Republic of Estonia
Information System Authority

Cyber Security in Estonia 2021

Republic of Estonia
Information System Authority

Cyber Security in Estonia 2021

Contents

FOREWORD

2020 – ANNUAL REVIEW

SAFER CYBERSPACE

eITS

Solving a (Digital) Crisis Requires Clear Leadership

The corona crisis increases our dependence on digital solutions even more. This means that a greater contribution toward the digital state and its security is needed, writes **Margus Noormaa,** the Director General of the Information System Authority (RIA).

The year 2020 was unprecedented. COVID-19 epidemic ravaged and continues to ravage the world, so we must learn to live with the consequences of the global crisis. Working remotely will remain one of the forms of employment because consuming certain services requires increasingly fewer physical meetings.

Any kind of crisis or new situation fosters development, albeit sometimes negative development. Criminals cannot infiltrate a personal meeting, they can however do so in the case of a digital transaction if that transaction is not conducted wisely and safely. The increasing frequency of phishing campaigns during the year of the pandemic was not a coincidence, as this is how fraudsters attempted to access people's data and money; in addition, businesses had to work on restoring their web pages and information due to cyberattacks more often.

Security Requires Increased Attention

We do not have to look far for cautionary tales. Last autumn, criminals were looking for weaknesses in web pages. Their targeted and specific labour bore fruit – among all else, they managed to access the servers of three Estonian ministries and retrieve sensitive health data. The ministries and the Information System Authority (RIA) reacted quickly, thus preventing the worst-case scenario; however, it was clear that we need to be a lot more critical about the security of our digital state. Discovering a fault during an annual inspection is better than finding it while driving down the road at 90 km/h. If the breaks fail, then a disastrous accident could occur. We at RIA do everything in our power to have state authorities pay full attention to their solutions and keep their systems in the best condition.

Although we have been building our digital state for over 20 years and definitely have an advantage compared to the rest of the world in that regard, the system is not flawless. We need different solutions to synergise, use data better, and have a better understanding of the tasks ahead of us.

MARGUS NOORMAA
Director General of the Information System Authority

> It seems to me that the question of security is clear to everyone; people understand why it is necessary and know how to ask for advice. RIA is happy to help in this domain.

Health care, which is already under a tremendous amount of pressure due to the crisis, has not been able to implement good e-solutions that would support the daily work of doctors and nurses. There are no such solutions because these were not considered essential before the crisis. This adversity will presumably properly impel the field of medical IT and solutions that otherwise would have taken another decade will be completed at supersonic speed. Could we have predicted it and planned and developed those solutions better in the past? Yes and no.

So far, the digital success of Estonia has been driven by the IT sector and the activists in that community. It is high time that the business side, i.e. the state as a client, would lead the way; the client should state their needs and determine the order of meeting those, as well as set national priorities. The client should also finance projects accordingly. Only then, we can hope that we will be better prepared for the next crisis, at least regarding digital solutions.

Everyone Can Contribute

Cyber security is easier – everyone can contribute. The principle of the weakest link applies here, i.e. the strength of the weakest links in our security chain determines the security of our environment.

It seems to me that the question of security is clear to everyone; people understand why it is necessary and know how to ask for advice. RIA is happy to help in this domain.

I would like to give some examples. RIA’s CERT-EE offers various free tools for finding critical faults and fixing them before any criminals show any interest. We offer those to everyone who is interested. The new Estonian Information Security Standard created by RIA is a similar tool – it provides institutions with a framework for organising information security in a way that protects databases and helps them function smoothly.

Have we valued the role of IT enough when managing our businesses? Have we paid enough attention to the issues of information security? How could we organise the work of our people so that all boring routines would be completed by technology, freeing humans to devote themselves to work, healing, leading, building, defending, and teaching? We should take some time to think about those questions. To think long and hard. Only then, there is hope to have less digital panic and more unity when faced with the next cataclysm. ●

2020 in Cyberspace: A Record Number of Phishing Attempts

The year 2020 in cyberspace will be remembered for a record number of phishing attempts, the insidious malware Emotet, and denial-of-service attacks

When we wished each other Happy New Year during the first minutes of January, no one could have guessed that 2020 would be so different from the previous years. COVID-19, a coronavirus that started in China, finally reached Estonia in February; on 12 March, the government declared an emergency situation to stem its spread.

In only a few days, businesses and institutions switched to remote working and schools to distance learning. Our digital state was put to a test: the use of e-services for learning, working, shopping, entertainment, and finding information made a sudden jump. Electronic education information system eKool could not withstand the sudden increase in workload during the first day of distance learning; however, it resumed its activities after new resources were added.

New digital services were rolled out and new accounts were created in a rush, which too often meant recycling old passwords. All of these factors and the anxiety caused by the corona crisis created a good environment for a sudden increase in the number of cyber incidents. Although we saw growing numbers regarding some types of fraud or attacks, we can say that we passed the 'stress test' quite successfully when looking back at the past year.

Bank Account Phishing

A type of cyber incident that we saw with increasing frequency were phishing attacks. Last year, the number of registered incidents grew by a fifth and made up over a quarter of all incidents with an impact.

Phishing can be divided into two groups: phishing for bank account data and for e-mail account data. In 2019, a wave of fraudulent e-mails began which was an attempt to phish for passwords and PINs for accessing internet bank accounts and making payments; this wave continued last year.

We received information about 41 fraudulent pages phishing for bank account data.

Usually, the fraudsters sent spam e-mails where they impersonated bank employees, asking the recipients to log into their internet bank accounts through a page that was identical with the actual internet bank web page. While the victim was entering account data on the fake page, the fraudster did the same in the real internet bank by using the information revealed by the victim on the fake page. When an unsuspecting user typed in the PIN of their Smart-ID or Mobile ID in their smart device or phone, the criminal gained access to their bank account and transferred all the funds to their own account.

In such cases, CERT-EE, the Incident Response Department of the Information System Authority (RIA), informs the web hosting provider whose server is hosting the phishing page and asks them to remove the page; regardless, the best defence against such frauds is a user who is aware and observant. When looking more closely, the recipient of the e-mail would notice that the address of the sender and the phishing page are different from the usual addresses and might not belong to the bank. When logging into the internet bank, the address should be entered on the address bar personally; the service should not be accessed through links received in suspicious e-mails.

During the third quarter, we were notified of such scams almost every week, but then something happened on 28 September that ended those temporarily. Three men were detained in Romania as a result of a joint international police operation; those men are suspected of the phishing attempts described here. Their phishing e-mails reached up to 100,000 people in Estonia and the criminals managed to gain access to at least 400 accounts.

Altogether, they tried to withdraw about 150,000 euros from the accounts of their victims.

Altogether, they tried to withdraw about 150,000 euros from the accounts of their victims. Not all attempts were successful – in some cases, the intended victims realised that they were being scammed and did not confirm the transaction with the second PIN; in other cases, banks blocked the suspicious payments. According to the information available to the police, the criminals managed to steal from about 40 people and the damage caused was over 100,000 euros.

After the arrest in Bucharest, phishing for bank account information stopped for about a month, but it started to spread again at the end of October.

Phishing for E-mail Accounts Could Lead to Invoice Fraud

If the damage caused by bank data phishing are immediately evident, then the consequences of e-mail account phishing could become apparent much later.

A criminal who has gained access to the e-mail account of a victim could monitor their e-mails with colleagues and partners for months, and gather valuable information for the next crime, such as invoice fraud. At an opportune moment, the fraudster interferes in the correspondence, impersonating the owner of an e-mail account, and informs the recipient that the company has a new bank account, attaches an invoice, and asks for it to be paid to the new account. If the recipient of this invoice does not check this information (by calling the partner, for example) and transfers the amount indicated on the invoice to the new account, this sum could be lost forever.

If in 2019, the largest known amount to be transferred to the wrong bank account due to fraud was 112,000 euros (fortunately, it was recovered owing to the cooperation between banks), then last year, the largest single fraudulent transfer was 41,000 euros which was transferred by one of the partners of a company in Viljandi to a fraudulent account. In a year, we receive reports of dozens of such cases but the actual number and damage caused are definitely far greater. Fraud is explained in greater lengths on page 20.

If a victim has the same username and password for several services, the potential damage could be greater because a criminal could use the same keys to gain access to the other accounts of the victim. Therefore, we recommend using unique passwords and multi-level authentication whenever possible.

Denial-Of-Service Attacks for Blackmail Are Back

In 2020, distributed denial-of-service (DDoS) attacks started to affect everyday life once again; they also grew both in number and impact. In the case of smaller attacks and more efficient counter-measures, the damage was limited to a somewhat slower functioning of the company's website or perhaps it was unavailable for a few minutes; unfortunately, there were DDoS attacks with more serious consequences that affected a large part of the society.

In autumn, Estonian commercial banks were attacked. In the case of the most serious DDoS, payment terminals were down for a couple of hours; this meant that millions of euros worth of transactions were cancelled or postponed. At the same time, many clients could not access their internet bank accounts or use the mobile app.

Most of the denial-of-service attacks followed the same pattern – a blackmail notice was sent to a company, followed by a trial attack and a threat to attack again at a much larger scale if the extortion amount was not paid (sometimes in cryptocurrency).

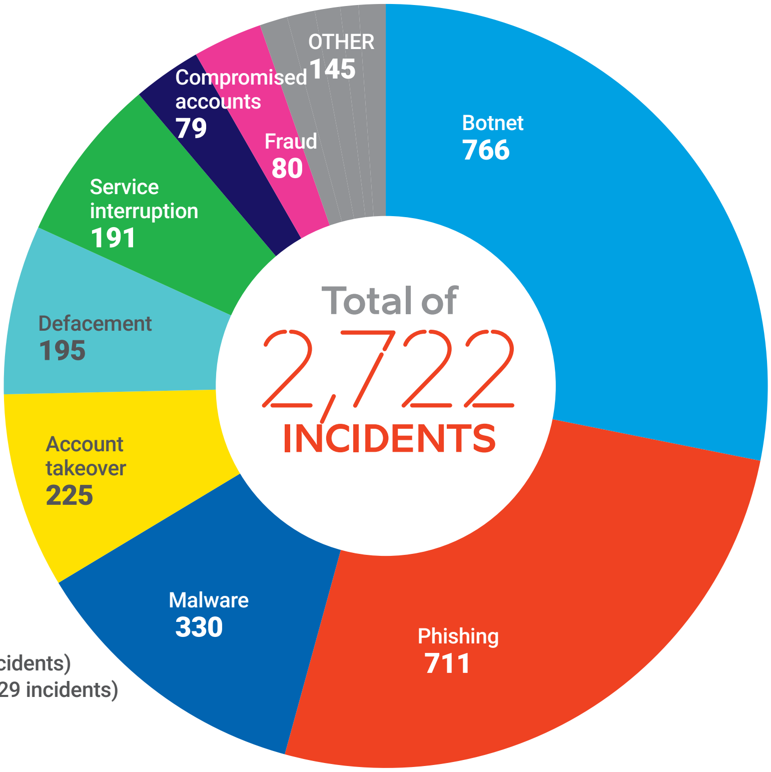
Denial-of-service attacks are described in greater detail on page 16.

2020 IN NUMBERS

In 2020, the Incident Response Department of RIA (CERT-EE) received 22,896 REPORTS

This means 63 REPORTS PER DAY on average

Incidents Registered in 2020 which Impacted Data or Systems



‘OTHER’ includes

- Ransomware (32 incidents)
- Denial-of-service attack (32 incidents)
- Command-and-control server(29 incidents)
- Data leak (21 incidents)
- SEO spam (18 incidents)
- Crypto mining (13 incidents)

Weak Spots in Security That Could Have Had a High Cost

In 2020, CERT-EE identified several previously unknown security flaws while monitoring the cyber space or solving an incident. We notified the owners of products or providers of services and the weaknesses were removed before any greater damage could be done.

