Republic of Estonia
Information System Authority

2013 Annual Report Cyber Security Branch

of the Estonian Information System Authority

2013
in Estonian Cyber Security

135 incidents reported by state institutions

25% **caused by attacks**

Several crypto solutions in use in Estonia
have to be replaced within 2–5 years

In Estonia: 13 denial of service attacks
240 defacement incidents

Estonia attained **second place in the NATO CCD COE**
cyber security exercise Locked Shields

RIA organized
18 security-related training sessions, **497** participants

43 reports presented by state institutions
pursuant to new information security system regulation

Contents

Foreword: 2013 in Cyber Security

Cyber security circles will always remember 2013 as the year of Snowden. The contracted employee of NSA who having escaped to Hong Kong on May 20, 2013, showed the world in the following few months how modern intelligence works and how little hope people actually have of remaining anonymous in cyberspace. Almost a hundred years earlier, in 1929, the Secretary of State of the USA, Henry L. Stimson, disbanded an intelligence unit with words that have remained in history: "Gentlemen do not read each other's mail." Although the need to start decoding encrypted messages arose again soon enough, nobody could have imagined the huge opportunities of today's intelligence at that time.

Monitoring human communication that has moved to cyberspace allows superpowers to guard their security better, but the price they have to pay for it is very high. It is impossible to expect privacy in cyberspace. Besides nosy security services, private companies and cybercriminals, it is becoming increasingly easy for anyone to obtain means that enable them to spy on and monitor others. Using ordinary email is like sending a postcard. True, it is unethical to read other people's postcards...but it is also simple and easy. And in spite of the efforts of protectors of privacy, the Internet tends to remember everything: traces of one-time foolish acts will remain on the cave walls of the Information Age for a very long time to come. Therefore, one must retain common sense, self-control and caution also in cyberspace.

Another important topic for Estonia is the renewal of the cyber security strategy. Our understanding of the need to ensure cyber security for our country in order to guarantee the functioning of the state and the society in a world increasingly dependent on computers has become clearer since 2008. The results of a cyber-attack can be figuratively compared to damaging the nervous system of a society, a state or an individual: it can cause hallucinations or damage the senses (cyber-attacks as means of information/psychological warfare), it can paralyse (obstructing the operations of means of communication and electronic automated control systems) and unfortunately it can also kill (terror attacks against critical services). What is frightening is the efficiency of cyber warfare – a relatively cheap, extremely quick and focused attack can damage the operation of important services. An added bonus from the perspective of the attacker is the possibility to hide and protect themselves better than it would ever be possible in the case of immediate physical attack. Increased dependency on technology and a changed security situation dictate the need to reassess the risks and find new ways to mitigate them.

On the international stage, cyber-issues have become increasingly important and the awareness of cyber-risks is undoubtedly better than it was a few years ago. Unfortunately, the capabilities to mitigate detected risks are still lacking. Therefore, it is pleasing to see, for example, one of the goals of the cyber security strategy of the Netherlands: to change from a risk-conscious society into a society with skills (to mitigate risks). After all, one should keep in mind that security depends mainly on the skills of the user. An unskilled user can damage himself with ordinary kitchen utensils, grabbing a knife from the wrong end can even have fatal consequences. Estonians have learned to use Internet banking, e-state and technology quite well. Therefore, hearing an expert express concerns about the security risks of Estonia's e-solutions sometimes feels like hearing the good European missionaries worry about the dangers of people getting hurt when eating with chopsticks in the East. The people of Estonia have been practicing "eating with chopsticks" for over ten years and can usually manage without causing damage.

It is good to state that no large-scale or serious cyber incidents occurred this year and the people of Estonia can feel quite safe in our e-Estonia.

Have a continuously cyber safe 2014!

Toomas Vaks

Deputy Director of RIA in the Field of Cyber Security

Summary of the Report

This report is a summary of the most important events and topics of 2013 in the cyber security of Estonia.

