REPUBLIC OF ESTONIA
INFORMATION SYSTEM AUTHORITY

# Trends and Challenges in Cyber Security

Quarterly Assessment, 2nd Quarter 2021

## Ransomware attacks continue

### SITUATION

In recent months, ransomware has been an issue for both Estonian businesses and private individuals. For example, we were informed of a case wherein ransomware called LockBit was used against a company providing IT services, eventually hitting four more businesses using their Remote Desktop Protocol (RDP). A wholesale company operating in Tallinn also reported of an incident in which data on their server (including accounting documents and backups) had been encrypted.

Although criminals generally use ransomware to target businesses, private individuals can also occasionally get hit. A video and photo editor reported that two of their hard drives and their Synology files were encrypted. As they had not backed up the information, restoration proved difficult. In this case too, the infection likely occurred through RDP.

Globally, there were several serious cases of ransomware attacks in the second quarter that garnered a lot of attention, forcing the general public to be aware of the dangers of ransomware and the related damage. The attack on the US energy company Colonial Pipeline affected the pipeline which provides almost half of the fuel used on the East Coast of the country. The pipeline was shut down for almost a week, leading to fuel shortages in several states. A cyber-attack on the Irish healthcare system using the ransomware called Conti also caused great damages, as patient data was stolen and disclosed during the attack and medics did not have access to diagnostics or medical records. The provision of healthcare services in the country was disrupted for more than a week.

### ASSESSMENT

The damage associated with ransomware attacks is often great and can have long-term consequences for both an individual and an organisation. Although no one has complete protection against ransomware, it is still prudent to do everything in one's power to ensure that even if cybersecurity measures fail, the impact would be as painless as possible. In particular, this means that data needs to be scattered, backed up, and recoverable.

The number of known ransomware incidents in Estonia remains usually between 5 and 10 in a quarter and no major incidents have occurred so far. However, the outlook for the future is worrying, as ransomware attacks have become a very lucrative type of crime for criminals globally. The issue of ransomware is also increasingly being discussed in the context of national security, although in the past, governments have focused more on the activities of state-sponsored cyber groups. Ransomware attacks may be unpredictable and devastating, as the motivation is money. Unlike state-sponsored hackers, these groups are not constrained by political guidelines and the choice of targets is not limited by moral considerations (e.g., even hospitals have been attacked several times).

So what can you do besides protecting yourself, your business, or your organisation with appropriate cybersecurity measures? At the national level, various options are available: increasing the efficiency of law enforcement in prosecuting international groups, as well as making the use of cryptocurrencies less anonymous, so that it would not be so easy for groups to demand money from their victims only to disappear soon after. It could also be discussed whether and how the payment for ransomware (also through insurance companies) is legal, considering that this means financing criminal activities. The issue of ransomware is far from being a new concern, but its impact on society is growing and so we will surely reflect on this issue also in future quarterly reviews.

## Cybersecurity of the service provider is also your risk

### SITUATION

This year, we already know of four cases in Estonia where the customers of an IT service have been attacked after the service provider was compromised. At the beginning of the year, the hosting server of a technology company providing a popular information management system for many private and public institutions was hacked using a software vulnerability. Fortunately, the company quickly identified the incident and gave notice to customers. In addition, in the ransomware case described above, the target of the attack was the IT-service provider and thereby it was also possible to encrypt the data of four more companies. There was also a case in May where a company providing accounting software was attacked and access was gained to the systems of one of the local governments using the software.

### ASSESSMENT

A successful attack against a service provider can be highly lucrative for a criminal, as attacking a service provider gives them also access to others. A prior overview of customers who depend on the company providing this service makes this option particularly attractive. Such lists can often be easily found on a service provider's website, containing private companies as well as government agencies. It is usually done for building reputation, but it is not a very good practice in terms of customers' cybersecurity. The more information criminals are able to gather about the customers of a company in a short span of time, the greater the motivation may be to attack and plan further steps. Thus, the Information System Authority encourages at least government agencies and providers of vital services to think critically about whether they should allow all of their partners to use their name for advertisement.

Another reason why incidents of this type are increasingly common is that the level of cybersecurity of external service providers is often lower than that of organisations using these services and the latter do not have very specific tools to improve this. When selecting a service provider, cybersecurity may not have been amongst the most important selection criteria. Recommendation of the Information System Authority is to include cybersecurity aspects in contracts with service providers as precisely as possible. Such aspects should include the obligation to report incidents and to haveV effective contingency plans. Against the backdrop of attacks on global supply chains, which we discussed in the previous quarterly overview, the general trend in Europe and the United States is towards stricter requirements for cybersecurity, at least for companies providing services to the public sector.

