Republic of Estonia
Information System Authority

# 2015 Annual Report of the Estonian Information System Authority's Cyber Security Branch

# Contents


Foreword 2

2015. Statistics 3

Introduction 4

What threatens us? 4

Vital Services 6

Security Incident Management 7

Exercises 11

Cyber Security Legal Framework 12

Studies 13

Changes to ID-card Usage 15

National Information Systems Security and Financing 17

Supervision 18

International Cooperation 19

# Foreword

It is a pleasure to introduce the 2015 annual report of the Estonian Information System Authority's (RIA) Cyber Security Branch by concluding that, for Estonia, another year has passed without incidents that had major consequences. Estonia's cyber security is born out of the daily cooperation between companies and the state, and this cooperation has produced good results.
The field of cyber security, however, is developing very fast and the risk environment is constantly changing. Every day we hear news about emerging vulnerabilities and threats. Yet we don't necessarily need to buy new and expensive systems to reduce these risks; it's enough to follow the basic principles of information security. The last year showed that vital services can be at risk of disruption from something as simple as a ransomware attack. Carelessness and apathy in the performance of elementary security procedures (i.e. creating back-ups and adequately administering user rights) can bring about the total destruction of all of a company or organisation's data. Unfortunately, this still happened last year.

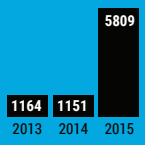
The last year also demonstrated once again how dangerous it can be to use cyber tools as a weapon. The attack that caused extensive interruptions in Ukrainian electrical networks on Christmas Eve reminded the world, that cyber attacks are by no means purely digital and can cause very tangible effects. Damaging the modern way of life with cyber tools can be quite simple and effective, and unfortunately ever more feasible for terrorists, for example.
For this reason, cyber security holds an important spot on the list of security challenges faced by European states and the first steps toward closer cooperation have been taken. The upcoming implementation of the European Union Network and Information Security Directive will bring about closer cooperation and information sharing not only between states, but also between the public and private sector. The latter is very important, because the cyber domain is completely dependent on the private sector's infrastructure and services. In Estonia, there has been considerable investment in cooperation: we are one of the few countries in the world who helps their critical infrastructure companies assess and test their information systems, organises exercises, and has been successful in the creation and support of communities of cyber security providers. Increasingly, raising awareness about cyber threats as well as developing the skills and knowledge to use technology safely have become a central aspect of ensuring cyber security. After all, the technology itself doesn't create risks – they occur from the malicious, rather than intended, use of technology. The more aware we are about the possibilities of technology, the more we can predict threats and prevent detrimental consequences.

I wish you a secure rest of the year!

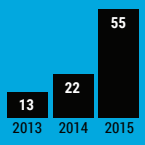
Toomas Vaks
*Director of Cyber Security, Head of Cyber Security Branch*

# 2015. Statistics

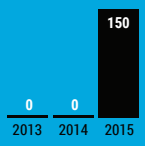
## Estonian cyberspace:



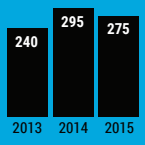

**5809**
Cases handled




**55**
DDoS attacks

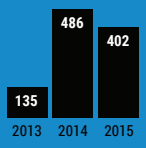



**150**
Encrypting ransomware cases




**275**
Defacements

## Governmental agencies:




**402**
Incidents reported by governmental agencies

**Most common causes:**

- attack
- software
- external service provider
- administrator error


**27%**
Reported incidents were high criticality
(20% in 2014)

### 420 000 ID-cards need new certificate

required for increasing the security and enable continuity of ID-card usage

### SHA-1 probability of breakage is too high

Google, Microsoft, Mozilla consider vulnerable

### CyberHEDGEHOG 2015 - largest cyber exercise in Estonian history

Exercises - CONEX, Locked Shields, Cyber Coalition, Cyber Europe

### Cyber security legal framework needs improvement

More than ten laws define the current arangement of Estonia's cyber security

# Introduction

Among highly developed countries, Estonia has garnered significant positive attention for the large amount of well-functioning digital services that citizens have become accustomed to and whose functioning we consider to be a natural part of everyday life. At the same time, this means that the state is largely dependent on the functioning of these digital services and that cyber security is a very important part of our overall security.

Estonia's cyber security is founded on the principle that every organisation or vital service provider is responsible for the security of its information systems and for ensuring business continuity. Vital service providers and national agencies are required to notify the Estonian Information Systems Authority (henceforth RIA) about incidents that affect service provision and to implement appropriate information security measures according to RIA's recommendations.