2013 was a relatively peaceful year in Estonia as far as serious incidents are concerned. The number of classic isolated incidents decreased compared to earlier years, while we saw incidents that received wider attention, where cyber incidents were but a part of a carefully designed information warfare operation. Of such combined operations, the case of #opindependence was undoubtedly the most conspicuous. **13 cases of DDoS attacks** were registered in Estonia by RIA in 2013; **defacements** were much more numerous: **240 cases.**

In preventing cyber risks, RIA continued to pay a great deal of attention to training, international cyber-exercises, and penetration tests of state institutions and critical service systems. An important milestone was the completion of another study of the lifecycle of cryptographic algorithms. It was a clear reminder that in the next 2-5 years, Estonia will have to replace several crypto-solutions, including the ones used in digital ID, m-ID and ID cards issued before 2011.

There was a significant development in the number, regularity and quality of reports presented to RIA by state institutions. On January 1, a Government regulation entered into effect that obliges state institutions to inform RIA of important incidents and make quarterly summaries of same. All in all, state institutions informed RIA of 135 incidents last year. Availability incidents were reported most often. There were less reports of cases related to integrity and confidentiality. Although communication with the heads of cyber security of state institutions was constant and information about the most important incidents reached RIA even before the regulation, the regulation-based reporting system has significantly organised the system; it also provides an opportunity to pay more attention to the impact of an incident.

Several reports of phishing campaigns, infected webpages and service attacks came from schools/colleges in 2013: at least 7 campaigns were organised against educational establishments, and kindergartens were also affected. There was one case in which the phone system of an educational establishment was hacked into and hundreds of long distance calls were made.

A new phenomenon was the voice phishing wave. A person introducing himself as a representative of Microsoft encouraged non-suspecting computer users to download a program and/or disclose passwords that would enable the impostor to access the victim's computer and, through that, their bank account.

Of changes in the legal framework, the most important in 2013 was initating the **Law Enforcement Act Amendment and Application Act** which enhances the rights of RIA in the supervision of state databases. The amendment will become effective from July 1, 2014.

This report is aimed at strategists and specialists ensuring cyber security and interested in the field. The authors do not presuppose a deep knowledge of IT, and they will gladly receive questions or comments at riskihaldus@ria.ee or in the comments of RIA's weblog on cyber security https://kyberkirjutised.ria.ee/2013kokkuvote/.

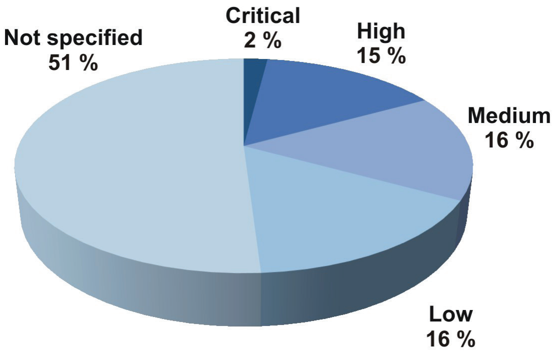
Incidents in State Institutions of Estonia

On January 1, 2013, a Government regulation entered into effect that obliges state institutions to inform RIA of important incidents and make quarterly summaries of same. All in all, RIA was informed of 135 incidents last year. Availability incidents were reported most often. There were less reports of cases related to integrity and confidentiality (e.g. intentional attacks). The reason behind that may be that discovering such incidents is more complicated and takes more time. Here follows a more detailed breakdown of the incidents:

- Availability 65%
- Availability and integrity 11%
- Integrity 9%
- Integrity and confidentiality 7%
- Confidentiality 3%
- Integrity, availability and confidentiality 3%
- Unspecified 2%

In their quarterly security incidents report to RIA, institutions are also expected to evaluate the criticality level of the occurred incidents. In 2013, this information existed in approximately half of all cases; in 66 cases, criticality was not evaluated.

