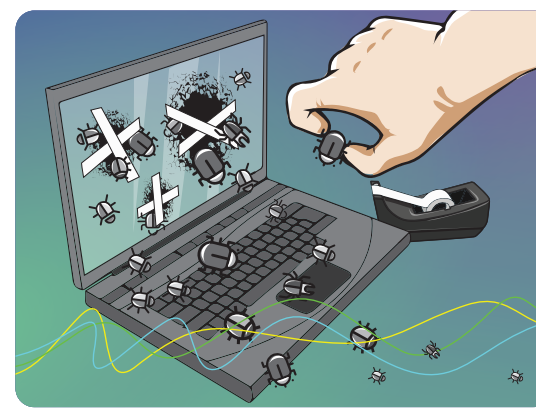
Republic of Estonia
Information System Authority

CYBER SECURITY IN ESTONIA 2023

Republic of Estonia
Information System Authority

Cyber Security in Estonia 2023

Contents



SAFER CYBERSPACE

CYBER SECURITY is part of national defence and internal security

Last year reminded us that freedom, independence, and security cannot be taken for granted and that cyberspace is not something separate from the physical world. In order to ensure the normal functioning of society even in crises, we must treat cyber security as a part of broad-based national defence and internal security, says **Gert Auväärt**, Director of Cyber Security of RIA.

Photo: Seiko Kuik

Gert Auväärt

Last January, it became clear that the escalated situation in cyberspace requires greater attention and readiness from our entire country to preserve our digital lifestyle. Russian invasion of Ukraine, which started on the anniversary of the Republic of Estonia, confirmed the vulnerability of (cyber) security and once again brought up the question of whether and how we can cope when our information systems are hit by attacks that deprive our people of electricity, communication, water, or other basic necessities.

I am sincerely grateful to our Ukrainian colleagues who, at a critical time when their country is doing everything to save the lives of its people, have shared with us their painful experiences and crucial information about the attacks. They have helped us to be better prepared – to find tools that have enabled us to protect services against major attacks.

This is the current situation, but it can change quickly. We work hard 24/7 to ensure that we are prepared and protected against cyber threats. As we have confirmed before, Estonia will do everything it possibly can to help Ukraine win the war, including in cyberspace.

ATTACKS ON RELIABILITY

Despite the fact that there have been no attacks with more serious consequences on our services and systems, I can confirm that it is not because criminals have not attempted that. We were hit with the biggest waves of attacks in spring and autumn, when websites and services important to the country were hit by a record number of denial-of-service attacks. There were

so many of them that when briefing our allies, quite a few of them raised their eyebrows. In some cases, services were partially unavailable and websites were down, but they did not lead to extensive interruptions that could affect the well-being or safety of our people.

The success of criminals in making our lives difficult depends on the developers, administrators, and users of IT solutions. The wisdom of every link is necessary to keep criminals away from our data, sensitive information, and money. The state has an important role in raising awareness of protection measures and threats, and the employees of RIA have made significant efforts to play this role well.

A CYBER RESERVE THAT IS UNIQUE IN THE WORLD

During the year, we introduced new tools that provide better protection against attacks, increase monitoring capabilities, and help prevent threats and respond to incidents immediately. We will raise the level of preparedness again for the upcoming parliamentary elections – election security continues to be an absolute priority for us.

Together with other providers of important services, we have mapped the risks and formed a cyber reserve with the Government IT centres and the Defence League to have a pool of experts that we could turn to in case of a major cyber incident. At the end of last year, we organised an exercise focusing on this reserve. With the help of partners from the US, we have offered world-class training for members of the cyber reserve and providers of vital and important services, including in the energy sector. We will continue to carry out such trainings this year as well.

We have regularly provided members of the government, the top leadership of the state in general, as well as the IT sector, the cyber community, and companies with overviews and threat assessments. In October and November, we organised an awareness campaign to emphasise the importance of IT-conscious behaviour for all people in Estonia. We have consistently increased the scope of supervision and piloted the launch of the new Estonian information security standard with dozens of agencies. We will continue to work on this in 2023 as well.

The new information security standard that entered into force at the beginning of the year is a challenge for approximately 3,500 agencies that perform public sector tasks or provide critical services. Implementing the standard is one way to protect services. The overall success of the agency depends on how well its processes are thought out, threats identified, plans drawn up, and the level of information security determined, because an incident involving IT systems can stop the work of the entire organisation. We have seen this happen in Estonia as well.

TENSIONS REMAIN HIGH

2022 was an eye-opening year for many people. The Russian invasion of Ukraine continues, and tensions in cyberspace remain at their peak.

There are few countries in the world where you can draw an equal sign between the digital state and the state itself. In Estonia, they are two sides of the same coin. What happens in cyberspace affects us at every turn. I ask the readers to take the threat assessments, notifications, and recommendations of RIA seriously and take the necessary steps to protect yourself. Each of our recommendations includes specific steps you can take to protect your systems.

Each of our recommendations includes specific steps you can take to protect your systems.

Life has shown that for a successful attack, you often need nothing more than determination and a security vulnerability, for example an outdated computer. Protecting yourself in cyberspace takes effort and without it, cyber security is not achievable.

I am glad that the RIA cyber security service has grown into the civil cyber competence centre of the country. We will continue to grow and your expertise may be what we need next. Write to personal@ria.ee and we'll see you in the office!

Situation in cyberspace: A YEAR OF DENIAL-OF-SERVICE ATTACKS

The hope that 2022 would be normal after two pandemic years died in the early morning of 24 February, when Russia launched a full-scale war against Ukraine. The conflict extended into cyberspace and resulted in an unprecedented number of denial-of-service attacks against Estonia.

In addition to the usual cybercriminals looking for easy income, pro-Kremlin hacktivists and groups carried out politically motivated attacks last year.

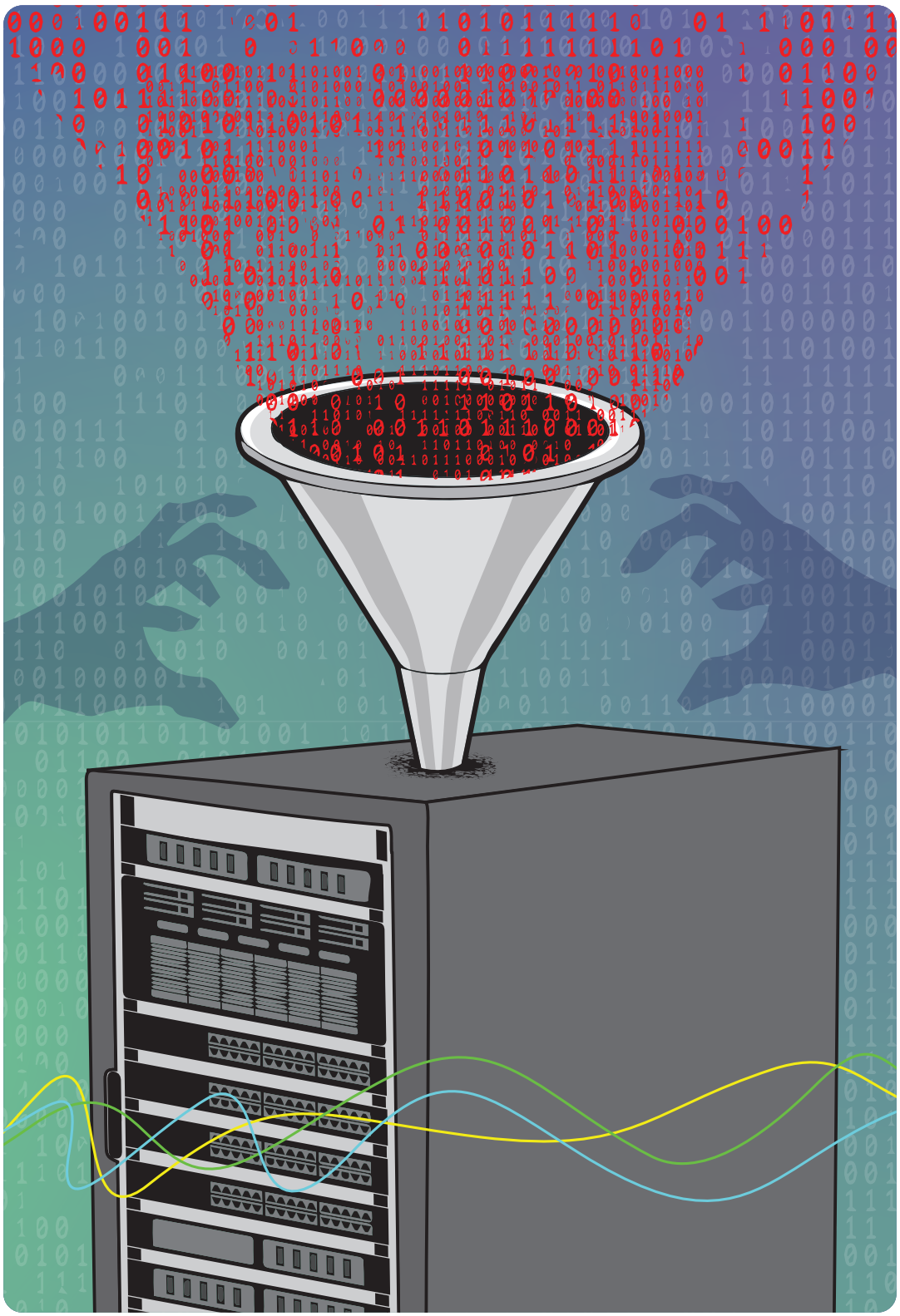
We also noticed that uninvited guests were more active than usual exploring web pages and services located in Estonian cyberspace. They looked for everything that would allow to break in more easily: security vulnerabilities, outdated important software, and incorrect configurations. This kind of information gives the attackers a good overview of whether they should come back to with more serious intentions and to which sites.

In order to prevent high-impact incidents and, if necessary, respond to them quickly, RIA has been operating at high alert since January of last year. In other words, we adapted our daily work to the changed threat situation. We also enhanced the technical defences we provide to state agencies early last year, including protection against denial-of-service attacks. As the following months showed, we did the right thing.

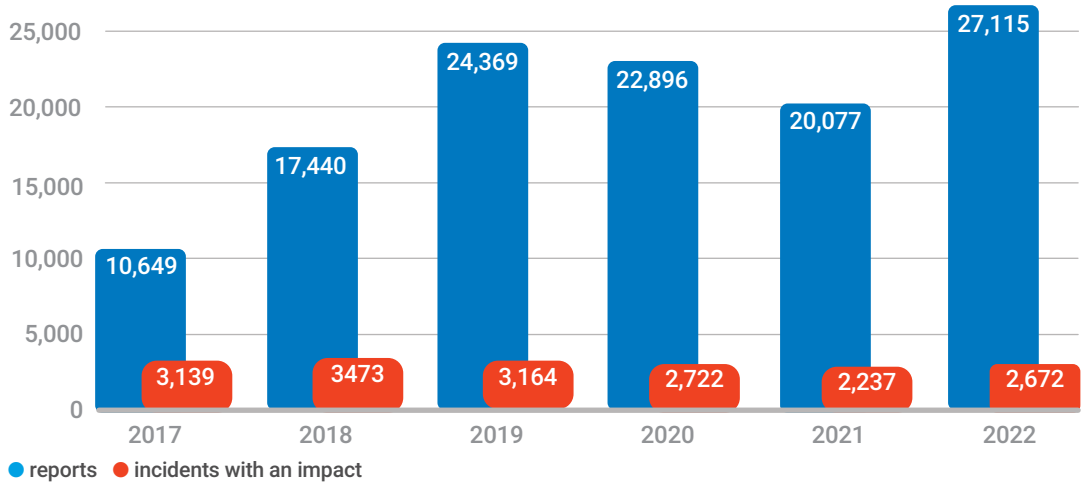
ONE WAVE OF ATTACKS AFTER ANOTHER

There have been times in the history of this publication when we have had to think long and hard about which keywords to use to sum up the past year. This year, it was easy. In 2022, Estonia was hit by waves of denial-of-service attacks, the likes of which we have not seen before.

The volumes of the attacks were sometimes more than a hundred times higher than in 2007, when, after the removal of the Bronze Soldier monument, our eastern neighbour disrupted the work of our e-services and thereby our daily life with mass requests. Fifteen years



Number of incidents and reports submitted to CERT-EE



ago, they were more successful in this. The attacks of last year were fortunately mostly not even noticed by the average user. Occasionally, an important website or service would run slower than usual or be down for a short period of time, but most denial-of-service attacks were managed so that the public did not even notice that important websites or services were under massive attack.

The volumes of the attacks were sometimes more than a hundred times higher than in 2007, when, after the removal of the Bronze Soldier monument, our eastern neighbour disrupted the work of our e-services and thereby our daily life with mass requests.

Let us take an example from 18 October, when the Riigikogu adopted a statement condemning the annexation of Ukrainian territory and declaring the Russian regime a terrorist one. This was followed by a denial-of-service attack against riigikogu.ee – more requests were made in 24 hours than are made in 7.5 years under normal circumstances. However, the visitors of the website did not notice the attack – thanks to the protective measures, it functioned as if nothing special had happened.

Normally, we record less than ten significant denial-of-service attacks per month. In April 2022, there were 25, in August, 66, and in November, 43. In twelve months, there were a total of 302 attacks, which means a fourfold increase compared to the year before. About a hundred of them had an impact. According to Cloudflare, in the second quarter of 2022, Estonia was ranked seventh in the world in terms of the number of denial-of-service attacks directed at the application layer. In terms of population, we are below the 150 mark.

The favourite targets of the attackers were as expected: valitsus.ee, riigikogu.ee, president.ee, eesti.ee, politsei.ee, and id.ee, but the transport sector and media companies were also targeted.

While in previous years, we saw denial-of-service attacks with a financial motivation (pay, otherwise we will attack more and longer!), then last year, most of the denial-of-service attacks were carried out by pro-Kremlin hacktivists who expressed their dissatisfaction in this way. They were upset by the moving of the Narva tank monument and they did not like the

suspension of Russian TV channels or our support for Ukraine.

While learning information systems and schools were often the target of denial-of-service attacks in 2021, they were targeted less last year. Looking at the timing and handwriting of these attacks, it can be assumed that students were mostly behind them. More about denial-of-service attacks on page 18.

PROBLEMS WITH TELEPHONE OPERATORS

While denial-of-service attacks went unnoticed by most people, some service interruptions that did not result from an attack but from human error, lost power connection, or hardware or software failure affected tens of thousands of people.

In the late evening of 15 February, a large-scale voice communication and M2M service disruption started in the network of Telia. M2M solutions are used, for example, to open gates and barriers in parking lots and to start and end m-parking.

Problems with parking caused inconvenience, but more dangerously, the service disruption also affected calls to the emergency number 112. In a situation where there are errors in the network of your mobile operator but you need to call for help quickly, we recommend removing the SIM card from the phone or restarting the device and instead of entering the PIN code, calling the emergency number – in this case, the phone uses the network of another operator to make the 112 call.

While such problems usually do not last long, this time, the services were not restored to working order until the following evening.

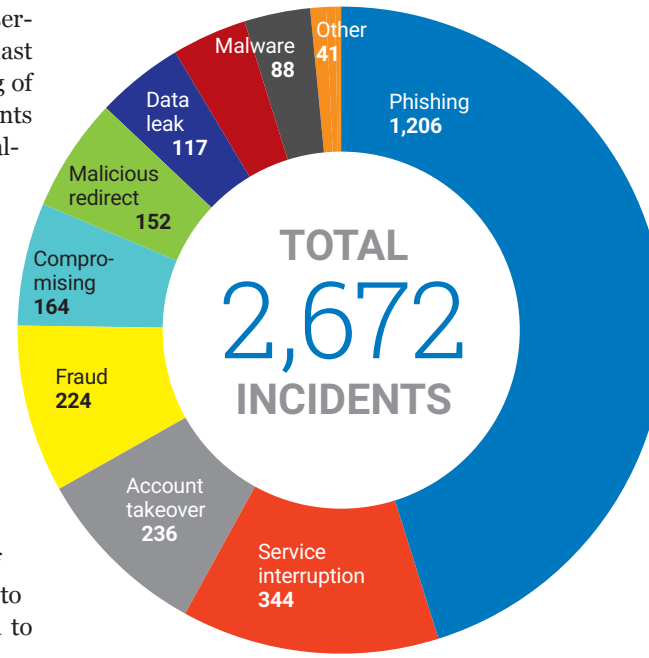
Unfortunately, this was not the only time Telia had issues. On 23 August, voice and mobile data services were disrupted again – this time, for about an hour. The disruption affected people all over Estonia – approximately one third of the calls could not be made or were interrupted during that time.

Voice and data services were also disrupted in December, when Saaremaa and Hiiumaa suffered a power outage due to a snowstorm. This affected the services of all operators. Batteries were placed near many of the masts, with the help of which they continued to function after the power cut, but these batteries eventually died. Emergency teams tried to bring mobile generators to the poles, but it sometimes proved impossible because the roads were impassable due to heavy snowfall.

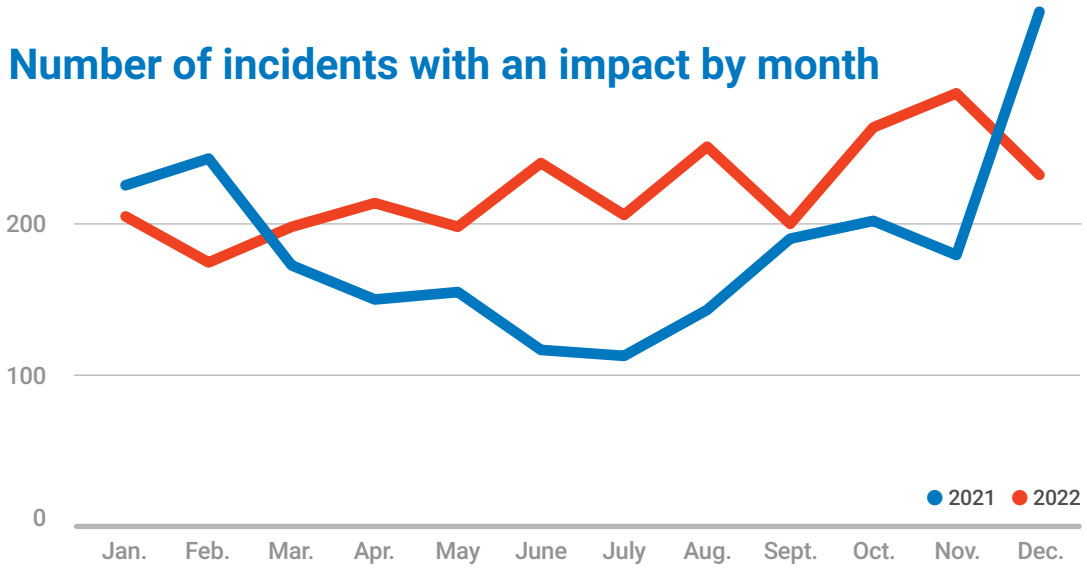
There were also repeated interruptions in the functioning of eID tools. One of the most inconvenient of them was what happened on 30 August, when all services SK ID Solutions services, including three authentication tools – ID card, Mobile-ID, and Smart-ID – were simultaneously offline for three hours. Following this incident, RIA started supervisory proceedings against the company. Read more about supervision on page 48.

Technology also failed a family health centre in Tallinn: a recently acquired server stopped working, resulting in the loss of both the data in the database and fresh backup copies. The last working backup copy was half a year old, and it was not possible to restore the data stored in between. Naturally, this caused a lot of problems for the family health centre.

Incidents with an impact in 2022



● Denial-of-service attack



However, there were also failures in services, the continuity of which does not depend on Estonian companies or agencies, but which have many customers here. Due to an error in the Gmail server, some emails did not reach the recipients on 10 December and some were delayed. In Estonia, it affected nearly 180,000 users.

DATA THAT NEEDED BETTER PROTECTION

One of the most important data leakage incidents of the past year is related to the logistics company Itella Smartpost. In the late evening of 6 November, information began to spread on social media that one user had obtained the information of approximately 10,000 people and companies who have sent or received parcels via Itella Smartpost: their names, phone numbers, email addresses, and for some shipments, door codes or the parcel machines where the parcel was located.

In addition, the attacker got hold of the usernames of business customers. They tried to see if some of them use their username as their password and, unfortunately, in dozens of cases, the answer was yes.

Nothing justifies the theft of the data of thousands of people, but there are lessons here for the company as well. The data was not sufficiently protected and the leak could have been easily avoided. The police started a criminal procedure to investigate the case.

Smaller data leaks occurred every month. For example, after a payment software update, it was discovered that by entering the name of a third party in the search bar on the payment page of a commercial bank app, the app displays the last payments related to them. The bank corrected the error within a few hours.

In addition, we received information about the leakage of bank card data of Estonian residents. They were probably stolen over a long period of time through phishing pages. We informed the banks and asked them to close the cards with the leaked data, if necessary, so that criminals could not steal money from the users.

SCAMS AND PHISHING

Last year did not bring any major changes or innovations in terms of scams and phishing. Phishing continued to account for the largest proportion of incidents recorded by CERT-EE. Attempts were made to swindle naive users of their passwords, bank card details, and money.

More cynical criminals took advantage of the goodwill and desire of people to support Ukraine – they sent a fraudulent email, promising that the donated money would go to a charity and through it to Ukraine, but in reality, it ended up in the accounts of the criminals.

Phishing emails and messages sent on behalf of courier companies were very popular last year. They informed the recipient that in order to receive their parcel, they had to pay a few euros to the courier company. The link in the email or

message led to a fake page identical to the real site, where the person was asked to enter their bank card details. Those who did this soon discovered that not two, but 200 or 2,000 euros had been taken from their account. Only then, many people remembered that they were not even expecting a parcel from the courier company.

We also received hundreds of notifications from people who were sent an email that appeared to be from the police, informing them of the start of proceedings for possession of child pornography, committing a sexual crime, or something similar. The recipient of the email was asked to send their reasons to the indicated address within two days and threatened with 'immediate arrest' and disclosure of the committed acts if they did not respond.

The police do not send such emails. It was a scam designed to steal data and money. By replying to the email, the person received further instructions on how to avoid a long court saga by paying a 'fine'. Read more about scams and phishing on page 20.

FEWER RANSOMWARE INCIDENTS

While in other parts of the world, there were several significant ransomware attacks, Estonia managed to avoid them. Last year, we recorded 21 ransomware incidents, which is half the number of the year before. Fortunately, most of the victims had backup copies of their data, thanks to which the work of the agency or company could be restored, but unfortunately, the life of the attackers is often made too easy by leaving the RDP connection for remote access open to the whole world. There are examples from last year where the attack happened just hours after an RDP connection was opened for a remote employee.

However, besides investing in technical solutions, we must not forget that the weakest link is often the so-called ordinary computer user.

2022 IN NUMBERS

- In 2022, the Incident Response Department of RIA (CERT-EE) received 27,115 reports. This means 74 reports per day on average.
- 2,672 of those had an impact, which means that the confidentiality, integrity, or availability of information or systems was interrupted.
- We received 1,206 reports of phishing pages. This is 50% more than in 2021.
- We received 344 reports of service interruptions. These included all kinds of services, from voice communication to digital prescriptions.
- We received 263 reports about user account takeovers, mostly social media accounts.
- We received 21 reports about a ransomware attack that hit Estonian companies or people. Their number dropped by almost half.

IT service providers, who also have access to the systems of their customers, should be especially careful. If adequate defence measures are not implemented, dangerous malware can quickly spread to them as well. Read about ransomware attacks on page 24.

EVERY CLICK COUNTS

There is no reason to expect that the tense security situation in our region will ease this year. This also means a higher level of danger in cyberspace and a higher probability of a significant cyber incident affecting a large part of society.

Pro-Kremlin hacktivists and groups will continue to attack Estonia and other supporters of Ukraine. Alongside relatively simple denial-of-service attacks, there will be more complex and dangerous attacks.

For Estonia, this means an ever-increasing need to invest in cyber security. However, besides investing in technical solutions, we must not forget that the weakest link is often the so-called ordinary computer user. No matter how good the antiviruses, firewalls, and other technical protection solutions, one wrong click or password entered into a phishing page can trigger a chain of events that none of us wants to have to deal with. Be IT-conscious!

RUSSIAN AGGRESSION IN UKRAINE: war in cyberspace

On 24 February 2022, Russia launched a full-scale war against Ukraine. In addition to kinetic warfare, Ukrainian governmental authorities, critical infrastructure, local governments, the security and defence sector, and companies were also targeted in cyberspace.

On the day the Russian troops crossed the border of Ukraine from several sides, the satellite communication connection with Viasat's KA-SAT satellite was lost for hours there due to a cyber attack against KA-SAT satellite, which was later attributed to Russian military intelligence. In addition to Ukraine, the cyber attack also affected other parts of Europe – such as France, Germany, Italy, and Poland – where satellite communications were temporarily disrupted.

One of the most extensive attacks since the beginning of the invasion took place in March against the largest Ukrainian telecom company, Ukrtelekom, which left almost 80 per cent of customers without an Internet connection for hours. There have been other, less significant cyber attacks against the Ukrainian telecommunications sector, and direct military action has also naturally caused service disruptions. This made recovery from some cyber attacks difficult, because some equipment had to be physically accessed, but due to military action, it would have been life-threatening for the employees.

The Ukrainian energy sector was also targeted. In April, Russian military intelligence allegedly tried to knock out a large Ukrainian energy company, but failed. Hackers tried to disrupt power substations using the Industroyer2 malware. This malware, designed to attack industrial control systems, was also used by the Russian military intelligence in the December 2016 attack on the Ukrainian electricity system, which left parts of Kyiv without electricity. However, last year, CERT-UA, in cooperation with the cyber security company ESET, managed to detect the attack on the energy company in time and protect the network.

INTIMIDATION BEFORE THE INVASION

On 13 January, the websites of dozens of Ukrainian governmental authorities were defaced – the attackers replaced their content with their own message. On the websites, you could read in Ukrainian, Russian, and Polish, 'Ukrainian! All your personal data has been

uploaded to the public network. The data on your computer has been destroyed and it is impossible to recover it. All information about you has become public – fear and expect the worst. This is your past, present, and future.'

The Ukrainian government announced the next day that most of the affected websites had been restored and no personal data had been leaked or changed. Website defacing is technically a relatively simple cyber attack, but it can still have a significant effect: creating anxiety, undermining the authority of the Ukrainian government, wasting the time of investigators, etc.

DENIAL-OF-SERVICE ATTACKS BECAME COMMONPLACE

Before the invasion, Ukraine was also hit by significant denial-of-service attacks. For example, the e-services of Ukrainian state-owned banks (Privatbank and Oschadbank) and the websites of the Ministry of Defence and the Armed Forces were down. The websites of the banks were available, but it was not possible to log in to the account.

The governmental authorities and banks of Ukraine were also hit by a powerful wave of denial-of-service attacks the day before the

→

start of the Russian full-scale military attack. These kinds of attacks continued throughout the year: websites of, for example, Ukrainian governmental authorities, security services, and several ministries have been taken down with varying degrees of success.

SPREAD OF DESTRUCTIVE MALWARE

Several types of destructive malware have been found in Ukrainian information systems and networks since the beginning of last year. It is a tool for erasing data and making devices unusable. One of them allegedly hit one of the Ukrainian border crossing points, which is why border crossings had to be formalised with paper and pencil for a while.

Destructive malware was used to attack Ukrainian organisations both before and after the invasion, but in some cases, the impact was not limited to Ukraine. For example, in addition to the attack on the Viasat KA-SAT satellite, a cyber attack also had a cross-border impact in the case of another piece of destructive malware, which, in addition to the target, was found in the networks of Latvian and Lithuanian offices of a company cooperating with the Ukrainian government.

CYBER ATTACKS IN INFORMATION OPERATIONS

The purpose of some cyber attacks was not to disrupt the work of a website or service, but to spread false information. For example, the websites of local governments were compromised, where false information was posted on behalf of the local governments that Kyiv had fallen and a truce was signed with Moscow.

Compromised Ukrainian news portals (e.g. Ukraine 24) circulated a deepfake video about Ukrainian President Volodymyr Zelenskyy.

MASS PHISHING

Several threat actors targeted Ukrainian people and organisations with phishing emails during the year. The targets were governmental authorities, armed forces, NGOs, law enforcement agencies, and media workers. Organisations and officials in other countries and international organisations that coordinate the provision of military or humanitarian aid to Ukraine were also targeted.

The main purpose of the attacks was most likely to obtain sensitive information, gain access to systems, and use the compromised organisations to attack the next targets. CERT-UA also warned civilians against phishing, through whom threat actors tried to carry out information operations or reach someone else that could be useful for them. The phishing emails used war and related themes as bait: for example, references were made to country maps, refugees, or NATO meetings.

The main purpose of the attacks was most likely to obtain sensitive information, gain access to systems, and use the compromised organisations to attack the next targets.

The theme of war was also used in the phishing campaigns for the targets of several other countries. Both state-linked cyber groups and financially motivated cybercriminals saw this as an opportunity to trick people into opening malicious files and links. For example, Google reported that the Chinese cyber group Mustang Panda actively exploited the war in Ukraine in phishing emails sent to European organisations. The emails contained an attachment infected with malware, for example called 'Situation at the EU borders with Ukraine.zip'.

THE WAR LED TO A WAVE OF HACKTIVISM

In the ongoing war, not only countries, but also several ideologically motivated hackers – hacktivists – chose sides. Shortly after the invasion, the Ukrainian government called on all volunteers with IT skills to join the so-called IT Army to help protect the critical infrastructure of Ukraine and repel offensive operations by Russian cyber groups.

In addition to network protection, the Ukrainian IT Army has carried out denial-of-service attacks, defacement campaigns, as well as more sophisticated operations against

Russian websites and companies. For example, the IT Army is said to have carried out denial-or-service attacks against Russian banks, state agencies, and media outlets, but also disrupted the work of Russian cinemas and knocked out the Russian alcohol accounting information system, which caused temporary problems with alcohol supplies.

In addition to the Ukrainian IT Army, pro-Ukrainian hacktivists also became active in other parts of the world. For example, there were many reports of attacks by members of the Anonymous group against Russian websites and services and a large amount of leaked data, as well as hacktivists changing the names of databases, folders, and files of Russian institutions to pro-Ukrainian ones (e.g. 'Slava Ukraini', 'putin stop this war'). Among others, the largest taxi service in Russia, Yandex, was targeted in autumn: On 1 September, taxis in Moscow were ordered to one address, which caused a big traffic jam in the city centre.

Pro-Ukrainian hacktivists also used software. Namely, the largest bank in Russia, Sberbank, warned Russians against software updates that carried messages critical of Russia. These were publicly available programs whose authors modified the software in such a way that it began to display, for example, anti-war and pro-Ukrainian messages after the update (so-called protestware).

FRIENDS OF UKRAINE BECAME TARGETS

However, pro-Russian hackers did not waste any time either – soon after the start of the full-scale war, several groups of pro-Kremlin hacktivists became active. Their target was not only Ukraine, but also many countries supporting Ukraine, including Estonia, Finland, Latvia, Czechia, Romania, Poland, and others.

The range of targets of denial-of-service attacks is broadly the same from country to country: ministries, state agencies, the most important e-services, the transport sector, banks, and media outlets. Often, the waves of denial-of-service attacks were prompted when the country made a political decision in support of Ukraine, for example, declaring Russia as a state sponsor of terrorism.

It must be taken into account that by providing support or assistance to one or another country, the person or country may become a target of cyber attacks itself. In previous attacks, the targets were generally predictable, but this may not be the case in the future.

DO NOT PARTICIPATE in DDoS attacks

In February of last year, calls to support Ukraine by participating in denial-of-service attacks against Russian propaganda channels began to spread on social media, including Estonian groups. RIA strongly discourages Estonian people from going along with any calls to take part in cyber attacks, no matter how noble the cause.

While it may seem like allowing an app on your phone to run requests against some Russian propaganda site is a good way to do something for the Ukrainian people, there are dangers involved. By doing so, the user is giving their device to a botnet and running unknown code – both actions are impermissible from a cyber security point of view. Among other things, one cannot be sure which target will be attacked next. There are better ways to help Ukraine.

THE CONTINUITY OF UKRAINE IS REMARKABLE

In terms of cyber security, the resilience of the critical services of Ukraine has been impressive – the digital services of the country, as well as water, electricity, and other necessary systems, are functioning. Disruptions have mainly been caused by kinetic warfare.

Countries as well as several global IT and cyber security companies have also come to help Ukraine in the cyber domain. According to the Ukrainian Security Service SSU, more than 4,500 cyber attacks were successfully blocked in 2022, which is more than five times more than in 2020, when 800 cyber attacks were recorded.

One of the secrets of success is the fact that cyber attacks against Ukraine did not start last year – organisations there have been the target of cyber attacks since at least 2014. The previous experiences are now coming in handy.

A RECORD NUMBER of denial-of-service attacks

2022 in Estonian cyberspace will be remembered above all by the daily denial-of-service (DDoS) attacks. The total number of DDoS attack rose four times compared to 2021. Why did the number of DDoS attacks increase so much, what was their impact, and what can we learn from them?

The catalyst for the increase in DDoS attacks was Russia's full-scale invasion of Ukraine that started on 24 February. The ongoing war has resulted in a massive wave of cyber activism/hacktivism that we have never seen before.

Ideologically motivated hackers – hacktivists – formed many groups and tried to force through their agenda with denial-of-service attacks: the agenda being usually to discredit state agencies and cause fear and/or discomfort in the general public. Both public sector institutions and companies of national importance were attacked. The (apparent) success of the attacks was later reported to fellow members on social networks.

Estonian agencies and organisations were also affected by DDoS attacks by hacktivists, but their impact was marginal. The hacktivists launched two types of DDoS attacks: some focused on attacking websites directly, while others targeted the lower layers of network.

WAVE AFTER WAVE

The first more intense wave of denial-of-service attacks hit Estonia in April – at the same time as the international cyber security exercise Locked Shields was held in Tallinn. The websites of both transport companies and state agencies were attacked. The attackers managed to take down some websites for a maximum of a couple of hours but there was no wider impact.

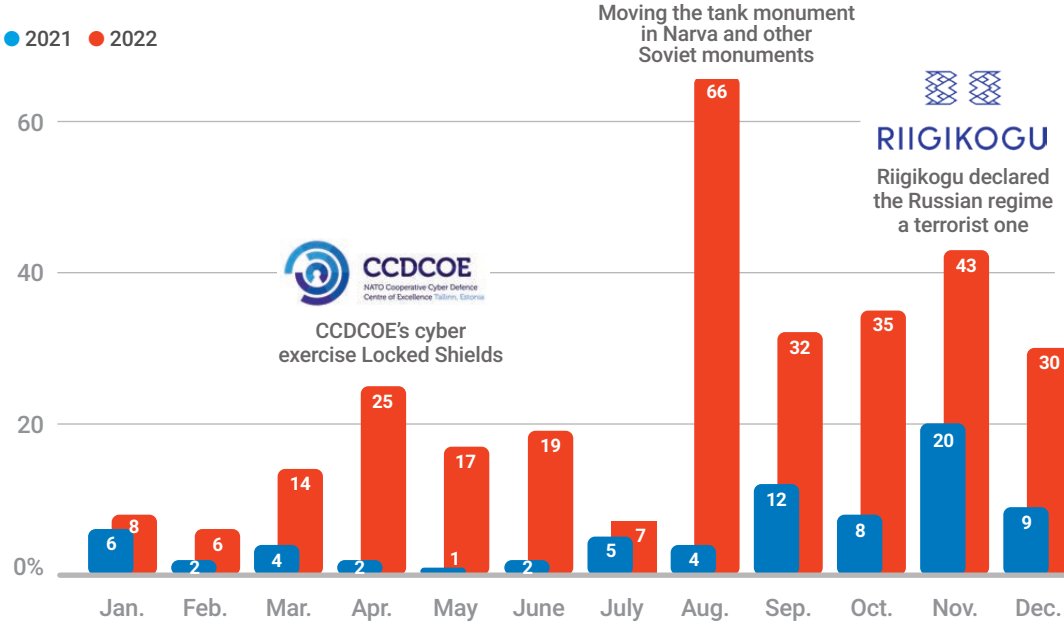
In August, Estonia was hit by the next wave of DDoS attacks. A record 66 denial-of-service attacks were carried out that month – more than 16 times more than at the same time in 2021. The main targets were public sector websites and the transport and financial sectors. The large number of attacks was most likely related to the moving of the Soviet monuments in Narva. Most of the attacks had no significant impact.

Estonian agencies and organisations were also affected by DDoS attacks by hacktivists, but their impact was marginal.

After August, the number of attacks stabilised and remained at a few dozen every month. However, the attackers became more active again after certain political decisions or statements. For example, on 18 October, the website

The number of denial-of-service attacks quadrupled in 2022

Moving the tank monument in Narva and other Soviet monuments



of the Riigikogu was hit by a wave of attacks immediately after the Russian regime was declared a terrorist one.

WHY DID MOST OF THE ATTACKS HAVE NO SIGNIFICANT IMPACT?

With the help of additional funding from the Estonian government, CERT-EE was able to implement additional protective measures in 2022, thanks to which the waves of denial-of-service attacks that hit Estonia did not lead to major service interruptions. This does not mean that we can rest on our laurels and hope that the security measures will protect us from DDoS attacks now and forever. Denial-of-service attacks are here to stay. It is also highly likely that the attackers will try to find ways to bypass the protective measures. If one thing does not work, they will try something else.

Therefore, we must always be ready to analyse new types of DDoS attacks, counter them, draw conclusions, and take the necessary steps to minimise their impact. The faster technology develops, the more extensive the attacks become, and the more capable our devices must be.

HOW TO PROTECT yourself from denial-of-service attacks?

- Make sure your servers are running on updated software.
- If possible, use additional DDoS protection.
- Make sure that your servers and network equipment are sufficiently capable because from time to time, even legitimate users cause a large load of network traffic. In addition, attacks against the network or transport layer may be small enough to prevent DDoS defences from being deployed, but large enough to overwhelm network devices.
- Analyse service bottlenecks and try to find ways to fix them, as the attackers are also looking for ways to reduce the number of requests, but still overload the web page (for example by doing queries which put stress on the database).

A PARADISE for e-fraudsters

Fraudsters and their victims: the darker side of the e-services coin. People mostly fall victim to scam emails and phishing pages, but large losses were also caused by crypto scams.

The coronavirus changed the world in many ways. Working at home became the norm. Life was organised in such a way that you did not have to leave home to buy anything. Even if you did leave the house, it was only to meet the courier or to walk to the nearest parcel machine. Any contact with a person could be dangerous.

A FERTILE GROUND FOR FRAUD

These developments – the reduction of human contact and the increased use of e-services – created fertile ground for online fraudsters. Ordering goods with a couple of clicks is convenient, but it comes with risks. During the golden age of online commerce, the customer base of fraudsters grew because suddenly everyone was ordering goods online.

People who used to be in the office, where they could discuss urgent matters with their colleagues, now worked from home. When verifying the authenticity of emails and text messages became a bit more cumbersome, this step was often skipped.

In 2022, more than a thousand phishing pages were reported to RIA. These are web pages that have fallen into the hands of or have been created by criminals. Criminals use these pages to try to trick people into disclosing information, such as their credit card details or passwords. Even though there are pages that are very poorly designed, most of them look authentic enough to mislead users.

EXAMPLES of successful scams

- On 4 June, a user received a text message imitating the bank SEB. They were directed to a phishing page, where they were asked to identify themselves via Smart-ID. After entering the PIN2 code, the user lost approximately 800 euros.
- On 13 December, a person received a text message imitating the courier company DPD. The message directed the user to a phishing page that asked for their bank card details. They lost 513 euros.
- On 4 December, a user received a text message imitating the bank LHV. The user was directed to a phishing page, where they were asked to log in. As they were not paying enough attention and the page looked authentic, the user entered their Smart-ID PIN2 and lost approximately 700 euros.

FRAUDSTERS IMPERSONATE BANKS AND COURIER COMPANIES

During the year, we received numerous reports of fake emails and messages imitating courier companies operating in Estonia. The criminals mostly imitated Omniva, DPD, and DHL.

Another group that the fraudsters tried to impersonate were banks. Every month, we received dozens of reports from users who received phishing emails from SEB, LHV, or Swedbank.

There are also victims who were approached on Facebook when they were selling something there. In these cases, the fraudster appears to be interested in buying the goods. However,

before making the deal, the criminal gives excuses and reasons why the seller should be the one to pay the buyer – for transport or for insurance. These messages should be disregarded as soon as possible.

Fraud on Facebook Marketplace is not uncommon, and both buyers and sellers need to pay attention. Last year, a Facebook user lost a few thousand euros when they wanted to buy audio equipment. The fraudster presented the person with false invoices and fake delivery notifications.

Such scams come in waves and their credibility varies. Our recommendation is to always double check where you enter your data. In addition, you should remember that entering your PIN2 is equivalent to signing – it is more serious than confirming data or logging in.

ONLINE SCAMS TEACH PAINFUL LESSONS

Invoice frauds and scams with account details, which we have written about in previous yearbooks, are also still used. Scams are carried out in every possible way: through emails, Facebook, Telegram, and other social media platforms, and even through online games.

More than 150 financial frauds were reported to RIA in 2022. Some victims were robbed of less than a hundred euros, but in some cases, representatives of companies transferred tens of thousands of euros to the criminals.

At the beginning of 2022, an employee of a large Estonian company received a convincing phishing email in which the criminals pretended to be the CEO of the company. The accountant transferred more than 14,000 euros to the criminals. In March, an Estonian industrial company lost more than 17,000 euros due to a similar fraud. In June, the next victim lost about 8,000 euros when paying a fraudulent invoice. In August, an Estonian company lost 44,000 euros due to a similar scam. In November, a car sales company lost more than 70,000 euros. The criminals posed as the Scandinavian partner of the company and sent the Estonian company a fraudulent invoice. The actual payment was made to a bank in a southern European country.

Some of these scams had victims outside Estonia, too. In October, a citizen of Lithuania contacted RIA because they had lost 2,500 euros when they wanted to buy pellets from criminals posing as an Estonian company.

CRYPTO SCAMS

In the last months of 2022, the Federal Bureau of Investigation (FBI) started proceedings against two crypto companies connected to Estonia and Estonians. Almost a month before Christmas, the police arrested two Estonian citizens who are suspected of causing damage of more than half a billion euros.

In December, an investigation was launched into the Estonian cryptocurrency brokerage platform 3Commas to find out if the platform was involved in hacking that caused millions of dollars in damage. RIA was also contacted. Users have reported thefts with losses ranging from tens of thousands to a few million dollars.

In October of last year, the National Criminal Police arrested four men suspected of an investment scam, in the framework of which they provided false information, sold the dagcoin they created, and earned eight million euros.

RIA is mostly informed about frauds related to various crypto-platforms and cryptocurrency thefts. At the beginning of November, a user reported that 4,500 euros were stolen from them through the Metamask environment. A month earlier, another user reported that 50,000 dollars' worth of tokens were stolen from their Ledger Nano S cryptocurrency wallet.

REAL LOSSES IN THE GAMING WORLD

There are other ways to lose money on the Internet, too. For example, money is stolen from people through games that allow microtransactions. In November, we received two reports of scams related to the popular game Fortnite. Only a phone number and a code sent to it via text message is needed to make in-game purchases. A player asked a child for their phone number. The child also shared the code sent to them by text message. This way, the malicious player was able to make in-game pur-

ANATOMY OF A SCAM

The beginning of January 2022 was an exciting, busy, and stressful time for Johanna (name changed) from Tallinn. She gave birth to her daughter, which meant a lot of joy, but the baby understandably needed a lot of attention. Their whole life had to be rearranged and, in addition to everything else, clothes and other things had to be bought for the newest member of the family.

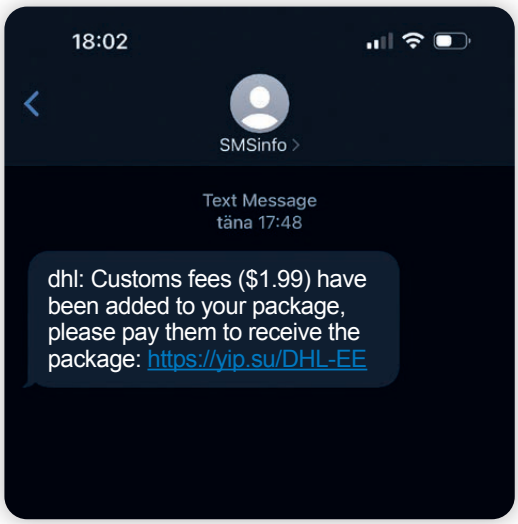
It was a busy period, and to save time, she ordered things online. In addition, the coronavirus was still a very real threat. Therefore, Johanna was expecting several parcels, one of which was shipped by DHL from abroad.

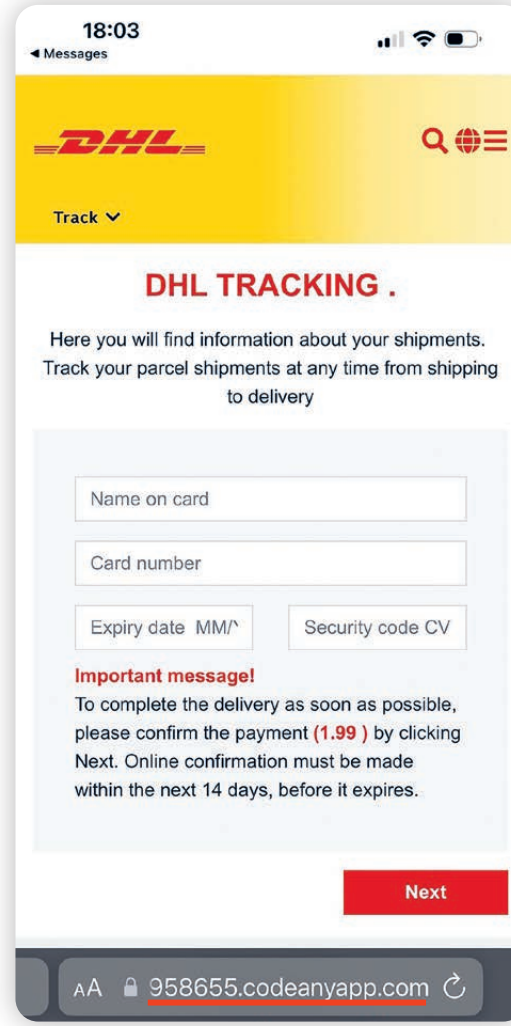
One evening shortly after 8 p.m., when the baby had just fallen asleep, Johanna received a message. 'Your package is awaiting delivery. Confirm the payment (2.22 EUR) under the link below: bid.do/Estonia-Express.' She did not think much of it because it was common to receive information about different packages via text message.

Johanna clicked on the link in the message and a web page opened that looked like the website of DHL. There, she saw the package number, its route, and confirmation that the package has reached the border of Estonia. 'It seemed authentic. For a moment, I thought about checking the package number, but I did not do it. It was a bit suspicious that the package was stuck in customs and I had

Two parts of one fraud attempt

A person who had not ordered a package via DHL received a text message with a link to a phishing page. There, they were asked to enter their bank card details. See the URL on the screenshot on the right that indicates a fraud.





chases for 168 euros at their expense.

Another parent also reported a similar incident in Fortnite. Two Estonian players convinced a child to share the codes sent to them by text message. They used the codes to make in-game purchases for 225 euros. Once the fraud was discovered, the players stopped communicating with the victim.

to pay two euros to get it. Unfortunately, I did not pay enough attention to the red flags,' says Johanna.

By pressing the 'Next' button on the website, she was directed to a page where she could pay the so-called customs fee. 'I entered the bank card details and then the Smart-ID confirmation code was displayed. It seemed to me that I had to confirm something via Smart-ID,' she describes.

In reality, however, the criminals were already making the payment. The Smart-ID verification code was designed either to create trust in the user or to mislead them. 'While I was waiting for the Smart-ID confirmation, I received a bank app notification on my phone that I had made a payment. I saw that 745 euros were deducted from the account. Only then I understood what had happened,' recalls Johanna, who immediately called her home bank, but was told that the payment could no longer be reversed. 'The bank employee sighed deeply,' says Johanna, 'apparently I was not the first to fall victim to this scam.'

She then approached the web constables, who helped as best they could, but said at the outset that there was very little chance of getting any money back. About four months later, Johanna received a notice from the police about the termination of the proceedings. It turned out that her bank card had been used to make a payment at an electronics store in Saudi Arabia.

RANSOMWARE ATTACKS: fewer in number but just as dangerous

Although we registered fewer ransomware attacks last year and most victims had backup copies of their data, these attacks still caused significant damage and inconvenience to Estonian companies.

In 2021, we registered 30 ransomware attacks against Estonian companies, agencies, and individuals. Last year, there were 21. The victims included companies in production, trade, accommodation, logistics, energy, etc.

BACKUPS DO NOT SAVE FROM LOSSES

Even when victims had backups of their encrypted data, ransomware attacks significantly disrupted their operations. To name a few examples: in one company, the production management software stopped working due to the attack; in another, customers could not be served due to the locking of cash register systems; and in a third company, internal work processes and information exchange were interrupted.

In most cases, CERT-EE does not know how much the attackers are asking for the key needed to recover the data. In the initial message, they ask the victim to contact them to discuss the amount, but most of the time they do not receive a reply. As far as CERT-EE is aware, no target paid the ransom last year, at least in Estonia.

WHICH RANSOMWARE ATTACKS WERE CARRIED OUT IN 2022?

The year started with ransom demands for four Estonian companies. In two cases, the work of the company was significantly disrupted because they could not access their information systems. For the most part, the companies managed to recover their work processes and data thanks to the backups, but in one case, the backups were stored on the same server that was encrypted during the attack. Therefore, we recommend keeping the backups in a separate environment so that in the event of an attack, the criminals cannot encrypt them as well.

In July, ransomware called Loki was used to attack a company that had made changes to its IT systems and left more services publicly available than would have been safe. The criminals took advantage of the opportunity, penetrated the virtual server, and encrypted its contents.

The company took the virtual server offline, restored the encrypted data from a backup, and the criminals had to accept defeat.

LIGHTNING NEVER STRIKES THE SAME PLACE TWICE?

In the summer of 2022, one company was hit with ransomware twice. In both cases, it was possible to restore the data from the backups, but the work of the company was still significantly disrupted by the attacks. As the server was down, the customer management programs that depended on it were not working either.

The attacks were likely successful because the network device management interfaces of the company were publicly available, and the attacker was able to take over the account of one user.

In addition, the passwords in the company were too short and did not contain enough characters or symbols. Cracking such passwords is relatively easy for an attacker – several possible examples already exist in attack dictionaries. There was also no expiration date set for the passwords. After gaining access, the data of the company was encrypted with ransomware called Phobos. A case like this is a reminder of the importance of following the basics of cyber hygiene.

In the second half of the year, we saw a relatively new threat called the Royal ransomware, which hit a company operating in the energy sector. During the attack, both the workstations and servers of the company were infected. The spread of the malware was limited to the office network – production and end users were not affected.

In November, criminals attacked an Estonian company that provides services to vital service providers. Thanks to the quick response, the worst-case scenario was prevented and the attacker did not reach the systems of the partners of the company.

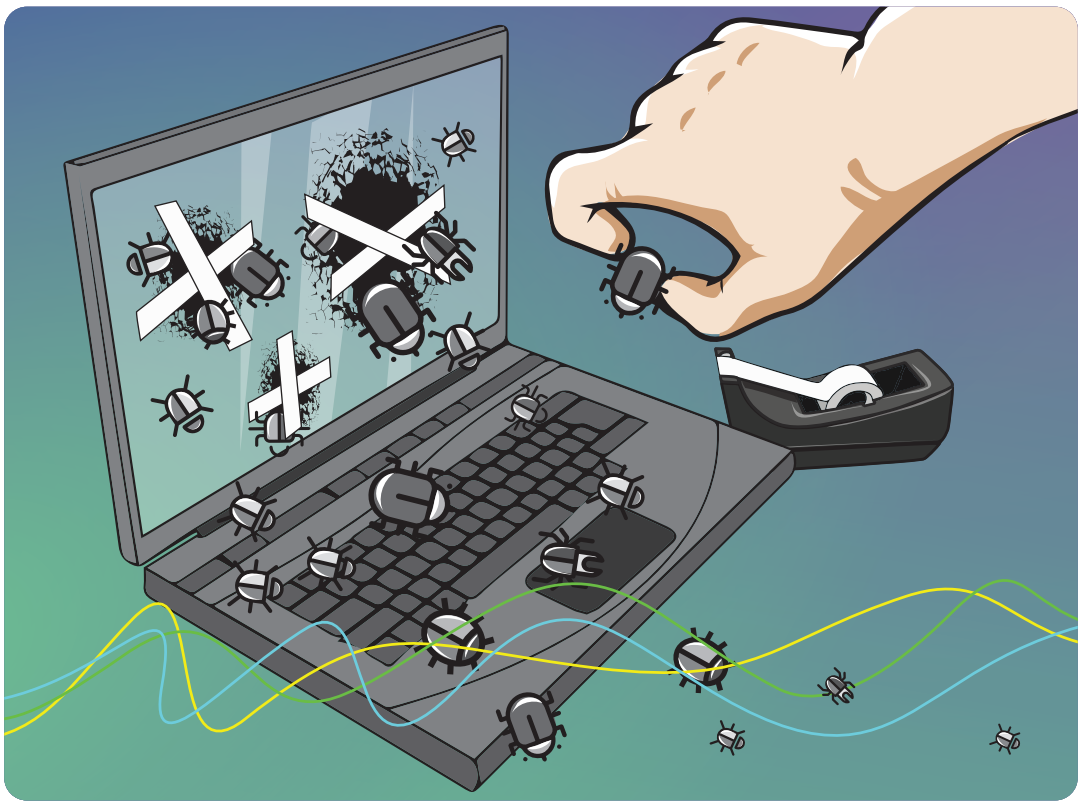
DO NOT PAY THE CRIMINALS. INSTEAD, INFORM CERT-EE

We remind everyone to not cooperate with criminals in the event of a ransomware attack. Paying the ransom does not guarantee data recovery, but it does give criminals more incentive. If your company or agency has fallen victim to a ransomware attack, write to **cert@cert.ee.**

The ROOT of the problem

In more than half of the cases, the attackers penetrated the systems of the victim via Remote Desktop Protocol (RDP). In March 2022, we published a threat assessment providing guidance on securing the remote desktop protocol.

1. Use a virtual private network (VPN).
2. Allow connection only from specific IP addresses.
3. Use two-factor authentication.
4. Limit the number of failed authentication attempts.
5. Update the software.
6. Use secure passwords and update them regularly.
7. Configure and monitor logs.
8. Set up monitoring and notifications.



More vulnerabilities, LESS IMPACT

Last year, the capability to identify security vulnerabilities, fight against them, and report them increased significantly.

First, the bug bounty programme was launched in 2022. Through the programme, CERT-EE was informed about the vulnerabilities threatening Estonian organisations much more than before: in 2021, we sent 1,473 notifications related to security weaknesses. Last year, however, we sent 2,634.

Second, we implemented an additional layer of protection to the state network, which blocked hundreds of millions of attack attempts. This also includes attempts to find security vulnerabilities and exploit them.

Third, RIA started to publish regular overviews in September of the most important security vulnerabilities of the week that may also affect Estonia. We publish them weekly on the RIA blog and website.

Even though 2022 did not offer attackers as

many high-profile security vulnerabilities as 2021 (such as Log4Shell or Microsoft Exchange's ProxyLogon and ProxyShell vulnerabilities), there were still a couple that attackers could have used to cause a lot of damage. For example, such vulnerabilities were discovered in Magento, Confluence, and Microsoft Exchange, which are widely used in Estonia.

OVERLY EXPOSED E-SHOPS

After the records set during the coronavirus period, the use of e-shops among Estonians showed a slight decline in 2022. Yet, they are still popular. This leads us to Magento, a widely used e-commerce platform in Estonia. In February and October, security vulnerabilities in the Magento were disclosed. These allowed attackers to completely take over e-shops which used the respective software and put malware on the affected servers or use the compromised e-shop for phishing to steal the credit card data of the customers.

In total, CERT-EE notified the owners or administrators of websites affected by the Magento security vulnerabilities 588 times in February and October. CERT-EE is not aware of any specific significant incidents related to these vulnerabilities from the past year.

SPRING4SHELL – THE NEW LOG4J?

In April, it was discovered that a new vulnerability called **Spring4Shell** is circulating on the Internet. In retrospect, was there reason to be afraid? Yes and no. The aptly-named vulnerability, similar to Log4Shell, was related to the Java programming language framework and allowed attackers to execute malicious code on vulnerable systems. The relatively widespread use of this framework in various applications around the world made the vulnerability more dangerous. Thus, several prerequisites for a security vulnerability with a severe impact were seemingly there.

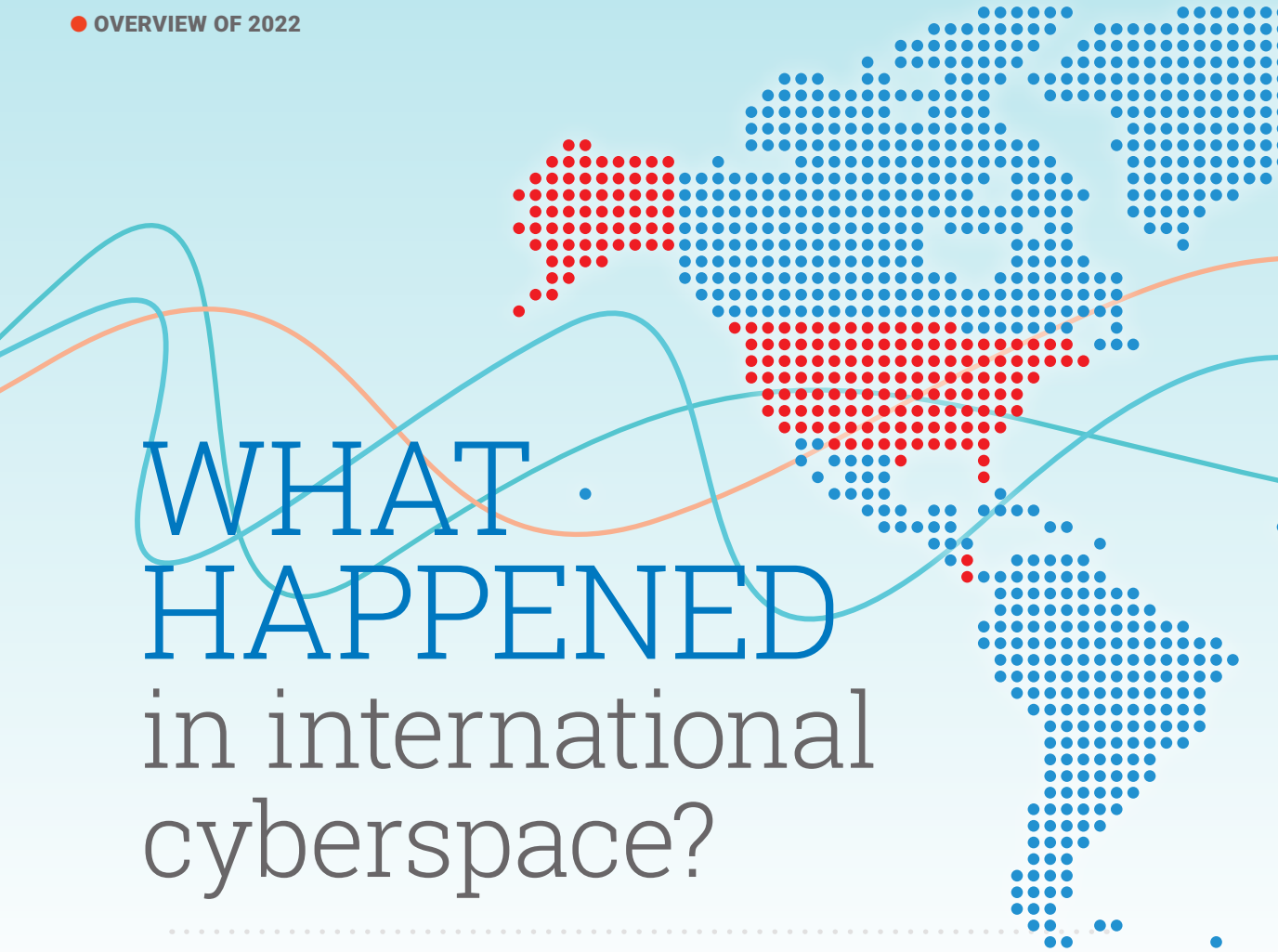
RIA responded immediately and alerted both partner agencies and the public of the potential impact and provided guidance on what to do to address the security vulnerability. We monitored cyberspace and collected information about attack attempts, but the impact of the vulnerability remained marginal in Estonia (and the world). RIA saw that criminals tried to exploit the vulnerability, but the extent of these attempts was far lower compared to other security weaknesses. Despite this, Spring4Shell is still likely to be used in the future. For example, the new botnet Zerobot has added the vulnerability to its arsenal.

CONFLUENCE – WE MET AGAIN

In June, Atlassian reported a critical vulnerability in the Confluence corporate software. It is probably not the first time that the reader of the RIA yearbooks hears about Confluence — in 2021, we also wrote about a critical vulnerability that affected the same software. As it is used relatively widely in Estonia, any critical vulnerability concerning it is also a potential cyber security threat for organisations operating here.

The vulnerability was used to mine cryptocurrency using the compromised systems around the world and could be abused to take over entire systems or carry out ransomware attacks. Fortunately, the effect of the vulnerability in Estonia was minimal. As far as RIA is aware, attackers managed to exploit the security vulnerability in only one case, when a financial company was successfully attacked. In this incident, the vulnerable system was successfully compromised just a few hours after the vulnerability became public. Although the incident had no major consequences, it shows how quickly vulnerable systems are found and attacked today.

In this incident, the vulnerable system was successfully compromised just a few hours after the vulnerability became public.



WHAT HAPPENED in international cyberspace?

In 2022, international cyberspace was shaped by developments related to the Russian invasion of Ukraine, but cyber criminals and state-sponsored cyber groups continued their usual activities elsewhere as well.

In summer, **Albania** was hit by two significant waves of cyber attacks. In July, the websites and e-services of state agencies were offline for hours. In September, the computer systems of the police were targeted, which meant that the computer systems of ports, airports, and border crossings also had to be shut down. Albania says Iran's state-sponsored hackers were behind both attacks. The first attacks on Albania took place before the conference World Summit of Free Iran, which was linked to an Iranian opposition group based in Albania. A day before the scheduled start of the conference, it was postponed due to the threat of terrorism.

Following the cyber attacks, **Albania** severed diplomatic relations with Iran. NATO allies expressed solidarity with Albania and condemned malicious cyber attacks on the critical infrastructure of the country. Solidarity was also expressed by the European Union.

The digital infrastructure of **Montenegro**, the neighbour of Albania, was also hit with an unprecedented cyber attack in summer. The country was hit by both denial-of-service (DDoS) and ransomware attacks, knocking out many critical services (including transport and water services). For example, the power grid of the country was switched to manual mode.

While Montenegrin officials initially announced that Russian special services were behind the attacks, a criminal cyber group using Cuba ransomware later claimed responsibility. According to various cyber experts, the Cuba ransomware group is not connected to Cuba, but is managed by Russian-speaking people.

The incident in **Costa Rica** was also notable: a state of emergency was declared due to ransomware attacks that hit the systems and services of the country. The ransomware group Conti claimed responsibility for the attacks, demanding 10 million dollars from Costa Rica for the decryption key. The ransom was not paid and the country tried to restore the systems in a different way, but even a month later, the services of the Ministry of Finance, the General Customs Administration and the General Tax Administration, the Social Security Fund, and several other agencies were disrupted.

Interruptions of the digital services of the state understandably also affected the work of the private sector. For example, import and export documents could not be declared in the General Customs Administration, which meant that documents were completed manually at the borders. This took significantly longer than usual and the food items spoiled due to the long wait. The declared state of emergency allowed the government to implement more efficient measures to act in the crisis.

CYBERCRIMINALS TARGETED EUROPEAN COMPANIES AND AGENCIES

Last year, cybercriminal groups actively targeted critical entities, hospitals, educational institutions, local governments, and other organisations around the world. One of the most active groups was **BlackCat**, whose ransomware attacks caused financial loss and inconvenience in many parts of **Europe**. For example, in early February, the group claimed responsibility for an attack on the **German** oil and gas storage company Oiltanking. Due to the attack, the func-

→

tioning of the IT systems of the company was disrupted. Mabanaf, an oil trading company belonging to the same group, was also hit. The services of the companies are used by the oil and gas company Shell, which had to switch to an alternative supply chain due to the disruptions.

The public sector was also targeted – for example, the systems of the **Austrian** state of Carinthia were attacked. According to public information, the website and email system of the state were out of order, and the administration could not issue passports or traffic fines. The criminals demanded five million dollars for the decryption key, but according to the state, the ransom was not paid.

Local governments in other European countries also fell victim to cybercriminals. For example, the systems of the **Belgian** city of Antwerp were out of order because the company that provided IT services to the city was hit by a ransomware attack. City services for residents, schools, kindergartens, and the police were disrupted. There were also some problems with the telephone lines and the email system. Among others affected were nursing homes for the elderly, which were unable to use software to help keep track of who should receive what medicine. This meant that 18 nursing homes had to use paper and pencil to keep track.

RANSOMWARE FORCED HOSPITALS TO DIVERT PATIENTS

French hospitals were affected by cyber attacks last year. In August, the Center Hospitalier Sud Francilien (CHSF), a 1,000-bed hospital, was hit by a ransomware attack, which knocked out business software, recording systems, and information systems related to patient admissions. Patients requiring emergency care and radiology services were redirected to other hospitals in the area. Operating rooms were also affected by the technological outage.

A few months later, another French hospital in Versailles had to cancel surgeries and send patients to other hospitals due to a cyber attack. The phone lines, Internet, and computer systems of the hospital were out of order. Additional employees had to be called into the intensive care unit because, although the machines there were working, they were not connected to the network and therefore needed more monitoring. According to the French Minister of Health, almost the entire work of the hospital had to be reorganised due to the cyber attack. The criminals demanded a ransom from the hospital to decrypt the systems, but it was not paid.

PROTESTS IN IRAN SPURRED HACKTIVISTS INTO ACTION

Pro-Western hacktivists from the Anonymous group were politically active in many parts of the world last year. For example, in response to the death of 22-year-old Iranian Mahsa Amin, an operation called OpIran was launched. Amin was arrested by Iranian police for allegedly wearing a hijab improperly. She died at the station – police say it was due to heart failure. After the incident, many Iranians began to protest against the authorities.

During the OpIran campaign, Anonymous attacked Iranian government websites, including those of the intelligence services and police. In addition, the hackers leaked sensitive information, such as the phone numbers and emails of officials and maps with sensitive information.

The Atomic Energy Organisation of Iran said that hackers working for a 'foreign country' broke into its branch network and gained access to its email system. The attack was claimed by a little-known hacker group called Black Reward, which demanded Tehran to release political prisoners as 'ransom'. According to the hackers, they leaked 50 GB of data, including internal correspondence, contracts, and construction plans for the Bushehr nuclear power plant in Iran. Due to the protests, the state authorities began to restrict Internet access. In response, hacktivists began distributing tools and advice to Iranian protesters on Telegram, Signal, and the dark web to avoid Internet censorship, which included offering proxy and VPN servers.

DATA LEAKS LED TO AMENDMENTS IN LEGISLATION

Last year was a wake-up call for **Australia** in terms of cyber security. Namely, in autumn, Optus, the second largest telecom company in Australia, announced that the data of nearly ten million customers had been stolen from them due to a cyber attack. According to the com-

pany, the data of current and former customers, including their names, dates of birth, home addresses, phone numbers, email addresses, and passport and driving licence numbers, were leaked. The alleged attacker published samples of the stolen data online and demanded a million dollars' worth of cryptocurrency for not leaking the rest. A few days later, the hacker released the details of more than 10,000 people, but in an unexpected twist, they soon deleted them, dropped the ransom demand, and apologised to Optus. Optus did not pay the hacker, but cooperated with law enforcement.

A few weeks after the Optus leak, the Australian health insurance company Medibank also announced that in a recent ransomware attack against them, hackers gained access to the personal and health data of all 2.8 million customers. As Medibank did not pay the ransom to the group, the criminals began to disclose the stolen health and personal data. According to the Australian Federal Police (AFP), they identified the hackers in cooperation with Interpol – they were Russian cybercriminals.

These incidents prompted Australia to tighten its cybersecurity and data protection laws, such as significantly increasing fines for companies for data breaches.

EUROPEAN CYBER POLICY TOOK SEVERAL STEPS FORWARD

Last year brought significant developments in the cyber policy of the European Union, which will directly affect Estonia in the coming years. For example, the Member States of the European Union adopted the new network and information security directive, or the so-called cyber security directive (abbreviation NIS 2.0). Compared to the current one (the so-called NIS 1.0), the new directive states more sectors that are critical for the functioning of the economy and society and should contribute to their cyber security.

These include, for example, waste management, postal and courier services, the space industry, the chemical industry, charging points for electric cars, the public sector, and many others. In addition to the new so-called critical sectors, with the NIS 2.0 directive, stricter cyber security requirements will apply to critical entities, the levers of state supervision will increase, international cooperation will be enhanced, and much more.

Another significant development in the cyber policy of the European Union was the start of negotiations on a Cyber Resilience Act, which should make the digital products of Europeans more secure in the future. Under the new proposal, all digital products – software and hardware – produced and sold in the EU would have to meet certain high cybersecurity requirements. This would cover almost all digital products, including computers, smartphones, smart watches, children's toys, etc.

EVENTS abroad

- **Uber** fell victim to a cyber attack. An 18-year-old hacker gained access to the internal systems of Uber and the documents there, including vulnerability reports. The attacker reportedly used the Slack environment of Uber to notify employees of the hack.
- The largest train operator in **Denmark**, DSB, had to stop train services for a few hours due to a cyber attack. The criminals targeted its IT service provider Supeo, which was forced to shut down its servers, meaning that DSB was unable to use the train control software.
- The print version of the **German** newspaper *Heilbronn Stimme* was not published for four days because the printing office of the media group was hit by a ransomware attack. According to the IT manager of the publication, a good backup strategy saved them from the worst, thanks to which they managed to restore production-critical systems relatively quickly.
- In the **Netherlands**, 120 dental practices were closed for days due to a cyber attack. Colosseum Dental Benelux, which has a total of 130 branches in Belgium and the Netherlands, was the target of the attack.
- The **US media company** News Corp fell victim to a cyber attack, as a result of which (allegedly) Chinese hackers gained access to the emails and Google Docs materials, including article drafts, of the journalists and other employees. The company owns several publications, such as *The Wall Street Journal* and the *New York Post*.

TELIA: cyber threats are growing

The number and complexity of cyber threats has been constantly increasing. The pandemic years as well as political tensions and the war in Ukraine have contributed to this, writes **Aigar Käis**, Head of Security at Telia.

Looking back on 2022, we can say that both attackers and defenders became smarter. Cybercrime continued to develop rapidly, but at the same time, we were able to deal with it increasingly well and repel attacks. We learned a lot of valuable lessons, which we can use as a basis to strengthen the defence capabilities of our customers in 2023.

Photo: Telia

Aigar Käis

SMALL COMPANIES ARE MORE VULNERABLE IN CYBERSPACE

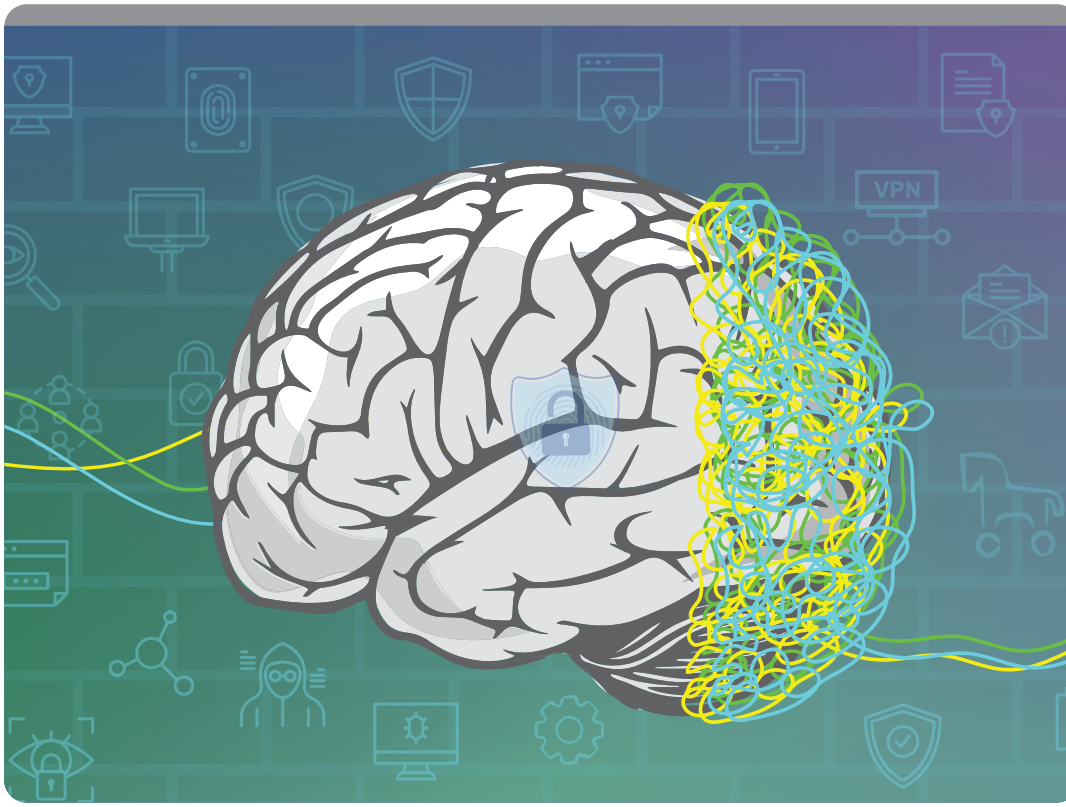
For companies, one of the most significant trends in 2022 was a significant increase in denial-of-service (DDoS) attacks. These attacks often resulted from political decisions and actions. For example, the decision of Finland and Sweden to join NATO led to a massive wave of attacks towards these countries. Similarly, cybercrime increased in Estonia in response to decisions to move the tank monument from Narva, stop broadcasting Russian TV channels, etc.

Unfortunately, we will see the same trend continue in 2023 – criminals will update and diversify their toolbox, and the politically unstable situation and related decisions will continue to affect the intensity of attacks.

DDoS attacks are mostly targeted at the larger public and private companies: disruptions in their services produce a quick and visible effect. In addition, massive automated attacks are also carried out on companies. In these cases, the size of the company does not matter – the purpose of such attacks is to look for security vulnerabilities through which they can enter the systems of the company.

Because large companies often have better defences, small companies are often easier and more profitable prey for cybercriminals. If the phishing attack is successful, it is usually followed by the installation of malware and a ransom demand.

In order to keep criminals at bay, you should first ensure that the network of the company is protected, but it is also important to protect the devices. As many workplaces are no longer stationary and work is done outside the secure network of the office, it is necessary to install



modern anti-virus protection on computers and smart devices. In addition, we must keep in mind that no matter how powerful the security solution is, humans are still the weakest link in the chain. In other words, raising employee awareness plays a key role in mitigating cyber risks.

THE IMPORTANCE OF A MENTAL FIREWALL

Cybercrimes against and attacks on private individuals are also still common. These include scam calls, all kinds of fraudulent campaigns spread by means of emails and messages, etc.

The best protection and recommendation is building a mental firewall for yourself – raising awareness, a critical mind, the ability to distinguish between wrong and right, and a 'think before you act' are useful approaches. At the same time, you should also be careful when choosing devices. Preference should be given to manufacturers who invest in the security of their devices. In addition, you should always make sure that the device has a functioning regular security update cycle.

The best protection and recommendation is building a mental firewall for yourself.

The cyber world around us is becoming increasingly complex. We must actively raise awareness among both companies and individuals. It is also important for every company to find a competent partner who can help identify cyber risks and come up with proactive and flexible solutions, because every company and every attack has its own specifics that must be taken into account. Investments in cyber security will definitely pay off and must continue to grow in the coming years.

Comprehensively cyber-secure ESTONIA

In order to create a cyber-secure Estonia that can withstand technological developments and possible threats, we need to cooperate, writes **Liisa Past**, National Cyber Director and Department Head at the Ministry of Economic Affairs and Communications.

When talking about cyber security in 2023, we must also mention the events of 2022, most remarkably the full-scale invasion of Ukraine by the Russian Federation. The changed threat situation demanded a quick response both in terms of the information security of organisations and national security. RIA contributed significantly to minimise the impact of cyber attacks on Estonian people and information systems. For example, massive denial-of-service attacks were stopped largely before they could do any damage.

Photo: Kristi Sits

Liisa Past

2023 will hopefully be the year of cleaning up. Last year, we learned some lessons on how to ensure the best possible cyber security and saw how even in the most difficult moments, Ukraine was able to protect its information systems and keep e-services running. When ensuring national cyber security, we ask ourselves what threats and scenarios we need to be prepared for and how we protect our society – people, services, information systems, and everything necessary for them – in the event they materialise.

Our goal is a comprehensively cyber-secure Estonia that can deal with technological developments and possible threats as well and as flexibly as possible. This year, we want to agree on and adopt a national cyber security strategy for the years 2023–2027 so that everyone knows how to protect themselves.

EVERY PIECE COUNTS

Cyber security is like a patchwork quilt consisting of many pieces: the security measures of agencies or companies, centrally provided protection solutions, requirements, and norms, and threat-aware and IT-conscious end users. Separately, none of them provide sufficient protection, but together, they form a shield that is difficult to penetrate.

This means that achieving a cyber-secure Estonia is the responsibility of all IT and digital service providers, those who depend on such services, and the state centrally. This approach requires input from all parties.

In doing so, we should organise several things centrally. RIA (CERT) is responsible for monitoring the .ee domain. The information security standard E-ITS and several services are also centralised. When it comes to the central services of RIA, the Estonian IT Centre, and other IT centres, the information security factor is built in and they cannot be offered or ordered without it. Information security also plays a key role in the national IT development model.

However, each service provider must be responsible for its own services and systems. Risks must be managed and security must be part of the design of services and systems. Security is not an end in itself, but a means. Without it, there is no trust, and without trust, there is no service.

CERTAIN UNCERTAINTY

We do not know what the technology around us will be like in five or ten years, but we work hard to ensure that Estonian society is ready for future developments and threats and that our e-services and environment remain secure. Among other things, this means continuous work to get rid of legacy systems and a transition to more flexible IT operating models. We also review current regulations to support the implementation of modern technologies and the creation of a more secure cyber environment.

Cooperation is a prerequisite for ensuring the cyber security of Estonia or the information security of any system. For the national cyber security team of the Ministry of Economic Affairs and Communications, this means, first of all, that we do everything described above in cooperation: by involving and consulting other interested parties. Regardless of what the year 2023 will look like in terms of geopolitical and technological developments, the people of Estonia will be best protected against cyber threats if we work together. Therefore, whenever and wherever you can, join us to discuss and think along to make Estonia safer together.

CHALK, CHEESE, and the Cybersecurity Act

At first glance, cyber security and migration are as different as chalk and cheese. However, Russian aggression in Ukraine has resulted in a number of unpleasant lessons, which means we will have to cram the two together into one chapter in national risk analyses in the future, writes **Uku Särekanno**, Deputy Executive Director of Frontex.

Criminals attacking vital services and the continuity of e-society aim to sow confusion and reduce resistance. It is a systemic part of both preparatory and supporting activities for kinetic warfare and a cheap tool, the use of which can be conveniently delegated to criminal associations, publicly washing your own hands clean of responsibility. A country under attack is forced to resort to measures in the event of a major crisis that provoke public criticism in a democratic state governed by the rule of law.

Photo: Arno Mikkor

Uku Särekanno

WHAT HAPPENED THERE...

In the summer of 2021, hundreds of migrants simultaneously started arriving in Lithuania illegally through Belarus. A state of emergency was established. and by the end of the summer, more than 4,000 immigrants had arrived in Lithuania. The local governments had serious difficulties in accommodating them. They wanted to follow the rules in force, starting with the right to asylum and ending with requirements for detention centres.

There was no doubt that the migration flow towards Lithuania was organised deliberately and, in this case, not only with the help of human traffickers. This was confirmed by Frontex footage that reached the international media at the height of the crisis, showing Belarusian officials transporting citizens of third countries to the border. It was all an orchestrated security operation by the Lukashenko regime.

Lithuania did what it could. The border was closed, its security was strengthened, and access to international protection became significantly more limited. In less than a month and a half, the crisis intensified in the direction of Poland, escalating in December 2021.

... WILL HAPPEN HERE

The parallel with cyber security is obvious, as the modus operandi of the criminals is similar. And it cannot be ruled out that the criminals behind the attacks are the same people. Belarus has so far been one of the few to publicly state that it uses migration to exert political pressure. Although other dictators have made similar statements in the past, the campaign against Lithuania and Poland was essentially something new. It is no secret that the whole campaign was a result of the cooperation of organised crime and security agencies.

It is only a matter of time before what happened in Lithuania and Poland happens in Estonia. We have to be ready from both a legal and an operational point of view. The Russian border is guarded by the FSB. It is an agency that is a successor to the KGB and reports directly to the presidential administration. If a few thousand immigrants reach the green border of Estonia, we are dealing with a security operation, unless the refugees are Russians themselves or Ukrainians when events escalate. Preventing such an operation requires very fast and resolute action, which means suspending or restricting several rights.

