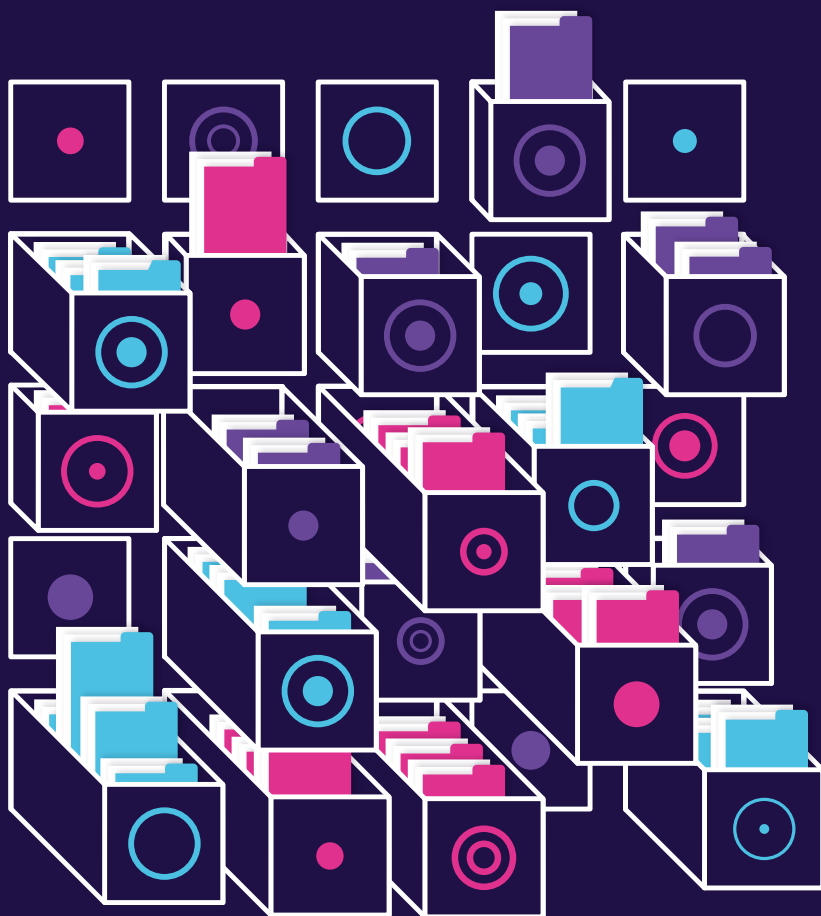




REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Estonian Information System Authority **Annual Cyber Security Assessment 2019**



Contents

Introduction: A Stronger e-Estonia	4
Cyber Security in 2018	
The Situation in Estonian Cyberspace	6
Trends and Challenges in Cyberspace	8
Human Error Cut Connection to Emergency Services	21
How Business Email Compromise Results in Fraud	23
How a Vigilant Community Helped Patch a Critical Vulnerability at Eesti.ee	26
What We Do	
The S4a Monitoring Solution Helps You Sleep at Night	28
Cyber Security of Election Technology	30
Baseline Standards for State IT Security Get a Makeover	32
Security Testing Isn't Black Magic	34
EU Invites Estonia to Help in Asia and Africa	36
CyberSIIL to Return This Year	38
Cyber Security Depends on Cooperation	
Police: How to Prevent Cyber Crime	40
Cyber Ambassador: Rules Must Apply in Cyberspace	43
Views From Abroad	44
Secure Identity	
Estonia Working on Post-Quantum Cryptography	46
Timeline of the New ID Card	49
Cyber Security Strategy 2019–2022	52
RIA's Key Private Sector Partners	56

CYBER SECURITY IN 2018

INTRODUCTION

A Stronger e-Estonia

A chain is only as strong as its weakest link, and 2018 saw a number of events that confirm this saying.

Hundreds of Estonian companies saw thousands of euros go up in smoke due to business fraud, the Land Register narrowly escaped burning to the ground. On a number of occasions, card payments were unavailable across the entire country, the emergency services were inaccessible to customers of one major wireless operator for an entire day. Sensitive personal data on members of the Defence Forces and schoolchildren leaked out, media outlets came under attack, ransomware attacks targeted major companies and general medical practices. The list of incidents can be continued at some length. We received 17,000 reports, which is more than 60 per cent higher than in the year before.



Uku Särekanno
Director of Cyber Security

Yet in spite of it all, 2018 was a good year, with a high level of security. Notwithstanding the dramatic increase in reports, fewer critical incidents were registered than the year before. There were no major international campaigns comparable to Not-Petya and Wannacry. The foundations of Estonia's digital society – such as the ID card and the X-road data exchange layer – remained stable without experiencing any major problems.

A number of basic steps were taken in 2018 that will allow Estonian digital society to remain on a stable footing. The legal framework was tightened and tidied up, and the government decided to allocate significant additional funding to the ICT sector. At the European Union level, the General Data Protection Regulation (GDPR) and the Network and Information Security Directive (NIS) entered into force, while in Estonia, the Cyber Security Act and the Personal Data Protection Act came into effect.

The Cyber Security Strategy 2019-2022 was passed. Its three main focuses are development of a new information security standard, establishing a national cyber security centre and systematic prevention efforts. Indeed, the entire new strategy is informed by the view that an ounce of prevention is worth a pound of cure – the same principle that leads the police to emphasize crime prevention and the Rescue Board on fire safety. Determining the risks and mitigating them is ultimately the more effective and less costly approach.

RIA's function under law is to mitigate risks, raise awareness and ensure that the key components in digital society work as they should. We offer Estonia's most secure state network to 400 establishments and network monitoring services for 15 major corporations, security testing for numerous companies and threat reports for hundreds of businesses. We offer all Estonian citizens and organizations secure solutions for authentication, digital signing and exchange of data.

All of this adds up to quite a lot, but it isn't enough. Above all, we need a broader change in attitude at the level of the heads of government institutions and business leaders –the realization that cyber security deserves attention and it isn't just a matter for IT departments or technicians. If it is neglected, products and services will suffer, reputations will be harmed, and customers and money will vanish. RIA can be a good partner and consultant in this regard, yet it's up to every business leader and senior official to understand the need and responsibility. There's nothing good about being the weakest link.

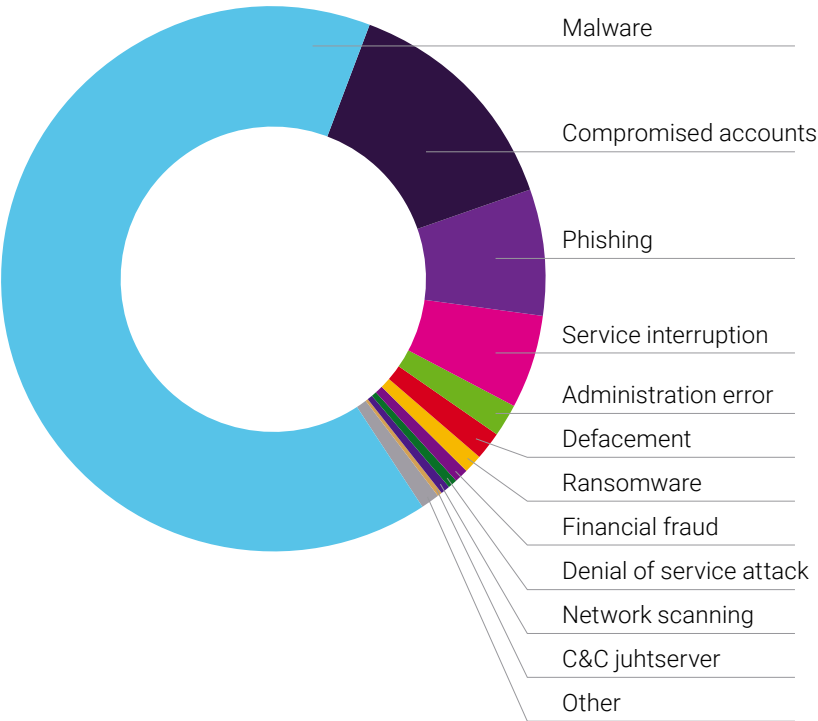
The Situation in Estonian Cyberspace

The new regulations on cyber security and data protection that came into force in 2018 gave us a more systematic picture of the situation in Estonian cyberspace. Compared to the year before, we received nearly double the number of notifications (17,440); among these were 3,390 incidents that had an impact on the data or information systems.

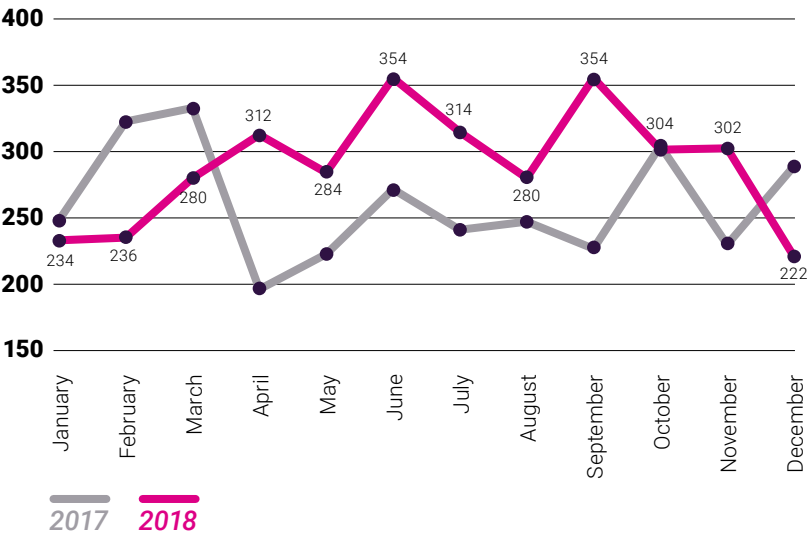
Notifications RIA has received in the last three years.



Incidents registered in 2018 which impacted data or systems



Incidents which had direct impact on the confidentiality, integrity or availability of information or systems.



