Republic of Estonia
Information System Authority

# 2014 Annual Report Cyber Security Branch Of the **Estonian Information System Authority**

# Contents

# 2014
# in Estonian Cyber Security

## In Estonia in total:

**1,151** incidents handled
(**1164** in 2013)

**22** denial-of-service attacks
(**13** in 2013)

**295** defacement incidents
(**240** in 2013)

**127** quarterly summaries and incident reports submitted to RIA (**73** in 2013)

## In state institutions:

**486** incidents in state institutions
(**135** in 2013)

**The most common reasons for incidents:**

- attacks
- power cuts
- data communication disruptions
- software malfunctions


of reported incidents were highly critical.

## Dangerous vulnerabilities:

Heartbleed and Shellshock

## 23 cyber security training events,

total number of participants **744**

## International cyber exercises:

Cyber Europe, Cyber Coalition and Locked Shields

## 60% of people in Estonia use smart devices.

**75%** of children say, "My parents are not interested in what I do on my smart device."

# Not only do we need Plan B, but we also need Plan C

> *The sense of tragedy is that the world is not a pleasant little nest made for our protection, but a vast and largely hostile environment, in which we can achieve great things only by defying the Gods; and that this defiance inevitably brings its own punishment.*
>
> Norbert Wiener
> The Human Use of Human Beings: Cybernetics and Society (1950)

When Norbert Wiener, the father of modern cybernetics, wrote down his vision of the world as an insecure place in 1950, he was probably more affected by the recently ended Second World War than the vision of the threats in the future digital society. Today, more than half a century later, the world around us, including the cyber environment, entails numerous threats and risks. Our ability to handle them is mostly dependent on ourselves and our ability to identify the risks and our readiness to manage them.

Estonian capacity for handling cyber risks can be considered satisfactory. The survey published by the International Telecommunication Union (ITU) in 2014 places us in the honourable 5$^{th}$ position in cyber capability; in Europe, we even hold the 2$^{nd}$ position. Estonian society trusts its E-State. The recently held elections set a new record as 176,491 voters gave their vote electronically. The high level of trust also sets increasingly higher expectations for guaranteeing cyber security and the capabilities of managing incidents and crises.

We also faced many new challenges in 2014. The security situation deteriorated noticeably. A war is being fought in Europe and we have to operate in that context. The increasingly serious security situation was also reflected in the incident statistics. The number of incidents related to foreign special services has increased significantly. Throughout the year, there were several denial-of-service attacks which tested the limits of Estonia's e-services. Several critical disruptions clearly proved the fact that the functioning of the Estonian state, including the external border guard and the functioning of internal security, is today dependent on the Estonian government network and the data exchange between the state institutions.

At the international level, the field of cyber security is still affected by the PRISM scandal of 2013 and public interest in the activities in the field of security is continuously high.

Several bugs in the implementations of cryptographic algorithms were discovered (OpenSSL etc) but also the breaking of older encryption algorithms (DES and RSA1024) with cheaper (cloud-)computation services or dedicated processors. Discovering and attributing exploitation of these vulnerabilities may be extremely difficult if not impossible.The bugs received significant media attention already weeks before software developers could create patches. At the same time, simple attack instructions, which explained how to take advantage of the vulnerabilities and harm systems, were spreading on-

line. This was especially alarming in the case of Heartbleed because it is very complicated to identify and verify the occurrence of an attack after it has taken place. There is no reason to believe that the situation will change in the upcoming years. For example, at the very beginning of 2015, Ghost, a critical vulnerability in the Unix operating system, received considerable media attention.

Both the ID-card and other important Estonian e-infrastructures are based on cryptography. The secure lifespan of cryptographic algorithms has become shorter, which in turn means that the time to take action before these algorithms are broken is even shorter. In the next few years, Estonia needs to pay significantly more attention to cryptography than before. This is needed to guarantee the secure functioning of the base infrastructure of the E-State.

The surveys and risk analyses that have been carried out suggest that the risk awareness of the Estonian people and institutions is rather high. However, there are also some problematic issues. For instance, in order to guarantee the continuous operation of the critical infrastructure, it is essential that the infrastructure companies not only understand who they depend on but also know which services depend on them. It is easy to say that a service will be disrupted in case of a power outage, but it also needs to be acknowledged that ensuring power supply is, in turn, dependent on the functioning of telecommunication services.

In 2014, RIA aggregated its functions related to guaranteeing cyber security into the cyber security branch. Resources can be used more efficiently now that incident response, risk control and regulatory supervision as well as research and development activities are more clearly organized into one unit. We have been able to contribute to increasing the security of our working environment and improving our professional competency. In international cooperation, there are increasing opportunities to contribute to building the cyber capabilities of other countries, thereby giving us the chance to enhance cyber security on a wider scale. The cyber environment is global and all countries need to contribute to overcoming the threats it contains.

In the upcoming year, RIA will prioritise the fields in which the incidents taking place have a direct impact on the life and health of people or the society as a whole. The developments in medical technology, internet of things and new challenges in guaranteeing the security of the Estonian state are just some examples of the fields that require significant attention in the near future.

It is difficult to predict or prevent the full impact of a massive cyber incident. The main means for organisations, the state and each individual to increase their level of cyber security is to improve their skills and knowledge, in order to identify risks and have functioning back-up plans, in case something actually happens. To alleviate the consequences of the incidents, just having a plan B is not enough – we also need a plan C.

Toomas Vaks
Director of Cyber Security

# Significant trends in Estonian cyber security in 2014

The keywords characterising the incidents in 2014 were the following:

- Several bugs in the implementations of cryptographic algorithms were discovered (OpenSSL etc) but also the breaking of older encryption algorithms (DES and RSA1024) with cheaper (cloud-)computation services or dedicated processors. Discovering and attributing exploitations of these vulnerabilities may be extremely difficult if not impossible.

- Many flaws were identified in widely used software products (for example, Wordpress, Joomla, Drupal, Saurus).

- Ignoring the maintenance obligation of IT resources. The first two problems are magnified by the fact that several organisations do not react to security mistakes in a reasonable period. This kind of reaction gap poses a danger not only to web applications but to all information systems, i.e. SCADA systems connected to the internet that regulate the functioning of water supply, electricity and heating etc.

- Constant and clever spreading of malware both via e-mails and websites, which are not effectively identified by traditional antivirus tools. Malware spread by e-mail is prepared in an increasingly clever way. Employees of one organisation can receive messages with the same content, but the malware added to the message is slightly different in each case. At first, the antivirus program might not understand that there is something suspicious added to the e-mail. In addition, more complex malware is often constructed in a way that it can recognize attempts to analyse it with simple devices, e.g. when it is launched in a virtual machine. In this case, the malware behaves completely differently and appears less malicious than when it is in the computer of its victim.

