi* journalist, when someone using his name sent inquiries to Lithuanian and foreign countries' institutions and news agencies reporting alleged breaches of public order by NATO allies in Lithuania. One more disinformation attack was against the Kaunas Jewish community. Using the identity of this community's chairman, false reports about the alleged anti-Semitic crime, supposedly committed by the NATO battalion troops stationed in Kaunas, were distributed to the responsible services.

A cyber attack was also carried out against the MoD leadership, which spread false information about the Minister receiving a high-value bribe from the US officials. During the attack, at least several web pages were hacked and content discrediting the Minister was published; moreover, links were created to a web portal which was designed specifically for this case and imitated the website of the Special Investigation Service of the Republic of Lithuania, where a statement of false information was uploaded.

06

CONCLUSIONS AND RECOMMENDATIONS

CONCLUSIONS

01 The impact of cyber incidents is still underestimated in Lithuania.

Classification of cyber incidents by impact, which was approved by Resolution No 818 of the Government of the Republic of Lithuania, has allowed the NCSC to diversify and elaborate the cyber incident detection process. For this reason, the NCSC specialists handled almost three times as many cyber incidents of this type than in the previous year, i.e. 3 241. In addition, it enables to identify another challenge, i.e. their effects are underestimated. It is often thought that cyber incidents are insignificant. For this reason, there are other problems that the NCSC faces in its activities. Users in Lithuania are not yet inclined to use basic malicious software detection tools – commercial tools are not required in order to detect the malicious software which is most common in the Lithuanian IP range. Cyber security entities also tend to rely on typical cyber incident detection tools. However, the number of malware cases detected by the NCSC's technical cyber security measures has been decreasing. A wide range analysis of metadata (not just session level) has made it possible to detect a much more cases of malicious software compared to other critical service sectors. Underrated views on cyber security incidents can have significant consequences. The news website *https://kaunas.kasvykstа.lt* was exploited multiple times for cyber and information attacks in 2019. Another event, which received much more public attention, was the 2019 cyber incident of *UAB Kauno vandenys*. Insufficient attention to cyber threats, requirements and recommendations may have lead the data encryption virus to disrupt water supply in Kaunas.

02 Improving cyber security of the websites of the public sector does not change the significance of risk

In 2019, the NCSC increased the number of secure websites by 11% through direct communication with website owners in the public sector. However, Lithuanian websites those CMS were not updated on a regular basis increased to 63%. The NCSC also assessed the possibility of logging in to all ".lt" website management accounts – 37% of such sites were identified. Additionally, the NCSC has discovered a cross-site scripting vulnerability in the CMS of one manufacturer whose software is often used in the public sector. The NCSC estimates that as long as site owners do not have the resources to maintain their websites, make timely updates to the CMS and plugins, install website firewalls and use trustworthy cryptographic tools, the vulnerability of their websites will remain significant.

03 Formal implementation of cyber security requirements is increasing, but there are challenges in the implementation of practical measures to control cyber incident risks.

While monitoring the implementation of cyber security requirements, the NCSC has recorded a breakthrough in the realisation of CII owners' requirements. New NCSC audit capabilities have led to the finding that requirements are often formally implemented without actual risk control measures in place. Formal compliance and sporadic enforcement complicate the abilities of the entities to monitor anomalies, detect cyber incidents and, most importantly, ensure business continuity in the event of critical cyber incidents.

04 End users may be affected by cyber incidents regardless of vulnerabilities exploitation or malware.

Hardware and software research conducted by the NCSC has shown that users may suffer harm if they grant software excessive access to data or device functionality or if they purchase software or hardware whose data can be submitted to third countries that do not provide data protection.

05 Hybrid attacks cause the greatest resonance in the society.

The National Cyber Security Centre under the Ministry of Defence has continued to record hybrid incidents consisting of informational and cyber components.

RECOMMENDATIONS

The NCSC provides basic cyber risk management recommendations based on the cyber threats described in the report (Table 7). It should be noted that the recommendations are general. More detailed recommendations as well as free tools to detect possible threats are provided by the NCSC's website.[15]

