



REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Cyber Security in Estonia 2022





REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Cyber Security in Estonia 2022

Contents

6

Learning From Security Vulnerabilities Makes Us Stronger

Last year will go down in history as the year of security vulnerabilities, where in the race against time and criminals, we had to learn some painful lessons. However, all experiences are useful and must be shared, says **Gert Auväärt**, Director of the Cyber Security Branch of the Information System Authority (RIA).

8

The Situation in Cyberspace: A Year of Security Vulnerabilities

2021 will go down in the history of cybersecurity as a year of major security vulnerabilities. The largest of these was the vulnerability identified in the Log4j logging application, but there were also those that only affected the Estonian e-state.

14

How Did a Hacker Steal 300,000 Document Photos?

One of the most serious incidents last year was due to a security vulnerability in the service of RIA. The attacker downloaded nearly 300,000 document photos, but was caught a few days after the data theft was discovered.

16

Legacy Brought Bad Surprises

The access rights system of the state portal eesti.ee was a painful reminder that if the attitude towards data protection changes, so must the information system.

18

Patching Vulnerabilities Is Still a Problem

People tend to put off until tomorrow what they can do today. Last year, we saw all too often what happens when this principle is followed when fixing critical vulnerabilities.



20

Log4j Caused an IT Earthquake

In December, IT professionals had to respond to one of the biggest security vulnerabilities in recent years: the Log4j zero day vulnerability. The IT community witnessed a severe earthquake all over the world at the same time and started preparing for a devastating tsunami.

22

In 2021, There Were 50% More Denial-Of-Service Attacks Than Last Year

Last year, we registered 47 impactful denial-of-service attacks, which is twice as many as in 2020. Until the spring, ransom denial-of-service attacks targeted companies, but in the autumn, schools and learning environments became the victims.

24

Financial Fraud Has Become More Diverse

Last year, we received 20% more reports of fraud than the year before about incidents in which Estonian people and companies lost money. RIA only sees the tip of the iceberg, because victims of financial fraud turn primarily to the police.

28 Cannot Get Through the Gate Until the Gate is Open

Most of us follow simple principles to ensure our physical security, but many seem to think that digital assets are able to protect themselves, writes Oskar Gross, Head of the Cybercrime Unit of the Central Criminal Police.

30 Ransomware Attacks Rarely Have a Happy Ending

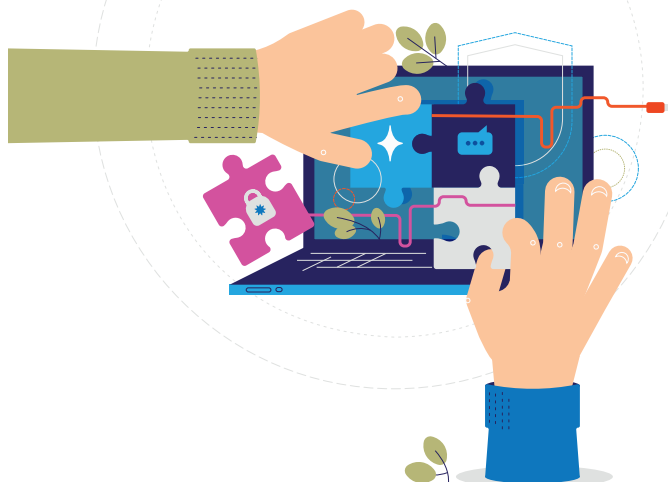
While heroes in Hollywood hostage films are usually able to escape, then in hostage-taking in cyberspace, where criminals gain access to corporate or personal information, the victim often has to choose between bad and very bad options.

32 What Did We Learn From the Local Elections?

Some functional errors caused public disapproval, but we did not identify any malicious activity that could have impacted the 2021 local elections.

34 Hackers, Help the State!

We are working on a model that would allow state agencies to work with hackers and pay them for information about security vulnerabilities.



36 What Happened in International Cyberspace in 2021?

Last year, news of cyber incidents and security reached even those who had not heard of these topics before. Many incidents directly and severely disrupted the daily lives of people and crossed the news threshold.

40 Potential Disasters Avoided

When it comes to cybersecurity, the focus is often on high-impact incidents and the damage they cause: be it stolen data, encrypted systems, or lost money. However, there are also incidents with a happy ending.

42 The Cyber Hygiene of the Estonian Population is Improving

The level of the cyber hygiene of the Estonian population has improved in three years, but there is room for improvement, according to data collected in cooperation with Statistics Estonia.

44 What Will 2022 Bring in Cyberspace?

Last year brought a lot of security vulnerabilities and a ransomware epidemic. What's in store this year?

Learning From Security Vulnerabilities Makes Us Stronger

Last year will go down in history as the year of security vulnerabilities, where in the race against time and criminals, we had to learn some painful lessons. However, all experiences are useful and must be shared, says **Gert Auväärt**, Director of the Cyber Security Branch of the Information System Authority (RIA).

My time in RIA started with big challenges. In July, two critical weaknesses were identified in our own systems that allowed access to users' personal data. In essence, you could say that even though the door was locked, the key had been left nearby.

A month later, we found out about possible vulnerabilities in other national e-services, as a result of which some personal data was not appropriately protected. Vulnerabilities in the real estate and marital property register were patched and according to our current knowledge, the data had not been misused in any way.

SECURITY COMES FROM COOPERATION

Both incidents with our services, the data leak of access rights in the self-service environment of eesti.ee for entrepreneurs and the illegal download of document photos (both cases will be discussed in more detail in this year-book) happened partly due to the fact that old system interfaces are still present in some ser-

vices and have not been renewed. We have carried out an internal analysis of these cases and streamlined the processes within RIA to avoid incidents like this in the future.

In both cases, we received the first indication that something may be wrong from people outside of our organisation. This illustrates that the state alone may not be able to find the weaknesses of a 20-year-old e-state and that security can be created in partnership with the community. It is very important that we all take security vulnerabilities seriously and patch them. We must share information because it allows us to learn from others and we must not ignore tips and suggestions. The consequences of the vulnerabilities depend on the speed with which we act – whether we are able to patch them before criminals manage to exploit them.

WARNINGS ARE NOT TAKEN SERIOUSLY

In March last year, when Microsoft disclosed its Exchange server vulnerability and provid-



GERT AUVÄÄRT

director of the Cyber Security Branch of RIA

ed information on how to patch it, we notified our partners and other authorities. However, a week later our monitoring revealed that two-thirds of those informed had not yet taken the necessary action. The e-mail servers of these organisations were still vulnerable, meaning that the mailboxes of the employees were essentially unprotected. The warning had not been taken seriously.

Unpatched systems usually result in criminals finding them and compromising them – installing malware, stealing data, etc. Cyber-crime is one of the most lucrative and thus the fastest growing types of crime in the world. However, catching those criminals is difficult, as it is easier to hide traces in cyberspace and the consequences of crime can appear after several years.

IT systems around the world are being attacked all the time, and the security vulnerabilities that have been discovered and made public can be of great benefit to those who are trying to get rich or gain influence. RIA regis-

ters more than 20,000 notifications and nearly 2,500 cyber incidents a year that have a real impact on the system or how it works. Although most attempts to attack fail, we must stay vigilant.

FOR A SAFER ESTONIA

Ransomware attacks, which are becoming more and more popular in the world, cause losses to entrepreneurs that are comparable to the budget of an average Estonian state agency. Estonia has not yet been successfully targeted with high-impact ransomware attacks, but it is only a matter of time as our daily lives, including the functioning of the country, depend on digital services.

Although the security of the systems is the responsibility of their owner, we must all play our part. Just as the state must protect its people who have entrusted their data to it, so must any other owner of a database or service. The digital society is based on trust.

In order to protect the reliability and security of our e-state, we have also increased our capabilities in RIA, both in terms of people as well as our tools and infrastructure. We put together a team of testers, developed a bug bounty programme to detect and patch service vulnerabilities, and increased the security of the state network.

In order to create and maintain security, we have taken another important step in RIA: the Estonian Information Security Standard (E-ITS) is finally ready. This is the most important guide for companies to prevent potential risks. At the end of 2021, the first pilot group started its work, the main role of which is to develop best practices in the implementation of the standard and to prepare new E-ITS experience consultants. Together with the University of Tartu, the initial E-ITS-based maturity model was completed, which gives organisations a quick assessment of their information security situation and allows authorities to compare the level of information security.

That is how we are building a safer Estonia step by step. ●



The Situation in Cyberspace: A Year of Security Vulnerabilities

2021 will go down in the history of cybersecurity as a year of major security vulnerabilities. The largest of these was the vulnerability identified in the Log4j logging application, but there were also those that only affected the Estonian e-state.



There are security vulnerabilities in almost every system and in every code – you just have to search for them. Most of them are identified and addressed quickly. It is a common practice in information security communities that the person who discovers a security vulnerability notifies the owner of the system or service first. They give enough time to develop security patches or code updates, and only then reveal the vulnerability to the rest of the world.

This was not the case with the major security vulnerabilities discovered in 2021. Serious security vulnerabilities have impacted the society before, but in 2021, there seemed to be no end to them.

IF YOU DO NOT KNOW YET THAT YOU ARE VULNERABLE

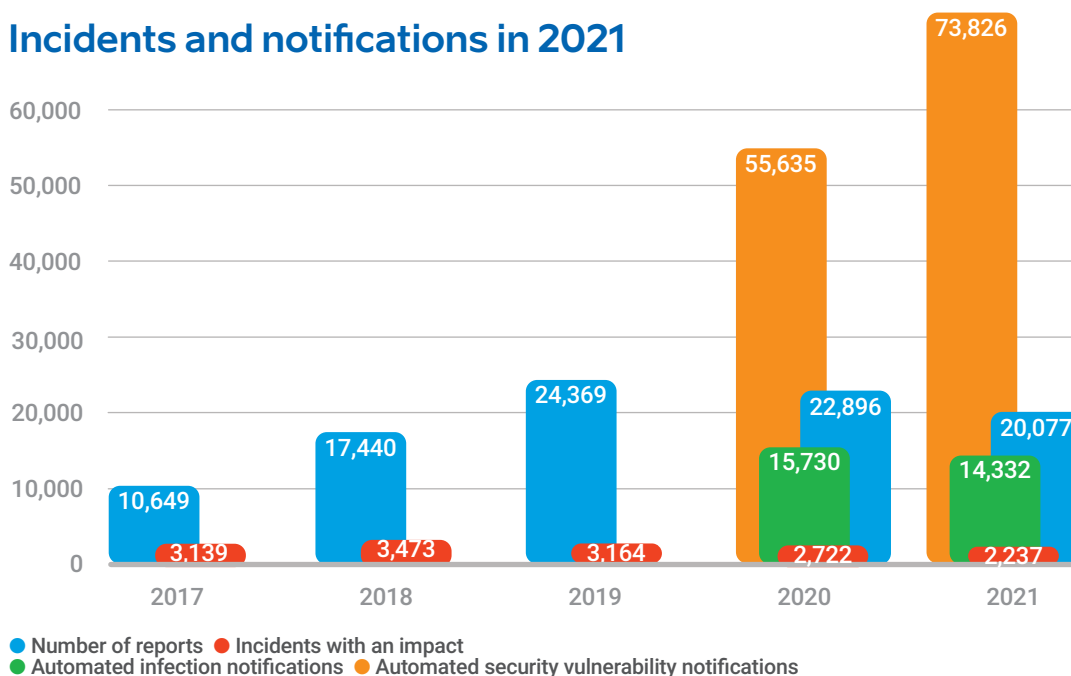
In 2021, the Estonian society was probably most affected by the news that an attacker found a security vulnerability in the system managed by the Information System Authority (RIA) and obtained document photos of hundreds of thousands of people (you can read more about this attack on page 14).