In July, CERT-EE identified nearly twenty web pages with vulnerabilities that did not check the validity of an ID card certificate when using it for authentication. In two instances, there was no verification of whether the certificate was signed by SK ID Solutions. This means that a user could sign the certificate themselves when logging in to use the services and to log into the environment with the name and personal identification code of virtually anyone. We informed the owners of those web pages of the vulnerabilities that we found and asked them to correct those.

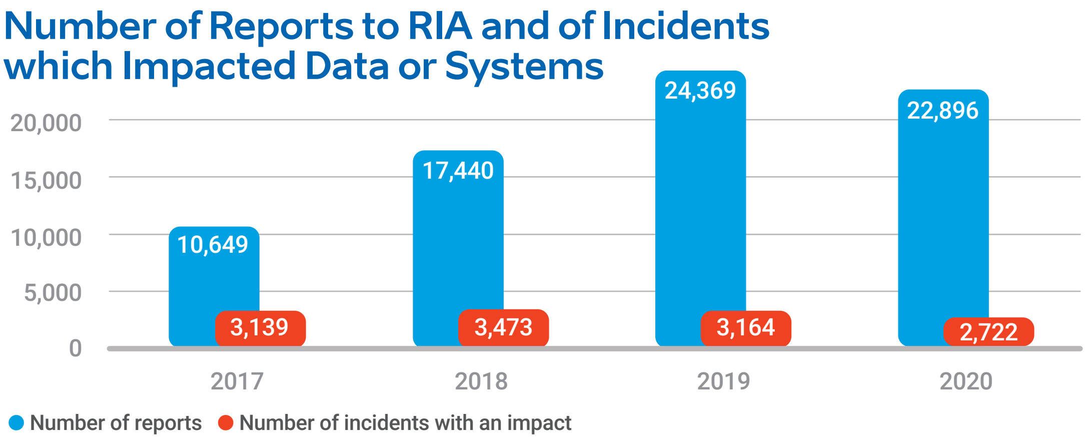
In December, this issue was once again relevant when we discovered a similar vulnerability on the web page of an unsecured personal loan provider. This could have been used for borrowing money in someone else’s name. We informed the company and helped them eliminate the flaw.

The majority of cyber incidents could be prevented by an aware and cautious user; however,

2,722 of those **HAD AN IMPACT,** which means that the confidentiality, integrity, or availability of information or systems was interrupted.

We received 711 **REPORTS OF PHISHING PAGES** Phishing pages imitating the web pages of banks gave us the most trouble

We were notified of 225 **INSTANCES OF USER ACCOUNT TAKEOVER** Attackers mostly managed to take control of e-mail and social media accounts.



Number of Reports to RIA and of Incidents which Impacted Data or Systems

with such vulnerabilities, the responsibility lies with the provider of the service. A properly configured website does not let attackers abuse the users in this way. All companies using public authentication services should review their web server settings and make sure to follow the best practices. Updated instructions for web server settings are available in the portal www.id.ee.

At the end of the year, researchers of the University of Tartu announced that they discovered a vulnerability in the browser extension of the ID card that is used for adding digital signatures. Criminals could have exploited the vulnerability of the service if they either took over or had a website that offers the possibility of authentication with an ID card. If a user had logged into a website controlled by a criminal with an ID card, the criminal could have used the authentication information for logging into another e-service impersonating the user.

Although taking advantage of this vulnerability is complicated and never been done as far as we know, we always take such incidents very seriously. Together with partners, we fixed the vulnerability and issued the improved ID software this January.

The Insidious Emotet Reached Estonia

Last summer, Emotet, one of the most dangerous and insidious malwares, reached Estonia once again. It was a trojan that created a backdoor in the infected systems. Cyber criminals could use this to install other malware on the victim's computer for stealing data or carrying out other attacks.

Emotet mostly spread through files attached to e-mails. An e-mail was received from someone the victim would know as a continuation of previous correspondence; the subject line would state 'New invoice in attachment' or 'Please confirm', for example, and the e-mail would contain a seemingly normal Word or Excel file. If it was opened, the programme would notify the user that macros were disabled and ask to click on 'Enable Content'. The unsuspecting user would give an order to install Emotet malware in their computer by doing so.

Fortunately, we can discuss Emotet in the past tense.

We received hundreds of reports of devices infected with Emotet in Estonia last year. There were reports from almost all domains: from hotels to health care, from state and local government offices to design companies.

Fortunately, we can discuss Emotet in the past tense. At the beginning of 2021, an international police operation managed to destroy the Emotet infrastructure that consisted of hundreds of servers across the globe. After this, we have had no new reports of recent infections and the owners of devices that were infected also do not have to worry about Emotet any more.

Service Disruptions Affected Us All

In 2020, we received 170 reports of service disruptions. Mostly, these were caused by human error or faulty settings; however, sometimes services were disrupted by malicious attacks. Fortunately, we had no service disruptions with serious consequences.

There were several disruptions in the State Network that provides data communication for the public sector. For example, on 23 January, State Network traffic was redirected to a backup line for the duration of planned maintenance. Unfortunately, the backup could not handle the increased load and data communication was disrupted for about 2.5 hours for up to a third of State Network clients.

In thirteen instances, there were disruptions to the e-services of the Estonian Health Insurance Fund, the most well-known of which are e-Prescription and checking the validity of health insurance.

Most of the incidents affecting the government network and the Health Insurance Fund took place during the first half of the year, with their reliability increasing significantly during the second half.

On 23 February, the internet bank and mobile app of Luminor were unavailable for five hours. On 8 October, Swedbank's sservices (the internet bank, mobile app, and card payments) were disrupted for over three hours.

Botnets Are Still Active

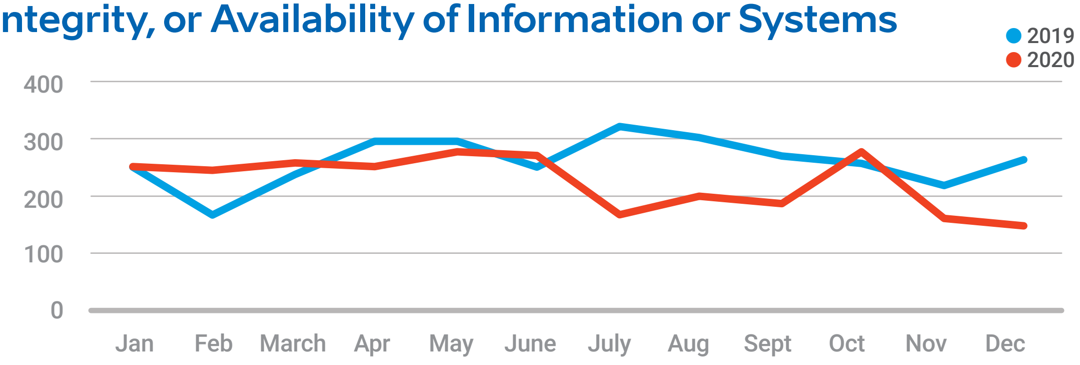
For years now, the majority of incidents with an impact that are registered by CERT-EE concern devices that have been added to a botnet. This means that devices are infected with malware that gathers them into a network controlled by criminals. These botnets, some of which could consist of hundreds of thousands of computers, are used for cyberattacks. Most of the time, the owners are completely unaware that their computer has been infected by malware and that it participated in a service interruption attack against a telecom company, for example.

Information about infections is sent via an automatic notification service to the providers of communications services; unfortunately, it does not always reach end customers whose devices have been infected with malware and added to a botnet. When we investigate the causes of incidents, we have seen a sad confirmation in those incidents that could have been prevented if the service provider would have forwarded CERT-EE warnings to their clients in time.

Starting from July 2020, the statistics of CERT-EE do not include infections with Avalanche and Necurs, which made up about 95% of registered botnet infections and about 60% of all incidents with an impact. Avalanche was stopped in December 2016 as a result of an international police operation, but infections continued nevertheless. Microsoft managed to gain control of the Necurs network in March 2020.

Still, there are many devices in Estonian networks that are infected with an active botnet and send out phishing e-mails or participate in denial-of-service attacks without the owner's knowledge, maybe even against the preferred bank of the owner of the device. ●

Incidents which Had Direct Impact on the Confidentiality, Integrity, or Availability of Information or Systems



The Most Painful Lesson of the Year

In November, we discovered three similar attacks against the servers of the Ministry of Economic Affairs and Communications, the Ministry of Social Affairs, and the Ministry of Foreign Affairs.

When comparing and analysing those, we saw that the attacker used a similar method in all three cases. First, the web servers were scanned. If a vulnerability was discovered through a technical .git catalogue which had remained public by accident, malicious code was uploaded through that. After gaining access to the servers, the attacker stole all the data that they could and started to look for more ways to take advantage of the server. We have seen this pattern after the attacks published in December as well.

No One Is Perfectly Protected

Successful attacks against the public IT infrastructure show that no one is completely safe. Estonian Ministries use uniform external webs but their web servers could host other pages that have been developed individually. In addition, not every ministry or domain would configure their pages in a similar manner. There are many tiny nuances that could open an attack vector if variant settings were used.

This is why the autumn attack had the largest impact in the administrative domain of the Ministry of Economic Affairs; the attackers managed to gain access to the administrative servers of the Ministry after attacking the web server and stole several hundred gigabytes worth of data.

The most prominent data leak came from the Ministry of Social Affairs, where the criminals successfully gained access to a web server and acquired information related to the COVID-19 pandemic about 9,158 individuals. The information was in a database on the compromised web server as a temporary solution.

The Ministry of Foreign Affairs escaped with the least damage: the attacker got stuck on their homepage and did not receive any sensitive information.

Painful Lesson

Compromising data or systems (in other words, gaining unauthorised access to those) remains a huge threat. A criminal who accesses such information could alter the data, delete it, or encrypt it, and by doing so, cause serious interruptions in our daily communication with the digital state. Imagine what would happen if the Buildings Register would be unavailable for a day or as long as a week.

An attacker could also be interested in money; they might want to sell data to the next attacker – to someone who will go through each line of leaked data and look for new potential targets.

The incident that was made public in December was a good lesson for the Information System Authority in protecting the national IT infrastructure better. Every institution is responsible for its own cyber security, but we have a legal obligation to inform the Estonian public whenever a potential threat arises.

Therefore, we provided recommendations in varying degrees of detail to the information security managers of the public sector, to the providers of public services, and to the wider cyber security community. These recommendations are never too complicated and emphasise basic IT security: do not reveal too much information, keep current with your assets and users, and monitor your systems.

Currently, we are much more aware of the types of information that the attackers are after, the manners of using the data, and the segments that need better monitoring. ●

CERT-EE Recommendations for Information Security Managers:

- **Update:** standard web applications have critical weaknesses that are mostly caused by outdated software.
- **Publish only what is necessary:** do not expose your code publicly through a .git catalogue. This could provide necessary information for an attacker.
- **Have a clear overview of the users and give administrative rights with good reason:** often, web applications have unnecessary (often outdated) administrative accounts with potentially leaked passwords.
- **Separate external web from internal assets:** insufficient or unsafe separation of web servers from the rest of the information system provides an attacker with an opportunity to gain access to the sensitive information assets of an organisation through the web.
- **Guard sensitive information well:** a web server should not be used for storing information that should be properly protected. Even if an attacker gains access to the external web, they should not have automatic access to sensitive data.

Currently, we are much more aware of the types of information that the attackers are after, the manners of using the data, and the segments that need better monitoring.

The Number of DoS Attacks Grew, Newly Coupled with Blackmail

Last year, the number of denial-of-service attacks against Estonian companies and organisations grew by a half. Several had a considerable impact on the daily lives of Estonians.