Table 7. Basic recommendations for the management of cyber security risks

Recommendations for the management of risks related to social engineering		
№	Threat	Recommendation
1	**The user will click on the link leading to the malicious page.**	Hover your cursor over the link and check if the displayed website address is real, make sure that the address is free of grammatical errors and that the title is logical and easy to read.
2	**The user will enter his/her password on a fake website.**	Make sure that the session with the site is encrypted, i.e. SSL certificate is used (https tag is required for the web address) as well as multi-factor authentication tools (e.g. password, mobile device, fingerprint).
3	**The user will reveal his/her credentials to the hacker.**	Use at least two-factor authentication, keep your login credentials secure and in no way keep them as clear text at your workplace, on your computer or mobile phone.
4	**The user will make a money transfer to the hacker.**	Critically evaluate advertisements on the Internet and in e-mails (especially those offering large discounts); verify your money transfer requests by other means (e.g. with phone calls).
5	**The user will install malicious software.**	Do not open the contents of documents, uploaded files and software that are downloaded from untrusted sources (such as illegal sources of software distribution).
6	**The user will fall victim to malicious manipulation.**	Do not make quick decisions, do not give in to emotions, find out in detail the necessity of the actions requested.

[15] https://www.nksc.lt/rekomendacijos.html, https://www.nksc.lt/irankiai.html

Recommendations for the management of risks related to harmful software		
7	**Making use of a vulnerability, a hacker will install malicious software in the CIS.**	Use legal OS and software, including anti-virus software, scan data on the device on a regular basis and immediately install new software updates.
8	**The user will download malicious software.**	Do not download files from untrusted sources, install plugins to detect malicious websites in your browser, scan suspicious files with antivirus software and check them with the tools proposed by the NCSC.[23]
9	**Malicious software will run automatically from the infected storage media.**	Do not use unreliable, untested storage media. Format them regularly, disable auto-play of files and allow the antivirus software to scan them before opening files on the media.
10	**Malicious software will encrypt data on the user's computer.**	Periodically back up your data and store it on another device, separate from where it was made. Store important information on separate media or media that does not have a direct connection to the Internet (such as external media).
11	**Malicious software will allow a hacker to access confidential information.**	Encrypt confidential information and, if necessary, protect it with a secure password. Use cryptographic techniques such as e-mail encryption to transmit the information safely.
12	**The computer will be infected through the CIS network.**	For offices, use network segmentation and multiple filtering tools (such as network and server firewalls) to physically separate important CIS.
Recommendations for the management of risks related to cyber security in websites		
13	**The hacker connects to the CMS through a user or adminis-trator account.**	Change login addresses for the CMS administrator and users of the website, enable login by IP addresses, change passwords on a regular basis, create a limited number of login attempts.
14	**The hacker exploits vulnerabilities of the website.**	When purchasing website programming services, include the requirement for site code verification according to the Open Web Application Security Project (OWASP) methodology in your purchase specification. Regularly update the OS of the server, the CMS and related plugins, do not use unnecessary plugins in the CMS, use application firewall, ban unused ports, check web site vulnerabilities using regularly available logging tools and implement a reverse proxy solution to prevent the hacker from identifying the CMS.

15	**The hacker installs malicious software on your website.**	Configure firewalls so that the CMS can only connect to websites from trusted IP addresses (create a list of allowed IP addresses).
16	**The host does not provide cyber security measures for the website.**	When purchasing website development, hosting and maintenance services, include in the contract a requirement for the service provider to ensure the cyber security, hacking protection of the website and compliance with the governmental, organisational and technical cyber security requirements.
17	**During the connection to the website, information is intercepted, connection traffic is interfered, user data and/or login credentials are intercepted.**	Using HTTPS protocol to access the website will ensure encrypted communication. It is one of the most effective cyber security tools for the websites.
18	**Website access is impaired.**	Use an application firewall, order more bandwidth, purchase additional services that prevent the DDoS, for example, from a website hosting provider.
Recommendations for the management of risks related to intelligence in electronic communication networks		
19	**The hacker identifies active services and devices.**	Change device ports to less used ones, disable unused ports, enable a reverse proxy to prevent external identification of the active services and hardware or software.
Recommendations for the management of risks related to hardware or software reliability		
20	**Data leakage and/or service disruption.**	It is recommended to purchase hardware and software only from official sources and suppliers that operate under the General Data Protection Regulation and store data in NATO or the EU countries, to limit hardware or software functionality and access to information and services (e.g. disable your smart phone's functionality to record audio or activate camera and prevent any technological network from connecting to the Internet in your organisation).
21	**Spyware.**	It is recommended to purchase hardware and software from sources that are of good repute and do not pose a risk related to cooperation with non-NATO and non-EU foreign intelligence services.
22	**Unauthorised technological network interface with the Internet.**	Provide limited CIS access for contractors, avoiding remote CIS access; monitor and audit communications logs.

