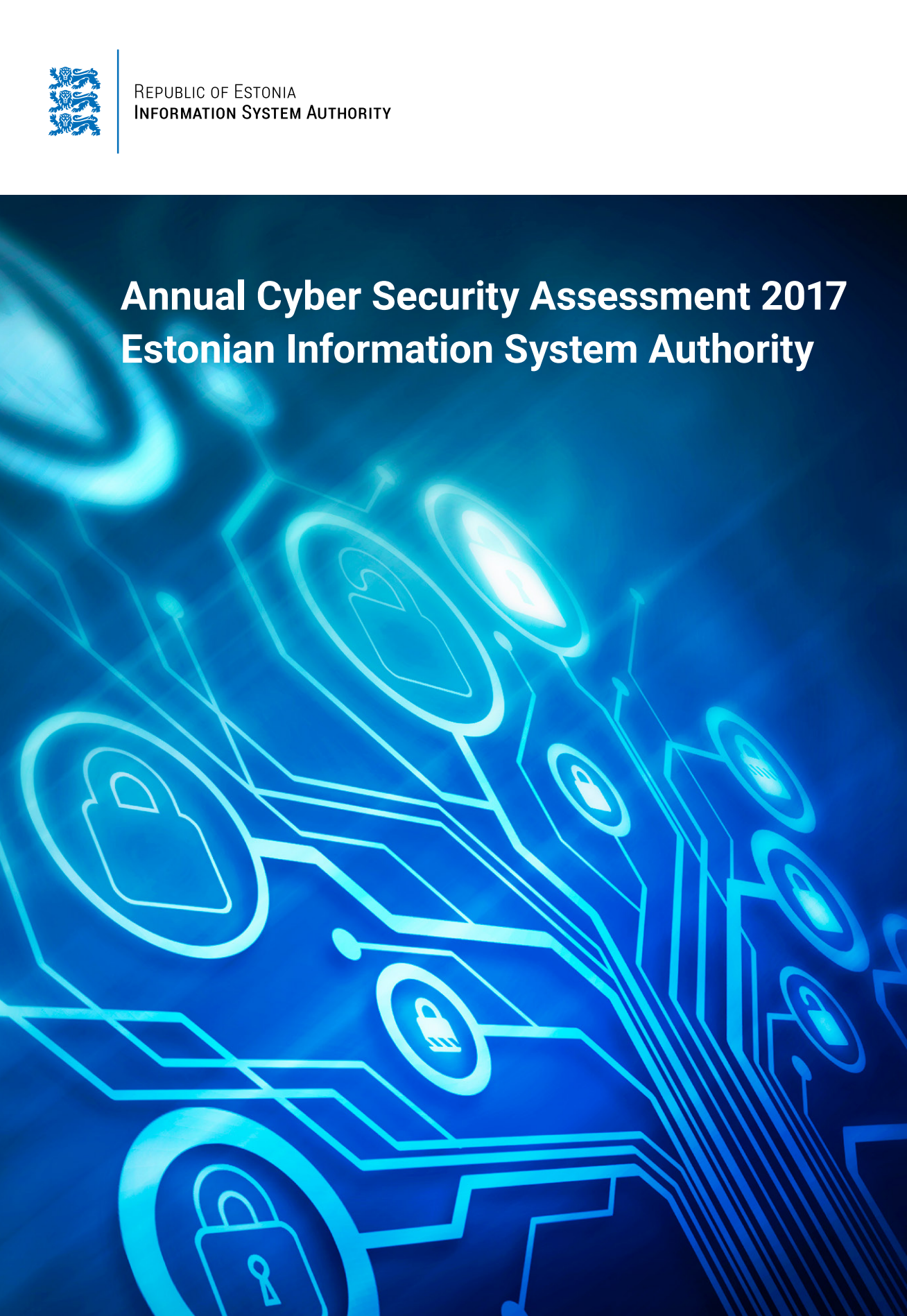

Republic of Estonia
Information System Authority
Annual Cyber Security Assessment 2017
Estonian Information System Authority

Annual Cyber Security Assessment 2017
Estonian Information System Authority

About the Estonian Information System Authority

The Estonian Information System Authority (RIA) is a governmental agency that fosters and protects Estonia's digital society. Operating under the Ministry of Economic Affairs and Communications, the organisation is tasked with the development and administration of Estonia's state information system and the coordination of national cyber security, including cyber incident response, emergency preparedness and management, regulation and supervision.

RIA is responsible for Estonia's e-government platform, including national eID infrastructure and the data exchange layer X-Road. The agency also provides data communication and Internet services to state agencies and local governments.

Contents

Foreword. Cyber security depends on every one of us

This April marked the tenth anniversary of the cyber attacks that hit Estonia in 2007. Although the attacks were relatively unsophisticated and the consequences were limited, they ultimately had a more significant impact than anyone could have imagined at the time. The attacks prompted the first serious public discussion on the possible impact cyber attacks could have on national security, and the classification of cyber attacks as a means of warfare rose on to the agenda. Most importantly, the public began to realise that the malicious use of "bits and bytes" in cyber attacks could have spillover effects on everyday life in the so-called real world: people can't read the news, online banking sites are down, and social media channels – now a everyday means of communication – are not accessible. The attacks also boosted Estonia's reputation as an advanced digital society and among the world leaders in cyber security.

Ten years on, it is clear that the decisions made by Estonia in developing its cyber security sector were, by and large, the right ones. The country's current cyber security is bolstered by high-functioning e-government infrastructure, reliable digital identity, a system of security measures that is obligatory for all government authorities, and a central system for monitoring, resolving and reporting cyber security incidents. The most important element of all is likely the common understanding that cyber security can only be ensured through cooperation and that a joint contribution is required at all levels – state, corporations and individuals. The events of 2007 were resolved in cooperation: a "collective brain" consisting of state and private sector data security experts acting in concert was able to repel the attempted attacks and helped to develop an action plan for the coming years – one we have been able to follow to this day.

Cyber security cannot be ensured by the state alone. Even large countries would be unable to do so, because the internet is not controlled by states. The success of efforts to ensure cyber security depend just as much on intergovernmental cooperation as on cooperation of governments with internet service providers and organisations that ensure the operation of the internet.

2017 is the final year covered by Estonia's cyber security strategy

2014–2017, the second such strategy Estonia has developed. Cyber security has now become indisputable, a fact of life. In the last ten years, Estonia has not suffered any cyber incidents that caused major disruption of everyday life in society.

Yet the functioning of the Estonian state and society is more dependent than ever on cyber security. Amidst a worsened international security situation, foreign governments' special services have become more active in cyber espionage and preparing cyber attacks. The communication networks of Estonian government institutions are "cased" constantly – probed and mapped to check the capability of Estonia's communication systems – and attempts are made to hack into computer networks of vital service providers. However, attacks by cyber criminals pose an even greater risk to everyday security: by spreading crypto-ransomware in its lust for ill-gotten gains, organised crime can even put people's life and health at risk. Frequent attacks on hospitals can, in the worst case, deprive patients of medical care. Even the best information technology systems and the most competent cyber security teams cannot completely prevent such attacks. Such attacks succeed only if the attackers find a computer or device user who is unaware of the risks or who is careless.

Cyber security depends on every one of us. The ability to operate in a secure manner and to correctly assess risks in cyberspace is the key to ensuring cyber security at the individual, community and state level. The only effective cyber defence is comprehensive defence – an effort that requires a contribution from everyone. I hope that every reader of this publication will discover good insights on how they can improve cyber security in their own lives, the organisation they work for, and all of society.

Toomas Vaks
Director of Cyber Security
and Head of Cyber Security Branch
Estonian Information System Authority

Cyber security review: 2016 in Estonian and international cyberspace

Introduction

Cyberspace plays an increasingly important role in the functioning of relations between individuals, the business community and NGOs. Fundamental rights and freedoms cannot be realised separately from the environment in which people operate. The smooth and secure functioning of IT systems therefore directly impacts opportunities for individuals to exercise their rights and freedoms, as well as the functioning of the business environment and civil society as a whole. The security of a country's digital environment is thus a part of national security.

Developments in international cyberspace are increasingly complex and it is difficult to delimit the impact of cyber threats to clear areas or actors. 2016 will be remembered for a number of unprecedented cyber incidents around the world. We saw one country attempt to influence the electoral process in another country, and witnessed power outages caused by cyber attacks on electrical grids. We saw how the internet of things – devices and home appliances connected to the net – was exploited to attack fundamental services of the internet, the effects of which transcended national and continental borders.

Estonia is not immune to developments in the international environment and there is no reason to expect global trends in cyberspace to pass us by. At the same time, Estonia has specific strengths, vulnerabilities and interests in the cyber environment that stem from the choices made in developing its digital state and from the role that information and communication technology plays in functioning of society. As a result, in this year's annual report from the cyber security division of the Estonian Information System Authority (RIA), we will discuss

the incidents that took place in Estonia and the rest of the world and the trends in cyber security for the people living in Estonia and the Estonian government. The purpose is to convey to readers an understanding about the threats we face, what sorts of risks must be considered, and how to protect ourselves better.

Just as cyber security is an issue no one should be ambivalent about, this annual cyber security report is also meant for the public in the broadest sense. Some of the risks in the digital environment affect every computer user; others pertain only to those in specific fields. We refrained from covering solely general interest topics and the other extreme, solely specialist topics – cyber security is just as an intertwined and multifaceted challenge as shown by the issues covered. The publication is thus meant to offer food for thought for individuals and staff, managers and IT specialists in the public, private and third sectors so they could be aware of the risks and take steps to improve their security.

RIA's annual report on cyber security is divided into two parts. The first focuses on assessing the threats to Estonian cyber security – we cover last year's cyber incidents and the threats and vulnerabilities currently faced by Estonia. In the second part, we will look at RIA's main activities for increasing cyber security in 2016 and which were not covered in the threat assessment.

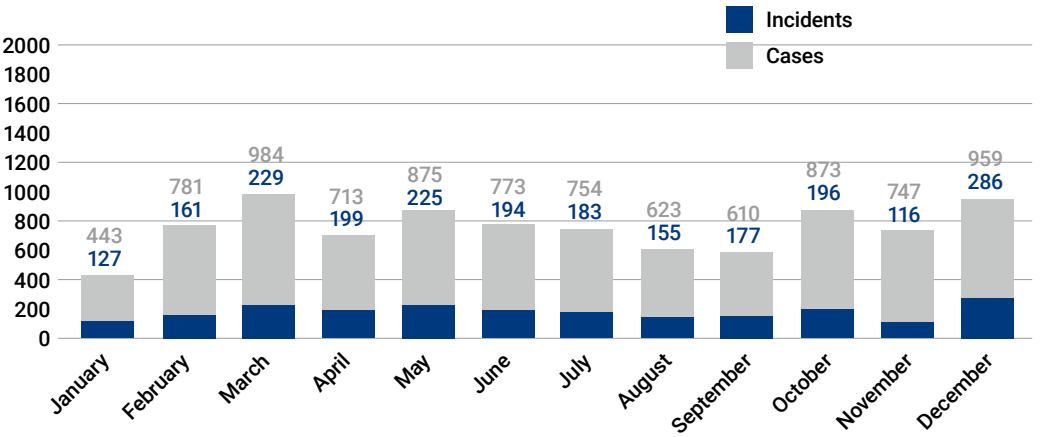
2016 incidents in Estonian cyberspace

CERT-EE (the Computer Emergency Response Team of Estonia), the department at RIA that responds to security incidents in .ee networks, handled 9,135 recorded cases last year in Estonian computer and data communication networks. Of these, 2,248 – about one-fourth – were found to be cyber security incidents, meaning that they directly impacted the confidentiality, integrity or availability of information or systems.

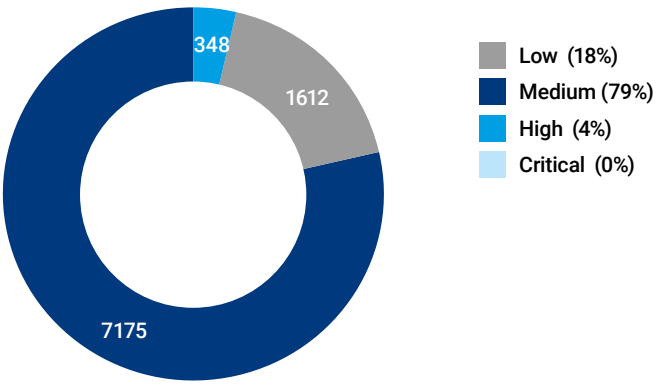
Information on cyber security incidents reaches RIA in one of two ways: partner institutions or the persons affected notify us, or CERT-EE discovers potential cyber incidents in the course of monitoring.

There were no critical cyber incidents that would have posed a threat to people's life or health in 2016. However, there were 348 high-priority incidents that affected the functioning of a service or website considered important for the state. This also includes interruptions or attacks against vital service providers' information systems. RIA responds to high-priority incidents immediately, as the incident often needs to be resolved or the attacks must be halted in a matter of minutes.