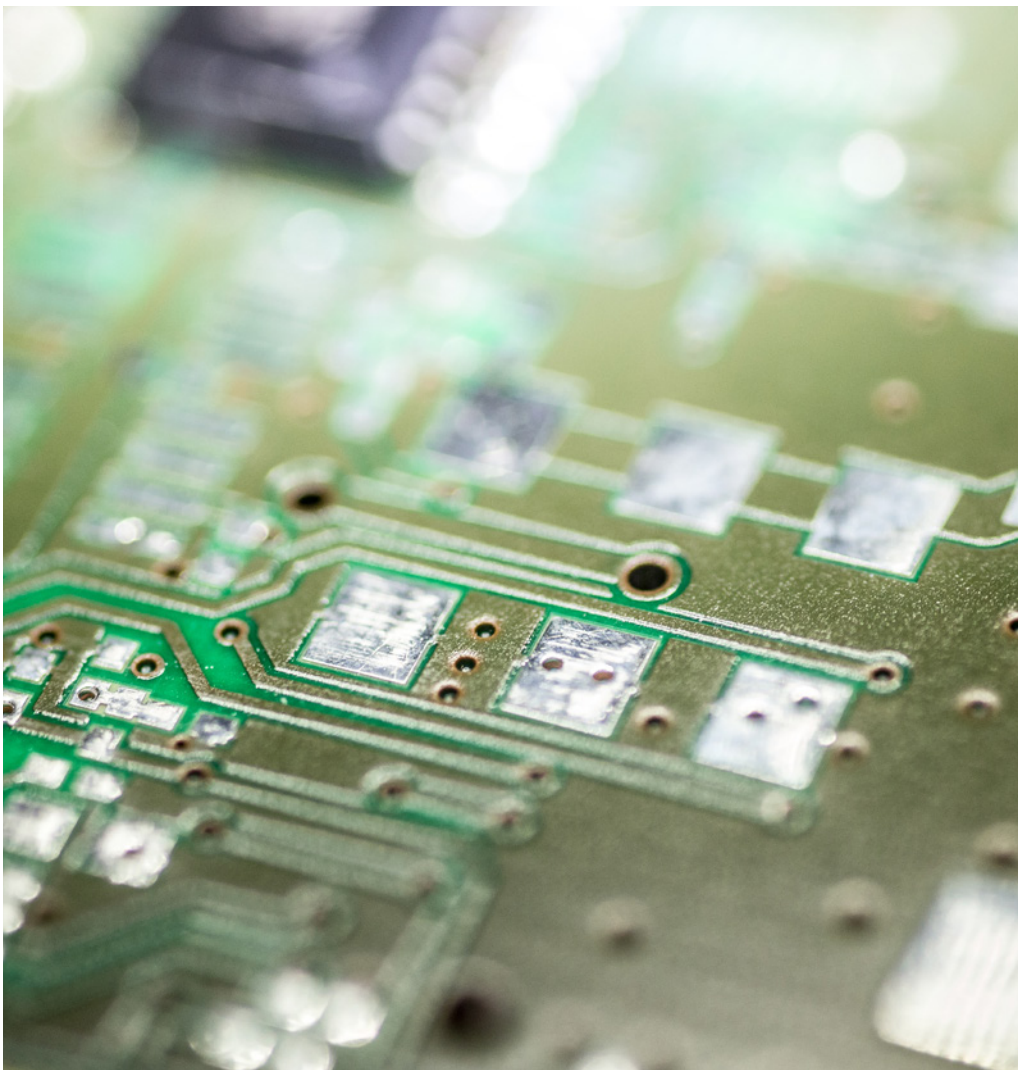
Cyber Security Means Constant Attention

LAST YEAR, WE WROTE: *Security vulnerabilities in mainstream technologies are not a one-time shock but endemic to this environment, and it is clear that attempts will be made to exploit any new flaws that emerge. Security does not end when an information system is completed or a piece of equipment is acquired. Maintaining it means continual work and the first responsibility for the security of a device or system lies with its owner.*

► **THE SITUATION IN 2018:** 2018 saw a continuation of the trend that whenever devices are vulnerable, that vulnerability gets exploited. Last summer, it was discovered that certain internet routers designed for small businesses and home users can be used to conceal malicious activities and information theft and, by the same means, to mine cryptocurrencies. We issued a warning to alert users to the need to update their software. In spite of the warnings issued in the spring, we still see devices in private and public networks use the same vulnerable software that has not been updated.

We also noticed that a large percentage of the email accounts of Estonian companies and institutions continue to be easily spoofed to spread malware or request that funds be sent to unauthorized bank accounts. Some security protocols and technologies for email servers are been around for years but are still not being used.

Web servers and websites with out of date software or security standards applied are similarly being compromised.



If a new security standard is available it can be considered irresponsible to use an older version,

► **THE WAY FORWARD:** Maintaining cyber security in Estonia requires constant effort and vigilance from business and government leaders. Updates and security standards are important and it is also vital to invest time and money into updates and standards. To be able to avoid cyber incidents with a major impact in the future in Estonia, this work must be done. Whenever a new version of software is developed or a security standard is updated, it can be considered irresponsible to continue to use the old version, as it jeopardises the entire organization. That goes for email protocols, web servers, operating systems and communication channels.

Vulnerabilities Will Be Exploited – It's Only a Matter of When

LAST YEAR, WE WROTE: *The threat of a cyber attack does not depend on whether your data are valuable for the criminals but rather whether your data are valuable to you. Most cyber attacks are unselective with regard to the target themselves, but simply hunt for vulnerable devices and user accounts.*

► **THE SITUATION IN 2018:** Companies that sustained losses as a result of hijacking of email accounts in Estonia in 2018 weren't limited to one specific sector or even connected to each other – all it took was one user with a particularly weak password, and they became the attacker's point of entry to the server.

Nor did we see a definite pattern in regard to ransomware victims who had left a door ajar via the Remote Desktop protocol – if such a point of entry was discovered on the server, and an account with a weak password was found, that organization was victimized.

In the case of the most widespread malware campaigns, it also didn't seem to matter to criminals what particular employee accessed the phishing link and downloaded malware on to their computer. An even wider net was cast by criminals who hoped merely to frighten users with the claim that they had been watching them through their webcams.



More and more devices are connected which increases risks for companies.

► **THE WAY FORWARD:** Even now, the average Estonian company starts thinking about cyber security, protection of data and system continuity only after an incident has already occurred. Regulations now require vital services to adopt various measures. In the case of large companies, risk to reputation or income is another incentive. Often, such companies also have the resources for mitigating risks.

But for smaller businesses and home users, devices and systems connected to the internet have become more affordable. Managing and keeping an IT network secure (i.e., human resources) is in higher and higher demand and as a result, is getting more costly. Such a situation can lead to many new weaknesses that criminals will start discovering and exploiting.

Cyber Incidents Continue to Hurt Us

LAST YEAR, WE WROTE: *The [Wannacry and Notpetya] ransomware campaigns caused losses in the billions of euros, and endangered not only property, but the lives and health of people. In Estonia, thanks to prevention and timely response, the losses were minimal. These attacks will not be the last, however.*

► **THE SITUATION IN 2018:** Malware campaigns are not the only ones that cause damage to people and companies. After a short delay, Estonian users were hit by a corporate email hijacking campaign that had done much damage worldwide, attacks on Office 365 accounts, the so-called sextortion campaign, the Remote Desktop Protocol ransomware installation campaign and the Loki-Bot malware campaign.

As a result of financial fraud that could be traced back to hijacked email accounts, Estonian small and medium-sized companies sustained at least 600,000 euros in damage in 2018. More important than the total losses is the fact that for small businesses in Estonia, even a loss of 10,000 or 20,000 euros is a noteworthy blow – we saw such losses happen on an average of once a week. Companies lost customers and turnover and also lost time recovering data when they were hit by ransomware attacks.

We can be sure that the abovementioned sums do not reflect the entirety of the damage sustained by the Estonian economy, as there

were doubtless victims who notified only law enforcement and not RIA. In cooperation with the law enforcement agencies, we sent out a letter to all Estonian companies warning them against cyber fraud. We'd like to thank all of the companies who reported cyber incidents to us last year – only in this way is it possible to get an accurate view of the threats and incidents in Estonian cyberspace.

► **THE WAY FORWARD:** The situation isn't one that can be accepted. Either we make criminals' lives very easy or more difficult. Even companies that pay much attention to cyber security can be harmed because of a business partner who has failed to do so. Criminals look for the weakest link and once they've found it, they try to convert the data to ill-gotten monetary gains.

We will continue our information outreach day in and day out, urging people to follow basic cyber hygiene. Aside from that, we will take a separate look at how can we help with cyber security at Estonian companies. We welcome feedback from company executives and IT personnel as to how we can be of better assistance.



Estonian companies have been victims of fraud when procuring goods from abroad.

Critical Data Require Critical Attention

LAST YEAR, WE WROTE: *In particular, cyber security in the healthcare sector needs more effective support. In a situation where hospitals and family medicine centres process our most sensitive personal data and their work depends largely on the functioning of digital systems, they must not be stranded in a situation where cyber security is competing for resources with healthcare provision.*

► **THE SITUATION IN 2018:** Last year, we saw additional cyber incidents in the healthcare sector and leaks of health records. For example, the information systems at one general practice were encrypted in a ransomware attack that posed significant disruption to service provided to patients. The state's own document management systems had mislabelled data and as a result, Defence Forces members' and schoolchildren's health records were visible. This isn't only an issue in Estonia – leaks of health records and sensitive personal data are occurring all over the world.

At the same time, we worked constantly to enable the healthcare sector to more securely handle information. We organised numerous training courses for hundreds of healthcare professionals across Estonia. General practitioners now have a digital test on cyber hygiene that they can use to develop their skills, and they have been diligent in making use of it. We ordered a separate analysis of nationwide information systems used by GPs to process health data and organize work.



Contemporary medical care relies on the access to uncorrupted health data.

► **THE WAY FORWARD:** The first important step for preventing leaks of personal data is to ensure cyber security. That means systematic implementation of the measures necessary for this purpose, and here, too, it's imperative that heads of organizations devote attention to this. Risks to personal data storage and processing systems must be constantly mitigated, and software updates and changeover to new, more secure standards must take place, regardless of the size of the organization.