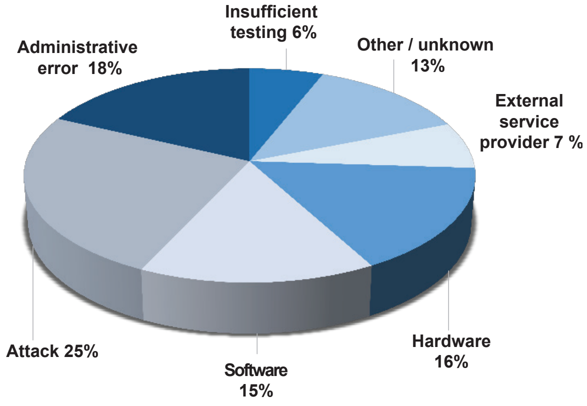
Incident criticality



At the same time, 116 of the 135 cases were realised incidents, meaning that they had direct impact on the operation of systems/services. The rest were either discovered weaknesses or there was not enough information in the report to draw conclusions.

As causes for the incidents, attacks and administrative errors were cited most often, followed by deficiencies in software and hardware.

Causes of incidents



Among the attacks, indirect and direct attacks can be discerned on the basis of the reports. Infections with a virus or malware causing considerable problems (e.g. mass forwarding of spam mail) were reported as indirect attacks. There were also cases of infection with a virus or malware with no impact or no discovered impact (or this was not specified in the report). The following were the most conspicuous directly identifiable incidents:

- deliberately caused denial of service attacks,
- isolated intrusions into information systems,
- isolated cases of overtaking server user accounts,
- isolated phishing e-mails.

Although communication with the cyber security managers of state institutions was constant and information about the most important incidents reached RIA even before the regulation, the regulation-based reporting system has significantly organised the system; it also provides an opportunity to pay more attention to the impact of an incident.

In short – reporting is off to a good start. This is good news for the cyber security service of RIA and provides an opportunity to analyse the security of state institutions on the basis of their own assessments, in addition to the monitoring data of the state network. Reports by the Ministry of Justice, the Ministry of Social Affairs and the Ministry of Foreign Affairs deserve special recognition. At the same time, the analysis of the causes and results of incidents is quite brief in several of the reports, although the mapping of information resources and assigning of security classes to them could be a good starting point for assessing the severity of an incident.

The risk management unit of RIA plans to pay special attention to insufficient analysis of cause and result in the reports in the future.

The Most Important Incidents and Issues of 2013 in Estonia

- A **large-scale malfunction** occurred in Elion in January, caused by a problem in the software of the central data storage device. Services of smartTV, mail, web hosting and hot.ee webmail were disrupted. The incident caused a lively discussion on backup methods and their redundancy in IT circles.

- It was discovered in January that the phone system of the Estonian Aviation Academy had been hacked in late 2012 and hundreds of long distance calls had been made. The incident was reported by Elion.

- In January, the Estonian Data Protection Inspectorate began supervision proceedings of the ticketing system of Tallinn's public transport system, assisted by the information security specialists of the State Information System Authority. The supervision proceedings, ended in May, found that there were insufficient grounds for the general 7-year storage term of the data set and that the security measures of storing personalised data (data hashing) was not sufficient.

- In early February, the webmail systems of Elion and Elisa as well as the users of a similar mail service of the Estonian University of Life Sciences were affected by a **phishing attack**. Users were directed to a fake website to enter their mail address and password in order to handle "security problems". A similar phishing attack was launched on the users of the mail service of the University of Tartu as well as the users of the education and research network EENet.

- In May, fake messages were spread among the Estonian users of Skype, containing links with the Skype username of the recipient and a text inviting the user to click (e.g. "this is a very nice photo of you http://some.place/string? id<username>". CERT-EE published information about domain names and IP address ranges to watch and block in order to avoid such attacks.

- In April 2013, RIA brought to public attention an issue that could have endangered a third of the computer users of Estonia a year later. Users of the popular operation system (OS) **Windows XP** were called upon to update their software or replace it with an operation system by another provider. In April 2014, Microsoft stopped supporting XP, meaning that the OS could no longer receive security updates, thus leaving users vulnerable to attack. The public information campaign proved successful. While **1/3 of Estonia's computer users** used XP to go online in April 2013, that proportion had decreased to approximately 1/5 a year later. The state portal eesti.ee was visited by users of computers running XP in 15% of cases in March-April, 2014. From the state network, an estimated 10% of computers connected to the Internet using XP in April, 2014.