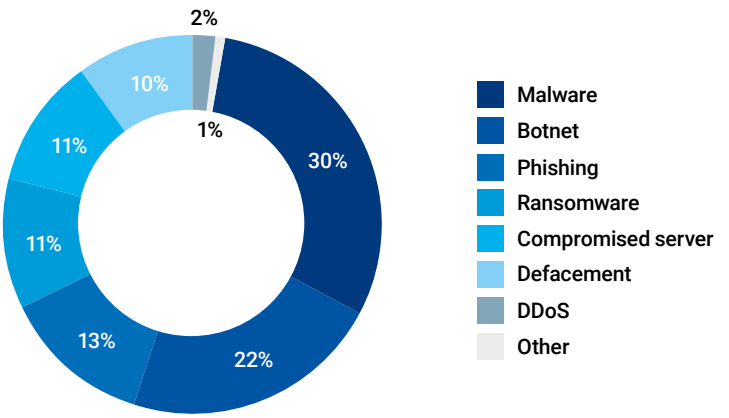
Cases and incidents by month in 2016



2016 cases by priority



2016 incidents by category



Pervasive cyber threats

Cyber crime and influence operations conducted by foreign countries still top the list as the most important cyber threats for Estonia's population and state. The user of any internet-connected device is potentially a target for global cyber crime, either through a fraud attempt or a device hijacking in order to attack other persons or connections. Ignorance or carelessness of computer users, coupled with a security weakness in a service or institution, can cause a monetarily measurable loss, and could also create the possibility of an attack on vital services or government functions.

E-mails and web domains that spread malware made up the largest share of the cyber security incidents registered in Estonia in 2016. This category was followed by reports of devices infected and hijacked by botnets, and, with more or less with the same frequency, phishing attempts, ransomware incidents, and incidents related to compromised devices and defaced websites. A large share of the incidents is directly or indirectly caused by use of outdated software. Threats related to emerging technologies and services deserve separate treatment, as last year's trends make it evident that these will increase in frequency.

Ransomware is increasingly sophisticated and poses a threat to vital services

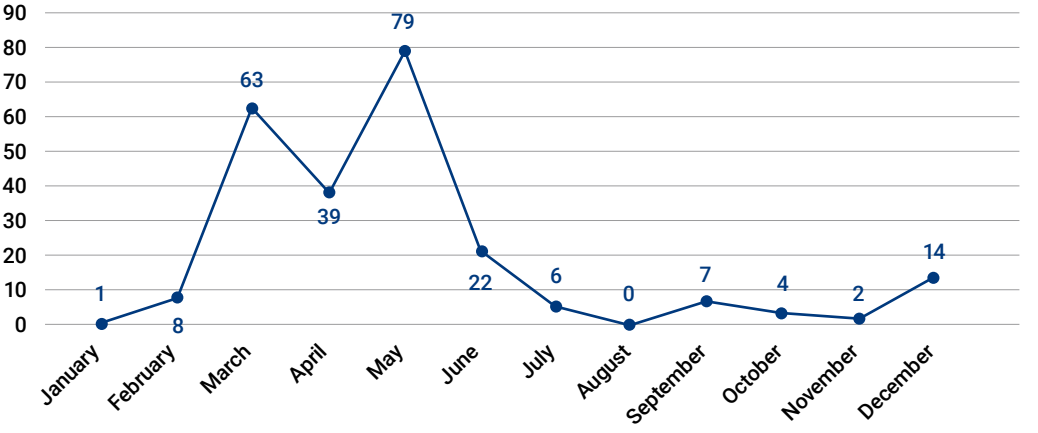
Among the cyber threats that received the most coverage in 2016, both in Estonia and elsewhere in the world, was ransomware spread through e-mails and websites. In typical ransomware cases recorded in Estonia last year, e-mail was sent to one specific recipient, generally did not contain significant spelling and grammar mistakes, and had an attachment consisting of an invoice, CV or other document that appeared outwardly

BOTNETS AND THEIR ROLE IN ATTACKS

One-fifth of the cyber security incidents that required a response in 2016 involved botnets. A botnet is a computer network consisting of "zombie" computers – devices that unbeknownst to the user have been compromised – and which are used for mounting cyber attacks such as spamming or distributed denial-of-service attacks.

Information on the devices used as infrastructure for such cyber attacks reaches RIA through reporting by partner institutions in other countries and through its own constantly improving monitoring capabilities. The majority of devices taken over by the botnet are computers that were not kept properly updated with security patches. Where such devices are discovered, the device owner is sent a notification in cooperation with internet service providers, informing the user that they need to re-establish control of the compromised device to keep the attacks from continuing.

Ransomware incidents 2016



authentic. There were even cases where such a message appeared to have been sent by a legitimate institution such as the Tax and Customs Board, using a service that makes it possible to spoof the sender's address.

When the attachment is opened, the file encrypts the files on the computer and, if there is access to the network drive, the latter as well. The computer user then is given instructions for paying a ransom for getting the key needed to decrypt the data. Failure to pay the ransom on time runs the risk that the data will remain encrypted. A user without a backup copy of the data thus faces a choice: pay the criminals or lose their data.

The peak of the ransomware incidents was in spring, but variations on the scheme were seen all year, and continue as of this writing as well.

"Career" criminals are often responsible for spreading ransomware, and since their income depends on how professionally they go about their schemes, the e-mail messages are often carefully composed and seem legitimate. The e-mail sender also takes advantage of the functioning of the organisation's ordinary work processes – for example, the sending of invoices by e-mail. To circumvent antivirus software, new versions of the ransomware are developed. It is thus not always possible to avoid becoming infected. Consequently, it is all the more imperative that users be aware of the dangers posed by ransomware and act in a responsible manner when using personal and work computing devices.

It is essential that institutions practise judicious IT management and system administration policy and make backup copies, especially if business-critical functions or vital services are at stake. Last year unfortunately included a number of examples where administration errors compounded ransomware infections at the organisation level. In several cases, the infection spread from one user's workstation to the entire organisation's information system because

that user had been assigned higher privileges than they should have been entitled to.

Attacks where critical or vital services are targeted – healthcare and the energy supply are examples – are especially dangerous. Such services often depend directly on the availability of time-critical data – in such a case, criminals tend to presume that it will be easier to get the ransom payment in the case of a successful attack and thus exert efforts to make sure the attack succeeds. The e-mail used as the cover for the ransomware might be written to seem as plausible as possible for that specific establishment. During 2016, there were 12 incidents of ransomware infections at vital service providers in Estonia. The objective of such attacks is generally criminal in nature, but ransomware can also be used to undermine national security.

RECOMMENDATIONS

Users

- Don't open attachments and links if you aren't certain that they are from a trusted source. Seek out an IT specialist or user support at your organisation. Forward suspicious e-mail along with headers and attachments to cert@cert.ee (or upload it to https://paste.cert.ee), then delete it immediately on your own system.
- Don't pay the ransom. That only supports criminals and doesn't guarantee that you will recover your data. Even if you don't have a way of restoring your files, keep your infected hard drive: in general, a way to recover data emerges sooner or later.
- The best protection against ransomware is a backup copy. If you don't know how to make a backup copy of the contents of your computer or device, contact user support at your organisation or an IT specialist.

CIOs

- Avoid use of out of date software and keep your anti-virus program regularly updated.
- Partition your hard drives, and give users only the access privileges they actually require.
- Arrange for regular backups of data – we recommend an up-to-date backup copy that is independently stored in at least three copies and using at least two different technologies, with at least one copy stored in a physically different location.

Organisational management level

- Be aware of the impact that cyber threats have on your organisation's main activity and the services your organisation offers. Develop a cyber security policy to mitigate the risks.

CONCLUSIONS

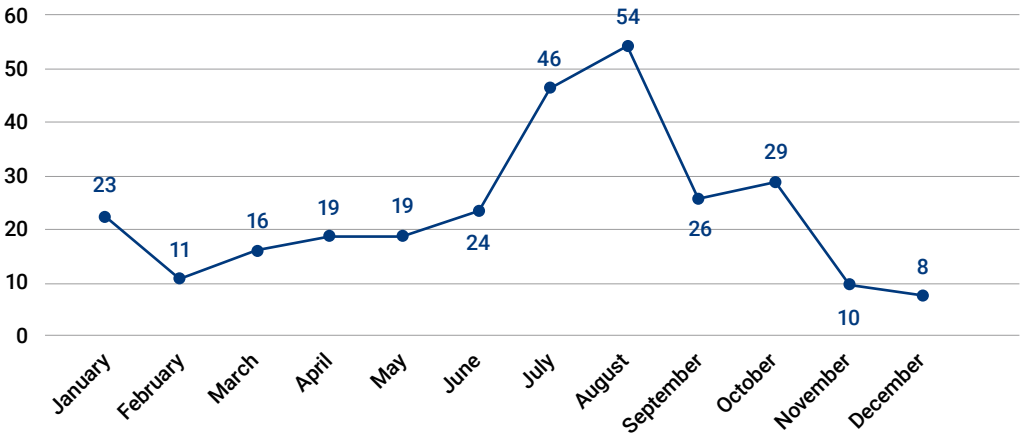
- Estonians' awareness of crypto-ransomware has risen, thanks in part to CERT-EE's publicity efforts and media coverage. Yet it is human nature to take the path of least resistance and so changing behaviour will require a continuing effort.
- The knowledge of IT personnel at organisations has improved when it comes to harm prevention and remediation. However, the pattern of recurring incidents, at health care institutions in particular, is still a cause for concern. The recurrence of near-identical incidents shows that the management at organisations is not sufficiently aware of the risks related to public servants and employees' activities and their actual impact on the services provided by the organisation.

Phishing attacks target money and sensitive data

Every year, one of the most widespread cyber threats has been phishing – a scam where users are induced by various means into entering data for their e-mail account, online payment site or other services on websites that spoof legitimate sites. Phishing attempts are also seen on social media, especially Facebook.

In previous years, phishing e-mails were easy to see through – they seemed implausible, spelling errors were rife – and users now know enough to be suspicious about such requests. However, we are now more frequently seeing sophisticated use of social engineering where a serious effort is made to appear genuine and where the users' curiosity, fears or empathy are directly exploited. Examples include fake e-mails warning users that account limits have been reached or notifications on Facebook that their friend has posted a picture or video of them. In all of these cases, the pattern is the one and the same: some pretext is used to direct the user to a fake landing page, where the user name and password they enter fall into the hands of criminals.

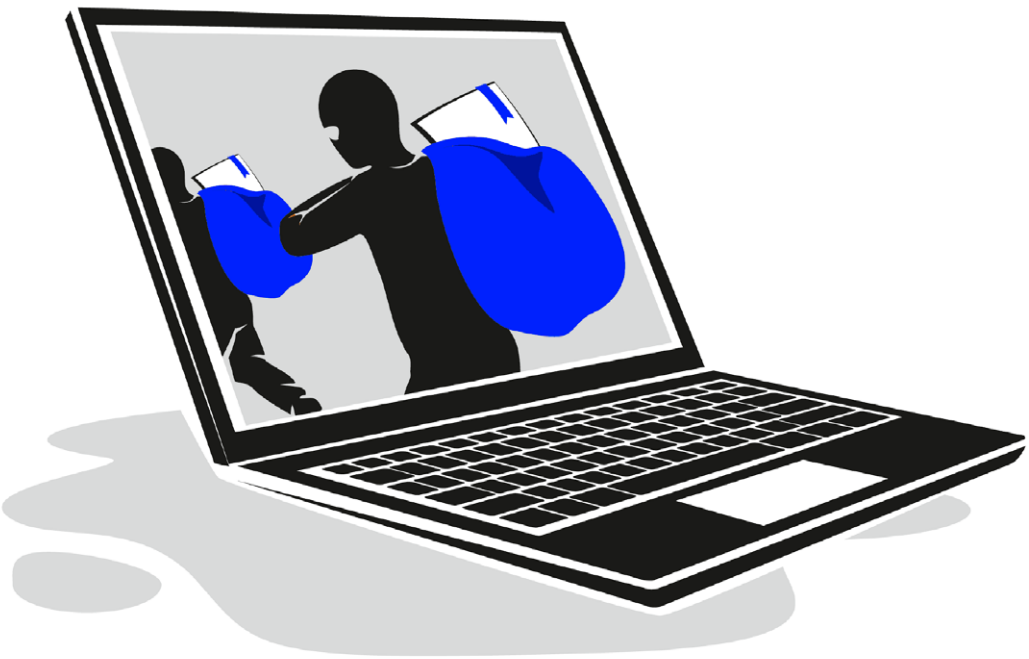
Phishing incidents 2016



To seem more plausible, such emails are also sent in such a manner to appear to be from Estonian service providers. There are examples where an e-mail warning that an account was about to be blocked was ostensibly sent by an Estonian communication service provider. An example of a concerted, targeted campaign was an incident from June 2016 where phishing messages purporting to be from the Tax and Customs Board were sent. The recipients were redirected to a page that imitated the official website. Users were prompted to enter their credit card information in order to receive a tax refund. None of the recipients are believed to have fallen prey to this specific attempt, yet reports sent to RIA every month of successful phishing attacks suggest that it is often not that easy for users to tell that an e-mail is spurious.

The landing pages for the phishing scams are mainly located outside Estonia. With its partners and Estonian service providers, CERT-EE has engaged in continuous cooperation for the rapid detection and removal of phishing pages. The result is that the number of phishing attacks targeting people living in Estonia has dropped significantly.