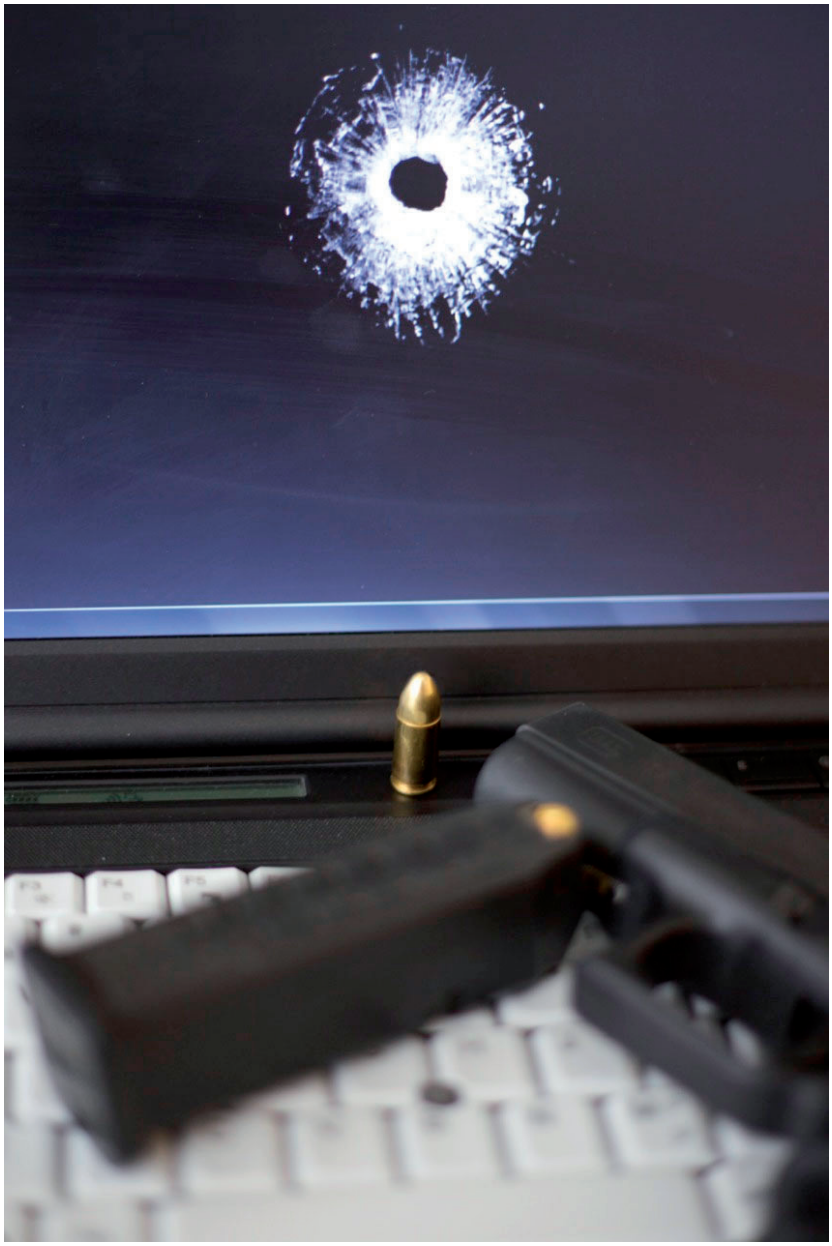
- Skilful phishing of cloud service accounts (e.g. Gmail, Hotmail), which has continued at unprecedented levels at the beginning of 2015 as well. E-mails seem to be coming from a seemingly trustworthy source and have significantly improved in quality both in terms of content and Estonian language usage. This means that the receiver of the e-mail has to be even more attentive and critical in order to detect the fraud.

- Denial-of-service attacks, which are large-scale (both regarding the volumes and the amount of infected computers used in the attack) and multi-dimensional. That means that the attacker first uses one method, which is then blocked by the internet service provider. After that, the attacker implements a new method. This means repetitive and active additional work in configuring the traffic both for the internet service provider and the user, depending on where the rules that fend off attacks are implemented.

- Intrusion into websites is more difficult to identify. It is becoming more common that the infector uploads the malware for a very short time period and takes into consideration which IP-address is used to visit the site. For instance, if users visit the website from Estonia, they receive a different type of malware than users who access the website from the USA.

# Incidents in 2014

Incidents had an increasingly serious effect in comparison with previous years although in figures, 2014 was not very different from 2013. The number of incidents handled by CERT was approximately the same (1,151 handled incidents in 2014; 1,164 incidents in 2013). The rates of different types of incidents (e.g. defacement, infections, phishing) were also similar. Upon assessing the nature of incidents, it appears that there were more smartly and accurately targeted attacks that aimed to damage the services and/or reputation of the state.



The largest change in the incident statistics collected by RIA has taken place in the number of incidents reported by state institutions, which has increased significantly. While in 2013, state institutions reported 135 incidents to RIA, then in 2014, the number was already 486, which represented an almost fourfold increase (see a more detailed overview of the incidents in the section "Incidents in state institutions reported to RIA").

## Attacks

In recent years, both the technical diversity and the volume of attacks have increased. At the same time, the everyday dependence of the Estonian society on e-services and data connection is also increasing. This means that common technical breakdowns have a more noticeable effect.

If only a few years ago it was mainly state institutions and financial sector companies that had to deal with denial-of-service attacks then by now the situation has changed and denial-of-service attacks have become an everyday phenomenon in other areas of activity as well. What should be emphasised are the attacks directed at E-School services, which have in time developed from being students' experiments into a large-scale and continuous problem.

The traditional so-called iconic websites - State Portal, websites of the President of the Republic of Estonia, the Ministry of Foreign Affairs and NATO cyber defence - did not manage to avoid short-term attacks and attempted intrusions. The work of the institutions is not affected by such incidents but the incidents do succeed in causing reputational damage and public anxiety.

The capability of internet service providers to implement defensive measures and fend off denial-of-service attacks has increased significantly. Therefore, there are several instances when the attacker is unable to reach the target.

There is an increased need for additional defence of the government network as a result of serious incidents becoming more frequent in 2014. In the near future, RIA is developing a 24-hour manned security monitoring service, which will guarantee that the initial reaction to the incidents in jurisdiction of CERT will also take place outside working hours.

## Malware

In January, CERT received the first notices of ransomware spreading in Estonia. Fortunately, the spread of Cryptolocker (malware which encrypts your data and requires that ransom be paid to its creators to access it) was quite modest in Estonia in comparison with other European countries. Caution still needs to be implemented: a year later, CERT has been notified of a few incidents where the victims of Cryptolocker are not only individual users, but also organisations' network drives that host several users' files. Malware such as Cryptolocker poses a direct threat in sectors where preventing access to information or destroying information might put people's lives and health in direct danger, e.g. in the case of medical institutions and medical technology, alarm centres, air traffic control centres etc. As the spreaders of malware and credulous users are oftentimes a step ahead of security teams, the infection cannot always be prevented and you need to be ready for the consequences. These are milder if the organisation

has set a proper user rights management system, i.e. every user (and their infected computer) should not have access to all network drives and the files stored there. The backup policy of the institution needs to be analysed from the perspective of Cryptolocker and it has to be guaranteed that once the network has been hit by encrypting malware, it will be possible to save the situation and recover the data.

Out of all the handled malware incidents, the ones that took place via the Elron website are the most noteworthy. The website of a company providing important transport services was hacked into and repeatedly used to spread malware. This makes it plain that there is a need to acknowledge information security topics in a broader, more serious and consistent manner, not only at the level of the IT department but also in organisations and in the society as a whole.

Considering that Elron was the most "googled" word in Estonia in 2014, the incidents undoubtedly had a significant effect.

### Security bugs in software products

For several years, RIA has been worried about situations in which a company, a non-profit organisation or an individual chooses freely available software for providing their services, and after the service has been launched, they fail to perform any further maintenance or install security updates.

According to RIA's statistical data, the most common content management software in the Estonian internet (.ee) domain is Wordpress (26.2% of all the sites matching the query in .ee domain), followed by Joomla (7.1%), Drupal (2.6%) and the local Saurus (1.2%). The larger the number of users, the more interested the attackers are. In case of relatively frequently occurring critical bugs in content management software, the website administrator should react immediately and update the software. What happens in reality, though, is that the IT specialist who originally set up the site was only hired or asked to set it up. What happens later does not seem to be the administrator's or the website owner's business and the main method CERT uses to make the infected the site safe again is to communicate with the provider of the hosting service.

In 2015, RIA is especially worried about the fact that the support for Saurus content management software will be discontinued. According to a realistic and pessimistic forecast, many Saurus sites will still be online after the support is no longer provided, which means that after the security bugs occur, there will be numerous attractive opportunities for the attackers to deface websites and infect them with malware. In the government networks there are 16 domains that use Saurus as their content management software, including RIA's own website.