In 2020, we received information on 33 denial-of-service (DoS) attacks, once again with a visible impact. In one instance, people standing in lines in grocery stores were unable to pay with a bank card for two hours; twice, the clients' websites of a web hosting company were unavailable for hours; in several instances, people could not conduct their normal transactions in the internet bank.

Nothing We Have Not Seen Before. Or Is It?

We can point to a new trend of using denial-of-service attacks for repeated blackmail. Last autumn, several Estonian companies received a letter threatening to disable their activities with a denial-of-service attack unless the company paid the required ransom. The letter was accompanied by a trial attack; if this was ignored and ransom was not paid by the deadline, the criminals threatened to return with a new and more extensive attack.

The attackers claimed to be from an infamous cyber crime group, such as Fancy Bear, Cozy Bear or the Armada Collective, hoping that a well-known name and their previous crimes would increase the credibility of the threat.

The targets were not picked randomly; mostly, financial or technology companies were attacked. The ransom demands were between 0.5–10 bitcoins (10,000–400,000 euros, depending on the exchange rate of the cryptocurrency).

Today, we know that almost all targets of the attack in autumn were also targeted during the first months of this year. As these sectors already have a better cyber security level than an average company due to the nature of their activities and

> We predict that the effect and number of denial-of-service attacks will continue to increase in 2021.

they increased their technical countermeasures even more after the first incidents, the companies managed to avert the attackers in a few hours and return to business as usual.

Service disruptions or sluggishness could not always be avoided, with the longest interruptions lasting for about six hours. As far as we know, none of the companies accepted the terms of the criminals and the attackers did not receive any ransom money from Estonia.

Not All Attacks Are Motivated by Money

Attacks are not always motivated by money. For example, we saw a case last year where the web-based learning at a school in Central Estonia was halted by a student of the same school. Unfortunately, he did not achieve it with his IT prowess but ordered a service through a web page. There was another incident last year where the web version of a newspaper was unavailable for most of the day due to a denial-of-service attack; this was probably retaliation for a critical article.

How to Defend Yourself Against Denial-of-Service Attacks?

- **Update your software:** the software of applications, network devices, and servers could contain vulnerabilities. Make sure to use the most recent version of software and install all available security updates.
- **If possible, make your web pages static or use a web buffer.** As an alternative, keep a constantly updated static version of a web page that is created based on a dynamic web page; in case of an attack, you can quickly switch to the static one.
- **Defend all web forms with CAPTCHA** to prevent or slow down automated attacks against web pages.
- **Use a firewall:** if possible, use a web application firewall (WAF) to identify and block IP addresses that create malicious traffic.
- **Use separate servers for different services.** For example, do not use the same physical server for providing e-mail and web services.
- **If possible, limit foreign traffic:** if your services are only meant for Estonian users, you can contact your service provider in case of a (D)DoS attack to limit traffic from other countries temporarily.

Last spring, we saw a smaller wave of similar short-term denial-of-service attacks against several web pages that are essential to Estonia. Although their impact was small, we take a very serious approach to such incidents – sometimes, the primary goal of an attack could be the identification of weaknesses and the implemented defence measures; this data could be used for planning far more disastrous actions.

The better the companies are prepared for such attacks, the less profitable it is for criminals to attack them. However, we still predict that the effect and number of denial-of-service attacks will continue to increase in 2021. ●

Ransomware Attacks: Classics and Unknowns

You start your computer unsuspectingly and discover that all your files are encrypted. On the screen, you see instructions for transferring cryptocurrency by a certain deadline to regain access to your own data. Last year, this was the unpleasant situation at the start of the day for companies or private persons in 32 instances as far as we know.

The targets included representatives of a wide variety of areas – production and trade companies, educational establishments, architectural design bureaus, as well as two family health centres.

Mostly, these were classical ransomware attacks in three stages:

1. An attacker installs ransomware on a victim's computer or server. Remote desktop protocol (RDP) is increasingly used for this; however, a lot of malware is still sent via files and links added to e-mails.
2. The ransomware encrypts some of the files on the computer or server, or the entire hard drive. After that, the victim can no longer open their files.
3. The attacker demands a ransom for file recovery, i.e. for a decryption key, usually in some cryptocurrency, such as Bitcoin.

In the Estonian cases, the ransomware attacks were not aimed at specific domains; figuratively speaking, criminals go around in circles trying doors and if the owner has been careless, the damage is done quickly. The extent of this mostly depends on the existence of backup copies; if there are any, they are updated regularly enough, and saved separately from the rest of the information system, the time spent restoring the system is the main loss.

In last year's cases, we saw fast recovery due to excellent backup systems but also the loss of the entire accounting information or all data regarding the transactions and inventory from the past few months. Even though ransomware attacks cost Estonian companies in time, interrupted work processes, and caused direct economic damage, we can say that things could have gone much worse.

A Matter of Life and Death

Ransomware attacks are currently growing in numbers globally and causing greater damage that could amount to millions of euros per attack. Among all else, last year was characterised by ransomware attacks against hospitals and other health care institutions in France, the US, and elsewhere in the world with consequences surpassing financial loss – fast and appropriate treatment of patients was jeopardised.

In September, an attack with a symbolic significance took place in Düsseldorf, Germany, where a ransomware attack caused a human casualty; work at the hospital came to a standstill and a patient in critical condition was redirected but died on the way to another hospital.

The increasing and diversifying effect of ransomware attacks is also demonstrated in the new trend that emerged last year; often, the criminals no longer simply encrypt the data, they also steal it and threaten to publish it if ransom is not paid. This additional fear factor could be quite effective if the data is sensitive, such as a valuable trade secret or simply personal data which would bring hefty fines to the data holder if it became public.

Finland was shocked by a case last autumn where only stolen data was used for blackmail (there was no encryption), and some of that information ended up on the dark web. The information concerned personal data of clients of a psychotherapy centre and sessions with the doctors which is extremely sensitive information. A chain of therapy centres that did not pay attention to a data leak that led to blackmail in time to prevent it and lost confidence as a result is now bankrupt; thousands of patients are still traumatised by the incident and have no certainty about the fate of their medical histories.

How to Protect Yourself from Ransomware Attacks?

1. The best defence against encrypted ransomware is a well-planned backup system. At least one of the backup copies must be offline, for example, on an external hard drive.
2. Train your staff regularly about cyber hygiene and remind them that they should not click on unfamiliar links or open unfamiliar attachments.
3. Implement an access policy that grants users minimal rights necessary for the daily tasks.
4. Check the security policy of your e-mail system and whether logging is turned on.
5. If you are using remote desktop protocol (RDP), change their settings to the highest possible level of security.

> The goal of both old-school and new ransomware attacks is the same – to earn money for criminals.

The goal of both old-school and new ransomware attacks is the same – to earn money for criminals. If the number of successful attacks grows and more victims give in to ransom demands, then this type of crime will be progressively profitable and the criminals will be more motivated to update their methods and infrastructure. ●

The Number of Fraudulent Cases Increased

Although the number of fraudulent incident reports submitted to us increased last year, we had fewer cases of major loss events.

When an employee did not receive their salary on their bank account on the date agreed, they started to ask about the reasons. After contacting the accountant, they were surprised to learn that the salary had been transferred, but to a new account as per their own request.

After investigating the issue, they learned that a few weeks earlier, a fraudster impersonating the employee had e-mailed the accountant with a request to transfer the salary to a new bank account due to changing banks. After seeing the familiar name of a colleague on the screen, the accountant did not check the e-mail address of the sender (which was obviously suspicious), changed the account number in the accounting program, and transferred the salary on the date agreed to the bank account controlled by the fraudsters.

This kind of salary data fraud started to spread globally in 2019 and continued to cause damage last year.

The Invoice Seems Legitimate But Bears the Wrong Account Number

Simple invoice fraud is committed following the same pattern as the bank account fraud that was previously described. Often, the criminals no longer attempt to access someone's e-mail correspondence; instead, they send e-mails to companies based on public information asking to change the bank account information for any future settlements.

However, in some instances, the fraudsters go to greater lengths. After gaining access to an employee's e-mail account through phishing, they can patiently spend weeks or months observing the e-mail exchange on the account. Once the discussion moves to settling invoices, they insert themselves into the conversation by imitating one of the parties and send an invoice that is an exact match to the original – except for the bank account number.

Often, the deception is only discovered once the party waiting for payment starts to enquire why their invoice has not been settled. By then, it is extremely complicated to retrieve the funds that the criminals have acquired.

A Hospital Fell Victim to Fraud

Last year, one of the largest hospitals in Estonia, the East Tallinn Central Hospital, reported an incident of invoice fraud. This differed from others due to the fact that the criminals used public information from one of the public procurements of the Hospital to prepare and carry out the crime. They hijacked an e-mail exchange, switched the bank account numbers on the invoices, and managed to steal over 10,000 euros.

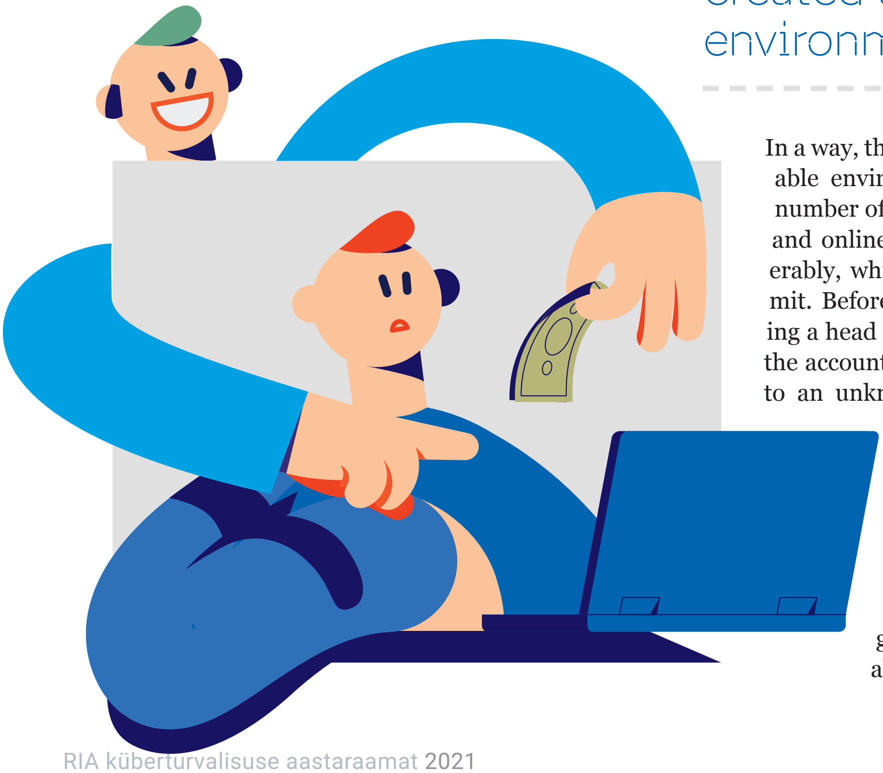
According to the information available to us, the single largest loss last year was over 41,000 euros; this amount was transferred by a partner of an Estonian company to the bank account of fraudsters. The incident itself followed the usual pattern: criminals compromised an account of an employee at an Estonian company and used it to monitor the correspondence. Once the discussion moved to payment, the fraudsters inserted themselves into the conversation through a similar e-mail account and informed the partner that the invoice should be settled to a new account because the old bank of the company was under investigation. The partner did as asked.

Last year, we registered dozens of similar schemes; fortunately, the losses were not exceedingly large. However, at the start of this year, there was an attempt to commit invoice fraud which would have caused record damage of about 900,000 euros if it had been successful. Due to the attentiveness of employees, the criminals did not receive the payments; regardless, this demonstrates the high cost of carelessness.