In September, fraudulent e-mails engineered to target specific recipients and produced in a professional manner were received by public sector and government institutions. Some of them also targeted the private sector. The e-mails, purporting to be from directors general of government authorities, and even from the prime minister, were sent to accountants at the institutions, and attempted to



defraud them of sums up to 35,000 euros, which were to be sent as bank transfers. No actual transfers were made in the public sector, although in some cases in the private sector, money was sent.

The "stranded traveller" phishing scam is also still a standard part of the repertoire, and is sent to contacts or address list of a hijacked e-mail account.

The motive behind the various types of phishing attacks is generally criminal gains, but other objectives can include access to monetarily valuable or sensitive data, or to persons that could, in future, be exploited to steal valuable information. An example of such a motive could be conjectured in a spring 2016 campaign to phish for information from users in the national defence sector. The landing page resembled a webmail login page that had formerly been in use.

All too often, the damage is not limited to just one account being compromised. Since there are many digital environments and human memory is finite, it's all too common for users to use the same password for different services and environments, and one stolen username and password can often unlock more than one user account.

Users are generally aware of phishing risks, but have trouble applying their knowledge in a practical situation, where phishing methods are constantly improving, changing their cover story or "bait", and varying the channels used to deploy the bait. Because of this, in 2016 CERT-EE strove to consistently keep the public up to date on the new changes in phishing threats and the spread of phishing methods. RIA's partner institutions and media outlets have made a praiseworthy effort to raise public awareness.

RECOMMENDATIONS

Users

- Before you type in a password or username, make sure you are on the actual page for that service provider. If you have any suspicion regarding the web address in the address bar, it's imperative that you don't enter your data. If you've already entered your password, change your password immediately.
- Don't send any money or respond to phishing e-mails. If a letter asking for money appears to have been sent by a friend, call the friend and ask whether they really do need help. If you have already sent money to the phishing e-mail sender, get in touch with the police (cybercrime@politsei.ee) and hold on to your correspondence with the fraudsters.
- Turn on two-factor authentication, if you have it – especially for e-mail accounts. RIA publishes instructions for this on its blog (in Estonian).
- Report suspicious addresses or phishing e-mails to cert@cert.ee.

Organisational management and CIOs

- Don't use shared accounts, where multiple employees enter the same account in alternating fashion using the same username and password.
- Keep employees' personal and work e-mail accounts separate and institute proper password policies.

A FEW IMMUTABLE AND UNIVERSAL TRUTHS OF CYBER SECURITY

1. If you connect it to the internet, someone will eventually try to hack it.
2. If what you put on the internet has value, someone will invest time and effort to steal it.
3. Even if what is stolen does not have immediate value to the thief, he can easily find buyers for it.
4. The price he secures for it will almost certainly be a tiny slice of its true worth to the victim.
5. Organisations and individuals unwilling to spend a small fraction of what those assets are worth to secure them against cyber crooks can expect to eventually be relieved of said assets..

Source: Brian Krebs*

* https://krebsonsecurity.com/2017/01/krebss-immutable-truths-about-data-breaches/

CONCLUSIONS:

- Phishing techniques and methods are getting better all the time. It is becoming harder to distinguish spurious e-mails from authentic correspondence, as the scammers hijack real people's accounts and target their personal contacts, or e-mails purport to be from an actual service provider familiar to the user. Phishing plays on users' curiosity, profit motive, fear or empathy.
- The motive behind most phishing attacks is money. E-mails phishing for sensitive information are considered high-risk, as the attacker's intentions are not limited to gaining access to a single account or service – they are looking to use them as a springboard to other accounts. Herein lies the hazard of cross-platform use of the same password – attackers can often gain access to other services as well.

Out of date software is the cause of most registered cyber incidents

An eternal problem that was in some way behind most of the cyber incidents registered in Estonia in 2016 was out of date software – whether it was carelessness or ignorance that led to the failure to update it.

A standardised software solution developed for a large user base is generally both convenient to use and secure, because any security holes that appear during use are addressed quickly by version updates. On the other hand, criminals are well aware of the vulnerabilities of standardised solutions and if software is not kept updated, there is a serious risk that the weaknesses and vulnerabilities will be exploited for data theft, spreading malware or DDoS attacks against third party services. Especially inviting targets for would-be hijackers are web-based services that are used to conduct actual monetary transactions and send information with monetary value (such as credit card data). Exploiting these types of vulnerabilities is often a basis for a whole criminal "sector".

As of last year, over 20% of Estonian web pages administered using WordPress content management software – also in wide use in Estonia – had not been

updated to the latest version. The situation with the Joomla platform was even worse – close to 85% of the pages were running an out of date version.[1] The price of ignorance or inaction on the part of the website owner is not just their own vulnerability to attacks, but the fact that visitors to the pages can also be infected with malware. Under Estonian law and service agreements, communication service providers have the right to restrict service to customers if their action (or lack thereof) poses a threat to the functioning of the service and other users.[2] When necessary, Estonian service providers have done so to protect network security and integrity.

An example of how out of date software can lead to actual financial losses to a service provider's customers occurred last year, when an older version of Magento, an e-commerce platform widely used in Estonia as well, had a security hole that allowed users' credit card data to be stolen. Even after a patch for the problem was released, thousands of online stores around the world, including about a dozen Estonian online retailers, continued using the vulnerable version. CERT-EE contacted all of the online retailers affected and provided instructions on how to fix the vulnerability. It is not known whether any of the clients of the online stores sustained actual losses, as people in Estonia tend to pay for online purchases by clicking on a link to their bank's online site. But online shopping is gaining in popularity in Estonia, and Estonian users will certainly not always remain unscathed.

1 CERT-EE monitoring data as of late October 2016.
2 Section 98 of the Electronic Communications Act.

CONCLUSIONS

- Out of date and unpatched software is either directly or indirectly behind most cyber incidents in Estonia.
- The use of out of date content management software is epidemic. The price of ignorance or inaction of the webpage administrator is not just their own vulnerability to attacks, but the fact that visitors to the pages can also be infected with malware. Operators of websites that have become a hazard should bear in mind that user access to the website may be restricted in order to protect the network and other users.

RECOMMENDATIONS

- Install software updates immediately after a new version or patch is released.
- Check the RIA website and social media channels for regular posts from CERT-EE about new security patches and newly discovered vulnerabilities.

Risks related to emerging technologies and services

Around the world, cyber threats related to emerging technologies and services are an increasingly relevant topic. The range of use for smart devices and the internet of things is widening and their security risks now have an impact on previously unaffected areas. One example was apps leaking extensive

sensitive consumer health information, which was covered in the international press late last year; or the disclosure of Ukrainian national defence information to the adversary via malware implants in mobile devices.[3] Distributed denial-of-service (DDoS) attacks that exploit internet of things devices are also becoming a bigger headache – the number of such attacks is increasing and there are no effective ways to prevent such attacks.

MOBILE DEVICE VULNERABILITIES AND SPYWARE

In November 2016, Kryptowire reported a security flaw in Android devices running Adups firmware that put confidentiality of information for many device users at risk. A backdoor was found in firmware on certain Android devices that sent personal and sensitive user information – such as call logs and the content of text messages – to third-party servers. About 700 million devices in more than 200 countries were reported to have this backdoor.

CERT-EE determined that Estonia also had many such devices that communicated frequently with servers that collect confidential information from users. Estonia has thousands of the BLU phones mentioned in the Kryptowire article. Yet the problem is not at the phone manufacturer level, but rather built in to the specific Adups firmware, FOTA (Firmware on the Air). The firmware manufacturer is aware of the vulnerability and has already issued a new version of FOTA where, it says, the backdoor has been closed.

Preliminary checks have not indicated that devices with this vulnerability had access to information systems (such as e-mail servers) at Estonian government institutions. RIA warned government agencies and worked with large wireless operators, which also adopted measures to mitigate the risks to users.

* https://www.kryptowire.com/adups_security_analysis.html

RECOMMENDATIONS

- Don't buy devices made by lesser-known manufacturers. Learn about the security risks in smartphones and other devices and the principles of secure use. The RIA website provides recommendations for ordinary users and developers for secure use of devices.

CIO/CISO

- Identify any infected devices in your organisation's information systems and take measures to block these devices' access to the information system.
- RIA strongly urges all organisations to devote attention to data security policy and not to purchase devices made by lesser-known manufacturers.

3 See https://www.ria.ee/public/Kuberturvalisus/RIA_KTT_kokkuvote_detsember_2016.pdf.

When devices attack: denial of service attacks by the internet of things

The number of devices connected to the internet is already many times larger than the number of devices we would traditionally call computers. The estimated number of devices hooked up to the internet of things (IoT) stood at 15.4 billion in 2016.[4] The range of uses for the interconnected devices is continually expanding, ranging from surveillance cameras and activity monitors to medical equipment and remote-controlled thermostats, all of them playing a bigger role in everyday life.

The inception of the IoT has led a new kind of risk that neither manufacturers nor users anticipated. Last year saw a number of cases where IoT devices were targeted by cyber attacks or became an instrument in perpetrating such attacks.

The very high number of distributed denial-of-service (DDoS) attacks that relied on TV converter boxes, security cameras and other interconnected devices in the latter half of 2016 was indicative of a new worldwide trend. The security of home appliances connected to the internet is predominantly weak and they are all too easy to infect with malware and hijack for an attack.

The very high number of distributed denial-of-service (DDoS) attacks that relied on TV converter boxes, security cameras and other interconnected devices in the latter half of 2016 was indicative of a new worldwide trend. The security of home appliances connected to the internet is predominantly weak and they are all too easy to infect with malware and hijack for an attack.

THE MIRAI BOTNET

One of the record number of DDoS attacks in the autumn hit the biggest domain name service provider in the US.* As a result of the incident, over a thousand websites were unavailable for US and European users for many hours, among them globally popular social networks, international media groups and retail and e-commerce giants like Amazon and PayPal. The interruption also affected the availability of Swedish government and Civil Contingencies Agency websites, which are used to notify the public in case of emergency.**

Home appliances infected by malware called Mirai targeted the base architecture, with a relatively small number of devices used to generate a attack of a strength that experts judged to be bigger than anything seen before (up to 1.2 terabits per second using 100,000 endpoint devices).***

* DNS lookup converts verbal domain names into numerical IP addresses, allowing user queries to be transmitted.

** https://www.ria.ee/public/Kuberturvalisus/RIA_KTT_kokkuvote_oktoober_2016.pdf.

*** http://www.computerworld.com/article/3135434/security/ddos-attack-on-dyn-came-from-100000-infected-devices.html.

4 https://www.forbes.com/sites/louiscolumbus/2016/11/27/roundup-of-internet-of-things-forecasts-and-market-estimates-2016/#e2c59c9292d5.

The above clearly attests to the fact that the security (or lack thereof) of smart home appliances is not a matter of a given' user's personal privacy, as it is often thought. An attack can impact the availability of vital services – such as ones provided in a national emergency – and the economic activity of many companies.

Given the small relative size of the Estonian internet infrastructure, it does not take particular skills or funding to organise cyber attacks similar to the ones experienced in 2007. The same is true for much larger countries.[5] Judging by the patterns of past DDoS attacks, it cannot be ruled out that such attacks can be used to attack the root infrastructure of the internet, with the purpose of taking down the whole internet – the question is not so much the capability of committing such attacks but rather who could be motivated to do so.

CONCLUSIONS

- No specific cyber security requirements and standards exist for IoT devices. Manufacturers have not paid much attention to security, and the whole sector has developed so rapidly from the ground up that market regulators have not kept up with the development of the technology. As a result, the approach to the threats from devices on the IoT has been reactive rather than preventive: the focus is on minimising and eliminating consequences of the incidents.
- Large-scale DDoS attacks that rely on IoT devices are a potential threat to countries as well as to the basic internet infrastructure itself. Spearheading a DDoS attack does not take significant resources and the malware needed for it is available online. Often attacks are mounted by teenage hackers out of curiosity or a profit motive. Currently no means of preventing DDoS attacks exist – the major 2016 attacks were not stopped, they ceased of their own accord. It is highly likely we will see more such attacks in the future, in increasing numbers.[6]
- Besides the possibility of exploiting vulnerabilities for cyber attacks, the interconnected devices themselves are vulnerable. Anything that can be administered remotely or transmit information to the internet can be targeted by criminals.

5 https://www.ria.ee/public/Kuberturvalisus/RIA_KTT_kokkuvote_november_2016.pdf.
6 https://pages.arbornetworks.com/rs/082-KNA-087/images/12th_Worldwide_Infrastructure_Security_Report.pdf.

RECOMMENDATIONS

- Any time you connect a specific device to the internet, consider whether it is really necessary. If the answer is yes, buy the IoT device from a manufacturer who can provide security.
- Know the possibilities for your devices, especially the ones your life, health and physical well-being depend on (medical equipment).
- Change your password for a stronger one and let your device run in a secure WiFi network. If possible, use a separate secure WiFi network that is reserved only for IoT devices.
- Update software running on the IoT devices as soon as the update or patch is released.