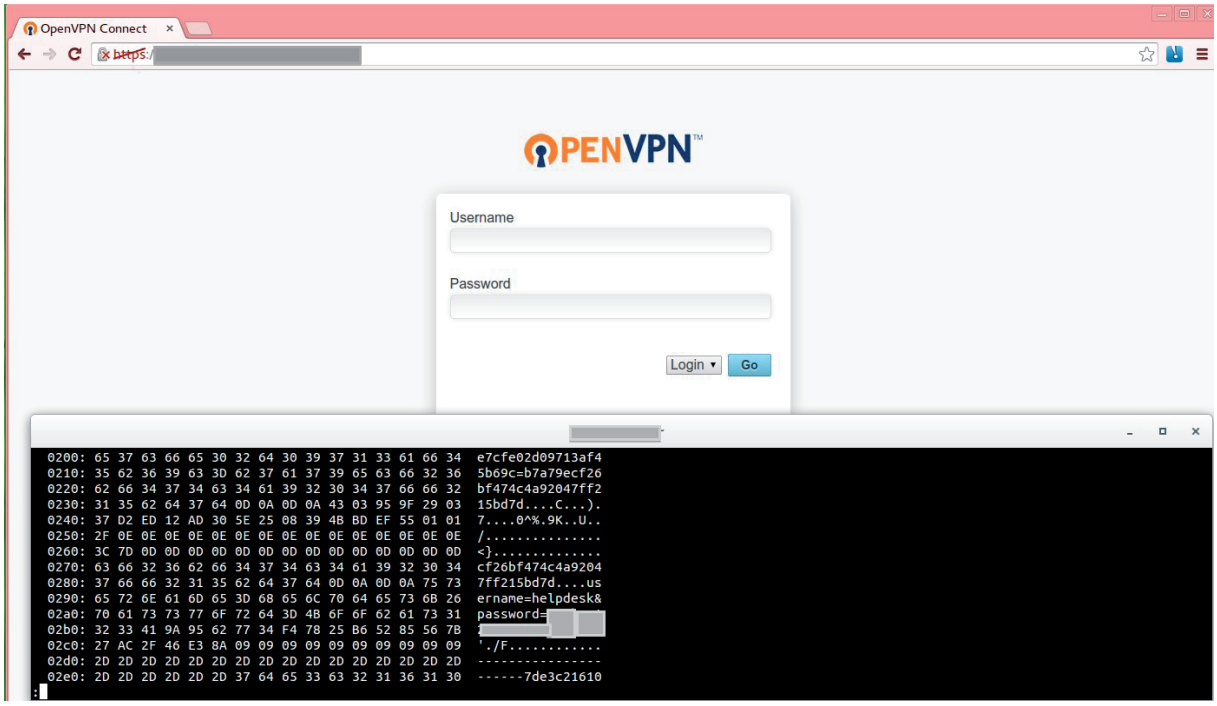
What is remarkable about the software bugs that occurred in 2014 is their PR-aspect. Two most noteworthy instances, the Heartbleed vulnerability in the freeware OpenSSL, and Shellshock, which was a threat to systems administered by Unix, were given a catchy name and a mesmerising logo, which enabled publishing the errors widely in the mass media. In case of these well-branded bugs, even the nature of the bug and the attacking instructions were discussed in media on a large scale and in detail. This happened days, and even weeks, before the software producers using these components could develop the necessary patches.

## Heartbleed

On 7 April, security experts from Finland and Google declared their discovery of a security vulnerability. They called the vulnerability Heartbleed. Heartbleed is a serious vulnerability in the OpenSSL freeware, which is widely used, e.g. in encrypting web traffic, e-mail solutions, for guaranteeing secure remote access and in chat programs. RIA identified approximately one hundred vulnerable servers in the government network ASO and notified their administrators of the need for patches. The servers in the government networks were patched within a couple of days. Altogether, the bug is estimated to have affected about 5% of servers in Estonia.

What also made Heartbleed serious in addition to its wide spreading was the fact that the exploitation of the bug left no trace in the logs of the server providing the service. It makes it impossible to identify based on the logs, whether, when and to what extent the confidentiality and/or integrity of the data located in the unpatched servers had been compromised.

Although the devices in the government network were quickly patched thanks to an intense notification campaign, there are always some institutions that will connect a new service where this vulnerability has not been patched to the network. For example, as late as 9 months after the disclosure of the vulnerability, RIA identified a recently added VPN service in the government network ASO, with administrator user credentials easily detectable with Heartbleed vulnerability.




## The end of XP support

The software producer Microsoft stopped providing technical support to Windows XP operation system in April 2014. This means that the security bugs appearing in this version of Windows are no longer fixed. A computer running on Windows XP can operate without any errors but it is significantly more vulnerable to security threats. With such outdated software, the most concerning fact is the

number of ordinary users. However, an even more critical shortcoming is the fact that the outdated software might be widely used in important institutions and companies, such as in the medical field.

RIA began notifying the public of outdated software risks as early as in the spring of 2013, when about 20% of Estonian users used Windows XP. In the course of the campaign, various popular websites informed the user of the need to update their software. In November 2014, the proportion of users of state portal eesti.ee with Windows XP had decreased to 10.4%.

### Mobile network, mobile devices and the internet of things

With mobile networks, an important global trend at the moment is the accessibility of mobile base stations. In addition to ordinary people interested in technology, these can also end up in the hands of people with malicious intentions, as it happened in Norway at the end of 2014[1]. Although no incidents regarding false base stations have been reported to RIA, readiness has to be maintained.

In handling cases related to internet of things, the most common problem is that the default passwords are left unchanged. For example, in October, the Estonian media wrote about security cameras connected to the internet. The owners of the cameras had not changed the user name and password after taking the camera out of the box. The picture transmitted by this device could be seen online by everyone. Another problem has to do with the fact that the software of the device is not usually updated or the producer is not interested in creating and spreading software updates. In a situation where more and more homes connect their devices to the internet in order to save energy and use smart solutions, such vulnerabilities mean that it is easier for the potential attacker to exploit the devices.

### Phishing campaigns

In 2014, phishing letters circulating in Estonia made a qualitative leap. The campaigns were aimed at the employees of state institutions, accountants, university staff, university students and Foreign Service staff. There was a noticeable trend, e.g. in the case of state institutions, that the letter was not sent to all the contacts found online, but to carefully-selected contacts who could find the content of the specific fake letter relevant, such as the management and the accountants.

As in 2013, the police received reports of different criminals acting as the employees of Microsoft or Windows, who made phone calls claiming that there was a virus in a person's computer. In order to eliminate the virus, the person was asked to send their internet bank passwords or insert credentials to a website that was almost identical to the website of the internet bank.

In the summer, Apple phishing letters circulating all over the world reached Estonia. That is, letters seemingly coming from Apple warned against the expiration of a user name and password. The users were asked to enter their user name and password on a website that was identical to the service provided by Apple itself. The accounts of the victims were locked and ransom was required for opening them.

---

[1] See the news published in Aftenposten about the fake mobile base stations discovered in the Norwegian parliament http://www.aftenposten.no/nyheter/iriks/Secret-surveillance-of-Norways-leaders-detected-7825278.html

A little later, many local government officers received e-mails written in good Estonian and sent by an organisation that introduced itself as the ELGO (European Local Government Officers Database). The letter asked the receivers to update their own, their colleagues' and their organisation's contact information in the database and correct the data that had been inserted without the local governments being aware of it. They also offered the opportunity to add other Estonian local government officers to the database. In order to do that, the e-mail also included the username and the password required to enter the database. According to EU-CERT, ELGO is not related to any European institution; they are probably a private enterprise trying to come across as a credible European institution. It can't be excluded that the campaign is a part of a more complex criminal attack – later the use of data might help to seem trustworthy in order to receive more confidential data. Neither would it come as a surprise if the users of the database received an invoice for using the service.

Sample e-mail:

```
Dear XXX (name of receiver)

We are hereby sending you the username and password of the Database
of the European Local Government Officials, Members of the European
Parliament, Members of the European Commission, and the Ministers of
the Member States. With your login credentials, you get an access to
more than 220,000 contacts in all the areas of European local gov-
ernments.

Should you find mistakes concerning your own establishment, please
feel free to correct your own, your colleagues' or your organisa-
tion's information. If you wish to add some of your colleagues to
the database, please send us an e-mail via the contact field. Subse-
quently, we will send them their personal username and password that
allow access to the database.

Username XXX (e-mail address)
Password xxxxxxxxxxx
hXXps://www.elgo.xxxxxxx
Yours sincerely,
Marcin Bialas
Database Manager

ELGO
119 Altenburg Gardens
London
SW11 1JQ
```

The year culminated with a Gmail account hijacking campaign that involved circulating e-mails that seemed to be coming from a trustworthy sender and written in nearly perfect Estonian, which called for transfering money to a contact that was in trouble. Automatic translation programs cannot produce such an accurate translation, so translators must have been involved. The investigating authorities are identifying more detailed circumstances of this case.

