Republic of Estonia
Information System Authority

Trends and Challenges in Cyber Security

Quarterly Assessment, 1st Quarter 2020

Taking Advantage of The COVID-19 Pandemic

SITUATION:

At the end of the first quarter, the coronavirus pandemic is affecting everyone's daily lives. Among other things, this means a significant increase in the use of e-services for working, studying, shopping, and leisure time. It has also created a huge demand for information related to, for example, the spread of the COVID-19 virus or the resolutions to the situation. Electronic communication with workplaces, schools, and e-service providers has also increased. All this creates a breeding ground for cyber incidents.

In March, a global trend arrived in Estonia of criminals trying to exploit the panic surrounding COVID-19 for both malware distribution and phishing – we saw an e-mail mimicking the Health Board's recommendations and were also informed of fraudulent calls where criminals tried to gain remote access to a user's computer by saying that they were checking the computer's security settings. Attempts are also being made to take advantage of teleworking, which is an unfamiliar situation to many – there was an e-mail campaign asking people to open links to activate teleworking applications that actually installed malware on the person's computer.

CERT-EE has learned through global reporting networks and seen through its tools a wide range of malware, phishing e-mails, and spam, all of which use the COVID-19 situation to cause people to click on them. Estonia (including the Estonian language) is still largely untouched.

ASSESSMENT:

We have seen before that global trends arrive in Estonia with a delay of a few weeks or a few months, so we can expect a large number of incidents in the near future, the starting point of which is an e-mail or application that uses COVID-19 as bait. It is also unlikely to depend on the length of the emergency situation, as the need for information on the spread, prevention, and elimination of the virus will last longer.

Particular attention should be paid to schemes that exploit the fear of the virus, which may become increasingly attractive to criminals. Every day thousands of new COVID-19 related domains are registered, some of which are linked to criminals hoping to use them in phishing campaigns and other fraudulent activities. A number of new online stores have already been set up (albeit in English) that sell fake vaccines and products that protect from the virus. We are also aware of campaigns in other parts of the world that promise to reveal to the user the people living around them who are infected, but only for a certain amount of money.

We share the most operative information about e-mail scams, fraudulent calls, and more on the Information System Authority's Facebook page, where we also give recommendations for avoiding and recognising them.

Incidents Related to Increased Teleworking

SITUATION:

Working and studying from home has accelerated the transition of companies, schools, and public authorities to teleworking. New video conferencing facilities and communication channels within institutions are likely to be in place by now, but in the case of communication with other institutions/companies, including counterparties abroad, new platforms for communication, file sharing, and other collaboration are still being agreed upon, where data processing procedures are not known to all parties.

This may mean that sensitive information for internal use or sensitive information about the company may be accidentally shared with service providers, who may, in the best case scenario, use it only to personalise advertisements, or, in a worse-case scenario, save it in a place over which the owner of the information does not have sufficient control. Databases of large service providers are also known to leak from time to time.

In addition to service providers, we are also aware of the unsafe use of data and equipment at the individual level. For example, leaving the institution's salary details and passwords on a board behind the speaker during a video call; sharing screens in a video call so others can see other files or browser tabs of the sharer; installation of databases and work software on personal computers (without the institution knowing the level of security).

Criminals who use compromised accounts or weak e-mail protocols to defraud employers of wages to third-party bank accounts have also become more active. Without the usual face-to-face communication in the workplace, such attempts at fraud are more difficult to detect than usual.

ASSESSMENT:

It is clear that, in the current situation, the priority is that work can continue at all; thinking about security and data protection has sometimes remained secondary. However, once the situation has stabilised a bit, this needs to be addressed, because the more we work, learn, and communicate online, the more important cybersecurity is. This is true when interacting with teachers, clients, employers, or employees.

As the need for teleworking is likely to last for a while, both in Estonia and elsewhere, we can expect to see more campaigns where criminals try to distribute malware or steal data mimicking different teleworking applications. The popularity of the Zoom video conferencing application is already being used by criminals who send fake notifications or links to pages seemingly connected to Zoom, in an attempt to collect user data.