Threats by sector

The Estonian public sector is a target for both indiscriminate and targeted attacks

Government institutions were involved in 20-30% of all cyber incidents last year. During the year, CERT-EE registered 1,687 cyber events related to government sector institutions. The significant increase from 2015 can mainly be associated with the increased activity of institutions in reporting incidents and more effective cooperation between RIA and government agencies. A large share of the reports made by government agencies are related to security vulnerabilities or administration errors that did not involve an actual incident but where reporting nonetheless provides RIA with a better situational awareness, aiding in prevention of incidents.

Besides technical malfunctions and human error, the most common reasons for incidents continue to include cyber attacks. However, most of the cyber incidents with serious consequences are not due to attacks but stem from underestimating risks and human error.

In a number of areas, the work of Estonian government agencies depends heavily on the functioning of information systems. In internal security, even less than an hour of downtime can be critical for systems that service, e.g., the border guard or emergency responders. The lack of alternatives is also a particular feature of public sector services: disruptions in information systems that support public services can lead to an interruption in vital services with no possibility of switching to a different service provider. Examples of such services include communication services in internal security, the Population Register, and digital prescriptions. We therefore maintain that ensuring the continuous operation of vital services provided by government institutions will require serious attention and additional investments to ensure availability of services.

Starting in 2008, Estonia has employed a three-level IT baseline security system called ISKE,[7] which ensures the minimum necessary base level of security of data processing in state and local government databases. The capability of government institutions to ensure that the databases they administer are in conformity with ISKE security measures has significantly improved over the last two years – this is demonstrated by the fact that last year the share of ministries' databases that have undergone an ISKE audit reached 80% for the first time. If the databases operated by agencies in the ministries' area of government are included in the count, the figure is nearly 70%.

The measures used by local governments to ensure cyber security and the implementation of ISKE security measures for ensuring database security are still very inconsistent. After the current administrative reform is completed in Estonia, the local governments are expected to improve in their level of cyber

7 System of security measures for information systems (Government of the Republic regulation no. 252 of 20 December 2007; RT I 2007, 71, 440).

security awareness and their capability for ensuring it.

Analysing the experience of state and local government institutions, it can be concluded that data security is first a matter of management, and only then a question of resources. All too often, low cyber security awareness is due to lack of interest and vice versa. In the absence of knowledge, the dearth of resources tends to be inflated in importance; yet the experience of those who have applied security measures for information systems shows that much can be done to improve security even without major spending.

Ordinary phishing and spear phishing campaigns designed to defraud or gain access to sensitive data were the most common types of cyber attacks against government institutions last year. In some cases, it appears the agencies simply happened to be among the targets, while the elements in a number of other attacks suggest that the attacker intended to target a specific addressee. Examples of this were above-mentioned fraud attempts – messages purporting to be from directors general of state agencies and the prime minister were sent, the circulation of phishing e-mails aimed at national defence structures and the creation of customised spoof landing pages.

There were also a few instances of extortion targeting government agencies, which were threatened with a DDoS attack if they did not comply with the demands. In most cases, the demands were for money, but ideological or political positions were also expressed. The ultimate impact of these incidents proved insignificant and they did not disrupt operations at the agencies in question.

CONCLUSIONS

- As to cyber risks in the public sector, the two areas most at risk are the operational continuity of the information systems that support other public services or national security (where the cause of the incidents was largely due to internal, not external factors) and attacks mounted with the aim to defraud or on political or ideological motives.
- Attacks aimed at public servants were mainly to try to gain access to non-public information, but attacks can also be used for preparing acts of sabotage – creating an opening for disrupting the operation of the information system or to alter or delete data.

Leaks of user data

Estonia did not register any serious data leak incident in 2016 at either government institutions or service providers or companies. However, the Dropbox breach in September did receive broader attention: in this case, a user account database with the password hashes of 68 million users that had been stolen at some prior date was made available on the internet. An RIA analysis found that 20,000 accounts linked to Estonian e-mail addresses were among the data. Among them were accounts belonging to senior Estonian state officials and employees from important agencies; the individuals in question had used their work e-mail addresses to enter this public cloud service. By comparing the leaked password hashes, it was concluded that the passwords for some of the accounts were very weak. The data security managers

and heads of IT of all of the affected organisations were notified of the findings of the RIA Cyber Security Branch.

The data leak and the problem of using work e-mail addresses in public services obviously does not affect only public servants – it is common practice both in Estonia and abroad. For the Estonian state, the risk is that people's official accounts and the related agencies and organisations could be compromised because of the leaked credentials. Criminals and intelligence services of foreign countries are well aware that people are in the habit of using the same or similar passwords across different sites and services. Hacking one password makes it easier to mount attacks against other addresses in use.

Large-scale password leaks have become common. Last year, Yahoo reported that the data of close to a billion of its users had been leaked. This breach was the largest of the known leaks, but there have been a number of data thefts involving hundreds of millions of accounts. Last year alone, over four billion data records are known to have been leaked.[8]

CONCLUSIONS

- Authentication by password alone can no longer be considered secure. Once they have cracked one password, hackers run it on as many other platforms as possible to see if it works and find the cross-links rapidly. This means that use of solely a password for authentication is not secure, no matter how well a specific service runs its affairs; a tight ship doesn't reduce the risk of misuse of user data leaked from other sites. In the case of such massive leaks, it is impossible to close all the user accounts affected or change the passwords.
- In Estonia, state systems and e-services that use ID-card- and mobile-ID-based authentication systems

8 https://en.wikipedia.org/wiki/List_of_data_breaches; https://en.wikipedia.org/wiki/Yahoo!_data_breaches; http://www.securityweek.com/42-billion-records-exposed-data-breaches-2016-report.

RECOMMENDATIONS

Users

- Avoid linking your work e-mail address to accounts meant for cloud services and private use. If you do, that will make it easier for cyber criminals and foreign intelligence services to mount attacks against official and work accounts, because it allows to narrow down the millions of users to the ones that it is worth to spend time hacking for passwords and data.
- Avoid using the same password for multiple sites and services – above all, don't use the password for your work computer for other services. If at all possible, enables two-factor authentication.

CIOs

- Assume that password authentication is intrinsically insecure and that people use the same passwords for different services.
- We recommend configuring two-factor authentication for services wherever possible.

are well-secured. Compared to the rest of the world, this makes it complicated and costly to access data from Estonia's government and bank services, and reduces the attractiveness of these services as a target for criminals. Major global service providers such as Google, Facebook and Microsoft have successfully launched two-factor authentication and its use rose significantly in 2016.

Security awareness in the private sector is inconsistent and investments into security are insufficient

As expected, the majority of cyber incidents last year affected the private sector, which is where the greatest number of users is found. It includes companies large and small, NGOs and individual computer users whose levels of digital dependence and cyber security awareness vary widely. It is also true that the importance of functioning of digital solutions tends to be underestimated and that instead of preventing risks, attention is devoted to security only after an incident occurs.

While vital service providers are required by law to assess and mitigate ICT risks and protection of their information systems is better organised, SMEs and NGOs tend not to be aware of cyber risks and often do not consider they might be a target for cyber crime. Insofar as their resources are limited – in particular NGOs which are largely volunteer-driven and non-profit – investments into IT are not a priority.

Studies from outside Estonia have also shown this. Even though the cyber risks for NGOs are similar to those of companies, they tend to have low risk awareness as well as limited resources, which makes them an easy mark. NGOs also include some particularly inviting targets such as associations with political agendas: criminals and intelligence services could have an interest in their internal information. It should be recalled that the Russian cyber operation for meddling in US elections started by targeting a political party's information system, not the election system itself.

The most frequent cyber security weakness for NGOs and micro-companies is out of date web pages where vulnerabilities are exploited for data theft and spreading malware. Poorly secured websites may, due to well-known vulnerabilities, pose a risk to the personal data of employees, employees, members, customers and partners, and publicly available e-mail addresses may become the target of phishing attempts or ransomware schemes. In addition to the above, a primary concern for small enterprises and NGOs is security flaws and administration errors in their information systems, which may be exploited by cyber criminals for attacks.

The challenge for the Estonian economy is the capability for offering higher-value-added products and services[9] and digitisation offers a noteworthy opportunity for competing regionally and globally. Estonia's high-tech and strategically important companies in tech-heavy sectors (energy, ICT, chemical industry and biotechnology) should consider that their activities may be targeted

9 https://valitsus.ee/sites/default/files/content-editors/failid/majandusarengu_raport.pdf.

by digital industrial espionage or sabotage attempts. Such attempts tend to be underwritten by a foreign country, as economic and industrial espionage is usually extremely time-consuming and does not offer a rapid return for criminals.

Vulnerabilities in industrial control equipment are inevitable: industrial systems have a very long life cycle and this limits ways of improving security through updates. Nor is it possible to keep the device cordoned off from the internet, as attackers usually find a way to insinuate attackware into such networks. Every provider of a vital or vital service must have a backup plan in case the ICS/SCADA[10] system becomes unusable.

CONCLUSIONS

- The private sector's awareness of cyber risks is spotty, both on the individual employee and corporate level. Small companies and NGOs in particular don't think "it could happen to them" and don't invest into security.
- Companies in Estonia's tech-heavy sectors may be targeted by digital espionage. Sabotage motives cannot be ruled out either, especially in the case of vital service providers.

10 Industrial control systems (ICS), used for automation, monitoring and control of industrial processes. A Supervisory Control and Data Acquisition (SCADA) is one type of ICS.

TARGETED ATTACK AT VIRU KEEMIA GRUPP

In 2016, traffic bearing the hallmarks of malware was spotted in the computer network of Viru Keemia Grupp (VKG), an Estonian group of oil shale, power and public utility companies. Software experts found the Mimikatz malware in the VKG office network, used in Windows systems to extract identity credentials (such as passwords, password hashes etc.). A backdoor was also found, used for communication with the control server. A full scan that followed turned up a number of suspicious connections and certificates that were similar to ones used for backdoor connections. A scan of the internal network did not turn up any more (malware) connections to the control server, nor were any other infected devices found.

In June 2016, it was again found that there had been a network connection to the same control server. This time it proved possible to identify the name of the computer that initiated the connection as well. Upon further investigation, it was found that a workstation in the SCADA monitoring segment was infected. The workstation was then removed from the network. Computer software experts found that installed on the computer was the same backdoor that was found previously in the office network computers.

Network traffic and examples of malware found on computers all pointed to a targeted attack. The malware and control server used have been linked to the APT28 cyber espionage group.*

RIA experts advised VKG in resolving the incident, in improving the security of its network architecture, and assisted in updating the company's IT admin procedures. RIA also helped to raise the security awareness of the company's employees.

* See e.g. https://www.fireeye.com/blog/threat-research/2014/10/apt28-a-window-into-russias-cyber-espionage-operations.html.

RECOMMENDATIONS

- Check RIA's cyber threat notifications regularly. They can be found on the RIA website, CERT-EE Twitter account and in the mass media. RIA blog's has longer instructions and articles on the topic of the digital state and cyber security (in Estonian).

Vital services are increasingly cyber-dependent

Disruption of a vital service due to a cyber incident continues to be seen as a significant risk for Estonia. Since 2013, RIA has regularly conducted studies on vital service[11] continuity and resilience that indicate growing digital dependence among vital service providers.

In 2016, a RIA-commissioned study of factors that impact the provision of vital services assessed cyber risks of mission-critical services that are needed for the functioning of the state, and the solutions employed for ensuring continuity of these services.[12] The study confirmed that without exception, all of the vital service providers[13] studied depend on communication and power supply to provide their services and that many of them consider their dependence of these systems to be critical. More than one-fifth of the service providers surveyed depend to a critical extent on ICT infrastructure or services provided by third parties – meaning that the functioning of a particular vital service directly depends on external ICT services.

Many of the companies in question only conduct general assessments of IT risks and only one-third of the companies had an updated risk analysis and business continuity plan. IT security risk management is effectively organised in companies in the power, telecommunication and financial services sector, yet none of the service providers in the study said that their company was fully compliant with the requirements of the information system security measure system[14] and many service providers do not have a detailed overview of the ICT-related cross-dependencies of their services. The study also found that companies have made too few preparations for long-term power cuts, and have too few technical resources to rely on alternative solutions to continue providing services during an interruption.

Estonia is actively engaged in finding alternative solutions for reducing vital services' dependence on third party services and foreign infrastructure and thereby reducing business continuity risks. The Emergency Act tasks service

11 Vital services as defined by the Emergency Act in force until 30 June 2017.

12 https://www.ria.ee/public/publikatsioonid/Summary-Study-Mapping-the-Factor-which-Influence-Provision-of-Vital-Services.pdf.

13 The following services were covered by the study: supply of electricity, natural gas and liquid fuels, navigability of national and local road, and functioning of railway freight services, telecommunications services, financial and healthcare services, utility services such as supply of district heat, water supply and sewage, functioning of ports and vessel traffic management, and aerial navigation services, airports and airfields.

14 ISKE or ISO 27001 standard.

providers with the duty to ensure continuous operation based on business continuity plans and the Estonian private sector and public authorities work together closely to fulfil this obligation.