How to Defend Yourself from Bank Account and E-mail Account Fraud?

- If you receive an invoice from a partner with a different bank account number, make a phone call to ask whether they really changed banks.
- If an employee asks to transfer the salary to a new bank account, do the same as recommended in the previous sentence.
- Even if you recognise the name of the sender, check their e-mail address. Sometimes, fraudsters use visual deception where they replace one letter in a name or change the domain slightly (company.ee vs compnay.ee).
- Increase the security level of your e-mail by using SPF, DKIM, and DMARC protocols. More detailed instructions are available on RIA's website.

In a way, the coronavirus created a favourable environment for fraud.



In a way, the coronavirus created a favourable environment for fraud – a record number of people were working remotely and online communication grew considerably, which made fraud easier to commit. Before, when criminals impersonating a head of a company sent an e-mail to the accountant asking for a quick transfer to an unknown account, the accountant could simply ask their superior a few metres away whether they were serious, thus uncovering the fraud. When working remotely, a few extra steps are needed for this; however, a little effort goes a long way as described above. ●

The effect of COVID-19 on Estonian Cyberspace

Although cyber criminals took advantage of COVID-19, the coronavirus did not bring more cyber incidents with a greater impact to Estonia.

On 8 March last year, the Estonian Health Board e-mailed the residents of Estonia with official information about the coronavirus. Only two days later, fraudulent e-mails were sent that imitated the Health Board and also offered information on COVID-19, except for a different reason. At the end of the e-mails, there was a link to the file 'Eeskiri.7z'. After clicking on that, a seemingly normal prevention poster opened on the screen; under its cover, malware was installed on the victim's computer that stole passwords and bank card data saved in browsers.

Phishing E-mails as a Favourite Gimmick

There were other waves of phishing e-mails that took advantage of the fascination and anxiety surrounding COVID-19. Some of those contained malware, while some featured fake invoices for protective masks that the recipient had not ordered. Still, compared to some other countries, the Estonian cyberspace was relatively unharmed; we did not suffer attacks against medical communities or fraudulent schemes revolving around COVID-19 that caused extensive financial losses like in some European countries.

The second wave of the virus that began in autumn also failed to cause any remarkable COVID-related developments, although elsewhere in the world, cyber criminals attempted to steal classified information about the development of vaccines.

The COVID Incident With the Largest Impact – a Personal Data Leak

The most serious cyber incident of 2020 in Estonia took place in the jurisdiction of the Ministry of Economic Affairs and Communications (read more on page 14). We have reason to believe that at the end of November, the same criminals accessed the personal information of 9,158 individuals which was related to the spread of the coronavirus and in the possession of the Ministry of Social Affairs. As a temporary solution, the data was kept in a database on a web server. The attacker's access was eliminated on the same day and the Health Board informed those whose data was accessed by the criminals.

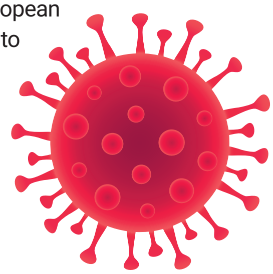
RIA Supports Health Care

The Critical Information Infrastructure Protection (CIIP) Department of RIA's Cyber Security Branch supports several sectors in issues regarding cyber security. One of the most important sectors is health care; our plans focused on that before the pandemic already.

We started training family physicians whose IT systems must meet the requirements established in the Cybersecurity Act starting from 2022. Naturally, the main task of the medical field is providing health services; however, they need to focus also on cyber security.

In March, or right after COVID-19 reached Estonia, we advised the Family Physicians Association, health care workers, and hospitals on switching to remote work, on the rules of cyber hygiene, and on digital capabilities. We helped assess the security level of software that doctors needed for working remotely. Through the year, we informed them of potential cyber threats and the best practices of cyber defence.

CyberEurope, a pan-European training exercise devoted to healthcare organised by ENISA was cancelled, but it will take place in 2021.



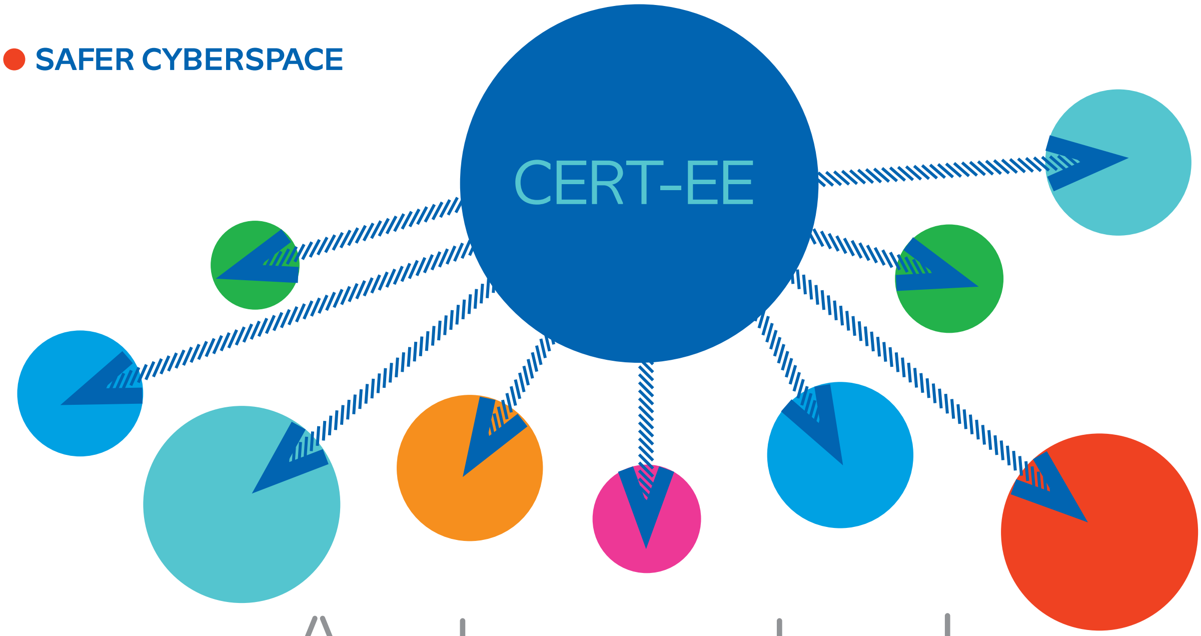
> We regularly repeated well-known cyber hygiene principles through various channels and added basic messages about distance learning and working.

Focus on the Security of Remote Work

When people suddenly found themselves learning or working remotely in March, many needed to create new accounts on a communication platform. The amount of information exchanged electronically with the employer, school, and online service providers also increased, creating a favourable environment for cyber crime.

We regularly repeated well-known cyber hygiene principles through various channels (update your software, do not click on suspicious links, do not enter your PIN carelessly, back up your data) and added basic messages about distance learning and working.

In addition, we managed to organise an awareness campaign for remote workers in less than three weeks which explained the steps to ensure cyber security at a home office (see also page 32). ●



Automated Notifications About Security Threats

CERT-EE sends daily automated notifications to Estonian telecom companies, web hosting companies, and organisations that manage their own networks about the misuse and vulnerabilities involving their networks. Often, this information is not forwarded to end users.

In the first quarter of 2020, one of the companies in the Estonian energy sector notified CERT-EE of an incident with their server. They indicated that a service called 'memcached' had been left publicly available online; its purpose was to cache information temporarily for its service. Unfortunately, this could be misused in denial-of-service attacks for amplifying internet traffic; one package is sent as query to the service and it responds back with 500,000 times that amount of information. As a result, information in the cache will leak. This was the type of attack that was reported to CERT-EE.

The incident itself was nothing unusual. The company fixed its service; CERT-EE helped check their logs and made recommendations. What sets it apart is that CERT-EE had informed the internet provider of the company about the open memcached service repeatedly, but the security notification had not been forwarded to the energy sector company. There are several similar examples of situations where an incident could have been avoided by forwarding security messages.

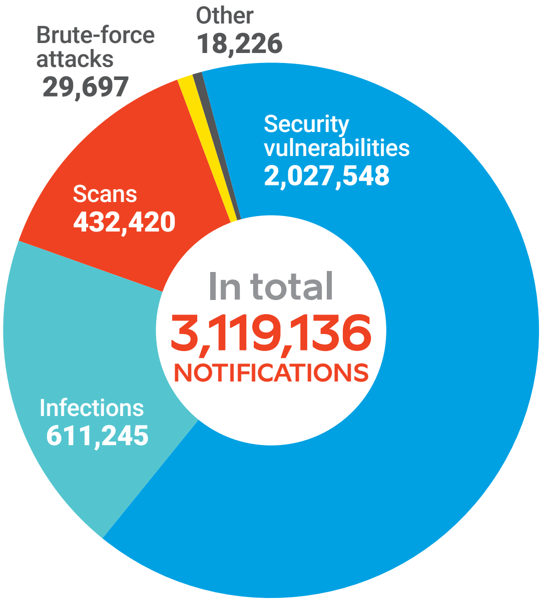
We Send Daily Threat Notifications

Starting from the summer of 2019, CERT-EE has sent automated notifications to Estonian telecommunications companies, web service hosts, and organisations managing their own networks about misuse and vulnerable devices/settings in their networks at least once a day.

CERT-EE receives this information from its partners, who scan the entire internet or gather many indicators during their activities which show security vulnerabilities, well-known infections, and the sources of brute-force attacks and scans.

Our automated system gathers all notifications, screens them, and then forwards them to network service providers registered in Estonia or to larger organisations whose IP ranges we know. They in turn should forward this information to end users because ultimately the owner is responsible for the security of their systems.

Automated Notifications from July to December 2020



Over 800,000 reports

Due to automated messaging, it might appear as if the number of incidents that CERT-EE is solving has decreased over the last years (from 3,164 in 2019 to 2,722 in 2020); however, this number only shows incidents that have involved CERT-EE technicians.

> In 2020, we notified the Estonian service providers of over 800,000 infections at over 2,000 IP addresses.

For example, we stopped adding infections of Avalanche and Necurs botnets to the incident list of CERT-EE in July 2020 and forwarded those notifications to the automated system to reduce the workload of specialists. The Avalanche botnet was stopped in December 2016 as a result of an international police operation, although it continued to infect devices, and Microsoft gained control of the Necurs botnet in March 2020; therefore, it is safe to say that these two botnets are no longer an active threat in cyber space. Without changing the methodology, the number of incidents in 2020 would have been 3,439, i.e. even greater than in previous years.

In 2020, we notified the Estonian service providers of over 800,000 infections at over 2,000 IP addresses. This includes many repeated infections but also malware which is already neutralised but remains active in the computers long after these have been cleaned.

With a growing number of devices with an internet connection and increasingly skilful cyber security specialists, the number of detected security vulnerabilities, infections, and malicious internet traffic also increases. Automated forwarding of security warnings to network owners is therefore the only thinkable way to maintain the level of cyber safety. However, as the incident described at the beginning demonstrates, CERT-EE sending notifications is not enough – service providers must forward those to the end users. There is still room to grow in this regard. ●

RIA: Defending Estonian Democracy

In the fall of 2021, Estonia will hold municipal council elections. To protect the functioning of our democracy, we take a comprehensive approach to the cyber security of election technology.

In Estonia's case, the internet voting or i-voting system receives the most scrutiny and there are many security aspects to pay attention to. The most visible component of the system to the Estonian voter is the actual voting application. We need to ensure that voters reach the correct voter app (i.e. that no one would lure voters to install malware on their computers) and that outdated electronic ID software would not stop voters from voting.

Candidates and Parties

The experience of other democracies has taught us that attacks are often aimed at the candidates or parties, not the organisers of elections. This has happened in the USA, France, and elsewhere. Websites of candidates and parties, their social media pages, or e-mail servers could be attacked by a foreign adversary, domestic attacker, or trolls.

