Republic of Estonia
Information System Authority

Trends and Challenges in Cyber Security

Quarterly Assessment, 4th Quarter 2021

The Biggest Vulnerability of the Year Affects Hundreds of Millions of Systems

SITUATION

On December 9, a critical vulnerability in the logging feature of the Java programming language, known as Log4j or Log-4Shell, was published.

It quickly became clear that this was the most important security vulnerability of the year: this logging feature is widely used in devices and software products around the world, and the vulnerability is relatively easy to exploit, allowing an attacker to easily access the information system if certain conditions are met.

Although various software vendors and developers responded immediately and began to develop the necessary security patches and updates, the list of affected products and devices is so long that the process is still on-going. A number of additional security vulnerabilities that need to be dealt with in parallel have also been identified.

ASSESSMENT

After the news came out, Estonian IT and information security professionals became very busy: they had to identify which products and services were affected by the vulnerability, which were most at risk, which security patches were available and then start implementing them. The same was done for the services managed by the Information System Authority, and like many others, we found ourselves spending tens and tens of hours patching the log4j vulnerability.

What have been the consequences of the security vulnerability so far? After the disclosure, criminals began actively monitoring cyberspace to find vulnerable systems; CERT-EE could see the same in Estonia. In December, we received reports of the first local victims whose systems had been compromised through that vulnerability and, in some cases, malware had been installed to mine cryptocurrency. In addition to crypto mining, there are cases in the rest of the world where vulnerabilities were used to prepare for ransomware attacks. According to international media reports, some criminal groups (particularly those linked to China and Iran) have tried to exploit this vulnerability for intelligence purposes.

So far, there are no reports of mass attacks via the log4j security vulnerability. However, we may be in a period of calm before the storm: the initial wave, where criminals aimed primarily to find and gain access to vulnerable systems, is likely to be followed by new waves with more serious attacks. The accesses found in the first wave will be analysed, expanded where possible, and resold, and it is likely that we will have to deal with the consequences of the log4j vulnerability for months and even years to come.

What can you do to protect yourself? For the average user, the first step is making sure that the software used on the devices has been updated to the latest version. Employees of companies and public institutions can contact their information security officers to find out what steps have been taken to reduce the risk of this security vulnerability.

Although all systems and services should be updated, special attention should be paid to those that are open to the Internet. If you suspect that the information system has been compromised, please inform CERT-EE.

DDoS Attacks on Schools Have Increased Significantly

SITUATION

As the new school year started in September, the number of denial-of-service (DDoS) attacks on educational institutions and e-learning environments increased sharply. General education schools, vocational training institutions, and universities were attacked, as well as the e-learning environments Tahvel and Moodle.

The DDoS attacks on educational institutions and services accounted for more than 70 per cent of all DDoS attacks between September and December. The various types of attacks (e.g. DNS gain attack, TCP SYN flood, DDoS L7) lasted from a few seconds or minutes to a few hours. During some of the attacks, the services of other institutions using the infrastructure of the Education and Youth Board (HARNO) were disrupted as well.

ASSESSMENT

When analysing the timing of the attacks, a pattern emerges: as a rule, they were carried out during the day on weekdays. They were not carried out during weekends and school breaks but reappeared with the start of studies. Most likely the persons responsible for the attacks were students who wanted to disrupt the school work and ordered the attacks from specialised forums. Interference with other institutions and services was likely to be an unintended but dangerous side effect.

It is often difficult for schools, especially smaller ones, to defend themselves against DDoS attacks. It requires specific knowledge, tools, and money. As one solution, schools should consider joining the state network that offers DDoS protection to their customers. In order to find out more about the possibilities of joining the state network, the school should turn to the local government.

Efforts on Election Cybersecurity Paid Off

SITUATION

From 11–17 October 2021, local government council elections were held in Estonia. As usual, it was possible to vote both on paper at the polling station and electronically. However, these elections differed from previous ones because, for the first time, voter lists at the polling stations were electronic, not printed on paper. This means that an employee of the polling station checked the voting rights of the voter on their computer from the election information system (VIS3). That allowed voters to vote in any polling station, not just the one close to home.

From a cybersecurity perspective, going from paper to electronic obviously added some new challenges. In addition to e-elections, it was necessary to pay attention to, for example, approximately 1,000 computers of the employees of the polling stations, a secure network connection, the cyber hygiene of users, and the election information system.