On the basis of worldwide events in 2016, the ever higher impact of cyber incidents could be seen mainly in the energy, healthcare, financial services and transport sectors. Two attacks on the energy system structures in Ukraine a year apart received heavy international coverage. The first of these left a quarter million people without power and the second left one-fifth of the capital in the dark.[15] In both cases, power was restored in a few hours, yet this marked a sea change. A year ago, crippling of the energy system was considered an extraordinary occurrence, but in 2016, hazardous cyber vulnerabilities were a topic in very advanced, stable countries as well.[16]

Of course, not all extensive cuts in digitally dependent vital services were due to cyber attacks, as two examples from Estonia's own region show. Last spring, airspace in and around Stockholm was shut down for hours due to "IT problems". A couple of months earlier, also in Stockholm, a solar storm disrupted the radar system and shut down air traffic control.[17]

In 2016, Estonia did not experience cyber incidents that affected vital services and which had significant impact. Starting from last year, CERT-EE distinguishes cyber incidents affecting vital service providers, meaning that such incidents need not have impacted the functioning of vital services but rather the service provider itself. There were 253 such incidents, which is under 3% of the total number of recorded cases and 11% of incidents identified (i.e. those cases that had a direct impact on the confidentiality, integrity or availability of data or a system). Most of the identified incidents involved infected and botnet-exploited devices in communication service providers' networks, but there were also twelve cases involving ransomware infections.

The greatest number of reports pertained to vital communications service providers, which is to be expected, considering that many other services rely on the functioning of communication services; thus the "pain threshold" is low in case of cuts to such services and incidents are efficiently reported. Most of the incidents in this sector were caused by equipment failures or deviation from ordinary functioning during maintenance, with impact restricted to a limited time or geographic area.

Cyber threats in healthcare

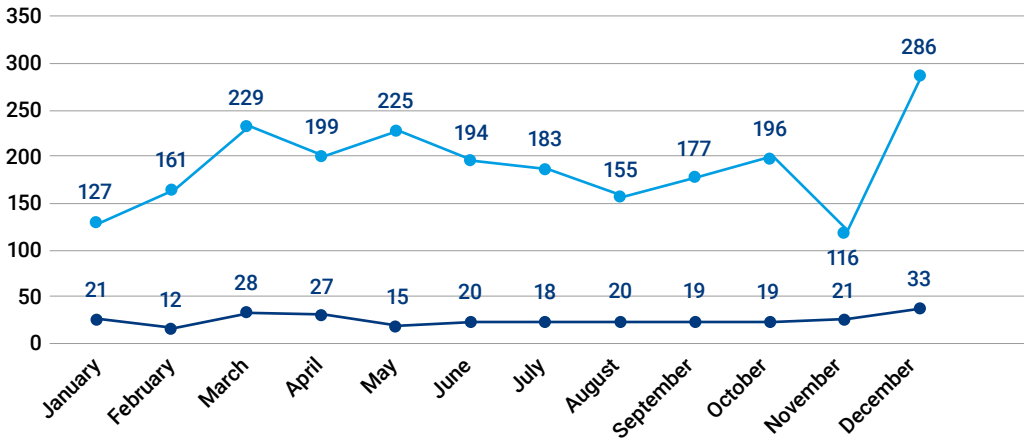
Crypto-ransomware could likely be considered the most significant of the salient threats to the healthcare sector in 2016. The number of ransomware attacks and infections in the sector worldwide implies

15 http://www.reuters.com/article/us-ukraine-crisis-cyber-attacks-idUSKBN1491ZF; see also RIA Cyber Security Branch annual summaries from January, February and December 2016 https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html.

16 http://www.ibtimes.com/after-ukraine-cyberattacks-fbi-dhs-urge-us-power-companies-develop-better-safety-2355649; https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/.

17 https://www.ria.ee/public/Kuberturvalisus/RIA_KTT_kokkuvote_mai_2016.pdf; http://www.thelocal.se/20151104/solar-storm-grounds-swedish-air-traffic.

Vital service provider incidents against the total number of recorded cyber incidents in 2016



A ZERO-DAY VULNERABILITY IN COMMUNICATION NETWORK DEVICES

An incident of a critical nature occurred in October in the core network of one of Estonia's largest internet service providers. Early on the morning of 5 October, some of the equipment in the company's core network, which ensures functioning of the transmission network, began experiencing spontaneous restarts. A preliminary analysis of logs showed that the devices sent an error report right before restarting. The company contacted the device manufacturer with the error report, who confirmed that a DDoS attack had taken down the devices. In cooperation between RIA and the company, the attack packets were captured and sent to the device manufacturer for analysis. The packets helped the manufacturer develop software solutions for patching the critical flaw. Until the patch was developed, the company successfully used alternative methods to keep the incident from recurring.

RIA's conclusion is that the incident was not necessarily a targeted attack. There have been previous analogous incidents involving various manufacturers' network devices where no external intervention took place. On the basis of the currently available information, it is likely it was a software bug in the device that was simply unable to process certain types of packets. It also could have been an attempt to scan Estonian networks for SIP/VoIP* devices for the purpose of committing VoIP fraud, and that this activity had the side effect of causing a large-scale availability incident at one of Estonia's largest ISPs. The company's quick and responsive action helped prevent the spread of a dangerous zero-day vulnerability in a core network.

* Session initiation protocol/voice over IP.

that because of the time-critical nature of the data, criminals see their chances of extorting money from this sector as higher than in others.

Last year there were a number of examples of hospitals in Europe and North America that fell victim to ransomware, culminating in patient medical records being rendered inaccessible and hospitals having to cancel scheduled operations, appointments and diagnostics procedures for several days.[18] It is important to understand that due to its high level of digitalisation, the Estonian healthcare system is just as exposed to these risks and there is a danger that the disruption will not be constrained to availability of e-services but the provision of medical care as a critical service itself will be disrupted.

Even though there were no incidents as dramatic in Estonia, the healthcare system in Estonia did not go unscathed by ransomware schemes. At one of Estonia's largest hospitals, ransomware from infected computers spread to the file server. While provision of medical services was not disrupted, there were serious problems in other operational processes. The incident did not remain a single occurrence, unfortunately.

Data backups and risk-minimising administrative policies are indispensable for preventing ransomware related damage. Last spring, a hospital in the US state of Kansas experienced a case where the data were not recovered even after the ransom was paid; instead, the hospital received a new demand to pay another sum. This should be a clear lesson that it is unwise to pay a ransom in the hopes that the criminals might provide the key to decrypt the data.

As to Estonian healthcare, last year's cyber incidents clearly pointed to the need to improve specialists' skills and the awareness of users of information systems regarding cyber risks and risk avoidance. Even if a configuration error or malware infection do not take down the medical service itself, an exploit of staff e-mail accounts or unauthorised third-party access to the healthcare institution's information system is a serious problem from the standpoint of protection of sensitive personal data and the trustworthiness of the healthcare institution. This year, RIA has devoted more attention to ensuring data security in Estonian healthcare in particular – through training, security tests and publicity efforts.

CONCLUSIONS

- Vital services are becoming more dependent on e-services and ICT with each year, yet service providers are not sufficiently aware of the risks that jeopardise the functioning of vital services, and risk assessments are drawn up inconsistently and with varied level of detail. The core reason is low awareness – a problem seen at levels from specialists to top management – and lack of skills. Moreover, Estonia's legal environment for ensuring central coordination and preparation at the state level in the event of crisis is insufficient, the contribution made by the vital services' business continuity planners (primarily

18 These events were covered in more detail in the March; May and November 2016 summaries of the RIA Cyber Security Branch: https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html.

ministries and local governments) is very uneven by sector, and there is a lack of clarity about what service levels must be adhered to in each sector.

- The healthcare, energy, financial services and transport sector all stand out as particularly attractive targets for cyber threat; in Estonia, healthcare is specifically at risk. The high cyber risk in the healthcare sector stems from a combination of several factors: the fact that people's life and health depend directly on the functioning of healthcare services, the provision of healthcare services depends on the availability (time-critical) data processed in an information system and not enough attention has been devoted to IT security in this field. All this makes healthcare providers easy targets for cyber criminals.
- Digitalisation of services that support provision of healthcare services cannot be merely seen as an opportunity for saving on costs. IT service is no longer just a support service in any sector – without its functioning ensured, even an organisation's main tasks are not fully certain. As a consequence of disruptions or a cyber attack against information systems, medical services can be interrupted or availability degraded. Confidentiality and integrity of patient records is also at risk. Mitigating these risks requires investments and better awareness on the part of the entire staff; security must also be made a priority at the hospital management level. As long as cyber security is not considered important in healthcare, we will see more of the types of incidents seen in 2016, and sooner or later, a cyber incident will have a palpable rather than abstract impact on the functioning of medical care.

RECOMMENDATIONS

Vital service providers

- Providers of vital services that depend on communications must have redundant communication connections to avoid dependence on just one communication service provider and on a single physical infrastructure.
- Measures should be specified in vital service risk analyses and business continuity plans to ensure the management and storage of sensitive information.

Vital service providers' business continuity planners and coordinators

- Review the service provider's service portfolio and distinguish vital services from those needed on public interest or business considerations. Establish, by law, specific business continuity and availability requirements for vital services.
- Consider creating a single secure electronic environment for safeguarding risk analyses and business continuity plans and facilitate secure document exchange.
- Considering that vital services are now universally dependent on the existence of power supply, prepare plans for supplying backup power to high-priority vital services in the event of a long-term power cut.

- Ensure that the parties that are affected and needed have situation awareness regarding service interruptions. Where necessary, offer assistance for analysing incidents and modifying processes to keep incidents from recurring.

Healthcare providers

- To prevent a cyber attack from causing leaks of patients' sensitive personal information or risks to the provision of healthcare service, it is of the highest importance to ensure quality IT service. To do so, we strongly advise investing in IT personnel and resources or outsourcing service – either independently or in cooperation with other organisations. We advise that smaller healthcare institutions in particular consider the last step if they themselves have limited capability on ensuring quality IT security.

Sources, actors and motives

Put simply, the state, companies and individuals are targets for cyber threats for two basic reasons: money and influence. Cyberspace offers low-risk opportunities for countries hostile to Estonia to advance their interests; it is also a field where professional criminals can attempt to pocket criminal gains.

Foreign governments' cyber operations are mainly aimed at obtaining information and influence

Foreign countries are increasingly experienced in tapping the possibilities of the digital environment for securing their geopolitical (diplomatic, economic or military) positions. State-organised cyber operations are not conducted randomly – the choice of targets typically reflects the geopolitical interests of a specific country. There is an established pattern that tensions between countries also find expression in cyberspace.

Estonia cannot disregard the fact that its eastern neighbour Russia views the NATO alliance as a threat to its security and routinely uses cyberspace to increase its influence and achieve its goals.[19] 2016 saw a spike in overt cyber activity from Russia aimed at NATO members. The most vivid example was an influence operation directed against the US presidential election, which combined cyber attacks, data leaks and state-funded propaganda on media and social networks to ensure victory for the candidate more favourably predisposed to the Russian Federation's leaders.[20] Several European countries have recently publicly reported cyber attacks originating in Russia. Among these countries are Germany, France, the

19 https://www.ft.com/content/6e8e787e-b15f-11e5-b147-e5e5bba42e51; http://static.kremlin.ru/media/events/files/ru/l8iXkR8XLAtxeilX7JK3XXy6YOAsHD5v.pdf.

20 https://www.dni.gov/files/documents/ICA_2017_01.pdf.

ADVANCED PERSISTENT THREATS

The keyword APT (Advanced Persistent Threat) is used when discussing cyber threats originating from state actors. Since 2006, APT attacks often denote a high-level or "advanced" battery of attack methods developed to target a specific type of victim, such as government institutions. The attackers enter the victim's information system and acquire long-term or "persistent" covert control over the information kept and processed there. Usually the attackers (the "threat") are an organised group of individuals who are acting in the interests of a country's intelligence services.

APT attack campaigns are distinguished on basis of characteristics. The group called APT28 in a 2014 report from FireEye* has been linked to the Russian special services, namely its main military intelligence agency. Among other things, the malware used for the attacks was developed in Russia and the group was active on weekdays from 8am to 6pm in the NW Russian time zone.

On 10 February 2017, US-CERT released a thorough overview of the APT campaign Grizzly Steppe, which attacked US government agencies.**

- The most common APT method is spear phishing. Public servants who handle sensitive information must always be very careful about e-mails sent to them and if anything looks off – the contents of an e-mail, list of recipients or the sender's address doesn't make perfect sense – they should notify their organisation's IT security person.
- Organisers of the APT campaigns are constantly analysing the success of the attacks and changing their means and methods. It is thus not all that likely that such attacks could be repelled in the future using a perimeter defence alone. The only solution is to constantly monitor users' behaviour and look for and analyze deviations from the ordinary network traffic.
- Although the objective of the APT campaigns is mainly cyber espionage and they act in a state's interests, private companies can also be involved in the attacks, and the information stolen can be used for criminal purposes.

* https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-apt28.pdf.

** https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf.

Czech Republic, Sweden and Poland.[21] We can expect Russia to continue to use cyber operations hand in hand with traditional influence activity based on its technological capability, its doctrine and foreign policy opportunities.