As we did in the last election cycle, the Cyber Security Branch of RIA is organising cyber hygiene trainings for candidates and campaign teams to advise them on securing their accounts and recognising attacks. In addition to cyber hygiene trainings, RIA offers the political parties a chance to get an overview of the security protocols of their web and e-mail servers and tips for improving security.

But there are many other components of the i-voting system that demand cybersecurity attention. For example, RIA hosts and secures the ballot collecting system (called Koguja) where voters send their encrypted ballots. These servers work in the background and need to have robust defence measures in place to ensure the confidentiality of the voting, the integrity of the systems and data, and availability to voters.

New Information System

Modern-day elections require many other technologies to be able to take place. In Estonia, a version of the Election Information System (VIS) – responsible for managing the lists of voters and candidates, counting paper ballots in polling stations, and for storing i-voting results – has been in use for a long time and its components no longer correspond to the best practices of modern information security. Therefore, a newer version of the software has been in development at RIA since 2018. This software – called VIS3 – will be completed by the summer of 2021; after security testing, it can be launched in autumn.

VIS3 is an important development because of an amendment to the election laws; this amendment requires the use of electronic lists of voters (until now, these were printed on paper) and to hold i-voting and regular voting at the same time. This would mean that a person can vote at any polling place in Estonia, for example. And as a security measure, the i-voter ballot may be overturned as late as on the election day (see valimised.ee for Estonian i-voting security measures for context).

All this requires VIS3 to be in operation on time, the right individuals to have the right privileges, all auxiliary systems (population register, business register, prison register, etc.) to be available, and that no unauthorized person could alter the registration of a candidate or strip a voter from their right to vote, for example.

Like Clockwork

VIS3 is also the platform for counting ballots and sending correct data to the election website in a timely manner. This means that the website also requires much more attention on the evening of the elections than at other times. For example, if the website were to be compromised and the election results changed on the site, it would have a huge impact on the reliability of the elections despite the possibility to correct the record at a later time.

Alongside the technology directly responsible for election, we will also monitor other auxiliary systems necessary for the Estonian elections – electronic identity, various registries, the state network, and the internet service of local governments. Understandably, there may be interruptions to the availability of those systems, but during the election period, all incidents receive heightened scrutiny by us, by the voters, by the candidates, and by all participants of the democracy we are tasked to defend. ●

Who Does What?

In January 2021, the **Ministry of Economic Affairs and Communications**, **RIA**, and the **State Electoral Office** signed a cooperation agreement to determine the respective tasks of the institutions in organising elections and ensuring the cyber security of voting.

The task of the State Electoral Office is to develop and manage the i-voting system (EHS), testing the security of the system, conducting a risk analysis, and processing data regarding the i-voting at the elections. The Electoral Office also answers the questions of voters and various parties involved in the organisation of i-voting, develops the website of elections, and manages its content.

RIA supports the State Electoral Office in technical issues and its most important task is to organise the technical development of VIS3 and related applications. RIA provides hosting and administrative services for VIS3 and the i-voting ballot collection system Koguja. In addition, RIA will be responsible for managing the cyber security notifications of the elections.

The Ministry of Economic Affairs will audit and analyse the cyber security of the elections information system (VIS3) and the i-voting system.

The New Estonian Information Security Standard Is Complete

RIA led the completion of **the New Estonian Information Security Standard** (Estonian acronym E-ITS), which was in development for several years. This will replace the current IT Baseline Security System (Estonian acronym ISKE) by 2024.

The state and local governments have a lot of data and many databases. For example, the Estonian Health Information System contains the medical histories of patients or a city's system has information for applying for and processing benefits. Data records help manage procedures more efficiently, organise the exchange of information between authorities, make decisions, and allow the state to function as a state.

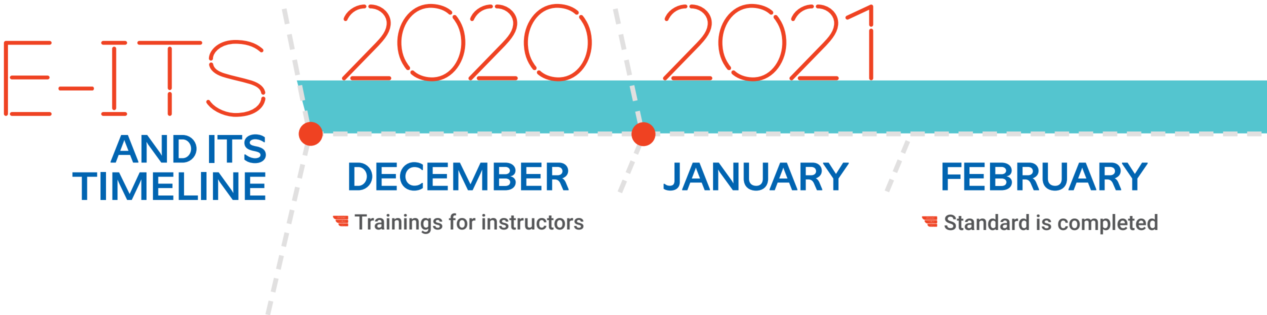
A large part of this information is sensitive and can only be used by authorised persons. For others, the door is closed. ISKE, or the IT Baseline Security System, sets the requirements for this door and determines the manner of authenticating people who can enter through that door.

We would once again like to use health data as an example – it must have guaranteed confidentiality (not available to everyone), integrity (cannot be changed or deleted without authorisation), and availability (a doctor must be able to use the data when necessary).

ISKE in the past and now E-ITS are tools that were created primarily for the public sector; these help ensure that the information security of all institutions that fulfil public duties would be at a comparable level.

Clearer and Shorter

ISKE, which came into force in 2004 and consists of about 5,000 pages, making it unfathomably



E-ITS AND ITS TIMELINE

2020

DECEMBER

Trainings for instructors

2021

JANUARY

FEBRUARY

Standard is completed

bulky, has a poor reputation. We stopped updating it in 2018 when the German standard that we used as a basis was no longer updated. Therefore, we needed a fast solution.

In addition to ISKE, we made it possible to use the international standard ISO/IEC 27001. Unfortunately, its implementation is manageable only to organisations that are aware of information security and capable of risk management.

The goal of E-ITS is to provide a basis for organisations for managing information security that would be written in Estonian and compatible with the laws of Estonia and the ISO/IEC 27001 standard. E-ITS provides benchmark measures for information security and an implementation system which helps organisations achieve a level of information security compatible with their needs.

The better we can implement E-ITS, the better we can tackle any unexpected events, be more transparent in our activities, and guarantee trust for the state information systems and the state as a whole.

Primarily a Public Sector Tool

Using E-ITS should become a natural part of the work process for public sector employees, necessary for avoiding the realisation of specific risks.

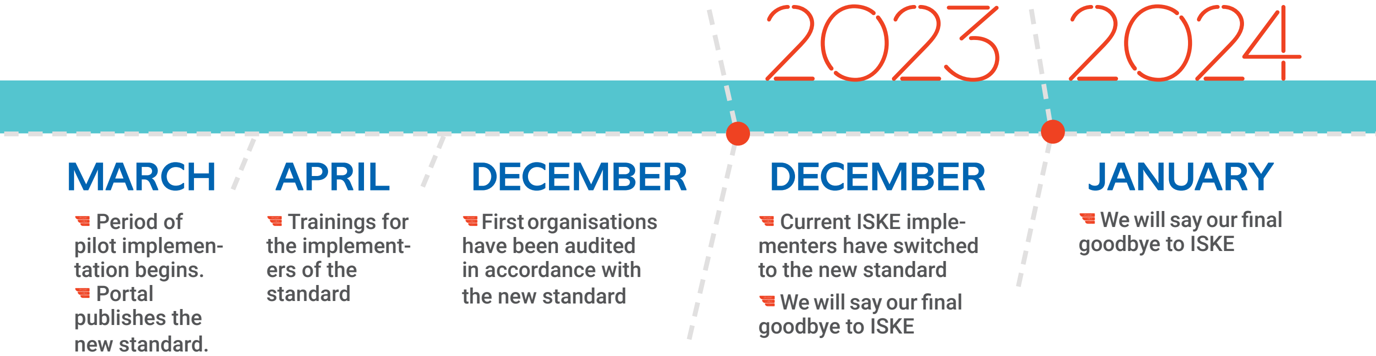
> E-ITS is like a block of flats that has been built in compliance with laws and specifications.

The double-tier information security standard E-ITS is like a block of flats that has been built in compliance with laws and specifications. However, each flat is designed and decorated by its owner according to their needs and preferences. If the risks are higher, other measures must be added.

We hope that the new information security standard will be accepted in the next few years and every organisation discovers useful tips for managing information security risks better and easier.

E-ITS was created within the framework of the European Union's structural funds support scheme 'Raising Public Awareness about the Information Society' and funded from the European Regional Development Fund.

All materials regarding E-ITS are available on the website eits.ria.ee. ●



MARCH
- Period of pilot implementation begins.
- Portal publishes the new standard.

APRIL
- Trainings for the implementers of the standard

DECEMBER
- First organisations have been audited in accordance with the new standard

2023

DECEMBER
- Current ISKE implementers have switched to the new standard
- We will say our final goodbye to ISKE

2024

JANUARY
- We will say our final goodbye to ISKE

DigiTest Helps Improve Cyber Hygiene

Since 2017, the Information System Authority (RIA) and cyber security company CybExer Technologies have offered the cyber hygiene training platform **DigiTest** to the employees of the public sector. It has currently been completed by over 15,000 users.

It is Friday night. A long and exhausting work week just ended. The accountant is about to close the computer when she notices a new e-mail from her boss in her mailbox. 'Hello, Anna! I attached an invoice that I forgot to send earlier. The deadline was the day before yesterday. Please transfer 40,000 right away! Otherwise, they will add an interest on arrears. Thank you! Maria' What would you do if you were the accountant in that situation?

How would you recognise invoice fraud and phishing e-mails? How can you create safe passwords? How can you use public Wi-Fi networks and external data carriers to avoid unauthorised access to your and your employer's data?

DigiTest, taken by over 15,000 public sector employees, covers these and many other cyber hygiene topics.

Cyber Security Begins With the Person Behind the Computer

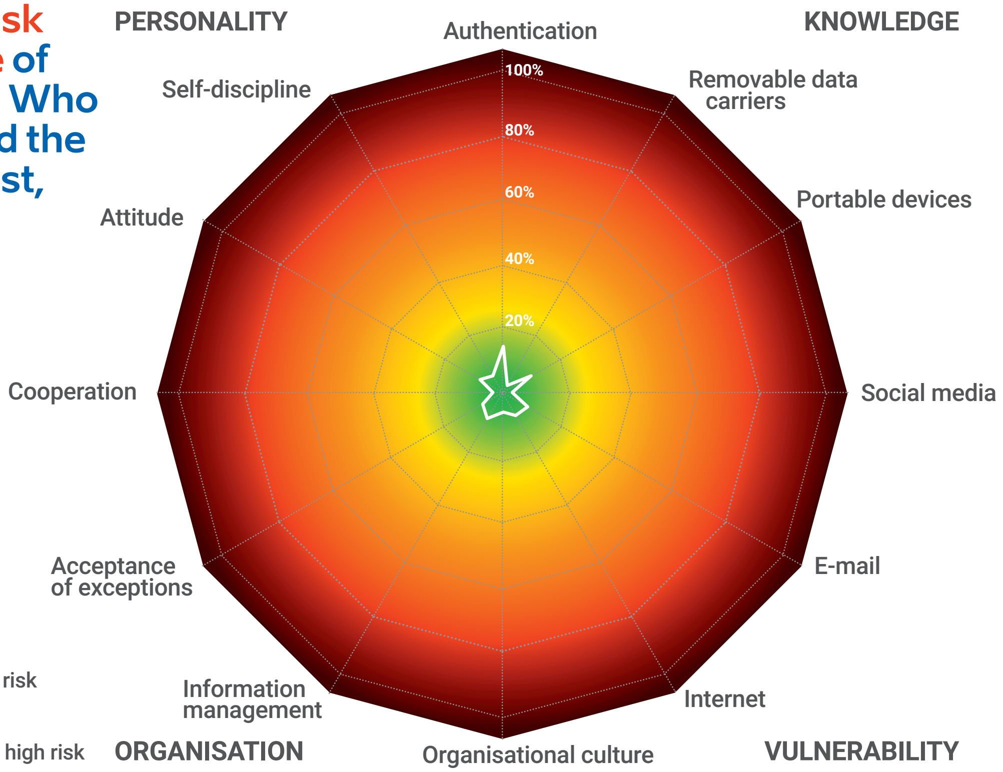
The cyber security training platform DigiTest was launched in 2017 and its goal was to increase awareness of cyber security because this is the most efficient way to prevent smaller and larger cyber incidents.