In the healthcare sector, for example, general medical practices with small staff size – not just hospitals – must also determine their cyber risks and be able to mitigate them, as required by the Cyber Security Act. To this end, we offer general medical practices training to support them in developing the necessary and appropriate measures. We will also continue administering cyber hygiene training geared at healthcare professionals.

Clearer Regulation Means Clearer Responsibilities

LAST YEAR, WE WROTE: *The Cyber Security Act will bring greater legal clarity but the legislation will not resolve all concerns in the vulnerable sectors. The new Cyber Security Act will bring a more rational system to the roles, terminology and responsibility in organizing cyber security in Estonia, but besides implementation of the act, close partnership with state and private sector institutions will remain important.*

► **THE SITUATION IN 2018:** In mid-2018, Estonian Parliament passed the Cyber Security Act, which established stronger requirements for businesses and government institutions for preparing for cyber threat, management of information systems and databases and reporting cyber incidents. The Act had the most direct impact on vital service providers, such as providers of electricity, medical care or authentication services.

All providers of digital services are required to more stringently guarantee the security of their clients' data, ranging from online retailers to search engines that wish to operate in Estonian cyberspace. To implement the act, an executive regulation was drafted last summer, setting out more detailed requirements for ascertaining risks and security measures.

In late 2018 Estonian government approved the Cyber Security Strategy for 2019–2022, which states the objectives for RIA and other government institutions and foundations connected to the government. We discuss the strategy in more detail in this yearbook as well.

THE WAY FORWARD: The Cyber Security Act laid down specifically who is required to comply with which rules. Last year, persons in the purview of this act had to assess their risks and set out how they intended to manage them. These actions must now be carried out. Thanks to the better and clearer system now in effect, we can presume that providers of vital services and digital services are better protected this year. The new system improves our knowledge about what is going on in Estonia, as a result of which we can expect an even higher number of registered incidents this year.



The cyber security of vital services is in everyone's interest.

Trends and Challenges in 2018

GREATEST PERCENTAGE OF ALL INCIDENTS

Malware and Botnets

The integrity of information systems (meaning that someone has modified the information or information system without permission) was impacted the most. Most of these cases involved botnets, something we've written about in previous yearbooks as well. Despite the regular reports sent to owners of infected devices, we still saw in 2018 that devices from thousands of IP addresses contacted botnets on multiple occasions.

How botnets are exploited by criminals

A component of a botnet can be used for a denial of service attack or for spreading malware (e.g. for theft of bank data). An infected device may also be used for downloading some malware – for example, a botnet is leased out to criminals who are looking to expand the circle of malware recipients (crimeware-as-a-service infrastructure).

In the public sector, malware infections are rooted out quickly. In most cases, the bot (the infected device) identified in the public sector jurisdiction is an individual's infected computer that they have decided to use at that moment over some public WiFi network, and they were assigned a public sector IP address.

If a botnet-infected device is discovered in a private sector network, the ISP is alerted. But the information may not reach the end user, and even if it does, they may not realize what the implications are and how their computer can be protected.

INCIDENTS THAT RESULTED IN THE GREATEST MONETARY LOSSES

CEO fraud scheme

This is a form of financial fraud where an accountant receives a brief query purporting to be from the CEO and asking that money be transferred quickly to an unfamiliar bank account. Usually an unfamiliar email address is used with the CEO's name just added as the account holder.

Financial fraud originating from compromised corporate email accounts

Last autumn, we started receiving reports of a scheme a couple years old where criminals try to swindle money out of companies by using compromised email accounts and content of email correspondence. In one phase of the extended exchange of emails, the compromised partner requests bank account data for a transfer between companies. For a short period of time, neither party is aware that the email correspondence has been hijacked.

NOTICED, BUT GENERALLY HAS NOT MANAGED TO CAUSE DAMAGE

Sextortion

In summer 2018, the world saw a wave of extortion attempts where the criminals tried to frighten recipients by claiming that they had access to the victim's IT devices and knew which websites the person had visited. To make the extortion attempt seem plausible, criminals used passwords leaked over the years and included one such password, email address or telephone number in the email sent to the target. A majority of the passwords used by criminals leaked many years ago.

HAS MAINLY CAUSED DAMAGE IMPERCEPTIBLY

Use of computer power for mining cryptocurrency

With the rise in popularity (and price) of cryptocurrencies in late 2017, criminals tried to find better ways of amassing it – mining it usually requires electricity and processing power. Computers with publicly known vulnerabilities (such as routers in home use) running outdated software gave attackers easy ways of harnessing other people's computing power. A trend spotted in the first half of 2018 in particular.

WHERE INCIDENTS OFTEN STARTED

Phishing emails and malware distribution emails

We saw a number of campaigns where emails containing malware or phishing attempts were sent purporting to be from well-known companies. RIA is aware of only a few cases of actual infection – users have become more aware of the dangers opening attachments in unfamiliar emails and filters often catch such emails. Yet users still fall victim to phishing emails where user data is stolen. Passwords entered in the wrong field often led to new cyber incidents such as follow-up phishing emails, financial fraud and malware distribution.

WHICH IMPACTED THE GREATEST NUMBER OF PEOPLE

Service interruptions

Estonian society is heavily dependent on digital services, ranging from authentication to healthcare services. Thus, short-term downtime in public sector networks affected the greatest number of people. These were often caused by administrative errors.



Human Error Left a Wireless Operator's Subscribers Unable to Reach 112

The year's incident with the greatest impact occurred near the very beginning of 2018. On 24 January, many of Elisa Estonia's customers were unable to call the emergency number 112. Over eight and a half hours, 151 people tried to place 600 calls but could not get through. Luckily, the incident resolved before serious consequences occurred.

Although the first unsuccessful call from the Elisa network was made to emergency services at 10:40am (the callers received the "Number is not in service" message), the problem was identified only eight hours later. The Ministry of the Interior's Information

Technology and Development Centre (SMIT) staff learned of the problem at 6pm, when an Elisa customer who called the police information line notified them that it wasn't possible to call the emergency number.

SMIT technicians alerted Elisa and the emergency services centre learned of it only a few hours later. Fifteen minutes after receiving the information, an Elisa technician modified the network configuration, and the problem was resolved by 7pm.

The problem was caused by a change made to the network con-

figuration the same morning. While resolving an earlier bug, it wasn't noticed that the problem also affected calls to 112. While not all Elisa customers were affected, it did cut off mobile users connecting from one central switchboard, including customers of foreign operators who were using Elisa roaming service. It isn't known how many customers found alternatives for calling for assistance – such as using a different phone, removing the SIM card or calling the police at 110.

The incident showed dramatically how a minor technical error could lead

to a situation with a direct impact on people's lives and health.

Elisa didn't notice the problem and learned of the incident only thanks to the IT and Development Centre.

For Elisa, the critical incident sounded a challenge as to how improve fault identification and notification capability within the company and develop measures that would rule out similar situations arising in future. In 2018, we saw clearly how awareness of different risks grew at Elisa and steps were taken to keep a similar situation from recurring.

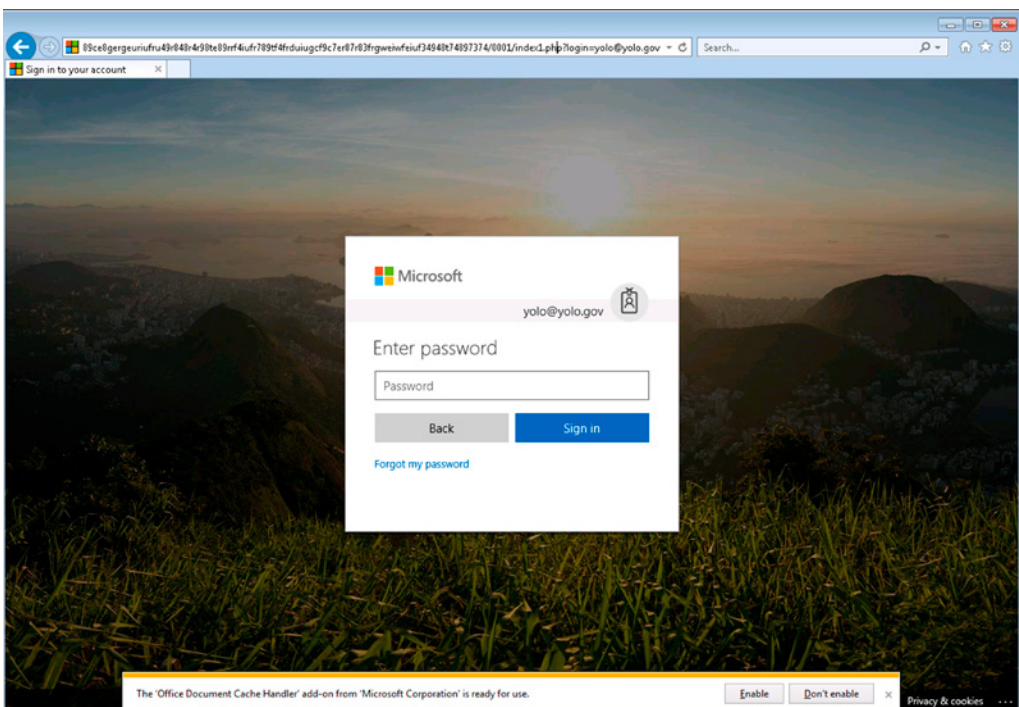
Elisa Eesti AS communications director Marika

Raiski: The incident at the start of 2018 was caused by human error and regrettably it is hardest for a company to have to defend itself against such errors. In light of such incidents, we always review internal fault notifications and information movement process and learn from our mistakes, by training and teaching Elisa employees based on the experience gained.

To keep the same situation from repeating, we have made improvements to the planning of changes. For example, we now carry out tests ahead of time when planning changes that may affect calls placed to emergency services or other priority numbers. Before making the change, we also plan system recovery actions that will allow us to restore the previous system state quickly if a problem arises.

How Business Email Compromise Results in Fraud

Last year, different types of financial fraud caused the most economic losses. Some of them were simple spoof emails requesting that a company's accountant send funds to an unknown account. In other cases, financial fraud started with a simple phishing attempt that gave the criminal access to an employee's email account.



An employee of a particular company received an email on July 9th asking them to confirm their email account data by accessing a link in the email. The employee did so, which took them to what appeared to be the Microsoft Office 365 login page. The employee entered their username and password, upon which they were told that the data were in order.