Serious security vulnerabilities have impacted the society before, but in 2021, there seemed to be no end to them.

Although the vulnerability only gave the attacker access to document photos – with which one can do almost nothing in the age of digital documents – it raised legitimate concerns about whether the Estonian e-state can keep data secure and protect it from thieves. However, the course of the incident proved that the principle of data separation we use in our e-state is correct. Every query for a document photo left a trace, which allowed the police to detain the attacker and he was not able to obtain any other data.

By security vulnerabilities, we also mean configuration errors. One of these was discovered by an observant citizen in the self-service

Incidents and notifications in 2021



environment of eesti.ee for entrepreneurs, where the first and last names, personal identification codes, places of work, and, in some cases, connections with previous positions of more than 300,000 people related to legal entities were visible. The system was originally designed so that authorised persons could see the data of other authorised persons and it had not been updated over the years. We are extremely grateful that the case was reported to us: we were able to fix the bug before the general public or a malicious attacker had the opportunity to view or misuse third-party data.

A security vulnerability that is so new that only an attacker knows about it and the owner of the service has not even had a day to fix it is called a zero-day vulnerability. However, if an update to a vulnerable service already exists, it is a whole other story. Unfortunately, owners of larger networks and e-services often do not have a detailed overview of all their online services and their vulnerabilities. The owners should look at their IT infrastructure through the eyes of an attacker, as they are constantly looking for security flaws.

At the end of 2020, the Ministry of Economic Affairs and Communications, the Ministry of

Social Affairs, and the Ministry of Foreign Affairs were attacked, and we saw attacks with similar handwriting also in 2021. What is common for all of them is that the attacker scanned web servers with publicly available tools, found security vulnerabilities, uploaded malicious code, and thus gained unauthorised access to the servers.

In February, we were informed that a company which provides cloud services and software to many public sector authorities (ministries and local governments) and another company which provides remote access services to public sector authorities had been compromised. Both of them handled the incidents professionally: they fixed their services, informed customers, and worked in full cooperation with CERT-EE.

IF THE WHOLE WORLD KNOWS YOU ARE VULNERABLE

The public will only hear about the consequences of some security vulnerabilities much later, as their effects may become apparent in a matter of months. In March, Microsoft disclosed four zero-day vulnerabilities in its mail server software that allowed attackers extensive access to the entire server, including e-mails and passwords. According to Microsoft, the attackers

quickly built tools that began searching the entire world for vulnerable Exchange servers that had not been updated and once they found them, the servers were compromised and infected with malware.

At the end of August, Atlassian announced that their world-wide wiki platform Confluence also had a critical security vulnerability that required a software update. Confluence is commonly used for business process documentation or internal web sites. By early September, attackers had already been able to exploit the vulnerability and use automated systems to gain access to Confluence servers exposed to Internet around the world, including in Estonia (see page 18 for more information).

The security vulnerability with the greatest impact was only revealed at the end of the year, when players on the popular Minecraft gaming platform began experimenting with a newly discovered security vulnerability that allowed them to send commands to the game server. The critical security vulnerability Log4Shell identified in the Log4j logging function of the Java programming language, which is used in billions of devices and software products around the world, had already been patched by

The owners should look
at their IT infrastructure
through the eyes of
an attacker, as they are
constantly looking for
security flaws.

the manufacturer, but these same devices and the software used in them had not been updated yet.

As news of the vulnerability spread, IT professionals, developers, and security professionals around the world rushed to update the Log4j function in their own software and then wait for software updates for all their other products — industrial devices, network devices, antivirus



Log4j vulnerability – what is it?

The critical security vulnerability Log4Shell was identified in the Log4j function of the Java programming language used in billions of devices and software products around the world. The severity of the security vulnerability is rated the highest possible by the international CVE standard (10 out of 10 points), potentially allowing an attacker to run their code freely on a vulnerable device.

An attacker could exploit the vulnerability by sending a command in a specific format to a vulnerable server, device, or system (beginning with '\$ {jndi:}') and adding a reference to malware that may be located on a third-party server. The vulnerable server logs the command, Log4j searches for the uploaded malware, downloads it, and runs it. Depending on the nature of the malware, it may give a third party access to the device.

software, web services, and more. This was also the case in Estonia, as many Estonian e-services use the hugely popular Java programming language as well as the Log4j function.

The general public may not have noticed this, but the combined effort of the global IT community to identify the extent of the vulnerability and to support each other was impressive. IT professionals did not mind national borders, open-source or commercial services and occasionally they even forgot their sleep and loved ones. However, we will most likely see the full impact of the Log4j vulnerability only later, when it becomes clear how much the attackers managed to exploit the vulnerability before it was patched.

IT ALL STARTS WITH ACCESS: RANSOMWARE AND OTHER INCIDENTS

Ransomware attacks received a lot of attention around the world this year – and for good reason. The attack on Colonial Pipeline, a U.S. fuel

Incidents with an impact in 2021

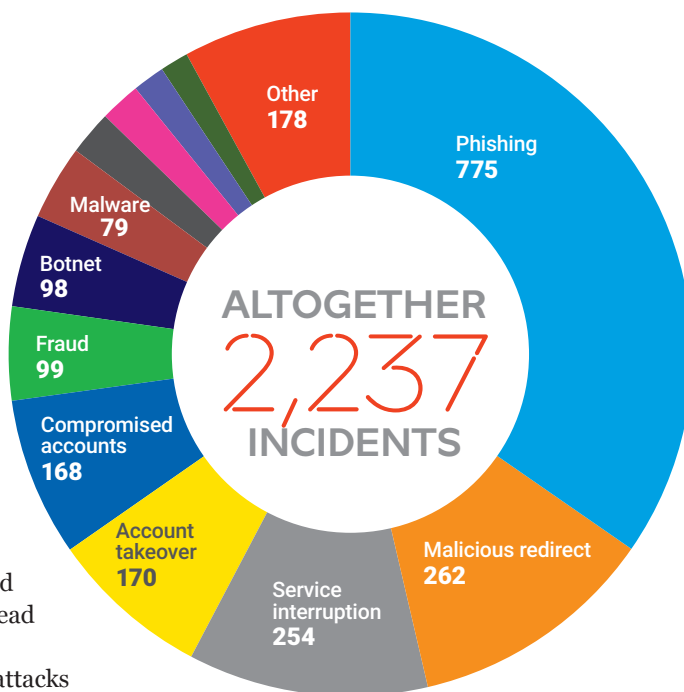
- Denial-of-service attack 47
- Data leak 43
- SEO spam 34
- Ransomware 30

supplier, made headlines, halting fuel supplies to the U.S. East Coast, but multi-milliondollar ransom demands and encrypted IT systems caused widespread problems in many countries.

The most expensive ransomware attacks usually target companies operating in the United States or in the wider English-speaking business environment. In Estonia, ransomware incidents involve smaller enterprises, and the demands are usually in the range from a few thousand euros to tens of thousands of euros. We were informed of a total of 30 ransomware incidents in 2021 (33 in 2020). It seems that the small size of Estonia and our language environment works in our favour, as does the steadily improving cyber hygiene.

Cyber hygiene and compliance with standards are relatively effective against ransomware attacks. In 2021, attackers accessed the systems of their victims mostly through a remote desktop application (Remote Desktop Protocol or RDP in Windows). Some versions have publicly known security vulnerabilities, and in some cases, passwords that are still in use can be found in leaked password databases.

IT companies providing services to third parties should pay special attention to the prevention of potential ransomware attacks. In April, we learned of a case where a ransomware attack targeted an IT service company, through which it spread to four more companies. In May, there was an attempt to launch a ransomware attack against a local government which had been accessed through an accounting service provider that had been compromised.



On many occasions, CERT-EE specialists have been able to help recover data that is encrypted with ransomware without the victims having to pay the ransom. Sometimes, ransomware has left much of the data available (for example, it encrypts only the beginning or the end of the files); other times, decryptors can be found to recover the data. In case of a ransomware incident, we encourage companies to contact CERT-EE and to always keep in mind that paying the ransom only motivates the criminals to launch further attacks.

WHAT HAPPENED TO THE YEAR OF PHISHING?

We called 2020 the year of phishing in the last yearbook – the number of phishing sites had increased by a fifth, and phishing was often a means by which attackers could learn the passwords of an employee of an organisation.

Phishing attacks continued in 2021. The number of phishing site incidents increased both in percentage (35% of all incidents with an impact compared to 26% a year earlier) and in overall numbers (755 in 2021 and 711 in 2020, respectively). These figures reflect how many times phishing sites have been taken down at the request of CERT-EE specialists; the numbers of notifications are much higher.

Similarly to the year before, the sites can be broadly divided into two: bank account phishing and account credentials phishing. The phishing sites are usually almost identical with the originals, but the address is different. In the case of bank account phishing, the victim unknowingly sends money to the wrong account, and the passwords entered on the account credentials phishing sites are most often used to break into e-mail accounts. As a rule, using multi-factor authentication helps to protect your account even if you have accidentally entered your password on a phishing site.

Bank account phishing attacks that have targeted Estonians for several years are already familiar to us. It seems more profitable for the criminals to call victims and persuade them to send money. In terms of account details, however, it does not look like the phishing attacks will cease any time soon.

BOTNETS ENABLE NEW DENIAL-OF-SERVICE ATTACKS

The unpleasant surprise of 2021 was the high impact of distributed denial-of-service (DDoS) attacks. The overall figures also show an increase: compared to 2020, the number of major DDoS attacks increased from 32 to 47 (these are the attacks that were reported to CERT-EE). We have also gained better visibility of smaller DDoS attacks since the summer of 2020, which also shows a clear upward trend.

In 2021, we saw several waves of DDoS attacks with a significant impact. In January and February, several banks and technology companies operating in Estonia received DDoS attacks accompanied by extortion letters. Similar attacks had been carried out on the same companies three months earlier, and the threatening letters referred to previous attacks, saying 'we have not received your payment', 'we are back now, pay off', and 'if you do not pay us now, we will be back soon'. Similar attacks took place in other European countries (at least in five Member States according to CERT-EU) and beyond.

We also saw the first attack on a school in Tallinn in January, which briefly disrupted the work of educational institutions throughout the city. This became a trend in spring and autumn. Since

September, we have seen continuous short-term attacks on general education schools, vocational training institutions, universities, as well as the e-learning environments managed by the Education and Youth Board.

The attacks are often ordered by schoolchildren from relatively accessible online forums. In such places, DDoS attacks are offered as a service: an attacker has amassed a large number of routers and other IoT devices with security vulnerabilities or poor configuration on the botnet and is using it to launch DDoS attacks for a small sum of money.

However, these attacks affect not only the infrastructure of that school, but also other authorities that use the same name servers, for example.


It seems that the small
size of Estonia and our
language environment
works in our favour,
as does the steadily
improving cyber hygiene.

In one of the denial-of-service attacks in May, we identified a router with a security vulnerability in Estonia that was connected to a botnet and participated in an attack on a vocational educational institution. We informed the owner of the router, and at least this device can no longer be used for a DDoS attack. Read more about denial-of-service attacks on page 22.

This incident also shows that security vulnerabilities, out-of-date software, and configuration errors enable attacks that have a major impact on our daily lives. Therefore, it is extremely important for device and system owners to pay full attention to security patches and security vulnerability notifications (including the daily notifications of CERT-EE). This way, you can trust that your router, smart TV, or fridge does not give attackers a chance to disrupt Estonian life. ●

How Did a Hacker Steal 300,000 Document Photos?

One of the most serious incidents last year was due to a security vulnerability in the service of the Information System Authority (RIA). The attacker downloaded nearly 300,000 document photos, but was caught a few days after the data theft was discovered.