- Foreseeing that e-voting in the local elections of 2013 would not pass without political attacks, RIA summoned an e-voting related open discussion group of specialists in April, with the participation of several experts interested in the security of e-voting as well as members of the National Electoral Committee in charge of the solutions and procedures of e-voting. The meeting gave the last impulse for the server code of e-voting to be published and the **subsequent security testing** by independent volunteer specialists to be carried out. The testers reported several minor deficiencies to the Electoral Committee, which were fixed before the elections. The general conclusion of specialists was that the system remains reliable and secure. This conclusion was not shaken by the political attack on e-voting launched in 2014, immediately before the European Parliament elections.

- In the spring of 2013, RIA received notices of several **attacks on the information systems of schools** using attack tools available on the Internet. System logs and social media posts directed law enforcement authorities to minors. In August, several schools had the problems of pornographic webpages being placed on their servers as well as pages distributing malware and selling pharmacies. Because of denial of service attacks, web police officials and CERT-EE visited schools and spoke of the serious consequences of cyber-hooliganism. Recommendations on this subject to school network administrators by Anto Veldre can be found in Õpetajate leht ("Teachers Newspaper").

- Like elsewhere in the world, some malware was carried into Estonia on the back of current affairs: after the April terror attacks at the **Boston Marathon** a wave of **mails** appeared promising fresh photos of the Boston explosions, but directing to infectious websites.

- In July, numerous people in Estonia **received a phone call from an English-speaking person who introduced himself as a representative of Microsoft**, encouraging non-suspecting computer users to download a program and/or disclose passwords that would enable the impostor to access the victim's computer and, through that, their bank account.

- In late August, considerable public attention was paid to a **theoretical vulnerability in the ID software (i.e. there were no signs of it having been exploited maliciously)**. A patch had already been issued for the vulnerability, and so there was more fuss about the topic than it actually deserved – after all, this was not the first or the last security update to ID software. As with every software, updates are performed regularly for ID software to ensure reliability and security. Instigating public panic would be understandable only in a situation where a large-scale use of the vulnerability was taking place, i.e. an attack which exploited an unpatched weakness of ID software. The same discussion raised the point that there is still no **forced update** mechanism in ID software, which gives an important role in patching the application to the user, who has to accept the offered software update onto his or her computer. Forced update, i.e. a situation where the software updates itself automatically, without intervention from the user, will be added to ID software in 2014.

- In August, a malware that infected the ilm.ee website received a great deal of attention from the public, and in October the website php.net, which is popular among web developers, was infected by the same malware. The reason for the ilm.ee incident was a backdoor in the ad-displaying software OpenX, which criminals used for infecting the site with malware.

- In October, local government elections were held. 21.2% of all voters participated in e-voting. Like before, e-voting was conducted without problem, although there was some traditional political propaganda against it from a party that in the past elections have gained only a small part of the e-votes.

- **In November, a data leak occurred in the services of the software giant Adobe**. The leak included password hashes and password hints making it easier to guess the user's password. Tens of thousands of users with mail addresses ending with the Estonian domain .ee were published on the Internet.

- In early November, simultaneously with the NATO exercise Steadfast Jazz, several websites in Estonia as well as elsewhere in Europe were attacked. The denial of service attack was announced in social media with the tag **#opindependence and Anonymous Ukraine; the case received much media attention**. No serious harm was inflicted on the information systems of Estonian public institutions or companies. A longer report on **#Opindependence is available here**.