We have compiled the basics of cybersecurity for working and learning from home on the Information System Authority's blog and the Estonian Association of Information Technology and Telecommunications has called on companies not to mitigate information security requirements solely due to the emergency situation. The ISKE standard and the Cybersecurity Act continue to apply. E-mail fraud can still (largely) be prevented by SPF, DMARC, and DKIM protocols as well as multi-factor authentication.

Vulnerability Reports Are Not Reaching Intended Recipients

SITUATION:

Since summer of 2019, we started sending automated notifications about misuse and various vulnerable devices/settings in their networks to Estonian telecommunications companies, web service hosts, and institutions managing their own networks.

We send such notifications at least once a day if we have identified infected devices, security vulnerabilities, or configuration errors that could result in a cyber incident. To simplify: if we determine that an IP address is contacting the malware monitoring server for instructions, we will use the IP address to notify the service provider of the client whose device is infected with malware.

At the same time, we have repeatedly received notifications of cyber incidents in Estonia, the root causes of which we have previously discovered and informed the service providers of. For example, in March, a company's server was compromised through a vulnerability known to the company's service provider thanks to our monitoring activities. This shows that the information transmitted by CERT-EE is often not forwarded from the service providers to the clients, which, in turn, means that the client cannot do anything to eliminate the risk, prevent it, or correct the error.

ASSESSMENT:

The more companies use external service providers to host their e-services – service providers who provide their own infrastructure but leave the responsibility and control to the client – the more important it is that reports of potential threats and security vulnerabilities are not overlooked.

CERT-EE has the obligation arising from the Cybersecurity Act to monitor the Estonian Internet space and identify cyber threats there, as well as to forward alerts for the prevention and resolution of cyber incidents. As CERT-EE does not have access to the client's data of the online or hosting services, we are not able to use the IP address to inform the person affected directly. This is the service provider's responsibility. However, many incidents would not have occurred if the alerts we sent had been used correctly and communicated to the clients.

CERT-EE monitors cyberspace 24 hours a day and we urge online or web hosting providers to forward the information sent to them more quickly – the clients of the service have a legitimate expectation to be informed and warned. We also call on companies with a large digital footprint to ask their service providers what procedures are in place to ensure that alerts received from CERT-EE reach the client or who is ultimately responsible for exploiting these security vulnerabilities.

GOING WELL:

Estonian E-services Coping Fairly Well With Increased Traffic

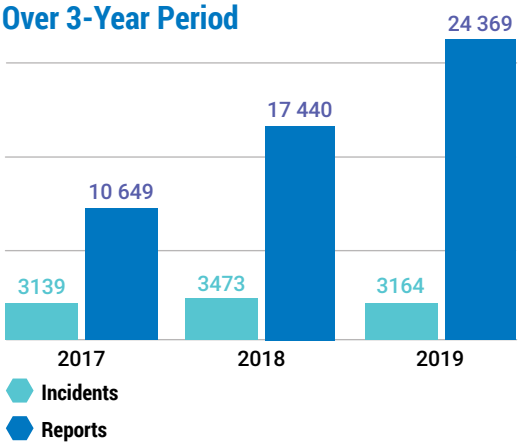
Despite the significantly increased workload in the crisis situation, Estonian e-services are generally doing well. There have been a few short-term service interruptions due to high traffic in the learning environment or in the field of healthcare, but for the most part, we consider the viability of the e-state to be good. In addition, the transition of many companies to teleworking has been successful so far without major cyber incidents.

COULD BE IMPROVED:

Service Interruptions Call For Increased Spending

Regardless of the emergency situation, however, it is important to note that regular service interruptions have a wide-ranging effect in Estonia – especially in the emergency situation. In most cases, service interruptions are due to outdated software and hardware, which, in turn, indicates insufficient investments in infrastructure. Managers need to realise that the security and reliability of services depend directly on these resource-intensive decisions, and that they should not focus on saving money on the timely maintenance and upgrading of systems, especially as the criticality of the service to the society can change overnight.

Reports Submitted to CERT-EE Over 3-Year Period



Incident *means the confidentiality, integrity, or availability (CIA) of information or systems has been compromised.*

Reports *are all notifications of incidents with and without impact to CIA, reported service interruptions, spam e-mail notifications, questions to CERT-EE, summary reports of partner institutions, etc.*

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