 On 21 July, CERT-EE detected that 286,438 document photos had been illegally downloaded from the database of identity documents. They had been downloaded en masse from 9,000 Estonian and foreign IP addresses since 12 July. This was caused by a security vulnerability in the photo transfer service (so-called photo

service) that is used when a person wants to download their document photo.

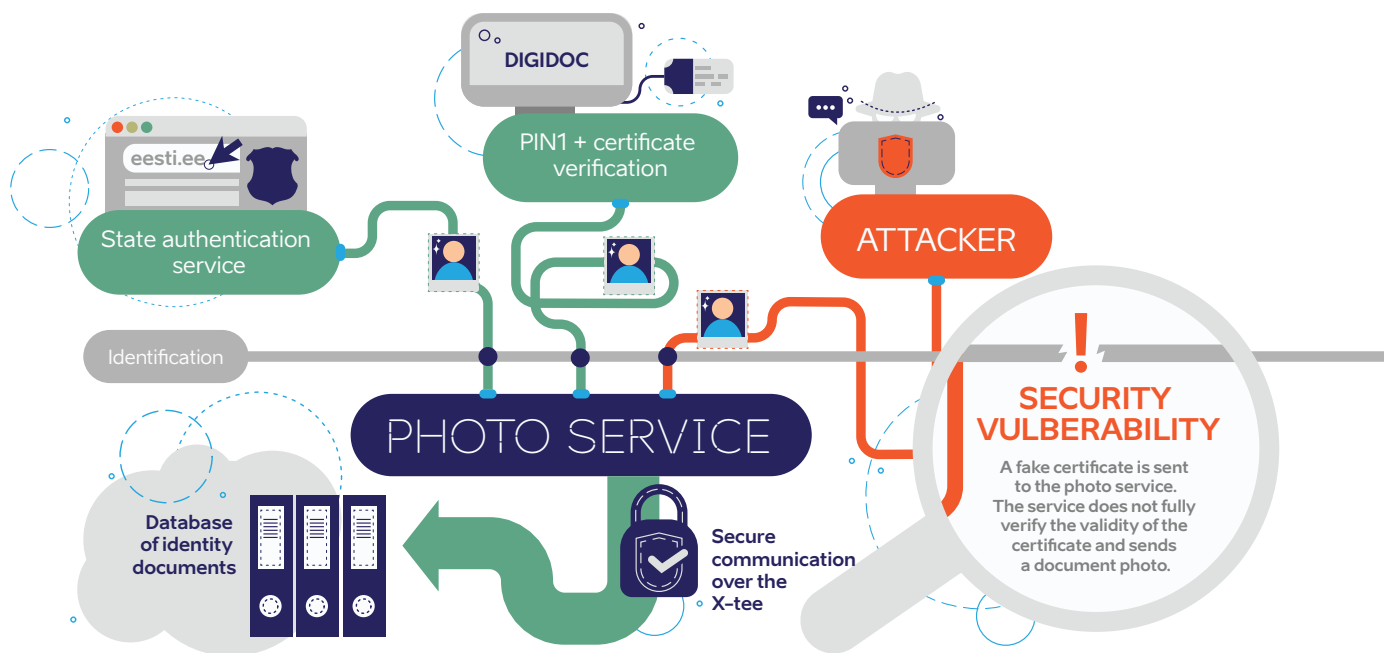
You can download your document photo either directly from the state portal or through the DigiDoc application. In both cases, the person must first authenticate themselves. Once the request has been made, the system requests the photo from the service that mediates it, the so-called photo service, which is managed by RIA. The photo service requests the photo over the X-tee from the database of identity documents, which belongs to the Police and Border Guard Board, and sends it back to the person. Upon detection of the attack, RIA temporarily closed this function for DigiDoc.

Lessons from the photo theft

RIA analysed and improved its workflows to prevent future incidents caused by such security vulnerabilities. In addition, the case inspired us to create a national bug bounty programme to motivate good hackers. This means that in the future, hackers who have discovered security vulnerabilities in state systems may receive a reward from the state. However, the reward is only paid if the hacker follows the established rules and conditions. The rewards programme is currently being worked on.

HOW WAS THE ATTACKER ABLE TO DOWNLOAD THE PHOTOS?

DigiDoc makes requests over a public URL. By manipulating this, the attacker managed to give the photo service the impression that the request comes from an authenticated user who wants to download their document photo. However, behind the request was an attacker



who turned directly to the photo service using forged or self-created certificates (see figure). To create a fake certificate, the attacker had to have the personal identification code and name of the person.

The photo service should have recognised that the certificates used by the attacker were not issued by SK ID Solutions – that they were forged. Although the attacker had marked SK ID Solutions as the issuer of the fake certificates, ‘looking in’ them would have shown that they actually came from elsewhere. Due to the security vulnerability, the service did not do this.

As a result of the attack, the criminal did not have access to the database of identity documents, but managed to download document photos from it. A few days after the discovery, the security vulnerability was patched and RIA reopened the photo service for DigiDoc so that people could download their document photos again.

WHAT CAUSED THIS SECURITY VULNERABILITY?

Reportedly, the security vulnerability in the photo transfer service occurred in November 2018. The interruption of the service was probably related to the exchange of ID-card certificates – changes were made in the information systems to support authentication with new certificates.

CERT-EE analysed logs starting from 30 June 2018 and found no other anomalies. This leads to the conclusion that the security vulnerability of the photo transfer service had not been abused before (i.e. before July 2021).

The police detained the suspect a few days after the incident was discovered and confiscated the downloaded data. Preliminary information suggested that the photos were simply stored on the computer of the attacker. The proceedings conducted by the Office of the Prosecutor General are still ongoing.

The police detained the suspect a few days after the incident was discovered and confiscated the downloaded data.

It is not common for attackers behind cyber incidents to be caught so quickly. They are often located abroad and their traces are difficult – if not impossible – to detect. In this case, we managed to do so thanks to quick and efficient cooperation between the police, CERT-EE, and the Prosecutor’s Office. ●

Legacy Brought Bad Surprises

Last summer, we got a painful reminder that if the attitude towards data protection changes, so must the information system.

On 6 July, an entrepreneur informed us that on the website for entrepreneurs on the state portal eesti.ee, a database with 336,733 data rows is available to users authenticated in the self-service environment of the access rights management system (AAR). The first and last names, personal identification codes, places of work, and, in some cases, connections with previous positions and roles (e.g. job title, start and end date of employment) of people were visible. The database contained persons from both the public and private sectors.

This data was visible to the people appointed to represent the authority or company, i.e. to all those for whom there was a row in the same database. All data rows became visible when somebody performed a so-called empty or parameterless search. The person also saw the

data of others when, for example, they searched for 'Paul' – in which case they were shown all the people called Paul in the database.

It was not a classic cyber incident – the system was not attacked or broken. However, that information should not have been visible in that way. So what happened?

THE SYSTEM BECAME OUTDATED

The entire administration system for access rights – including its self-service environment on the state portal – was designed and built so that all data is visible to all people in the database. The world around this system has changed, especially the approach to data protection. Thus, the structure of the system became inappropriate.

It was clear we had to change it. In July, the Information System Authority (RIA) closed the self-service environment of the access rights system on the state portal. Now, the RIA helpdesk must be contacted at help@ria.ee to change roles and grant accesses. Before, customers themselves could provide access quickly and directly. Now, however, it has become a little more inconvenient. It takes more time and effort to create an authorisation, digitally sign it, send it to RIA, and receive a response.

We did not consider it appropriate to contribute to the thorough development of the old system to reopen the self-service environment

What is the AAR?

The AAR, or administration system for access rights, is a system for authorised persons of an authority or a company in which they can provide others access to various services. For example, the head of a company can grant rights to an accountant to transfer employee data to the employment register maintained by the Tax and Customs Board.



there. One important argument was that RIA is already developing a new administration system for access rights, Pääsuke. Another important argument was that changing old systems, or so-called legacy systems, may not be as easy as one might think.

A WIDER PROBLEM

Legacy is a system, technology, or software that is still running but is actually outdated and becoming more and more vulnerable over time. Legacy is a problem in many long-established companies and authorities. For example, the current owners of a system developed 10 years ago may not have a full understanding of its structure and functions. Organisations change over time, people are replaced, and often, the solutions put in place are not properly documented for the new employees. Therefore, it is often not known exactly what effect an upgrade of one part may have on another part of the system.

The state is contributing to the solution of the problem with legacy systems

An additional 14.4 million euros was allocated from the state budget in 2022 for the updating and maintenance of outdated information systems and platforms. In addition, the government allocated 500,000 euros from the reserve fund for additional investments for the rapid updating and, if necessary, closure of the outdated information systems of the state portal eesti.ee.

Outdated systems are used in both the public and private sectors. This is understandable in many ways – replacing the legacy is costly and time-consuming and can also lead to a change in the usual functionalities. So what can you do? The first step could be to get to know the legacy systems of your organisation. This gives you an idea of the state of the system, what features it offers, as well as its vulnerabilities and crossdependencies.

So what can you do?
The first step could be to get to know the legacy systems of your organisation.

This is exactly what RIA has done. We have become even more familiar with our legacy and set up processes so that our systems are updated at all times. ●

Patching Vulnerabilities Is Still a Problem

People tend to put off until tomorrow what they can do today. Last year, we saw all too often what happens when this principle is followed when fixing critical vulnerabilities.

On 2 March 2021, Microsoft announced that the popular e-mail server software Exchange Server had four zero-day vulnerabilities that could allow an attacker to install malware on the server of the victim and gain access to their e-mail, contacts, passwords, and administrator privileges. In the same announcement, Microsoft also released security patches and asked users to install them as soon as possible.

Until that point, few people knew about the vulnerabilities (according to Microsoft, they were used for attacks by the Chinese cyber group HAFNIUM), but from 2 March, the information was available to everyone. This marked

the start of the race against time – between the attackers who used automated tools to search for and attack vulnerable mail servers and the server owners and administrators who now had the means to patch the ability.

THE MAÑANA ATTITUDE DOES NOT HELP

In many cases, the attackers won. On 3 March, Microsoft announced that there were ‘a limited number of victims’. On 8 March, however, there were more than 60,000. The day after the vulnerabilities were disclosed, CERT-EE identified more than 80 mail servers with the mentioned vulnerabilities in the Estonian cyberspace. We informed their owners and administrators, as well as public sector security managers and vital and important service providers. When we repeated the monitoring on 10 March, we unfortunately discovered that two-thirds of these servers were still using unpatched software and were therefore vulnerable to attacks. While three-quarters of the vulnerable servers were patched worldwide in a week, only a third were patched in Estonia.

Therefore, we were not surprised by reports of compromised mail servers. The criminals managed to attack local governments and pri-

Speed matters

There is nothing new about critical security vulnerabilities in software, but the pace at which cyber groups and individual criminals detect and compromise unpatched systems is unprecedented. It used to take weeks, but now, it only takes days or hours. Those responsible for cyber security must keep pace and patch dangerous security vulnerabilities as soon as possible, rather than postponing them.

Record number of vulnerabilities

- ❖ The National Vulnerability Database (NVD) of the US National Institute of Standards and Technology (NIST) recorded 20,046 vulnerabilities in 2021 (18,351 in 2020, 17,382 in 2019, and 17,252 in 2018).
- ❖ Attackers did not need good technical skills to take advantage of 90 per cent of these vulnerabilities.
- ❖ For 61 per cent of the vulnerabilities, carrying out an attack did not require any action on the part of the victim: clicking on a link, sharing passwords, launching software, or the like.

vate companies, as well as the medical sector and educational institutions.