After taking the course, the system compiles a risk profile for the user based on their answers where it points out high risk issues that need further attention. Likewise, DigiTest provides an

Greatest Risks to DigiTest Trainees Between 2018 and 2020

2018	2019	2020
E-mail (25%) – indicates whether the user understands risks involved in using e-mails. For example, can they identify a phishing e-mail?	**Managing information** (16%) – indicates whether the user understands and follows important security measures of an organisation.	**Authentication** (14%)
Internet (24%)– indicates whether the user senses threats inherent in internet. For example, whether they use public Wi-Fi networks and how.	**Internet** (14%)	**Portable devices** (10%)
Authentication (24%) – indicates how the user creates and stores passwords, whether they use multi-level authentication, etc.	**Portable devices** (9%) – for example, how to protect data saved on a flash drive.	**E-mail** (9%)

The Risk Profile of Those Who Passed the DigiTest, 2020



aggregated overview to the person who is responsible for the information security of the respective organisation. This would help clarify the cyber hygiene issues that need further training among the colleagues for reducing risky behaviour and concurrent dangers.

Level Has Improved Every Year

By compiling an aggregate portrait of thousands of users of DigiTest and observing its change over the years, we can say that the results are good and improve every year.

DigiTest measures the risks of various domains on a 100-per cent scale where 0 means no risk and 100 is maximum risk. In 2018, the three riskiest domains were in the vicinity of 24 or 25 per cent; last year, this had dropped to 9–14 per cent.

Three years ago, the most critical issues were related to e-mails (e.g. can a user recognise phishing e-mails), internet (e.g. whether to use public Wi-Fi networks and how), and authentication (e.g. how to create and preserve passwords and use multilevel authentication).

E-mails and authentication remained in the top three of risks; however, internet was replaced by portable devices (e.g. how to use a laptop securely in a public place or protect data on a flash drive).

> The goal of RIA is to have all public sector employees pass the DigiTest or some other cyber training platform at least once a year.

The goal of RIA is to have all public sector employees pass the DigiTest or some other cyber training platform at least once a year. This way, we could help internalise the existing knowledge about well-known dangers but also provide new information about new risks. ●

Awareness Campaigns at the Service of Cyber Security

The Estonian Information System Authority (RIA) organises regular prevention and awareness campaigns to improve the level of cyber security in Estonia. Last year, the focus was on remote working, small and medium enterprises, and the Russian-speaking elderly.

In the autumn of 2019, we organised an awareness campaign ‘Ole IT-vaatlik!’ (Be IT-Conscious!) for the elderly. Encouraged by its success, we planned two larger campaigns to take place at the beginning of 2020 – the first was aimed at small and medium enterprises and the second once again at the elderly Estonians, but this time, we focused on the Russian-speaking population.

Sometimes, life finds a way to change your plans; the two campaigns were smaller due to the second wave of the COVID-19. At the same time, we added a third one during the emergency situation in the spring that concentrated on secure remote working. In cooperation with our previous campaign partner Havas, this reached the public in less than three weeks in April.

Be Especially IT-Conscious During the Emergency Situation!

Many remembered the slogan ‘Be IT-conscious!’ from the autumn of 2019; therefore, we decided to use the same solutions and familiar colour scheme six months later. This time, the main message was ‘Be especially IT-conscious during the emergency situation!’

The campaign outputs were the basic principles of cyber security, broadcasted through the advertising banners of local media portals and TV and radio commercials during two weeks at the end of April and beginning of May. These were spiced up by the fact that increased remote working also causes more potential weaknesses.

Protect Your Company From a Cyberattack

In September and October, we focused on small and medium enterprises. We continued with the already familiar slogan ‘Be IT-conscious’ and added ‘Protect your company from a cyberattack!’. Our campaign partners were advertising bureau Age, communication agency Akkadian, and consultation bureau Haap Consulting.

During the campaign period, we had promotional clips on TV and radio, decorated the bus shelters and city lights in Tallinn (the capital city),

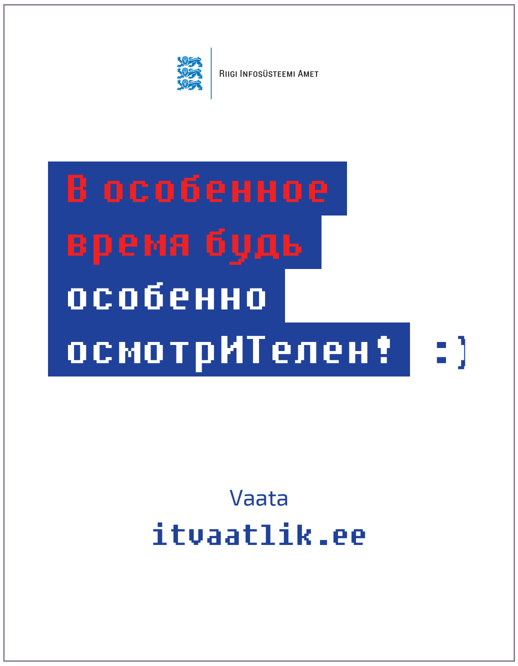
KAITSE ETTEVÕTET KÜBERRÜNNAKU EEST
ARVEPETTUS
Eesti tuleviku heaks
Euroopa Liit Euroopa Regionaalarengu Fond

Finantspettus, kus kurjategijad kaaperdavad ettevõtete omavahelise meilivestluse sel hetkel, kui on vaja arveid maksta, ning muudavad arvetel salaja pangakonto andmeid.

ETTEVAATUST! TEGEMIST ON LEVINUD PETTUSEGA EESTIS.

Ole IT-vaatlik!

itvaatlik.ee


Riigi Infosüsteemi Amet

В особенное время будь особенно осмотрИТелен! :)

Vaata

itvaatlik.ee

published opinion stories in newspapers, and had blinking banners in social media.

Although COVID-19 was making a comeback, several events took place in larger cities; the campaign messages were delivered as presentations or voiced during discussions with participants by the representatives of RIA and the private sector.

Special Attention to the Non-Native Elderly

A follow-up study of the 2019 campaign for the elderly demonstrated that the group that we managed to reach the least were the non-native elderly. For this reason, we organised a follow-up campaign with Havas targeting that group specifically.

Unfortunately, the second wave of the coronavirus hindered us quite seriously. As the elderly belong in the COVID risk group, we could not conduct the trainings we had planned or other contact events in Eastern Estonia or the libraries in Tallinn.

Instead, we recorded longer training videos and clips that explained the main cyber threats. We also organised virtual cyber trainings for the employees of libraries who will be able to help their clients even better regarding issues with computers and smart devices. We published press releases, went on air on ETV+ and Raadio 4, and in cooperation with the telecom company Telia, opened a helpline for pertinent issues that operated every Wednesday in November and December in the Central Library of Tallinn.

What Next?

The next big awareness campaign is aimed at IT-conscious e-voters before the local elections in October 2021. Before that, at the beginning of September, we want to reveal a new and improved version of the itvaatlik.ee website to the public; all past campaigns have ended up there, so in time, it should become a considerable prevention and awareness website dedicated to cyber security.

In the next few years, we want to organise needs-based targeted campaigns for the groups identified by statistics and various studies. Naturally, we are ready to react in a flexible manner like we did during the emergency situation in spring. We need a permanent budget line to achieve this; it would enable us to plan our activities better and longer in advance. ●

How to Guarantee the Security of 5G Networks?

Raul Rikk, the National Cyber Security Policy Director of Estonia, explains how to find a balance between the interests of national security and the interests of telecom companies.

The security of the new generation of communication networks has been one of the most important issues in cyber security in the past few years. This has been discussed domestically and internationally, in the European Union and globally. It is not a surprise because the functioning of developed societies depends almost completely on communication and information systems. 5G and newer-generation networks will continue to increase this dependence because the number and speed of transmission connections will increase several times compared to the current volume.

Security Issues Are Inevitable

As can be guessed, all devices will soon be connected to communication networks and the internet – smart devices, self-driving vehicles, robots, medical equipment, and other vital technology.

This will be immensely convenient, but will also set extremely high expectations to security. As all data moves through communication networks, communication infrastructure will acquire strategic importance in digital information societies.

However, we do not have avenues for checking the security of the technology in technical terms because it is complex, involves high levels of design, and is produced and assembled outside Estonia. Contemporary gadgets are so complex that it is impossible to really assess whether they contain malware, back doors, or significant security vulnerabilities. Frequent software updates and critical security patches, which need to be installed immediately, add to the complexity of the issue.

This poses a problem not only for Estonia, but for everyone. Even large countries, such as the US, the UK, France, or Germany, have limited capacity for inspecting hardware and software regardless of having large cyber security organisations with a staff of thousand or more strong.

Trust Is the Basis of Cooperation

Therefore, we find ourselves in a situation where the security of a digital state depends on trusting ›

Timeline

5G 2019

DEVELOPMENTS IN THE EUROPEAN UNION

12 March

European Parliament Report

22 March

Conclusions by the European Council

26 March

The Commission published a Recommendation for Member States to take concrete actions to assess cyber security risks of 5G networks and to strengthen risk mitigation measures.

technological producers. Technological producers are now more than just suppliers of devices and software; they offer a wider range of technological services and we build long-standing partnerships with them.

The issue is not with a single company or its technology, it is broader; can we trust them with providing solutions under circumstances where actual complete control of technology is impossible? When evaluating trust, we must assess the situation in which technology is produced, such as the legal implications and security-related behaviour of the manufacturer's country of location.

The member states of the European Union published a toolbox of joint measures at the beginning of 2020 which establishes the basis for ensuring the safety of 5G communication networks. This tells the member states to enforce higher security requirements for mobile network operators, evaluate the risk profile of technology suppliers, and apply restrictions on high-risk suppliers. Additionally, it is important to guarantee that the providers of communication services would use the hardware and software from several technological producers appropriately to avoid excessive dependence on one supplier and on high-risk technological manufacturers.

Regulation on the Security of Communication Networks

To implement the measures agreed between the European Union Member States, the Ministry of Economic Affairs and Communications has worked closely with various state authorities and communication companies on a regulation on the security of communication networks for the past two years. The regulation seeks to ensure that the construction of communication networks and using those for providing communication services would be done with secure technology and trustworthy partners. In order to do this, we need to exclude high-risk technology and also apply relevant security measures to acceptable technology.

> We find ourselves in a situation where the security of a digital state depends on trusting technological producers.

The high-risk technology and its potential threat to national security is evaluated during the procedure for issuing a permit for the use of hardware and software. The communication company must issue an application for the permit before using new technology. This will be processed by the Cyber Security Council at the Security Committee of the government, which evaluates whether the technology is high-risk hardware or software or if its use could threaten national security for other reasons.