ASSESSMENT

There were a few cyber-related incidents, only one of which had a significant impact on the conduct of the elections. It occurred on October 16, when a large number of the employees of polling stations did not have access to the election information system for about 40 minutes. This was caused by a security measure put in place by RIA for the national authentication service TARA to prevent possible denial of service (DDoS) attacks.

During those 40 minutes, the employees of the polling station used the so-called envelope voting method. This means that the voter put their ballot paper in an anonymous envelope, which in turn was placed in another envelope with the details of the voter on it. When the operation of the election information system resumed, the voter data on the outer envelope was entered into the election information system and the inner envelope was placed in the ballot box.

There were also some functionality issues at the beginning of the election week (e.g. wrong time in the voter application), but these did not affect the cybersecurity of the elections in any way.

In general, e-voting software worked exactly as intended. We did detect two attempts to modify the data sent from the voter application to the vote collector. Those attempts failed and the suspicious activity was directly visible to CERT-EE.

Overall we assess that the efforts before and during the elections to ensure cybersecurity were successful. The work will now continue in view of the 2023 parliamentary elections, and based on the recent experience we will know what to focus on even more.

The Cyber Hygiene of the Estonian People Improves Steadily

A year ago, we were pleased that the results of a survey conducted by Statistics Estonia showed that the cyber hygiene of the Estonian people has slightly improved. We have now received data for 2021 and it seems that the positive trend is continuing.

The most positive discovery is that the strength of passwords has improved in all age groups. In 2018 we saw that many people, especially among the elderly do not use different passwords in different environments and since then, we have emphasised the importance of strong and unique passwords in all of our awareness campaigns.

The situation has gradually improved in other areas as well. To the question listing different cyber security practices, 11.3% of respondents answered that they have not followed 'any of them' in 2021, which is 1.7% lower than in 2019. While the change may seem marginal, it is that answer in particular that we consider an important indicator of the general level of cybersecurity among population. Our goal is to achieve a situation where the percentage of people not following any cyber hygiene practises at all is even lower.

What are actions you have taken to strenthen security or privacy while using the internet for personal purposes?

Proposed option: Strengthened passwords or using different passwords (including passwords that are longer and more complicated than the minimum requirements, regularly changing them etc)

Age	2019	2021	Change
16-24	82,5%	87,1%	+4,6%
25-34	77,2%	80,7%	+3,5%
35-44	72,3%	74,9%	+2,6%
45-54	58,1%	65,7%	+7,6%
55-64	47,2%	54,5%	+7,3%
65-74	33,1%	42,1%	+9%
Total	**64,1%**	**68,9%**	**+4,8%**

Adult activities in the household to protect children under 16 from potential dangers in cyberspace	2019	2021	Change
Active monitoring of behaviour in social networks (e.g. on websites such as Facebook, Instagram, Vkontakte, content of posts by children, friend lists)	46,1%	47,2%	+1,1%
Active monitoring of Internet usage other than on social networks (e.g. videos watched on Youtube; games played; forums and news portals visited, tracking web history)	53,2%	48,2%	-5,0%
The device used by the child is subject to restrictions (e.g. use of parental control apps, change of security settings, allowing only certain websites or apps)	32,6%	41,7%	+9,1%
The internet use time of the child is limited	58,9%	56,5%	-2,5%
Discussions with the child about the dangers in cyberspace and how to behave in online activities	75,5%	73,8%	-1,7%
I would like to help protect them but don't know how	...*	...	...
No restrictions at all on online activities for children	3,7%	5,2%	+1,5%
The child is not allowed to use the computer or smart devices	7,9%	6,5%	-1,4%

Data: "IT in the Household" study by Statistics Estonia;
**... below threshold*

GOING WELL:

In November, the European Union Agency for Cybersecurity ENISA, in cooperation with the e-Governance Academy of Estonia, published a comparative overview of public awareness raising on cyber security in the Member States. Estonia is among the countries that pay attention to both regular reviews and targeted campaign activities. In the autumn, RIA also launched the updated itvaatlik.ee website in Estonian and Russian which gives advice on good cyber security practises for different target audiences.

COULD BE BETTER:

Although there have been no major financial losses in recent months, Estonian companies and individuals are regularly targeted by ransomware attacks. Unfortunately, the trend is clear: ransomware is here to stay and caused incidents with a wide social impact in several countries last year. The initial attack vector for ransomware attacks is often the Remote Desktop Protocol (RDP), which is why CERT-EE recommends reviewing the configuration to avoid unnecessary RDP exposures.

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.