DIFFERENT SOFTWARE, THE SAME SCHEME

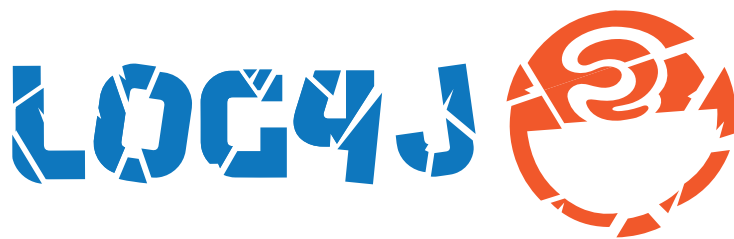
A similar sequence unfolded in late August and early September. On 25 August, Atlassian, the maker of the wiki platform, announced that their Confluence software contained a critical vulnerability that could allow remote code execution. The security vulnerability allowed an unauthenticated user to compromise the Confluence server of an enterprise or authority and edit, add, delete, and/or copy data there. In addition, it allowed malicious code to be installed on the systems of the victim to mine cryptocurrency or create a backdoor to carry out new attacks. Atlassian rated the threat severity of these vulnerabilities with 9.8 on a ten-point scale.

Confluence is not as common as Microsoft Exchange, but it is also used by many Estonian state agencies and private companies as an intranet platform.

In September, we learned that three state agencies had been attacked through this security vulnerability. Early detection of the attackers allowed the agencies to avoid major damage, but these attacks would have been preventable if the software had been updated in time. ●

The criminals managed to attack local governments and private companies, as well as the medical sector and educational institutions.





Log4j Caused an IT Earthquake

On 9 December, IT professionals had to respond to one of the biggest security vulnerabilities in recent years: the **Log4j zero day vulnerability**. The IT community witnessed a severe earthquake all over the world at the same time and started preparing for a devastating tsunami.

Java is one of the most widely used software development platforms. Its open source logging framework Log4j is very common – billions of computers use it to keep apps and services running. The function is used by Apple, Steam, Twitter, Amazon, Tesla, IBM, Minecraft, LinkedIn, and thousands of other well-known and lesser-known companies.

WHAT IS THE LOG4J FUNCTION?

Each software logs or stores data in one way or another to have an overview of what is going on with the software. This is necessary for three reasons: to keep the software running, for development, and for ensuring security. Logging or storing data is essential.

Logging can be compared to a smart camera on the main street and square in a city. It gives the city authorities the opportunity to check whether the Christmas tree is still standing, whether the streets are covered in snow, or whether city services are working as they should. In addition, it helps to analyse how people behave there: whether they use the existing

sidewalks and crosswalks or crossing the streets in wrong places. If there is an accident in the area, the police can find out the circumstances of the accident by looking at the recording. This is essentially how logging works.

However, if a vulnerability of the camera allows the information systems and databases of the city government to be taken over, the situation is equivalent to the critical vulnerability of Log4j, which gives criminals power not only over this particular function (camera) but the entire infrastructure.

HOW IS THE SECURITY VULNERABILITY EXPLOITED?

Although a tsunami was expected after the weakness became apparent and people started getting ready to board Noah's Ark, the end of the IT world has not yet come. The impact of the vulnerability may not become apparent for years to come. At this time, we do not know if and where the attackers intruded before the security updates were installed.

Attackers could exploit the vulnerability by

sending a message in a specific format and an additional reference to malware located somewhere on the third server to a vulnerable server, device, or system that could be accessed from the Internet. The vulnerable server read the command from the message, Log4j searched for the malware, downloaded it, and ran it. It was as if a person were knocking themselves out. Depending on the nature of the malware, it may give a third party access to the device.

The security vulnerability primarily affects companies and authorities, as it is potentially possible to gain access to their systems. Once it is exploited by criminals and they are able to install malware on popular services, it will also affect end users.

As at the end of 2021, there has been no mass exploitation of the Log4j vulnerability in Estonia or in the world, but as we wrote, its impact could still be revealed. Criminals are currently actively monitoring online services to find systems that have not been addressed. Vulnerable devices are also being searched for in Estonia.

WHAT SHOULD I DO?

First, inspect services built on the Java platform that are part of your service portfolio. Check for updates to the products you use. If there are updates, install them as soon as possible because they address a critical security vulnerability. This is especially important for systems that are available online.

However, this does not mean you are safe. On 28 December, a smaller vulnerability was discovered in the next version of Log4j. IT professionals need to keep a close eye on what is going on with this vulnerability and be prepared that the update needs to be updated as well. It should also be borne in mind that a security patch has not yet been developed for all services. The vulnerability may never materialise if the vulnerable service is not open to the Internet or devices are prevented from accessing the Internet.

What did RIA do?

- On 10 December, we informed the Estonian public about the security vulnerability and its impact.
- On 13 and 19 December, we sent additional information about the security vulnerability to the public sector and vital service providers.
- On 22 December, we published a post on the RIA blog focusing on the security vulnerability.
- We identified RIA services that are affected by the vulnerability. We installed updates or countermeasures.
- CERT-EE monitors what is happening in Estonian cyberspace 24/7 and searches for attack attempts.

SITUATION IN ESTONIA

In the days following the disclosure of the security vulnerability, CERT-EE identified Estonian companies and authorities that were at risk due to the vulnerability and asked to update or close the respective services. CERT-EE will continue to look for new cases, as not all service users have yet patched the vulnerability. In addition, there is not a security patch for all services yet.

RIA has not received reports of attacks with serious consequences resulting from the Log4j vulnerability. However, malware has been installed in Estonia on computers through the vulnerability, which mines cryptocurrency. Because this malware slows down services, these cryptocurrency miners are quickly found and removed.

There have been reports abroad that attempts have been made to prepare for ransomware attacks through the vulnerability. If criminals have launched malware on a system that is difficult to detect right away, data leaks can occur much later. ●

First, inspect services built on the Java platform that are part of your service portfolio.

In 2021, There Were 50% More DDoS Attacks Than Last Year

Last year, we registered 47 distributed denial-of-service attacks (DDoS), which is 50% more than last year as in 2020. Until the spring, ransom denial-of-service attacks targeted companies, but in the autumn, schools and learning environments became the victims.

One cold afternoon in February, a threatening e-mail was sent to a commercial bank operating in Estonia. Transfer two Bitcoins (worth nearly 56,000 euros at the time) to the account specified on the e-mail, or we will launch a massive denial-of-service attack against your business. The bank had received a similar e-mail and undergone a so-called sample attack four months prior.

Usually, the victim is given more time to react. This time, however, the attack started ten minutes later. At one point, neither Internet banking, card payments, nor the internal services of the bank were available. Although the attack lasted with varying intensity until the evening of the same day, and its effects were felt by both the customers and employees of the bank, the protection measures helped to prevent the worst.

RANSOM DDOS ATTACKS ENDED

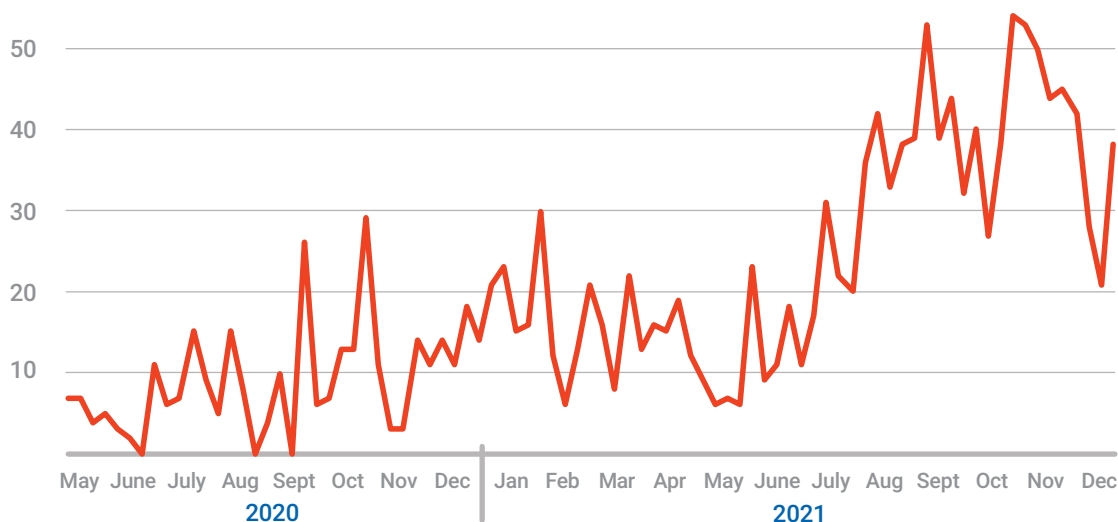
Such ransom denial-of-service attacks returned to Estonian cyberspace in the autumn of 2020 and continued in the beginning of 2021. The targets were a number of companies in the technology and financial sectors that have a lot to lose from the disruption of e-services, but which also have above-average levels of cyber security.

The victims who were attacked in the autumn were attacked again a few months later. The attacks were mostly based on intimidation, but there were exceptions. For example, a blackmailer who organised a denial-of-service attack wro-

To prevent safe-looking devices from becoming a dangerous tool in the hands of cybercriminals, always make sure to update their software.

The number of DDoS attacks is growing

From the summer of 2020, we also collect automatic notifications of denial-of-service attacks without a significant impact, which are clearly on the rise.



te that they needed money for their daughter's surgery and had ran out of other ideas to earn the money they needed.

The methods, scale, and impact of the attacks varied, but the victims were united by the decision not to submit to extortion. The fact that the business plan of the criminals did not work was probably the reason why ransom denial-of-service attacks almost disappeared after the first quarter.

ATTACKS ON SCHOOLS

They were replaced by a new problem: attacks on schools and the Tahvel and Moodle learning information systems. These attackers were not motivated by the desire to get rich – as far as we know, there have been no attacks on educational institutions that involved a financial demand. Instead, we suspect that students in the same school who had not prepared for a test or did not want to go to school were behind the attacks. The attacks on schools or learning information systems usually took place during school hours. They disappeared during weekends and school breaks, and returned when school began again.

In September, we received reports of denial-of-service attacks on schools or learning environ-

ments almost every day. Some of them did not have a significant impact, but some of the attacks disrupted the daily work of the schools: it was not possible to add or view lesson plans, grades, absences, teaching materials, and take tests. There were also attacks that affected other authorities that used the same network or name servers in addition to the target school.

A young person might think that by ordering an attack on their school, they could avoid taking a test or could skip school without anyone noticing. An adult, however, knows that this is not the case.

DEVICES LOCATED IN ESTONIA ARE ALSO USED FOR ATTACKS

In most cases, foreign devices are used in denial-of-service attacks against our e-services, but when analysing incidents, we have also found Estonian IP addresses. Their owners may not be aware that their router, printer, or security camera is infected with malware, is connected into a botnet, and attempts to 'take down' their home bank or the school of their children. To prevent safe-looking devices from becoming a dangerous tool in the hands of cybercriminals, always make sure to update their software. ●

Financial Fraud Has Become More Diverse

Last year, we received 20% more reports of fraud than the year before about incidents in which Estonian people and companies lost money. The Information System Authority (RIA) only sees the tip of the iceberg, because victims of financial fraud turn primarily to the police.

While attempts are still being made to defraud companies of money with various invoice frauds, last year stood out with the number of frauds against individuals. This may be due to people having more money on their account as a result of the pension reform and the pandemic situation, as well as the growing interest in cryptocurrencies. At the same time, the fraudsters are evolving rapidly and successfully using psychological manipulation techniques. In addition, they have always been able to reap the benefits of changing circumstances.

FRAUDULENT CALLS FROM THE BANK AND THE POLICE

Much of the reports we receive about financial fraud against individuals still involve fraudulent calls on behalf of a bank. The caller is usually a Russian-speaking person, but at the end of the year, there was also a trend where the conversation was started in Estonian and only then handed over to a Russian-speaking 'customer service representative'. The purpose of the calls is to find out the PINs of the person and use them to clear the bank account.