The main aim of cyber espionage directed against Estonia is to gain access to (classified) information, above all pertaining to the political decision-making process, security and national defence (including NATO's activities) and foreign

21 https://www.theguardian.com/world/2016/nov/29/german-spy-chief-russian-hackers-could-disrupt-elections-bruno-kahl-cyber-attacks; http://www.businessinsider.com/ap-intelligence-agency-russia-trying-to-destabilize-germany-2016-12; http://www.france24.com/en/20170219-france-condemns-cyberattacks-targeting-presidential-candidate-macron-points-russia. See also the RIA Cyber Security Branch annual summaries from January 2016: https://www.ria.ee/ee/kuberturvalisuse-kokkuvotted.html.

relations. Possessing such information would give an adversary a way of influencing the internal political situation or international reputation of a country and, by extension, the decisions made by the country's allies. The target of cyber espionage is mainly government institutions and government personnel who have access to key information. Yet no less significant are attacks mounted to gain access to the information systems of vital service providers or strategic companies, either for creating an opening for espionage or sabotage. The cyber operations linked to Russian special services that were carried out in different parts of the world last year are indicative of how cyber attacks in general have expanded their range in the last decade: in addition to procuring information and blocking access to services, they are also profitable for interrupting the functioning of the services themselves or manipulating public sentiment.

A characteristic of cyber operations supported by foreign powers is that the attackers have a long-term interest, and thus do their utmost to avoid detection. Espionage incidents are detected rarely – generally only a long time after a successful intrusion – as the aim of the "agent" who has burrowed into the system is to collect and transmit the information over a longer period or achieve a holding position inside systems that process sensitive information and to await further opportunities. For these reasons, it is difficult to evaluate the total number of incidents in this category. It is also clear that there are even more unsuccessful attempts to access critical systems. As to specific incidents, there is reason to believe that the VKG incident described earlier in this report was an attack organised with the support of a foreign country.

Cyber crime

The criminals operating in the digital environment come in all different skill levels, from garden-variety e-mail scammers to groups who carefully plan exploits of entire information systems. Cyber criminals' skills are constantly developing, adapting to technological changes and the market situation, which can also be seen in the pattern of ransomware and phishing attacks described in this annual report. At the same time, cyber crime is no longer the province of a few masterminds: even laymen can outsource "service" to criminals.

Unlike attacks from state actors, which reflect international tensions and spheres of interest, cyber criminals have no equivalent geographical preferences: the user of any digital equipment is potentially a target for global cyber crime, due to the possibility of defrauding the victim of money or information with monetary value or hijack their device in order to attack other persons or connections. Information obtained in phishing attacks – credit card data, usernames and passwords – are used for committing computer fraud or re-sold to criminal organisations on the basis of a price list. A malware-infected computer can be used for DDoS attacks or for extortion on threat of a DDoS attack. Ordinary computer users who never considered themselves likely targets also fall victim to automated attacks – weaknesses such as out of

date software and the lack of anti-virus systems are exploited to attack other individuals.

Extortion is another possibility afforded by cyber crime. Crypto-ransomware, DDoS attacks and data theft are used to demand funds from the victim, generally in the virtual currency Bitcoin, in exchange for ceasing the attack or refraining from disclosing data. A constitutional institution in Estonia also received such an extortion demand in 2016 – the attackers threatened a denial-of-service attack if demands were not met. The institution did not comply, but no attack ensued.

With potential gains disproportionately larger than the level of risk for criminals, it isn't surprising that cyber crime is rife. According to Europol's 2016 threat assessment, the number of cybercrimes in some EU member states exceeds that of traditional crimes.[22] Since 2012, Estonia has recorded an annual increase in cyber crime in the neighbourhood of 5–12% – crimes against property overall having decreased 35% in the same time period.[23] We can suppose that a large percentage of cyber crimes go undetected and unreported. It is also clear that criminals keep careful track of their risk to reward ratio, and thus secure architecture for services (including robust electronic identity), clear legal space and effective response from law enforcement reduce Estonia's attractiveness in the eyes of cyber crime.

CONCLUSIONS

- Most cyber crimes – including the ones reported in Estonia – fall into the category of fraud, in which the criminals take advantage of the victim's greed or gullibility. Those who fall victim to fraud are often astonished after the fact at how easily they took the bait, and transferred money to parts unknown, without getting that "jackpot" in a lottery they did not participate in.
- Poor security level and user negligence, deficient skills and low awareness play a role in risks becoming realised.

22 Internet Organised Crime Threat Assessment (IOCTA) 2016.
23 http://www.kriminaalpoliitika.ee/sites/krimipoliitika/files/elfinder/dokumendid/kuritegevus_eestis_2015.pdf.

RECOMMENDATIONS

- In all interactions in the cyber world, be aware that your partner in the exchange might not be who they say they are. Extra caution and scepticism doesn't hurt. Send funds, personal data and other important information only if you are sure about the identity and intentions of the other party to the transaction.
- No matter whether the victim is a service provider or consumer, always notify the police if harm has occurred due to cyber crime (cybercrime@politsei.ee).

Terrorism, ideological and incidental actors

So far, terrorist attacks have not been carried out through cyber infrastructure. Terrorist groups such as the Islamic State use the internet mainly as a propaganda and recruitment tool. Still, on the backdrop of terror attacks, one can discern an elevated threat of cyber attacks that are not necessarily of terrorist origin – for example, a wave of cyber attacks occurred in Belgium in the wake of the bombings in Brussels in March 2016.[24] Estonia in cooperation with its domestic and foreign partners is becoming aware of the need to keep a critical amount of funds and competence from becoming concentrated in the hands of terrorist groups and to prevent attacks on vital infrastructure that could lead to major harm to the civilian population and destabilise the country as a whole.

International tensions also tend to activate hacktivists with political and ideological motives; their repertoire typically includes DDoS attacks and website defacements for propaganda purposes. Special services with an anti-Estonian agenda may collude with hacktivists and cyber criminals, with both sides benefiting from this brand of "public-private partnership". It all renders the situation more and more complicated for Estonia as there are practically no clear answers: it is no longer possible to be sure that an attack by ostensible fraudsters was not actually ordered from criminals on the basis of some other criterion.

At the end of the day, cyberspace is also simply a technological environment used and misused by people with very different skill level and interests, often without thinking of the consequences. The motive behind cyber attacks may be curiosity. Others may be seeking a challenge. Cyber bullying is another reason. The police should always be notified whenever data or equipment fall prey to illegal manipulation.

24 http://cytegic.com/wp-content/uploads/2016/02/DyTA-Intelligence-Report-March-2016.pdf.

The challenges ahead

Possible increases in cyber and information operations against the digital state

In CERT-EE's ten years of activity, we have seen a constant increase in cyber security incidents in Estonian cyberspace and 2017 is unlikely to be an exception. Besides the natural organic growth in cyber activity, Estonia faces several important events this year, which will pose higher requirements for the secure and impeccable functioning of the country's digital infrastructure.

In connection with Estonia's six-month presidency of the Council of the European Union starting in July, RIA is contributing significantly to bolstering general cyber security in Estonia. Preparations started in early 2016. Adoption of technical solutions needed to carry out the presidency, including ensuring that officials

and visitors have secure communication solutions, requires smooth cooperation between many agencies. As the experience of our southern neighbour Latvia in 2015 showed, a country is likely to come under increased pressure and attacks from cyberspace during its EU presidency. We are therefore taking into consideration that key events related to the presidency will make Estonia a more attractive target for foreign intelligence services and cyber criminals, as well as for cyber activists who wish to forward a political message.

The adoption of technical solutions necessary for organising the presidency and the increased attractiveness of Estonia's ICT infrastructure as a target for cyber attacks require significantly higher readiness for threat prevention on behalf of government agencies. To improve preparedness, RIA has since 2016 carried out a series of cyber security trainings for Chancellery of the Riigikogu (Parliament), Government Office and ministry personnel to raise public servants' awareness of salient cyber threats and the fundamentals of cyber security.

There are also other reasons that Estonia could see an uptick in cyber and disinformation operations against both Estonia in general and the digital state in particular. More broadly, these are tied to Russia becoming more active in advancing its strategic interests. It is well-known that Russia aims to replace the current international security architecture and among other instruments it uses to do so are influence operations that attempt to undermine public trust in democratic processes and institutions of public authority.[25]

The cyber attacks against the 2016 US presidential elections were part of an information operation, where publishing the internal documents stolen by breaking into the Democratic National Committee's information systems served the aim to manipulate public sentiment and ensure success to a preferred candidate. Similarly, aggressive cyber espionage against states increased dramatically prior to elections in EU countries, coupled with information operations. This shows the readiness to apply the lessons learnt from the US elections against countries in Europe.

Estonia is not left unaffected[26] by the increase in information operations among our allies, and there is no reason to expect that cyber attacks would not be included in this formula. The upcoming events in 2017 may be seen as a good opportunity to score propaganda points. This April marks the 10th anniversary of the massive cyber attacks that hit Estonia in 2007 after a Soviet-era bronze soldier statue was relocated from a Tallinn city centre park to a cemetery. The NATO units now being hosted in Estonia are drawing attention from cyber intelligence and propaganda, as the Estonian Information Board has noted in their annual review.[27] Also on the calendar for the autumn are the first local elections in Estonia since administrative reform. For the first time, MPs can also stand as local candidates.

25 For more on Russia's information war doctrine, see Richard Weitz, "Silmitsi Venemaa hübriidohtudega" (Eye to eye with hybrid threats from Russia). Diplomaatia no. 135, November 2014. https://www.diplomaatia.ee/artikkel/silmitsi-venemaa-hubriidohtudega/. For a longer analysis see Ants Laaneots, "Putini Venemaa doktriin" (Doctrine of Putin's Russia). Sõdur, 05/2014. https://issuu.com/sodur/docs/sodur0514_veeb.

26 See e.g. https://www.propastop.org/, which tracks spread of anti-Estonian propaganda in the media.

27 https://www.teabeamet.ee/pdf/EIB_public_report_Feb_2017.pdf.

It is expected that cyber activity will ramp up for these events.

It is also possible that the reliability of the state's digital infrastructure itself will be targeted by influence operations. In the context of elections, that could mean that the trustworthiness of electronic voting would come under fire.

CONCLUSIONS

- In the context of politically important events, including elections, there is a greater risk of aggressive cases of cyber espionage, cyber attacks and influence operations. There is no reason to believe that Estonia's local elections will be unaffected. We can expect cyber attacks to be used in the backdrop to prominent events in 2017, and that they are intended to serve as an instrument for information and influence operations.
- Estonian institutions and the security expert community have worked to ensure a high level of security of internet voting ever since it first became an option for voters in the 2005 elections, and cooperation will continue prior to and during this year's elections as well.

RECOMMENDATIONS

- The security of the Estonian digital state and internet voting are well protected. A critical attitude should be taken toward hypothetical threat scenarios where the critics attempt to discredit internet voting by mechanically transposing unrelated risks associated with other countries' electoral systems. Abstract scenarios regarding the "risks of e-voting" in general should not be taken seriously.
- The Estonian Electoral Office or RIA (cert@cert.ee) should always be contacted if concerns arise related to the security of internet voting.
- Just as voters are used to scrutinising the security of their own votes in ballots cast in a traditional manner, the voter's responsible behaviour is also important in the case of internet voting.

Digital innovation has an impact on the functioning and security of the digital state

Information systems are an integral part of the Estonian state. Estonia's laws presume the existence of access to registers and business processes are built on the concept of self-service. Every change in information systems thus means a greater or lesser change in how the state functions – and software innovation thus inevitably means state innovation. Any kind of innovation intrinsically runs risks.

Two categories of risks are related to Estonia's state digital architecture. First, digital services must function smoothly if state and society are to function in the manner that people are accustomed to. Thus the digital state must be able to keep up with the changing expectations as to the ease of use of services and also ensure that the same services are protected against emergent threats. Second, Estonia must take into consideration that it will not be just a specific system that comes under fire if risks connected to a

given technological innovation become realised; rather, the whole of national security will be impacted.

In developments pertaining to availability of services, RIA proceeds from the principle of security by design. This general principle for development also pertains to updates developed due to technological advances and which pertain to the foundations of the Estonian digital society, such as solutions for the electronic identity used for authentication (eID) and the state information systems' data exchange layer, X-road.

The functioning of the Estonian digital society deeply relies on the trustworthiness of services, which entails the use of strong cryptography. A trusted electronic identity is becoming more and more important in digital society: it is extremely important that we know with certainty who is who in the digital environment. Estonia has been a trailblazer in the field of electronic identity and we have often been cited as a model worth following. Yet ensuring a strong electronic identity comes with its fair share of challenges in the rapidly changing digital domain.

Some of these challenges are related to changes in the legal environment. The FBI-Apple standoff in the US last February, where FBI contended that the tech giant should create a back door on its devices to allow the authorities to access data on encrypted phones, again brought up the debate on strong encryption. As the American legal system is based on precedent, accepting the FBI's demand would have meant that US law enforcement could have required back doors to be enabled in devices in principle, thus making it possible to bypass encryption on devices marketed internationally as well.