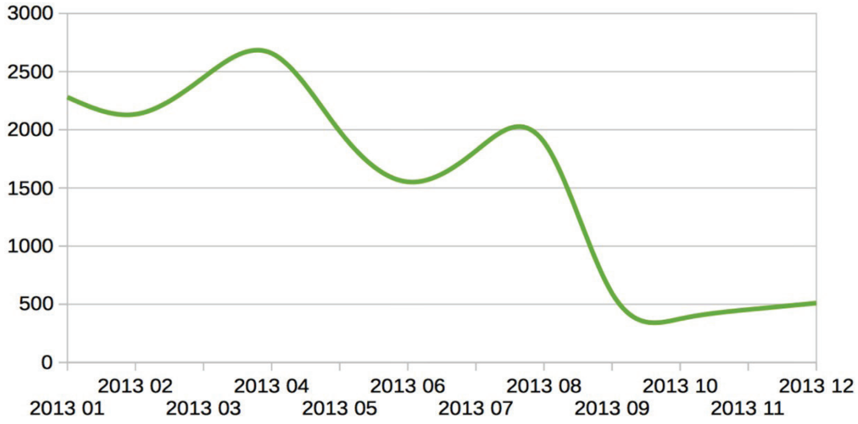
- In November, RIA together with several private companies launched the project NutiKaitse 2017 ("SmartDefence 2017"), the aim of which is to raise the security awareness and user skills of smart device users, developers and sellers, thus creating opportunities for secure software to be available in a simple and user-friendly manner.

- In autumn, several servers were broken into in Estonia in order to dig for bitcoins on the overtaken servers. In at least one case, the intrusion happened through a security hole in PHP5. This is a new and relatively easy way for cyber criminals to earn income by misusing server farms.

- **13 cases of denial of service attacks**, which are more visible than other incidents, were registered in Estonia in 2013, while **defacements** were much more numerous: **240 cases**.

- Signs of APT (Advanced Persistent Threat) have probably been identified by most Western governments, be it network scanning or deceitful scam mails that carry with them software that export the contents of the hard drive elsewhere. Like their colleagues abroad, Estonian law enforcement and security authorities take these cases seriously.

Malware Incidents in Estonia in 2013

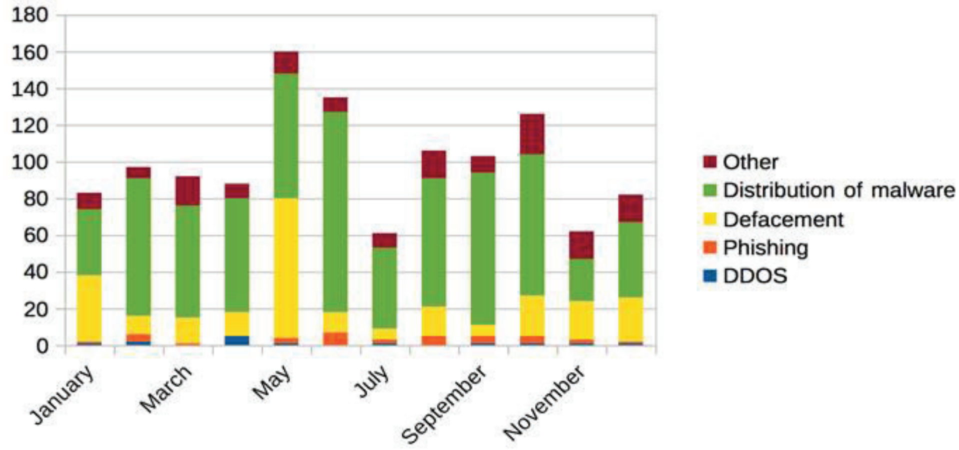


This graph shows statistics collected by CERT-EE about malware incidents (computers/webpages that participated in spam campaigns, denial of service attacks, distributed malware, etc.). The statistics are based on the data of several reputation services on the IP address range of Estonia.

The graph shows how many malware incidents per day took place in a month on average. This kind of automated statistics shows mostly infected or otherwise blacklisted (personal) computers / IP addresses. It must be kept in mind that the recorded events are probably not unique, because of, e.g. dynamic (changing) IP addresses and possible repetition of data from the partners. The repetition of data can occur as a result of the same incident being named differently as well as variations in the arrival times of the notifications. Therefore it is wrong to say, quoting automated statistics, that in December 2013, there were over 15,000 infected computers or webpages in Estonia, distributing malware (in the worst case), participating in spam campaigns or denial of service attacks, etc.

The considerable decrease in early autumn of 2013 in the number of incidents counted in this manner comes from changes in the counting system of reputation services: they stopped counting computers infected with Conficker. Conficker is a malware that, despite being discovered 5 years ago, no negative impact of it has yet been found.