Although both the police and the Estonian Banking Association have worked hard to raise awareness of the problem (see, for example, the campaign page eiaitah.ee) and it has also been widely covered in the media, there are still many people who believe the callers and end up losing their savings. The figures speak for themselves: according to the police, in the first ten months of the year, people lost 2.8 million euros in this way. The fraudsters were most active during autumn.

At the end of 2021, there was also a wave of calls imitating the police: the caller claims to be from the Estonian police and informs the person that a large loan has been taken on their behalf, or asks for information about a third party and then informs the person that the bank account of the person has been hacked. The purpose of the call is to phish the personal identification code and other data that can be used to carry out frauds.

The fraudsters try various techniques to increase their credibility, such as mentioning their police token number. Behind these calls is an internationally organised network whose call centres make thousands of calls a day and



constantly seek to make them more credible to generate revenue.

CRYPTOCURRENCY FRAUDS ARE A RISING TREND

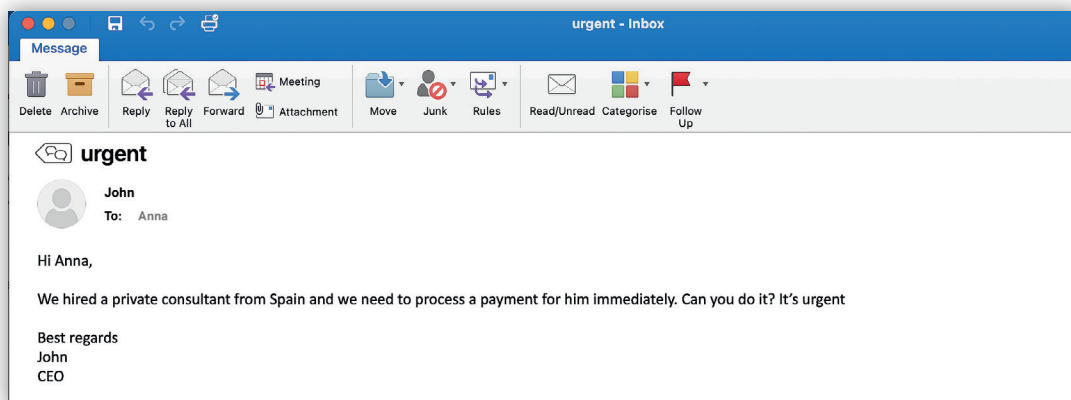
Various frauds related to cryptocurrencies, the losses of which ranged from a few hundred euros to almost 100,000 euros, were a growing trend last year. The most typical were cases where a person had created an account and started operating on a cryptocurrency trading platform, but found that later it was no longer possible to withdraw the money. It often turned out to be a fake platform – a temporary environment specially created by criminals to entice people to make transactions there. After a while, the platform was closed and the money was stolen.

Frauds also have indirect victims

In addition to direct financial loss, invoice fraud can also have indirect victims whose business or reputation may be temporarily damaged. In 2021, there was an example of a company in the medical sector, whose name and details were used to send fake invoices to partners in the same field. This temporarily damaged the good name of the company and also caused delays in receiving payments, as partners no longer knew which invoices to trust and which not.

Various frauds related to cryptocurrencies, the losses of which ranged from a few hundred euros to almost 100,000 euros, were a growing trend last year.

An example of a classic CEO fraud



It is relatively easy to carry out this type of fraud scheme, as the regulation of cryptocurrencies is still under development all over the world (a bill regulating the respective field in Estonia is expected to be approved this spring). So far, almost anyone can create or buy a trading environment for cryptocurrencies, buy fake users and followers, and advertise it on influential social media channels. While the initial recommendation before purchasing any cryptocurrency or joining any environment is always to do a thorough background check, it may not be enough – fake platforms may have fake user reviews and negative feedback from deceived customers may not reach the forums until it is too late. In addition, there are criminals also following the forums and rushing ‘to help’ those who have lost money and direct them to new phishing sites or fake environments.

Upistic disappeared with the money of the investors

In the last two months of the year, we received reports about the environment upistic.com, which advertised itself as the leading provider of crypto investment services in Estonia and attracted investors from all over the world. However, the environment stopped working and investors, mostly foreigners, lost their money. In the cases reported to us, the damages ranged from a few hundred to a few thousand euros.

In addition to fake platforms, we also received reports of criminals breaking into a crypto wallet of a person (the application where crypto assets were stored) and stealing the contents. The average reported loss was around a few thousand euros. Well-known applications, such as MetaMask, are not inherently unsafe, but they are vulnerable to common threats such as weak passwords, security vulnerabilities in applications such as web browsers, or the user accidentally entering their own crypto keys on a phishing site. While in the case of banks, the responsibility of the bank for depositing money is very clearly regulated and depositors are protected by law, theft in the crypto world usually means the permanent loss of one's assets.

INVESTMENT ADVICE FROM TINDER?

Many of the frauds we found out about were linked to a specific scheme. In this scheme, victims meet the fraudster on a dating platform – often on Tinder or Facebook Dating. After some time, the ‘beautiful Asian girl’ or ‘young French man’ starts talking about investment opportunities that they have used to improve their lives and on which they have been consulted by a ‘relative working in the finance field’.

The conversation was often not intrusive at all and the topic was casually mentioned while talking about their daily activities. These fraudsters often wait for the victims to become interested and start asking additional questions. Once they got to know each other more and some trust was established, the new acquaint-

ance agreed to share their investment recommendations, helped create an account in a specially designed environment, and showed how the initial investment was earning good profit.

Over time, they encouraged the victim to invest ever-increasing amounts of money. However, when the person wanted to take out the investment, it proved impossible. It was essentially an investment fraud, but instead of aggressive telephone sales, contact was made on a dating platform and the fraudster spent time to get to know the victim.

THERE WERE FEWER FAKE INVOICES THIS YEAR

2021 broke the record with two attempts to commit invoice fraud, the figures of which were unprecedented in Estonia. Fortunately, they remained only attempts. The largest of these took place in the early summer, when criminals began to monitor the e-mail exchange of a large Estonian company with a cooperation partner abroad. At the appropriate time, they intervened and presented fake invoices for a total of several million euros on behalf of the partner.

The e-mail filter system of the company discovered the fraud fairly quickly and no losses were incurred. The Estonian company also did not find any signs of a break-in in its e-mail system, so it could be assumed that the mailbox of the cooperation partner located in Central Europe had been compromised.

The second case took place at the beginning of the year, when the attentive staff of a construction company was able to prevent a similar attempt to commit invoice fraud for 900,000 euros. Both of these cases show that appropriate protection measures and staff awareness of the most common scams pay off indeed.

There were some successful invoice frauds too in 2021. To our knowledge, the largest amount lost was 35,000 euros.

In addition to the way described above, where fraud is carried out by breaking into the system and hijacking the e-mail conversation, the classic CEO frauds are also still used. In December, a dozen companies informed us that their accountant had received a letter from the CEO

The story of one fraud

Martin is a successful middle-aged entrepreneur who works in the field of consulting and communicates with a large number of people in Estonia and abroad. One day, he received a Facebook friend request from a lady who introduced herself as a representative of the international fashion industry. She said she had been on holiday in Estonia and was looking for marketing contacts here. Her communication style was polite and professional. In addition, she sent Martin materials related to her professional work and was not in any way intrusive. The lady also talked about her background and achievements and sent pictures – nothing seemed suspicious.

After several weeks of communication, she mentioned her experience in crypto and her plans for specific transactions. As Martin was also interested in the field, he asked for more information and received references and links to various environments. Martin checked them and found no indications that the environments were fake.

Martin then decided to invest 1,000 euros in crypto, which started to make a profit, and initially, he was able to grow his investment. Encouraged by the positive experience, he made two additional investments.

At one point, however, Martin said his 'intuition awoke' and when he tried to transfer the earned money back to his crypto account, it failed. In total, Martin lost 8,000 euros. The police says there is not much hope to get it back and Martin will have to take it as a lesson.

As for money and investment, his advice is to be very careful with any new contacts and not to trust their advice, no matter how skilfully presented.

or a member of the management board requesting an urgent transfer to a foreign bank account. In at least one case, the transfer was made and 15,000 euros reached the account of the fraudster. However, general awareness of this type of fraud has grown over the years and there are fewer cases of major financial losses. ●

Cannot Get Through the Gate Until the Gate is Open*

Most of us follow simple principles to ensure our physical security, but many seem to think that digital assets are able to protect themselves, writes **Oskar Gross**, Head of the Cybercrime Unit of the Central Criminal Police.

A year ago, in the RIA Cybersecurity Yearbook, I described the role of the police in investigating cyber incidents and explained why it is important to upgrade our systems and keep logs. The principles of cybersecurity, like the trends in cybercrime, have not changed over time. Therefore, it is appropriate to remind everyone of this 'mantra'.

I called a colleague from CERT-EE and asked a simple question: if a company has not paid any

attention to cyber security, what are the three things it should do first to protect itself? They said the exact same thing the police would have.

1. Know what systems you are using and what data is there.
2. Update your systems regularly.
3. Train your users to know the dangers.

By following these three rules, you still cannot be 100% sure you are protected from all cyber threats, but the probability of falling victim is still significantly reduced.

THE DAMAGE IS GREATER THAN IT INITIALLY APPEARS

Cyber security is no different from other types of security where everyone can do a lot by themselves to avoid becoming a victim. In ensuring our physical security, we follow simple principles on a daily basis to protect our property. We know where the windows and doors are in our home and when we leave, we make sure they the windows are closed and the doors are locked. We keep our valuables in a safe (principle 1). If the door lock breaks, we replace the

The direct and indirect damage that can result from cybercrime is significantly greater than it initially appears.

* Estonian proverb

lock (principle 2). We teach our children how to lock the door (principle 3).

We replace a broken door lock even though it costs us time and money. Our home and the things there are more expensive than the cost of a new door lock, and I dare say the same goes for our digital data.

Cybercrime investigators very often see problems with system updates and logs in their daily work. Human mistakes are also common – people do not recognise phishing scams and reuse passwords.

The direct and indirect damage that can result from cybercrime is significantly greater than it initially appears. The consequence can be a great financial loss to an individual or a company. The police always try to help the victim get their money back, but it must be taken into account that money is transferred quickly between countries and it is not uncommon for it to be withdrawn in cash in some other country before the victim even realises that something has happened.

MAJOR INVESTIGATIONS LAST YEAR

When talking about cybercrime, we must talk about the important investigations of the past

year – downloading more than 280,000 document photos and offering money laundering services to cybercriminals.

In the first case, it is significant that, in cooperation with our partners, we identified the suspect as early as 24 hours after the attack was discovered. This was mainly thanks to the fact the crime was committed in Estonia. In the case of cybercrime, the international element is the rule rather than the exception.

The money laundering service was also offered from Estonia, this time to criminals abroad, and it is suspected that they earned nearly 1.5 million euros.

You might (rightly) ask why the cyber police are investigating money launderers and not hackers. We are, of course, investigating classic computer crimes, but here, too, we are guided by the principle that crime must not pay off.

Given that cybercrime is mainly committed for financial reasons, the investigation of money laundering also plays an important role. We strive to increase the capacity of cybercrime investigation and due to the interdisciplinarity of the field, we need more and more specialists in other fields in addition to people with IT knowledge. ●



Ransomware Attacks

Rarely Have a Happy Ending

While heroes in Hollywood hostage films are usually able to escape, then in hostage-taking in cyberspace, where criminals gain access to corporate or personal information, the victim often has to choose between bad and very bad options.

In 2021, CERT-EE registered 30 ransomware attacks (32 in 2020). This number does not seem large, but it must be borne in mind that the consequences of a ransomware attack are one of the most serious: these attacks have stopped production lines for days, and companies have lost all of their files, along with customer data.