RIA's objectives in the field of cyber security are to gather information and analyse incidents taking place in Estonia's cyberspace, improve readiness for cyber attack response, as well as to develop standards for information security implementation and oversee their implementation, including by focusing primarily on ensuring the cyber security of vital service providers. In the following pages, we provide summaries of the last year in Estonian cyber security and explain many of the challenges that lie ahead.

# What threatens us?

Military action without a declaration of war, or hybrid warfare, is a defining characteristic of contemporary security affairs and one that Estonia has to constantly consider because of our geopolitical location. Cyberspace is the ideal battlefield for achieving hybrid warfare objectives because, in addition to being able to hide one's identity with ease, it can also be used to sow instability or achieve traditional military objectives. Compared to other highly developed states, it is possible to achieve those objectives much faster against Estonia by using cyber attacks because the dependence of the state and the people on digital services is already very high and continues to increase.

**We are accustomed to the fact that Estonia's networks and information systems are regularly mapped and measured to obtain information that would be useful for planning any kind of large-scale activities against Estonia.**

However, it is impossible to agree with claims that have appeared in the news media that, in today's society, access to a keyboard is equivalent to owning a weapon. The dangers stem not from the inherent nature of the technology but rather from the voluntary actions of concrete individuals.

For Estonia, the most important cyber threats include:

1. Cybercrime in all its forms. Global organised cybercrime threatens everyone and can easily become a threat to

national security as well. A good example of that are cases where ransomware renders inoperable the information systems of vital service providers.

2. Cyber espionage, data breaches and lack of applying principles of information security, which can result in the reduction of trust towards information systems and digital services. In many countries, extensive data leaks and interruptions in the functioning of information systems have brought about substantial loss of trust and cast doubt on the ability of states and companies to protect the information of its citizens or clients.
3. The use of cyber tools in armed conflict. The incident in Ukraine in 2015 is a painful reminder about the vulnerability of modern societies to attacks in which cyber tools are used to disrupt industrial control systems by hindering their work or rendering them inoperable.
4. The fact that an important role in the perpetuation of cyber threats is played by the lack of security knowledge, skills, and awareness among users of information systems. Human carelessness or ignorance is the primary source of most serious incidents.

Estonia cannot ignore the fact that we are located next to Russia, which uses aggressive rhetoric, is constantly developing its cyber attack capabilities, and for whom activities directed against other states in cyberspace are merely an instrument to increase its influence and accomplish its objectives. We are already accustomed to the fact that Estonia's networks and information systems are regularly mapped and measured to obtain information that would be useful for planning any kind of large-scale activities against Estonia. In addition to Russia, our cyber threat analyses cannot ignore the need to take into account terrorists and hostile cyber activists. The fact that Daesh includes the Estonian flag in its list of enemies should make us consider the possibility that terrorists who have up until now preferred physical attacks can also initiate cyber attacks against Estonia.

In cyberspace, it is progressively challenging to differentiate between criminals that are motivated by personal gain and the security services of a neighbouring state that are interested in employing hybrid warfare against Estonia in pursuit of national objectives. The cooperation between cybercriminals and security services that are hostile toward Estonia takes place on a daily basis and is mutually beneficial for both parties. This makes Estonia's situation more challenging because there are almost no clear answers. We can no longer be sure about whether an attack against an Estonian vital service provider that appears to be for monetary gain hasn't actually been commissioned from cybercriminals according to a different criterion.

The year 2015 has demonstrated that, in the grand scheme, Estonia's cyber security is also threatened by the inability to quickly draw conclusions about known threats and implement

**In cyberspace, it is progressively challenging to differentiate between criminals that are motivated by personal gain and the security services of a neighbouring state that are interested in employing hybrid warfare against Estonia in pursuit of national objectives.**

necessary changes in information systems. Last year in Estonian cyber security was characterised by the exploitation of vulnerabilities from 2014 and 2013, because open-source security warnings and RIA's own notification efforts were left unnoticed by the owners of information systems. This also increased the total number of incidents handled. The primary lesson of 2015 is that avoiding threats depends upon being able to deliver security alerts to all of Estonia's IT specialists in a way that ensures they take prompt action.

# Vital Services

**Continuity of vital services can be affected, or even crippled, by simple ransomware campaigns that weren't even intended to disrupt those services.**

98% of vital service providers have acknowledged that their business operations are directly dependent on the functioning of the IT-systems. This needs to be taken seriously by the state. The national cyber security strategy states that one of RIA's main tasks is to increase awareness among vital service providers about cyber risks and increase their capacity to cope with them.