The leap in the quality of phishing campaigns means that the correct Estonian spelling and grammar as a significant obstacle to the credibility of the letters has been overcome and the success of the campaigns and the financial loss proceeding from them are increasing. Therefore, it requires a lot more attention from the user to recognise such e-mails.

## Incidents in state institutions reported to RIA

In 2014, both the number of submitted incident reports and the summarising quarterly reports increased. The incidents are mostly reported in the quarterly summarising reports. In comparison with 2013, state institutions reported over four times as many incidents to RIA. On the one hand, this trend shows both increasing activity in cyber space (increasing use of information systems, rising number of unplanned disruptions, more malicious activities), but also the increased maturity of security management processes. Institutions pay more attention to acknowledging, analysing and communicating incidents. Professional reporting of incidents shows that there is a functioning information security policy in the organisation. Incidents and their effects on services are identified and the necessary lessons learned and conclusions are drawn.

The quality of reports is on a rise in general. The IT aspect of the incident is mostly quite accurately described in the reports (e.g. whether it was a problem in the specific version of one or another software), but there is room for development in the analysis of business impact, i.e. the analysis of what the incidents meant for the operation of the institution. For example, if the e-mail system did not function for an hour, it should be analysed how many users and processes this problem affected, how critically it affected them, and what would have been the possible alternatives.

### Number and frequency of incidents in state institutions

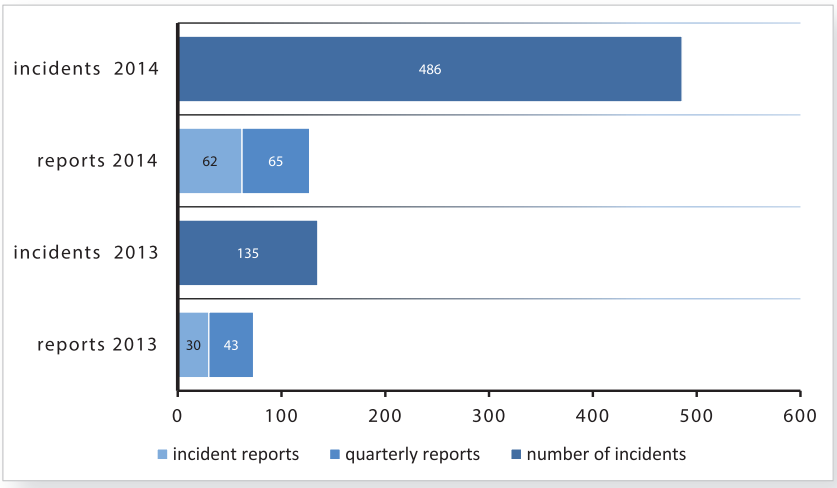



Figure 1: number of incidents and reports submitted to RIA in 2013 and 2014.

Most of the reported incidents took place in late spring, in the second half of May and in June. They mostly included traffic indicating malware and port scanning the exact impact of which to the operation of institutions has not been described and which the reporters considered to be incidents of

low criticality. According to RIA's estimate, these were merely test attacks, not incidents that had a serious effect on the operation of institutions. In June, there was also the so-called OLAF campaign (OLAF – European Anti Fraud Office), when several accountants of state institutions received seemingly real but actually infectious e-mails (see https://www.ria.ee/kes-on-olaf/ for more information).

There were also several incidents affecting various institutions in the third quarter. In the middle of September, many state institutions reported that their users had become infected with malware that had been received from Elron's website. The effect of the incidents was generally seen as average. At the same time, it is important to note that "Elron" was the most googled word in the Estonian Google in 2014, so the influence of the infection in Estonia in general is quite large.

At the end of August and the beginning of September, there were three disruptions in the work of the state data communication network. The disruptions were caused by technical faults and affected several state institutions. The reports about the influence of those disruptions were received from 8 institutions altogether. However, there were more institutions that were affected, as in some cases the reporters were central IT institutions that provide services for several organisations. In six cases, the criticality of the incident was deemed to be high and in three cases average; for example the operation of digital prescriptions and border inspection points was disrupted.

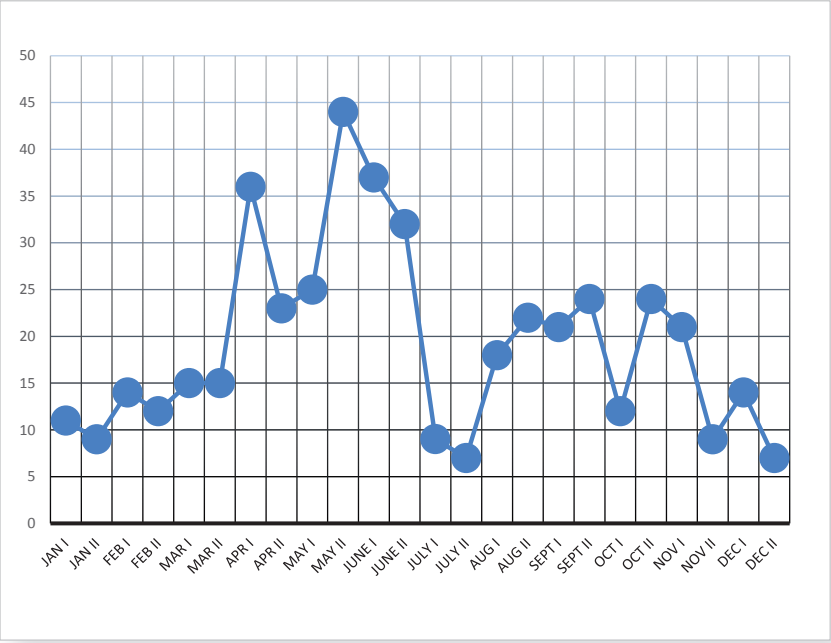



Figure 2: frequency of reported incidents in 2014

## Type of incidents (availability, confidentiality, integrity)

In 2014, just like the previous year, most incidents reported by state institutions were availability incidents, but there was also a noticeable increase in the percentage of confidentiality incidents. Here, it is important to emphasise that with several incidents, the report states that they fall under several categories; e.g., some malware can give the attacker a chance to influence both the integrity and confidentiality of data. The columns below therefore rather describe the percentages of how many times the types of incidents were mentioned, not the percentages of the nature of incidents.

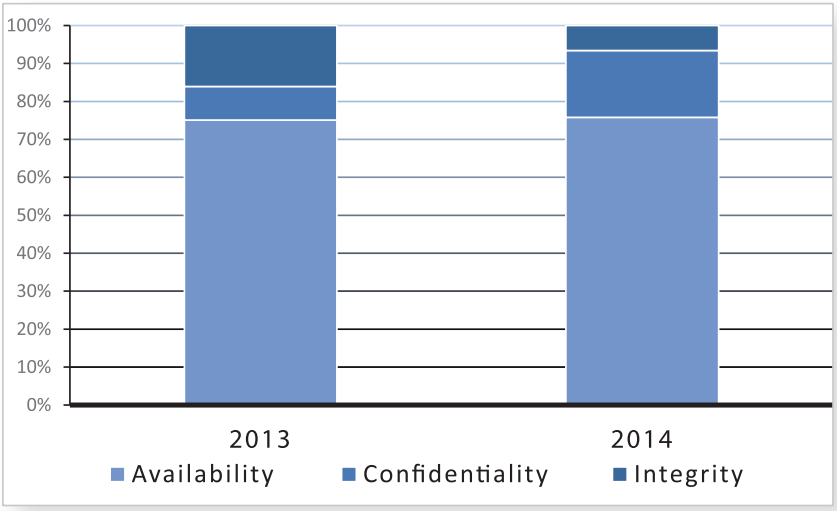



Figure 3: Percentage of availability, confidentiality and integrity incidents in 2013 and 2014

The incidents threatening confidentiality were mentioned most frequently in the 4th quarter, which was when the number of attacks, mainly phishing e-mails and infected computers increased (see Figure 10).