Malware incidents reported to CERT-EE and registered by CERT-EE



The amount and share of malware, defacements, phishing and denial of service attacks were quite stable throughout the year. Only May stands out with a large number of defacements and June with a large number of incidents of distribution of malware. The defacements shown in the statistics for May actually occurred over a longer period and were included in the statistics as a result of a scanning performed on the basis of a one-time discovery. Considering the domain-based number, June could be the month of most defacements in 2013, as the server of a web hosting provider was broken into in June and the contents of 600 webpages was substituted for something else. The amount of malware distribution incidents in June is probably related to the typical earn-money-before-vacation behaviour of cyber criminals.

The Activities of RIA for Preventing Cyber-risks

Training. Last year, RIA organised 18 security-related training sessions financed by the EU structural funds program "Raising Public Awareness about the Information Society", with 497 people participating from state institutions, companies providing critical services, and local governments. Technical (e.g. Apache Web Server training, ipv6 workshop, IDS practical training), practical (practical application of ISKE) as well as general information-day type events were organised.

Penetration tests (pen-tests). RIA has organised and commissioned almost 50 penetration and vulnerability tests since 2012. RIA has often consulted partners on how to commission a penetration test and how to describe the initial task. Penetration tests are among the most efficient tools for ensuring the security of networks and systems, helping to discover vulnerabilities before malicious attackers. RIA also regularly scans Estonia's public networks and visits state institutions and local governments to test the security of their networks and consult them on same. In 2013, RIA's surveillance assessed the data security level of 20 town and rural municipalities; three state institutions were also audited together with the Data Protection Inspectorate. Compliance of the institutions' procedures and computer networks with ISKE requirements was checked. RIA also conducted a tender for evaluating the security level of the local governments service portal (KOVTP).

Exercises. At the international "Locked Shields 2013" cyber-exercise **organised by NATO Cooperative Cyber Defence Centre**, representatives of state authorities and companies practiced fending off cyber-attacks in real time in systems built for the exercise. The team of NATO was considered the best in the exercise; Estonia took second place. Estonia's team consisted of representatives of providers of critical services and of RIA. Valuable lessons were learned together about trusting third parties, the importance of web traffic and log analysis as well as teamwork.

RIA also contributed to the organising of the **NATO Cyber Coalition exercise** and participated as a player in the exercise testing the skills and information exchange of technicians from various countries. In 2013, this exercise for 30 states and 300 participants was conducted from Tartu.

In late 2013, the study **commissioned by RIA and compiled by Cybernetica AS** on the usage areas and life cycle of cryptographic algorithms was completed. The study makes several recommendations based on research and international reports on how to forestall possible cryptography-caused weaknesses in public institutions as well as the private sector. The study stressed the fact that within 2-5 years, several cryptographic solutions will have to be replaced in Estonia – the ones being used, for instance, in some banks, m-ID, digi-ID, but also in the ID cards issued before 2011.

The Most Important Changes in the Legislative Framework for Cyber Security

At the RIA conference "Cyber Security – a Need and an Opportunity", many critical service provider representatives expressed the opinion that more specific state regulations governing companies that provide vital services are needed for taking action in the case of large-scale cyber incidents and for considering the needs of the society. It was already in the same month that a Government regulation entered into force, specifying the operating conditions for e.g. power supply, the phone network and payment services.

The following are the most important legal acts and their amendments influencing cyber security:

- In 2013, RIA published the new **ISKE application guide and folders version 7.0** as a beta version. New additions include, for example, client systems running on Windows 7 and Mac OsX, Open LDAP, logging and web applications.
An analysis of the ISKE application tool was also completed in 2013, becoming the basis for several amendments in 2014. Measures of ID card and X-Road were added to ISKE in 2013. A major wave of ISKE auditing will reach state institutions again in 2014 and 2015.
On the recommendation of the heads of security of state institutions, RIA reconciled the base principles for availability calculations of ISKE and ITIL.

- On July 1, 2014, the **Law Enforcement Act Amendment and Application Act** started in 2013 comes into effect. According to these amendments, the surveillance competency of the Technical Surveillance Authority over communications networks and services will be transferred to RIA. The same legislation draft also stipulates RIA's surveillance competency in the Emergency Act and the Public Information Act.