2015 proved that the continuity of vital services can be affected, or even crippled, by simple ransomware campaigns that weren't even intended to disrupt those services.

At the end of the year, cyber attacks were carried out against electrical systems in Ukraine. Estonia needs to draw serious conclusions from this fact. It's another example of how cyber tools can be used to create direct physical consequences and seriously affect the daily life of individuals. The main lesson of the Ukraine case is that the proper application of information security measures can actually significantly reduce the consequences of such attacks or even prevent them entirely. While vital service providers in Estonia are much better prepared than the Ukrainian colleagues, Estonia still cannot rest on its laurels in any way. We have considered the lessons of the Ukraine case and are planning several activities to improve the cyber security of vital service providers.

According to law, there are currently 46 vital services in Estonia that are critical to ensure the functioning of society, the provision of healthcare as well as security, and the management of economic and social wellbeing. These services are provided by more than 140 public and private sector organisations who are all required to inform RIA of all security incidents that have taken place.

In 2015 we organised various types of trainings for more than 120 specialists from vital service providers. We will continue these educational activities in 2016; we have planned 14 trainings. Last year, many vital service providers also took part in a national cyber exercise organised by RIA, which will be described below.

Estonia is the only country in Europe that tests the security of vital service providers' IT systems itself. In 2015, RIA evaluated the IT systems of three vital service providers. We attempted to

identify if and how a potential attacker could gain access to a provider's critical information systems. We will continue this kind of testing in 2016.

Interdependence among service providers constitutes a significant challenge to ensuring the business continuity of vital services. Last year we managed several significant security incidents where one vital service provider IT systems disruption triggered incidents to other vital service providers. For this reason, we are commissioning a study in 2016 to clarify the factors that affect vital service provision in order to improve the state's understanding of both important IT-related cross-dependencies between vital service providers in Estonia as well as of cross-border dependencies.

Intensive information sharing among experts is crucial for ensuring that the provisions of any vital services in Estonia aren't disrupted by cyber threats. Regular awareness-raising activities and meetings of specific commissions that bring together cyber security experts by sector facilitate information sharing. In 2015, many vital service providers took part in the KüberSIIL (CyberHEDGEHOG) exercise. This year we will also organise numerous trainings for experts to increase their readiness level. It is always useful for information security specialists or managers from organisations that provide vital services to get in contact with RIA's Cyber Security Branch even if the reason is merely to obtain information, mention a security risk they have identified, or to provide suggestions to improve our mutual cooperation.

# Security Incident Management

RIA's Cyber Security Branch also fulfils the tasks of a national computer emergency response team (CERT) and is the international point of contact for global CERT/CSIRT networks. CERT/CSIRT organisations exist around the world and cooperate closely, including by sharing information about cyber incidents and notifying partners and the public about cyber threats.

The Incident Response Department of the Cyber Security Branch (CERT-EE) identifies, analyses, and resolves security incidents that take place in Estonian computer networks, raises awareness about threats, and conducts incident monitoring. In January 2016, CERT-EE celebrated its 10th birthday.

Around-the-clock manned monitoring of Estonian cyberspace has taken place since the summer of 2015. We also adopted new and improved monitoring technologies. Activities in cyberspace are continuous and in no way bound by Estonia's time zone. As a result of the around-the-clock monitoring, we have prevented, discovered, and reacted to significantly more security incidents than in past years.

**As a result of the around-the-clock monitoring, we have prevented, discovered, and reacted to significantly more security incidents than in past years.**

A good example of the successfulness of the around-the-clock monitoring is the identification and expedient takedown of a fake website that was designed to look like that of the Estonian Tax and Customs Board. The fake website was set up to steal users' credit card information.

Even though the attackers had planned to gather unsuspecting individuals' credit card information over the weekend, when the relevant officials were not on duty, CERT-EE discovered the well-crafted fake website on Friday night and it was taken offline one-and-a-half hours after it went live. The Estonian Tax and Customs Board notified RIA about a possible phishing attack on Monday morning, at the start of the new workweek. Although the criminals had planned to conduct the attack after regular working hours and managed to coax unsuspecting computer users to enter credit card information on their website during a limited timeframe, the attack was successfully stopped because of around-the-clock monitoring before anyone was known to suffer losses from it.