European countries also differ in their positions on the encryption debate. In January 2016, the Dutch government ruled in favour of strong encryption, which emphasised the importance of encryption for protection of citizens, the state and the economy, and reported that it would hold off on establishing legal standards that provided for encryption backdoors.[28] The UK's Investigatory Powers Act adopted in autumn, on the other hand, gives authorities broad powers to surveil internet traffic and access user data, including enabling them to require service providers to remove encryption or provide backdoors. France and Germany have also demanded that strong encryption be restricted in the fight against terrorism.[29]

From Estonia's perspective, strong encryption is vital for ensuring trust in the state's digital services, as all of the e-services provided by the government and many private sector e-services are based on strong encryption (Estonian digital identity). In the longer term, building in backdoors would thus reduce trust in

28 https://www.tweedekamer.nl/downloads/document?id=b12f7a99-2615-441b-89a1-ab42631715a5&title=Kabinetsstandpunt%20encryptie.pdf.

29 https://www.theregister.co.uk/2017/02/28/german_french_ministers_breaking_encryption/.

the digital state, but trust is an extremely important value for Estonia. As a result, Estonia has not supported building backdoors into e-services, and the objective and function of RIA continues to be to ensure the high level of trust in Estonian digital identity.

In 2015, it emerged that many of the ID cards that were issued by Estonia were using authentication certificates that major software companies were planning to stop recognising or already had stopped recognising. To ensure that Estonian ID card certificates would continue to meet recognised standards, the Police and Border Guard Board (PPA) and RIA launched preparations in cooperation to replace the ID card certificates. Last March, the ID certificates began to be updated through the Estonian ID card's basic software: that means that persons whose ID card certificates needed to be updated could do so without leaving home or office.

WHY IS UPDATING CERTIFICATES NECESSARY?

As computing power grows, earlier encryption algorithms (in this case SHA-1) become vulnerable as well-funded attackers develop the possibility of breaking them. For the time being, this is only a theoretical vulnerability but in the longer term, retaining the existing algorithms could pose a risk to Estonian public key infrastructure, which ensures secure authentication of people by way of ID card, mobile ID or digital ID.

In order to prevent the risk from being realised, out of date encryption algorithms must be replaced with stronger ones: ordinary users would have to replace their certificates on the ID card chip with ones based on stronger encryption (SHA-2). There are about a million of such ID cards and they were issued before 1 March 2016, when SHA-2 algorithm encryption certificates began to be issued for new cards.

Software developers have set a definite course toward discontinuing support for the SHA-1 hash function, because the likelihood of breaking it has become too high. The fact that the older cryptographic algorithms are gradually becoming insecure as computing power increases is a normal course of events in encryption.

During 2016, more than 70,000 card holders updated their ID cards. The automatic update option was made available in the first few days of 2017 and since then about 10,000 cards per week have been updated. A new ID card is expected to be rolled out in 2019.

There is as yet no clear solution as to the future of mobile ID. The ever-more universal use of smartphones and tablets has spurred the development of e-SIM products that integrate SIM cards with the phone. Estonia's mobile ID service is, however, based on keys located on the SIM card, and thus a physical SIM card is required. With an integrated SIM, there is no longer a place to store the keys on. Both Apple and Samsung are expected to release products with eSIM, but they have not yet done so as of this writing and wireless operators are not yet ready to support telephones that completely lack conventional SIM cards. Thus the new eSIM telephones will still support conventional SIM cards and Estonia's mobile ID will continue to work in the near future. It is technologically possible to use mobile ID with eSIM, but in that case it is not certain how eIDAS-level certification of devices would be handled and how the level of binding digital signature would be retained. RIA is actively monitoring market developments in this regard.

Another challenge is the use of ID cards in all web browsers, not all of which have support for chip cards. The biggest concern is the Windows 10 Edge web browser, where a conventional solution in the form of a plug-in is not possible, and hopes will have to be placed on Microsoft support. Due to the frequent occurrence of such problems, new web plug-in architecture is being considered.

CONCLUSIONS

- It is important to understand that neither forgoing innovation or reducing digital dependence are solutions in a situation where the direct and indirect benefits from information systems provide the current level of value for Estonian public services. The emphasis must therefore be placed on risk management, with technological changes carefully weighed and more attention paid to security by design.
- RIA constantly monitors the influences stemming from technological advances and the geopolitical environment and the security of the Estonian electronic public services. We must be capable of adapting – updating our security standards and legal environment – as well as participating in dialogue on developments that are fundamentally important to the functioning of Estonia's electronic services, such as retaining strong encryption even in the context of the fight against terrorism.

THE RISE OF AI ATTACK TECHNOLOGIES

Last year showed that computer networks and information systems are becoming smarter and more autonomous. The 2016 DARPA cyber challenge* featured autonomous systems going head to head for the first time. Computer networks sought out each other's weaknesses and patched themselves autonomously, without being controlled by humans. This ability is something that today only the world's top research institutes are capable of, but we can expect that sooner or later this ability will come into the hands of hackers and actual attack systems.

* http://archive.darpa.mil/cybergrandchallenge/.

RIA cyber security branch in 2016

The activities of the Cyber Security Branch are based on three central focus areas: prevention and resolution of cyber security incidents; managing risks to vital services' information systems and the Estonian information system; and consolidating a network covering the Estonian cyber security community – vital service providers and heads of security at government institutions in particular – in order to promote exchange of information and high competency at this level.[30] To support these three main areas, the Cyber Security Branch organises a number of cross-sectoral activities. They include notification and information outreach with regard to the public and specialists, organising and supporting exercises, research and development, and engaging in developing a legal space that ensures cyber security, as well as international cooperation. This chapter recaps the most important activities for the unit in 2016.

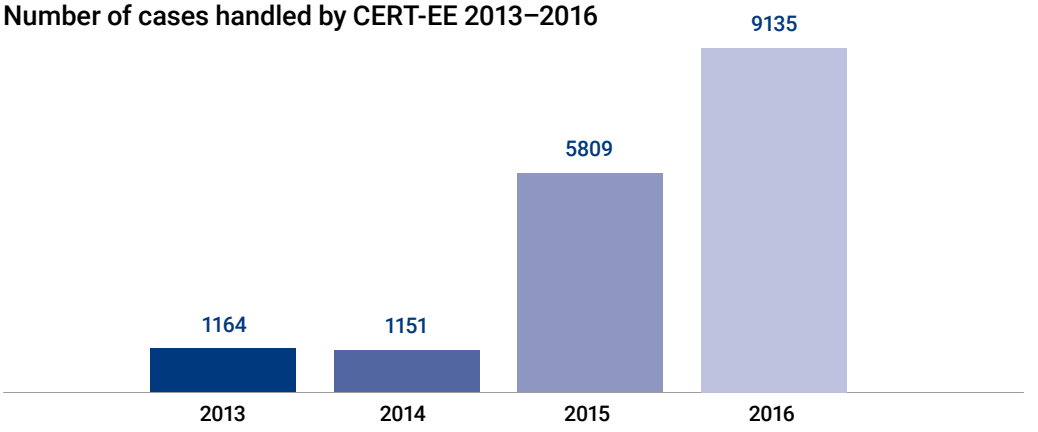
30 Statutes of the Estonian Information System Authority (Minister of Economic Affairs and Communications regulation no. 28 of 25 April 2011; RT I, 29.12.2016, 14) § 13.

Prevention and resolution of cyber incidents

CERT-EE organises monitoring of cyber incidents and monitors, identifies and resolves security incidents in Estonian computer networks. Besides monitoring and resolution of incidents, a key area of activity for developing cyber security is the constant improvement of situation awareness in Estonia at both the technical and strategic level.

In the past year, around the clock monitoring of Estonian cyberspace has given us a much better understanding

Number of cases handled by CERT-EE 2013–2016



of developments in Estonian cyberspace. The number of cyber incidents identified and resolved by us has also increased significantly in that space of time.

Continuous development of situation awareness is necessary both through securing resources and developing the legal space. We work to ensure that a number of components – cyber incident identification, monitoring, analysis, risk assessment and oversight as well as notification and information activities related to threat assessments and developing security rules systems – all function as a unified system.

TOOLS AND SERVICES PROVIDED BY CERT-EE

Web-based anti-virus tool
CERT-EE provides an online tool for users of the government institutions' data network and private sector partners, meant for scanning suspicious email attachments and other files of uncertain origin. The advantage of this tool over similar ones found online is that the files uploaded are not left in limbo in unknown locations but rather are located on the Estonian government authority's file server and deleted regularly.

Reporting IT security incidents
https://raport.cert.ee
This environment can be used to send RIA a report on an IT security incident. It is meant mainly so that government departments and service providers can send more detailed information. A basic incident report can be sent to the address cert@cert.ee as well.

File transfer environment
https://paste.cert.ee
This tool allows suspicious files to be sent to CERT-EE for analysis. It is suitable for sending phishing e-mails and related attachments, samples of malware and the like.

CERT-EE sandbox
http://cuckoo.cert.ee
File analysis tool for IT specialists, allowing them to check in safe mode how operating systems on various virtual and physical platforms behave when a suspicious file is opened.

CERT-EE warnings and notices
https://twitter.com/cert_ee
The most efficient way of keeping up to date with reports and warnings from CERT-EE (in Estonian).
Daily news summaries (in Estonian)
A summary of cyber and IT news from public sources, published every day and delivered to subscribers by e-mail.

Risk management

RIA's risk assessment activities are mainly aimed at raising security risk awareness among public sector and vital service providers and management. In cooperation with vital service providers, we conducted security tests of information systems last year to give companies a better overview of where their vulnerabilities and risks might lie. Where incidents emerged and in our responses to the incidents, we provided consultation to vital service providers; we moreover organised sector-specific information events and exchange of information. Where possible, we involve vital service providers in domestic and international cyber exercises.

With regard to raising the security level of the Estonian information systems, we have set a clear goal of making sure that the compulsory baseline information system security system ISKE is actually implemented by administrators of databases of government authorities and local governments. To do so, we have simplified the system for implementing ISKE, without making any concessions in the actual level of security requirements. In addition to opening the ISKE portal[31] in 2015, we re-structured the contents of ISKE, as a result the volume of ISKE was cut by approximately one-fifth. This year, we are continuing the work started and revising the text so that it is more specific and better graspable. Along with the new version of ISKE established in early 2017, we also modified the implementation and audit guidelines. In order to develop the ISKE tool, we will conduct a procurement in coming years to build a solution that will simplify the work of the implementers, giving a better overview of information assets and interlinks between the assets, and enabling more fluid reporting.

In the first half of 2016, an ISKE working group evaluated the sustainability of ISKE as the system that guarantees the Estonian information system. An assessment of alternative risk management-based methods led to the conclusion that ISKE is the optimum method for public sector institutions and a transition to some other methodology that would result in an equivalent level of security would not mean a lower burden for users but rather additional expenditure. We

31 https://iske.ria.ee/.

PUBLICATIONS AND AWARENESS RAISING TOOLS BY RIA

RIA-commissioned research reports (in English)

Cryptographic Algorithms Lifecycle Report (Cybernetica 2016)
https://www.ria.ee/public/RIA/Cryptographic_Algorithms_Lifecycle_Report_2016.pdf

Vital Service Dependencies (KPMG 2016)
https://www.ria.ee/public/publikatsioonid/Summary-Study-Mapping-the-Factor-which-Influence-Provision-of-Vital-Services.pdf

RIA blog
https://blog.ria.ee
Includes lengthier analyses, guidelines and other writing on salient topics, including cyber security (in Estonian).

therefore set a course toward updating ISKE information security rules and ensuring that the rules are fully appropriate for conditions in Estonia. We recognise that there must be greater cognisance of the cross-use of information systems and the intertwined responsibility of private and public sector for the functioning of society. Development of ISKE must become a regular and continuous process, for which funding and legal and administrative framework must be ensured.

The Branch's supervisory division performs oversight regarding implementation of information security measures. This division verifies that ISKE audits are conducted, determines risks and draws attention to shortcomings. Alongside the supervisory proceedings set out in legislation,[32] the supervisory division also carries out supervisory activities that may not necessarily culminate in proceedings if it is possible to achieve the desired result by less invasive means. The division furthermore draws attention to preventive measures (raising awareness, advising ISKE implementers etc.) to help to prevent potential losses.

Regular meetings of a Security Managers Committee, consisting of sectoral experts, take place for the purpose of development and organising security of the state's information system. We use the committee as a forum to coordinate the activities of security managers and exchange best practices related to organising cyber security.

32 The Public Information Act (AvTS), the Emergency Act (HOS), Electronic Communications Act (ESS) and, starting from last year, the Electronic Identification and Trust Services for Electronic Transactions Act (EUTS).

Cross-sector activities

Awareness raising and training

RIA's notification activities in 2016 were mainly aimed at increasing end user awareness. On our website and over our social media channels, we dispensed practical tips for steering clear of ransomware, keeping e-mail accounts secure and avoiding risks lurking on social media. As a separate public communication initiative, we focused on the adoption of stronger encryption on national authentication systems: we provided guidance to various user groups on how to replace the encryption components of ID cards, residence permit cards and digital ID documents (including the e-residency card) by remote updates.[33] More than 70,000 people updated their documents during 2016.