Estonia has developed a legal framework for a scenario where migration is used as a weapon against the state. Similar to Lithuania, the situation is approached from a security point of view, for which we are largely responsible on our own. Estonia also practices cooperation with Frontex, which is important to respond to a crisis jointly and under the European flag. This way, the European public can see that what is happening is not only our problem, but a problem for all of Europe. It also ensures that we can rapidly deal with evidence, countermeasures, and hybrid attacks.

HOW DOES THIS RELATE TO CYBER SECURITY?

Similar to migration, we should really think about developing cyber security legislation. We should assess whether the Cybersecurity Act adopted five years ago is sufficient in the context of hybrid warfare and whether the measures described in it and the responsibility and capabilities bestowed upon RIA take into account the new security situation.

In the case of migration, we have special measures, the operational capacity of internal security agencies, and the support of Frontex. Hopefully, European countries also have a clear understanding that what happens at the external border directly affects everyone, because there are no internal borders in the Schengen area.

The structure is similar for cyber security – special measures, operational capability, and building shared responsibility with like-minded people. It is important that we are not left alone in a cyber crisis, will be able to attribute swiftly and that everyone quickly realises that, similarly to the migration crisis in Lithuania, a cyber attack against a Member State is also an attack against the whole of Europe.

This article expresses the personal views of the author.

The new tools of CERT-EE protect Estonian cyberspace

Last year, we took several important steps to improve the security of Estonian cyberspace: the state network got an additional layer of protection, we implemented additional measures against denial-of-service attacks, and we have taken a closer look into the dark web.

For many years, a large part of the Estonian public sector – ministries, agencies, and local governments – has been using the state network, which offers fast and secure data communication. The Estonian internet exchange point (RTIX) also belongs to the state network, which enables internal data exchange directly between telecommunication service providers.

In 2022, RTIX underwent an upgrade – its equipment and architecture were modernised, resulting in improved reliability and speed of data exchange. The possibility of malicious interference with internet traffic within Estonia also decreased.

THE STATE NETWORK BECAME MORE SECURE

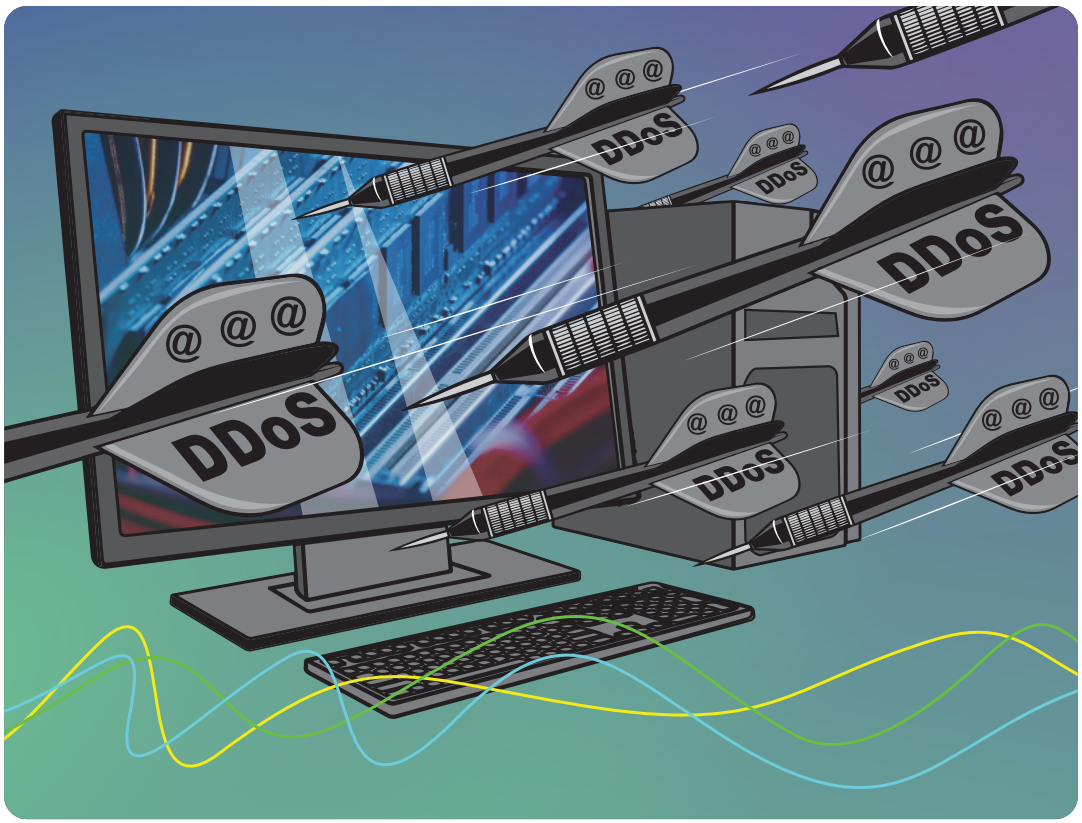
As the state network is managed by RIA, CERT-EE is able to detect attack attempts directed at the state network and all kinds of malware that are used to attack its customers. In February 2022, RIA implemented an additional security layer for all users of the state network, which offers more effective protection against attacks without slowing the connection down.

The new security filter detects potential threats and blocks attack attempts before they reach the end user – there are millions of such prevented attacks, blocked threats, or vulnerability exploitation attempts recorded every month. Using an analogy from the ordinary world, it is like an invisible filter in front of the living room window, which prevents dust, pollution, and pathogens from getting inside, thus protecting the health and well-being of all residents.

ADDITIONAL PROTECTION AGAINST DENIAL-OF-SERVICE ATTACKS

We have previously noted in our yearbooks and other publications that, as in many other fields, there is a constant race between attackers and defenders in cyberspace. Just like the private sector, the state must be flexible and agile, and last year, it succeeded on several occasions.

In 2022, a wave of denial-of-service attacks hit several websites that are important or symbolic



for the people of Estonia, with the aim of temporarily shutting them down. Most of them did not have any significant impact because the owners of the websites and services had prepared for such attacks and introduced an additional layer of protection through CERT-EE. Denial-of-service attacks are carried out in different ways, so the defence must also be versatile.

Without burdening the reader with technical details, we can say that although Estonia was at the top of the world in terms of the number and intensity of certain types of DDoS attacks last year, the defence generally held up and the efforts of the attackers were in vain.

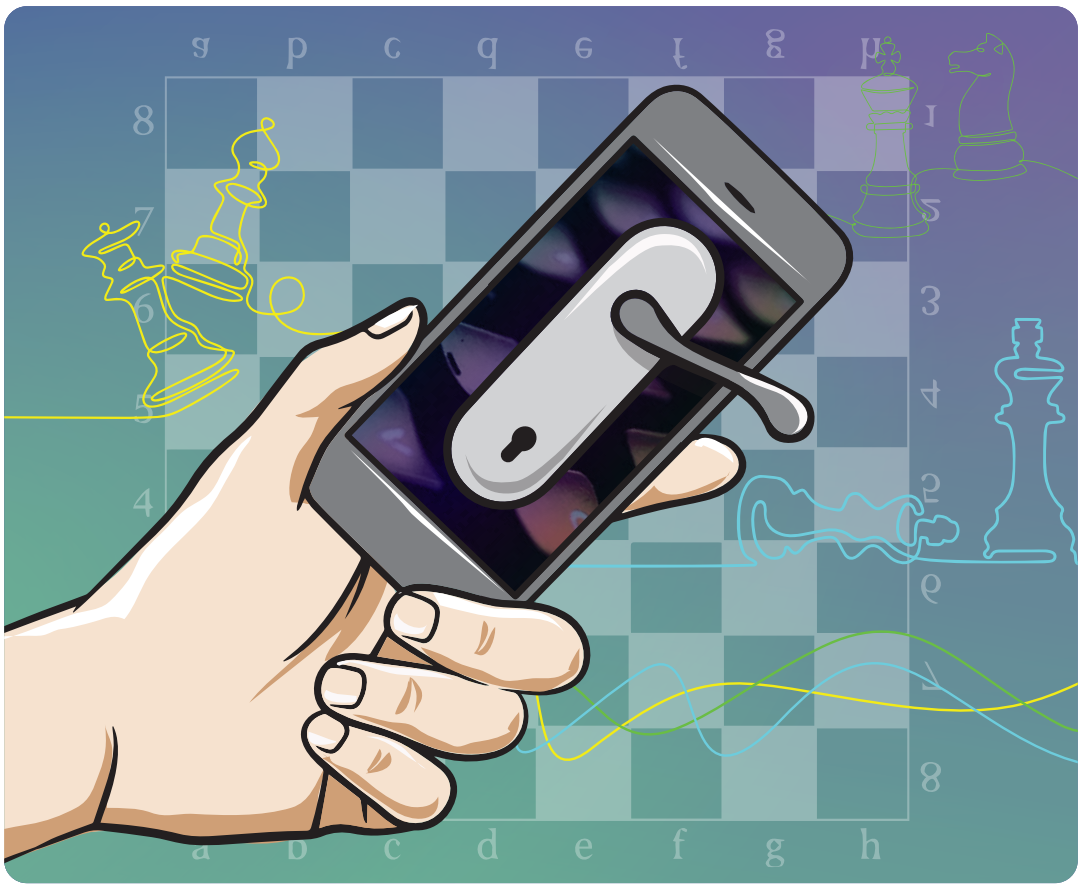
KNOW YOUR ENEMY

Modern cyber security requires not only the construction of defensive walls, but also knowing the motivations and logic of the attackers, as well as the opportunities available to them. RIA cooperates with other agencies in this area, but our own respective capabilities also made a leap in development in the past year.

Denial-of-service attacks are carried out in different ways, so the defence must also be versatile.

The so-called backroom of CERT-EE includes people who monitor what is happening on the dark web and also keep an eye on what is happening in the hacktivist community. In addition, CERT-EE now includes a Red Team to help RIA customers identify and fix vulnerabilities in their networks before criminals do.

Sound intriguing? Write to **cert@cert.ee** and find out more.



Looking for RIA`s vulnerabilities

As far as we know, RIA is the first state agency that openly asks 'cyber criminals' to consistently challenge it.

In the spring of 2022, RIA signed a continuous red teaming (CRT) contract. This means that the contract partner Clarified Security regularly tries to break through the defences of RIA.

Using the vocabulary of the construction industry, classic penetration testing is comparable to the activities of an inspector who assesses whether the doors and windows of a house are secure and, if necessary, advises whether and where additional locks need to be installed. Using the same analogy, red teaming is comparable to the activities of a classic criminal. They do not care that the windows and

doors on the ground floor are securely locked. They notice a balcony window upstairs, which the family has either accidentally or deliberately left open, and head to the balcony to break into the rooms to look for valuables – the quieter the better. In other words, the purpose of continuous red teaming is to get a complete overview of the risk areas. This, in turn, helps us to better protect RIA.

As far as we know, RIA is the first state agency in Estonia that has a contract for continuous red teaming. When it comes to CRT, four teams are distinguished. The red team looks for security holes and vulnerabilities and attacks. The blue team prevents and repels attacks. The purple team is a joint team of the members of the offensive and defensive teams that notices vulnerabilities in real time. The white team is in the role of liaison officer and solves so-called current problems.

RIA's PHISHING CAMPAIGN

Every RIA employee knows that all it takes is one wrong click for the criminal to get into your systems. That is why the Information Security Department of RIA places great emphasis on raising the awareness of its employees. In the summer of 2022, the Information Security Department and CERT-EE organised the first major phishing campaign for RIA employees, where colleagues were enticed to click on a suspicious link.

The goal was not to point fingers, but to get an overview of the current situation. It is unrealistic to expect that no person will ever click on any malicious link, but the goal is to reduce the number of such clicks through continuous prevention and awareness-raising.

JOINT COOPERATION PHASE

RIA and Clarified Security are currently in the phase of joint cooperation – this means that, together with the attacker, we are trying to understand where RIA is vulnerable. We have not yet moved into a sustained attack phase because we want to make sure our level of maturity as an agency is worthy of it.

> We have not yet moved into a sustained attack phase because we want to make sure our level of maturity as an agency is worthy of it.

Broadly speaking, CRT focuses on specific segments that are mutually agreed upon in advance. The other party has certain rules that they follow. We take it step by step with the aim of making sure that the developments are monitored and/or prevented.

Red teaming is not used for RIA's services offered to the general public. In the case of public services, classic penetration testing is applied, during which no personal data is processed.

Cooperation with Clarified Security is going well. It is no secret that CRT excites the information security team members of RIA, because the opposing team is really good and puts the technical knowledge of our people to the test.

PROTECTING THE CROWN JEWELS

The experience of continuous red teaming so far has been very educational and eye-opening. We naturally cannot go into detail, but there are things we can do differently, both in terms of content and process, to protect our crown jewels even better.

We also recommend other state agencies to use the CRT service and review their monitoring capabilities, because the situation in Estonian cyberspace is quite heated due to the war in Ukraine. There are still few red teaming service providers on the Estonian market, but several companies are creating this capability in the near future.

Towards a more cybersecure Estonia with PREVENTION CAMPAIGNS

In 2022, we conducted two major information campaigns to improve the cyber hygiene of Estonian residents. In summer, we focused on people who speak Russian as their native language, and in autumn, we called on all Estonians to be more IT-conscious.

The cyber hygiene of Estonian residents of other nationalities is significantly lower than average, and the use of the best practices of cyber security decreases with age. We based our choice of messages and target groups for our prevention campaigns on these conclusions, which are based on the data collected by Statistics Estonia.

RADIO PROGRAMME *ENTER PASSWORD*

At the beginning of the summer, we launched the Russian-language radio programme *Введи пароль* (*Enter Password*). Listeners were informed about the dangers and concerns in cyberspace and their personal responsibility in preventing and dealing with the consequences of cyber incidents. The cyber security programme, which aired on Raadio 4 over the summer, proved to be very popular. Nearly 45,000 people listened to each episode of the 13-part programme.

In parallel with the radio programme, we organised a cyber security awareness campaign aimed at the Russian-speaking population, which conveyed basic prevention messages to the target group and encouraged them to listen to the aforementioned radio programme. The cyber security campaign achieved very good visibility and coverage, reaching more than 90 per cent of the target audience.

IN OCTOBER, WE LAUNCHED THE *KONTROLLI ÜLE*! CAMPAIGN.

In October, which is Cybersecurity Awareness Month, we launched the nationwide awareness campaign *Kontrolli üle!* (*Check Again!*). It focused on the most common fraud and criminal schemes in Estonia, as a result of which hundreds of companies and people lose money, data, and accounts. We called on people to pay more attention on the Internet – for example, which link they click on, whether they use a strong password and where do they enter it, whether they are convinced that the email they received from a friend was really sent by that friend, and whether what they download from the Internet and install on their computer is safe and necessary.

Nearly four-fifths of Estonians and half of non-Estonians noticed the *Kontrolli üle!* campaign either on TV, radio, outdoor advertising, newspapers, or digital media.

The follow-up survey of the campaign revealed that we made every other Estonian think about cyber issues: 13 per cent of them searched for additional information about cyber security during the campaign and eight per cent took at least one step to increase the cyber security of themselves or their loved ones.

A quarter of the main target group of the campaign, i.e. residents aged 60–74, improved their cyber security during the campaign period.

Data confirms: CYBER HYGIENE is improving

Every spring, as part of the 'Information technology in households' survey, Statistics Estonia examines which measures people use to ensure their security and privacy on the Internet. Fortunately, the data shows a continued increase in cyber awareness among residents.

In 2019, 64 per cent of respondents to the survey by Statistics Estonia said they used stronger passwords than the minimum requirements or different passwords for different accounts. In 2022, this percentage had increased to 71.

Awareness has also increased regarding unexpected emails or messages and the links and attachments they contain. In 2019, 62 per cent of respondents checked links and attachments in emails received from unknown senders. In 2022, however, this percentage had risen to almost 68.

The data of Statistics Estonia does give an idea of the level of cyber hygiene, but does not explain the reasons for cyber-safe behaviour. In order to better understand cyber behaviour, in 2022 we teamed up with the research company Kantar Emor, which studied the cyber behaviour of the 16–24-year-old and 45–54-year-old population at the request of RIA.

People who took part in this survey also pointed out that they protect themselves primarily with different strong passwords and two-factor authentication. However, it turned out that people do not think it is likely they could fall victim to a cyber attack, because they believe that they are sufficiently critical and aware of cyber threats. Unfortunately, overconfidence can dampen the sense of danger. Cybercriminals, who are perceived to be increasingly cunning, are sure to take advantage of this.

A NEW CYBER TEST is being prepared at RIA

In order to improve the awareness of public sector employees of the dangers lurking in cyberspace and teach them to behave more safely, RIA created a new e-learning environment where you can update and check your knowledge in this area.