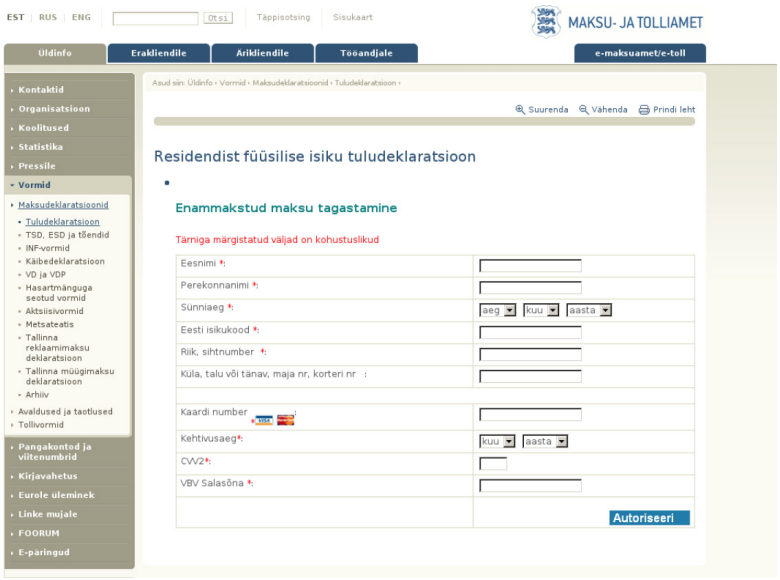



*Figure 1 Example of faked Estonian Tax and Customs Board website*

Malware attacks that were conducted for the purpose of extortion, otherwise known as ransomware incidents, were more difficult and consequential than the above in 2015. Ransomware encrypts the data on a user's computer and, if possible, on external drives connected to that computer, thereby making them unreadable to the user. A ransom, payable in virtual currency called bitcoins, is then demanded for the necessary cryptographic key to unlock the data. Usually if the ransom is not paid then the data will remain unusable. In 2015, we were notified of 150 such cases.

An especially large amount of ransomware cases were registered in the last two months of 2015; over four times more than in the previous ten months combined. Typically, the data on a regular user's hard drive was encrypted. However, there were cases where data was encrypted on shared server drives. The increasing cleverness of cybercriminals means that it is impossible to completely prevent ransomware infections.


*Figure 2 Screenshot of computer infected by ransomware*

RIA's Cyber Security Branch specialists always analyse malware variants found on victims' systems as well as identify and shut down their distribution channels. An analysis of ransomware incidents in 2015 revealed a disproportional amount of victims among governmental agencies and vital service providers, which in certain cases points to targeted attacks against them.

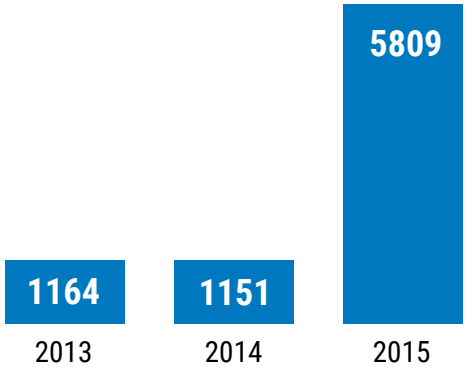



*Figure 3 Information security incidents registered by CERT-EE*

The main conclusion that can be drawn from 2015 is that, even with the best information security practices, it is difficult to completely prevent ransomware infections. Making back-up copies of data in information systems can certainly help to reduce the damage done by ransomware. Losses can also be minimised by well-defined and controlled distribution of user rights in information systems. And, of course, general security awareness and safe behaviour can help against all cyber attacks as well.

**Damage caused by ransomware is reduced when regular data back-ups are available.**

Last year's incidents once again confirmed the results of previous studies conducted in Estonia: a relatively large number of Estonians have theoretical knowledge about how to avoid cyber threats, but often they are not applied in practice. Usually, unsafe behaviour is caused by human laziness or curiosity.

Activities to improve security (regularly changing passwords, backing up data, software updates) do not seem important and e-mail attachments written in faulty Estonian and coming from an unknown address are mostly opened due to sheer curiosity.

In addition to malware attacks, there were also several distributed denial of service (DDoS) attacks last year for the purpose of extortion. Such incidents follow a typical pattern: the organisation first becomes a victim of a short DDoS attack, then the attackers send a message to the contact e-mail telling them that if the ransom is not paid in time, a substantially larger and longer attack will follow. It can be assumed that attackers have usually conducted an initial analysis to calculate the organisation's revenue or its presumptive losses in case the victim is not able to provide its services to clients. There is no public information about any Estonian company that has paid a ransom to avoid a DDoS attack.