About three weeks later, at the close of business on July 25th, the criminals emerged, sending out about 600 phishing emails from the compromised email account within the space of 18 minutes. The company's head of IT blocked the employee's account, changed the password, checked for malware on the computer, and not finding any, reopened the email account. This flurry of emails was just a diversion by the criminals, though.

It was two months later that the company's business partner alerted the company to the fact that they had been communicating with an unknown person since July 17th who purported to be an employee of the company. The business partner was misled to conduct a transaction (involving a noteworthy sum) to the bank account number supplied by the criminals.

WHAT TO DO IF YOU SUFFERED A BREACH?

Considering the trends of exploiting email accounts, RIA recommends businesses and organizations closely scrutinize all incidents where employees' email accounts were accessed.

Teavita oma koostööpartnereid

Notify your business partners

Criminals may lie low for several months before they attempt to use your business or organization as a cover for trying to defraud your partners. If an employee at your organization has their email account compromised, alert your partners immediately that you have fallen prey to a crime that may later have an impact on partners – if someone on your side starts talking about changes to bank account details, your partners should be alerted. This sort of an important change should be confirmed through multiple channels. In this

way, you show your partners that you take security seriously.

Take good care of your name

While SPF, DKIM and DMARC procedures might strike the layman as overly technical concepts, for experts they are elementary and inexpensive ways to reduce the possibility of criminals using your name to send out phishing attempts or malware. Make life much harder for criminals!

Use multi-factor authentication if possible

Think about how your company could use multi-factor authentication to make it as hard as possible to access emails from a computer. Besides major international providers, a number of Estonian service providers have also enabled two-level authentication.

Similar incidents were seen regularly last autumn – email correspondence was monitored for a longer period of time; then the criminal intervened at the exact moment of the transfer to provide bank account details. The victims included both Estonian companies and their business partners in other countries. For that reason, together with the Police and Border Guard Board, we sent out a warning to that effect to all Estonian companies.

RANSOMWARE ATTACKS CONTINUED TO DISRUPT BUSINESS OPERATIONS

Alongside financial fraud, Estonian companies were also impacted by ransomware attacks, as a result of which organizations lost potential customers and also valuable hours of work. Ransomware attacks have received much attention in recent years. Last year we also saw cases where companies' security measures succeeded in staving off losses.

For example, Estonia's biggest office supply company Büroomaailm was hit once again by a ransomware attack last year, but this time it was ready for it. "We were attacked over the RDP protocol. The attackers gained access to our terminal server and infected it with a cryptovirus," said Büroomaailm's head of IT Sebastian Sõeruer.

"The problem actually lay in one of our terminal servers, which was outdated. It wasn't protected by our company's security policy yet was still being used. This made it easy to attack and access our server," he said. "This is the third case of its kind over the last three years where we have been hit by a cryptovirus."

Previous experiences led to the company developing readiness, and now such incidents can no longer cause serious damage to its IT systems. Sõeruer says that the damage from this attack was limited to about six of his own hours at work and a few rows in a spreadsheet.

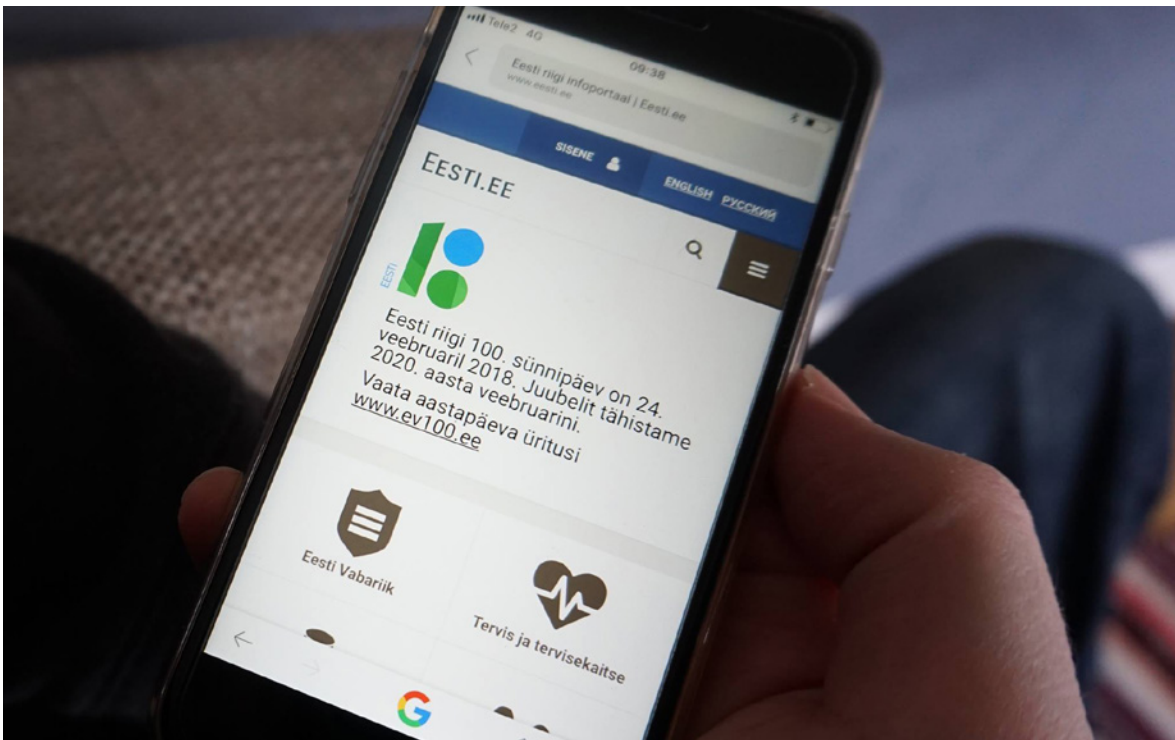
The first measure for protecting oneself against all kinds of incidents, said Sõeruer, is the making of backup copies, advisably in multiple locations. Sõeruer has developed a multi-level backup system – virtualized server copying, regular backups to external hard drives in different physical locations, use of cloud environments, etc. "The importance of backups cannot be overestimated," he said. Secondly, he said strict control of user privileges is important – a poor decision by one user shouldn't cripple the whole system.

Estonian Cyber Community Helped Us Patch a Critical Vulnerability at Eesti.ee

On June 29th, cyber security experts at an Estonian company notified us of a security vulnerability on the state portal eesti.ee, which if exploited could allow a person to log into the state website as a different user, using a bank link. Upon realizing the seriousness of the situation, we disabled the option of entering the state portal via a bank link and started to fix the vulnerability and mitigate the risk. This took four days.

The vulnerability lay in the fact that the eesti.ee website, upon receiving an authorization query via a bank link, did not verify whether it was signed with the bank-provided key and whether it met the technical specification of the bank link. The flaw allowed the portal to be entered as a different person if the person logging in used the bank link's technical specification to generate an illegitimate bank confirmation themselves and was able to send it to the eesti.ee portal as a login confirmation. In other words, a successful attack would have required quite an advanced level of technical knowledge and acumen.

The vulnerability stemmed from eesti.ee's outdated platform and was not connected to any bank or other e-service. In a later investigation, we determined that the flaw arose in the course of modifications made to the basic software of the website in October 2015 and in the course of introduction of a new bank link. It wasn't a malicious error but just a lapse on the part of RIA and the developer hired by RIA.



Use of bank links makes up about 30 per cent of logins to Eesti.ee in a given month – a typical month sees 100,000 logins via bank link.

To determine possible losses or malicious activity we checked the state portal entry logs since the date of the modifications. The review of the logs, which lasted several days, turned up nothing indicating that the vulnerability had been exploited. No one's data had been compromised and no improper logins were recorded. After several days of intense work and security testing by external experts, we restored the bank link login functionality on July 4th.

This episode showed that even we are just as capable as anyone else of making mistakes in developing information systems and the lessons learnt from this case led to several changes in our development process to keep such incidents from recurring. The vulnerability was discovered only thanks to the Estonian cyber security expert community outside RIA, who remain vigilant in ensuring that Estonia develops a digital society that is just as secure as it has been to this point. Thank you!

WHAT WE DO

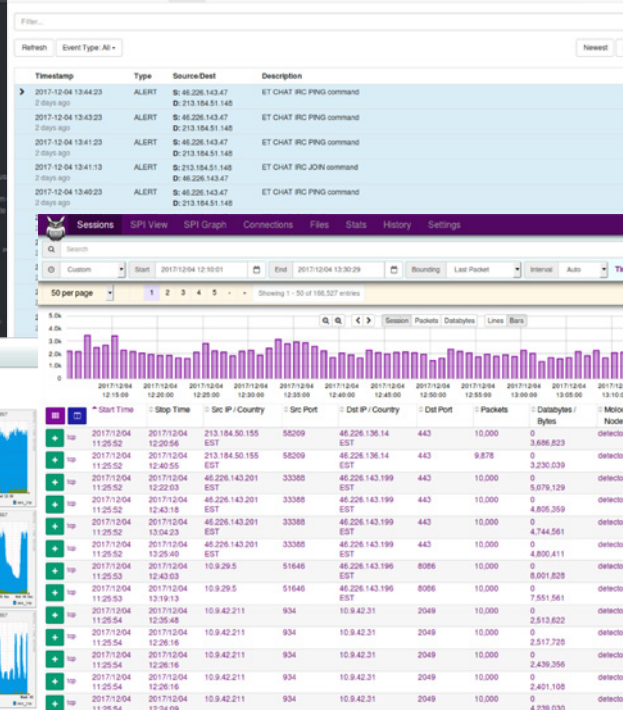
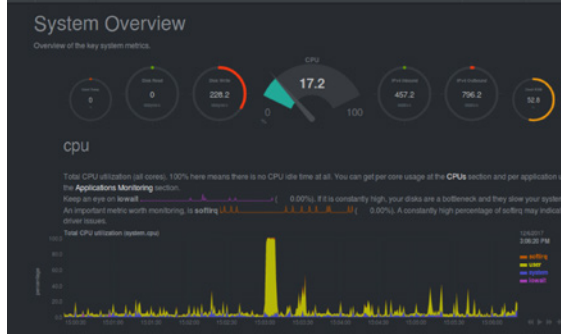
The S4a Monitoring Solution Helps You Sleep at Night

To reduce the time needed to detect and respond to cyber incidents in Estonia, RIA has developed and started offering companies an automated solution called Suricata-4-all (S4a), made possible with EU support. Using this system, we can share the attack indicators we know as rapidly as possible with our clients and support institutions in detecting malicious network traffic.