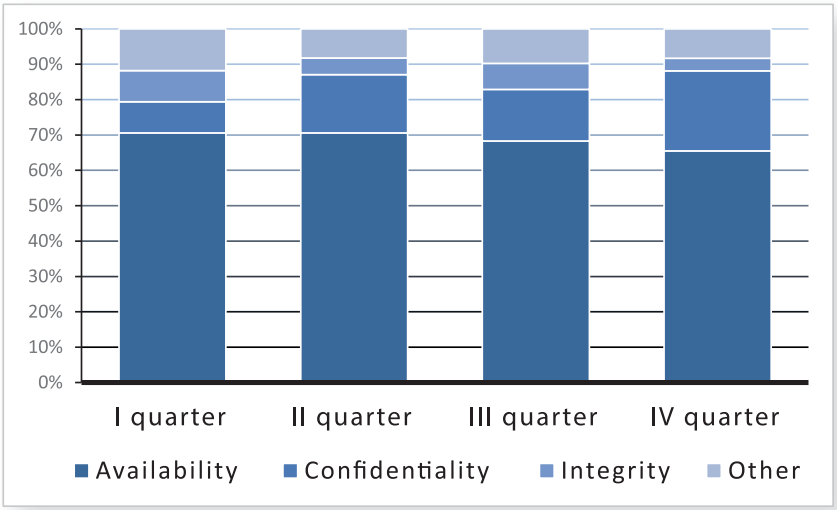



Figure 4: Percentage of availability, confidentiality and integrity incidents by quarters

## Effect and criticality of incidents

In 2014, there was a slight increase in the percentage of incidents that had actual consequences for the institutions and users. For instance, the use of a document management system was disabled or, in more severe cases, digital prescription or Schengen information systems were down. There are still many reported incidents the impact of which has not been described and/or with an impact hard to identify based on the report. In 2013, the proportion of reported incidents with an unidentifiable effect was 10% of all reported incidents; in 2014, it had already increased to one third of all the reported incidents. The proportion of avoided incidents or which turned out to be merely identified threats, also slightly increased in 2014.

In order to improve the quality of reporting, RIA is planning to continue raising awareness regarding the importance of reporting both in state institutions and with vital service providers. There are also plans to take steps in order to organise the reporting process; complementing the reporting form and making it machine-readable.

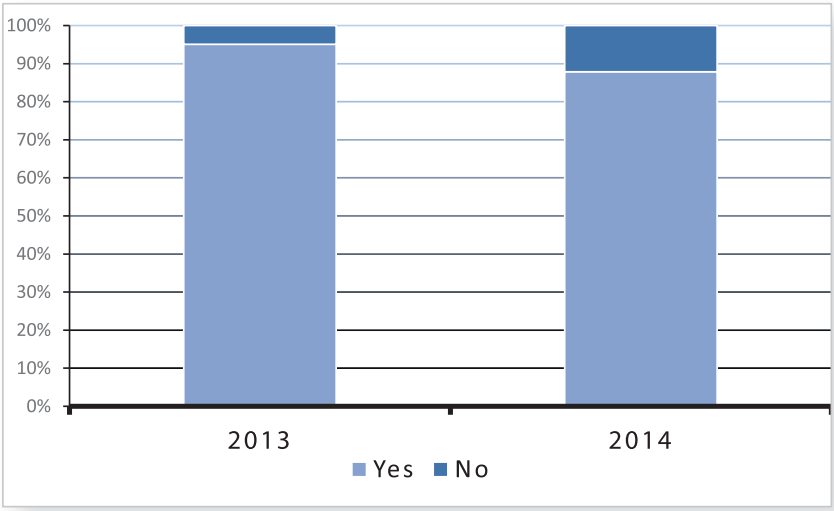



Figure 5: Influence of incidents in 2013 and 2014

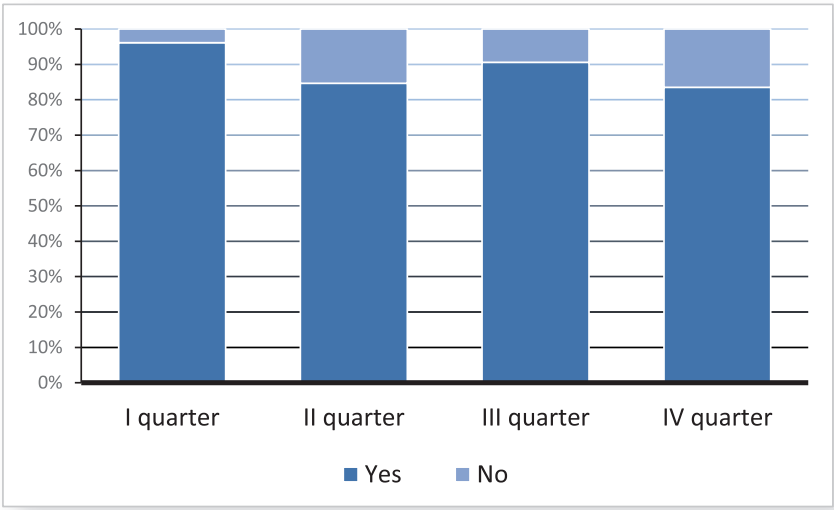



Figure 6: Influence of incidents by quarters in 2014

## Criticality of incidents

In 2014, state institutions provided a significantly improved overview of the criticality of incidents. At the same time, the proportion of critical incidents of all reported incidents has stayed on a similar level, around 20%. The proportion of incidents of average and low criticality has risen in an equal manner with a significant decrease in the "not specified" category.

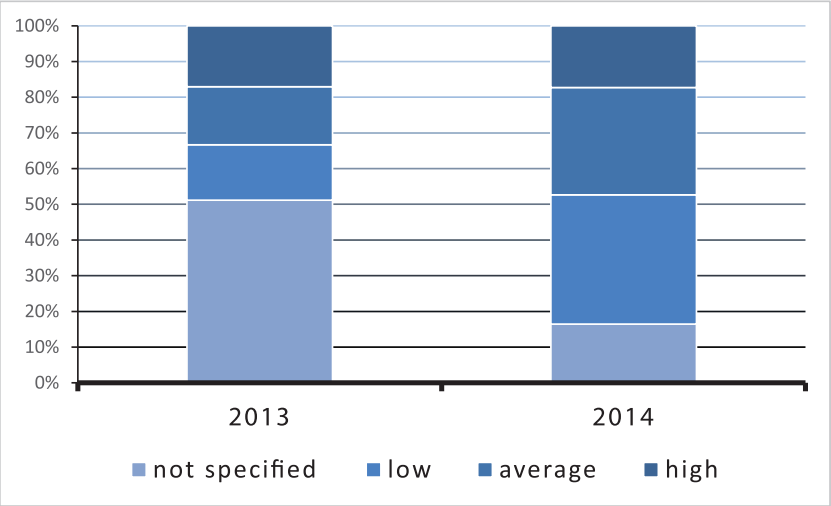



Figure 7: Criticality of incidents in 2013 and 2014

State institutions reported the largest number of critical incidents in the second quarter. These were mainly data communication disruptions that affected several institutions at the same time. The Heartbleed vulnerability was discovered in that quarter as well. There were no actual violations related to Heartbleed reported to RIA in the spring, but such reports came later, in cases when IT specialists had connected a new device in the network that was unpatched for the dangerous and widespread vulnerability. In such cases, RIA reacted fast and decisively and the problem was solved. Also in the 4th quarter, the majority of critical incidents were incidents caused by a disrupted data connection, but there was also Shellshock, another widespread vulnerability that kept the reporters and security officers busy.