Even though in 2015 we dealt extensively with cyber attacks that were conducted for monetary gain, we cannot forget that foreign governments continue to be interested in Estonian computer networks. We regularly identify DDoS attacks and network mapping in Estonian cyberspace that have a high probability of being perpetrated by other states. For RIA's Cyber Security Branch, the identification and management of DDoS attacks is a common task. Last year we registered an average of one DDoS attack per week. We can assume that in many cases this has been a method that is used test the ability of organisations to cope with attacks. It is also evident that DDoS attacks are becoming longer in duration. Most DDoS attacks are conducted by using home or office computers that have been infected with malware and assembled into so-called botnets, with most users being unaware that their computers are being used to attack a third party.

**Regardless of whether the victim is a service provider or an end user, the police must be notified about the losses suffered from cybercrime.**

Regardless of whether the victim is a service provider or an end user, the police must be notified about the losses suffered from cybercrime. RIA's Cyber Security Branch and the Police and Border Guard Board cooperate closely, but only the victim of a cybercrime can make an official report to the police.

To notify the police about a cybercrime, please e-mail:
cybercrime@politsei.ee.

# Exercises

In 2015 we organised our own exercises and also participated in several national and international cyber exercises. The most important of these were the national cyber exercise CyberHEDGEHOG 2015 that we organised and which took place in September 2015 as well as the cyber exercise in April 2015 in the framework of the national crisis management exercise CONEX 2015. Additionally, we coordinated Estonia's participation in the NATO exercise Cyber Coalition 2015 as well as the European Union exercise Cyber Europe 2015.

For CONEX 2015, RIA and the Ministry of Interior cooperated to organise a cyber security exercise for the leadership of the Ministry of Economic Affairs and other organisations in its area of governance. The table-top exercise was led by the minister of economics and infrastructure and focused on the strategic dimensions of responding to a large-scale cyber incident. The exercise scenario included data breaches and cyber attacks involving the ID-card infrastructure, the data exchange network used by public and private companies, the population registry, the e-residency program, and vital services (energy and shipping). The government's action plan was updated with the lessons learned from the exercise.

In the fall of 2015, we organised the national cyber security exercise CyberHEDGEHOG 2015. The main objective of the exercise was to practice implementing the incident response plan for a large-scale cyber event. This included overviewing the rights and duties of organisations aiding in emergencies, cooperating with outside partners, testing readiness, facilitating information sharing and other internal RIA procedures. Command staff units at the operational and strategic levels practiced resolving crisis situations. Although this wasn't a technical exercise, it did involve practical, real-time crisis management and cooperation between participating agencies.

**The organizations that took part in the exercise demonstrated good cooperation in resolving the crisis.**

CyberHEDGEHOG 2015 was Estonia's largest cyber security exercise to date. 21 organisations (incl. security and law enforcement agencies, public and private vital service providers) and over one hundred people took part in the exercise.

The CyberHEDGEHOG 2015 and CONEX both demonstrated that:

1. The organisations that took part in the exercise demonstrated good cooperation in resolving the crisis, and the existing processes for sharing information and developing joint situational awareness worked. The participating organisations had a good understanding and overview of their roles and could successfully complete their tasks.
2. A separate law to increase legal clarity and define responsibilities at the national level is still needed in order to ensure more effective cyber security organisation.

3. The roles and responsibilities of organisations involved in ensuring the functioning of the ID-card system need to be more comprehensively and clearly defined in legal statutes.
4. The effects of incidents involving the national trust service and internet infrastructure need to be more clearly understood and a procedure needs to be developed to resolve them.

# Cyber Security Legal Framework

**The legal framework for ensuring cyber security in Estonia needs improvement.**

The legal framework for ensuring cyber security in Estonia needs to be improved.

In 2015, the lessons learned from the CyberHEDGEHOG 2015 exercise, the amendment of the Emergency Act, and the adoption of the European Union Network and Information Security Directive (NIS) confirmed the need for a clear cyber security law that takes into account modern conditions.

Additionally, as it stands, the Public Information Act does not sufficiently consider technological trends and therefore prevents the adoption of new technologies and hinders Estonia's digital development.

The Ministry of the Interior has developed a new draft of the Emergency Act, which will clarify the field of vital services. This change will have a significant influence on the provision and organisation of cyber security in Estonia.

The new Emergency Act will no longer apply to those vital services whose functioning may be necessary and expected by people in their daily lives, but whose operation in emergency conditions is only provided if possible because they are not directed towards satisfying the primary needs of the population during times of crisis (for example, airports). Additionally, the new Emergency Act does not regulate services that are crucial for the functioning of the state (for example, the work of the Cabinet of Ministers). For this reason, there will be a series of services that the new Emergency Act will not regulate but whose possible malfunction could significantly affect national security (for example, railroads and airports). According to different risk analyses, these services are largely dependent on the functioning of IT systems; therefore information security measures need to be implemented to ensure their operation. In the future, the obligation to do so will stem from the sector-specific laws (for example, the Railways Act). More than ten laws define the current arrangement of Estonia's cyber security. The changes mean that at least four more laws will be added to that list and Estonia's legal framework for ensuring cyber security will become even more complicated.