S4a is a freeware-based network traffic analysis system that makes it possible to detect attacks and malware – and in some cases, vulnerabilities and configuration problems as well. Rules – essentially the indicators that the system should identify – are regularly updated by the community and by us based on the worldwide threat landscape.

The name S4a derives from its main component, the Suricata free intrusion detection system, which uses a rule/signature-based method for identifying attacks. While Suricata is freely useable and installable on any network, monitoring and updating intrusion identification indicators can take excessive time and money.

This is where we come in and can help Estonian companies and service providers with our knowledge, based on identified risks. The S4a solution consists of a central system at CERT-EE and sensors which the network owners can install at their company or organization. The central system sends the sensors rules (which are used to identify the attacks) and the sensors send reports to the central system whenever they identify malicious traffic.



S4a uses a mix of tools to increase detection into your systems.

In addition to identifying intrusions, the system provides the option to record, index and analyse network traffic. This gives organizations that have installed the sensor the possibility, if problems arise, of analysing network traffic and request our help for doing so.

The intrusion detection system establishes the initial attack vector and saves fragments of malicious network traffic that match the description in the rules. Using additional analysis of network traffic, it is possible to get a more detailed view of attackers' activity that the intrusion detection system alone cannot distinguish from ordinary network traffic.

Security Begins With Taking Responsibility

Cyber security always starts with each organization's responsibility to determine and neutralize their own risks. Institutions that provide important services in Estonia are always subject to the duty to hedge risks and report incidents. S4a gives organizations an additional layer of security and refines the view of the situation in Estonian cyberspace.

To join the system, prospective users should acquire the required software and ask cert@cert.ee for the installation software. Write us and ask whether S4a automated network monitoring can be a useful solution for your company.

Cyber Security of Election Technology Means More Than Just Online Voting

2019 is an election year in Estonia – both parliamentary elections and European Parliament elections are being held. As no elections were held in 2018, it allowed us to look more systematically at security of technological solutions used for elections. Under the aegis of the Europe NIS Directive cooperation group, and led by Estonian and Czech analysts, a manual on election security for European elections was prepared in June 2018, consisting of practical recommendations and examples of how voting has been kept secure to this point.

As far as the public is concerned cyber security of elections has largely meant discussions about the security of internet voting. There has been public discussion about how transparent the process is for the ordinary voter, and how to ensure that a given person's vote is definitely recorded and that observers have a way to monitor the whole process.

But security of elections is about more than online voting. The US and French experience in 2016 and 2017 showed that the candidates were the victims of cyber attacks. Bulgaria and the Czech Republic saw DDoS attacks in 2015 and 2017 targeted against their election services' websites. In addition, all sorts of media outlets and platforms are vulnerable to being used to spread misinformation and disinformation. They also have a critical role in publicizing the election results.

The abovementioned manual examined methodically all stages of elections from candidate registration and voter lists (which are likewise based on electronic channels) to protection of platforms for releasing election results. We approached the security of elections in 2019 based on European best practices – the experiences of our partner institutions.

The government allocated close to 304,000 euros for raising the level of information and cyber security of election information systems. These funds were used for commissioning DDoS countermeasures for the government network, increasing the volume of testing and buying hardware to allow online voting to run smoothly under a higher load.

In cooperation with the State Electoral Office, RIA provided cyber hygiene trainings for candidates and campaign teams. On four occasions – three times in Tallinn and once in Tartu – we held events about how elections could be jeopardized and how to protect email and social media accounts.

In cooperation with State Electoral Office, we offered Estonian political parties the possibility of checking the state of security of their websites and email servers – how servers appear to potential attackers. All the parties represented in parliament decided to take the opportunity. We sent each party sealed envelopes in which we asked them to devote attention, where necessary, to the use of security standards, such as configuring protocols like SPF that make email servers more resistance to falsification, use of HTTPS and other possibilities for preventing attacks.

During 2019, our role is to be a partner for the State Electoral Office, not only keeping internet voting running but also having the capability of taking a broader view of electoral cyber security. Our next plans are to update the application for entering the results of elections – the election information system, the new version of which should be tested and ready to go by the 2021 local elections.



The share of i-voting keeps growing.

Baseline Standards for State IT Security Get a Makeover

The cyber security requirements obligatory for all government institutions and local governments are widely deemed to be too complex to implement and not practical enough to increase cyber security in real-life situations. To protect valuable data and information systems, we are rewriting the security standard called ISKE that is used in Estonia to make it easier to implement and more practical to use on a daily basis.

In 2008, ISKE became obligatory for state and local government institutions that use databases. The security measures described in ISKE are grouped according to categories (organizational, physical and information technology-based) and the need to implement them depends on the security level of databases (low, average, high). As there are many threats and risks, there are also many measures and it makes the standard quite unwieldy and cumbersome.

Thus, we have reached a situation where use of ISKE is more of a formality than a basis for ensuring everyday security. The head of IT for the city of Tartu, Rein Lindmäe, notes that ISKE is important for him mainly at the point when an ISKE audit must again be commissioned. "ISKE isn't one of the volumes on our table every day," he says. "If it were written in more of a human language or it were easier to relate to on a daily basis, it would be much more convenient and better to use."

Lindmäe stresses he has nothing against such a baseline standard in principle. "The basic fundamentals of ISKE are sound but we assess our risks based on slightly different kinds of audits."

For example, instead he commissions attack audits to assess the cyber security of his organization, but doesn't run checks whether the ISKE requirements are met. Lindmäe says the city of Tartu has resources and possibilities to sufficiently assess its own risks, while smaller institutions and local governments may not have them. For that reason, Lindmäe says, ISKE is definitely well worth it.

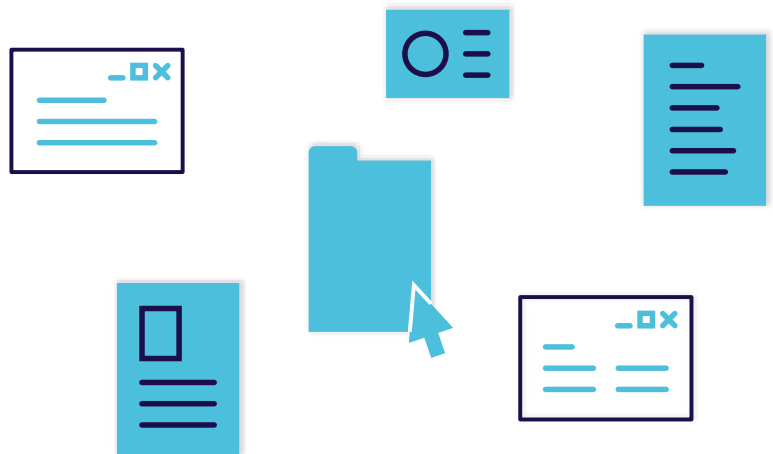
"ISKE could be made simpler, more of a practical document," he says. "In that way it would be of genuine benefit. We can't say that we constantly 'use' ISKE. Yes, we order an audit but we don't check cyber security against ISKE in the case of everyday activities."

Risk Assessment as a Baseline

ISKE has been a requirement for ten years. During that time, it has been regularly updated and supplemented. The rapid development of the IT sector has brought new risks and threats that require new measures and approaches and they have been introduced into ISKE constantly. In addition to the rapid development of IT, organizations have developed as well, and many of them have become more mature and capable. That means that Estonia already has a number of organizations that are capable of applying a more risk-based approach and more precisely assess their needs and possibilities for cyber security.

That is why we have launched the development of a new information security standard that takes into account the size, particularities, capabilities and possibilities of institutions. In

it, we devote more attention to risk analysis, which unlike existing baseline protection enables greater flexibility. The new standard is again based on the corresponding standard in Germany, which has undergone a thorough updates and is already being applied. Although the new standard has many structural innovations and substantive changes, not very many fundamental changes have been made to the principles of data security: just like a door, a computer must be kept locked.



Security Testing Isn't Black Magic

Security testing gives a very good look at the current state of cyber security in any organization, and should not be neglected when introducing new services to market.

For six years, we have organized security testing for providers of vital services in order to ensure cyber security. Tests are carried out by private companies that awarded contracts at public tender. Last year we ordered security tests for six institutions through these channels. This year, we plan to test information systems at seen companies and institutions.

For example, for eight years, Estonia has offered a service called Clarified Security, headed up by Mehis Hakkaja. "It's important to bear in mind that if you order an information system and a penetration test, it should be the direct cost for the customer, not the developer who's awarded the contract. Validation of security should be conducted by an impartial evaluator," says Hakkaja. "It's just like the oversight performed on the construction of a building – the customer has to order this separately."

Hakkaja says Estonia's public sector is moving in the right direction with regard to security of commissioned systems, but the whole life cycle of the development and what can influence this life cycle has to be considered. "Sometimes a security test performed at the end of a massive development project yields a long report that has a large number of findings requiring a rapid resolution before it can go to production. However, the deadlines and the business side need things to be ready now," Hakkaja says, pointing out that security validation is just one small part of the whole chain.

Besides manual security testing, red-teaming is also important. The goal is not to find all flaws but rather the path of least resistance that an attacker might take to achieve their main goals.

"In the case of one major foreign customer we sent them one of their yet-to-be-released stock market press releases to demonstrate that they were exposed to a breach. This and our reports on exactly how we gained access helped this publicly listed company become aware of the serious shortcomings in their security," said Hakkaja. "Reviewing the same company a year later, it's cyber defences were much better, above all with regard to monitoring."