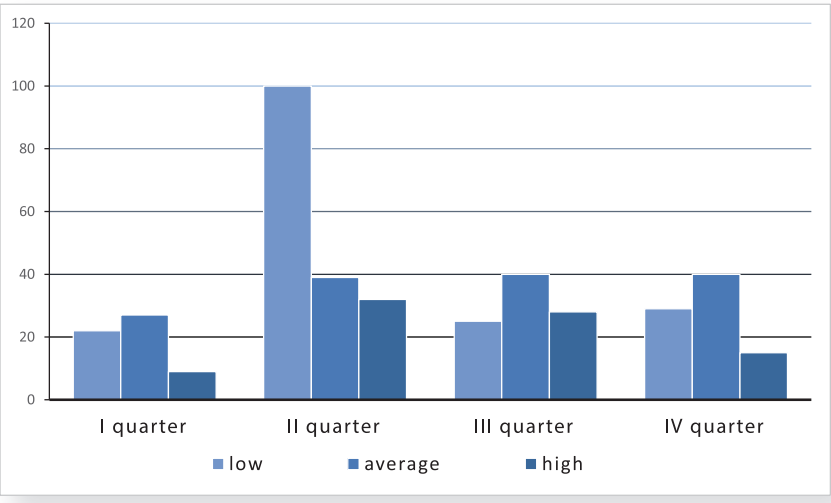



Figure 8: Criticality of incidents in 2014 by quarters

## Causes of incidents

The proportion of attacks of all cited incidents did experience a slight decrease in 2014; however, attacks were still the most common causes of incidents, closely followed by "other" reasons (usually "other" causes include power outages). Other common causes for reported incidents were software deficiencies and external service providers' errors (this category also included power cuts and data connection disruptions).

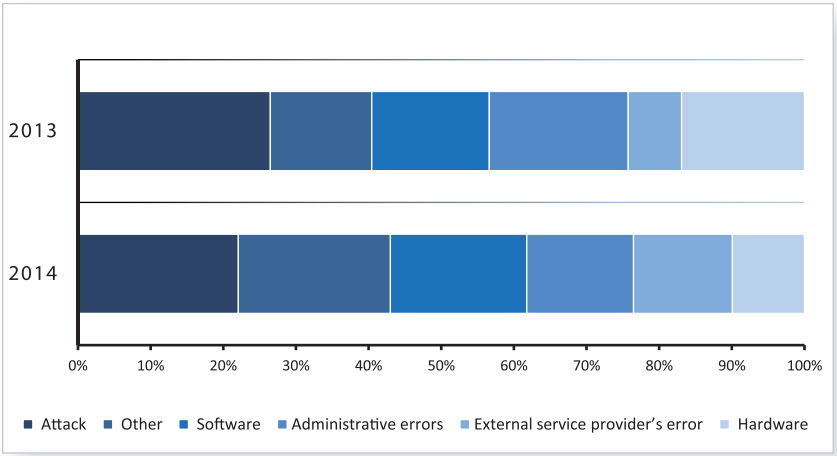



Figure 9: Most common causes of incidents in percentages in 2013 and 2014

The largest number of attacks was reported in the fourth quarter of the year, although the proportion of attacks in relation to other types of incidents was the highest in the second quarter. The incidents at the end of the year were mainly virus outbreaks and well-aimed phishing letters, but also distributed denial of service attacks, many of which did not last for a very long time, but according to RIA's estimate, seemed to be mapping the resilience of systems. On the one hand, the increase of such seemingly pointless and short-term distributed denial of service attacks (DDoS) is worrying; on the other hand, the increasing number of DDoS is a global trend resulting from their constantly increasing availability and falling prices.

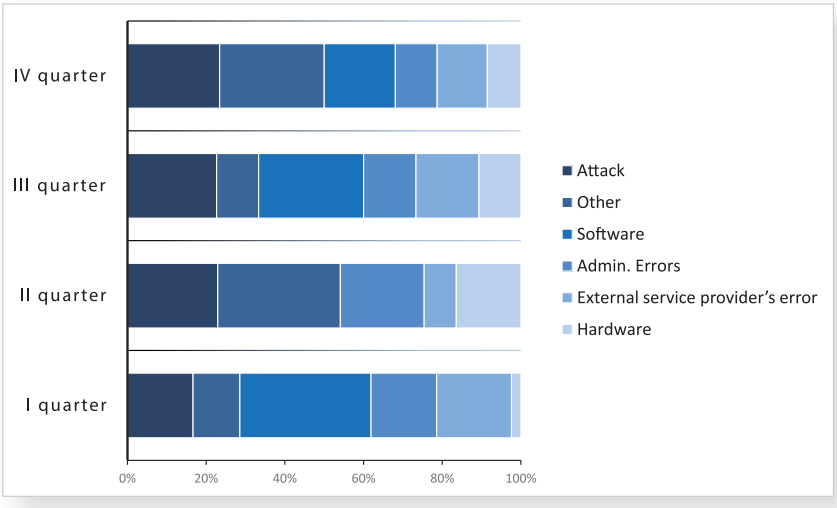



Figure 10: Percentages of the most common causes of incidents in 2014 by quarters

# Studies and guidelines

In 2014, RIA commissioned three large studies: a study of security awareness and security-related behaviour of smart-device users; a subsequent edition of the study regarding the life cycle of cryptographic algorithms, and; a guide of security requirements for large significant data centres. In addition to that, RIA conducted a smaller study on its own in order to find out the risk perception of state institutions and providers of critical services.

### Perception of IT-risks in state institutions and critical service providers

In the autumn, RIA conducted a questionnaire among the IT managers and IT security managers of state institutions and critical service providers in order to find out how IT-related risks are perceived in these institutions. The questionnaire was anonymous and was filled in by 16 critical service providers and 25 IT managers and IT security managers of state institutions.

- IT managers and IT security managers perceive malfunctions as the greatest risk. These are followed by politically motivated attacks and information collection.
- Only some of the responding organisations have not introduced information security requirements or appointed a person responsible for information security.
- 88% of the respondents estimated that the dependency of the organisation's operation on ICT systems is high or very high. 78% of the respondents also said that in the last three years, risks have been analysed and evaluated in their organisation.

For RIA, important conclusions from the results of the questionnaire were that the quality of reporting as well as the risk awareness of the management need to be improved. Information security managers and management need systematic training. In order to assess risks wisely, it is important to contribute to identification and analysis of cyber risks, especially through independent audits and tests.

### Study of security awareness and security-related behaviour of smart device users

In the autumn, TNS Emor carried out a study commissioned by RIA and Look@World Foundation concerning the security awareness and security-related behaviour of smart device users.

The study showed that in 2014, 60% of the Estonian population aged six or older have smart devices and/or have access to them. At the same time, it appeared that people have insufficient understanding of the dangers related to using smart devices, and often, they lack practical skills. For example, seven children out of ten can use a smart phone at all times and as much as they want, and 75% of them say that their parents are not at all interested (19%) or rarely interested (56%) in what they do in their smart devices.

The study was prepared in the framework of the EU's Structural Funds programme "Raising Public

Awareness about the Information Society" funded by the European Regional Development Fund of the European Union. The results of the study are available at the website of Look@World: http://www.vaatamaailma.ee/wp-content/uploads/veeb-Nutiseadmete-kasutajate-turvateadlikkuse-ja-turvalise-k%C3%A4itumise-uuring_ARUANNE-2014.pdf

### Study of the life cycle of cryptographic algorithms

In the spring of 2015, the second study of the life-cycle of cryptographic algorithms used in Estonia will be finished. Among other things, the study re-emphasises several recommendations that were already published in 2014. To summarise, cryptographic methods of several important Estonian software products and services need to be updated in the upcoming years. At times, this might cause inconveniences for users, because due to the complexity of systems, it is not always possible to forecast all possible impacts of changes.

As the life cycle of all algorithms is limited, the time to act in order to update all the cryptographic methods of services is even more limited. At some point, it might appear that smooth transition period has not been sufficient; e.g., when powerful quantum computers are used to break the cryptography. We need to have an action plan for the scenario when any of the algorithms important for some Estonian e-service has been broken. RIA sees a clear need to have such plans and to rehearse them.

### Guide of Security Requirements for Data Centres

In May, the Guide of Security Requirements for Data Centres was commissioned by RIA and prepared in cooperation with AS Elion Ettevõtted. It is meant, primarily, as a guide for designing, building and maintenance of server rooms and data centres that host databases of public services critical services of high availability requirements. The guide is available on the ISKE guides website (https://www.ria.ee/iske-dokumendid/).