Even if the malware is removed from the systems and the machines start working normally again, the files may be lost forever. In other words, do not hope for a happy ending and instead, prepare for great losses and, in the worst case, bankruptcy.

TWO MILLION EUROS OR ELSE...

In December 2020, a trading company fell victim to a ransomware attack through the RDP protocol, which enables remote connections, and its work stopped as a result of the attack. The criminals encrypted the data of the company – including the customer list and reports – with the Cry-Lock malware and demanded 100 Bitcoins for releasing and not selling the data. At that point, 100 Bitcoins were worth almost two million euros.

In January 2021, an IT services company announced that they had discovered ransomware on their servers that was encrypting data. The IT specialist of the company was able to stop the attack but by then, half of the servers were already encrypted. The company backed up their data regularly and they were able to restore the files from the copies.

In February, an employee of a wholesale company discovered that they did not have access to the systems running on their server. Upon further investigation, they discovered that the files, e-mail server, backups, etc. were encrypted by ransomware and a ransom demand was left in the folder. The company disconnected the old systems, cleaned the equipment, and reinstalled the software. To prevent such attacks, they changed their work organisation and installed new security solutions.

In the second half of February, a ransomware attack hit a nursing home in Harju County, the server of which was encrypted by the Phobos ransomware. The nursing home was able to get the systems up and running three days after the



attack. To our knowledge, the company paid the attackers and were able to decrypt all files by the beginning of March.

In March, an electrical work company in Tallinn reported that attackers had accessed their server via the remote desktop protocol, or RDP. The ransomware was discovered when one of the employees could not open Microsoft Office. It turned out that their data was encrypted by the LockBit ransomware. The company removed the servers from the network and began cleaning the equipment. Some of the data was backed up three months ago, so it was not possible to restore all the data.

In April, a business software company reported that they had fallen victim to a ransomware attack through RDP and four of their customers could also have been infected with the same malware. The attack was carried out with a newer version of the LockBit ransomware, encrypting the file servers and virtual servers of the company.

In July, we received information that there had been a ransomware attack on the device of an enforcement agent through an IT service company, and criminals demanded money from the enforcement agent. To our knowledge, the criminals were not able to encrypt the backups.

In November, an industrial company reported a ransomware attack. The malware encrypted the server used to store the files, which also contained the accounting software of the company. Based on preliminary information, the

How to protect yourself?

There are some simple rules to follow to prevent getting infected with malware and mitigate the consequences:

- use the latest software version and make sure all updates are installed,
- make regular backups,
- restrict the rights of system users,
- train your employees on cyber threats.

backups were also encrypted.

These examples are just some of the ransomware attacks reported to CERT-EE.

YOU SHOULD NOT PAY THE CRIMINALS

Paying the criminals will motivate them to continue what they are doing. This money is used to further develop malware and crime: this means that attacks are becoming even more dangerous and the ransom demands higher. Payment of the money does not guarantee the release or return of the data. There have been cases where data stolen from the victim was released for sale after the ransom was paid.

If you fall victim to a ransomware attack, let us know at cert@cert.ee.

If you fall victim to a ransomware attack, let us know at cert@cert.ee. We can advise on how best to deal with the particular situation, how to identify the attack vector, the attacker, what malware has been used, whether the data has been stolen, and what to do to prevent a similar incident from happening again. For many ransomwares, there are free decryptors available. This means that the encrypted data can be restored without having to pay the criminals. ●

What Did We Learn From the Local Elections?

Some functional errors caused public disapproval, but we did not identify any malicious activity that could have impacted the 2021 local elections.

In addition to the State Electoral Office, the Information System Authority (RIA) had two major tasks: to run the necessary systems for the elections (the election information system VIS3 and the electronic ballot box called Koguja) and to coordinate the cybersecurity of the elections in general.

Estonia is the only country in the world where nationwide internet voting can be held thanks to the infrastructure of the e-state. But alongside the i-voting, the votes cast on paper and counted by hand are also stored in information systems

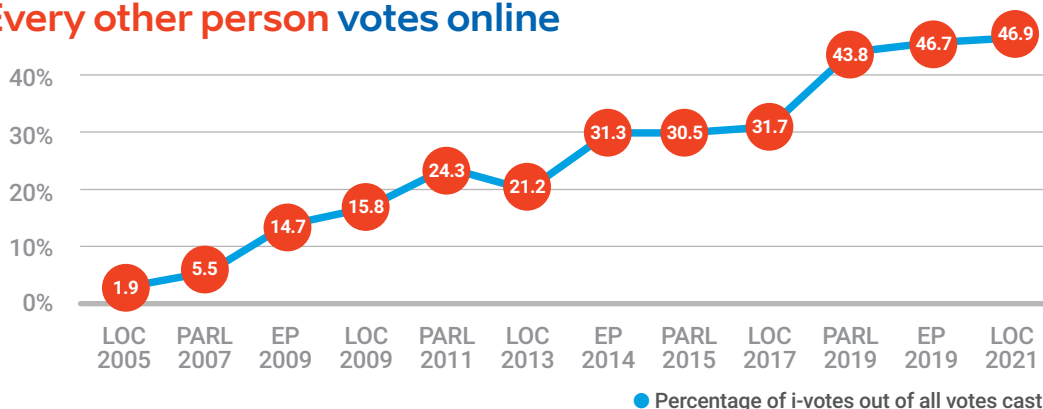
and transmitted to the public digitally, which is why the cyber security of all election technologies is crucial. Therefore, we were extremely happy that we did not identify any incidents with a significant impact during the elections.

IT WAS NOT ALL SMOOTH SAILING, HOWEVER

At the beginning of the election week, some functional errors caused public disapproval. For some MacOS users, the voter application did not work with the ID-card; errors were found in the documentation of the e-voting application; the public has rediscovered that e-voting is



Every other person votes online



not possible with the popular authentication application called Smart-ID.

Such errors do not and must not go unnoticed. We must learn from them and take them into account before the next elections. The election results showed that they did not leave a deep mark on the reputation and credibility of i-voting: ballots cast over the internet set another record in terms of both the share of all votes and the total number of i-votes.

There were no indications of malicious activity in any of the incidents related to the election, nor did they affect the confidentiality of the votes or the integrity of the system or data. On the Saturday of election week, a failure occurred when – due to the excessively high levels of protection against denial-of-service attacks – employees of the polling stations could not access VIS3 in about half an hour. However, voting continued and voters were registered in the information system afterwards.

SECURITY WAS THE FOCUS

Election organisers have never before paid as much attention to cyber security as we did in 2021. Security testing, risk analysis, threat assessments, and awareness-raising at all levels put the issue of cyber security at the forefront of the elections. We worked with political parties, other state agencies, employees of the polling stations, and international partners to prepare for potential risk scenarios.

The next elections – the parliament elections – will take place in the spring of 2023. We are already preparing for them. The autumn elections of 2021 taught us what we need to ensure there are no incidents with a significant impact during the elections. ●

Activities of RIA in the 2021 local government elections

The State Electoral Office is responsible for the general organisation of elections (including the operation of i-voting and the use of the election information system). RIA is a partner of the State Electoral Office on the basis of a cooperation agreement.

RIA hosted the electronic ballot box called Koguja, developed the new version of the election information system VIS3 for the State Electoral Office (together with external partners), provided customer support, and organised cyber security activities:

- organisation and coordination of the security testing of technical solutions,
- coordination of risk analysis and threats,
- cyber hygiene training for VIS3 users,
- providing a cyber hygiene Digitest for employees of the polling stations,
- providing workstations to polling stations and their monitoring (in cooperation with the Centre of Registers and Information Systems),
- a voluntary service provided to political parties free of charge regarding the overview of the security of e-mail and web servers,
- 24/7 readiness of technology and cybersecurity teams during election week,
- monitoring the entire Estonian cyberspace in heightened readiness during the election week.

In addition, we helped State Electoral Office run an e-voting information campaign 'Lase oma e-hääle kõlada!' ("Let Your E-voice Be Heard!"), which focused on awareness of the new e-voting period and existing security measures.



Hackers, Help Your State!

RIA is working on a model that would allow state agencies to work with hackers and pay them for information about security vulnerabilities.

This form of cooperation called the bug bounty is common in many countries, including the US, France, the United Kingdom and our neighbour Finland. Its purpose is to work with independent experts who look for potential vulnerabilities in the services and pass this information on to the service administrator, who pays a fee for identifying the vulnerability. Our system is based on a model developed by US experts. We hope to reach the first successful contract this spring.

THE FIRST LESSON

Despite the incomplete system, RIA wanted to pay a reward to a hacker in August last year, when information was sent to our general e-mail about a possible security vulnerability in state e-services, including the state portal eesti.ee managed by RIA. Our experts checked the information received and identified two possible vulnerabilities in the e-services of the Centre of Registers and Information Systems (e-land register and marital property register).

Then, we forwarded this information together with the materials sent by the hacker to specialists of the Centre of Registers and Information Systems. They confirmed the existence of these security vulnerabilities and eliminated them. No security vulnerabilities were identified in the state portal eesti.ee.

The weakness of the services of the Centre of Registers and Information Systems was that it was possible to obtain information from the land register and the marital property register without authentication in the respective service. No misuse of personal data has been reported. The person who informed us of these vulnerabilities was supposed to be the first to be reimbursed by RIA. The first reward was to be between 3,000 and 4,000 euros. Although the development of the whole system was still in its infancy and the legal bases supporting it had not been described and approved, we still tried to find ways to pay the reward. However, there were some conditions.

One of the conditions was that the security vulnerability had to be in a critical service and no more data had been used or downloaded to detect it than was appropriate to document the vulnerability. This form of cooperation also requires confidentiality on both sides – as a rule, the hacker must refrain from commenting for the next 90 days so that the service owners can analyse and patch the security vulnerabilities and perform additional analyses. As the hacker violated all the above conditions and raised doubts about their motives with further conduct, RIA decided not to pay the reward. The Director of the Cyber Security Branch of RIA admits that we could have approached the situation differently.

RIA ENHANCES THE ABILITY TO IDENTIFY SECURITY VULNERABILITIES

In February 2022, a team was set up as a separate unit in CERT-EE to test our services and identify potential vulnerabilities before cyber-criminals find out about them. In the past, RIA has involved various Estonian experts to test its services. However, this year, we will increase our capabilities and involve our own experts in

We would behave differently today

GERT AUVÄÄRT

Director of the Cyber Security Branch of RIA



The state alone cannot identify all the bottlenecks in our e-state, so cooperation with the community is essential. RIA has collaborated with several scientists and experts to help resolve a number of major and minor incidents. We wanted the cooperation to be successful and pay the reward in this case as well. However, we could not rush with signing the contract, as such transactions require a number of conditions to be met and procedures to be followed, such as validation of information, assessment of security risks, analysis of logs, and so on. We also explained this to the hacker.

There are things we could have done differently. The state has not cooperated in this way before, so the communication was rough at times and there were times when we had to take a break to see what we want to do and what the law allows us to do. RIA could have made it clearer that the reward would only be paid if all the agreed conditions were met. We will be smarter next time and hope to sign the first bug bounty contract in the spring this year.

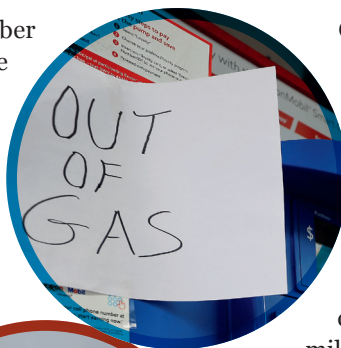
addition to external testers. The team of testers (usually known as RedTeam in the exercises) will initially work on the services of RIA. In the future, it is planned to expand the scope of the team to include testing support for other state agencies.