Threats Shift Over Time

Hakkaja warns that threats around the world are becoming increasingly complicated and global. "Just take Estonia's e-Residency programme, which can give anyone in the world access to our information systems. Many systems are built on the presumption that the person logging in with a chip card is a local citizen who can use some e-service. Often information systems use personal identification codes in a lax manner – queries are based on the code and sometimes secondary authentication is neglected – it isn't verified whether the person making the query is the one who should be obtaining data associated with that identification code," says Hakkaja in regard to flaws that potentially make Estonian information society more vulnerable to attacks. "Basically, we distribute keys to our amazing solutions all over the world, but can we also protect these solutions from this wider audience?"



*Mehis Hakkaja,
Head of Clarified
Security*

European Union Invites Estonians to Develop Cyber Security in Asia and Africa

Since early 2018, we (along with partner institutions from the UK and the Netherlands) have been assigned by the European Union to support the cyber development of four countries in Africa and Asia – Mauritius, Sri Lanka, Ghana and Botswana. The Cyber Resilience for Development (Cyber4Dev) project will run until June 2021.

The goal of the mission is to increase the four countries' awareness of cyber security, help to develop cyber strategies and action plans, increase the capability of incident response teams and share experiences with vital services providers and government institutions. Activity is already under way in all four countries.

The countries vary in terms of level of cyber security: whereas CSIRT teams have been operational for some time in Sri Lanka and Mauritius, a CSIRT was only now set up in Botswana. Of the four countries, Mauritius is the most similar to Estonia. The island state with a population of 1.3 million has an ambition to be the leader in the cyber sector in the Indian Ocean region.

Train And Advise

In all four countries, IT and cyber security sector lacks personnel – there are few skilled workers and they gravitate to better paying jobs. The population's awareness of cyber threats is low, cooperation between state and private sector in improvement of vital

services could be better and support should be provided in order to bolster CSIRT capabilities.

In the course of the project, we evaluated the level of cyber security in each of the countries – a report was drawn up for each country with recommendations about what could be improved. In Sri Lanka and Mauritius, we also met the local CSIRTs and analysed what kinds of trainings they need in future. We have also already held trainings and workshops in these countries.

This year, we will continue training programmes in all of these countries. We will put the greatest focus on the structure of CSIRTs, the protection and regulation of critical information, risk management and crisis drills, cyber legislation and strategies, cyber hygiene and awareness. We will also introduce various solutions that help ensure cyber security in Estonia and which were developed in cooperation with Estonian companies. Sri Lanka and Mauritius have expressed interest in Estonia's experiences in building a digital society, including use of government-issued electronic identity. Experts and politicians from these two countries have also visited Estonia to learn more about our experiences.



The experts of participating countries have also visited Estonia to learn about our e-services.

CyberSIIL to Return This Year

In the biggest Defence Forces military exercise of all time in Estonia, Siil (Hedgehog), held in May 2018 was built around the scenario of a military conflict between a fictional Murinus and its vassal states. At the same time, on May 7th and 8th, a cyber security exercise called CyberSiil was held, simulating cyber attacks against a number of Estonian authorities and service providers simultaneously with military hostilities on Estonian soil.

The core principles of Estonian security policy mean that cyber security must be organized using the same structures in peacetime as well as wartime. Thus, activities of cyber security personnel in a wartime situation and cooperation with units that organize the military defence of Estonia must be practised regularly as well.

The sites hit by the attacks in the exercise were the Ida-Viru Central Hospital, Pärnu Hospital, Tax and Customs Board, the Port of Pärnu, and a fuel company Alexela. They all coped well in the situations they had to resolve.

Almost every cyber exercise trains responses to incidents. What made CyberSiil special was that it practiced exchanging information between the command of a military operation taking place on Estonian territory and activities taking place in cyberspace. For the staff in charge of military defence of Estonia, it is critically important to have real-time awareness of which vital services have been hit by cyber attacks and what the possible consequences might be.

In the long term, it is exceedingly important that the Cyber Security Council decided that cyber exercises must take place at the same time as the annual major Defence Forces exercise.

EXERCISING MAKES YOU STRONGER. OR PREPARED, AT LEAST.

Lauri Luht, Head of the Cyber Defence Exercises at the NATO CCDCOE

The key in tackling cyber crises is preparedness and preparedness comes by practice. The NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) has been conducting live-fire cyber exercises since its establishment in 2008. The largest international live-fire cyber exercise Locked Shields that annually takes place in Tallinn has earned high visibility. What is less known is the highly complex but low-profile technical exercise Crossed Swords (XS) that precedes the Locked Shields.

XS is one of the most challenging cyber exercises not because of its size, but because of the scale of different complex and interdisciplinary activities. This exercise takes participants into a very complicated and constantly changing environment with hostile actors and lots of simultaneous incidents that demand response and penetration to the adversary's networks.

The focus for the XS participants is to come together as a team of skilled experts, collaborate with different



agencies and get into the minds of potential adversary. They have to be able to deploy a full range cyber operations to solve the mission critical tasks in cooperation with special forces and intelligence. Among other challenges, the experts have to tackle kinetic threats by cyber means in the adversary networks.

The aim of XS exercise is to be realistic and provide an array of attack vectors that can occur in today's environment. Military is not the only tool to solve cyber problems as cyber crises could be military, civilian, or both, and most often of hybrid nature. Developing a comprehensive up-to-date exercise is a craft, as it takes thousands of work hours of planning and preparation by the international team of CCDCOE working jointly with experts from CERT.LV, TalTech and Estonian Cyber Command.



CROSSED SWORDS

CYBER SECURITY DEPENDS ON COOPERATION

Recognizing Red Flags Would Help Prevent Cyber Crime

Criminals in the cyber world are quite clever, exploiting both gaps in people's knowledge and weaknesses in systems. The greatest task for the police is to find resources to prevent severe (i.e., targeted and high-impact) cyber attacks and use prevention to raise people's awareness.

The head of the Cyber Crime Unit at the Central Criminal Police, Oskar Gross, says that although crime cannot be completely rooted out, it is possible to make things more secure even with limited opportunities.

What's currently the biggest worry for the police in relation to cyber crime?

Probably what might be called "cyber street crime" – far-reaching cyber crime with a fairly simple operating mechanism like phishing and various kinds of invoice fraud that easily claims victims among people who lack knowledge – these cases result in the most police reports.

We should definitely devote more attention to prevention of this category of cyber crime. For one thing, these incidents are quite hard to investigate using criminal investigation methods and rarely produce results. Yet these crimes are the ones that sow the most insecurity for society. If we could instil in people the a corresponding sense of danger, the number of such crimes would start going down simply because they have been rendered ineffective, and the police could direct more resources to investigating targeted, high-impact crimes.

What, if anything, makes it harder to identify cyber criminals compared to other types of crime?

Certain aspects make cyber crime different from other categories of crime. For example, the rules for the cyber environment are different than those for the physical world and the focus of investigations is probably a little different. Investigation of cyber crimes requires very good classical criminal police work skills and very good technical acumen. I don't see it possible to solve complex cyber crimes with only one skill set.

What might be the forecast for the coming years – will trends change in some manner?

As the field is changing all the time, there will certainly be some surprises. The same goes for cyber fraud. At some point the current phishing campaigns will not be effective enough, and some other scheme will be hatched. We'll keep our eyes open and try to respond on a running basis.

How to improve prevention, which is also much simpler and cheaper than criminal proceedings?

The big question about prevention for us is how to aim at the right target group. The media is certainly an important channel for spreading the word, but I personally feel that since attention spans tend to be short in today's society, we need a method that would get people to take a more in-depth, serious approach.

For instance, together with RIA, we tried out direct emailing of company executives at the end of the year, in which we warned them of widespread invoice fraud. Although this could have been done in a more subtle way, the feedback was on the whole very positive. In future we could consider a state notification system that would allow us to notify a specific target group of cyber attacks.

Does Estonia somehow stand out from the rest of the world in terms of cyber crime?

No, Estonia doesn't stand out very significantly when it comes to cyber crime. One thing that is a bit unusual is the fact that thanks to Estonia's ID card system, there are likely fewer attacks against bank clients than there are elsewhere.



Oskar Gross, Head of the Cyber Crimes Bureau at the Police and Border Guard Board

SUCCESSFUL INVESTIGATION OF CYBER CRIMES REQUIRES COUNTRIES TO SHARE THE SAME VIEW OF THE SERIOUSNESS OF THE SITUATION

Piret Paukštys, state prosecutor

Cyber crime is an increasingly widespread category of crime. It knows no national borders and it is possible for criminals to pocket extensive ill-gotten gains. A criminal might be sitting in a café in Italy on a laptop, and in a matter of minutes they can do something that affects servers in the US or other parts of the world. International cooperation and rapid exchange of information are key when it comes to conducting proceedings on such crimes.

Proceedings on international cyber crimes require countries to have a common understanding that this is a priority field that must be tackled. Having that common understanding of the problems is very important for making progress. In 2016, the European Judicial Cybercrime Network was established at Eurojust. Estonia is among the countries that makes a contribution to this prosecutorial network. The goal of the network is to speed up cooperation between countries, seek solutions to problems that come up in proceedings on cyber crimes, and to share experiences to how to deal with new future crime



categories.

In addition, the European Commission proposed last year that the police and law enforcement bodies should be able to get electronic evidence faster if they could send queries directly to service providers. Work to draft the corre-

sponding legislation continues actively this year as well. In addition, solutions to problems related to encryption are sought – for example, how to access encrypted data.

With each passing year, the prosecutor's office puts more emphasis on proceedings on cyber crime. It is expressed most in the number of people who have received procedural decisions – 27 in 2018 and 18 the year before that. The majority of criminal cases are local, so to speak – intrusions into strangers' internet user accounts and deletion or copying of data there.

In the 21st century, law enforcement bodies must take into account new technological challenges for apprehending criminals. Proving a cyber crime requires electronic evidence, but it should always be remembered that it only takes one keystroke to "lose" the evidence.

READINESS TO ATTRIBUTE CYBER OPERATIONS IS THE BASIS FOR STABILITY AND TRUST IN CYBERSPACE

Heli Tiirmaa-Klaar, Ambassador at Large for Cyber Security

In recent years, cyber security has become an important area for foreign and security policy. Increasing focus must be placed on responsible behaviour by countries in cyberspace, which presumes that state actors abide by international law, cyber standards and confidence and security-building measures. Some countries fail to do this, which makes it increasingly important to call on countries to follow rules in cyberspace.