## Preventing cyber risks

### Weblog on cyber security

In 2014, the cyber security service created a weblog in order to provide fast and practical guidelines to patch the vulnerabilities threating the Estonian internet environment and to acknowledge malware campaigns. The blog also includes posts that discuss other topics relevant to the Estonian cyber security. The weblog is available at https://kyberkirjutised.ria.ee/.

### Training courses

In 2014, RIA organised altogether 23 security-related training sessions, seminars and information days, financed by the EU structural funds program "Raising Public Awareness about the Information Society", with 744 participants. The training events included both workshops for developing practical security skills (IDS, IPv6, OpenDNSSEC) as well as seminars aimed at non-IT specialists and general information-day type events.

## Exercises

RIA plans and organises international exercises, and in addition to participation leads the international cyber exercises on the domestic level. The planning stage usually starts a year before the exercise and includes recruiting participants and adjusting the enacted incidents to the Estonian circumstances.

**Cyber Europe.** In 2014, ENISA carried out the international exercise Cyber Europe, covering both the technical level and the interagency operational level. The participants of the exercise included 20 member states, European information security and cyber security organisations, and Iceland and Norway. There were altogether more than 670 people from more than 200 organisations involved in the exercise. The first stage of the exercise in April 2014 was technical and allowed the participants to solve 16 different security incidents/tasks altogether. In two days, they were asked to examine and analyse incidents that might affect data confidentiality and integrity of these organisations, leaking of information or critical infrastructure. From Estonia, there were 9 teams and 34 people from 6 different organisations participating in the technical exercise Cyber Europe 2014. In the second operational phase of the exercise, the same agencies practiced cooperation, exchange of information and coordination of activities both on the domestic interagency level and the EU level. The third strategic phase of the exercise was carried out in Brussels in February 2015. In the exercise, RIA was in the role of planner, moderator, national contact person, player, and assessor.

**The exercise Cyber Coalition** was organised by NATO in Tartu for the second consecutive year. The Estonian governmental agencies participating in the exercise stood out with their skilful solving of technical incidents. For example, Estonia was one of two countries whose specialists were able to solve the forensics task of Android malware at the exercise. The content of the exercise also required coordination of work and exchange of information between the agencies. The lessons received from the exercise will be implemented in planning further activities as well as exercises.

The technical exercise **Locked Shields** organised by NATO Cooperative Cyber Defence Centre is permanently held in Tallinn. This is an exercise where systems created in a fictional environment are attacked and protected in real time. The exercise proved the excellent level of Estonian technical competence once again; Estonia was the best forensic team at Locked Shields. Overall, the Estonian team achieved the third place this year. The team included specialists from state institutions, ISPs and companies providing critical services.

## The Committee of Information Security Managers

In 2014, the Committee of Information Security, which had so far been gathering unofficially, was given an official form and working order. This is a body gathering information security managers of state institutions which has a management board, regular meetings and decision-making power. In 2014, among other things, the Committee discussed topics related to the implementation of ISKE, exchanged information and experience in implementing security measures and in the occurrence of dangerous vulnerabilities.

## DNSSEC

In Estonia, the Estonian Internet Foundation opened a DNSSEC service for sites in the .ee top-level domain. DNSSEC (Domain Name System Security Extensions) protects the internet users and domain owners by making sure that the user is not being redirected to some other site instead of the page they want to visit without them knowing about it. The first domain signed with the security extension was the state portal eesti.ee.

Protecting the domain system by DNSSEC is an important step towards a more secure internet in Estonia. In order to raise related awareness, RIA and the Estonian Internet Foundation organised a notification campaign targeted at the domain owners. RIA offers free implementation of DNSSEC to its partners, i.e. state institutions and local governments. More information about the DNSSEC service is available at www.ria.ee/vorguteenused.

## Risk analysis methodology

In 2014, RIA started to complement the IT risk analysis methodology targeted at critical service providers. Pursuant to the Emergency Act, critical service providers are obligated to assess their risks, including ICT risks. Having gone through more than a hundred risk analysis and contingency plans, RIA had to conclude that the analyses include scarce and very general information about ICT risks, so the state's expectations regarding ICT risk analyses should be described in a more detailed and unified manner. A thorough and updated ICT risk analysis will primarily benefit the critical service providers themselves but also the state, so that it can assess the cross-dependencies of ICT infrastructure and services.

RIA will finish compiling the guideline in 2015, including by involving the Ministry of the Interior and critical service providers in the preparation process. The guideline is planned to be used to supplement the Minister of the Interior's regulation No. 16 of 8.06.2010 "Guideline for preparing contingency risk analysis" (https://www.riigiteataja.ee/akt/13326405).

## Public awareness of cyber security

The results of the Eurobarometer 2014 survey showed that Estonians trust the state as the guardian of personal data more than in Europe on the average. Estonians are also less worried about the consequences of cyber-attacks and claim to be good at identifying fake e-mails.

40 percent of Estonian respondents are worried that state institutions do not store their personal data securely. The average indicator in the European Union was 67 percent. Whereas 53 percent of Estonian respondents distrust storing data on websites, an average of 73 percent of respondents in the European Union distrust this way of preserving data.

Estonian respondents are the least worried about the possibly of not accessing the internet and public and banking services due to a cyber-attack. In Estonia, 39 percent of respondents are concerned about it, while the average percentage in the European Union was 50.

In comparison with the European average, there are more respondents in Estonia who have in-

stalled an antivirus software on their computer, do not open e-mails with unknown content, use only their own computer and regularly change their passwords. Estonians are also clearly less worried about phishing attempts than Europeans on average.

The Estonian factsheet of the survey:
http://ec.europa.eu/public_opinion/archives/ebs/ebs_423_fact_ee_en.pdf

The entire survey: http://ec.europa.eu/public_opinion/archives/eb_special_439_420_en.htm#423

# International cooperation 2014

The year 2014 was active in terms of foreign contacts. RIA was visited by numerous foreign delegations that came to exchange experiences on building and developing cyber security (organisations). In addition to partners from Europe and North America, we also received delegations from the Middle East, Africa, Japan, South Korea, Singapore and New Zealand.

There were several bilateral expert meetings with important partner organisations in Europe (the United Kingdom, Germany, France, the Netherlands) and in the USA to exchange experiences about protecting critical information infrastructure, risk management, cyber security exercises and training. In the autumn, RIA held an interagency cyber security seminar in Tartu in cooperation with colleagues from the United Kingdom. In cooperation with the George Washington University in the USA, there was an Estonian cyber seminar held in Washington, where RIA introduced Estonian developments, solutions and the cyber security strategy for 2014–2017 to a large audience made up of listeners from the US governmental agencies, the private sector and universities.

As a new priority, RIA decided to improve the visibility of Estonia in the Western Hemisphere and, in October 2014, concluded a cooperation agreement with the Organisation of American States (OAS) to support the cyber security capabilities of the region. Since the summer of 2014, RIA has been included in five training projects of the OAS in Colombia, Dominica, Trinidad and Tobago, Washington and Jamaica. The focus of the training projects has been different, ranging from the topics related to interagency coordination and organisational structure of cyber security to technical base training.

# Significant changes in the legislative and strategic framework for cyber security

### New competencies and obligations of RIA

On 1 July 2014, the Act for the Amendment and Application of the Law Enforcement Act entered into force. Pursuant to this act, starting from summer 2014, RIA is a law enforcement body. According to the changes, the Technical Regulatory Authority's supervisory competency of guaranteeing the security and integrity of communication networks and services set in the Electronic Communications Act was transferred to RIA. The same draft also established RIA's supervisory competency in the Emergency Act and the Public Information Act.

RIA is the institution that the communication companies need to inform of important incidents threatening the security and integrity of communication networks and services. Contact persons appointed in the critical service providers need to notify RIA immediately of any security incident of significant impact. RIA is the body conducting extra-judicial proceedings regarding the violation of electronic security requirements pursuant to the Emergency Act and regarding the violation of requirements set for security and integrity of communication networks and services pursuant to the Electronic Communications Act.

Pursuant to the Public Information Act, RIA is now responsible for checking and coordinating competency of registration of data collections. This competency was previously a task of the Ministry of Economic Affairs and Communications, but a large part of the coordination process was also previously conducted in tight cooperation with RIA.