23	**A standard password can be used to log into the device.**	Change the login credentials for the IoT devices over the Internet or via Bluetooth interface to secure ones.
24	**The device is accessed through a non-protected vulnerability.**	Update IoT applications and software on a regular basis.
25	**The hacker can see passwords and other sensitive infor-mation stored by the user.**	Disable password storage in IoT devices.
26	**The hacker may intercept information or passwords during communication between devices.**	Purchase and use devices whose communication sessions are encrypted.
27	**The hacker takes advantage of excessive device functions to gain access to CIS.**	If possible, check your device for excess functionality (open ports).
28	**The device communicates with the outside and, possi-bly, is leaking information.**	Before purchasing a device, make sure that the manufacturer of the device meets the requirements of the General Data Protection Regulation and that the data transmitted is protected by the EU law.
29	**An unsafe device is being purchased.**	Avoid unknown manufacturers those origin and reliability are difficult to verify.
Recommendations for the management of risks related to DDoS cyber incidents		
30	**Depleted resources will disrupt CIS availability.**	Monitor the resources of servers, clusters, applications and databases on a regular basis, highlight the critical elements, perform user-driven (externally) monitoring and, if necessary, increase bandwidth, acquire additional resources. Use routers with *traffic-shaping* and *rate-limiting* functionality.
31	**A direct DDoS cyber incident will disrupt CIS availability.**	Purchase anti-DDoS services from internet service pro-viders. Purchase firewalls with anti-DDoS functionality, use web application firewalls. When possible, intrusion detection and prevention systems may be also used.
32	**Exploiting infrastructure to execute attacks (e.g. rein-forcing DDoS attacks).**	Monitor network traffic (source and destination IP addresses and ports) and analyse logs to determine if infrastructure is being exploited for DDoS attacks. Keep your software updated.

Annex

Annex 1. Evaluation of cyber security status of public sector websites

Bedore 2018, the status of public sector websites was evaluated on the basis of individual vulnerabilities, regardless of the overall level of vulnerability. In 2019, the NCSC holistically evaluated the cyber security of public sector websites in terms of vulnerabilities per domain. For example, a website with two vulnerabilities for different exploits was ranked according to the threat of the most exploitable vulnerability (for example, if a website has two vulnerabilities that are qualified as "easy to hack" and "difficult to hack", then the qualification is treated as "easy to hack"). The NCSC also assessed that some vulnerabilities are unqualified – there is no clear information as to whether there are sufficient tools to exploit them or if certain expertise is required to do so. By this method, the NCSC recalculated the study results of 2018 (Fig. 25).

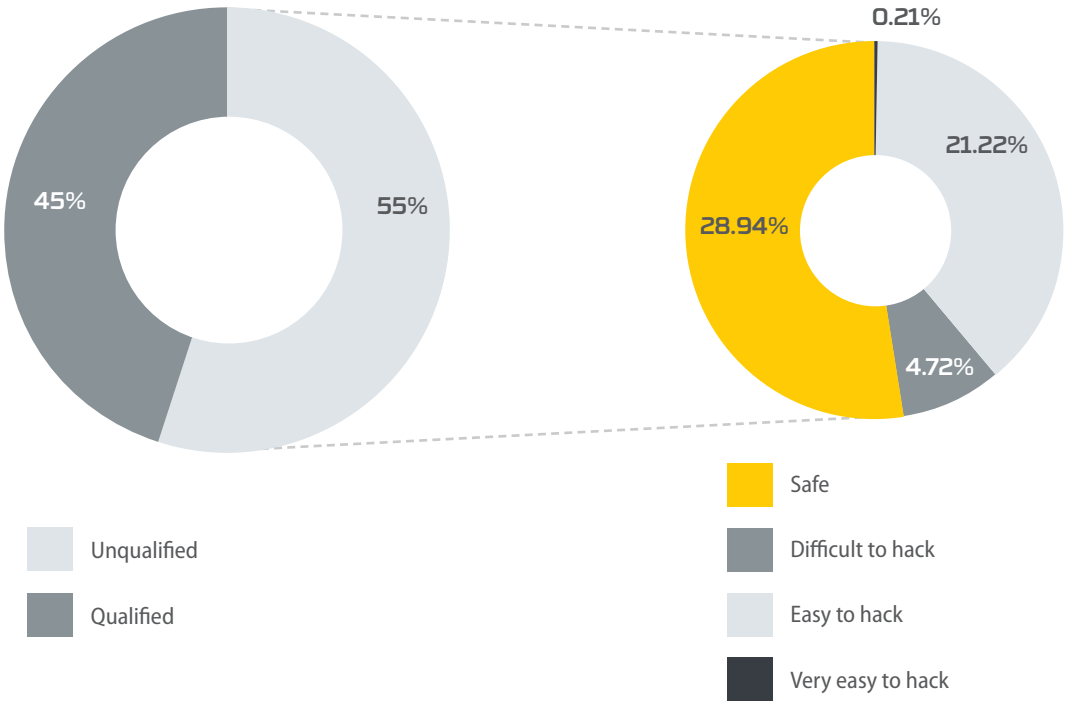

Fig. 25. Cyber security status of public sector websites by domain vulnerability qualification, 2018. [16]

According to the updated assessment of cyber security status of websites, the NCSC found that the number of websites whose vulnerabilities can be classified increased in 2019, while the total number of secure websites grew to 40% (Fig. 26).