According to the draft, the obligation to apply for a permit and the ban of high-risk hardware and software are implemented to hardware and software that is planned to be taken into use after the regulation comes into force. In addition, both apply to existing technology which implements or will implement 5G or newer functions.

9 October

The Member States finalised the EU coordinated risk assessment of the security of 5G networks.

21 November

The EU Agency for Cybersecurity (ENISA) published a report on threats relating to 5G networks.

29 January

Publication of the toolbox of mitigation measures by Member States. The Commission Communication on the implementation of the EU toolbox.

The obligation to apply for a permit and the ban of high-risk technology will be implemented in stages. They will apply to core networks immediately after the regulation comes into effect, but there is a period of transition for 5G and newer networks. This means that providers must apply for a permit for 5G networks immediately, but high-risk hardware and software can remain in use until 31 December 2025. Regarding other communication networks, the transition period is nine years or until the beginning of 2030.

Seeking Balance

Although the objective is clear – hardware and software used in providing communication services cannot be a threat to national security –, we have had many discussions and differing opinions on how to reach this.

Understandably, this regulation could cause additional expenses to communication companies. We have tried to find a balance between guaranteeing national security and the interests of communication companies. For this reason, we decided to have a period of transition. This would offer companies an opportunity to review their business activities and make necessary changes; on the other hand, it would ensure security of the 5G and other ICT infrastructure in the future.

In the autumn of 2020, a public consultation of the draft took place; after this, we made some amendments primarily based on the feedback of companies and considering their interests; for example, we extended the transition period for 5G networks from three to five years.

In March 2021, the Chancellor of Justice wanted to update the Electronic Communications Act before adopting the regulation. We hope to move as quickly as possible with the regulation because this security regulation is of essence for our tenders for frequency bands of 5G – we can start distributing frequencies after the security requirements have been decided.

Finding common ground regarding the regulation is in the best interests of everyone because communication companies and their clients stand the most to lose if we cannot move forward with the next generation of communication solutions. For Estonia, it is important to have reliable new communication solutions and IT infrastructure in general; we also want these to be free of high-risk technology. This is important for guaranteeing security and maintaining trust in our digital state. ●

The EU Toolbox for Guaranteeing the Security of 5G Networks

The member states should apply these measures and have authorisation for mitigating risks. The most important aspects for them to tackle are:

- Strengthening the security requirements for mobile network operators.
- Assessing the risk profile of suppliers; applying relevant restrictions to high-risk suppliers, including the necessary exemptions based on fixed assets.
- Guaranteeing a strategy with multiple service providers for each operator to avoid or limit excessive dependence on a single supplier and to avoid dependence on high-risk suppliers.

30 April

- The Commission invites Member States to take first specific and measurable steps to implement key measures.

30 June

- The Commission calls on Member States to prepare a report on implementation of key measures by Member States.

By October

- Review of the Commission Recommendation of 26 March 2019.

Cyber Security Is Not a Javelin Missile to Be Launched and Forgotten

According to **Oskar Gross**, the Head of the Cyber Crime Unit at the National Criminal Police, the digital world is intertwined with our daily lives quite independently and security must be an active endeavour of each person and organisation.

Cyber crime has been growing for years, and taking into account the brisk pace of digitalisation, it is safe to assume that its rise will not slow down. People often discuss the new or different characteristics of cyber crime but it is important to emphasise that cyber security principles have remained largely the same.

Marketing Challenge: Invisible, Yet Expensive

Sweeping dust under the carpet is useless; high-quality cyber security is expensive, particularly compared to a simpler plug-and-play solution. A great parallel would be taking a car for regular maintenance – when you drive away from the mechanic, you have paid several hundred euros but cannot see any visible changes to the vehicle. Yet we all know that if you neglect to change oil and filters, you might as well save a tow company's number on your phone. Cyber security lives in the current moment and the system that is working and safe now might contain security flaws in a year's time without maintenance.

This question is particularly important with software developments. The product looks exactly the same regardless of it being secure or unsecure. Unfortunately, the end user does not always care whether software has been developed to update all its components securely and automatically, whether it includes a log system that notifies the user of suspicious activity, whether logging into the program takes several steps, and whether the developers have considered the risks of unauthorised access and their mitigation.

Once the data of clients has been stolen, a computer has become a part of a botnet, or you see a

Guy Fawkes mask with the message 'H2cked by 1337 h4xx0r team' on your website one morning, it is too late to wonder, how.

The goal is not to blame the victim or justify the criminal but to point out that cyber risks are often underestimated. All components listed above are extremely important for preventing attacks and helping the subsequent police investigations.

The Level of Preparedness Determines the Outcome

Anyone can fall victim to a cyberattack regardless of the level of information security; however, the level determines the extent of the attack directly. Due to excellent preparedness, an information security team can quickly identify the access point to the systems, the number of computers that were compromised, and what kind of data was stolen, if any. It also allows to conduct a security analysis and evaluate what needs to be changed in the system to make it even more secure. We need competent people who know the type of information that needs to be gathered from the systems to identify attacks as quickly as possible. Even with excellent information security, some attacks are discovered only several months later; therefore, system logs should be stored for at least a year.

The existence of logs and system documentation makes involving CERT-EE considerably easier and ensures that an efficient police investigation can take place. If a victim has system documentation and logs, we can work to identify the criminal mostly independently and disturb your information security team to the minimum extent during the moments of crisis.

As a result of great cyber security, damage can be assessed quickly, the extent of the attack is determined and documented fast, and the functioning of systems is restored without delay. Otherwise, the confusion is great and the answer to the question of whether the criminal still has access to your systems is largely a guess because there is no information for the assessment. In addition, restoring the systems under such circumstances is frustrating and could be extremely expensive.

> The more information detectives can gather at the scene, the more likely the criminal is found.

In the case of cyber crime, the investigation begins at the scene of the crime, just like murder investigations in detective novels. The more information detectives can gather at the scene, the more likely the criminal is found. Cyber crimes resemble break-ins – they are easy to commit if the door is left unlocked but very complicated to investigate if the victim thoroughly cleans their home before the detective arrives.

Joint Cyber Operation of Estonia and the US

Estonia and the US Cyber Command held a joint online cyber operation in the network of the Estonian Defence Forces from last September until last November. Its goal was to stop malicious parties from accessing the network and strengthen the cooperation between the two countries as well as their cyber defence capabilities.

The cyber specialists from the US who are called the Hunt Forward team and the specialists of the Estonian Cyber Command looked for malicious actors in various networks and platforms. The US has conducted similar operations with other European countries, but it was the first joint operation with Estonian cyber experts.

The Goal is Ensuring Cyber Security

‘Joint operations with our closest ally, the US, are necessary to strengthen the cyber security of our services. They give our specialists an opportunity to share experiences and gain feedback about our current cyber defence capability. The operation was a successful milestone to our cooperation with the US partners,’ said Mihkel Tikk, the Deputy Commander of the Estonian Defence Forces Cyber Command.

‘Regardless of the pandemic, we have been able to be active in Estonia and elsewhere in Europe, which helps us learn about the enemies who could be a threat to the United States of America,’ stated Brigadier General Joe Hartman, the Commander of the American Cyber National Mission Force.

Respective teams actively seek and remove the malware of the opposition. Afterwards, they share information about the malware with the US government as well as private cyber defence companies and allies to increase the security of the critical infrastructure and related networks of the US.

Estonian National Defence Depends On Cyber Security

The US Hunt Forward teams play a critical role in the Persistent Engagement Initiative of the US Cyber Command. Its goal is to stop malicious activity in cyberspace that is not considered direct military engagement.

The task of the Cyber Command experts of the US is to defend the networks and platforms of the US government from enemies. The Defend Forward strategy of the US armed forces stipu-

lates cooperation with significant partners to prevent activities in cyberspace that could be used against critical US infrastructure.

'Estonian digital society depends on cyber, as does our national defence. For us, it is important that Estonia was one of the first to be included in this joint operation with the US. This provided us with an opportunity to evaluate the security of our networks. As we are a global leader in issues regarding cyber security, we must be ready to share our experiences with our allies to defend our networks better,' said Margus Matt, the Deputy Secretary General of the Estonian Ministry of Defence, whose responsibilities include cyber policies.

Cyber security is a team sport

By evaluating potential threats in cyberspace, this partnership between Estonia and the US gives both countries an opportunity to develop their cyber defence capabilities that, in turn, support global cyber security. Identifying malware and sharing information about it with the public and private sectors increases the security for all users when accessing cyberspace.

Cyber security is a team sport – no one can stop cyber threats alone.

'Cyber security is a team sport – no one can stop cyber threats alone,' stated Thomas Wingfield, the Deputy Assistant Secretary of Defence for Cyber Policy of the US. 'Our strategy is based on cooperation with our allies and partners in the private sector, academia, and governments to guarantee that our cyberspace remains a secure and open engine for innovation and development,' added Wingfield. The US Cyber Command cooperates with the US European Command and its NATO allies non-stop to prevent malicious activity in cyberspace.

Cyber defence cooperation between Estonia and the US takes place on multiple levels with the US Cyber Command, the US European Command, the Maryland National Guard, and the US Air Force Cyber Command. ●

Ciberseguridad: donde hay gana, hay maña*

EU CyberNet, funded by the EU and implemented by the Estonian Information System Authority (RIA), is building a cyber security centre in the Dominican Republic to provide support to all Latin America and the Caribbean countries.

The European Union is the largest donor of development cooperation in the world, increasingly aimed at digitalisation and cyber security.

The EU has executed several cyber security projects before, but in September 2019, the European Commission initiated the most recent one – the EU CyberNet, which is implemented by RIA.

What is the purpose of the EU CyberNet?

The goal of the EU CyberNet is to coordinate assistance that the EU offers to partner countries for improving their cyber security. In order to support this work but also to connect cyber experts all over the the EU, improve cooperation between them, and increase their professional skills, EU CyberNet is developing a network to include at least 500 experts and 150 organisations from all over Europe.

Having led the project for a little over a year, we received two significant announcements from Brussels at the end of 2020. First of all, the central role of the EU CyberNet was included in the new

Timeline

The Creation of the EU CyberNet

2013
- Cybersecurity Strategy of the European Union

2014
- Council conclusions on a rights-based approach to development cooperation, encompassing all human rights

2015
- European Agenda on Security
- Council Conclusions on Cyber Diplomacy

2016
- Shared Vision, Common Action: A Stronger Europe. A Global Strategy for the European Union's Foreign and Security Policy

2017
- European Consensus on Development
- Joint Communication 'Resilience, Deterrence and Defence: Building strong Cybersecurity for the EU'

EU Cybersecurity Strategy. Secondly, the European Commission proposed to extend the project by two years and added a task that is taking EU CyberNet's activities to a new level – to train the entire network of EU delegations in cyber security and establish a cyber security centre in the Dominican Republic that would cover the entire Latin America and the Caribbean region.

Why Latin America and the Caribbean?

In the context of cyber security, the countries in Latin America and the Caribbean are important partners for the EU due to their ambition to digitalise their societies and achieve better preparedness to counter cyber incidents, as well as for their shared values in general.

The general awareness of the Latin American countries about cyber threats has room for growth and the cyber resilience level differs from country to country. Few have established rules for the cyber defence of critical infrastructure or an effective partnership between the state and the private sector. Cyber exercises are rather rare and collaboration between the continent's countries to similar integration levels as in the European Union or the NATO does not exist yet.

If we add a booming ICT sector, then it is clear that the EU CyberNet can contribute to a significant extent because of its network of experts and practical assistance. EU CyberNet can increase the awareness of those states in cyber security matters and strengthen links between the governments, the academia, and the private sector.