### Cyber security strategy 2014–2017

On 11 September, the government approved the "Cyber Security Strategy for 2014–2017" and its implementation plan. The strategy continues to target several goals set in the previous cyber security strategy, but there have also been new risks and requirements added. The dependency of the functioning of the state on information technology has increased and cross-dependencies have also increased, meaning that the provision of several critical services is no longer dependent on the functioning of Estonian IT-systems but also on the infrastructure and e-services in other countries. The main aim of the cyber security strategy for four years is to increase the cyber-security capabilities and public awareness of cyber risks in order to ensure continuous trust towards cyber space.

Implementation of the strategy is funded from RIA's budget and the European Structural Fund. The challenge here is that the structural funds prioritise activities to develop the information society and do not in turn directly concentrate on the aims of cyber security strategy.

https://www.mkm.ee/sites/default/files/kuberjulgeoleku_strateegia_2014-2017.pdf

### Preparing for large-scale cyber incidents

In 2014, RIA, in cooperation with its partner organisations, developed common principles of readiness for emergency and cooperation in case of large-scale cyber incidents. An interagency working group lead by RIA prepared the draft for the Government of the Republic's order "Plan for solving a large-scale cyber incident emergency". The plan will be sent for approval to the Government of the Republic in the autumn of 2015, after testing it in 2015 both at local and international exercises.

Valuable lessons for implementing internal states of readiness and procedures in RIA were learned during the heightened state of security in the spring for the visit of Barack Obama, the president of the United States. Based on this experience and the described requirements, the document "Principles of States of Readiness in RIA" was prepared, which has been approved by the Director General's order in the first quarter of 2015.

## ISKE

Three-level IT baseline security system ISKE is an information security standard that has been created first and foremost for the information assets used to manage data collections of the state and local governments.

In the summer of 2014, the Minister of Economic Affairs and Infrastructure approved the ISKE application guide version 7.0. In this guide, risks, security measures and base modules were complemented, the ID-card measurements updated and the table with the responsible persons for the application of the 11 steps of ISKE (RAC) was added.

Presently, the web-based application of ISKE catalogues is being introduced. It will make ISKE catalogues more user-friendly, meaning that the applier of ISKE will no longer need to work with PDF-files but can navigate conveniently in the web environment of risks, measures and modules. In 2016, the completion of new and updated ISKE tool will be finished. The input for it will be the pre-analysis that was carried out in 2014 (analysis of complementing the ISKE application tool).

In the ISKE framework, RIA pays special attention to topics related to cryptography and cloud technology. In 2014, the cryptographic algorithm usage areas and life cycle surveys proved the need to change ISKE catalogues. (www.ria.ee/public/PKI/kruptograafiliste_algoritmide_elutsukli_uuring_II.pdf). These changes will be published in the next version of ISKE application guide in 2015.

In November 2014, the project "Analysis of Information Security of Cloud Technology" was launched. In 2015 the project will analyse whether and how to process state information systems in the

cloud. Based on the analysis, guidelines for state institutions, service providers and auditors will be prepared. Also, recommendations will be made regarding cloud-technology related additions to the ISKE catalogues.

A significant change in the legislative framework from the perspective of introducing ISKE in the state is the governmental order, which was sent for approval in February 2015. One of the conditions set for the subsidies paid from the EU structural funds is that the subsidised project will have to increase the security of the state's information systems proceeding from ISKE or other relevant and comparable security standard.
https://eelnoud.valitsus.ee/main/mount/docList/dbc25685-0631-4e7f-9ac5-cfab37154bea

# Summary

The year 2014 did not significantly differ from 2013 in the number of incidents, but it was clearly visible that the severity of the impact of the incidents increased. Denial-of-service attacks have seized being a novelty and occur in many areas that depend on data communication and technology.

In addition, the state institutions mentioned attacks, including both denial-of-service attacks and malware campaigns, as the main cause of incidents. The state's e-services were oftentimes disrupted by power cuts and data connection disruptions. For every e-service provider, including the state, these are probable risks that are difficult to manage. Preventing and predicting the causes of incidents is very difficult so emphasis needs to be put on handling the consequences of accidents and malicious incidents in order to ensure the viability of services,. What is needed is a good plan in case something happens, and then another back-up plan for that plan.

On the positive side, both the number of incident reports and summarising reports submitted by state institutions increased in 2014. On the one hand, this trend shows increased activity in cyberspace (intense use of information systems, increasing number of unplanned disruptions, more malicious activities) and also the increased maturity of security management systems, i.e. establishments pay more attention to acknowledging, analysing and reporting incidents. In comparison with 2013, state institutions reported approximately four times more incidents to RIA.

The phishing e-mails circulating in Estonia made a qualitative leap last year. Letters spreading among the public now usually come from a seemingly trustworthy source, are written in good Estonian, have reasonable content and include a seemingly believable attachment or a credible link that will infect the computer. In order to orient oneself in this flood of fake letters, the user needs to be more attentive and distrustful than before. Otherwise, they might lose the content of their inbox and in the worst-case scenario a hefty sum of money.

What deserves emphasising among the handled malware cases is the infection of several organisations, private companies and common users through the website of Elron. The website of the company, which provides an important transport service, was hacked into and it was used several times

in a row for spreading malware. It is a noteworthy fact that Elron was the most "googled" term in Estonia in 2014.

Both the global and the Estonian security communities were shocked by bugs in the implementations of cryptographic algorithms (OpenSSL etc). In the government network, the vulnerabilities were patched within a few days, thanks to RIA's aggressive monitoring and notification work, but later, there have been incidents when an unpatched device has been connected to the network. In the future, readiness has to be maintained for such widespread errors that are widely discussed in the media before patches are applied.

Regarding preventive activities, RIA continued organising cyber security training events and seminars as well as participating in international exercises. Active international cooperation was carried out with many countries from all over the world. RIA also continued informing the public and organising awareness campaigns in Estonia, e.g. concerning the risks related to using outdated software and safe use of smart devices. An important public notification channel is the weblog discussing cyber-related topics (https://kyberkirjutised.ria.ee), which provides information and instructions in case of vulnerabilities and incidents both to specialists but also to victims of phishing campaigns.

The awareness of Estonians regarding cyber risks is surprisingly good in comparison with the European average and the attitude to potential problems is calm. The Estonian respondents are the least worried in the European Union about not accessing the internet or public and banking services in case of a cyber-attack. At the same time, Estonians do not count on luck either – in comparison with the average European, more Estonians have installed antivirus software on the computers. They tend not to open e-mails with unfamiliar content, use their own computer, and regularly change their password. At the same time, the somewhat more specific survey about the safe use of smart devices commissioned by RIA and Look@World Foundation revealed that awareness regarding safe use of smart devices could be better, especially in relation to parents' interest in what their children do with the smart devices.

In addition to reacting to everyday vulnerabilities and risks, the key words for RIA in 2015 are improving the monitoring and resilience of the government network, cooperation with the field of medicine and solutions and risks related to the e-residents programme. What calls for constant attention are Estonian websites that are not maintained nor updated by their owners and are therefore subject to becoming easily infected. Emphasis will also remain on hindering malware campaigns and mitigating risks related to using outdated software.

# Recommendations for additional reading

### RIA weblog

https://kyberkirjutised.ria.ee/

### Threat Landscape 2014 of the European Union Agency for Network and Information Security (published in January 2015)

https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014

### The Global Cybersecurity Index of the International Telecommunication Union.

According to this index, which maps cyber security capability of countries, Estonia shares the 5th position globally with Brazil, India, Japan, South Korea, Germany and the United Kingdom.
http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

### Germany's summary of IT-security in 2014

https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html

### Annual review of the Finnish Cyber Security Centre (in Finnish)

As in the Estonian results, the review emphasises the phishing campaigns becoming more professional; also, the level of Finnish in phishing campaigns has remarkably improved.
https://www.viestintavirasto.fi/tietoatoimialasta/katsauksetjaartikkelit/tietoturva-artikkelit/kyberturvallisuuskeskuksenvuosikatsaus2014.html


National Security Archive,

Suite 701, Gelman Library, The George Washington University,

2130 H Street, NW, Washington, D.C., 20037,

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu