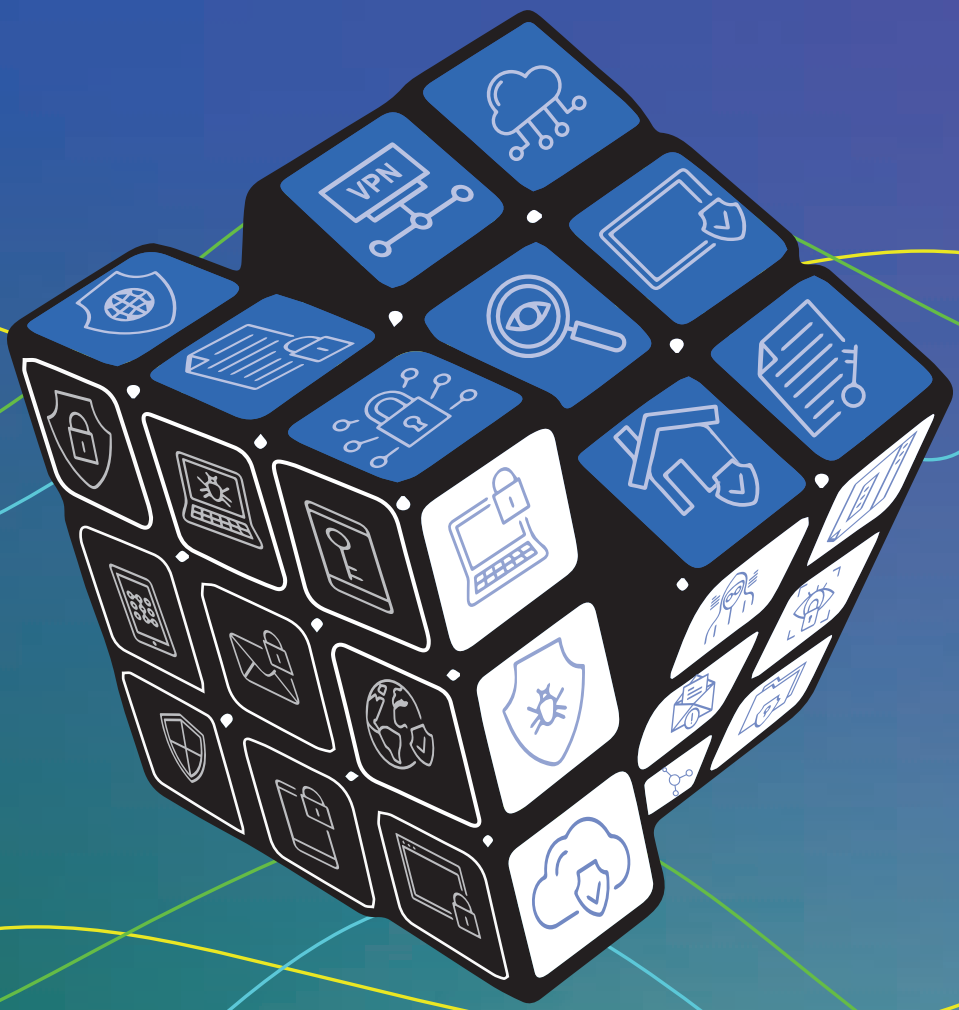
Republic of Estonia
Information System Authority



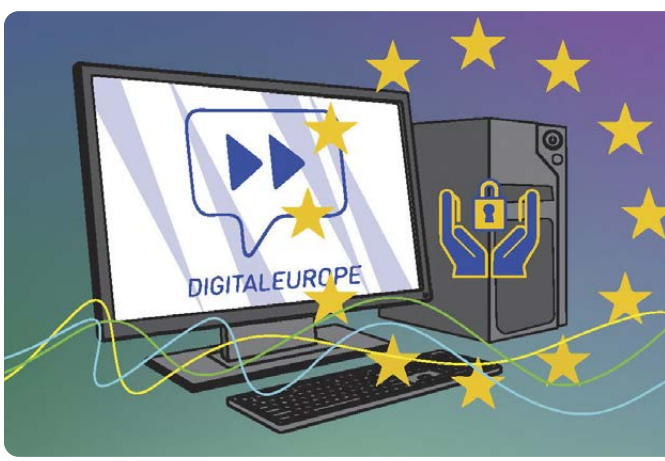
CYBER SECURITY IN ESTONIA 2024

REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

Cyber Security in Estonia 2024

Contents

SAFER CYBERSPACE



INCREASING PRESSURE

Cyber attacks have become more targeted and sophisticated, meaning that the chance of success also keeps on growing. We have to learn the lesson that what happens in cyberspace may affect us also in the physical world, writes **Gert Auväärt**, Director of Cyber Security of the Estonian State Information Authority (RIA).

Russia's full-scale invasion of Ukraine has enabled us the focus on the comprehensive approach to national defence, internal security, and secure digital solutions with the goal of keeping society functioning also in a crisis. Practically all of the critical infrastructure in Estonia is connected to IT systems and keeping it secure against cyber attacks is a national priority.

The international principle that a state should not conduct or knowingly support ICT activity that intentionally damages or otherwise impairs the use and operation of critical infrastructure of another state – enshrined in resolutions passed at the UN General Assembly in 2013 and 2015 – has been blatantly violated by Russia in Ukraine. This edition of the yearbook also includes a good insight from our Ukrainian colleagues concerning the challenges they have to contend with in cyberspace on a daily basis. Secure ICT solutions form an integral aspect of the protection of civilian infrastructure and it is gratifying to note that over the years, cyber security has once again become a priority in Estonia's state budget.

A NEW NAME

Only a few years ago, RIA's Cyber Security Service consisted of a total of 30+ enthusiasts; now, the centre employs over 100 cyber security experts with room for more. Starting from March 2023, we are also proud to be called NCSC-EE, as part of the wider family of National Cyber Security Centres across Europe.

NCSCs are centres of excellence engaged in the cyber security of the public sector and critical infrastructure. For the purposes of the Network and Information Systems (NIS) Directive, they are the competent authorities and contact points for cyber security.

Besides our efforts to improve Estonian cyberspace, this year saw many meetings and discussions with our allies and partners worldwide. There are no solo actors in cyber space and relationships cannot be forged when a crisis is already looming. Instead, lines of communication must already be in place, tested, and in continuous use.

Photo: Rene Riisalu

IDEOLOGICALLY MOTIVATED ATTACKS

Besides Russia's continuing aggression in Ukraine, 2023 brought an outbreak and escalation of the military conflict between Hamas and Israel. We saw – and will surely continue to witness – a growth in ideological 'hacktivism'

expressed in denial-of-service attacks against the government, financial, transport, and media sectors. September set a new record in Estonia, when we registered 84 DDoS attacks that may be linked with Estonia's steps to support Ukraine as well as with fake news spread in the media of the Russian Federation.

Compared to last year, ideologically inspired attacks have become more targeted, due to which we are also seeing an increase in the number of incidents with an impact. In November, a cyber attack against programmable logic controllers made in Israel disrupted operations in local Estonian district heating and pump stations. It was a painful reminder that in our interconnected world, even the impacts of a conflict taking place thousands of kilometres away can hit home.

Cyber attacks, it appears, have become yet another foreign policy instrument for hostile countries and groups looking to erode our sense of security. This new phenomenon must be taken into account and concrete steps should be taken early on to mitigate these risks in the public and private sector.

At the same time, we also have to contend with conventional cybercrime, with criminals themselves getting 'smarter' and intensifying their actions. Attempts are made to derail businesses with distributed denial-of-service attacks and to cripple business operations by holding data ransom. More and more, attacks against supply chains are being seen, where smaller service providers are exploited as a pathway to a larger goal. For Estonian businesses, such attacks caused losses in the millions of euros and jeopardised the payment of salaries to their employees.

TOGETHER, WE CAN DO THIS

We have worked hard to offer companies support for implementing cyber security. For one thing, we regularly draft manuals, issue warnings, and release overviews. All of these materials are freely available on ria.ee and itvaatlik.ee. This yearbook as well is full of specific guidelines and protocols that can be followed to increase cyber security.

Our support is not limited to giving guidance. In cooperation with Estonian Business and Innovation Agency, we offer businesses financial support for measuring and raising cyber resilience. RIA cannot ensure cyber defence alone, but we certainly can do so together with the private sector and other relevant partners.

Last year, RIA's supervision focused on the IT security situation of general medical practitioners, the family physicians that make up the first tier of the medical system. Due to its novelty, this process started off with a few minor disagreements, but as time went on, a better understanding of the necessity of cyber security took root. On our part, we tried to explain – without being overbearing – why and what sort of cooperation we expected. We conduct random checks to enforce compliance with the requirements of Estonia's information security standard.

The medical sector saw two very serious incidents last year. Due to a software bug, erroneous records concerning several hundred people were entered into the national health information system. In the second incident, the sensitive personal data of 10,000 people was stolen from a genetic testing company – data where we would all rightly expect that it be kept away from any unauthorised eyes.

Data protection and keeping one's own data secure is undoubtedly a field that requires our total vigilance in future as well. The amounts of money stolen from people in Estonia through various forms of fraud, such as phishing, can run into the tens of thousands per individual, and the total is several million euros. Although statistics show that cyber awareness among the Estonian public has grown every year, malicious actors also keep on fine-tuning the schemes they use in cyberspace.

To you, the reader, we wish to say that we are sincerely glad that you have found the time to dip into the RIA yearbook, which sums up the year in cyberspace in Estonia and around the world, and discusses the steps RIA has taken with its partners to ensure that our secure way of life continues. I hope you will find inspiration here to bolster your own cyber security, perhaps even discover the seeds of a deeper personal or professional involvement with the cyber sphere.


Backspace
Y
T
Enter
G
F
Alt

THE SITUATION IN CYBERSPACE: a repeat of the year of the DDoS attacks

Last year, geopolitical tensions once again left a mark on Estonian cyberspace. During a cold snap in November, the conflict between Israel and Hamas was felt on our distant shores in the form of cyber attacks that hit the Estonian district heating network. A recurring refrain last year was denial-of-service attacks, the overwhelming majority of which were related to Russia's full-scale war in Ukraine.

In late November, when Estonia was in the clutches of wintry weather, a district heating company came under cyber attack. It took down the control systems of eight boiler units. The boiler units were shifted to manual mode, so heat generation and transmission were not at risk, but the equipment was so badly damaged that they had to be replaced.

At least two other Estonian companies also fell victim to similar attacks, one in the water supply sector, the other in the construction sector.

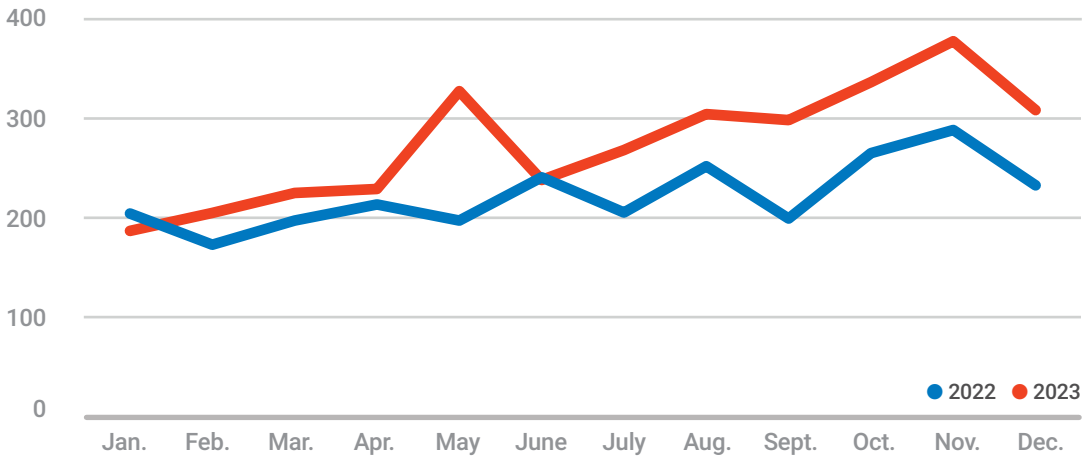
The target of the wave of attacks was not Estonian companies or institutions, but rather programmable logic controllers, or PLCs, made in Israel, irrespective of their location. Water utilities in the US were also targeted.

The attackers claimed to be a group with an Iranian background and the attack was a response to the conflict between Israel and Hamas. This was another example of how the effect of geopolitical tensions and military conflicts taking place thousands of kilometres away could also impact Estonia in the form of cyber attacks.

DENIAL-OF-SERVICE ATTACKS SET NEW RECORD

In Estonian cyberspace, one of the largest and most visible collateral effects of the full-scale invasion of Ukraine was the quadrupling of DDoS attacks. Activity on this front had already seemed frequent and fast-paced back in 2022, →

Number of incidents with an impact by month



but last year shattered the previous record. We registered 484 denial-of-service attacks, which is 60% more than in 2022. In the space of just one month, we registered more DDoS attacks than in an entire year before Russia began its onslaught in Ukraine.

We considered 139 of the attacks – less than a third – to have an impact. The damage was generally limited to a short period of downtime or slower response on a website or service, but a few cases were more serious. The most visible ones were the attacks against Ridango, the company that manages the ticket sales systems of state-owned train service Elron, in September. These attacks cut off sales of train tickets on the internet and payment terminals on trains for close to a day.

In the space of just one month, we registered more DDoS attacks than in an entire year before Russia began its onslaught in Ukraine.

Over the year, the attacks became more clever and targeted. Preparations were more thorough and energy was focused onto targets, with visible impacts. The attacks often occurred in two waves. The first one was short in duration and tested the target's resilience. If the opening salvo was successful – if it caused disruption or downtime –, a second, significantly longer phase followed.

The DDoS attacks were often linked to Estonia's decisions to support Ukraine or followed the imposition of new sanctions on Russia. We are also seeing waves of politically motivated attacks this year. For more on DDoS attacks, see page 26.

NOT ALL INTERRUPTIONS WERE CAUSED BY CYBER ATTACKS

Human error or technical problems were often responsible for a service going down. On 14 September, one Estonia's wireless operator's network went down for close to an hour, affecting voice communications for 25,000 customers. Calls went through between the same operator's phone numbers, but not to other networks. This was caused not by a cyber attack but human error. A wrong line of code in a file left tens of thousands without the ability to make a phone call.

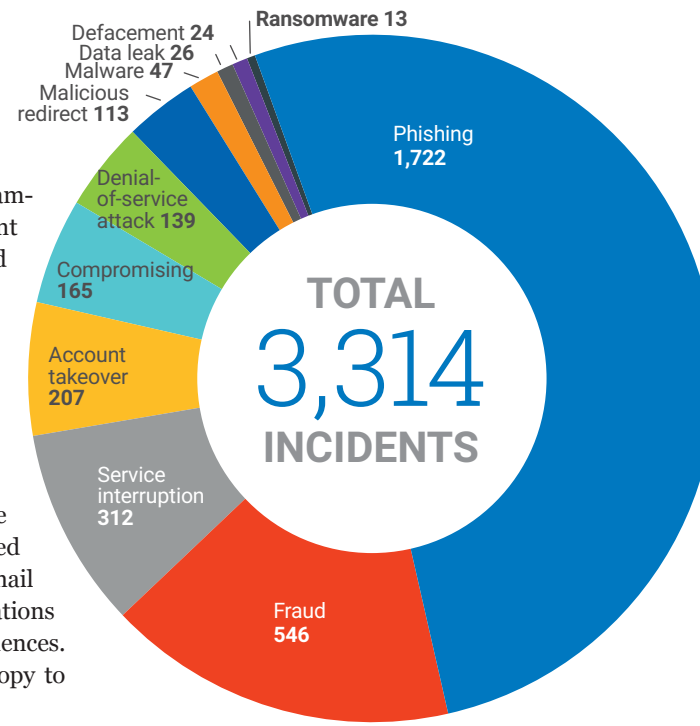
In early November, a hospital began replacing its UPS system, which provides backup power if mains go down. During this procedure, the power grid was overloaded, which tripped the circuit breakers, depriving UPS sockets of current. All equipment (workstations, printers, etc.) switched off, network devices went down, as did the patient monitoring devices and central mon-

itoring system displays. Power was restored about an hour after it was lost.

Another hospital also experienced disruptions in November. Communications (both data and phone) went down, in this case due to physical damage to a fibre-optic cable. The incident caused extra work for hospital staff but did not affect patient care. The problematic cable was replaced with a new one and ordinary communications were restored.

Unfortunately, these incidents were not the only such cases at hospitals. In late June, one of them discovered that a large number of files had gone missing from a server for unknown reasons. The missing documents were mainly connected with administrative operations (payroll, email service, food service). Healthcare operations continued, although with some inconveniences. Fortunately, the hospital had a backup copy to allow it to restore the data.

Incidents with an impact in 2023



DATA LEAKS

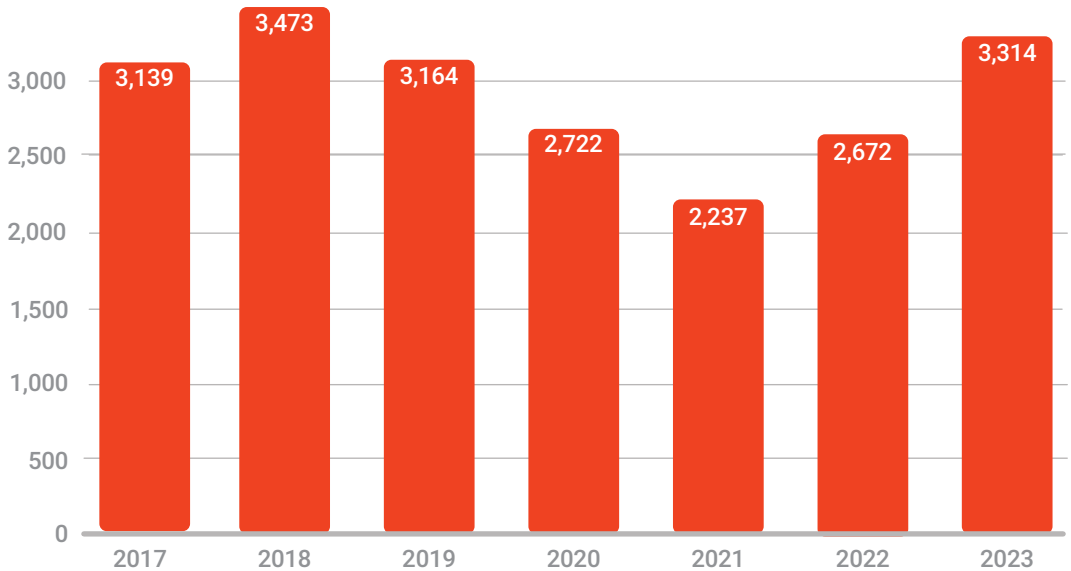
In May, it was revealed that criminals had gained access to data on students and graduates in the systems of an Estonian institution of higher education – names, usernames, email addresses, passwords, IP addresses, passport numbers etc. — and put them up for sale. As a vulnerability in outdated software version was used to steal the data, this provides us with another opportunity to sound like a broken record: patch security vulnerabilities as soon as possible – do not postpone this.

In March, we learned that over the span of 10 months, the Estonian Social Insurance Board had been releasing documents intended only for internal use on the *Ametlikud Teadaanded* public announcement site. They included detailed information about minor children and their parents: for example, parents who had not paid financial support; children separated from their families; support paid to children. Due to human error, 103 precepts issued by the board – which were not public information – had been published.

A worse incident lay ahead. In September, a bug was discovered in Medisoft's Perearst3 GP software, used by several dozen family medicine centres to transmit information to the national health information system. As a result, the wrong person's information was added to about 600 medical histories. Not only was the breach of confidentiality troubling; the insertion of incorrect data into a medical history could have even more serious consequences. After all, doctors diagnose and prescribe treatment based on medical histories. If the information in a case history is wrong, the treatment can also be incorrect. The Health Board urged ambulance crews and emergency rooms to take a critical attitude toward data from family medicine centres that use Perearst3.

The bug behind the problems lay in code written back in 2018. Medisoft was notified of the data integrity problems in March 2023, but the company considered it a one-off occurrence and did not devote sufficient attention to the problem. For more about this incident, see page 18.

Incidents with an impact



This year of leaks was underlined by the theft of about 100,000 files containing the personal and health data of 10,000 people from the systems of the genetic testing company Asper Biogene. The attacker threatened to publish them if a ransom was not paid.

There had been major data leaks before that as well. One of the most painful examples was the 2021 theft of document photos from a database of personal identification documents. The incident impacted about 300,000 people. However, in that case, the culprit was apprehended, along with the data, in a matter of days. In the recent incident, healthcare data leaked – information significantly more sensitive than document photos. See page 20 for how the attack on Asper Biogene played out and what lessons to learn from it.

NO END OR LIMIT TO FRAUD

Last year, when it comes to incidents with an impact, various forms of fraud experienced the most growth. CERT-EE recorded 546 incidents of fraud last year, an increase of 250% from the year before. According to the Police and Guard Board, Estonians were defrauded of at least 8.3 million euros. Telephone fraud alone accounted for the theft of 3 million euros.

The types of fraud ran a very wide gamut. Some fraudsters passed themselves off as police officers calling to help the victim evade fraud, but in fact emptied the victim's bank account. Another played a role of a prospective buyer on Facebook Marketplace, duping the seller into providing their bank card details or PINs. A third compromised a company's email account and used it to invoice partners, except with the bank account of the payee changed. Last year, the false invoicing scheme was used in an attempt to steal several million euros, but thanks to the counterparty's vigilance, it did not pay off for the wrongdoers. See page 28 for tactics used by fraudsters and how to avoid falling for scams.

RANSOMWARE: FEWER ATTACKS, MORE HARM

Although the number of recorded ransomware attacks fell, the harm caused tends to be on the upswing. Criminals do their homework, take their time, and, in the Estonian context, target relatively large and successful companies who can afford to pay a hefty ransom. We also saw criminals use IT and accounting service providers to obtain access to bigger, wealthier clients and implant ransomware that encrypts data.

This year's edition of the RIA yearbook has an extraordinary story of a ransomware attack that ended up costing the victim millions of euros in direct expenses and lost revenue.

What makes it exceptional is not the loss, but the fact that the business owner was willing to talk about it openly and publicly. Generally, people want to hush up or forget such unpleasant incidents, but we encourage talking about them. Bringing it to public light helps others realise that a devastating cyber attack is not a remote, abstract risk that befalls someone else far overseas, but a real danger that could sideline your own business. Making backup copies can instil a sense of security, but unfortunately, criminals sometimes manage to corrupt backups. See page 22 for ransomware attacks.

SECURITY VULNERABILITIES AS AN 'OPEN HOUSE'

Last year witnessed more zero-day security vulnerabilities than usual. Zero-day vulnerabilities are flaws in software that the developer was not aware of or for which no patch was available at the time the vulnerability was exploited. Cisco announced in October that the web interface for their devices was threatened by a critical vulnerability that allows a device to be completely taken over. Three days after the public announcement from Cisco, about 100 vulnerable devices in Estonia had been compromised.

Zero-day vulnerabilities are a hot topic, but tend to overshadow the fact that most attackers take advantage of vulnerabilities that are long known, where the developer has released a patch which has not been installed on all systems. By not installing crucial updates, they effectively open their doors to the cybercriminals of the world. The longer one waits, the greater the likelihood that some unwanted visitor will accept the 'invitation'.

Last year, for example, attackers exploited a vulnerability in an online retailer's platform and broke into the e-store of an Estonian electronics seller. The software developer had released a patch for the exploited vulnerability a year before, but it was installed only after the successful attack. See page 32 for the most significant vulnerabilities.

Relatively modest effort can raise cyber security to a level that will dissuade attackers from even trying and instead make them turn to easier prey

PHISHING IS STILL ALIVE AND WELL

The number and percentage of all conceivable forms of phishing continue to rise: in 2022, they made up 45% of all incidents, but last year, the share was more than half – 52%.

This field is a low-opportunity-cost one for fraudsters, as unfortunately the old schemes are still effective. RIA's tests show that a third of phishing attempt recipients take the bait, and 10–20% enter the data as bidden, such as an account password.

Broadly speaking, phishing attempts fall into two categories – account-related phishing (for usernames and passwords) and bank data phishing (credit card data, PINs). The latter category tends to have immediate consequences, while the damage from password leaks can become apparent months or years later. Phishing emails and texts purporting to be from a delivery firm are still widespread. In such schemes, the perpetrators ask for a few euros so that the 'parcel' can be released. Some people duly provide their bank card data despite the fact that they had not even ordered anything from an online merchant recently.

NO GUARANTEES

This book contains a number of tips and recommendations for keeping safe from cyber threats. We cannot give a guarantee that you will never fall victim to fraud or cyber attack – there is no such thing as 100% protection. But we do know that a relatively modest effort can raise cyber security to a level that will dissuade attackers from even trying and instead make them turn to easier prey.

WAR IN UKRAINIAN CYBERSPACE: what did 2023 bring?

Although traditional warfare in Ukraine garners more attention, it is accompanied by active offensive and defensive activity in cyberspace. What trends were seen in 2023?

The world has been following the Ukraine war in cyberspace with trepidation since 2015. That was the year that a cyber attack against the power grid cut electricity to around a quarter of a million people in mid-winter. Attacks against energy infrastructure on a comparable scale have not recurred in recent years, yet the situation in Ukrainian cyberspace is anything but calm.

THE ATTACK WITH THE MOST DEVASTATING CONSEQUENCES

In 2023, the sectors that came under attack the most were media and telecommunications, central government institutions and local governments, the Ukrainian Defence Forces and the defence industry.

The incident with the highest impact last year occurred on 12 December when a cyber attack hit Ukraine's largest telecom, Kyivstar. The attack damaged Kyivstar's infrastructure, causing mobile signal and internet services to be interrupted for millions across the country. It also affected the air raid warning system. A technologically highly capable group connected to Russian military intelligence (GRU) took responsibility for the attack. Kyivstar's CEO Oleksandr Komarov said the attackers exploited a compromised account of an employee of Kyivstar, but the detailed circumstances are still being investigated.

Attacks against courts and other judicial institutions emerged as a new trend. The goal of the Russian state-affiliated threat actors was to harvest data on detained soldiers and people accused of treason. They also sought access to materials gathered by Ukraine on war crimes committed by Russia.

The international media also devoted coverage to cyber attacks against the International

Criminal Court in the Netherlands. To facilitate investigations, the ICC opened an office in Kyiv last year and issued an arrest warrant for Vladimir Putin in connection with the deportation of Ukrainian children from occupied Ukrainian territories to Russia. The ICC also consulted with Estonian (RIA) experts for assistance in increasing cyber resilience and preventing future attacks of this kind.

CYBER RESILIENCE OF CRITICAL INFRASTRUCTURE HAS IMPROVED

Attacks against critical infrastructure continued in 2023 but compared to earlier years, their number was down: in the second half of 2022, Ukrainian cyber organisations received reports of 144 attacks; in the first half of 2023, the corresponding number was 27. Destructive attacks with wiper malware mostly coincided with the first year of the full-scale war, with one exception being the attack on Kyivstar in December 2023.

According to an analysis published by threat intelligence and cyber security company Mandiant, a significant incident occurred in autumn 2022 when a GRU-linked group called Sandworm caused a power outage in a city in Ukraine. The power utility's systems were compromised a few months earlier but the decisive phase of the cyber attack coincided with a missile attack by the Russian Federation in the same region. Mandiant's experts reckon it showed Sandworm's growing ability to target industrial SCADA systems and served as an example of combining kinetic and cyber operations. This is likely to become more common in future conflicts.

In the last year, Ukraine has made noteworthy efforts to improve the cyber resilience of its critical infrastructure, in terms of technical protection measures as well as strategic leadership. In autumn 2023, a national plan for critical infra- →

structure protection was adopted. The document defines obligations for vital infrastructure companies and relevant government institutions and also promotes collaboration with the private sector.

NUMBER OF CYBER INCIDENTS IS UP

The total number of cyber incidents in 2023 was not yet known at the time of writing this article, but based on the statistics of the first six months, we see that the number of critical cyber incidents fell. At the same time, there were more incidents with an impact than in previous years. In the second half of 2022, the average number of recorded incidents per month was 57; in the first half of 2023, the number was 128 (data from the UKR SSSCIP overview Russia's Cyber Tactics H1 2023).

The data from Ukraine also shows that apart from politically motivated attacks, cyberspace is teeming with 'ordinary' cyber incidents. Phishing for bank codes and account details continues even while the country is being hit by attack drones and missiles. Fake invoices are sent to companies and individuals fall prey to various scams that imitate support measures. Phishing, in which people are tricked into entering data or usernames on a fake page, has become one of the main attack vectors for both cybercriminals motivated by profit as well as state-sponsored threat actors.

Although traditional warfare in Ukraine justifiably garners more attention, cyber attacks are part of the everyday behind-the-scenes action in the conflict. As noted above, the number of successful cyber attacks against critical infrastructure in Ukraine was lower than in 2022. Ukrainians' extensive experience repelling Russian cyber attacks and new protective measures implemented with allied and private sector support are part

Ukrainian cyber security expert: the number of cyber attacks against countries that support Ukraine may increase

If the enemy fails to achieve sufficient success on the battlefield, they may resort to destructive cyber attacks against Ukrainian critical infrastructure and countries that support Ukraine, Ukrainian official **Serhii Prokopenko** told RIA.

How would you describe the threat landscape in 2023? What has changed compared to the year before?

The threat landscape is becoming more complex. Threats from Russian state-sponsored actors are still the number one threat to Ukraine, but we have seen several campaigns by other countries as well, primarily for the purpose of collecting cyber intelligence. All Ukrainian cyber agencies reported an increase in the number of incidents in 2023 (partly due to more diligent reporting), but the number of critical incidents has rather decreased compared to last year.

Serhii Prokopenko is Deputy Head of the Information Security and Cybersecurity Directorate at the National Security and Defence Council of Ukraine.

Russia is developing its offensive cyber capabilities in terms of tactics, tools, and personnel in the respective parts of its special services (FSB, GRU, SVR). It also improves planning capabilities for both cyber and hybrid operations.

of the reason for the lower number. Russia's limited capability to integrate cyber attacks for achieving the goals of an old-fashioned war of conquest is perhaps another reason.

TOO EARLY TO DRAW CONCLUSIONS

However, far-reaching conclusions should not yet be drawn about 2023 in Ukrainian cyberspace. A large share of the attacks in this domain and actions leading up to them are concealed, so significant incidents can come to light months or even years later.

The balance of forces in the cyber domain is inevitably changeable, as every new day can bring news of a critical vulnerability in a service or software that deals the adversary an advantage. In this context of uncertainty and unpredictability, countries, including Estonia, try to learn as much as possible from the Ukrainian experience.

TALLINN MECHANISM was established to provide cyber assistance to Ukraine

On 20 December 2023, the Tallinn Mechanism was launched, created by Estonia and its allies to amplify the cyber support of donor countries to Ukraine in the civilian domain. The aim of the mechanism is to match Ukraine's needs to what donors can do to increase effectiveness of aid and allow Ukraine to defend itself in the cyber sphere.

The donor states to the Mechanism are Canada, Denmark, Estonia, France, Germany, Netherlands, Poland, Sweden, and the US and the UK. NATO and the EU are observer members. The Mechanism has an Estonian front office in Kyiv, a Polish back office in Warsaw, and a coordination group that unites representatives of Ukraine and all donors. The Mechanism is open to new members.

Russian APTs (advanced persistent threats – Ed.) were characterised by the following in 2023:

- Specific institutions are being attacked, not the entire sector.
- The ability to coordinate cyber attacks with kinetic attacks on the battlefield is improving.
- The focus is not only on Ukraine, but also on cyber operations against Ukraine's allies.
- The information and data obtained from earlier attacks is analysed thoroughly and taken into account in planning new ones.
- Surveillance cameras and other IoT devices are attacked, primarily for intelligence purposes.

What would you recommend to other countries? How do you defend yourself against an enemy such as Russia in cyberspace?

I would recommend being aware of the danger posed by companies with a Russian background and personnel with a suitable background. Sooner or later, they can end up being used by Russian special services.

The effectiveness of exchanging cyber threat intelligence (CTI) ought to be improved. The Russian tech sector's access to useful technology must be blocked with sanctions. Sanctions must be enforced.

I would also recommend monitoring data leaks and limiting the disclosure of leaked data where possible. Early identification and prevention of (mis)information operations is also very important.

What do you predict for 2024? In addition to gathering cyber intelligence, is there a risk of destructive attacks?

Attacks against the defence and security sector are increasing. Information operations will become more sophisticated, including those with an AI component, and could be seen against all democracies. Leaked personal data is used for attacks on social media, denial-of-service attacks will become more powerful, and the risk of supply chain attacks will increase.

If the enemy fails to achieve sufficient success on the battlefield, major cyber attacks against Ukraine's critical infrastructure may increase.

The number of cyber attacks against countries that support Ukraine may also grow.

Mixed-up PATIENT DATA

Last September, a patient at the Raatuse family medicine centre discovered that their medical history contained someone else's diagnosis. The patient was one of almost 600 whose medical records had become mixed up with other individuals' data due to a software bug.

Not all incidents that may impact people's well-being and trust were caused by hackers or malicious actors. Sometimes, bad code can cause a crisis with serious consequences.

The patient who discovered erroneous data in their medical records contacted the Raatuse centre, and the medicine centre contacted their partner, Medisoft. The company's software, Perearst3, is used by family physicians to send data to the central health information system used for exchanging and viewing patients' health data.

A POTENTIAL THREAT TO LIFE AND HEALTH

Bad health data can lead to potentially severe harm, as data is the basis for diagnosis and treatment. The data is also used for allocating benefits and allowances, such as for sick leave or determining the severity of a disability. Health data is sensitive and personal and must be kept from being accessed by unauthorised eyes.

Perearst3 is used by 55 medicine centres to send data to the national health information system and 45 were impacted by the bug. The administrator of the health information system (TEHIK) restricted access to the corrupted documents and for several days, the work of ambulance teams and emergency medical departments was disrupted as well, as the Health Board urged them to treat with caution any data from family medicine centres using Medisoft software.

At first, 672 patient files were believed to be corrupted, but the final number was put at 580. The data became intermingled when the family physician had several case files open at the same time. Complaints, diagnoses, and treatment summaries were all potentially affected.

Medisoft was first tipped off about the data problem last March, but the developer considered it a one-off occurrence and did not devote enough attention to it. The bug actually originated in code written back in 2018. The bug did not impact the availability of the Perearst3, but did cause harm to data integrity and confidentiality.

Medisoft fixed the bug with a software update and affirms that the Perearst3 information system is now fully functional with no further errors in transmitting medical records. The Data Protection Inspectorate deemed the cause of the incident an infrequently-seen and hard-to-detect software bug and closed the proceedings by issuing a reprimand. The health data for the wrong patients seen in these mixed-up medical histories was, for the most part, not identifiable to that person. In a few cases, the data could allow the person to be identified, such as their name or personal identification code.

As to whether any treatment decisions or eligibility was assessed on the basis of the bad data, this is not yet known. TEHIK analysed the use of the bad data (e.g. for determining capacity for work, suitability for Defence Forces service, etc.) and sent the information to the corresponding institutions so they could amend any decisions, if need be.

WHO IS RESPONSIBLE?

TEHIK does not itself have a contractual relationship with Medisoft for developing information systems in the field of healthcare. General practitioners operating as private entrepreneurs have a contractual relationship with Medisoft, and the doctors are obliged to ensure the availability of health data throughout the healthcare system.

One broader lesson from this regrettable incident is the that contracts should regulate the cyber security obligations of private companies who provide services to the public sector or vital service providers but are not themselves subjects of the Cybersecurity Act.

The contracting authority bears liability for the security of a procured service – and this is also the case if the service itself or the number of companies that provide the software is limited. Contracts should thus spell out the requirements and responsibilities applicable to service providers, such as action to be taken in the event of a security incident.

For the state, it is worth considering whether the requirements of the Cybersecurity Act should be extended to companies that the public sector and other key service providers rely on for services. ●

For the state, it is worth considering whether the requirements of the Cybersecurity Act should be extended to companies that the public sector and other key service providers rely on for services.

ASPER BIOGENE DATA LEAK: what exactly happened?

In December, the public found out that the personal and health data of about 10,000 people had been illegally downloaded from the systems of the genetic testing company Asper Biogene. The attackers threatened to publish the stolen data.

Data leaks are far from being as rare as we would like them to be. We have written about them in previous yearbooks but have not yet had to report anything like this incident. What makes the Asper Biogene leak particularly distressing is that some of the most sensitive types of personal data in existence fell into unauthorised hands.

HOW WAS THE ATTACK CARRIED OUT?

As with many other attacks, this incident was caused by poor cyberhygiene. Back in September, attackers had tried different ways of attacking the company's servers and found one particular query that gave them the data they needed to mount a further attack. The attacker used the data to enter the Asper Biogene information system and started downloading data.

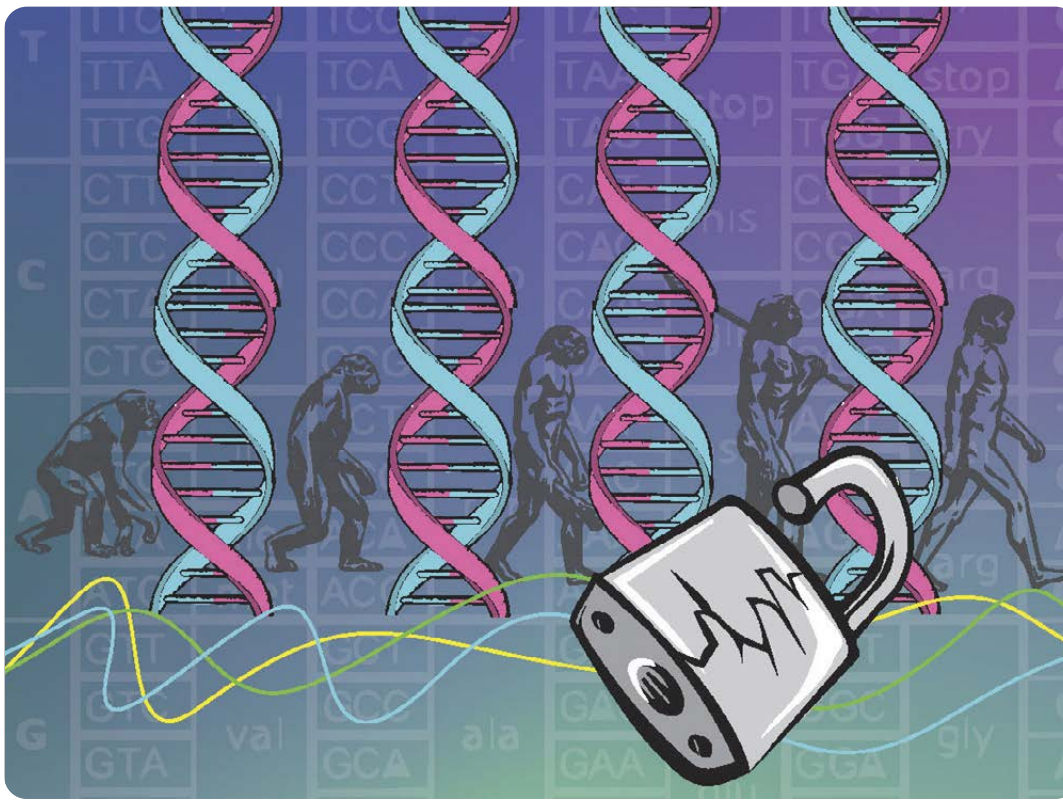
Over a week, approximately 100,000 files were downloaded, containing the personal and health data of about 10,000 people. Some of the files contained results of genetic tests ordered by hospitals and other healthcare institutions and individuals. The files included PDFs containing the person's name, personal identification code, and test results. The incident involved 42 hospitals and healthcare providers Asper Biogene provided service to. East Tallinn Central Hospital and Tartu University Hospital were the most prominent establishments.

'PAY UP OR WE WILL PUBLISH'

Asper Biogene learned of the incident only after much of the damage had been done, when they received the ransom demand on 11 November.

The company acted in the proper manner in this situation – they did not pay the ransom and contacted RIA, the police, and the Data Protection Inspectorate. At the same time, all accesses to the system were closed and the logs were examined.

This revealed that criminals had been trying to find weaknesses in Asper Biogene's systems back in September. The successful intrusion into the system occurred on 1 November and the files



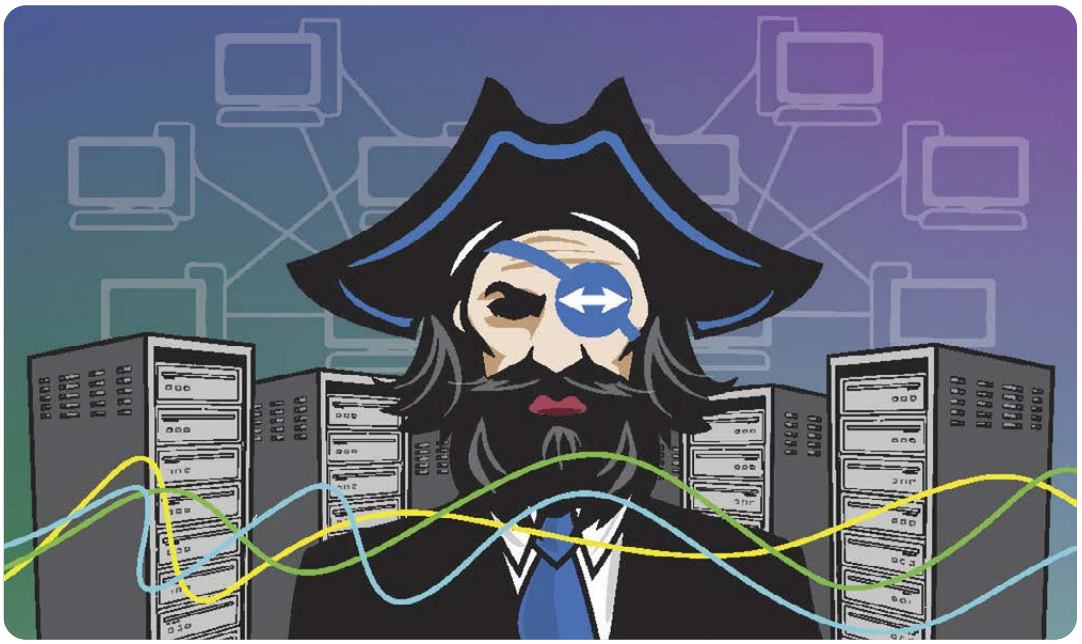
were downloaded from 3 to 10 November. The attackers stole a total of 33 GB of data.

The police launched a criminal investigation into the incident, and the Data Protection Inspectorate initiated an enforcement proceeding and a misdemeanour proceeding. The exact circumstances of the incident are still being clarified.

WHAT CAN BE DONE BETTER?

Here are a few specific recommendations for avoiding such incidents.

- Use two-factor authentication wherever possible. A leaked password will not end up being an express lane for attackers if a login also requires a one-time code sent to a phone.
- Use different passwords for different sites and platforms. The cross-use of passwords can bring down personal and business accounts if the password leaks.
- Make only essential services available on the public net. If you need to administer a website remotely, put the network devices behind a firewall and use a VPN with two-factor authentication.
- Use the latest software version and make sure you keep current with updates. Often attacks take place through vulnerabilities that have not been patched.
- Regularly back up the contents of your web server and database to an external location. A working backup copy can more quickly restore operations if a cyber incident occurs (such as installation of malware).
- Keep sensitive personal data (such as health records) encrypted. If an attacker manages to steal encrypted data, they will not be able to access them.
- Regularly red-team your systems. This will determine shortcomings and weaknesses and obtain information about what needs to be fixed.



RANSOMWARE DEMANDS hit several large companies

In the past year, CERT-EE, RIA's incident response department, was notified of a number of ransomware attacks that hit companies considered large by Estonian standards.

In October, malware was used to encrypt data on two servers at a large corporation in Tallinn. In order to reach their ultimate target, the attackers penetrated an accounting firm's systems using the Remote Desktop Protocol (RDP). Fortunately, the manufacturer had made recent backup copies of the data, and it was possible to restore the systems.

THREE LESSONS

Three lessons can be gleaned from this incident. One, supply chain attacks are a growing problem in Estonia, as they are in the rest of the world. IT and accounting service providers are often used

as a backdoor to target larger, economically more powerful companies. Companies who outsource such services should seriously analyse whether their partners' cyber security is up to snuff and which of their systems to allow them to access, with which privileges.

A poorly protected remote desktop or VPN network is also often a weak spot. Unfortunately, CERT-EE monitoring data shows that Estonia still has more than 1,000 RDP connections that can be accessed from the open internet, even though the proprietors are warned through communication service providers regularly of the risks involved.

There was a curious incident where an IT specialist set up a temporary remote desktop at the end of a work day, intending to close it in the morning, but criminals got there first and took down the company's systems. Hackers are constantly probing networks and can exploit weaknesses in a matter of hours.

The October incident again reaffirmed the importance of reliable backups kept separate from other systems when it comes to dealing with the consequences of an attack. In another instance, a manufacturing company in western Estonia managed to quickly get its IT systems and data up and running after a ransomware attack in late December. On this occasion, a weak VPN password was the point of entry.

Good cyber hygiene is indispensable, as many ransomware attacks start from a simple phishing attempt involving a hijack of an employee's user account. Attackers continue to feast on default passwords on devices, unpatched security vulnerabilities, and outdated software no longer supported by the developers. The use of two-factor authentication and automatic updates and keeping some services behind a VPN significantly lowers the chance of falling prey to an attack.

For manufacturing firms, an important way of mitigating the risk of a cyber attack is network segmentation, which keeps wrongdoers from roaming freely once they penetrate a system. Manufacturing equipment should be in a firewalled network that can only be accessed by verified accounts from verified devices. Network traffic should also be monitored. If services are kept in separate segments, potential attackers will have to cause much more 'noise' as they navigate. This will help to detect intruders.

DO NOT FEED THE CRIMINALS

If, for some reason, backups cannot be restored and systems have to be rebuilt from the ground up, the economic losses can be substantial. It is understandable that in this situation, some companies opt to pay the ransom. But it should be remembered that this perpetuates the problem and feeds the motivation for future attacks. The data stolen in the attack can also be sold and become the object of a later extortion attempt, and vulnerabilities that go unpatched can be exploited a second time.

On 1 November 2023, 50 countries who joined an international anti-ransomware initiative, Estonia among them, made a joint declaration pledging to not pay ransoms and set a positive example.

The declaration also underscored the need to make cooperation with the private sector more effective. As in most countries in the world, only a small share of ransomware incidents is reported in Estonia, and this complicates the fight against cybercrime. The business community has expressed fear that if they do report an incident to a government body, they may be penalised for violation of cyber security rules or face damage to reputation if the incident becomes public.

RIA will not punish victims, but rather help them resolve the incident, sharing its know-how and, where possible, decryption keys. It is up to each company whether to release information about the incident, but RIA considers it highly praiseworthy to do so – real-life stories associated with a specific named company are more effective as food for thought than anonymous warnings.

RIA will not punish victims, but rather help them resolve the incident, sharing its know-how and, where possible, decryption keys.

AN ATTACK that cost millions

Last year, two metal companies in Estonia's capital region that employ around 400 workers were hit by a ransomware attack. The management went public about what happened and the reasons that led to it so they could help others avoid similar threats.

AS Estanc and Tammer OÜ, owned by the same business family, make metal windows, doors, and receptacles. Their combined turnover amounts to 60 million euros. Early in 2023, both were hit by a ransomware attack that partially shut down production for a month. Mihkel Tammo, one of the executives, said that the lost revenue was a seven-figure sum, not including direct damage.

HOW THE ATTACK WAS DISCOVERED

The first sign that something was wrong became apparent early on the morning of 1 February. Tammer's IT director Indrek Kink was awakened by a phone call at 6.20 a.m. and told the IT systems could not be accessed, for unknown reasons.

On his way to the office, Kink made some calls and when he pulled into the Estanc parking lot at 7.15 a.m. it was clear it was a ransomware attack. "Unfortunately, the attackers had probably been inside our network for some time – they had mapped the system and devised plans," says Kink. He says the IT systems were not poorly protected – they were in fact aware of the dangers, had crisis plans in place and a system for regular backup copies.

TWO WORST CASES COINCIDE

The weak point was an old email server, whose functions had in fact already been moved to the cloud. After the move to the cloud, they found that they still needed the server and it was started up temporarily, but the update administration system was not integrated with it. As happens all too often, the temporary solution ended up being a prolonged one and an unpatched ProxyLogon vulnerability in the Microsoft Exchange Server opened the door to the internal network for the attackers.

It allowed the criminals to stealthily gather information about the company's systems. They realised that backup copies were made frequently, so there was no point in simply encrypting data that could be relatively easily restored from the backup.

'Unfortunately, we realised a full month after the incident that a zero-day vulnerability had been found in the software used to make the backup copies, and used to access an admin account. It was used to compromise both locally stored and cloud-based copies and the contents were simply erased,' said Kink. That gave the intruders the last missing piece of the puzzle – they disabled the possibility of using backup copies – and they launched their attack.

BATTLE ON SEVERAL FRONTS

Once the cyber criminals had crippled the systems and sent their ransom demand, production at one of the companies was halted almost completely for a month. The consequences of the stoppage lingered for several months afterwards.

'It was a critical situation at that point – we needed to pay wages to more than 400 workers at the two companies. Still, we managed,' recalls Mihkel Tammo.

The business end needed to do damage control, and the IT side laid out three possible approaches to a solution: restore data by getting at least one backup copy up and running, rebuild the entire data architecture from scratch, or strike as favourable a deal as possible with the attackers.

The services of the cyber security firm CYBERS were retained in the first days, and there was constant communication with CERT-EE.

Restoring the backup copies was a major effort. Some of the files were retrieved, but unfortunately, they were corrupted. At the same time, preparations were made to rebuild the systems from the ground up.

'By 18 February, we had tested out all the conceivable avenues and it seemed we would have to abandon our hopes of besting the criminals,' said Kink.

A DIFFICULT DECISION

The CEO of CYBERS, Jürgen Erm, took on the role of lead negotiator with the attackers: 'At first, with other possible solutions still on the table, we played dumb so as not to give away too much information to the bad guys. We also tried to get some proof or guarantee that we would actually get the data back after paying the ransom demand.'

Tammer OÜ's CEO Anti Tammo says the decision to pay the ransom was not made lightly: 'We thoroughly considered all the alternatives, our IT people worked untiringly on various solutions. As the ransom demand was many times lower than the expenses on rebuilding, management decided to give it a shot – even if we did not have a guarantee that we'd get the data back.'

LESSONS – AND THE COURAGE TO GO PUBLIC

Indrek Kink believes that the attack was made possible by several events coinciding: 'We have now updated our systems from the security aspect and added one more, completely offline backup copy.'

As people are generally reluctant to talk publicly about cyber attacks, Jürgen Erm praises the companies for their courage: 'It helps prevent the next possible attacks. At the moment, self-censorship is prevalent – there is a fear of harm to reputation. But this example is living proof that talking about it does not cause damage – on the contrary.'

DENIAL-OF-SERVICE ATTACKS: the previous record smashed

In terms of DDoS attacks, last year was a serious successor to 2022. Not only did the year bring the sheer scale of DDoS attacks in numbers, but they also became more accurately targeted.

In 2023, CERT-EE registered 484 distributed denial-of-service (DDoS) attacks – 182 more than in the year before. On average, every month saw about 40 DDoS attacks, with the brunt of them against the public sector. The point of these attacks was to flood the target with a large quantity of queries, to disrupt a website, database, or other service. Some of the DDoS attacks last year were very intense. For example, the number of queries that swamped one vital service provider last year in one attack amounted to the number seen over several years in an ordinary situation.

MOST ATTACKS HAD NO IMPACT

The lion's share of DDoS attacks against Estonia did not cause significant damage or extended downtime in vital services, although there were some unfortunate exceptions. In autumn, train ticket sales both online and aboard trains was interrupted due to an attack against Ridango, which administers the ticket sale systems of the passenger train company Elron.

September stood out, as CERT-EE registered 84 DDoS attacks in that month alone. That was the most we had ever seen since we have been measuring the attacks. In calmer years, that has been more like an annual total.

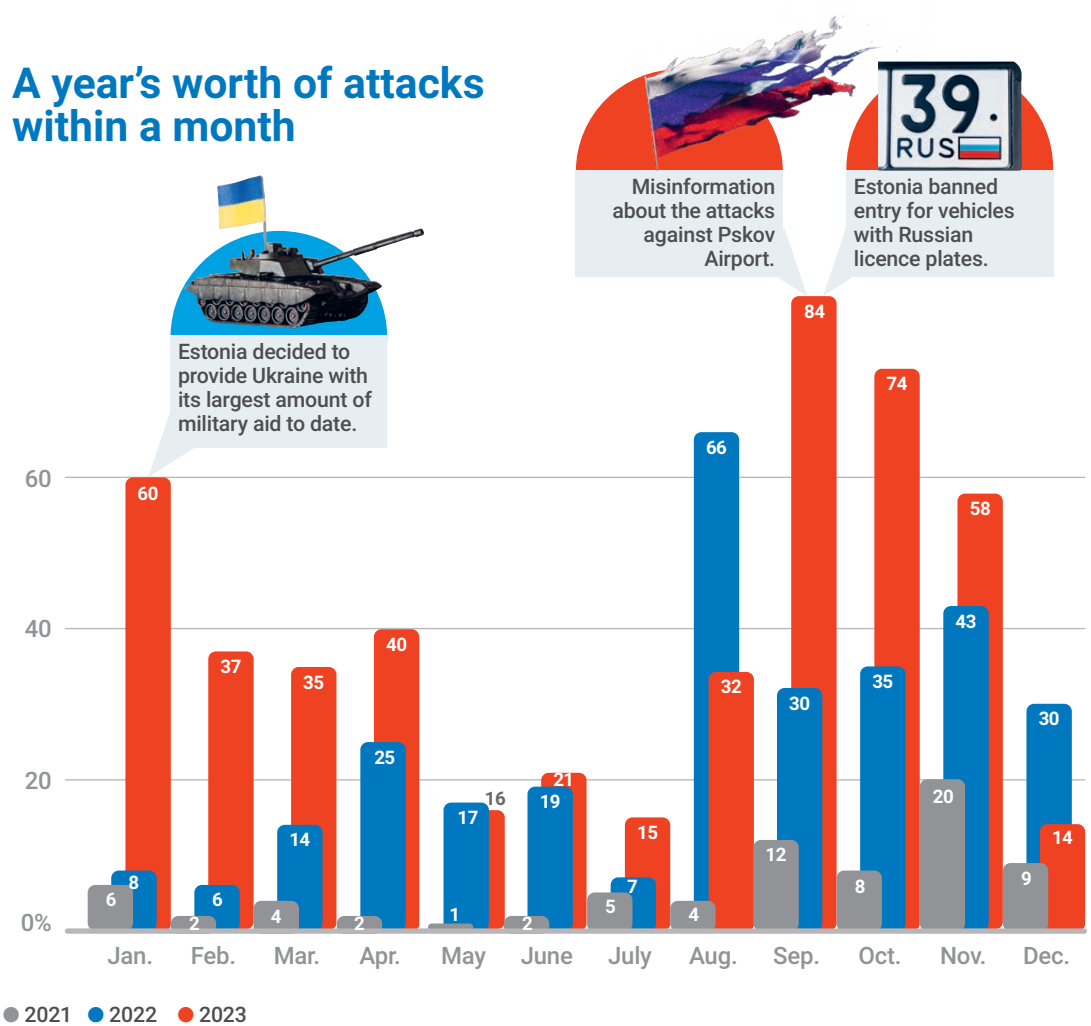
What was the reason for the record number in September? Two events were the likely cause. In late August, the media of the Russian Federation reported rumours that Estonia was responsible for attacks on an air base in Pskov. This was fake news, but led to a wave of DDoS attacks against Estonian websites a few days later. Another reason may have been Estonia's decision to ban cars with Russian Federation licence plates from entering Estonia.

DDoS attacks with roots in political events and decisions have become a common phenomenon and the trend is likely to continue this year.

ATTACKS BECAME MORE TARGETED

Last year also saw a few changes in DDoS attacks against Estonia. The DDoS attacks seen in 2022 tended to be less sophisticated, similar to each other, sometimes amounting to blunt-force attacks on websites that ultimately proved unsuccessful. In 2023, however, the attacks became more precisely targeted, the attackers

A year's worth of attacks within a month



made more careful preparations and tried to derail the targets with all their might.

For the most part, the attacks had a short duration and the servers of cloud service providers were used. The short-duration attacks tested the target's resilience. If the opening round of attacks was successful – if it caused disruption or downtime –, a second, significantly longer phase followed.

Besides the above attributes, attacks on domain name servers were more frequent last year. Like a phone directory, DNS matches up IP addresses and domain names – the user does not see a string of numbers delimited by periods, but rather a legible URL like ria.ee. A successful attack against a domain name server can impact the operation of many web services simultaneously.

What might 2024 bring?

- The calibre of DDoS attacks will likely improve, due to which the number of attacks with an impact could grow.
- The use of the servers of cloud service providers for DDoS attacks will continue.
- IoT devices may also increase the intensity of DDoS attacks. IoT devices often have lower levels of protection and are easier to compromise.
- Politically motivated DDoS attacks will also continue.

LOOKING BACK on a year of fraud

While companies were fighting against denial-of-service attacks, ransomware, and data leaks last year, individuals were surrounded by fraud from every conceivable origin. Last year, criminals defrauded people in Estonia of at least 8.3 million euros.

Like our digital society, cybercrime has been developing dynamically in recent decades. The first digital bank robbery occurred back in 1995, but cybercrime was still a relatively new and rare phenomenon in the first years of this century. The cyber criminals were often young. They used their skills and technology to destroy systems or cause disruptions, but generally, their goal was not to reap financial gain.

The situation changed as an increasing part of the banking and retail and communication moved online. Criminals gravitate to wherever people and money go. Fraud that is committed electronically, also known as internet fraud, has now become the most popular type of cybercrime and its share has also grown in Estonia.

A WELL-OILED MECHANISM

Internet fraud is increasingly sophisticated and ingenious. New technologies like AI and machine learning have taken their place alongside old tools and tricks. This form of organised crime has been honed to the details. Hundreds of people work in large call centres. Like telemarketers, they follow scripts, with separate scenarios written out for likely responses and reactions.

It is an assembly line of sorts: one 'specialist' establishes trust and rapport, another introduces 'investment opportunities', a third provides instructions for entering data and how to conduct the transaction. Instead of turning out a product, this assembly line is designed to separate the victim from their money.

One of the people who contacted RIA got a call from a person speaking Russian and posing as a Police and Border Guard official. The fake police officer persuaded the victim that a fraudster had made a notarised power of attorney in the victim's name, and that urgent action was required to ensure that their funds were safe. The impersonator tricked the victim into entering the PINs of their ID card. The next day, they found out that an attempt was made to take a bank loan of 5,000 euros. It did not go through, but unfortunately, the criminals did steal 10,000 euros from the victim's bank account and more than 1,500 euros from their spouse's account. The Police and Guard Board tallied 524 victims of telephone fraud alone and the losses amounted to 3 million euros.

Another person received a phishing email claiming to be from the logistics company Omniva, asking them to pay for a delivery. As they had recently ordered goods from a store and chosen Omniva to deliver it, they did as the fraudsters asked and supplied their bank card data. That

How to AVOID BEC scams?

- **Be careful online and never enter your password on suspicious pages.** Most BEC schemes start with a compromised email account and compromised email accounts start from a password leak or password entered on a phishing page. Easy-to-guess or simple passwords also make accounts vulnerable.
- **Educate co-workers** about the importance of being aware of BEC schemes and other scams.
- **Check whether the counterparty really wants to switch to different bank details.** Always be sceptical if someone is seeking a last-minute change in the bank account for a transaction. Contact them via a safe channel and make sure it is indeed your business partner, not someone impersonating them. Sometimes, a quick phone call is all it takes. Do not call the phone number in the email, of course, but go to the company's official website.
- **Apply security measures on the email server.** Authentication protocols such as SPF, DKIM, and DMARC help prevent email fraud. in addition, turn on two-factor authentication, as that substantially lowers the probability of criminals accessing email accounts.
- **Check the sender's email address and other irregularities.** Sometimes, fraudsters register a domain that bears a superficial resemblance to that of a well-known company. A difference of a single letter is not necessarily always obvious.

mistake cost the victim more than 10,000 euros.

A third person sold perfume on Facebook Marketplace. They were contacted by a potential buyer who asked for courier delivery to Elva. The prospective buyer sent the seller a link to a phishing page, also designed to look like Omniva's site, and asked that the seller enter their data and confirm the data with PIN. The victim complied. Meanwhile, the criminal logged into the victim's corporate bank account and stole almost 13,000 euros.

MILLIONS DEFRAUDED VIA BUSINESS EMAIL COMPROMISE

BEC (Business Email Compromise) is a scheme where the criminal compromises a business email account, monitors the correspondence, and, at an opportune time, sends out an invoice identical to a legitimate one. Only the account number is different.

Some online crimes, such as phishing and fraudulent phone calls, mainly target random user numbers and email addresses, but in BEC fraud, the criminals make thorough preparations and target specific companies. In terms of monetary losses, BEC schemes can thus be much more devastating than ordinary fraud.

At the end of the year, criminals used a BEC scheme to try to defraud a victim of an amount in the millions of euros, but fortunately, they came away empty-handed, as the employee double-checked with the partner whether they had changed to a different bank and whether the invoice was truly supposed to be paid to a new account.

BEC schemes can be carried out in two ways, depending on whether the buyer's or seller's email account has been compromised. In a scheme that compromises the email account of a company or individual planning to sell a service or product, the customer is sent an invoice with the wrong bank details. Many such customers do not suspect anything is amiss, as the invoice comes from the company's official email address, and they duly transfer the funds to the criminals. The fraud often comes to light several weeks later, when the buyer starts making inquiries about the status of the delivery. As far as the buyer knows, they have paid for it, but of course, the transfer was sent to the fraudulent account.

In terms of monetary losses, BEC schemes can thus be much more devastating than ordinary fraud.

Criminals who compromise the email account of someone planning a purchase have to take a different approach. First, they review the previ-

ANATOMY of Facebook Marketplace scams

Last year, CERT-EE received six times more reports of successful Facebook Marketplace scams than it did in 2022.

Criminals have lists of tens of thousands of emails and telephone numbers of people in Estonia. The success of mass emails and texts to these numbers – often purporting to be from a bank or delivery firm – hinges on the quality of the phishing texts and websites and sheer luck. When criminals send out phishing attacks imitating a specific bank or delivery company, many of them reach people who are not clients of that bank and

ous correspondence with the person to whom the email account holder plans to transfer funds. Using the information from the correspondence (such as the recipient's email name, transaction details, amount, etc.), the criminals send an email from a different email account to the same compromised email user, emulating the company to which the person was to make a payment. The fraudsters often change the rules on the compromised email account so that the emails from the transaction counterparty do not arrive, but are diverted to the fraudsters' email box.

TWO SUCCESSFUL BEC EXPLOITS FROM THE PAST YEAR

In October, Mary (name changed), an employee of a car sales company, got a letter from the accountant of a subsidiary telling her that Mary had sent an email asking for a change in the bank details on file for her company. Mary realised right away that something was off, as she had not sent such an email. Looking into the situation, she saw that the subsidiary had already transferred around 40,000 euros to a stranger's bank account.

As she had not found anything suspicious in her Sent box, Mary asked the accountant to send her the email where the fraudster impersonating her had asked to update the bank details. The accountant did so, but the email didn't arrive in Mary's inbox. So, it turned out that her email account had been compromised some time ago and the criminals had been sending mail for two months before the fraud was discovered. The fraudsters had deleted the email from her Sent items folder and changed the rules on receiving mail to make it harder to conceal the fact that the account was compromised.

John (name changed) wanted to buy a car from a German company. Having picked out a suitable vehicle, he contacted an employee of the company and after a brief exchange of emails, they agreed on the terms of the transaction. John sent the company's representative his contact information and other details needed to draw up the contract. A few days later, he was emailed the draft contract, signed off on it, and sent it back to the company. Just an hour later, someone claiming to be an associate with the same company contacted him and sent a new contract where the bank details had been changed. At first, John did not suspect fraud and transferred close to 50,000 euros to the new bank account. Only when he received a new email asking for 20,000 more euros – due to a rise in the VAT rate in Germany, the company allegedly needed additional money so it could release the car – did something seem rotten. John contacted the company's employee by phone and heard from them that they had not received any money from him.

are not expecting a parcel. Figuratively speaking, the criminals throw a pot of spaghetti at the wall in hopes that some of it will stick.

Scams perpetrated via Facebook Marketplace are slightly more sophisticated. In this case, the potential victims are people who are selling something, and are contacted to buy the item. They then come up with some excuse that the seller has to be the first to ante up money (for the delivery of the goods or insurance, for example). They promise to settle up afterwards, but first, the seller has to set up the order.

The fraudsters often ask for the seller's name, address, telephone number. No doubt they can sell this data for commission of subsequent fraud, but above all, they ask for it to make the exchange seem more plausible. The phishing site that the fraudsters send to the victim as a web link is the actual trap. The page imitates various delivery services (Estonia's Omniva, DPD, DHL, etc.).

The unsuspecting victim is glad to finally be able to unload the merchandise, enters the data as bidden and, 'confirms the transaction' using Smart-ID or Mobile-ID PINs. No sooner does this take place than the fraudsters use the credentials to log into the victim's bank account and help themselves to whatever they can.

More ZERO-DAY SECURITY VULNERABILITIES than usual

Similarly to previous years, various vulnerabilities proliferated in 2023, but what made the year extraordinary was the number of zero-day vulnerabilities and how frequently they were discovered.

In spring, an online store was hit by a cyber attack that may have resulted in the personal data of customers being accessed. Attackers exploited a vulnerability in the e-commerce software used by the store despite the fact that the vendor of the software had released a patch more than a year earlier. Although there may have been a number of reasons that patch installation could have been postponed (price, complexity, the need to keep the website available, etc.), any such delay has to be weighed against a successful attack and its consequences. Successful attacks can result in irrecoverable losses.

OUT-OF-DATE PLUGINS OPEN DOORS FOR ATTACKERS

CERT-EE sees frequent examples in Estonian cyberspace of websites that have their 'doors' wide open. Last year, it notified website administrators of vulnerabilities related to plugins on 500 occasions. CERT-EE also came across websites that had already been hijacked due to outdated plugins.

The more plugins a site uses, the wider the crack in the 'door' for attackers could be. Matters are often made worse due to the fact that updating the website's operating platform itself does not necessarily automatically update the plugins. For that, additional steps are required, which are all too often ignored. As a result, unwanted visitors could show up.

Once intruders have established access to a website, the rest depends on their goals. Among many other possibilities, malware can be added to websites to steal visitor data (including their bank credentials) or to redirect visitors to fraudulent sites.

A YEAR OF ZERO-DAY VULNERABILITIES

2023 will be remembered by the number and frequency at which zero-day vulnerabilities were detected. A zero-day vulnerability is one that has not been patched at the time it is exploited, or the developers may not be aware of the vulnerability at all. For example, during the past year, Apple patched 20 zero-day vulnerabilities, while Google patched seven in its Chrome browser. Zero-day

vulnerabilities are dangerous and also often favoured by different state actors. For instance, Norwegian government institutions were attacked in summer via a zero-day vulnerability related to a software platform, other similar examples could be additionally found from last year as well.

A zero-day vulnerability was also exploited in Estonian cyberspace in 2023. It was related to a vulnerability regarding Cisco software, of which the vendor first notified the public in October. The vulnerability put in danger all web interfaces related to the software, especially those that were publicly accessible from the Internet. In essence, the vulnerability allowed attackers to completely take over the affected devices. Three days after the public announcement from Cisco, about 100 vulnerable devices in Estonia had been hijacked.

The latter is a vivid example of how quickly attackers could identify vulnerable devices and compromise them in the modern era. Compromising devices is not a matter of days anymore, but it can happen in hours. The incident also demonstrated how high the risk is associated with anything that is publicly available on the internet. In some situations, it is essential for a device to be publicly available, as alternative solutions may not exist. However, the sad reality is that in 2023, CERT-EE saw, more often than not, devices accessible from the internet that actually should not have been there in the first place.

XSS VULNERABILITIES RAMP UP

Since RIA's bug bounty program was launched in 2022, we have received 11,000 reports on different vulnerabilities, 7,859 of them last year. More than half were related to XSS (cross-site scripting) issues. Figuratively speaking, an XSS attack is like a vandal sneaking a harmful message onto a public billboard, which then tricks people who see it into revealing personal information or performing unwanted actions. This occurs when a website unknowingly displays this malicious message, believing it to be harmless content. Web applications have to be regularly tested to detect XSS vulnerabilities. Software must be checked to make sure it is up to date, as outdated software is often the main source of XSS vulnerabilities.

9 RECOMMENDATIONS for keeping yourself safe against security vulnerabilities

1. **Keep your operating system, applications, and other software up to date.** Software updates often include patches of security holes detected after the last update. Allowing automatic updates ensures they will not fail to be installed.
2. **Use trustworthy and updated antivirus software.** Such programs can detect, block, and eliminate malware that tries to exploit security holes.
3. **Be IT-conscious when it comes to emails, messages, and websites.** Phishing attempts try to lure people into revealing sensitive information or download malware. Avoid clicking on suspicious links or attachments in emails, especially when they come from unknown sources.
4. **Create a strong and unique password for each account.** This helps to protect you especially in situations where a password of an account is compromised and it is used to access your other accounts that use the same password. Use a password manager, if needed, to better manage unique and strong passwords.
5. **If possible, use multi-factor authentication** (MFA), which gives another layer of safety if passwords leak.
6. **Keep yourself up to date with security risks.** We recommend subscribing to the CERT-EE newsletter and reading the RIA blog, where you will find weekly summaries of the most important security vulnerabilities.
7. **Limit assigning user privileges for the software and apps you use.** This can reduce the risk of malicious software accessing sensitive data.
8. **Protect your network.** Use a secure Wi-Fi connection and consider using a VPN to establish an additional layer of security.
9. **Educate yourself and those around you about good cyber security practices.** The more IT-conscious you are, the lower the chance of falling victim to cyber attacks. Visit itvaatlik.ee and ria.ee for more useful resources.

2023 EVENTS in international cyberspace

Geopolitical tensions – above all, continued Russian aggression in Ukraine and the escalation of the conflict between Israel and Hamas – were also reflected in international cyberspace. Ordinary cybercrime also continued.

How do APTs work?

APTs often use spear phishing: a person of interest, such as a journalist or diplomat, receives a normal-looking email and attachment. The attachment may be a report, institutional budget, or an invitation to an event – the bait is any topic that the target presumably is involved with day-to-day and thus does not arouse suspicion.

APTs are technically highly skilled threat actors who prepare their attacks carefully and usually aim to remain undetected in the networks for a long time. Hacktivists have the opposite profile. They frequently post on social media, impel each other to carry out punitive actions against countries, and brag about having disrupted websites and services.

State-sponsored groups known as advanced persistent threats (APTs) made attempts to gather strategic information about adversaries and spread malware.

UKRAINIAN GOVERNMENT INSTITUTIONS AND CRITICAL INFRASTRUCTURE TARGETED

In July, Ukraine's CERT announced that **Gamaredon**, a group with ties to Russia's FSB, had actively targeted the Ukrainian government. The targets were sent files containing malware. When opened, the malware began stealing data from the system.

As in previous years, Russian state-sponsored hackers posed a threat to Ukraine's critical infrastructure, trying to penetrate a Ukrainian power grid and cause outages. December saw a destructive cyber attack against the Ukrainian telecom operator **Kyivstar**, which left millions without a mobile signal and internet service for several days.

STEALING MONEY FOR THE STATE BUDGET

Cyber attacks against critical infrastructure also took place elsewhere, not only in crisis hotspots. In November, **DP World Australia**, the country's largest operator of ports handling about 40% of all imports, was hit by a cyber attack.

The company said critical systems had been compromised and marine transport and cargoes were seriously disrupted for several days. Although the attacker is not yet known, the technical sophistication points to some state-sponsored APT rather than cyber criminals out for financial gain.

Some APTs focused on filling their state budget – the North Korean group **Lazarus** was implicated in a number of attacks on large crypto trading platforms (**AtomicWallet, CoinsPaid, Alphapo**, etc). According to cyber security firm Recorded Future, Lazarus has stolen 3 billion dollars' worth of crypto assets over the last six years and used them to fund state pro-

→

grammes. The FBI also accuses Lazarus of a theft of 41 million dollars from the gambling platform **stake.com** in early September.

HACKTIVISM CONTINUES TO PROLIFERATE

Ideological hacktivism, which reared its head in 2022, also spread in cyberspace in 2023. Hacktivists principally rely on denial-of-service attacks, flooding websites of government institutions of countries whose policies they disagree with, as well as targeting the transport, financial, and media sector.

A typical example of politically motivated hacktivism was a denial-of-service attack against German websites in the beginning of the year, after Berlin had approved a decision to send tanks to Ukraine, and attempts to take down websites of Lithuanian tourism and transport companies in the run-up to the NATO summit in Vilnius in the summer of 2023. Hacktivists opposed to Israel caused concern in many parts of the world in December with a series of attacks on Israeli-made programmable logic controllers (PLCs). In County Mayo, Ireland, such an attack brought down a local water facility, leaving 160 households without water supply for two days.

RANSOMWARE BROUGHT CHAOS

Ransomware attacks were a widespread and lucrative category of crime in 2023, with a constantly evolving business model. The cybercriminal group **Lockbit** stood out as being particularly active in ransomware attacks.

In January, Lockbit attacked the UK's **Royal Mail**, causing thousands of cross-border letters and parcels to be delayed by several months. Facing disgruntled customers, the company was forced to implement improvements to its infrastructure and processes costing more than 10 million euros during the year.

Lockbit also penetrated **Boeing**'s IT systems in October and stole 45 gigabytes of data for the purposes of extorting a ransom. In early November, a ransomware attack traced to Lockbit hit China's largest commercial bank, **ICBC**.

Major business losses were also caused by a ransomware attack against the entertainment and hotel giant **MGM Resorts** – over 100 million USD. In addition, ransomware attacks disrupted various municipal services in American cities last year.

Ransomware criminals are generally opportunistic and will not spare even the healthcare sector. Early last year, a ransomware attack hit a **Barcelona hospital**, resulting in 150 scheduled surgeries being postponed and 3,000 cancelled doctor's appointments.

On 24 December, a German hospital chain was hit, forcing it to interrupt the work of the emergency medical department at three hospitals and scramble to reassign patients during the holiday rush period. A ransomware group called **Rhysida** attacked a hospital in Jordan and a prestigious private hospital in the UK, stealing sensitive medical records to apply more pressure on the victims.

DATA LEAKS CONCERNING TENS OF MILLIONS OF PEOPLE

Governments and private firms announced major data leaks on several occasions last year. In January, the global telecom **T-Mobile** said that the names and data of 37 million customers had leaked from their database.

In August, the UK Electoral Commission admitted they had fallen victim to a long-term, complex cyber attack. The hackers managed to get election register data on millions of voters, including their names, addresses, and phone numbers. Although the commission confirmed that the breach did not affect the security of elections per se, the leak of personal data does increase the risk of phishing and identity theft.

The French public employment service **Pole Emploi** also suffered a major data leak in August. Names and social insurance numbers of about 10 million job seekers had leaked; the breach was reported to France's data protection inspectorate. Allegedly, the database was put on sale on the dark web for just 900 dollars.

Leaks of sensitive medical records happened not only in Estonia. A scandal involving a reputable beauty clinic in Beverly Hills, California, broke in summer. The criminals had accessed the clinic's information system and stolen patients'

data. As the clinic rebuffed the extortion attempts, the criminals began posting 'before' and 'after' photos and details of cosmetic surgeries while the patients were not even aware that their sensitive data had leaked.

SUPPLY CHAIN ATTACKS: ONE VULNERABILITY, A THOUSAND VICTIMS

For years, Estonia and other countries have warned of the increasing risk of supply chain attacks. In 2023, one of the supply chain attacks that drew the most coverage concerned the file transfer app **MoveIT**.

A zero-day vulnerability was found in what was otherwise considered a very secure piece of software. The ransomware group **Clop** began exploiting the vulnerability actively in early summer. As MoveIT is used by many organisations all over the world, the number of victims rose quickly to 1,000 institutions and companies, most of which were in the US.

The data leak that hit Pole Emploi in France also started through the customer management software developer **Majorel**, which had fallen victim to the MoveIT supply chain attack a few months before that. Majorel has a branch in Estonia, but there is no information about Estonian customers being affected.

In March, hackers believed to be from North Korea compromised the conference call application of the software developer **3CX**. Its users range from international hotel chains to healthcare service providers that use the 3CX app for voice and video calls. The hackers managed to penetrate the software developer's systems through a different software developer, **Trading Technologies**, when a 3CX employee inadvertently downloaded malware-laced software. This was a supply chain attack that led to the next supply chain attack.

Attacks through service providers caused unfortunate incidents also in the Nordic countries. In July, the **Norwegian government** announced that 12 ministries had been impacted by an extensive cyber attack. All these ministries depended on a single service provider whose software contained a vulnerability.

In August, several hundred companies in Denmark lost access to websites, mail services, and other data entrusted to the cloud-based service providers **CloudNordic** and **AzeroCloud,** which were hit by a ransomware attack. The data could not be restored.

SOME OPT FOR SILENCE

Few, if any, countries in the world were completely unscathed by cyber attacks in 2023. There are, however, major differences in the extent to which governments and companies talk publicly about the incidents and what steps are taken to reduce cyber risks and curb international cybercrime.

In May, the **US government** and the Five Eyes intelligence alliance between Australia, the UK, Canada, New Zealand and the US announced that a joint operation had neutralised the Snake cyberespionage malware developed by the Russian Federal Security Service (FSB) and relied on for 20 years. It would be naive to expect that Russian cyber espionage would significantly drop in activity around the world, but it did point out the desire and capability of the Five Eyes countries to take concerted action against such threats.

In autumn 2023, the US urged its closest partners, including Estonia, to launch strategic dialogue to increase cyber security in the civil society, among groups that have received relatively less attention. It is too early to speak about results, but committing political and financial resources to cyber security is better than dealing with the consequences of significant attacks.

In closing, last year brought bad news for many officials fond of browsing TikTok videos on work devices in their free time. In February, the use of **TikTok** on the work devices of EU institutional staff was banned. Canada, Australia, Belgium, and Norway joined the list of countries who do not allow TikTok to be used on the work devices of government agencies. Estonia had banned TikTok on work devices in several government institutions earlier. Last year, the restriction was extended to all centrally administered mobile devices of government institutions.

RIA's RED TEAM: 'We want to attack infrastructure'

It might be surprising to hear such a comment coming from a member of the staff of the authority responsible for the country's cyber security, but that is precisely the goal of RIA's Red Team: subjecting information systems to a tough test so they would be better protected against malicious attackers.

RIA's Red Team was set up a little more than a year ago. Team members see themselves as partners for government departments and companies looking to find weaknesses in their systems, as well as in helping raise awareness among staff and management.

The team's work combines the human and technological sides of cyber security: they send out phishing emails and probe the security on websites and online services, also perform physical penetration testing. In short, to use criminal slang, they 'case the joint'.

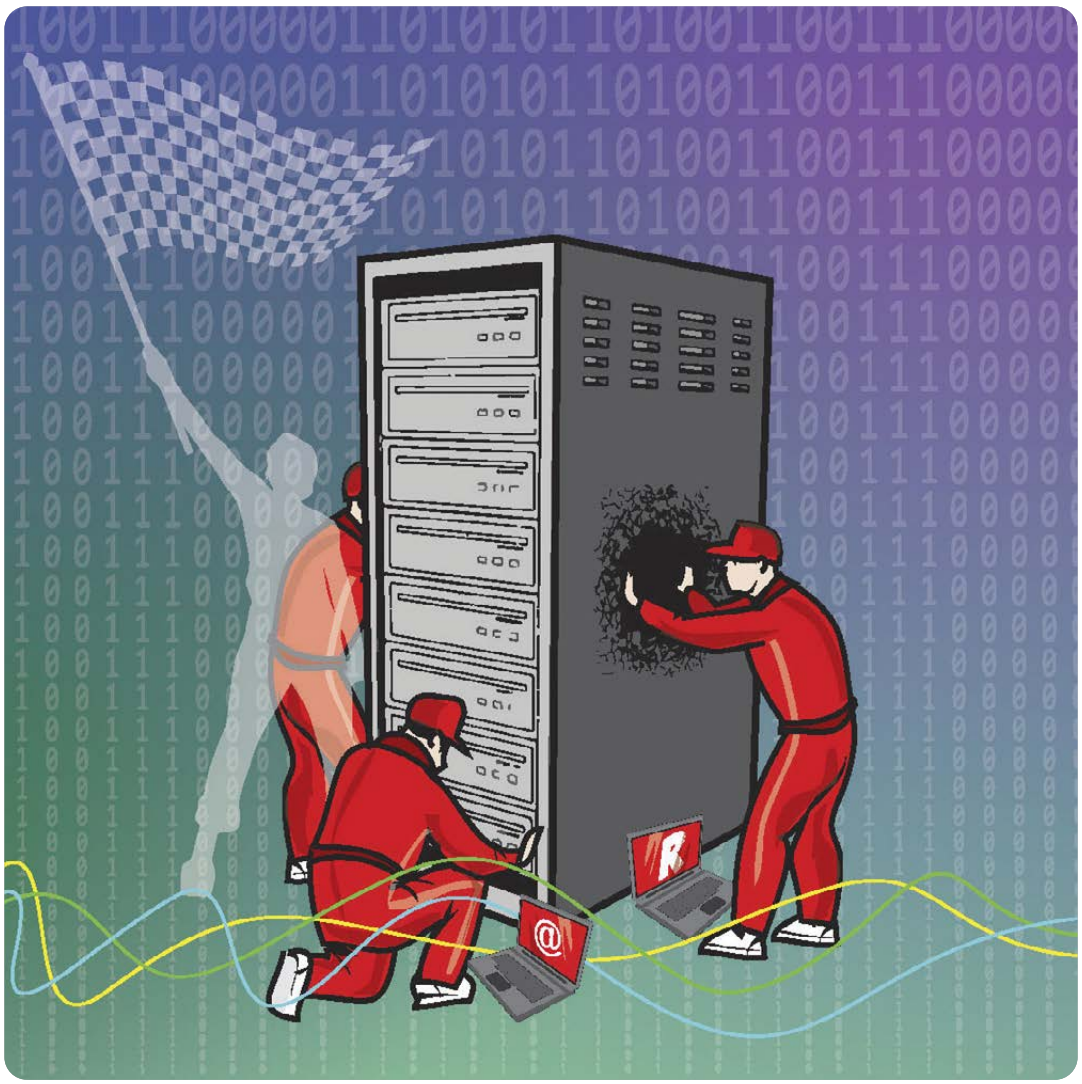
The Red Team tries to do what an attacker might do to see how easy it is to break in and what information could be stolen. An important consideration in performing any sort of testing is that it has to be non-destructive, and the vital service must remain available.

WHY AND FOR WHOM?

Red teaming encompasses the public sector and private vital service providers: government bodies, hospitals, telecoms, energy companies, and others. Interest has been so high that there have been waiting lists at times.

Most clients have already reached a certain level of maturity on data security matters and elementary problems have been resolved. There has been a shift to outside-the-box thinking: using IT resources for purposes they were not actually designed for.

The approach taken at a given organisation is determined in the course of a discussion with the organisation's chief information security officer (CISO) who is seeking an answer to a question or problem. How aware are the staff about cyber threats? Is anyone genuinely following the security requirements in place? How secure are the



The problems found must be eliminated, which usually means investment.

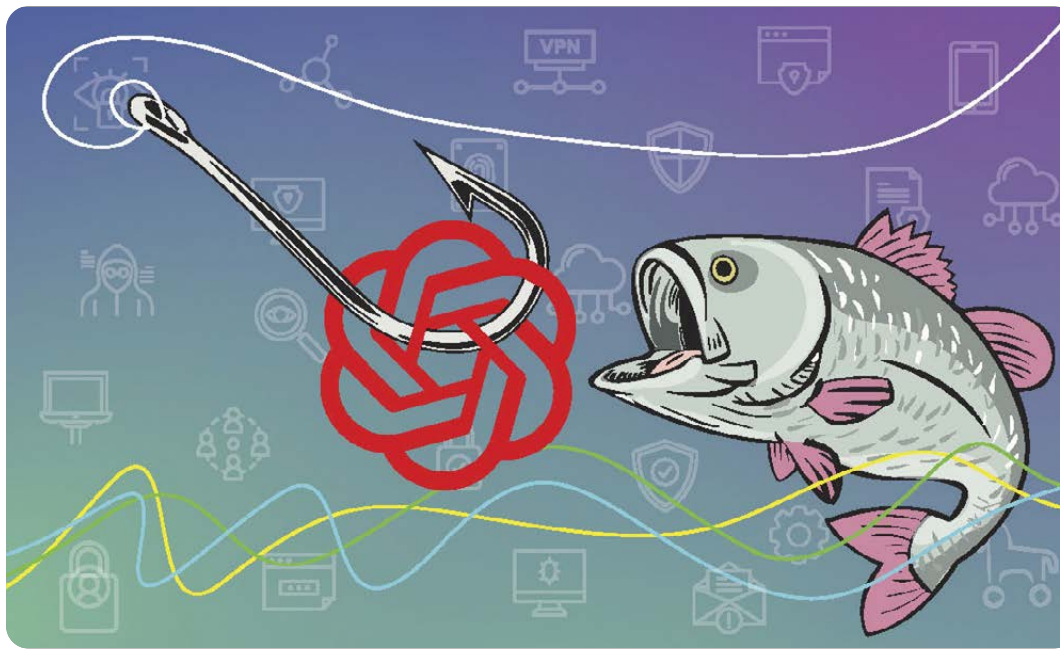
company's web services? How to get the importance of information security across to management? One of RIA's aims is to educate 'smart customers' so that CISOs can ask the right questions later on as well, for example when they outsource a service to the private sector.

The services of the RIA Red Team are taxpayer-funded. However, that does not mean the company ordering the service can just sit back. The problems found must be eliminated, which usually means investment.

ALL IT TAKES IS FOR ONE EMPLOYEE TO TAKE THE BAIT

Phishing attempts have been the most publicly visible aspect of red teaming. They were sent to more than 14,000 people working at central government, local government, or the business sector.

In the case of phishing, the person who receives the email usually clicks on a link and



Artificial intelligence makes life easier for Red Team members

Cybercriminals have discovered the possibilities of AI, but so have the watchdogs of cyberspace.

The RIA Red Team has used ChatGPT to generate ideas for phishing. The AI concocted the following scenario: an organisation has drafted a new workstation monitoring policy that can be read on the website. The AI managed the description of the policy well – a closer read showed that the text was boilerplate, devoid of content, but it might fool a superficial reader into thinking it was the real thing.

The AI also came up with very convincing phishing attacks and can even generate the code for the phishing pages. There are only a few giveaways in Estonian that seem to be based on English syntax and need some editing.

Some experts warn that the spread of AI can lead to automation and job loss on a massive scale, but RIA's Red Team is not worried. Instead, AI can free people from drudgery, letting them focus on aspects that still require human intelligence.

visits a page that prompts them for a username and password. In RIA's experience, about 30 per cent of recipients take the bait, and 10–20 per cent enter their data – and these figures are for organisations where there has been some past outreach on the topic of phishing attacks.

At one organisation, 60 per cent of staff disclosed their data. At some others, the percentage was very low, but there always tend to be a few 'generous' people. And one employee's data is entirely enough for criminals to penetrate and cause a world of hurt. Many of the most serious cybercrimes in Estonia of recent years started with one user's account being compromised.

The main lesson of phishing is thus a simple one: use two-factor authentication (2FA). This keeps the bad guys out of the network even if they have managed to get their hands on a username and password. For the same reason, remote desktop, intranet, and other employee-side services must never be accessible to the public, but only through a VPN with 2FA.

Simulated phishing attacks help raise threat awareness. People think nothing will happen to them, but if they take the bait, it gets them to think about cyber security topics. To make phishing actually useful for improving cyber

hygiene, it must be followed by a debrief – why it was done and how a person should have seen through the scam – and a cyber security training: otherwise, the significance of the incident may be lost on many employees and they might perceive it as harassment.

Phishing attempts also help to assess compliance with security requirements and the functioning of work processes: are suspicious emails reported, who gets contacted for assistance, or how administrators are getting on with their job. Clients must also take into account the risks related to phishing: several hundred employees may call user support at the same time; some may contact the police.

The CISO should carefully consider the climate within the organisation. if people are discontent because larger layoffs or restructuring are underway, it is not a good idea to elevate their stress level further with a mock phishing campaign.

VISITS TO OFFICES

When performing the security testing of websites and services, RIA's Red Team first subjects them to automatic checks in the interests of making the most efficient use of the workforce. Only then do they start looking for vulnerabilities 'manually'. Even if a web application has been tested in the post-development phase, it should be repeated if there have been modifications later or if a major update is being contemplated. Bugs that were not in the original version can arise in the course of the changes.

The must unrewarding scenario for the Red Team is if they discover a vulnerability but it still has not been remedied a year later.

In physical penetration testing, Red Team members try to infiltrate the institution's offices, for example to leave a spying device. They will get the institution's head to sign off on it to avoid later serious misunderstandings.

What does an employee do when asked to change their password due to a leak?

Phishing attacks simulated by the RIA Red Team expose concerning patterns in people's behaviour.

Employees at one institution were sent phishing emails claiming that their passwords had been leaked and asking them to change them. About 15 of the recipients duly entered their old and new password on the phishing page – and the length and first three characters were captured. Analysis of the data showed that for the most part, the beginning and length of the old and new passwords were similar – if the old one was 'Tallinn1', the new one was most likely 'Tallinn2'.

Yet the phishing letter itself mentioned that the password had leaked and in such a case, the password should be changed to a substantially different one. Cosmetic changes to a password will not pose much of an obstacle to criminals.

The CISO should consider what they want to prove by ordering an uninvited guest. Is the possibility of an unauthorised person accessing the office itself a threat? Or is that fairly benign if they cannot, in fact, access information systems?

One possibility is to measure compliance with security rules. For example, whether a stranger posing as a technician on a service call can access the offices, whether their name is registered, are they given a visitor badge or allowed access only with an escort. Are laptops on desks locked to prevent malfeasance?

Any testing is worth performing only if the proper conclusions are drawn – a training course for staff is held or changes are made to the organisation's security policies. The must unrewarding scenario for the Red Team is if they discover a vulnerability but it still has not been remedied a year later.

Let us boost CYBER SECURITY AWARENESS

Coping with growing cyber threats requires everyone to be aware of the threats and conduct themselves safely in cyberspace. With this in mind, we carried out two prevention campaigns last year – one for companies, the other for individuals.

Many companies know relatively little about common risks in cyberspace, as revealed by research by RIA and Statistics Estonia. All too often, cyber attacks cause damage not only to companies themselves, but also to their customers and business partners. The importance of cyber security often dawns on businesses after something serious has already occurred.

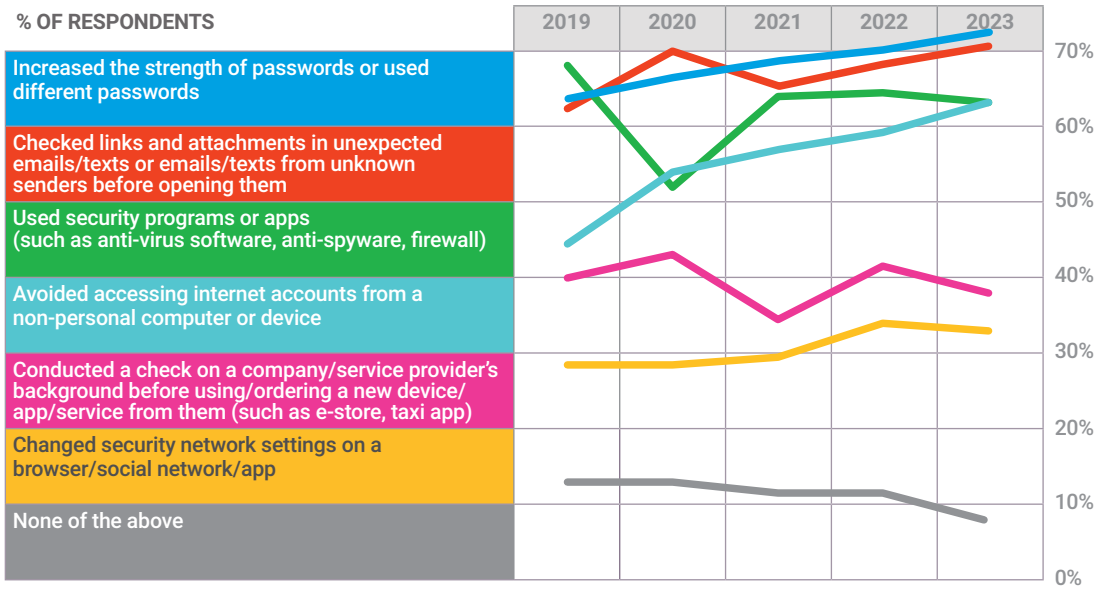
BE IT-CONSCIOUS!

In October, Cybersecurity Month, we kicked off a national campaign to promote prudent IT practices. We drew the attention of business leaders and officials to some of the most common cyber threats and explained how to stay safe: as part of the campaign, we handed out a new cyber security quick guide that helps smaller businesses take the first and most important steps in this field.

The reception from the business community was even more positive than we expected. 81% of the target group noticed the campaign and 91% of those who noticed perceived it as essential. It is gratifying to note that after seeing the campaign, 43% of the target group said that they started thinking about this topic or planned to raise cyber security at their company.

To raise the cybersecurity awareness of compa-

QUESTION: which of these have you done on the internet or an app for personal reasons to ensure your security or privacy?



nies, we partnered with the Estonian Association of Information Technology and Telecommunications and staged friendly attacks on three companies who volunteered as guinea pigs. Even though they knew their systems would be put to the test, all of the simulated attacks succeeded. The participants learned valuable lessons that will help them shore up their defences, and they also shared the experience with the public to raise awareness in the business sector more broadly.

PUT YOUR IT VIGILANCE TO THE TEST

In early summer, we sounded a general call to test IT security by taking a practical cyber defence course at itvaatlik.ee. The short course uses instructional videos to explain how to stay safe against common cyber threats. Knowledge can be tested with a 12-question test.

A nationwide cyber awareness-raising campaign spanned the same time period as the course. This conveyed the basic message of prevention and improved cyber hygiene to a wider audience and encouraged people to take the cyber defence course.

There was also an opportunity to learn about the latest dangers in cyberspace on a series that aired on Kuku Radio, *Ohtlik klikk* (Dangerous Click). Listeners learned about the most common scams, the importance of cyber hygiene, and the online behaviours of children. Experts talked about future technologies and accompanying risks, electronic public service capabilities, and the proliferation of cyber warfare and disinformation. *Ohtlik klikk* drew good reviews, with more than 7,000 listeners. It can be streamed wherever you get your podcasts.

FIVE YEARS OF DATA-BASED PREVENTION

For five years, with help from Statistics Estonia, we have been keeping an eye on cyber hygiene among the Estonian population. Results of the latest survey show that 73% of the population use strong passwords and 71% check emails or links they weren't expecting before opening them. What is particularly pleasing to note is that only 8% of the population have not done anything to increases their personal security or privacy. That figure was 11% a year ago.

The level of cyber hygiene among the Estonian population has improved but there is still room for improvement. Data also points to the fact that many do not use security software (such as anti-virus protection or firewalls) and just a third of people change their default security settings on social networks or phone apps. Thanks to the statistics gathered, we can plan our activities even better and focus on target groups whose cyber awareness is lagging.

CYBERTEST gets off to a fast start

Starting in April 2023, we are offering a free educational platform in the field of cyber security, Cybertest. Last year, more than 200 private and public sector organisations joined the initiative and more than 15,000 people underwent training and testing. What did the responses reveal?

We all use computers and smart devices every day: we send emails, use various information systems, shop online, make payments in internet banks, etc. Anyone performing these procedures should bear in mind the basic knowledge of cyber security and Cybertest is a good chance to brush up on them.

Most cyber incidents are caused by ignorance or human error. Informed computer users have an advantage over someone who is seeing a phishing attack in their inbox for the first time. As the Cybertest is an online course, users can take it at a time of their convenience.

Although the Cybertest is aimed mainly at the public sector and for vital service providers, we also welcome interest from other sectors. The Cybertest is free for all.

MORE THAN 200 ORGANISATIONS HAVE JOINED

During the first year, more than 200 organisations and enterprises joined the initiative. They include ministries and departments in their area of government, local government units, schools, hospitals, medical centres, and businesses.

By the end of the year, nine months later, more than 15,000 people had refreshed and tested their knowledge. The area of government of the Ministry of the Interior and the Ministry of Culture set a great example, with nearly all institutions having joined and successfully adopted Cybertest.

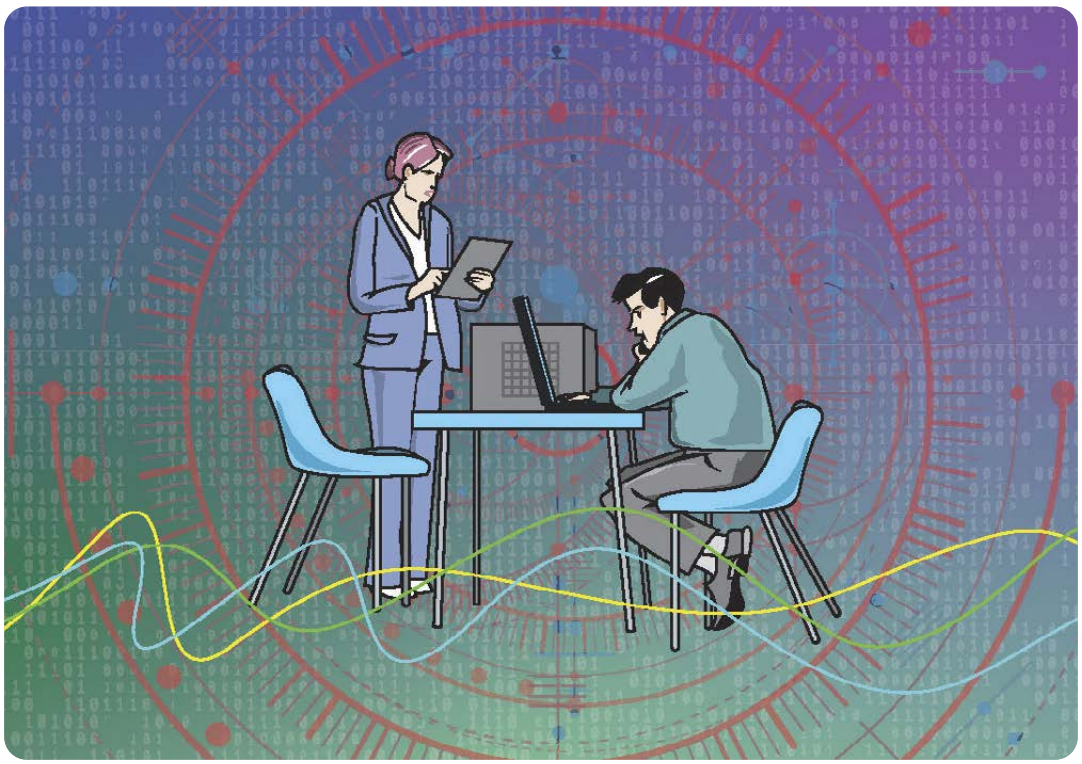
WHAT DO THE RESULTS SHOW?

Most Cybertest users are well versed in the need to protect smart devices and of the risks of remote working – most respondents answer the questions correctly on these topics. The questions that pose more challenges are related to recognising phishing attacks and taking the right action in such cases. Unfortunately, we see this trend when we look at the incidents registered by CERT-EE, too. Every month, close to half of the reports concern phishing and unfortunately, many people in Estonia fall victim to phishing attacks.

Another problematic area is the reuse of passwords – many respondents use the same password in their work computers and their private lives. That is a bad practice, because it could compromise both personal and work-related accounts if the password leaks.

THIS YEAR WILL BRING A CONTENT UPDATE

This spring, we will update the contents of the Cybertest course and test. The new version will cover all of the most important topics: passwords and account security, various phishing



attacks and scams, threats spread by email, secure use and configuration of Wi-Fi networks, USB drives and other media, safe remote work practices, use of smart devices, and dangers on social media.

There are also plans to add some instructional videos to Cybertest, covering all of the most important topics covered by the course. In the videos, we remind viewers of how malware spreads, how to use smart devices more securely, and what exactly a virtual private network (VPN) is. Besides Estonian, in the future the course can also be taken in English.

RIA's aim continues to be to ensure that all public servants pass the Cybertest or some other cyber security training at least once a year.

CYBERTEST IN FIGURES (as at the end of 2023)

- **205** institutions/companies have joined
- **15,160** people have passed the test

RIA's aim continues to be to ensure that all public servants pass the Cybertest or some other cyber security training at least once a year. We recommend everyone else also regularly take a cyber security course. This helps to remember well-known older scams and yields new information about emergent risks. Training participants will see examples of phishing attacks (emails, texts, and websites), making it easier to recognise them.

If you have an interest in joining Cybertest or have a question on this topic, send an email to **kybertest@kybertest.ee**. Visit the RIA website to sign up and to get more information.

THE SUBPAR CYBER HEALTH of family physicians

A screening revealed that cyber health at family medicine centres is far from solid and requires immediate action. The implementation of the new information security standard along with RIA oversight can help prevent serious consequences.

No matter what the state of their health, nearly every person living in Estonia has a family physician to whom they entrust their health data. We do this under the assumption that the data is accurate, cannot be modified by third parties, is accessible when needed, and that the confidentiality of the data is guaranteed.

As no one wants sensitive health data entrusted to a healthcare professional to leak or go missing, the family physician's trustworthiness also relies on cyber health alongside their medical expertise. All too often, the cyber aspect has been neglected.

RIA INSPECTIONS: LIKE A HEALTH SCREENING

The fact that RIA's Supervision Department tackled a comprehensive check of the cyber health of family physicians last year did not stem from any one incident, complaint, or tip. The goal is purely preventative, just like a cancer screening can single out signs of a higher risk. We conduct random inspections to determine how well family physicians adhere to cyber security standards. If the scrutiny reveals any problems, we draw attention to them and grant deadlines for eliminating the shortcomings.

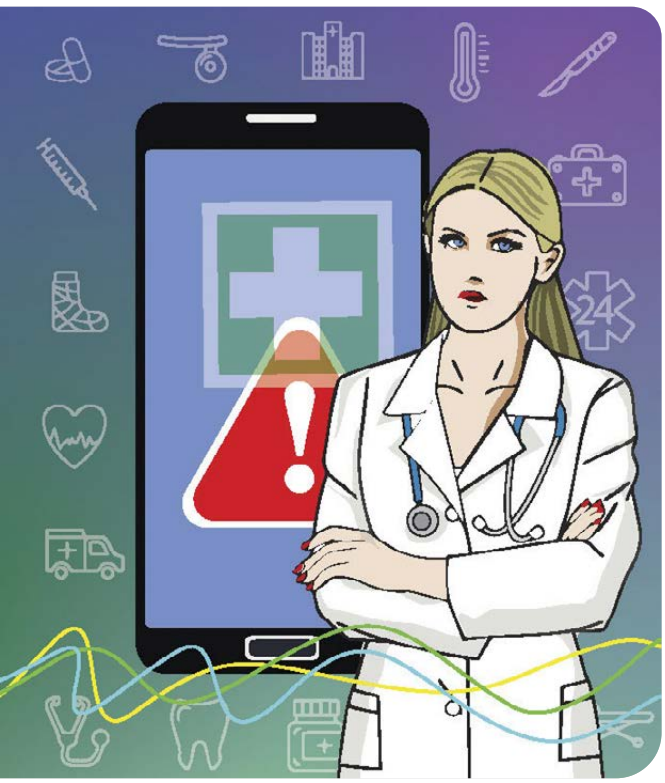
Cyber incidents in healthcare need not be the work of a malicious external party. Technical errors can result in the loss of patient data and one family medicine centre was closed for some time after a server failure. The consequences of the incident were aggravated by the fact that the centre kept the backup copies on the same server – a clear violation of good practice that could have been avoided if caught by an earlier inspection.

Data leaks have unpleasant consequences, such as the violation of patient privacy. Loss of data integrity may lead to a wrong diagnosis and treatment. That is literally a threat to life and health.

Errors caused by internal reasons pale in comparison to external factors. Cyber criminals are actively targeting the European medicine sector and according to ENISA, the European Union Agency for Cyber Security, healthcare is in the top three sectors when it comes to the number of targeted attacks and registered incidents. In

3 recommendations

- Every family physician should undergo RIA's cyber test.
- Every family medicine centre should have a strong IT partner who provides support for the implementation of the standard.
- RIA's recommendations should be followed before an inspection.



Some are HEALTHIER than others

Six family medicine centres – OÜ Aira Perearstikeskus, OÜ Tartu Raatuse Perearstikeskus, Karulaugu Tervisekeskus OÜ, OÜ Pirita Perearstikeskus, OÜ Järveotsa Perearstikeskus, and OÜ Pärnu Perearstid – passed the inspections with flying colours as they have actively and adequately implemented technical and organisational IT security measures. We clearly got the sense that the administration put value on IT security and that they understood and adequately evaluated the related risks. All had in common a competent IT partner who had helped to select and implement the measures.

PROCEEDINGS in figures as of the end of 2023

- 39 family medicine centres are being checked.
- 10 centres are complying with precepts.
- 23 centres are in the investigation and decision phase.
- 6 proceedings have been completed.

Estonia, the headlines about ransomware attacks on family medicine centres have grabbed more attention.

SEATBELT AND FIRE EXTINGUISHER

Any patient would have serious questions if a vaccination jab was not preceded by an antiseptic swab or if professionals did not wear a surgical mask in the operating room. Similarly to health requirements, cyberspace also needs rules.

The safety rules for IT systems have been consolidated in the Estonian Information Security Standard (E-ITS). It is like a cyber security manual that, if properly followed, ensures that an organisation is shielded against most cyber threats. RIA has created a separate profile for family medicine centres, listing the requirements necessary in their work and instructions for starting to implement security administration. We have provided family physicians with several introductory courses and seminars concerning these aspects to facilitate implementation of the standard.

Coming to an agreement and introducing any rules is a long process. Once the rules are finally in place, they also need to be enforced. Patients who have been diagnosed with high cholesterol and prescribed special treatment and a diet are usually summoned to follow-up appointments where, logically enough, another measurement of cholesterol is taken.

RIA has organised a number of free E-ITS training sessions and public engagement seminars for making it easier to implement the standard. We have also issued two memos to physicians about imminent obligations under the Cybersecurity Act and held a special one-day briefing for them. We also informed physicians that we would start enforcing compliance. We reiterated the sensitive and valuable nature of the health data in their hands, the risks arising from the attacks targeting the medical sector, and hence the need to apply cyber security measures.

The Estonian family physicians association is on board with the explanations and says it now has a better understanding of what RIA is seeking to accomplish; they say they will try to spread the knowledge among family physicians.

2023 was a historic year for I-VOTING

Last year's general election in Estonia was a historic one: for the first time, the number of i-votes outstripped paper ballots.

Active preparations for last year's parliamentary elections spanned the entire year at RIA. About 100 of the authority's staff members were engaged in the process in one way or another, in addition to external partners. We were in charge of developing and maintaining the election information system; administering the system for tabulating i-votes; administering and protecting the polling station staff's computers; and election cyber security. We also provided voters and polling station staff with customer support on technical issues.

A WORLD RECORD

Altogether, 615,009 people voted during election week, which ran from 27 February to 5 March. It could be seen as a world record for internet voting (313,514 votes). For the first time in 18 years, the number of i-votes outstripped paper ballots. For us, that is a sign of trust.

Compared to the previous general election four years before, in 2023, we had a new election information system (VIS3), which got its first initiation during the local elections in 2021. The version used for the 2023 election was a further development of the former, taking into account all principles of secure development and making life easier for election organisers, polling station staff, candidates, and voters.

With electronic voter lists, there is no need for workers at polls to use a ruler to keep a manual record of voters, candidates can also register through the election information system, and voters are no longer tied to one specific physical polling station, but rather can vote at any station in their district.

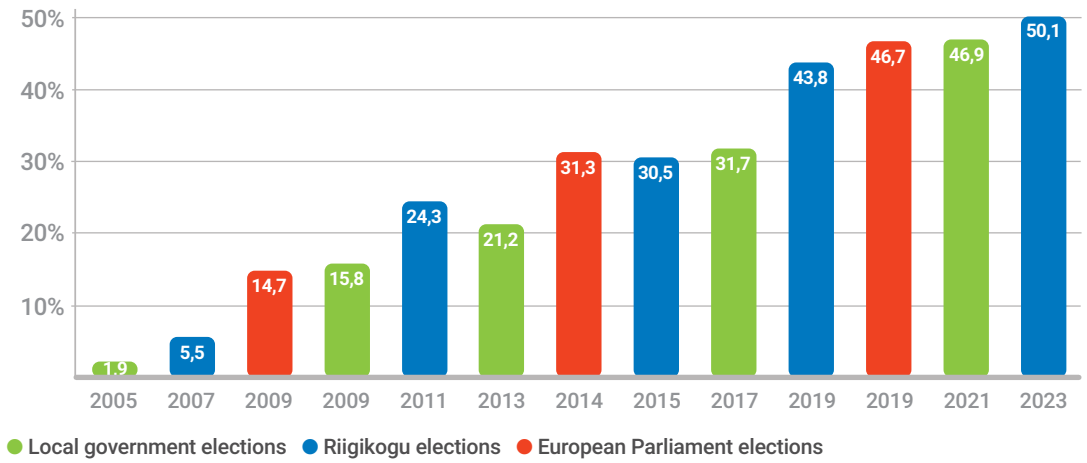
As a new feature, the voting period in 2023 was continuous, with no pause between online voting and election day. Online voters could also vote at a polling station by paper ballot on election day, superseding their previous online vote.

ALL QUIET ON THE CYBER FRONT

The election's IT systems did not experience any problems and it was relatively quiet on the cyber security front, with no attack against the electoral systems detected. There were a few attempts to i-vote using an unapproved app and one attempt at authentication using a Lithuanian ID card, but these were unsuccessful.

The most notorious mistake was caused by the fact that on the first day of the voting week, the last changes to the voter list were imported to the electronic voting system (EHS) after a lag time. As a result, 57 people whose place of residence had recently changed in the Population Register were shown their former electoral district and the candidates running there. The voters who cast votes in the wrong district were

A RECORD: more than half of the votes were cast online



asked to re-vote and in the end only three votes had to be voided.

Two bodies, the Electoral Commission and the State Electoral Office, are in charge of organising elections in Estonia. RIA's role as technology partner has grown since 2019, when we took over the obligation from the State Electoral Office to develop the new election information system (VIS3).

In 2021, election laws were changed, and new responsibilities were imposed for the system. Among other things, electronic voter lists, the open data function, and a referendum option had to be introduced.

In this manner, the government envisioned the election process becoming more efficient and less bureaucratic, like everything else about our digital society. Agreeing on a more permanent cooperation format and risk management model contributes to better planning and process-based organising of development, hosting, operation, analysis, and testing (including security, availability, and stress tests). Work tasks related to EHS are likewise currently divided between the two agencies.

NEXT UP: EUROPEAN PARLIAMENT ELECTIONS

The European Parliament election week runs from 3 to 9 June 2024. Preparations are now in full swing.

TECHNICAL READINESS for m-voting is in place, but is not enough

I-voting has strong support from the electorate but the current voting app can only be used on computers, even though society is increasingly geared to smartphones and tablets.

We have developed a prototype for online voting on other devices, and we have used it to test voting as well as the transmission and acceptance of votes. The prototype supports both Android and iOS devices, and there is support for both m-ID and Smart-ID authentication. ID card NFC support is also being developed, so that there will be one more way of authentication and secure signing. The app's prototype was developed by Cybernetica AS, which also developed the i-voting system. The introduction of mobile voting still requires some legal and organisational issues to be settled and as a result, it will not yet be possible to vote from smartphones and tablets at the 2024 European Parliament elections – only i-voting from computers and paper ballots will be available.

CYBER4DEV: mission accomplished

The first global development assistance project funded by the European Union, Cyber Resilience for Development (Cyber4Dev), came to an end in 2023. Dozens of Estonian experts contributed to making cyberspace safer in a total of 26 countries.

The goal of the project was to support increased cyber security in Africa, Asia, Latin America, and the Caribbean through training and consultation programmes.

For RIA, the five-year-long Cyber-4Dev was the first achievement in implementing international projects. Alongside the consortium partners – the UK and the Netherlands –, Estonia and the Estonian Information System Authority (RIA) provided the main part of the cyber expertise to the project. We drew on 60 Estonian cyber experts from RIA, and from the public and private sector. In total, these experts carried out 220 assignments in 26 countries.

Project activities in places far away from Estonia drifted from ordinary routine and comfort zones. The pandemic-related restrictions and different time zones meant night-time video sessions. Once traveling was possible again, it took more than 24 hours to reach regions on the other side of the world. Interpreters had to be used to train partner governments. Challenges included dealing with power outages and adapting to cultural differences.

DEVELOPMENT OF CAPABILITIES

Our aim was to take as comprehensive approach as possible. We started by assessing the current state of cyber security of our partner countries and identifying shortcomings and needs for training. We followed by drafting a joint work plan

TIMELINE

2017

The UK, Estonian, and Dutch consortium wins the contract to carry out the EU's first global cyber development assistance project. In December, the Cyber4Dev project agreement is signed.

2018

MARCH: first meeting of the project team and the official launch of Cyber4Dev.
SUMMER: first Estonian experts' missions to Sri Lanka, Mauritius, Botswana, and Ghana.

2019

JANUARY: visit of Botswanan, Mauritian, and Sri Lankan CERTs to Estonia.
AUGUST: the first high-level cyber security tabletop exercise **CyberBreeze** in Mauritius.
DECEMBER: Latin American and Caribbean countries are included in the Cyber4Dev project scope. RIA starts steering activities on this front.

with the local government partner and started the execution, mainly focusing on three areas.

1. **Legislation and general cyber awareness.** Estonian experts took part in developing national cyber security strategies for Botswana, Ecuador, Mauritius, the Dominican Republic, Costa Rica, Mozambique, and Cambodia. We raised governments' awareness of cyber threats, organising high-level tabletop exercises. In the last two years, we also laid emphasis on general cyber hygiene. We got inspiration from the cyber awareness campaigns and the Cybertest developed by RIA, which were adapted to Cyber4Dev, according to the needs of our partner countries. In Ecuador, for instance, more than 25,000 public servants used the analogous cyber test platform to improve their cyber hygiene.

2. **Working with cyber incident handling units – the computer emergency response teams (CERTs).** We held trainings for CERTs ranging from work processes to the use of technical tools. The CERTs of nine countries received long-term support from Cyber4Dev to improve their capability. Estonian experts contributed to building national CERTs for Botswana, Mauritius, Sri Lanka, and the Dominican Republic.

3. **We promoted regional and international cooperation.** We carried out regional seminars and conferences to bring together experts from the project's priority countries. The goal was to promote networking and trust between experts in a given region to enhance responsive cooperation in incident handling.

THE PROJECT INTRODUCED ESTONIAN SOLUTIONS AND COMPANIES

Estonia's active efforts in cyber development assistance in distant places like Mauritius, Sri Lanka and Ecuador might seem like a questionable use of resources at first. But in the course of the years-long collaborative engagements, we helped to find export opportunities for Estonian companies and increased Estonia's renown as a leader of a cyber-secure digital society.

> Estonia is an inspiration to many developing countries on how clear policies, decisions and actions can lead to a developed state architecture in just 30 years.

Estonia is an inspiration to many developing countries on how clear policies, decisions, and actions can lead to a developed state architecture in just 30 years. The 2007 cyber attacks against Estonia and the success story that started with the response to them are an instructive example for Costa Rica, who was under devastating cyber attacks in 2022 and who hopes to emerge stronger than ever from the crisis with the support of the international community.