Continued upgrade of technology solutions is inevitable to enable Estonian digital growth. For this reason, the state needs to adopt,

among other things, cloud-based technologies and solutions that are covered by the conception signed by the Cabinet of Ministers in September 2015.

Estonia is planning to create a national cloud to support the continuity of our information society. It will be a hybrid cloud that will include a separate cloud service to governmental agencies, shared clouds managed by the private sector, and data embassies based in foreign countries.

In addition to developing cloud solutions, attention needs to be directed towards the legal framework. The current legal framework governing databases and data processing dates back to a time in which cloud-based services were not widespread. According to the Public Information Act, the national and local governments are required to implement one particular information security system for their databases, which assumes the possibility of auditing and oversight. These requirements will be impossible to fulfil upon the adoption of cloud services that are based outside of Estonia. For this reason, it is necessary to develop regulations that enable and support cloud-based data processing and the adoption of different cloud-based solutions.

At the end of 2015, the European Council approved the Network and Information Security Directive (NIS). This is a new European Union legal act that will, for the first time, define the provision of vital services in member states and the operational cooperation of member state CERTs during incident response. The directive will improve the prevention, discovery, and response to security incidents and require member states to notify each other about cyber incidents or attacks with major consequences. The directive will come into effect in the first half of 2016. When it does, Estonia will have to incorporate it into its own legal system.

The current legal framework has two possibilities for achieving that. First, it is possible to review and amend a whole series of sector-specific laws, including the Emergency Act mentioned above. This solution will also require the development of a separate legal act because some of the requirements of the directive will probably not be possible to incorporate solely by amending the sector-specific laws. It would be a laborious process that would not improve legal clarity.

The preferred solution from the vantage point of legal clarity would be to develop one comprehensive and compact law to regulate cyber security, which would not only help to incorporate the requirements of the Network and Information Security Directive but would improve Estonia's cyber security as well.

**From the vantage point of legal clarity the preferred solution would be to develop one comprehensive and compact law to regulate cyber security.**

# Studies

Close cooperation with the research institutions is an inseparable part of ensuring cyber security. With this in mind, we conduct studies every year about technological developments and

their possible effects on cyber security in Estonia. In 2015 we integrated the insights gained from these studies directly into the improvement of e-government security.

The functioning of Estonia's e-government is largely dependent on its services credibility, which precondition is the use of strong cryptography. In 2015, for the third time, we commissioned a study to determine whether some cryptographic algorithms and their applications were in danger of breaking. For Estonia, it is important to stop using breakable cryptographic algorithms before it is used against the state or its citizens.

The massive information security incidents of 2014 and 2015 (HeartBleed, Shellshock) demonstrated that the primary problem is not the mathematical strength of cryptographic algorithms but rather the nuances of their practical implementation. Changes are being made starting in 2015 to raise the security level of ID-cards based on the results of the study. When beginning to design technological solutions, a general recommendation would be to take into account the occasional need to update cryptographic algorithms. For this reason, the use of algorithms and security solutions should be as flexible and quickly reprogrammable as possible.

In addition to algorithms, the 2015 study also addressed the security of contact-free chip cards and mobile platforms. With contact-free chip cards, data transfer takes place over potentially insecure radio channels (NFC). With mobile devices, the protection of users' private keys is problematic. If keys aren't stored on chips, then there is no good alternative for storing keys on mobile devices at the moment.

One option would be a so-called Trusted Execution Environment (TEE), but this is only beginning to be integrated into various manufacturers devices and therefore it is too early to assess its security. The results of the study have provided input for planning the use of contact-free ID-cards in Estonia and they should be taken into account during the development of future technologies by Estonian state institutions and companies.

**When it comes to data that citizens have entrusted to the state, it is extremely important to know where that data resides, who has access to it, and how well it is protected from different attacks.**

In recent years, there has been an increase in the amount of criticism regarding IT solutions used by the state. Opponents are unhappy that it is considered insecure to host national databases in the cloud when many private sector companies are using cloud storage for their clients' data. However, even though cloud services are considered to be cheaper, faster, and more reliable, using them is still not in line with Estonia's current laws and storing national databases on the territory of other states can still be considered to be fundamentally insecure.