However, people alone are not enough to increase security. Our equipment also needs constant improvement and development. At the beginning of the year, the CERT-EE team received new equipment to test their work in the state network. The purpose of the equipment is to enhance the protection of the state network. Thus, we can hope that the network of state agencies and local governments will be significantly better secured in the future. ●

What Happened in International Cyberspace in 2021?

Last year, news of cyber incidents and security reached even those who had not heard of these topics before. Many incidents directly and severely disrupted the daily lives of people and crossed the news threshold.

One of the most reported cyber incidents last year was the ransomware attack on the US energy company **Colonial Pipeline**. The nearly 9,000-kilometre pipeline of the company is used to transport nearly half of the fuel used on the entire east coast of the United States. As a result of the attack, the pipeline was shut down for almost a week, causing several states to face fuel shortages. To restore the systems, Colonial Pipeline paid the attackers, the Russian cyber group Darkside, 75 Bitcoins or 4.4 million dollars. Although tracing cryptocurrency is extremely difficult, the US Federal Bureau of Investigation (FBI) has managed to recover 2.3 million dollars of the money paid to the criminals.



Colonial Pipeline was not the only company to pay ransom to the attackers. **JBS**, the largest meat processor in the world, which was hit by a ransomware attack by the Russian group REvil, also paid the criminals. The company paid the group 11 million euros for the decryption key to avoid potential damage to restaurants, grocery stores, and farmers.

However, there were those who chose not to pay the attackers. In May, there was a ransomware attack on the Irish healthcare system, where criminals injected the system with the Conti ransomware. The encrypted systems prevented access to diagnostics and medical records. In addition, the attackers stole and disclosed sensitive patient data. The system was only almost completely restored several months later in September.



Due to many ransomware attacks with such serious consequences, the cybersecurity experts around the world were talking more and more about the ransomware epidemic. This was enhanced by a ransomware attack by a Russian-based group, REvil, on the software company **Kaseya** in July. It affected more than a thousand companies in 17 countries that used the cloud-based solution of Kaseya to remotely manage IT systems. One of the victims of the attack was the Swedish COOP store chain, which had to close 800 stores because their billing system was not working.



RUSSIA AND SOLARWINDS

In addition to cybercriminals, cyber spies also had a busy year. Just before the beginning of last year, in December 2020, a supply chain attack was announced against the US company **SolarWinds**, which provides the IT management and monitoring software Orion. The first half of 2021 was spent on investigating the attack and its aftermath.

In April, the United States and its allies (including Estonia) attributed the SolarWinds attack to the Russian foreign intelligence service (SVR) cyber group APT29 (also known as Nobelium). Through compromised software upgrades, they gained access to the systems of authorities and companies using SolarWinds software. There were 18,000 victims worldwide, including several US ministries and governmental authorities, as well as the National Bank of Denmark. Russia denies any responsibility.

CHINA AND MICROSOFT EXCHANGE

The world had not even recovered from the SolarWinds case when another high-impact incident was discovered. In early March, **Microsoft** announced that it had identified and fixed four zero-day vulnerabilities in its Exchange e-mail server software that allowed attackers to gain access to e-mails, passwords, and administrator privileges on servers.

It was immediately suspected that spies were behind the attack. In the summer, the United States and its allies (including Estonia) filed a formal indictment against the People's Republic of China for several cyber-attacks, including compromising Microsoft Exchange (cyber group Hafnium). The statement said that hackers linked to the Chinese government have also carried out a number of ransomware attacks and other cyber operations, not only for intelligence purposes but also to make money. China denies any responsibility.

Following the joint indictment, the French National Agency for the Security of Information Systems (ANSSI) announced that several French organisations are under attack by APT31, a cyber group with ties to the Chinese government. APT31 has focused on cyber espionage, providing information to the Chinese government and state-owned enterprises to achieve political, economic, and military leadership. It is also worth noting that the cyber security company Positive Technologies announced that APT31 was also targeting Russia for the first time.

RUSSIA AND GHOSTWRITER

Ghostwriter, which several countries say is linked to the military intelligence of Russia (GRU), also caused tensions in Europe. According to cyber security company Mandiant, Belarus is behind Ghostwriter. In June, Ghostwriter targeted Polish politicians and administrative agencies. The attackers were able to gain access to the personal Gmail accounts of the office manager of the prime minister and other members of the government. Some of the e-mails were leaked.

In the autumn, Germany announced that Ghostwriter was trying to steal the data of their members of parliament. Namely, Ghostwriter had been trying for months to reach members of the Bundestag and the Landtag, mainly targeting the Christian Democratic Union and the Social Democratic Party.



The European Union also soon filed a formal indictment against Russia. Russia was accused of malicious cyber-interference in the elections and politics of EU member states. According to the EU, Russia attacked the parliaments, officials, politicians, journalists, and civilians of EU member states with the Ghostwriter campaign. The hackers broke into the computer systems and personal accounts of the targets and stole data to spread disinformation and manipulate information.

BELARUSIAN ACTIVIST-HACKERS

Political tensions were also expressed in another way in cyberspace. For example, the **Cyber Partisans**, a pro-democracy activist group in Belarus, reported on their Telegram channel that they had gained access to Belarusian national databases. According to them, the Pass information system provided them with the names of Belarusian people, passport numbers, jobs, names of parents, etc. Among them were KGB staff and informants.

The hactivists are fighting against the current regime in Belarus. Last year, the group also announced on its Telegram channel a plan that promised a lot of action at 'moment X' to eliminate the 'fascist regime'. The group, which calls itself apolitical, wants new, free, and democratic elections.

LOTS OF DATA LEAKS

Many organisations in both the public and private sectors had to deal with data leaks. For example, hackers accessed the network of **GoDaddy**, one of the largest web hosts and domain registrars in the world. As a result, the e-mail address and customer number of 1.2 million GoDaddy customers were leaked. The leaking of e-mail addresses facilitates phishing attacks.

A lot of people's health data was also leaked. For example, a leak was reported by the Utah Imaging Associates (UIA) in the United States. The personal information of 582,170 people became public: their first and last names, e-mail addresses, dates of birth, personal identification codes, health insurance policy numbers, and medical information (diagnoses, treatment, prescriptions).

Hackers also gained access to other sensitive data. For example, e-mails from the Lithuanian Ministry of Foreign Affairs appeared on the web forum for sale. Hackers also obtained access to the e-mail system of the US defence industry company **Electronic Warfare Associates** (EWA). The company did not disclose whether the attackers also gained access to confidential technical documents.

SUSPECTS IN CYBERCRIME WERE ARRESTED

Last year, law enforcement agencies had several successes on the cyber front. Shortly after the attack on the Colonial Pipeline, the ransomware group **Darkside** ceased operations. In autumn, US authorities posted a 10 million dollar reward for information leading to Darkside members.

In the autumn, the US Department of Justice announced that two members of **REvil** had been arrested and charged. One of them was Jaroslav Vasinskiy, a Ukrainian citizen arrested in Poland, who was allegedly behind the ransomware attack on Kaseya. The second arrested was Yevgeny Polyanin, a Russian citizen who had received 6.1 million from ransomware attacks, which was later confiscated by the authorities.

There were also other arrests. For example, Interpol carried out an international operation that resulted in the arrest of 1,003 people suspected of being involved in a number of cybercrimes – for example, romance scams, investment frauds, money laundering, and illegal gambling. Authorities froze 2,350 bank accounts and more than 27 million dollars. Police from 20 countries (e.g. China, India,

What Else Happened?

- In December, a critical vulnerability was discovered in the **Log4j** logging function of the Java programming language, which affects millions of devices worldwide. Read more on page 20.
- In July, Estonian citizen **Pavel Tsurkan** pleaded guilty to computer crimes in an Alaska court in the United States. Tsurkan managed the Russian 2015 botnet, which had more than a thousand compromised computers and routers.
- In October, **Medtronic**, a manufacturer of insulin pumps, recalled remote controls for some of its insulin pumps due to cyber threats. Taking advantage of the security vulnerability, the control could be remotely manipulated, such as starting or stopping insulin pumping or changing the amount being pumped.
- Russian technology giant **Yandex** said the denial-of-service attack (DDoS) on them in August and September was the most powerful in history. There were a record of nearly 22 million requests per second.
- The Israeli company **NSO** helped its customers to spy on journalists, politicians, and activists. This was done using the Pegasus software developed by NSO, which can trigger the camera and microphone of the target phone, as well as access messages, photos, and e-mails, and record calls.



Romania, Slovenia, Angola, Colombia) took part in the operation that lasted from June to September.

A new ransomware group, **BlackMatter**, was formed in the summer, but in the autumn, it announced that it would close down due to pressure from the authorities and law enforcement agencies. Although cybercrime is still growing, these arrests can still be considered significant victories. ●

Potential Didsasters Avoided

When it comes to cybersecurity, the focus is often on high-impact incidents and the damage they cause: be it stolen data, encrypted systems, or lost money. However, there are also incidents with a happy ending.

These are cases where the cyber awareness of people and technical measures have helped to prevent greater harm. For consolation and motivation, let us look at some success stories.

PAY ATTENTION

In the summer, attempts were made to defraud millions of euros from an electricity company through invoice fraud. Namely, the criminals managed to monitor the correspondence of the company with a foreign partner (probably due to the compromising of the e-mail system of the cooperation partner). Once it was time for

sending and paying of the invoices, the fraudsters took over the correspondence and started sending fake invoices. Fortunately, the fraud was detected using the e-mail filter system. Although compromising the mailbox and monitoring the mail is still a serious breach of confidentiality, great financial damage was avoided.

Unfortunately, some other companies were not as lucky. On several occasions, fraudsters managed to monitor the correspondence and intervene at the right time to change the current account number on the invoices. The parties sending the invoices may not even realise that someone has interfered in the communication between them. They often only find out when the other party draws attention to the payment of the invoice again. However, once the money has been transferred, it is difficult to get it back.

It is therefore important to be aware of the risk of such fraud and to always check the accuracy of the data before paying any invoices. As can be seen from this example, this can save millions of euros.

DENIAL-OF-SERVICE ATTACKS WITHOUT A SIGNIFICANT IMPACT

Paying attention is always important, but efficient and properly configured systems also help to prevent greater damage. Last year, we often saw how automatic protec-



tion mechanisms, such as DDoS protection or a firewall, helped with denial-of-service (DDoS) attacks. For example, several denial-of-service attacks against the state portal eesti.ee and several public authorities were effectively blocked.

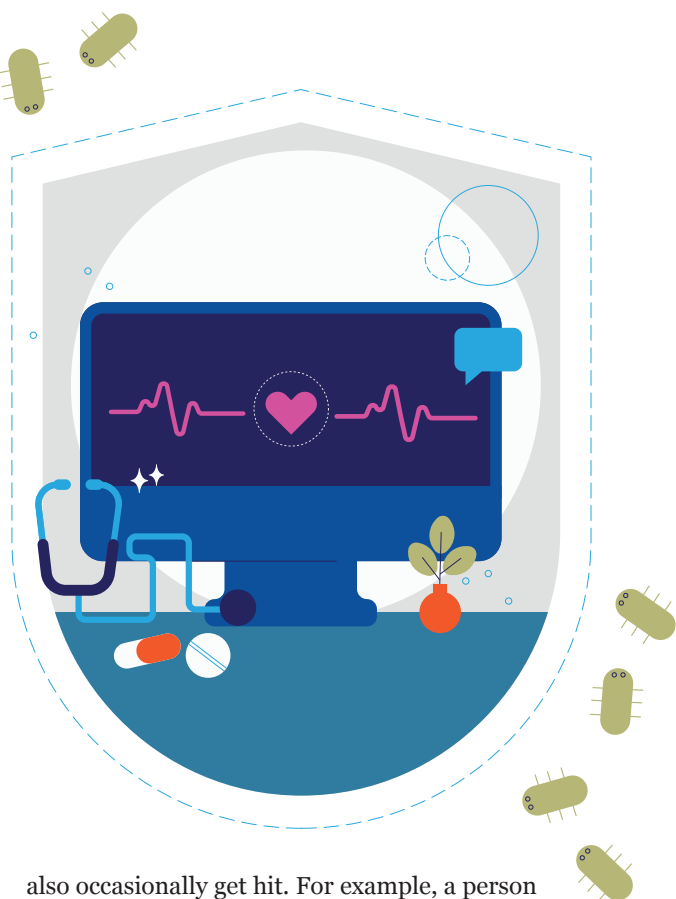
In the case of a denial-of-service attack, the system or website is flooded with requests so that it becomes inoperable. If there had been no protection and the attacks had been successful, the operation of the websites would have been significantly slower than usual or completely interrupted.