[16] **Very easy to hack** – technical knowledge or special programming skills are not necessary for the hack. In order to carry out a successful attack, the required algorithms are acquired easily and the instructions for the actions needed are easily found online.

Easy to hack – the skills and knowledge required for the hack are usually published in closed groups.

Difficult to hack – hacking requires the expertise of qualified professionals, often multiple attackers, as vulnerabilities are not yet publicly disclosed.

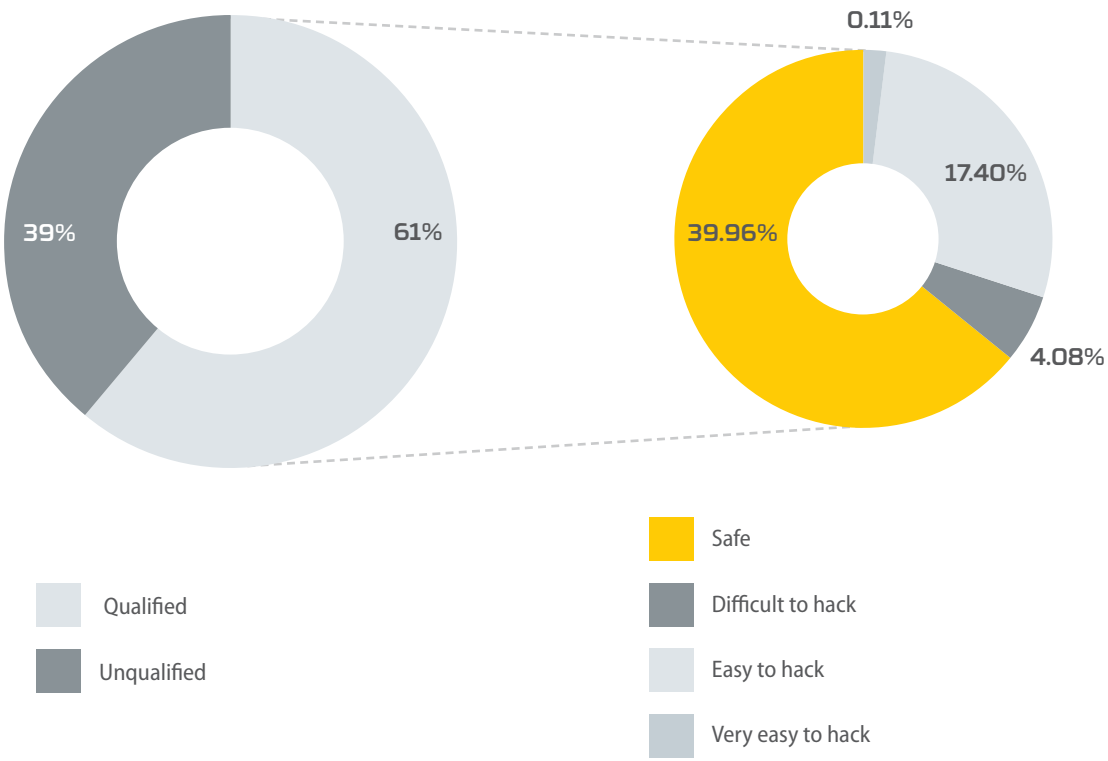

Fig. 26. Cyber security status of public sector websites by domain vulnerabilities, 2019.

National Cyber Security Centre under the Ministry of National Defence
National Cyber Security Status Report 2019
Translation Public Special Education and Counseling Center
Translation: Jurgita Benaitytė
Circulation: 500 units. Order GL-14.
Ministry of National Defence of the Republic of Lithuania,
Totorių str. 25, LT-01121 Vilnius.
Layout by the Visual Information Section of the General Affairs Department of
the Ministry of National Defence, Totorių str. 25, LT-01121 Vilnius.
Printed by the Military Cartography Centre of the Lithuanian Armed Forces,
Muitinės str., Domeikava, LT-54359 Kaunas District.