The media covered RIA's activities with regard to the implementation of the X-road in Finland, and there was also interest in the cross-use of databases across national boundaries. Threats on social media and crypto-ransomware infections received frequent coverage. In early autumn, there the Dropbox data leak was covered by the media, as it affected a number of senior state officials. During October's IoT attack against American service providers, we provided information to our Estonian audience regarding

33 For the transition to stronger encryption, see the subsection on electronic identity.

the nature and scope of this new type of attack. In the RIA blog, we posted longer articles, explainers and guidelines on cyber security topics.

In 2016, we carried out a series of trainings for raising cyber security awareness, focusing mainly on two main target groups: vital service providers, and public servants at the state and local government level. Among vital service providers, trainings aimed at healthcare and energy sector companies were of top priority in 2016; about 400 people took part in the medical staff trainings. Also last year, in connection with preparations for the presidency of the Council of the European Union, we launched training with a goal of raising cyber security awareness among public servants involved in presidency activities across the ministries and agencies involved.

Over 300 people attended either the cyber security officer training or the introduction to cyber security training. In 2017, we will continue trainings and broaden the target group to include key persons at government authorities and vital service providers and organisers, including mid-level managers and executives.

Emergency preparedness and exercises

One of RIA's fundamental tasks is to ensure preparedness for potential extensive cyber incidents. To ensure coordinated nationwide readiness for emergencies and rapid and effective resolution of emergencies, RIA and its partner agencies updated the national cyber incident emergency response plan, which was then approved by the Cabinet in May 2016.

The most significant change compared to the previous plan was the definition of the nationwide coordination level and its functions: if an extensive cyber incident takes place, RIA will form an operational staff involving, in various capacities, government authorities and other affected parties. The plan was tested for the first time in the nationwide cyber exercise KüberSIIL and exercises held in 2016 also ran drills to test this scenario.

In June, the RIA-led exercise RIA Operatiivstaap (RIA Operational Staff) took place where we tested interagency exchange of information and cooperation in resolving cyber incidents with significant impact. Along with RIA, six medical and transport service providers participated; agencies in the jurisdiction of the Ministry of the Interior and the Ministry of Defence also took part.

In autumn, cyber exercises carried out at the EU and NATO level took place, where Estonia's participation was led by RIA. Government authorities in the defence (including the Defence League cyber defence unit) and civilian sectors took part in the NATO exercise. The largest exercise in the EU, organised by the European Union Agency for Network and Information Security, ENISA, and called Cyber Europe, had participants from among Estonia's private sector vital service providers in the ICT and transport sectors.

The exercises show that various agencies have good technical competence for resolving cyber incidents. The most significant shortcomings are related to sufficiency of Estonia's legal framework to address events in the cyber environment. Among other things, there is a lack of measures for directing the work and

resources of agencies during crises. The exercises have also highlighted the need to supplement procedures and recovery plans to be able to cope with extensive incidents. These aspects are also essential for ensuring interoperability and effective action of various authorities in resolving extensive incidents.

Bilateral exercises organised by RIA with international partner authorities should also be noted. These exercises aim to improve cooperation in resolving international incidents. In addition to the practical lessons learnt, these exercises are important for strengthening ties with strategic partners.

Cyber security legal framework: does Estonia need a Cyber Security Act?

RIA's 2015 annual cyber security assessment[34] highlighted a number of technological and legal developments that create a need to update the legal framework in cyber security. Implementation of the Estonian government cloud[35] requires amendments to legal acts to ensure protection of confidentiality of information subject to access restrictions on the one hand, and availability of public information that is processed using cloud solutions, on the other. Estonia's cyber security safeguards are also affected by the new Emergency Act recently passed in Parliament, which reorganises the basic principles for ensuring business continuity of vital services, but leaves open organisation of cyber security of key services that depend on ICT. Finally, the need to transpose the EU's NIS directive[36] into national law should be considered: among other things, it makes it compulsory for vital service providers to report cyber incidents. All these circumstances will inevitably lead to changing the legal norms governing the sector.

In 2016, RIA commissioned a legal analysis of the cyber sector,[37] to determine whether the existing sectoral legislation – and possible supplementation of the acts with cyber security-specific provisions – is an effective and sufficient legal mechanism for ensuring cyber security, or whether a specialised piece of cyber security legislation should be developed. As a result of analysis of the applicable domestic cyber security, IT security, national defence and other sector-based legal acts, the study drafters highlighted gaps in the legal environment and problem areas, and made proposals for supplementing legal acts.

The analysis concluded that extensive review and refreshing of regulations in the cyber sector is necessary and that it would be expedient to do so by way of a specialised cyber security act. The main arguments in favour of a specialised act were legality, legal clarity and efficacy.

Currently, RIA's preventive and planning functions stem mainly from the authority's statutes, while RIA's role as a supervisory institution is set forth in

34 https://www.ria.ee/public/Kuberturvalisus/RIA_kuberturbe_aruanne_2015.pdf.
35 https://www.mkm.ee/sites/default/files/eesti_riigipilve_kontseptsioon.pdf.
36 http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148
37 A legal analysis of the current Estonian cyber security legal framework was commissioned by the Estonian Information System Authority from LEXTAL law offices and funded from the support scheme funded by EU structural assistance, "Raising awareness of information society". https://www.ria.ee/public/Kuberturvalisus/Kubervaldkonna-oigusanaluus-Lextal-2016.pdf.

various sector-specific pieces of legislation. The analysis pointed up that in areas where RIA's functions restrict personal liberties in regard to the organisation of security of information systems and networks, RIA's role as responsible for handling and resolving cyber incidents should be set forth by law. Due to their fragmented nature, the current legislative provisions on cyber security are not transparent for public sector institutions or for contractual partners or vital service providers who have to fulfil the requirements.

The analysis also found that RIA's effectiveness in evaluating risks related to network and information systems is unjustifiably dependent on whether the person conducting the risk analysis considers that evaluation of network and information systems is necessary. Analyses of business continuity and risk analyses do not currently contain an obligatory assessment of the cyber security of service.

A specialised sector-specific act would allow the rights and responsibilities needed for ensuring cyber security to be more clearly and accurately specified and thereby ensure the more effective performance of RIA's functions and better verifiability.

The legal analysis of implementation of the government cloud strategy[38] did not meet with fundamental obstacles that would rule out implementation of the solutions planned in the strategy, but did disclose a need to introduce moderate amendments to Estonian legal acts. For instance, before cloud technologies could be adopted, the Public Information Act would have to be updated, so that the duty of implementing security measures regarding restricted-access information in order to ensure integrity, availability and confidentiality of information would rest not only with the information possessor but the cloud service provider as well. Likewise, the existing support systems to state information system need to be expanded to include requirements for data processing in the cloud or, alternatively, the ISKE implementation guidelines should take into account the specifics of cloud data processing. The analysis also drew attention to problem areas in implementing requirements from the Personal Data Protection Act in the case of data processing in the cloud.

Drafting specific proposals furthermore requires the use or terminology (including basic terms such as digitaalne järjepidevus (digital continuity) and andmesaatkonnad (data embassies) that are related to government cloud to be defined clearly and unequivocally. Fundamentally, the prior definition of the goals of implementation of the concept and organisational structure is inevitable for updating the legal framework.

The state's secure data exchange layer – the X-road – expands

2016 saw the start of changes of a technical and organisation nature in the

38 The law office of Sorainen prepared the legal analysis for implementing the government cloud strategy. It was commissioned by the Ministry of Economic Affairs and Communications and as a result of a public procurement carried out by RIA. It was funded by from the support scheme funded by EU structural assistance, "Raising awareness of information society". https://www.ria.ee/public/Kuberturvalisus/Riigipilve-rakendamise-oigusanaluus-2016-sorainen.pdf.

Estonian information system's secure data exchange layer, the X-road.[39]

Among the noteworthy developments of 2016, cooperation started with Finland's Palveluväylä centre for introducing technical changes into X-road. The most important activities with regard to the second-generation X-road v6[40] being implemented in Estonia and Finland are arguably the audit of the solution's code and the monitoring option added to X-road; the latter can be used by the platform administrator and members to get an overview of the functionality of the services and the platform. To improve the transparency of the state's information system as a whole, people are now able to query state databases for information on how their data have been used.

The most important organisational achievement regarding X-road is the updating of the information systems' data exchange layer statute.[41] The new wording provides clearer-cut boundaries of responsibility for participants throughout the X-road ecosystem, lays down better principles for administering the ecosystem and provides more detail regarding the requirements applicable to members. Hence, X-road as a platform will be able to offer members better security. Another important organisational initiative is the creation of a trust-based federation between X-road and Palveluväylä, which will lay a foundation for data exchange between Estonian and Finnish state databases. The cooperation with the relevant Finnish authorities needed for the inception of secure cross-border services will continue in 2017.

In addition to the above, changes have also taken place in the fundamental approach to the X-road in order to improve X-road's security and transparency. The core technology development has incrementally been transitioned to a more open environment and the entire X-road core technology solution has been made public.[42] In the abovementioned government regulation, X-road is defined as a protocol stack – it is as yet not specified in sufficient detail but as a basic choice, this has longer-term sustainability than the past product-based approach.

International cooperation

2016 was a successful year for RIA on all fronts when it came to international cooperation. We implemented a number of important initiatives in the field of cyber development assistance, helped to shape Estonia's progressive digital image and maintain our reputation as a reliable international partner.

In the cyber security domain, RIA has strong cooperative ties with strategic partners in Europe, North America, the Middle East and Southeast Asia. Besides everyday information exchange between experts, 2016 saw regular meetings take place at the political and operational level to harmonise the threat picture, prevent major cyber incidents from taking place,

39 An animation introducing X-road can be found at: https://www.youtube.com/watch?v=Qbe5khu62jg; and a factsheet on the quantitative nature of the layer is at: https://ria.ee/x-tee/fact.

40 https://www.ria.ee/ee/uleminek-x-tee-versioonile-6.html.

41 "Data exchange layer for information systems" (Government of the Republic regulation no. 105 of 23 September 2016; RT I, 27.09.2016, 4).

42 https://github.com/vrk-kpa/xroad-joint-development; https://github.com/vrk-kpa/xroad-public.

and foster smooth cooperation for crises that require a rapid response and coming to the assistance of partners.

Besides bilateral ties with partner agencies, the most important formats for RIA's international cyber cooperation continue to be the cooperation frameworks of the European Union and NATO, as well as the CERTs' cooperation organisations FIRST and TERENA. In the Digital Five (D5) network that joins the world's more digitally advanced countries, RIA continued to contribute in the cooperation area for secure digital identification solutions, led by Estonia. In spring, we held a coordination meeting of the Baltic states' cyber experts in Tallinn, where the three countries reaffirmed their strong commitment to cooperation and mutual understanding.

RIA also supported a number of cyber security development cooperation projects in 2016. RIA experts took part in training missions in Georgia, Ukraine and South America. RIA also joined a consortium of European countries that in 2017 will start implementing the European Union's first cyber development aid project in Africa and Asia. Providing advisory services to countries set to advance their cyber security posture helps RIA expand its international reputation, increase its knowledge and experience, and fulfil Estonia's broader foreign policy goals.

Assessments and predictions for 2017

Digital dependence of vital services is increasing.
More than a fifth of vital service providers depend to a critical extent on ICT infrastructure or services provided by third parties. The impact of interruptions on the functioning of society, the economy and national security is increasingly significant.

The public sector is a target for both indiscriminate and targeted attacks
The main cyber risks faced by the public sector are related to service interruptions in systems on which national security depends and targeted attacks carried out for financial, political or ideological motives. Local governments in particular often lack knowledge and resources for managing cyber threats.

The private sector's awareness of cyber risks is spotty, both on the individual and corporate level.
Small companies and NGOs in particular do not consider themselves a target for cyber threats and fail to invest into security.

Cyber crime is increasingly professional.
The methods for spreading malware are becoming more sophisticated and focus on sectors that depend on time-critical data and which have not thus far prioritised cyber security (healthcare). Targeted attacks are becoming extremely plausible. Cyber crime is no longer the province of a few select masterminds: even laymen can outsource "service" to criminals.

Estonia will continue to be a target for Russian influence operations.

Russia uses cyber operations in tandem with traditional influence operations based on its technological capability, doctrine and foreign policy opportunities. We need to be prepared for an increase in cyber operations in connection with key events on the calendar in 2017.

Emerging technologies and services are vulnerable and security is not keeping up with technological advances.
Use of smart and IoT devices is expanding. So is the potential impact of security risks related to these developments, and they are increasingly becoming attractive targets for cyber criminals. We do not yet have a full understanding of what risks these rapidly developing digital products, services and forms of business will result in. It is likely that the current record levels for IoT attacks will be broken in terms of both volume and novelty of attack methods. In parallel, there will be increasing pressure for improved security of IoT devices.

Most reported cyber incidents happen because of out of date software.
Use of outdated content management software for websites is epidemic in Estonia.

Password-based authentication alone can no longer be considered secure.
Users cannot keep up with the increasing number of passwords and more complicated requirements for passwords. Their coping strategies, including cross-platform use of passwords increase vulnerability. Pressure is mounting for the adoption of more secure authentication methods (two-factor and biometric authentication).

Estonia's legal framework for cyber security needs to be updated.
The rights and responsibilities of organisations charged with ensuring cyber security must be set forth in law, not by secondary acts or internal administrative documents. Estonia's current legal regulation of cyber security is fragmented and lacks transparency for stakeholders.