Public authorities should consider joining the state network that offers DDoS protection.

BACKUPS

There is no absolute protection against ransomware attacks. However, people, authorities, and companies can do quite a lot to make getting hit as painless as possible. This means that data needs to be scattered, backed up, and recoverable. This ensures that if the systems are encrypted with ransomware, instead of paying criminals, you could restore the documents and files from the backup.

For example, a company reported that ransomware was installed on the computer of their accountant, from which it moved on to other computers. In total, the data was encrypted on six devices. Data was successfully restored from



also occasionally get hit. For example, a person working in the video and photography business reported that two of their hard drives were encrypted. Unfortunately, they had not backed up their materials.

Because ransomware tries to encrypt files on the local disk, external media, and network drives, the backup must be separate, or it may be encrypted as well. One backup should be kept offline.

AWARENESS IS KEY

The damage prevented by protection mechanisms and knowledgeable computer users is difficult to assess and calculate. It is not known how many malicious links there are that someone has not clicked on or how

many people have not entered their data on fraudulent websites. However, it is safe to say that greater awareness of and capability to cope with the dangers of cyberspace will mean more success stories. ●

Paying attention is always important, but efficient and properly configured systems also help to prevent greater damage.

the backup. There are many similar stories – using backups saved time and money.

Of course, not everyone got away that easily. Although criminals generally use ransomware to target businesses, private individuals can

The Cyber Hygiene is Improving

The level of cyber hygiene of the Estonian population has improved in three years, but there is room for improvement, according to data collected in co-operation with Statistics Estonia.

In 2019, 64 per cent of respondents said they used stronger passwords than the minimum requirements or different passwords for different accounts. In 2021, this percentage had increased to 69, with the largest increase in the 65–74 age group, where the figure rose from 33 per cent to 42 per cent.

MANY ATTACKS START WITH A WEAK PASSWORD

These results are especially reassuring to us at RIA because we have paid a lot of attention to passwords and multi-factor authentication in our information campaigns, public messages, and prevention activities. Reusing passwords or choosing weak passwords and the lack of multi-factor authentication allow the attackers to gain initial access to devices and systems.

The number of respondents who have made their passwords stronger (wording used in the poll: use of different passwords, passwords longer and more complex than the minimum requirements, regular changes, etc.) has increased in all age groups over three years. The base level was already high among young people (82.5 per cent of 16–24-year-olds chose this answer in 2019 and 87.1 per cent in 2021), but the level also increased significantly among older respondents (from 47.2 per cent in 2019 to 54.5 per cent in 2021 among those aged 55–64 and from 33.1 per cent to 42.1 per cent among those aged 65–74).

For context: in 2019, we launched an information campaign for elderly Internet users to emphasise the importance of cyber hygiene. We

are only now seeing the impact of this intervention (and the follow-up campaign aimed at the Russian-speaking population in 2020) in the survey results.

THE AWARENESS OF THE ELDERLY REMAINS LOW

The cyber hygiene level of the elderly remains clearly lower than that of the younger ones. However, the number of respondents who said they did not do any of the proposed activities has fallen from 13% to 11.3%. This decrease is mostly due to the improvements by respondents aged 45+.

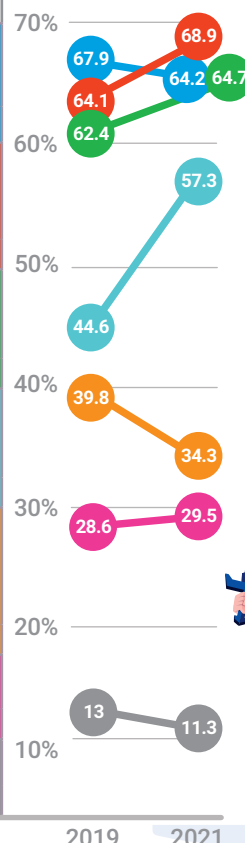
In some areas, though, we are also seeing a move in another direction. Compared to 2019, 5 per cent fewer people said they did a background check before using a new device, app, or service, and 3 per cent fewer said they used security programs or apps. Whether or how these issues may affect the cyber security incidents in Estonia remains to be seen.

One very clear factor influencing the level of cyber hygiene was the nationality of the respondents. Estonian residents of other nationalities (of whom the majority is of Russian, Ukrainian and Belarusian background) mentioned significantly less activities they do for their own security. While 72 per cent of Estonians mentioned strengthening passwords, this number was only 61 among representatives of other nationalities. The results for avoiding clicking on suspicious links were 68 per cent and 55 per cent, respectively. However, the cyber hygiene of respondents of other nationalities has also improved in almost all areas in three years. ●

Question: What have you done for personal security or privacy on the Internet or in an application?

	2019	2021
Used security programs or applications (e.g. anti-virus, firewall)	67.9	64.2
Change		-3.7
Strengthened passwords or started using different passwords (including passwords that are longer and more complicated than the minimum requirements, regularly changed them, etc.)	64.1	68.9
Change		4.8
Checked links and attachments in unexpected e-mails or e-mails from unknown senders before opening them	62.4	64.7
Change		2.3
Avoided using the Internet on a computer or smart device of a stranger	44.6	57.3
Change		12.7
Thoroughly researched the background of the company / service provider on the Internet before using their new device/application/ service or ordering goods from them (e.g. e-shop, taxi applications)	39.8	34.3
Change		-5.5
Changed Internet browser / social network / application security settings	28.6	29.5
Change		0.9
Have not done any of them	13	11.3
Change		-1.7

Source: Statistics Estonia



What is the Information System Authority (RIA) doing to improve cyber hygiene in society?

In addition to the cyber security of the public sector and critical infrastructure, we set an even broader goal for RIA with the 2018 National Cyber Security Strategy: to make the people of Estonia more cyber-skilled. The strategy approved by the government also set out a method for this: 'It is necessary to keep talking about the prevailing risks to the general public, dispensing advice for mitigating risks, and emphasising that development of knowledge and skills in the field of cybersecurity is the joint responsibility of everyone in cyberspace. /--/ Following the entry into force of the Cybersecurity Act, RIA has taken the central role in cyber hygiene, state prevention activity, and increasing awareness in society. Similarly to the Police and Border Guard Board and the Rescue Board, broad-ranging prevention and awareness campaigns will be launched to spread the word about cyber threats to different target groups, including businesses.'

A year later, we organised the first nationwide campaign 'Ole IT-vaatlik' (a wordplay on being careful online) for the elderly, then a follow-up campaign at the beginning of the pandemic, an IT-vaatlik information campaign for businesses in autumn 2020, and various additional information activities for the Russian-speaking population. Awareness activities are also planned this year.

The key question for campaigns and information activities is always how to measure their impact. After each campaign, we can find out how many people saw the TV ads and how many clicked on links on social media. However, in order to measure the level of cyber hygiene, we decided to start cooperating with Statistics Estonia in 2018, which conducts the survey 'Information technology in the household' among Estonian residents every spring.

What Will 2022 Bring in Cyberspace?

Last year brought a lot of security vulnerabilities and a ransomware epidemic. What's in store this year?

The year of vulnerabilities will have a sequel

We called 2021 the year of vulnerabilities. The same will be said of 2022, just as COVID-19 is affecting our lives for the third year in a row. Different problems caused by Log4j, which shocked the world in December 2021, will be revealed throughout the year. There will be reports of new major vulnerabilities comparable to those of Exchange or Confluence last year.

When it comes to Estonia, we must be prepared for the next incidents caused by legacy software. Those could have even more serious consequences than the incidents in RIA in the summer of 2021 or in the Ministry of Economic Affairs and Communications in late autumn 2020. We will continue to have problems with so-called anti-patchers, i.e. information security managers or administrators who do not bother to update their software when vulnerabilities are identified and patched by the manufacturer. Unfortunately, such people can be found in our state agencies as well as the providers of essential services. We would like to remind everyone – threat assessments and patching instructions from RIA must be addressed immediately! Criminals are always paying attention to those and people responsible for the security of critical information systems must do the same.



APT groups will become increasingly aggressive

The SolarWinds incident is now called the 'Cyber Pearl Harbor' in the United States. During the attack, attributed to Russia by the United States and its allies in the spring of 2021, hackers managed to break into several US ministries and large corporations. It will not remain the biggest of its kind. It is only a matter of time before groups led or commissioned by countries with strong cyber capabilities perform a successful attack on an even bigger scale. As new security vulnerabilities keep being discovered, but unfortunately not immediately patched, the detection of an attack vector that will lead to similar effects is very probable.



The number of and damage by ransomware attacks will grow

Both the number of and damage by large-scale ransomware incidents is increasing year by year. You know it is serious when it is not possible to buy petrol for days on the east coast of the United States and groceries from the Coop supermarket chain in Sweden or the IT systems of the Irish Health Service Executive stop working. So far, Estonia has not been hit as badly, also thanks to our little known language and the comparatively small size of Estonian companies. It is likely that the current stable situation – two or three malware incidents reported to CERT-EE every month – will continue in the near future. On a global scale, however, more and more incidents are to be expected, and even the loss of human lives cannot be ruled out if a health care institution is seriously hit.

Phishing and phone scams are not going anywhere

Phishing, which dominated 2019 and 2020 and set another record in 2021, is not going anywhere. Over time, phishing sites for both bank accounts and e-mail accounts will be looking more and more authentic and be written in increasingly better Estonian, which is why Estonians are still falling victim to phishing attacks.

The second and now more damaging type of phishing attacks is the increasingly popular Russian-language phone scams from either the 'bank' or the 'police'. Schemes related to cryptocurrencies (both in the form of fraudulent calls and phishing e-mails) are also on the rise, with individuals suffering losses of up to five digits in euros. According to the Police and Border Guard Board, phone scams cost the Estonian population a total of five million euros in 2021.



The response speed and capacity of RIA will increase

The capacity and capabilities of our Cyber Security Branch have remained about the same for the last five years or so. But we will make a leap forward in 2022, as can be read in the preceding pages. CERT-EE will receive several new tools and the resources of our supervisory, analytical, and critical infrastructure protection units will also increase.

It will take time to build up those new capabilities, but over the course of the year, we should be able to identify threats more quickly. We will also be able to instruct our IT community, companies, state agencies, and the general public on appropriate countermeasures in a swifter manner. Together with the Estonian population's steadily growing awareness about basic cyber hygiene, this will hopefully lead to a situation where the whole country is better protected in cyberspace.

Cyber Security in Estonia 2022

Publisher: **Information System Authority**
Pärnu mnt 139a, 11317 Tallinn

Design: **Martin Mileiko** (Profimeedia OÜ)

Illustrations: **Linda Vainomäe** (Profimeedia OÜ), **iStock**

Photography: **Seiko Kuik, Scanpix**

Printed by: Ecoprint AS

Read more: www.ria.ee/en