When it comes to data that citizens have entrusted to the state, it is extremely important to know where that data resides, who has access to it, and how well it is protected from different attacks.

When using commercial cloud services, it is impossible to know which country and data centre is currently storing our data and

which server administrator has access to that data at any specific moment. At the same time, the increasingly widespread use of cloud services is a natural part of technological development and in 2015 we initiated a comprehensive legal and technical analysis to specify what opportunities there are for Estonian government institutions to use cloud services after all.

Based on the results, we will put together a suitable instruction manual for Estonian government institutions that answers the following questions:

- Which data can be stored and processed in the cloud, and under what conditions; which cloud service products would be safe to use?
- What requirements have to be considered and which security measures must be implemented when commissioning cloud services?

In 2015 we became convinced about the necessity of thoroughly analysing both the legal questions associated with using cloud technologies and the risks connected to the integrity and confidentiality of data being processed in the cloud as well as the need to develop sufficient security measures to minimise those risks. A supplementary legal analysis about the government cloud that will analyse the objectives described above will be completed in 2016.

# Changes to ID-card Usage

**Stronger cryptography will be utilized for ID-cards.**

Estonia's cyber security in 2015 was significantly affected by the need to make changes to the ID-cards that have been distributed in Estonia. Halfway through 2015 it became apparent that a large proportion of ID-cards being used for personal identification in Estonia have the type of certificates that large software providers have already stopped, or plan to stop, accepting. Therefore, there was a danger that after a certain date it would no longer be possible to use the cards for identification through electronic channels. There was, however, no direct security threat from noncompliance with the standards and the privacy or confidentiality of the users would not suffer.

Around 420,000 active cards (Identification documents, residence permits, digi-IDs, incl. e-resident Digi-IDs) have certificates used for digital identification that do not comply with standards. Therefore, the sustainability of using those cards for digital identification and signatures in electronic environments cannot be guaranteed.

Until 2015 the noncompliance with standards had not become apparent because the relevant control mechanisms are usually relatively lenient when it comes to open-source software. However, as a result of the massive security problems with open-source software that came to light in 2014, major software

providers began to tighten the control mechanisms. Google, whose Chrome web browser is estimated to be used by more than half of Estonia's Internet users, was the first to announce relevant changes in the summer of 2015.

RIA and the Police and Border Guard Board began preparations to replace ID-card certificates in 2015 in order to ensure continued compliance with recognised international standards.

Until now, custom dictated that making changes to the ID-card certificates required a visit to the local office of the Police and Border Guard Board. However, this was clearly impractical in a situation where a large amount of certificates had to be replaced at the same time and many card owners were e-residents who were physically located abroad. For this reason, in 2015 the decision was made to restore the option to change the certificates located on chip cards by remote update. Starting in March 2016, affected card owners can perform the update independently by using the ID-card management software.

In addition to the remote updates, RIA also began to cooperate with the Police and Border Guard Board to increase the security of ID-cards in 2015 in order to ensure the cards' enduring sustainability. A majority of the ID-cards currently in circulation use certificates for authentication and digital signatures that employ the SHA-1 hashing algorithm. There are more than a million such cards that were issued before 3 January 2016.

As computing power continues to grow, earlier cryptographic algorithms (like SHA-1) become vulnerable to well-financed attackers. For the time being this is a theoretical vulnerability but in the long term, the public key infrastructure that enables secure identification of individuals with ID-cards, Mobile-IDs or Digi-IDs could be threatened. Aging cryptographic algorithms have to be replaced by stronger ones in order to prevent this danger. For the average user, this only requires that they replace the certificates on the ID-cards with ones that are based on stronger cryptography (SHA-2).

Software producers have taken a clear course to stop supporting the SHA-1 hashing algorithm because the probability of it being broken has become too great. The fact that older cryptographic algorithms slowly become more insecure as computing power grows and crypto analytic knowledge advances is a completely normal process in the field of cryptography.

Since 90% of Estonian Internet users use either Microsoft, Google Chrome, or Mozilla Firefox browsers, we analysed the baseline requirements of those software providers in 2015 and began to increase the security of Estonian ID-cards in combination with the certificate updates mentioned above. Software producers are relatively unclear in their statements on these topics, so it was decided that security should be increased in order to prevent future problems for users.

# National Information Systems Security and Financing

**We distribute best practices related to cyber security.**

In Estonia, national agencies and local governments are required to use a standardised system (ISKE) to ensure information security. The reason for implementing ISKE is to ensure sufficient security for data being processed in information systems. The system has been created primarily to ensure the security of information assets that are used by information systems connected to the databases of national and local government institutions. Regular meetings of commissions that bring together sector-specific experts take place in order to organise and develop the security of national information systems. We use these meetings to coordinate the activities of security managers and to distribute best practices related to cyber security.