Although it may sometimes seem like cyber security is the responsibility of IT personnel, it actually starts with the everyday behaviour of an ordinary computer user: what links and files they open, what they download on their computer, where they enter their data, etc.

The largest amount of the incidents registered by CERT-EE are caused by phishing pages, the purpose of which is to get an innocent user to enter their data. Information security specialists can do their best, but if a colleague in the next office enters their password on a phishing page set up by fraudsters or opens malware in an email attachment, it may still not be enough.

EVERY LINK IN THE CHAIN COUNTS

Cyber security can only be ensured with the help of people who are aware of the threats, and it is easiest to prevent those incidents that we can recognise. That is why it is necessary from time to time to review the basic knowledge of cyber hygiene and check your level of knowledge. One of the best ways to do this is an online training, which everyone can complete at their own time and pace.

Since 2017, RIA offered Digitest, a cyber security training platform, which was completed by thousands of government officials. Starting in 2023, we will be offering a cyber test created by us. The test is located on the Moodle platform, which is familiar to many. The purpose of the new cyber test is to raise and maintain the cyber security awareness of employees. The test can be taken by all existing Digitest users, i.e. state agencies, local governments, and employees of family health centres. We also offer the test to the public sector.

FIRST THE COURSE, THEN THE TEST

The new cyber test is divided into two parts. First, we ask the user to work through the training part, which covers a dozen important topics. Many of these include cautionary real-life examples, such as actual phishing emails and scams that have been sent to the CERT-EE team for investigation. These teach the participant of the course to be more aware of various scams and emails with malware and to avoid such phishing attacks more easily.

After completing the course, a test must be taken. Each user will immediately see their

score and receive feedback on correct and incorrect answers after completing the test.

The course provides answers to questions about how to create a secure password, how to recognise phishing pages and emails, what the most common scams are, how to set up a secure home Wi-Fi network, how to ensure the safety of working remotely, etc.

The cyber test does not replace the classroom and the specific trainings of the agency, but it is a good additional tool for organising information security trainings.

HELPFUL FOR THE AVERAGE USER AND INFORMATION SECURITY TEAMS

In addition to the fact that employees learn new knowledge on the topic of cyber security or remember what they have learned before, the cyber test is also a useful tool for the person responsible for the information security of the agency. Based on the results of the test, it becomes clearer to the information security manager of the agency in which areas and questions the employees make more mistakes and which topics require additional training.

The cyber test does not replace the classroom and the specific trainings of the agency, but it is a good additional tool for organising information security trainings.

The goal of RIA is to have all public sector employees pass the cyber test or complete other cyber security training at least once a year. This helps them remember well-known scams and allows them to learn information about new risks.

FREE ELECTIONS are the basis of democracy

In the 2019 Riigikogu elections, the role of RIA was much smaller. We are still responsible for the i-voting electronic ballot box and its protection, as well as the hosting of the systems, but now, we are also tasked with the development, operation, and hosting of the election information system and the protection of the computers of the polling station employees.

Everything has a lifespan, be it a car, a laptop, or a human being. So, the law stipulated that the previous election information system (VIS) had to be replaced for local government council elections, so that the state could introduce electronic voter lists.

There were other reasons for the replacement as well: greater security and better user experience.

The current VIS made its debut in the 2021 local government council elections and meets all current safe development principles. An advanced version of the same system will be used in the 2023 spring elections. The information system is primarily meant for polling station employees and other election organisers. However, others can use it as well.

If they wanted to, candidates could submit their candidacy through the election information system. In addition to managing voter and candidate lists, the system is necessary for counting paper votes in polling stations, preparing results protocols, calculating voting results, and communicating the results to the public. The system also has a public map application, which can be used to find detailed information about polling stations. During the elections, the map will be published on the website valimised.ee.

This means that the system is a place combining the votes cast electronically as well as on paper at the polling station. From there, the results are sent to the website valimised.ee, as well as to media portals. Our task is also to protect the website valimised.ee and the election results website from attacks.

AUDITS AND TESTS

The security of the elections and the reliability of the systems must be ensured in the best possible way. Both the election information system and the electronic ballot box have been repeatedly audited, security tested, and made more secure. In 2022, the information security audit of VIS ISKE and the audit of election processes were also completed, which pointed out the need to specify the roles of various agencies in the election process and supplement documentation

<table>
<tr><th colspan="7">RIIGIKOGU ELECTIONS 2023</th></tr>
<tr><td>Mon.
27/02</td><td>Tue.
28/02</td><td>Wed.
01/03</td><td>Thur.
02/03</td><td>Fri.
03/03</td><td>Sat.
04/03</td><td>Sun.
05/03</td></tr>
<tr><td colspan="6">PRE-VOTING</td><td>ELECTION DAY</td></tr>
<tr><td colspan="4">Voting in centre polling stations
12 p.m. to 8 p.m.</td><td colspan="2">Voting in all
polling stations
12 p.m. to 8 p.m.</td><td rowspan="2">Voting in all
polling stations
9 a.m. to 8 p.m.</td></tr>
<tr><td colspan="6">ELECTRONIC VOTING
Mon 9 a.m. to Sat 8 p.m.</td></tr>
<tr><td colspan="4">Voting on site 9 a.m. to 8 p.m.</td><td colspan="3">Voting at home 9 a.m. to 8 p.m.</td></tr>
</table>

and procedures. No critical weaknesses and deficiencies were identified in the systems.

Before each election event, the information systems are also thoroughly security tested, where the best experts in their field in Estonia try to take down or break into the systems. This is done early enough to eliminate all deficiencies before the election.

We not only test security, but also how systems and servers withstand heavy loads and how user-friendly they are.

ENSURING ELECTION SECURITY

We need to know what is happening with the election information system and the i-voting system throughout the election period. CERT-EE, the Incident Response Department of RIA, monitors our servers and systems 24/7 to detect any unusual interest in them.

We also monitor and protect the working equipment of polling station employees around the clock. In addition, all members of the electoral committee must complete training that includes a cyber threat module and a cyber hygiene test to help remind them of the threats of cyberspace. We also organise similar tests and trainings for candidates and polling station employees.

In 2023, Estonian cyberspace will continue to be a target for attacks – mostly denial-of-service attacks that disrupt the work of services. Criminals are also constantly searching for weaknesses to penetrate systems.

ROLE DISTRIBUTION of elections

- **The State Electoral Office** deals with the organisation of elections both in polling stations and electronically.
- **The National Electoral Committee** carries out supervision and deals with election complaints and violations and matters related to the credibility of elections.
- **The Information System Authority** manages election-related information systems and ensures the cyber security of elections.

We share this knowledge with political parties. RIA offered political parties and individual candidates participating in the elections the opportunity to assess the security of their digital solutions.

MODERN TIMES

Finally, we remind you that the election period for the 2023 Riigikogu elections is continuous, that is, there is no break between i-voting and election day. Voters can also change their i-vote on election day, i.e. 5 March, by voting with a paper ballot at the polling station. The last vote will be valid.

The introduction of the electronic voter list means that the voter is not tied to one particular polling station anymore. They can vote in any polling station within their district.

SUPERVISION: focusing on helping, not punishing

About 13 per cent of the proceedings initiated by the RIA Supervision Department end in precepts. Generally, the defects are eliminated within the agreed time, but sometimes, the company or agency also has to pay a penalty.

Last year, the RIA Supervision Department dealt with 54 proceedings. They mainly involved vital service providers, including liquid fuel, electricity, and gas suppliers, hospitals, and providers of authentication and digital signature certificate validity confirmation services. Other important service providers included, for example, an airport operator and traffic organiser, as well as organisers of cargo and passenger transport and port services.

THREE MOST COMMON PROBLEMS

Although our supervisory officers come across many issues in terms of compliance, three most common problems can be highlighted:

- there is no systematic approach to information security and IT risk management;
- the network does not have a logical structure and has not been described;
- legacy systems and insufficient attention to the detection and elimination of security vulnerabilities in network devices, i.e. the use of software not supported by the manufacturer and unpatched vulnerabilities in systems.

About 13 per cent of both planned inspections and proceedings initiated due to some incidents end in precepts, which are generally fulfilled within the agreed time. On some rare occasions, the identified deficiencies are not eliminated in time, and in that case, the company or agency has to pay a penalty.

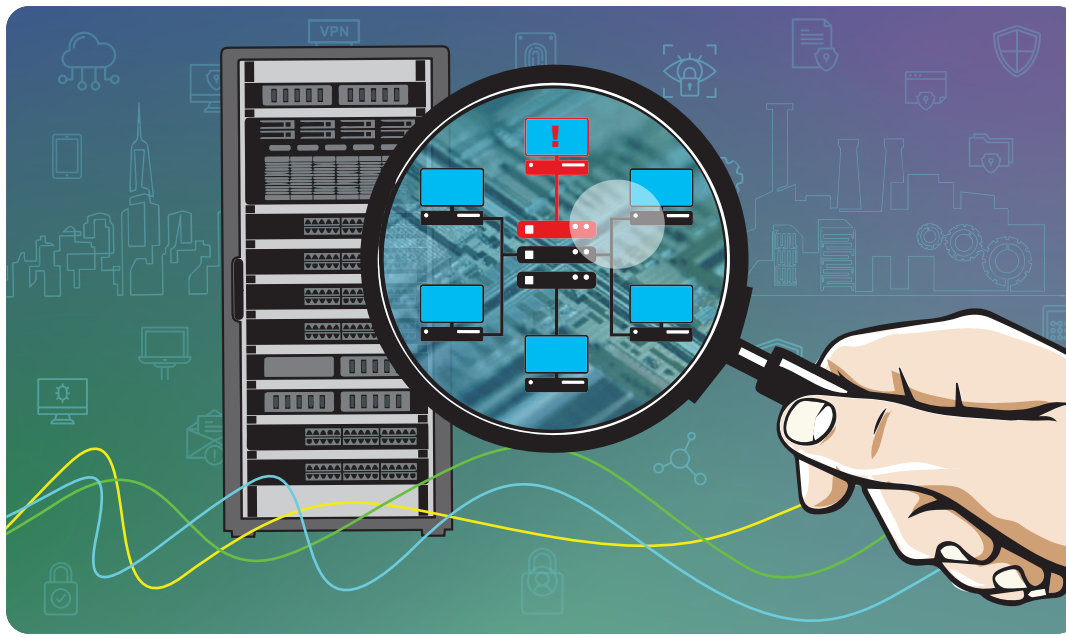
The imposition of a fine or penalty payment is the last measure to direct the attention of the management to information security problems and pressure them to deal with them. Paying it, however, does not save the company or agency from having to comply with the precept – the penalty may be imposed repeatedly until the precept is fulfilled. In addition, failure to comply with cyber security requirements may lead to misdemeanour proceedings, as punishment for which RIA can impose a fine of up to 20,000 euros on a person.

THE PURPOSE OF THE PROCEEDINGS IS GREATER SECURITY

In 2022, RIA issued precepts to six agencies (there were 33 completed proceedings). No agency had to pay a penalty payment (one such case took place in 2021), nor did RIA initiate any misdemeanour proceedings.

The limit of the penalty payment was 9,600 euros until 2021. Now, its limit has doubled, i.e. it reaches 20,000 euros. The payment of a penalty is generally an effective measure, but in some cases, a one-time penalty has not been enough, which is why the subject of the proceedings has had to pay the penalty to the state several times.

Although, pursuant to legislation, RIA super-



vises about 2,000 agencies and companies that either perform public tasks and/or provide important services to them (including energy, communications, transport, water, health, etc.), the department may, from time to time, also supervise smaller companies in the private sector that provide services to local governments. For example, the RIA supervision unit had to issue a precept to a company that provides IT services to many local governments. Security vulnerabilities were discovered in the systems of the company, through which it was possible to access the systems, including data, of the customers of the company. As far as RIA is aware, the vulnerabilities have not been exploited and the possible risks have not materialised. The company addressed the deficiencies pointed out by RIA in its precept.

THIS YEAR, THE FOCUS IS ON FAMILY PHYSICIANS

This year, RIA will visit family physicians and family health centres, as they must start meeting the requirements of the Cybersecurity Act that came into effect in 2018. This involves informing RIA about cyber incidents and ensuring incident resolution and prevention measures, conducting a risk analysis, and implementing other information security measures resulting from the law.

What does the RIA Supervision Department do?

The Supervision Department of the Cyber Security Branch of RIA checks compliance with the requirements of the Cybersecurity Act, focusing on the security measures of network and information systems and their adequacy. All approximately 2,000 agencies and companies that are subject to the Cybersecurity Act are under supervision, including all public sector institutions and vital and important service providers (family doctors, hospitals, electricity and water service providers, communications and transport, etc.). In addition, the department processes applications for activity licences of trust service providers, manages the Estonian trust list, and supervises the fulfilment of the requirements set for the service.

This year, the focus of supervision is on prevention – raising the awareness of doctors about the possibilities and responsibilities. RIA is also planning to organise an information day for family physicians. The 2023 supervision plan also includes inspections of state agencies, including local governments.

Protecting critical INFRASTRUCTURE

A state cannot function if there is no electricity, heating, medical care, or other necessary services. Similarly, it is necessary to protect nationally important data and databases. RIA contributes to the protection of Estonian critical infrastructure and the systems of agencies and companies important for the functioning of the country.

RIA The task of RIA's Critical Infrastructure Cyber Defence Department is to help the agencies and companies that are the most important for the state. We do this through training, testing, and exercises. In 2022, we conducted high-level exercises and training for both vital and important service providers as well as employees of the IT centres of the state.

GLOSSARY

- **Cyber reserve** – a reserve created by RIA, which includes experts from state agencies providing IT services to the Estonian state and the Cyber Unit of the Defence League
- **E-ITS** – the Estonian Information Security Standard, which corresponds to the ISO 27001 standard
- **IT centres of the country**– the IT and Development Centre of the Ministry of the Interior (**SMIT**), the Health and Welfare Information Systems Centre (**TEHIK**), the Information Technology Centre of the Ministry of the Environment (**KeMit**), the Estonian IT Centre (**RIT**), the Information Technology Centre of the Ministry of Finance (**RMIT**), the Centre of Registers and Information Systems (**RIK**), and the Information System Authority (**RIA**)
- **CR14** – a foundation under the Ministry of Defence of Estonia, the purpose of which is to develop cyber security research and development activities in the field of defence

WE HELP TO PREPARE FOR THE WORST

In autumn world-renowned and in-demand trainings focused on digital forensics and industrial automation security took place, each of which lasted six days. The training programme was so intense that some courses even took place on Saturdays. The courses were attended by representatives of vital service providers, IT centres, and the Cyber Unit of the Defence League, who received a comprehensive overview of what to do in the event of an incident, as well as how to collect and store data and conduct an initial analysis.

Employees of vital service providers using automated control systems were grateful for the industrial automation security course. The course showed how systems are attacked, what organisations can do to protect them, and how to ensure that the needs of the business side are met at the same time. The training involved special industrial automation equipment. Each participant had a set of equipment on the table and their own environment in which to perform the exercises.

Another group received an overview of how to properly audit the security of their information systems. The fourth group participated in cyber security and operational continuity trainings based on ISO standards. If you count all the training days organised in the second half of the year, we offered more than 500 man-days of world-class cyber security training.

Our goal is to provide exercises that are as lifelike as possible. One of these was Powergrid, which we organised together with our partner institution CR14. During the five-day exercise, technicians had to set up, attack, and defend equipment used to keep the power network running. Employees of hospitals, telecommunications companies, and banks also received technical trainings and exercises.

SECURITY TESTING HELPS TO PREVENT THE WORST

Both we and the organisations responsible for critical infrastructure have limited resources. Every year, we help to test the security of a handful of companies. By simulating attacks, we and the agency or company itself can see where money, technology, or working hours need to be invested to keep the systems and thus the services running.

Last year, we helped to security test and evaluate the resilience, recovery plans, and work organisation of IT systems of a hospital, a district heating company, and an aviation sector company. Although an attack itself can be very complex, solving it often depends on the working arrangements of the organisation and whether it has established how to deal with such a situation. It is difficult to deal with an error or attack if there are no logs, i.e. an overview of what is done in the systems, or a plan for what to do in such cases.

A CYBER RESERVE that is unique in the world

Under the leadership of RIA, the national cyber reserve was created, which brings together competent IT experts who can solve significant and long-term cyber incidents. The idea to create such a task force was born in 2020, and by the autumn of 2022, the cyber reserve was operational.