Cyber4Dev's work has been continued by the ongoing EU CyberNet project and the Latin American and Caribbean Cyber Competence Centre LAC4 in the Dominican Republic that serves as a centre of excellence to develop cyber capabilities in the whole region.

2020

DECEMBER: with the assistance of Cyber4Dev, the Dominican Republic's CERT joins FIRST, the international cooperation network for CERTs.

2021

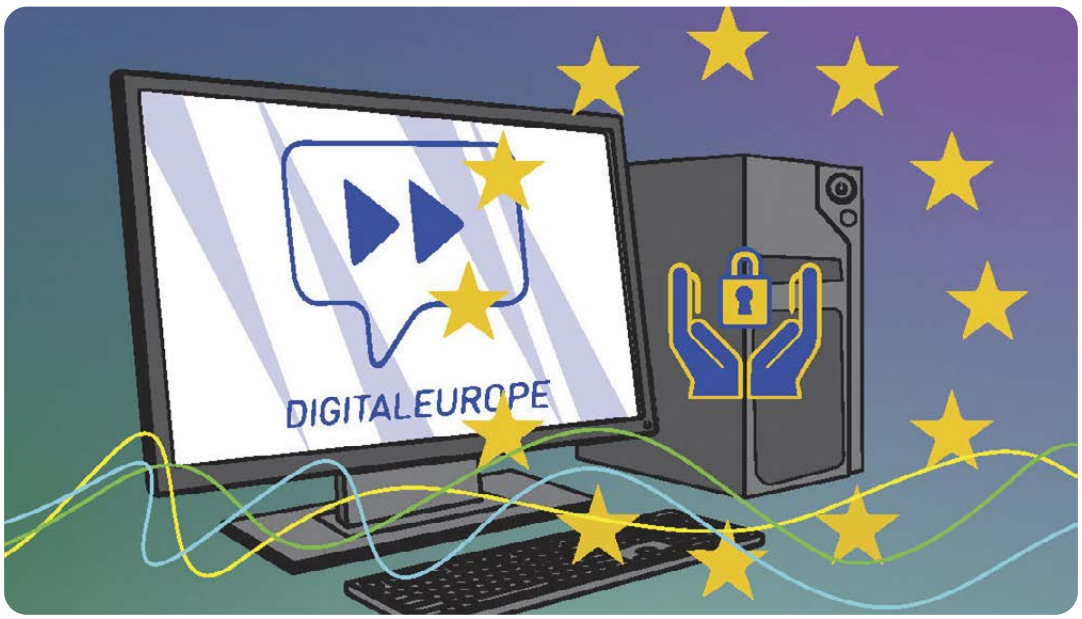
MAY: the Cyber4Dev project is extended by two years. The first high-level cyber security tabletop exercise **Cyber Llamas** for the Dominican Republic.
SEPTEMBER: study visit of the government institutions of the Dominican Republic to Estonia.

2022

JUNE: development of Ecuador's first national cyber security strategy.
SUMMER: study visits of the government institutions of Mauritius, Sri Lanka, and Ecuador to Estonia.

2023

MARCH: the first high-level cyber security tabletop exercise **Tormenta Cibernética** in Ecuador.
JUNE: the first high-level cyber security tabletop exercise for Seychelles. End of Cyber4Dev's active training activities.
OCTOBER: final conference of Cyber4Dev in Florence.



CYBER TRANSFORMATION GRANTS boost cyber resilience

RIA and the Estonian Business and Innovation Agency support small and medium-size enterprises to assess and improve their cyber security posture.

The Estonian government has been providing grants to businesses to boost their digitalisation for years now, distributing millions of euros. In that spirit, RIA rolled out dedicated grants in the spring of 2023 to assess and improve cyber security in small and medium-sized companies.

FIRST, A ROADMAP...

The targeted companies can apply for these grants to procure an assessment of their organisation's cyber security level. The grants are provided only if this assessment is conducted based on the methodology developed by RIA's Critical Information Infrastructure Protection Depart-

ment, which results in a sort of roadmap: suggestions for how the company might improve its cyber security posture within the timeframe of a year.

Standardised methodology – the CyberTransformation methodology – developed by RIA is one element in ensuring the quality of these services. The common approach also gives the entrepreneurs the opportunity to get competitive quotes for a similar service. At launch, 21 cyber security service providers signalled interest in offering the CyberTransformation assessment based on RIA's methodology.

As a result, cyber security service providers find themselves on a new competitive playing field, where prices have come down and more effort has to be spent on sales, references, and generating value added.

...AND THEN, ACTION!

Once the roadmap is produced, companies can apply for an additional grant to implement proposals from the roadmap. The grants available reach up to 50,000 euros depending on the work needed – in some cases, that might mean network segmentation, migrating data to secure cloud services, or an employee training programme. Companies have a 50% self-financing rate in both the roadmap and implementation phases.

> Applications for RIA's CyberTransformation grants are still being accepted this year, as long as the Digital Europe funds last.

Applications for RIA's CyberTransformation grants are still being accepted this year, as long as the Digital Europe funds last. At that point, we can assess the impact of this pilot programme based on the outcomes and decide on the continuation of CyberTransformation.

RIA: growing the cyber security community

RIA fulfils the role of the national coordination centre for Estonia – NCC-EE, which is part of the Network of NCCs under the aegis of the European Cybersecurity Competence Centre. These local coordination centres in every EU Member State promote the local cyber community's research, technology, industry, and educational activities. NCC-EE's activities include:

- **Cyber camp for girls.** As there is a growing skills shortage in the field of cyber security, we are organising camps for youth to introduce the cyber security career path. There is a gender imbalance in this area in Estonia and all around the world, so we are focusing on providing training to girls in Estonia. 2023 saw two one-day camps held in cooperation with the girls' organisation Kodutütred (affiliated with the Estonian Defence League) and a large summer camp, where more than 70 girls from Estonia, Latvia, Czechia, and Italy learned the basics of cyber security.
- **Cyber Accelerator.** In partnership with the Tehnopol Startup Incubator, RIA launched the Cyber Accelerator programme in autumn 2023. Teams accepted to the programme get top-flight advice for developing an original concept and 48,000 euros in grant funding. The purpose of the accelerator programme is to generate new products and start-ups in the field of cyber security. The business ideas hatched by participants must meet one of two conditions: they must be state-of-the-art cyber security solutions for the private sector or a cyber security solutions that benefit new technologies in other sectors. We intend to train 15 start-ups in two cohorts, the second cohort starting in April 2024.
- **CyberMeetUp.** In March 2023, we started a new tradition for the cyber security community: the CyberMeetUp event. Every month, community members are invited to this informal event to hear about the threat landscape and new initiatives in cyber. Anyone who identifies as a member of the Estonian cyber community is welcome to join; the programme is also accessible to our international community in English. The programme is streamed online and can be viewed on demand on RIA's YouTube page.

RIA'S EXPERIENCE: how we are implementing E-ITS

Estonia's information security standard, E-ITS, is obligatory for about 3,500 organisations. RIA is one of them. Due to RIA's public responsibilities and our staff of about 300, we had to review 6,000 IT security measures.

E-ITS was created to ensure that organisations that play a vital role in society are resilient to cyber threats. The best practices of E-ITS are meant to be replicated across different organisations to save resources and time spent on IT security.

For smaller organisations with limited experience dealing with information security requirements, a graded baseline system of security measures might seem a bit intimidating and overwhelming. Yet, it is an opportunity to reconsider business processes – after all, cyber risks are also business risks.

MORE FREEDOM AND RESPONSIBILITY

Compared to its predecessor ISKE, E-ITS helps to attain a level of IT security appropriate to an organisation business needs. Organisation leaders have more freedom – and hence more responsibility – to decide which features and processes must be protected.

The point is to ask oneself what the organisation's objective is, why it is necessary, and what must be done to fulfil it. That will clarify the organisation's business processes. The organisation's protection requirement level is determined by adopting the requirements dictated by the objective and evaluating what damage could be incurred by whom in the case of non-compliance.

When the assets and resources needed to achieve the business goal have been identified in detail, security measures can be attached to them. If assets and resources are similar to those used in many other institutions, standardised security measures can be used. For more specific assets or a greater protection requirement level, measures can be determined by analysing risks.

Once the measures are decided, the organisation will have an idea of which of them have already been implemented and which ones still need to be addressed – in other words, activities can be planned and the implementation of the plan can be monitored. Naturally, not everything is possible at once, and management must be aware of and accept unresolved risks.

THE EXPERIENCE OF RIA

RIA started tackling the implementation of E-ITS in the spring of 2022, immediately after the regulation came into force. A nine-person steering group began seeking answers to the questions of what RIA considered a business process and how to start to determine the protection needs of the business processes.

At RIA, business processes are at the level of service area, and there are over 50 of them. Considering that each unit is generally responsible for its own technical solutions and the administration of servers, the protection requirement had to be determined and information security

measures implemented at this level. The task of determining the protection requirement was new for everyone, and some instruction was necessary. The samples made in the form of joint meetings and the protocol for determining the protection requirement found on the E-ITS portal were helpful.

The implementation plan issue had to be resolved after protection requirement parameters were assigned for service areas in September. We wanted there to be clear associations between assets and service areas to the extent that each business process would be assigned only the relevant information security measures and so that the implementation of these measures could be tracked conveniently and consistently. We decided to favour JIRA, which was already in use, so that the implementation of E-ITS would also be linked with everyday work and processes. By then, the steering group had evolved into a working group of five people with other duties to perform simultaneously.

A very labour-intensive stretch lay ahead – the assets that had so far been administered in different environments had to be moved over to JIRA. It was complicated to put the initial data structure into place, and there was a feeling of perplexity in trying to get all the associations and modelling to function correctly.

HOW DOES IT ACTUALLY WORK?

In early 2023, we tested the structure's functioning on the X-road service area. The pilot project with volunteers was successful and confirmed that the associations created were functional. The goal was to create a solution that is as automatic as possible. To do this, automations had to be created for collecting assets and creating tickets for measures. RIA's architects developed the first of them and we outsourced a second.

In late spring, we updated the service portfolio and reviewed our protection requirement levels with our annual risk management process. The work continued into the summer with developments of automations and we got the whole staff involved in identifying assets.

This was followed by the manual creation of process tickets, and in the second half of the autumn, we began testing with automation. We are now in a situation where tickets for E-ITS measures are generated automatically in the JIRA implementation plan, and their removal also takes place in a similar fashion. The system is viable and sustainable.

ACCOMPLISHMENTS AND CONCERNS

Over the year, a change in the mindset of many of our co-workers has taken place. The technical solution developed in interdepartmental cooperation is seen as a real benefit – it saves departments time implementing E-ITS and makes the implementation of security measures easy to track at the team and organisational level. Yet, just as valuable is the fact that walls between departments have come down as a result of working together due to a common goal and a workflow that bridges product, support, and management units has been created.

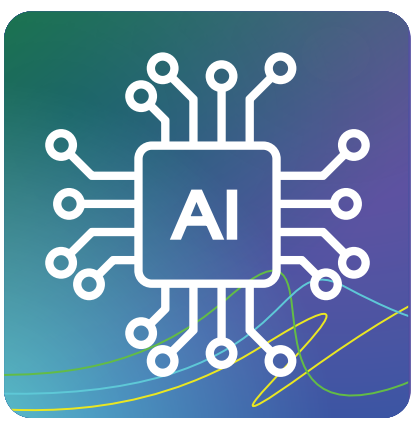
Over the last 18 months, we talked to many others implementing E-ITS to discuss the positives and the concerns. Over time, we have got good ideas from others and shared our solution with about 20 organisations. Last year, we brought our preliminary audit to a successful close and the goal is to complete the main audit in March 2024. We are prepared to share the completed implementation plan with all who would like to learn from our experience.

Looking ahead to the YEAR 2024 in cyberspace

ARTIFICIAL INTELLIGENCE as a game-changer

In recent years, AI has been developing at dizzying speeds, and it is already being used to generate phishing attacks and other scams. It is no longer a distant possibility that it could become a powerful cyber weapon used by criminals and state actors alike to perpetrate incidents with a high impact.

There is a brighter side to the same possibility – that AI can be also be used to architect clever security solutions, ranging from preparing a contingency plan to monitoring systems in real time. At any rate, the coming years will be fast-paced and fascinating in this field.



Cyber resilience in DEFENCE OF DEMOCRACY

Authoritarian countries, for example those situated to the east of Estonia, have been trying to tilt public opinion in Western democracies by spreading disinformation. Such activity usually ramps up before key elections (e.g. US presidential, German Bundestag). In June 2024, the 27 Member States of the European Union will elect their representatives to the European Parliament. Influencing activities can be expected to intensify then as well. Candidates who are not to the liking of hostile states may face attempts to have their email or social media accounts hacked and sensitive information leaked. Attacks against electoral systems are likewise a possibility.

While Estonia's method of internet voting is still unique, other technologically advanced countries also use a myriad of different IT systems for elections. Information security is thus paramount for Estonia and our allies in this context and both personnel at the polls and candidates must keep their guard up.

CYBER rises to management level

With each passing year, it becomes clearer that cyber security is not just something an IT specialist or data security manager has to think about. It has to be monitored constantly and clearly at management level, as the consequences of neglect could cause reputational damage , massive losses of income, or substantial fines due to data leaks. Ensuring cyber security means having to clarify risks, design processes and build teams and systems. All of it costs money, of course, but it should not be seen as an expense but as an investment. Outsourcing cyber security is a possibility, but it must be done carefully, making sure what you are getting for your money.
A company that follows these recommendations is not reinventing the wheel, but safeguarding the future. And that counts for something.

Estonian CYBER VIGILANCE improving

The results of the surveys of Statistics Estonia commissioned by RIA since 2019 show that the level of cyber hygiene among the population has seen marked improvement. Hopefully, the high-impact incidents of last year will also help in this regard – besides data leaks, there were problems buying train tickets and the operation of some district heating plants was disrupted – increasing the understanding of the importance of cyber security. Successful attacks can disrupt the normal flow of life and the most sensitive data can end up in criminal hands. But only awareness is not enough; action is also required. Updates and patches must be installed quickly, and other RIA guidelines for avoiding cyber risks must be followed. It often does not take more than one or two clicks!

DATA PROTECTION is a priority

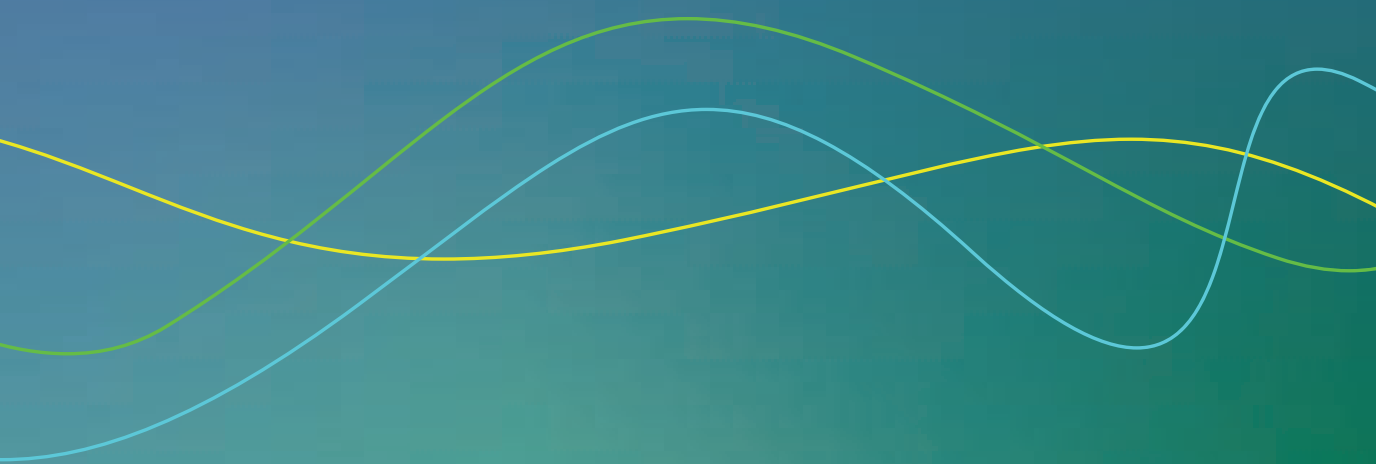
A data leak following a cyber attack is highly likely to contain personal data.

The issue of personal data leaks has not previously been a very hot topic for the Estonian public, but the Asper Biogene incident discussed in this yearbook – where the medical data of about 10,000 people was stolen – changed the situation and increased awareness of the importance of data protection. Concerns about data security and use were also raised by a case revealed in August, in which the data on thousands of childless Estonian women was accessed from the Population Register.

Although Estonia has yet to levy heavy fines for violations of the GDPR, we anticipate that the high public profile of the above cases will motivate institutions and organisations to shore up security of the personal data in their stewardship.

Cyber Security in Estonia 2024

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



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