To deter and prevent cyber operations organized or promoted by states, guidelines for attributing cyber operations were prepared and adopted by the Cabinet in 2018. The guidelines consist of political, technical and legal elements and define the remit of each pertinent Estonian authority in carrying out attribution of attacks. Estonia also supports the EU and NATO cyber defence policy frameworks and contributes to the development of stable cyberspace through developing the EU's cyber sanctions regime, collective attribution and application of other countermeasures.

On the background of ever increasing cyber challenges, greater digitalization and geopolitical conflicts, there is also increased foreign policy interest in Estonia's experiences in the sector. In the years ahead, Estonia will strengthen its relations with its primary allies in the field of cyber defence and cyber security initiatives in international organizations. We will also devote more attention to development cooperation in the cyber sphere.

Already now, Estonia is a great example for countries still building their digital society and cyber security, and we intend to continue sharing our experiences. We will also develop Estonia's expertise in regard to international law and in cooperation with Estonian universities and other academic institutions, we plan to establish a centre of excellence for international cyber law. The need for legal expertise in the cyber sphere continues to increase and Estonia has strengths to share with other countries in this area.



VIEW FROM ABROAD

THE CSIRTs NETWORK – AN IMPORTANT CONTRIBUTION TO CYBERSECURITY ACROSS EU



Otmar Lendl, Head of CERT.at

The NIS Directive, adopted in 2016, established the CSIRTs Network as a collaboration platform of all the national CSIRTs (+ CERT-EU) in the EU. As of today, the CSIRTs Network of the EU is an operational reality and contributes every day to the cybersecurity of the whole EU. It fell to our presidency trio (Estonia, Bulgaria and Austria) to nurture this collaboration forum of the IT security response teams through its formational years. Besides that, our Trio was the first one that created a common document laying out the ideas and priorities in the realm of Cyber Security for their terms as Presidencies in EU. Bolstered by this backing from the political level, the CERTs of Estonia, Bulgaria and Austria embraced the task of taking the lead in the CSIRTs Network.

The team of CERT-EE took their role very seriously. From my point of view, they did far more than the formal necessities. Estonia contributed by

offering the use of its Mattermost collaboration tool by the CSIRTs Network. That proved to be very helpful during the Wannacry and NotPetya incidents in 2017 where all the European national CSIRTs first gathered at this virtual “campfire” to coordinate the response and establish a common situational awareness picture across EU.

Another contribution was the time of its people. Experts from CERT-EE never limited their involvement to the official 6 months period of the chairmanship. Estonian experts helped to create necessary tools for the CSIRTs Network and create a suitable governance model for the Network to function well and contributed a lot to the “Cyber Europe 2018” exercise. I would like to thank here personally Klaid, Andres, Hannes and Sille from Estonia, who all have put in quite a bit of effort to make the EU CSIRTs Network a tool for effective information sharing between CSIRTs in EU and who I really enjoyed working with.



ESTONIA – A NATURAL PARTNER FOR THE NETHERLANDS

Michel Van Leeuwen, Head of Cyber Security Policy Department, Ministry of Security and Justice

The National Cyber Security Centre (NCSC) is the central information hub and centre of expertise for cyber security in the Netherlands. NCSC's mission is to contribute to the enhancement of the resilience of Dutch society in the digital domain, and thus to create a secure, open and stable information society. On an international level the NCSC is the Dutch point of contact in the field of ICT threats and cyber security incidents. The NCSC is also a key figure in the operational coordination during a major ICT crisis and the Computer Emergency Response Team (CERT) for the Dutch central government and the critical infrastructures.



The digital resilience in the Netherlands is still an issue. Not all organizations take basic measures to prevent cyber attacks. Even without the use of advanced methods the most precious information or data can be stolen. This is an important issue for the NCSC, taking in consideration the increasing complexity of the Dutch IT landscape. In our recently published National Cyber Security Agenda (NCSA), we have set out measures to meet such future trends.

This includes, among others, a nationwide network of cybersecurity partnerships within which information about cybersecurity can be shared between public and private parties more widely, and in a more efficient and effective manner.

The Netherlands is also in support of intensive cooperation on cyber security in Europe and hopes to cooperate with Estonia on further enhancing this level. Estonia is a natural partner for the Netherlands; both countries have a well-advanced digital, open and competitive economy. The NCSC has been closely collaborating with RIA/CERT-EE for years both in the field of operational cooperation but also in the area of policy development. This has not only been bilaterally but also in the framework of EU, which has helped to take the cooperation between EU Member States to a next level.

SECURE IDENTITY

Estonia Already Working to Ensure Post-Quantum Security

Professor of cryptography at the University of Tartu, Dominique Unruh, says that public-key infrastructure security systems such as the Estonian ID card can be broken with quantum computers. Although such a computer does not yet exist, secure solutions must be ready before that happens.

Professor Unruh, what is the current state of quantum computing? If there is no viable, working quantum computer in existence yet, then how can we prepare for quantum cryptography?

Today, only very limited quantum computers exist, and those are not useful for attacking cryptographic systems. While it is very hard to estimate when full-fledged quantum computers would be available, the research on them is making steady progress.

However, it would be a mistake to wait for quantum computers to appear before we start researching what is called “post-quantum cryptography”, the study of cryptographic systems that are secure against quantum computers.

To research, develop, and widely deploy new cryptography takes years, possibly longer than the development of a quantum computer. So if we do not take this problem seriously, we may be overtaken, with quantum computers being available before secure solutions are in place!

Preparing against quantum computers is, fortunately, possible without having quantum computers at hand. While we do not know exactly how a quantum computer will be built, we have mathematical models of their behaviour and principal limitations.



Donimique Unruh, Professor of Cryptography at Tartu University.

So we can mathematically analyse whether they could be used to crack a certain cryptosystem, without ever having laid hands on one. This way, we today try to design cryptosystems withstanding tomorrow's quantum computers.

How would you describe the risk of quantum computers for our everyday IT-systems? Is the public key infrastructure basically vulnerable to quantum computers by brute force search of private keys?

All widely used public key infrastructure is vulnerable to quantum computers (including, e.g., the Estonian ID card).

While we know of possible alternatives, those are not as well understood, and not as efficient, and therefore not used in practice. So yes, if someone has a full-fledged quantum computer, they can completely break most of today's public key infrastructure.

A precise analysis in what that means in terms of everyday risks would of course depend on how expensive quantum computers are, and whether they are available to criminal entities. This is hard to predict today.

You have received a grant of 1.7 million euros from European Research Council to study quantum cryptography. What is the aim of the research?

When analysing cryptographic systems (be it classical or quantum ones), we use mathematical proofs to analyse their security. However, mathematical proofs are very complex, and it is very easy for humans to make mistakes when writing or checking them.

Basically, if only humans check a complex mathematical security proof, we still will not know if the security proof is correct. "Formal verification" is a method to use a computer to check proofs - while a human may or may not have written the proof, we use the computer to check it.

Since computers do not have limited attention spans as humans do, they are perfectly able to look through many megabytes of proofs and will find the smallest mistake.

In my upcoming ERC project, we will design methods for formal verification specifically for quantum cryptography, and use them to verify the security of quantum cryptographic systems. This will support the development of quantum cryptography by putting its mathematical foundations onto a more solid underpinning.

Currently, there is one post-doctoral student and three doctoral students in my research team. With the ERC funding, this number is expected to double or triple. The daily research work consists mostly of performing mathematical proofs, and developing methods for formal verification, first on paper, and then as software. Besides that, we are also be involved in teaching in order to raise the next generation of high-level cryptographic experts.



Timeline of the New ID Card

Starting in December 2018, the Police and Border Guard Board (PPA) is rolling out a new ID card featuring a new chip, new security elements and design. But each such new feature takes time to develop: chips must be tested; certificates updated. Here's how the new ID card reached users:

January 2015 –

PPA and RIA launch preparations for a new procurement contract for the ID card.

November 2015 – the first public contract is announced.

February 2016 – deadline to bid on the contract. The manufacturer of the last card, Gemalto A.G, submits a tender, as does Oberthur Technologies S.A. and Safran Identity & Security Morpho.

April 2016 – PPA procurement commission selects the winner, but the result is contested.

August 2016 – the court declares the initial procurement result void and rules that PPA must review the results and the methodology used for evaluating the tenders.

November 2016 – PPA announces a new – the second – public procurement for the ID card.

January 2018 – in cooperation with SK ID Solutions AS, the new certification chain implementation plan is put into place.

April 2018 – a working group lays down the new card design and chip specification.

May 2018 – Development of an interim certificate for ESTEID18, which issues certificates for the ID card.

October 2018 – RIA replaces the test cards.

September 2018 – as a result of auditing of the trust service provider, the parameters of test cards are changed.

June 2018 – RIA issues test cards to companies and institutions for development of systems.

End of 2018 – PPA starts issuing new ID cards.

000001

000111

February 2017 – deadline to bid on the contract in the second procurement.

April 2017 – PPA signs the French company Oberthur Technologies to a contract for production of the ID cards, residence permit cards, digital IDs and diplomatic identity card templates, personalization of the cards and provision of certification service.

April 2017 – Gemalto contests the procurement after the signing of the contract.

November 2017 – Oberthur Technologies S.A. and Safran Identity & Security Morpho merge. The new company is called Idemia.

August 2017 – a group of researchers tells experts at RIA that they have found a security vulnerability in the chip used in the Estonian ID card.

September and October 2017 – PPA and RIA work to close the security risk.

November 2018 – the ID card's basic software supports the new ID card.

November 2018 – PPA issues 200 pilot cards for testing systems.

December 2018 – PPA service outlets start issuing the new ID cards.

December 2018 – critical services support the new ID card.

December 2018 – the contract with the producer of the past ID card, Gemalto, expires.

December 2018 – RIA releases the ID card software DigiDoc4 client, which supports the new ID card.

001010

110111

Cyber Security Strategy 2019–2022

In October 2018, the government approved the Cyber Security Strategy for 2019-2022. It is a vision of the directions Estonia wants to go in the field of cyber security over the next four years.