The first version of the ISKE portal was completed in 2015 in order to facilitate the implementation of ISKE in national agencies and local governments. Until then, ISKE was only accessible from the RIA homepage and was made up of numerous document files totalling more than 4,000 pages. Now ISKE is accessible from one convenient and user-friendly portal. Additionally, four information security management courses for ISKE adopters and seven information security awareness-raising courses for regular governmental users will be organised in 2016.

The substance of Estonia's national cyber security strategy is very ambitious and the objectives it contains have required large investments from the entire country, including RIA. For this reason, many of the activities that have been carried out have utilised support from European Union structural funds. In 2015, this support constituted nearly 40% of the RIA Cyber Security Branch's budget for cyber security development.

While European Union structural funds have been a welcome source of support for Estonian cyber security development, and indeed for the whole country's IT development, it is clear that this situation is not sustainable for the country in the long term. Primarily the resources of the state itself must ensure Estonia's security in cyberspace and therefore more financing than before is needed for IT development and the field of cyber security. This is a natural step; the European Union structural support has been used to build a solid foundation for our national IT infrastructure and now it is time to take primary responsibility for our IT investments and cyber security.

# Supervision

**Information security management of healthcare providers require attention.**

A risk-based, cooperative, and conservative approach to supervision is important to ensuring cyber security in Estonia.

In addition to evaluating the general level of information security, we inspected the implementation of information security measures and fulfilment of action plans in seven ministries in 2015. We also looked at the organisations' documentation and provided suggestions about which upgrades to make and how to address inadequacies.

We also analysed the implementation of information security measures and how organisations fulfilled the auditing requirement. A study involving eleven ministries and twenty-four agencies demonstrated that the level of implementation of information security measures in public sector organisations is satisfactory; deficiencies in the fulfilment of audit requirements were only found in some organisations. We introduced the results of the study at public sector organisations, to information security managers, and to the members of the Association of Estonian Information Systems Auditors.

Part of our supervision duties over telecommunications providers requires us to compile an annual report of incidents to submit to the European Network and Information Security Agency (ENISA). Even though companies providing telecommunications services in Estonia regularly conduct their own risk assessments and consider themselves able to respond to failures and attacks adequately, it is clear that dependence on telecommunications services also affects other (incl. vital) services. We continue to keep an eye on risks associated with telecommunications services, since they are of critical importance for ensuring cyber security in Estonia.

Information security management of healthcare providers continues to require our attention as well. Estonia's healthcare sector is highly dependent on the functioning of IT systems. In cooperation with the Data Protection Inspectorate, we comprehensively mapped the information security situation in Estonia's primary care provider centres in 2015 and we will continue this course of action in 2016 as well.

# International Cooperation

Estonia's cyber security arrangement and experiences continue to garner considerable international attention. The interest toward Estonia's cyber security policy and activities has also grown as a result of the geopolitical instability in relations between Russia and the rest of Europe and NATO. Hybrid warfare in Ukraine and Moscow's aggressive rhetoric toward its neighbours and NATO has provided the opportunity to contribute influentially to numerous international forums in Estonia and abroad. RIA's analyses and assessments regarding international cyber security trends are followed with interest and recognition.

Close cooperation with important partner countries in Europe and North America continued in 2015. The three Baltic countries signed a cooperation agreement in November that enables closer cross-border cooperation in the prevention and resolution of cyber incidents. It is noteworthy that Baltic ministers signed the document digitally and this is the first known agreement between three countries that has been signed digitally.

RIA's cooperation frameworks were supplemented by the cyber security cooperation agreement with Japan that was adopted in December. The agreement was signed at the third annual Estonia-Japan cyber security dialogue in Tokyo.

The Digital Five (D5) meeting that took place in Estonia in November featured cyber security topics as well. D5 is a format that was created in London in 2014 to bring together the five most digitally developed countries in the world: Estonia, Israel, South Korea, the United Kingdom, and New Zealand. The aim of the network is to share experiences and cooperation in the development of e-government solutions.

RIA experts also shared their know-how in the framework of several cyber security capacity-building programs in Eastern Europe and South America. RIA was visited by numerous delegations from developing countries in Africa and Asia, who were provided with suggestions about how to set up CERTs, implement public-private cooperation models, carry out national cyber security strategies, and compile regulations.

**Cyber security cooperation agreement with Japan was signed.**

Riigi Infosüsteemi Amet 2016