The first exercise for the reserve members took place in the largest hospital in Estonia, the North Estonia Medical Centre. The exercise focused on a scenario in which a ransomware attack had been carried out that took down the systems of the hospital. The systems had to be restored as soon as possible because the lives and health of people could be at risk.

The reserve includes IT employees of IT centres and other public sectors, as well as members of the Cyber Unit of the Defence League. If necessary, it is also possible to involve specialists from the private sector. The entire cyber reserve works on a voluntary basis, and the employer keeps paying the experts.

Currently, the reserve consists of about a hundred people. Our goal is to continuously educate and train all members so that they can develop themselves and have the knowledge and skills to help the country in the event of an attack. As the reserve was created in the autumn of 2022, it has not yet been involved in solving real incidents, but looking at what is happening around us, we might have to ask them for help soon.

How to increase THE CYBER COMPETENCE OF ESTONIA?

This year, RIA will take on a more ambitious role in supporting the Estonian cyber community. The goal is to contribute so that more companies offer cyber security services, research is turned into services and products, more specialists get involved, and everyone can have a say in the development of the European cyber ecosystem.

In 2021, a regulation establishing the European Cyber Competence Centre (ECCC) and the network of national coordination centres (NCCs) came into force. The ECCC will be physically located in Bucharest, Romania, and its main output will be the strategic direction of the cyber security fund money of Digital Europe and Horizon Europe. The role of the Estonian national coordination centre (NCC-EE) will be fulfilled by the new Research and Development Coordination Department of the Cyber Security Branch of RIA.

PRACTICAL OUTPUTS

Our focus is on building competences in the field of cyber security. To ensure more cyber security specialists, it is necessary to intervene in the field of education. To ensure that cyber security services are consumed and offered more, we can contribute with grants and the acceleration of start-ups. To ensure that the field of cyber security research is better aligned with the needs of consumers, we commission research and reviews of the security of future technologies from research institutions.

We do not do all of this alone. There are already several communities, initiatives, and forums in Estonia where cyber security specialists, industry leaders, interested parties, and enthusiasts come together to exchange ideas. The goal of RIA is to empower and leverage those initiatives that are already viable, and to provide a broad overview of cyberspace, the vision of our professionals, and opportunities to leverage the domestic and international networks of contacts of RIA. We could not achieve this without Startup Estonia and Enterprise Estonia. We also cooperate with the Tallinn Science Park Tehnopol and the European digital innovation centre AIRE in the field of AI and robotics.

YOU CAN ALSO HAVE A SAY

In addition to cyber security grants, start-ups, trainings, and research reviews, it is important to note that in the long term, through the NCC-

EE project, members of the cyber security community (companies, research institutions, and of course also private individuals) should be able to have a say in the development of European cyber security – be it societal trends, research needs, or investments and projects. In the long term, the institutions of the European Union want to support a vision through this initiative in which the European cyber security sector becomes clearly stronger and more visible in the world.

The vision of the NCC-EE project

In Estonia, cyber security services are offered by viable and forward-looking companies with sufficient workforce, who visibly contribute to the development of the sector across Europe with science-based activities and whose services are in strong demand both in Estonia and in the rest of the world.

Strategic measures

In order to reach the goals set in the vision,

1) **we increase the competitiveness of the cyber security sector.**
- We spread the knowledge gained from research and development in the field of Estonian cyber security both in Estonia and through the network of NCCs in other EU Member States.
- We support the participation of Estonian cyber companies in international R&D projects and the creation of start-ups.

2) **We promote the cyber resilience of Estonian society.**
- We raise the awareness of Estonian companies and institutions about cyber threats and the possibilities of how to better protect organisations from cyber threats in cooperation with other parties in the ecosystem.
- We implement a pilot project for the digital transition: grants for companies that want to increase the level of cyber security of their organisation.

3) **We increase the number of specialists, thereby ensuring the next generation of the field.**
- We find opportunities for all ages and educational levels to incorporate cybersecurity learning outcomes into existing curricula.
- We work with partners to increase the popularity of the field and attract more women and girls into the field.

4) **We monitor and support the development of the cyber security ecosystem in Estonia.**
- In cooperation with other members of the cyber community, we promote communication between service providers, consumers, the scientific community, and other parties, providing platforms for this both physically (events, seminars, and conferences) and virtually.
- Based on the experience of NCCs in Estonia and other Member States, we find opportunities to participate and encourage the community to participate in projects promoting the development of the Estonian and European cyber sector.

E-ITS: why and for whom?

The new information security standard (E-ITS), which entered into force in January, is a challenge for both state agencies and companies, which must undergo an audit within three years and prove that they can provide services using secure systems.

The updated standard is intended for a wider target group than the information security system ISKE, which was valid for 20 years. E-ITS describes the measures, following which the operational continuity of the organisation increases significantly – an overview of processes and risks is created and the capability to prevent and deal with the consequences of cyber attacks is improved.

WHO MUST IMPLEMENT IT?

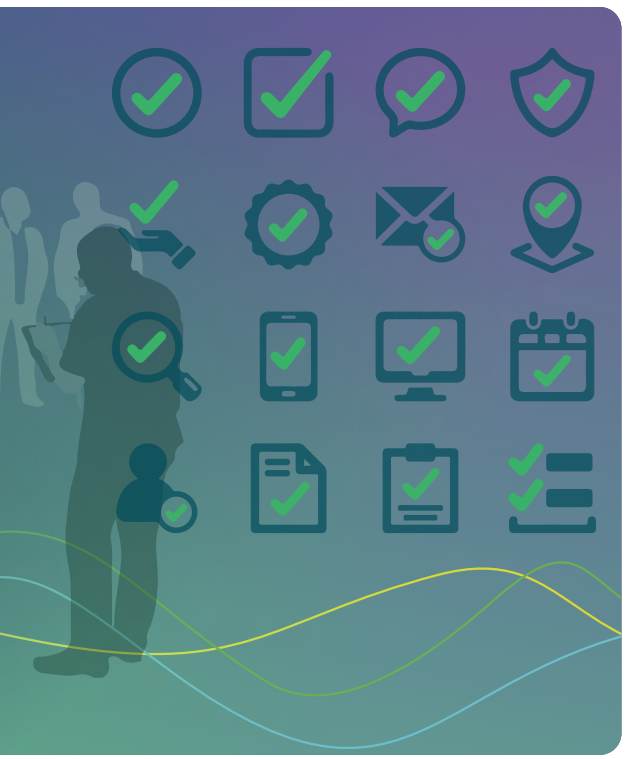
Work on the new standard began in the summer of 2019. From 2021 until April of this year, RIA is carrying out pilot projects for the implementation of E-ITS. The project involves more than 20 agencies. Three agencies that participated in the pilot are almost done with the implementation and are waiting for an audit.

As a result of the amendments to the Cybersecurity Act, approximately 3,500 organisations, including all public sector institutions and providers of services necessary for the functioning of society, are obliged to comply with the standard. Pursuant to the Emergency Act, such services are, for example, supply of electricity, natural gas, and liquid fuel, ensuring the operability of national roads, telephone and data communication services, digital identification and digital signing, first aid in health care, payment services, etc. Such services also include water supply and sewage management for local governments with at least 10,000 inhabitants.

All data processors and data controllers of the database, schools managed by the state and local government (except private schools), and digital service providers also have the obligation to implement the standard if the company employs more than 50 people and its annual turnover is greater than ten million euros. Software developers must implement E-ITS to the extent required by the contracting authority.

FLEXIBLE TRANSITION TIME

Organisations have up to three years to implement and audit the standard. However, the obligation to start taking the first steps – the concept and schedule of E-ITS implementation – is in effect from January this year. Private sector institutions that have not yet implemented ISKE must be able to prove that they have start-



ed implementation from 30 June 2023.

Public sector institutions, which until now were subject to the ISKE audit, must audit their information security implementation before the end of the validity of the ISKE audit, but no later than three years after the entry into force of the regulation establishing E-ITS, i.e. no later than December 2025. If several ISKE audits were carried out in the agency, the validity period of the audit ending the earliest must be taken into account. Agencies that were not previously subject to auditing (but now are) must be audited before the end of December 2025 (up to three years after the entry into force of the regulation).

Previously, the ordering of audits could be delegated to IT centres, but now, the agency itself is responsible for implementing and proving security measures. It is the responsibility of the institution to ensure that the information security of the service provider is at least at the same level that would meet the protection needs of the institution itself.

The supervision of the implementation of E-ITS is carried out by the Supervision Department of RIA. See also eits.ria.ee.

Opinion of a practitioner

MARTIN PARV, Chief Information Security Officer of the Tartu city government

The journey of the Tartu city government to E-ITS began with the creation of the position of chief information security officer at the end of 2021. The city government recognises the importance of IT and is ready to contribute to the security of the field.

We had already mapped the services and we also had a clear overview of the assets. The original idea was to come up with a list of measures to be applied to a specific asset, but this would have made life difficult for implementers and accounting for the asset would have been time-consuming.

Working through the measures, we came to the conclusion that it is most reasonable to group them together on the basis of the asset groups and create documents from them that contain the requirements and operations arising from E-ITS, as well as other requirements and actions necessary to protect assets.

We created logical documents which contain measures written in a language understandable to the implementer and linked to all the measures used so that our system corresponds to E-ITS. This way, in the case of changes to the measures, it is easy to monitor where a specific measure is located and whether something needs to be changed due to the update.

Our plan is to make the life of the implementer easier: instead of, for example, having to mark a large number of measures as implemented for each device, they have to follow the document about the specific device and act accordingly. This way, they only have to confirm once for each device that the measures have been implemented, as they deploy the asset in accordance with the document.

Bureaucracy, which requires the compilation of some procedure, guide, rule, or regulation, causes problems. Even when aggregated, there are too many for each agency to compile them on its own. There are no model documents containing measures, where all the required bureaucracy would be recorded, and a single tool for a small agency in Estonia, with the help of which the agency could easily achieve at least basic security.

What to expect in cyberspace in 2023?

THE THREAT LEVEL will increase even more

The list of attackers and targets is expanding. Among the latter, there are more and more state agencies and companies providing critical services for society, such as the water, energy, and fuel sectors, telecommunications companies, and banks.

Like many other fields, providers of vital services are also digitising their work

processes. This increases the possibility of serious life-disrupting incidents.

The cyber threat situation is influenced by developments in international relations and security. The full-scale attack of Russia on Ukraine, which began on 24 February 2022, significantly raised the cyber threat level for Estonia and the entire Western world. The ongoing war has shown that in addition to supporting kinetic warfare, cyber attacks are also used as a tool to respond to unpleasant political decisions or actions of other countries. In addition, it must be taken into account that cyber attacks against other countries can also affect Estonia.

The scope of activities of advanced persistent threat (APT) groups CONTINUES TO GROW

The main countries that direct cyber groups to act in their interests are currently in a very tense situation. Russia continues to bomb Ukraine, China is increasingly aggressive towards the Western world and Taiwan, and Iran is trying to suppress the opposition inside the country. Cyber attacks are a convenient way for the regimes ruling them to achieve their political goals, or at least demonstrate their will. In addition to simpler attacks – defacement of websites and denial-of-service attacks –, there are more complex and dangerous weapons in the arsenal of cyber groups controlled by aggressive superpowers: for example, derailing critical infrastructure, cyber espionage and selective leaking of information obtained in the process to cause reputational damage to opponents, or, specifically in the case of Estonia, disrupting the operation of some of the main components of the e-state that we are so used to.

We must not forget that figures connected to hostile countries regularly spy on the networks of Estonian agencies, and the discovered vulnerabilities are used to their advantage. That is why it must be emphasised once again that no state agency, company, or ordinary citizen

should take their cyber security lightly.

We can hope that the war started by Russia will end and life will return to normal, but unfortunately, it is likely that our neighbouring country, after losing on the battlefield to a smaller enemy, will have no choice but to take out the resulting bitterness in other domains, e.g. cyberspace.

CYBERCRIME is also evolving

Ransomware attacks have been in the spotlight for years as one of the most damaging types of cybercrime. The number of registered ransomware cases in Estonian cyberspace has remained around 20–30 in the last two years, and so far, we have been able to avoid ransomware attacks that seriously disturb society. However, the risk that Estonia will be hit by a high-impact ransomware attack is increasing for the aforementioned reasons.

It is also likely that in the coming years, with the development of technology – e.g. artificial intelligence – phishing attacks, which have caused problems in Estonia for several years, will become more believable, more targeted, and therefore more difficult to detect.

In addition to emails, phishing attacks are increasingly carried out through social media, such as job postings and advertisements. In order to increase credibility, current topics are used as bait to catch the attention of the person chosen as the target. So far, the fact that we use the Estonian language has protected us from phishing to some extent, but the better translation programs become, the more difficult it becomes to distinguish a phishing page or email from the real thing.

We have to be more vigilant about SECURITY VULNERABILITIES

In the previous yearbook, RIA called 2021 the year of security vulnerabilities. Security vulnerabilities will continue to cause problems. In 2023, several popular Microsoft products (Windows 7, Office 2012, etc.) will expire, and as a result, criminals may focus on hacking these products.

In all likelihood, we will not be able to escape critical-level security vulnerabilities either. RIA keeps an eye on various security vulnerabilities and regularly informs various agencies and companies, as well as the public, about them. We recommend constantly following the RIA blog and social media channels.

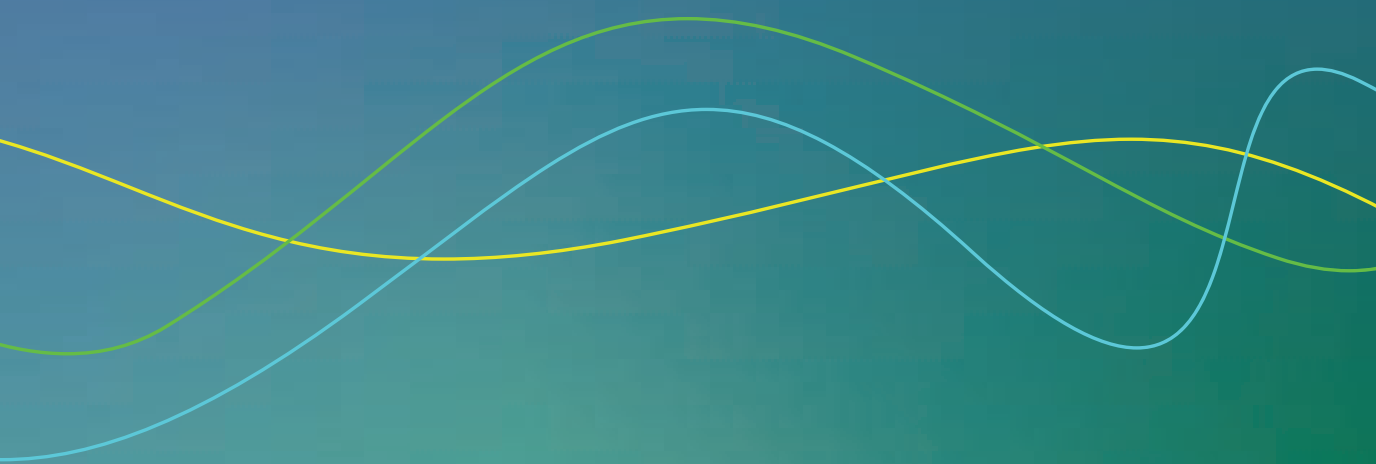
The so-called anti-patchers continue to account for a large part of the problem. Anti-patchers are security managers or administrators who unacceptably delay patching vulnerabilities discovered in software used in their agencies. Unfortunately, these people can be found in state agencies as well as among the providers of vital and important services. We ask again: respond to threat notifications and patching instructions from RIA immediately.

THE CYBER AWARENESS of Estonian residents is constantly improving

The future also holds positive developments. As can be read in the preventive activities chapter of this yearbook (page 42), the cyber awareness of Estonian residents has been growing consistently in recent years. In order to promote this trend, RIA intends to continue with preventive awareness-raising activities in the future. This summer, the Estonian Public Broadcasting will air another radio series which will introduce listeners to the dangers lurking in cyberspace and tricks to help them protect themselves. In the second half of the year, we will publish a cyber test on the RIA prevention website itvaatlik.ee, after passing which every visitor will know more about the main cyber principles. In addition, together with the Estonian Association of Information Technology and Telecommunications, we will focus on small and medium-sized companies, reminding them of the importance of protecting themselves in cyberspace and the main ways to do so.

Cyber Security in Estonia 2023

Publisher: **Information System Authority**
Pärnu mnt 139a, 11317 Tallinn
Design: **Martin Mileiko** (Profimeedia OÜ)
Illustrations: **Andres Varustin**
Printed by: Ecoprint AS



Read more: **www.ria.ee/en**