VISION

Estonia is the digital society with the highest level of cyber security. By coping with cyber threats effectively, Estonia is able to ensure smooth functioning of digital society, drawing on the joint capabilities of government institutions, purposeful and involved private sector and outstanding research competency. Estonia is an internationally valued trendsetter in the field of cyber security, which supports national security and contributes to the growth of global competitiveness of companies operating in the sector. Society as a whole perceives cyber security as a joint responsibility where everyone has their role to play.

To realize the vision, Estonia abides by the following fundamental principles in ensuring cyber security.

- We consider the protection and advancement of fundamental rights and freedoms just as important on the internet as in the physical environment.
- We see cyber security as enabling and amplifying Estonia's rapid digital development, which is the basis of Estonia's socio-economic development. Security must support innovation and innovation must support security.
- We are aware that ensuring the security of cryptographic solutions is uniquely important for Estonia as the entire ecosystem of the digital society is based on it.
- The basis of the functioning of digital society is transparency and public trust. To maintain it, we adhere to the principle of open communication from the government.

OBJECTIVE:

Estonia is a sustainable digital society with strong technological resilience and preparedness for coping with crises.

- State information systems and digital services must be developed taking into account both technological and organizational requirements, principles and standards.
- It is of key importance that government institutions and public sector follow baseline security requirements stemming from information security standards at least at the level mandated by law.
- Protection of digital resources that are important for Estonia is guaranteed (basic data on citizens, territory and legislative drafting. It is also important to review secure data communication between government institutions both in ordinary and crisis situations.
- To systematically analyse technical monitoring data, tools must be developed to create a close to real-time view of the landscape that measures the level of technical cyber security as an indicator of Estonia's development.
- The capabilities of different institutions' security will be determined and on their basis a national situation map is compiled and management of state networks' security, creating a cyber security centre (NCSC) on the basis of RIA cyber security service.
- Strong, cohesive and community culture based everyday cooperation has become the basis for Estonia's success to date in ensuring cyber security and preventing incidents with broad consequences and this practice will be continued and strengthened during the new strategy period as well.

OBJECTIVE:

Estonia possesses strong, innovative, research-based and globally competitive enterprise and research and development activity in the cyber security sector, covering all competencies that are important for Estonia.

- A cluster called the Estonian Information Security Association (EISA) has been established to coordinate effective cooperation between private sector, academia and the state.
- To ensure the more even development of cyber security research areas, focus areas for R&D in the field must next be defined. To leverage export potential, the state will ensure better inclusion of small (businesses) engaged in cyber defiance on business diplomacy mission and delegations.
- Startup Estonia will continue promoting the community in cooperation with the Ministry of Economic Affairs and Communications to make progress toward the establishment of an accelerator for companies in the cyber field and offer value for companies that are past the first phase of growth that are looking for global growth.



OBJECTIVE:
Estonia is a strong partner to be reckoned with on the international arena.

- It is important to continue the international cooperation in the field of cyber standards, trust-based measures and international law.
- It is in Estonia's interests to ensure that cyber attacks are successfully dealt with. This requires cross-border cooperation to be maintained and advanced, including ensuring that procedural information can be obtained rapidly and efficiency from other countries and general information exchange and cooperation reinforced.
- To maintain up to date cyber competence, rotation of diplomats and officials between establishments and sharing of knowledge and skills must be promoted.
- Systematic cyber cooperation with different key countries and the cyber agencies located there is important.
- The goal is to develop in Estonia a functioning procedure for attribution of cyber attacks at both the political and technical level and to take part actively in cooperation formats with likeminded countries in the field of deterrence and attribution. It is important to contribute to the discussion under way at NATO on collective defence in cyber space.
- Estonia must systematically support the development of cyber capabilities outside the EU and NATO and to do so, it must take part in the establishment of the EU cyber assistance network to develop a competitive and sustainable ability to render cyber assistance that would in turn reinforce that Estonia is one of the leading countries for cyber defiance.



OBJECTIVE: As a society, Estonia is cyber aware and a future supply of specialists in the field is guaranteed.

- Following the entry into force of the Cyber Security Act, Estonia takes a central role in growing cyber hygiene, prevention activities at the state level and raising awareness in society. Broader public awareness of cyber threats is ensured in cooperation between different agencies: both the ability to defend against threats and knowledge on how to act after a cyber attack.
- To raise the level of cyber hygiene at government departments, it will become obligatory for public servants in central and local government to pass tests on cyber security.
- Cyber security knowledge and skills among students and teachers will be measured systematically and a supply of cyber security trainings will be guaranteed for general education and vocational school teachers.
- Cyber security should be integrated into the information science syllabus and in-depth study of cyber defence should be taught in as many possible upper secondary schools as possible, thus laying the groundwork for a future supply of cyber specialists through the formal education system.
- Academic foreign policy competence, which is already healthy in Estonia, should be integrated with the cyber sphere. Besides this, possibilities for ensuring a future supply of legal experts should be ensured and Estonian competence in the field of cyber law must be reinforced through participation in international projects.

RIA'S KEY PRIVATE SECTOR PARTNERS



CybExer

cybexer.com

Address:

Toompuiestee 35, 10133
Tallinn, Estonia

Phone: +372 633 3266

E-mail:

info@cybexer.com

Cybexer Technologies was established to develop and commercialize specific cyber security products by combining the expertise and experience of two founding companies.

Field of Actions and Services

- Cyber Hygiene digital learning platform was launched together with the Estonian State Information Authority in spring 2017. It is meant for government institutions providing the risk profiles at the user, organization and state level.
- CybExer Technologies has developed a set of automation and visualization software solutions that enable extremely large volume exercises, making cyber exercises more accessible, scalable and at the same time allowing more sophisticated training experience.
- Vulnerability Visualization Tool. With the ability to connect multiple scanners to consolidate the data into a single view, CybExer will enable to focus and prioritize security investments to the most business-critical IT infrastructure and to connect real life risks with business metrics.



Cybernetica

cyber.ee

Address: Mäealuse 2/1,
12618 Tallinn, Estonia

Phone: +372 639 7991

E-mail: info@cyber.ee

Cybernetica is a research and development intensive ICT company that develops and sells mission-critical software systems and products, maritime surveillance and radio communications solutions. Cybernetica has been an active counterpart in developing critical e-Government systems, such as the Estonian X-Road, i-Voting, e-Customs and others. Today Cybernetica delivers its systems to across 35 countries in the world.

Field of Actions and Services

- Interoperability platform UXP (X-Road core technology)
- SplitKey secure authentication
- Sharemind secure analytics
- Maritime security
- Remote tower

RIA'S KEY PRIVATE SECTOR PARTNERS



Guardtime was founded in 2007 with a goal of eliminating the need for trusted authorities within Estonian Government networks. Since then Guardtime has become a global company with businesses across defense, telecom, life sciences, financial services, energy, government and others.

Guardtime

guardtime.com

Global Headquarters:

Avenue d'Ouchy 4, 1006
Lausanne, Switzerland

Tallinn office:

A. H.
Tammsaare tee 60,
11316 Tallinn, Estonia

United States:

5151
California Ave, Suite 210
Irvine, CA 92617, USA

Field of Actions and Services

- Guardtime's KSI®: a blockchain platform designed for enterprise solutions with security, scale and performance built in.
- Guardtime Research is devoted to building breakthrough technologies and applications in cryptography and computer sciences. With over 40 patents granted since 2007 and more pending, we have a proven track record in transforming foundational research into practical solution.
- Guardtime's international R&D division — with a hub in Estonia — features over 40 cryptographers, researchers, engineers, scientists and analysts, with qualifications in both foundational and applied research.



BHC Laboratory

bhclab.com

Address:

Toompuiestee 35, 10133
Tallinn, Estonia

Phone: +372 600 2444

E-mail: info@bhclab.com

BHC Laboratory is a cyber security capabilities development company that specialises in complex technical cyber security exercises, strategic cyber security exercises, security assessments and human behaviour-related risk management in cyber security.

Field of Actions and Services

- Exercises and Cyber Ranges: cyber exercise environment creation, management and facilitation; cyber ranges; strategic-level cyber exercises.
- Consultancy and Trainings: penetration testing; comprehensive security assessments; IT risk management; CSIRT trainings; specialized trainings on cyber operations and customized training packages.

RIA'S KEY PRIVATE SECTOR PARTNERS



Clarified Security

clarifiedsecurity.com

Address: Lõõtsa 12,
11415 Tallinn, Estonia

Phone: +372 603 6644

E-mail:
info@clarifiedsecurity.
com

Clarified Security is an Estonian information security company focused in delivering practical security services. Our home market is the "IT wonderland" of Estonia where Web is the glue and delivery mechanism of most of these wonders. Our strongest focus has been on manual WebApp pentesting while being generally happy to break anything that offers us technical challenges. They also teach practical security through the perspective of attacks in their hands-on security courses and do red teaming for large scale cyber exercises.

Field of Actions and Services

- manual penetration testing services, mainly web application pentesting based on OWASP AVSV
- practical hands on security courses through the perspective of attacks
- red teaming on production and for (large scale) cyber exercises



SpectX

spectx.com

Address: Mäealuse 2/3,
12618 Tallinn, Estonia

Phone: +372 452 4466

E-mail: info@spectx.com

SpectX is a software company developing the tool for quickly parsing and analysing difficult unstructured data. It is founded by security engineers with decades of hands-on SOC experience in Skype/Microsoft and Scandinavian banks.

SpectX is specifically designed for security analysts. The tool allows them to quickly dig into any volumes of raw data (logs) stored on-prem or in the cloud and find the root causes of security incidents. SpectX is unique because the data can stay where it has been stored in unlimited amounts.

Analysts need to spend no time and effort on importing and enriching data into an analysis platform. Large enterprises use SpectX also as a universal preparation tool for quickly creating a clean and structured view on top of any unstructured data, making it available for analysts working on different use cases (business, operations, security).

Photos by:

Pages 4, 41, 49: Police and Border Guard Board

Pages 9, 13, 55: Renee Altrov

Page 11: Raul Mee

Page 15: North Estonia Medical Center

Page 17: Taaniel Malleus

Page 21: Emergency Response Center

Pages 23, 27, 29, 37: RIA

Page 31: Rasmus Jurkatam

Page 35: Clarified Security

Page 39: NATO CCDCOE

Page 47: Andres Tennus, Tartu University

Page 54: Reimo Roonet