Through greater cohesion and cooperation, we can help prevent the critical infrastructure of the countries in Latin America and the Caribbean from falling victim to hostile activity as this could start a cyber crisis with global implications.

How are we going to achieve this?

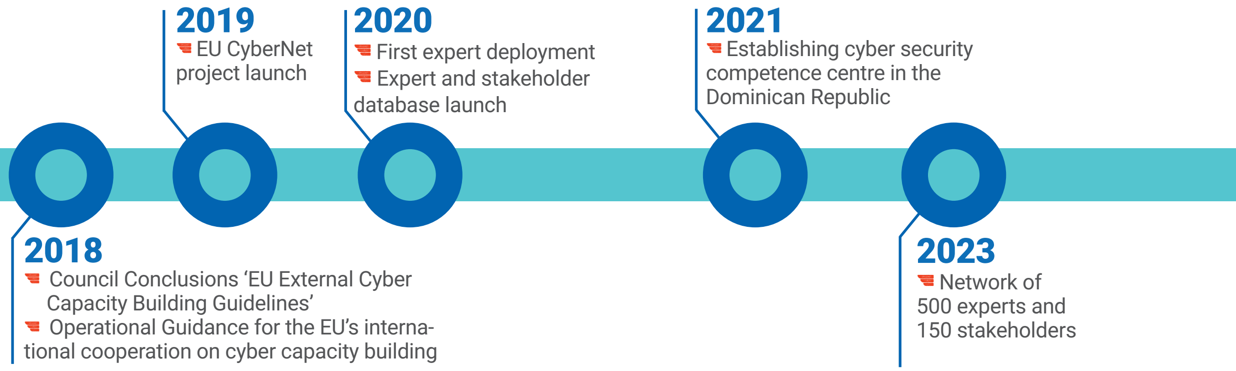
An international and regional organisation cannot be established overnight. Fortunately, Estonia has the unique experience of initiating and developing the NATO Cooperative Cyber Defence Centre of Excellence.

The number of regional cyber centres will continue to grow. For example, Singapore has created a cyber centre for the ASEAN countries. There are at least two similar initiatives in Africa. So far, Latin America and the Caribbean did not have one and this presents the EU and RIA with a huge responsibility.

It is possible to implement complicated projects far from home.

The centre should achieve initial readiness by the end of 2021. Our goal is to create maximum synergy with the original tasks of the EU CyberNet, i.e. the establishment of an international network of experts and organising trainings. We want to show that it is possible to implement complicated projects far from home if you have the will, a plan, and competent people.

If you know, for example, how to carry out sectoral and/or national strategies, increase institutional capacity, prepare laws that respect human rights, defend the critical information infrastructure, organise the work of CERT, or build international cooperation networks, please contact us through the following website: www.eucybernet.eu/expert-pool. *Adelante!* ** ●



2019
- EU CyberNet project launch

2020
- First expert deployment
- Expert and stakeholder database launch

2021
- Establishing cyber security competence centre in the Dominican Republic

2018
- Council Conclusions 'EU External Cyber Capacity Building Guidelines'
- Operational Guidance for the EU's international cooperation on cyber capacity building

2023
- Network of 500 experts and 150 stakeholders

* Cyber security – where there's a will, there's a way (in Spanish).
** Forward! (In Spanish)

Estonia as a Pioneer of Cyber Diplomacy

As a state hardened in a cyber conflict, one of the main directions in the Estonian international politics has been cyber issues. **Heli Tiirmaa-Klaar**, Director General of the for Cyber Diplomacy Department at the Estonian Ministry of Foreign Affairs, describes our achievements in this sphere.

In 2007, when Estonia was hit by massive cyberattacks, there was not a single international political mechanism in place to alarm the international community of the importance of cyberattacks, ask for help from other countries, or to condemn the perpetrators. Since then, Estonia has done a lot to raise the issue of cyber security in international organisations and in bilateral and multilateral diplomacy.

International Law Applies In Cyber Space

Currently, we find ourselves in a completely different situation. We have an International Cyber Stability Framework that reinforces the application of international law in cyber space and stipulates rules of behaviour for states.

This was created in the last decade as a result of the work done by the UN Group of Governmental Experts. Five times out of six, Estonian representatives have been selected to be a part of that group. The UN will remain an important organisation to help implement the framework, increase international trust, and raise cyber defence capability, particularly in developing countries.

The hard work of cyber diplomats can seem like a separate niche that is centred around working groups, reports, and conferences. For Estonia, increasing the wider understanding of cyber issues in the context of international security has been an important goal. This is the only way for countries to make conscious decisions.

We Condemned Cyberattacks Against Georgia

As a member of the UN Security Council until the end of 2021, Estonia is at the absolute centre of the most important diplomatic discussions in the world. We have used this as an arena to raise cyber awareness in an even wider circle. In March 2020, Estonia achieved something historic – together with the US and the UK, we condemned the extensive cyberattacks against Georgia that had taken place a few months earlier. This was the first time that specific cyberattacks were discussed around the official table of the Security Council.

We were also forerunners with an unofficial virtual session on 22 May 2020 that focused on the stability and conflict prevention in cyberspace. Estonia and many other countries expressed their strong conviction that cyberspace does not differ from other domains where international law applies and states must follow certain rules of behaviour. Altogether, about 60 states and organisations participated in the session. This year, we are planning to take the next step towards raising awareness about cyber issues in the Security Council. ●

Tallinn Summer School of Cyber Diplomacy

Large important summits are not enough to make cyber diplomacy a part of mainstream foreign policy. The Ministry of Foreign Affairs organises various trainings for the diplomats of the EU and the NATO as well as other countries actively involved in cyber issues.

In 2019, we started the extremely popular Tallinn Summer School of Cyber Diplomacy; through this, we have reached many diplomats all over the world. A virtual Winter School took place in February 2021; its sessions can be viewed on the website of the Ministry of Foreign Affairs at vm.ee/et/node/53915.

For Estonia, increasing the wider understanding of cyber issues in the context of international security has been an important goal.

The EU's New Cyber Competence Centre

The EU is remarkably increasing its investments in the research and development of cyber security. The EU is going to establish a Cyber Competence Centre and a Network of National Coordination Centres.

After lengthy negotiations, the lawmakers of Europe decided that the EU Cyber Competence Centre (CCC) with administrative functions will be located in Bucharest. In addition, a Network of National Coordination Centres (NCC) will be created and it will become the main driving force for the research and development of cyber security in the EU. The EU regulation will also prepare the ground for more regular cooperation with industry.

Member States Will Have More Rights

For the next long-term budgetary period of the EU (2021–2027), a new Digital Europe Programme (DEP) was created; the new Competence Centre will manage the 1.7 billion euros allocated to this programme for cyber security. In addition, the cyber security projects that are funded by Horizon Europe will be coordinated by the new Centre. This decision means that member states will have more say in setting priorities and approving projects in comparison to the current technocratic management of research.

Besides scientists, the driving force of the new network will be the National Coordination Centres, or NCCs; each member state will select one of their authorities or consortiums with cyber security capabilities as the local centre. NCCs are going to have a separate budget allocated from the DEP, which must be used for fulfilling the tasks stipulated in the regulation, including increasing the research and development capability regarding cyber security. The NCCs manage joint actions between member states where scientists and experts from different countries develop specific technologies or skills for cyber security.

Community of Enterprises and Scientists

The third important development is a community of enterprises and scientists; its members will coordinate research and development in their respective countries and in the entire EU, as well as advise the CCC in the creation of its working plans.

Although the lawmakers of the EU reached a compromise regarding the regulation already in December 2020, it will take effect in the first part of 2021. Every member state must appoint an NCC within the next six months; after that, they can begin with specific projects. Therefore, the new research and development framework for cyber security in the EU will be launched in the second half of 2021. ●

> The new research and development framework for cyber security in the EU will be launched in the second half of 2021.

Interreg CYBER Increases Cooperation in Cyber Security

The European Union promotes regional cooperation through the Interreg platform with a goal to intensify cross-border initiatives and help the less developed regions of the continent catch up with the rest. This cooperation format is novel in the field of cyber security. A programme was created to improve the competitiveness of small and medium enterprises (SMEs).

RIA represents Estonia in the Interreg CYBER project that will end in the summer of 2023. The capability of SMEs in the field of cyber security is increased through mapping the strengths and weaknesses of ecosystems, exchanging best practices, the implementation of Action Plans, and other activities.

RIA selected two practices from the good practices of other project partners, inspiring projects that are now in the implementation phase in Estonia: Cyber Breakfast, inspired by the region of Brittany, is a series of regular meetings for cyber security companies, universities, and national authorities; and a development programme for water companies that was prepared with recommendations from the Slovenian project partners in mind.

During the project, we have also held cyber security hackathons; this way, RIA contributed to the cyber defence competition KüberPuuring that took place in December 2020.

NIS 2.0: the Updated NIS Directive of the EU

Last December, the European Commission published a proposal for amending the Directive on **security of network and information systems** (NIS). What kind of changes would this bring if the amendments came into force?

The goal of the NIS Directive is to raise the level of cyber security in the European Union countries and harmonise pertinent laws. Intense negotiations lie ahead because the cybersecurity level of countries is vastly different, as are their opinions about the opportunities and the necessity for improving the situation.

Size Matters

One the central issues of the new proposal is the proposition to widen the scope of application of the NIS Directive and enforce the so-called Size Cap Rule. This means that in certain domains, such as food production, postal services and waste management, businesses with 50 or more employees must comply with the directive. In accordance with the proposal, the public sector is also included in the framework.

If this rule is included, the new requirements would apply to hundreds of thousands of businesses operating in the European Union; in Estonia, this would concern about a hundred entities. In addition, every state can include some smaller enterprises with critical importance.

Competent authorities in several member states feel like thousands of additional entities create an unfathomable workload, primarily due to supervision.

One Step At a Time

The Commission has set several recurrent goals with this directive; one of those is harmonising the organisation of cyber security in the member states. They intend to achieve this goal with detailed requirements that must be included in national cybersecurity strategies and national frameworks for cyber crises management.

ENISA, the European Union Agency for Cybersecurity, evaluates the efficiency of implementing these frameworks; it takes into account the indicators of the implementation of the strategies when preparing the index of cyber security maturity levels of the member states.

It also tries to increase the level of cooperation and trust between the member states with reciprocal evaluations which are conducted at the strategic, operative, and technical level. The Commission presented a plan to create a security vulnerabilities register of the EU that would meet

the needs of the EU, consider its unique characteristics, and complement the National Vulnerability Database of the US (NVD).

Management Is Responsible For Cyber Security

Compared to the directive currently in force, the new proposal takes a much more detailed approach to security requirements. Everyone who needs to conform to the directive should prepare specific guidelines for the security of the supply chain, the procedure of general information security, and the use of cryptography.

Another included principle states that the management body of a company is primarily responsible for the cyber security measures and they will be held liable for not meeting the requirements. The principle regarding the rules of supervision and the amount of fines has also changed; the fines that are issued in case of violations are similar to the fines of the General Data Protection Regulation. ●

Journey to NIS 2.0

- In 2016, the Directive on security of network and information systems (NIS) came into force; its goal is to improve the level of cyber security in the European Union Member States.
- In December 2020, the European Commission published a proposal to amend the NIS directive.
- The main amendments in the NIS 2.0 concern the scope of application of the directive, the exchange of information, security requirements, and amounts of fines for the violation of the directive's stipulations.
- NIS 2.0 will likely be adopted by the lawmakers of the EU within two years; after this, the member states have 18 months to transpose it into national law.

Compared to the directive currently in force, the new proposal takes a much more detailed approach to security requirements.

Cyber Security in Estonia 2021

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

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

Illustrations: **Tolm OÜ** ja
Linda Vainomäe (Profimeedia OÜ)

Photography: **Nelli Pello**

Printed by: Ecoprint AS

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