## Elections are not the place for experimenting with facial recognition

### SITUATION

An analysis by the cybersecurity experts of Cybernetica on the use of biometrics in electronic voting has just been published. This analysis states that the inclusion of facial recognition in elections is feasible, but that there are risks related to the infringement of privacy and technological complexity which may not be outweighed by the benefits.

The analysis leads to the main conclusions that facial recognition would be technically complex and require extensive technical changes. Using it would increase the risk of errors in electronic voting and significantly increase the requirements on the performance of the system. It is also impossible to avoid errors completely.

The electronic voting service would also become more inconvenient for the user, as it requires having a device with a good camera and the ability to use it. Infringements of privacy are also an acute issue. The analysis is public and available on the website of the Information System Authority.

### ASSESSMENT

Information System Authority is of the opinion that the use of facial recognition in electronic voting would require longer testing. This would mean fundamental changes to existing digital identification, including a new evaluation of risks and benefits and the introduction of new legal provisions. Prior to the introduction of electronic voting, we tested and security tested the principles of digital identity in hundreds of services in both the public and private sectors. As the wider use of biometrics is currently largely unregulated and there is no overview of the most secure solutions, there should be no rush to use this option. Additionally, there will be a number of organisational issues, such as the availability of a proper camera and of other tools, which may affect participation in electronic voting.

Using facial recognition in the future would require discussing the infringement of privacy (e.g., someone's home is captured with the camera) at the legislative level and in the society. It also requires an acceptable rate of error and accessibility (if a person does not have a good internet connection or a camera to participate in the voting process). Only then can we consider the volume of the new development, the new aspects of cybersecurity of this development, and the related data protection issues. As a centre of competence, the Information System Authority intends to take an active part in this discussion.

## A Joint Cyber Unit for Europe?

The European Commission has made the implementation of the principle of solidarity a priority in the field of cybersecurity – if the existing CSIRTs and the CyCLON networks provide for a close exchange of information at a technical and an operational level, then the Joint Cyber Unit proposed by the Commission would specifically deal with large-scale incidents.

The Commission notice discusses the plan to create both a physical and a virtual platform without a new legal body. The physical platform would be located on the premises of the CERT-EU and the representative offices of ENISA in Brussels. The scope of the unit would be fairly wide, as the Commission envisages that it would become a platform for communication and operational cooperation for the civilian, military, and intelligence communities. Certain private sector representatives would also be involved in the exchange of information and the exercises.

The central pillar of the Joint Cyber Unit would be the Rapid Reaction teams composed of experts designated by the member states and able to be deployed to the member state in need, The Commission has also set the aim of agreeing on a single EU cybersecurity crisis management plan.

As the plan of the Commission does not relate to any legislative act, it can be implemented through cooperation agreements between the member states and EU agencies. The success of a Joint Cyber Unit largely depends on the amount of resources that member states are willing to contribute to the joint activities. The main funding for the unit should come from the Digital Europe programme.

The cyber unit should be operational by the end of next year, but initial activities, such as capability mapping, will be conducted already this year. By autumn, it will become clearer how will the member states and the European cyber community accept the Commission's proposal.

### DOING WELL:

The Information System Authority offers an online learning solution DigiTest in cooperation with the cybersecurity company CybExer Technologies. This test aims to raise the cyber awareness of public sector employees. As of mid-June, more than 16,200 public sector employees had passed the DigiTest. This is about 70% more than two years prior. A new learning module was added to DigiTest in June, with the module focusing on the risks associated with teleworking.

### COULD DO BETTER: ⚠

Attacks on schools increased in May and June, during the peak of graduation, examination, and tests. In most cases, attempts were made to disrupt the work of educational institutions through Denial-of-Service attacks, but in some cases also using ransomware. Such attacks are often carried out by students of the same school who mistakenly hope that this way they can escape an exam or a test. However, instead of spending their time on ordering, preparing, and conducting an attack, students should use it for gaining more useful knowledge.

***This summary was prepared by the Cyber Security Branch of the Estonian Information System Authority (RIA) with the aim of explaining the trends of cyber threats to the widest possible audience, including readers outside Estonia. The situation in cyberspace is analysed in more detail in monthly summaries. CERT-EE distributes more technical recommendations at trainings and on RIA's website.***