- In 2013, the risk analysis "Large-scale Cyber Incident" was compiled on the initiative of RIA and with the participation of other concerned institutions, analysing the occurrence probability of an emergency and its consequences, and describing measures for forestalling emergencies as well as alleviating their consequences. The risk analysis is a prerequisite for further planning processes and for devising a plan for solving emergency situations.

- The regulation **"Information Security Management System"** obliges state authorities to pay systematic attention to information security issues, including the appointing of persons in charge of security, i.e. heads of information security. According to the regulation, the head of information security implements a routine for handling security incidents, informs RIA's department for handling information security incidents (CERT-EE) of serious security incidents and submits an aggregate three-month report of incidents to CERT-EE, as required by ISKE. In 2013, state institutions submitted a total of 43 aggregate reports to RIA.

- In March, Government issued **security requirements for electronic systems** that are needed for the functioning of critical services. The requirements specified, for example, conditions for the functioning of power supply, phone network and payment services.

- For many specialists in charge of cyber security in state institutions, 2013 was the year of updating the cyber security strategy. At the time of writing this report, the strategy is in the final stages of the official coordination route, and will be presented to the public in the autumn of 2014 at the latest.

Recommendations and Insight for 2014

Year after year, RIA is concerned by the large number of defacements taking place in Estonia's cyberspace. Most of these cases are caused by homepage software not being updated. We strongly recommend the owners of every homepage, especially those using content management systems by Wordpress or Joomla, to make sure their homepage is running the latest software. Defacements are not only embarrassing, but can also mean that malware is placed on the website and visitors' computers are infected.

We recommend all IT managers and heads of security in the public as well as private sector to acquaint themselves with the crypto-study published on RIA's homepage early this year and to review the crypto algorithms used in their institution or company accordingly.

RIA has continued with exercises, training and security tests in 2014. Because of the ending of the EU budgeting period, somewhat less training has been planned than in 2013: about 10 training sessions for 350 people. In addition to the traditional international exercises Locked Shields and NATO Cyber Coalition, 2014 will also see Cyber Coalition by the European Union Agency for Network and Information Security (ENISA).

In the beginning of the year, the Estonian Internet Foundation (EIF) along with accredited registrars started the DNSSEC service for the Estonian national domain .ee. RIA and EIF together also started informing domain owners about the EU structural funds programme “Raising Public Awareness about the Information Society”. The easiest way to protect your domain with the DNSSEC security extension is by using the help of your registrar or name server provider. An overview of the registrars offering the DNSSEC service to their clients can be found on the internet.ee homepage from the comparison table of accredited registrars of the .ee domain.

After the end of the support period for Windows XP, RIA is still drawing attention to risks caused by using computers with outdated software. In April 2014, a tenth of the computers visiting the Internet in the state network were running on the XP operation system; of the visitors of the state portal eesti.ee, 15% were using this outdated system. In the second half of the year, RIA will conduct another campaign explaining the need to update software and introducing free alternatives.

In the spring of 2014, the **Guide of Security Requirements for Datacenters** commissioned by RIA was completed. It is meant first and foremost as a guide for the designing, building and maintenance of server rooms and data centres that host the databases of public services and critical services of high availability requirements.

In Estonia, as elsewhere in the world, the spread of smart devices is continuing and, with it, the real time documenting of everyday life and the corresponding increase in data volumes. There is more and more data moving on the web, and consequently there are more and more issues whose integrity, availability and confidentiality is more or less important to consumers. By the end of the year, a detailed survey of the security behaviour of smart device users, commissioned by RIA within the framework of the NutiKaitse (SmartDefence) initiative, will be completed.

We hope to take an important and long-awaited step in the security of electronic identity in 2014 and start public fault management of the ID base software. RIA will also become the verifier of the technical solutions of m-ID. Transition to the new digital signature format .bdoc will continue, which will bring along compatibility with (future) digital signatures of the rest of Europe as well as digital signatures with a stronger cryptographic protection.