Cyberwatch Finland

WEEKLY REVIEW

WEEK 11/2024

"CYBERSECURITY IS BUILT BY SMALL ACTIONS AND MANAGEMENT OF LARGE CONCEPTS"

Cyberwatch Finland

KEY TAKEAWAYS

1. The Cyber Solidarity Act aims to improve the EU's cyber resilience and cooperation between Member States. It is a continuation of other EU cyber regulation, such as the NIS2 Directive and the Cyber Resilience Act.

2. Successful information management is a resource in organization's cyber security and helps in solving cyber incidents.

3. The recent trend in spam and scam messages has been fast and short-term attack cycles. Meanwhile zip files remain as a popular way to deliver malware to the victim.

1. EU REACHED POLITICAL AGREEMENT ON CYBER SOLIDARITY ACT

The European Union is stepping up cybersecurity regulation with yet another act. The Commission's April 2023 initiative for the Cyber Solidarity Act (CSA) received political approval last week in negotiations between the European Council and the European Parliament. Next, the proposal for a regulation will proceed to formal adoption by the European Parliament and the Council, after which it will enter into force in accordance with the EU regulation process. Acts are binding and must be applied in full and directly in the EU member states. In other words, they differ significantly from directives, where Member States can decide for themselves how to achieve the goal set by the EU. What is the Cyber Solidarity Act about?

According to the European Commission, the regulation aims to improve the EU's cyber resilience. At the same time, it is hoped that it will promote solidarity between member states and the EU's ability to identify, prepare for and respond to cyber threats. In practice, the regulation introduces three new functions for the EU. The first is the European Cybersecurity Alert System. Its task is to detect cyber threats and provide real-time situational awareness to authorities and other relevant actors. The alert system would consist of a network of Security Operations Centres (SOCs) operated by member states to identify and disseminate threat information across borders. Secondly, the regulation establishes a Cybersecurity Emergency Mechanism to improve the ability to respond to major and large-scale cyber incidents. The mechanism consists of three components: preparedness actions in critical sectors, the establishment of a so-called "cybersecurity reserve" and financial support from member states to a state affected by a major or large-scale cyber incident.

Thirdly, the regulation establishes a European Cybersecurity Incident Review Mechanism, which should review and assess cybersecurity incidents and make recommendations based on that to improve cybersecurity in the EU. The European Union Agency for Cybersecurity (ENISA) would play an important role in this, producing a report on what lessons can be learned from the event and what recommendations can be made.

Although the act seems to be more aimed at nation states, it also includes elements concerning private companies. This is the case, for example, with the above-mentioned idea of a “cybersecurity reserve”, where private sector “trusted actors” would be ready to act at the request of a Member State, an EU institution, agency or a partner non-EU country in the event of a large-scale cybersecurity incident. In addition, the preparedness actions mentioned in the emergency mechanism include coordinated testing of the preparedness of entities operating in highly critical sectors. Finland already has good cooperation between authorities and companies, unlike many other EU countries.

The regulation follows other pieces of EU legislation dealing with cybersecurity, such as the NIS2 cybersecurity directive and the Cyber Resilience Act, the latter of which aims to ensure the cybersecurity of digital and related products. For the time being, it is difficult to assess the effectiveness of the Cyber Solidarity Act – the underlying idea of cooperation, solidarity, sharing threat awareness and learning from mistakes is, of course, to be supported. Much will depend on practical implementation and on how cooperation can actually be made to work. From a critical point of view, the option in the emergency mechanism of financial support for a member state in distress is to be noted. One fear may be that the regulation will become one of the means of transferring funds within the Union, where member states that handle their cybersecurity well will have to pay for the mistakes or indifference of the less well-managed member states. This aspect has not been the subject of much debate so far, but as the level of cybersecurity varies widely across member states and as economic issues remain a sensitive political topic within the Union, it is also worth noting.

2. SUCCESSFUL INFORMATION MANAGEMENT HELPS IN CYBER INCIDENTS

Information management means that the information held by an organisation remains secure, in the right place and accessible. It also includes the goal that the organization knows at all times where information and data is stored, and that there are no extra copies or old versions anywhere else than where they should be. In addition to having a significant impact on improving the efficiency of an organization's day-to-day operations, successful information management also plays an important role in the implementation of cyber security. The importance of information management is emphasised especially in the event of the worst, i.e. when an organisation is the victim of a cyberattack, and when investigation on what information the threat actor may have gained access to is ongoing.

One example of the effects of failed information management in a data breach is a Finnish bank that was attacked in late 2023. It took time for the bank to map out all the information the attacker had accessed. When investigating the case, it also turned out that customer data had been processed not only in the customer information system but also in employees' emails. The disclosure of this was also likely to increase the reputational damage caused to the bank by the attack. If, due to inadequate information management, an organization cannot respond quickly enough to whether sensitive information related to customers or partners has ended up in external hands, it is not likely to strengthen the trust of these parties in the organization. At worst, it may lead to accusations that the damage caused by the attack is being covered up. This was the case, for example, with password management company LastPass when it came under attack in 2022. The company took several months to determine what information had been leaked in the attack. When it eventually emerged that customer passwords may have ended up in the hands of threat actors, the company faced accusations of attempted cover-ups and later a lawsuit against it for poor data protection.

Thus, proper information management helps to determine the damage caused by cyberattacks. Information management is also access rights management. When we know which systems and rights the intruders have had access to, we also know what information may have ended up in the attacker's possession. If an organization has accurate information about where and how its data is stored, it is likely to be better protected. The basis for everything is the classification of information into at least three categories: public, confidential and secret. Based on the classification, instructions can be given on the tools by which data may be processed and grant the rights to process the data in each category to a designated group.

In preparing for cyberattacks, information management emphasises that the organisation knows exactly in which environment each data is processed, where it is stored, and when and how it is deleted. However, guidance in this regard alone is not enough, as it must also be ensured that it is implemented. It is important that compliance with the guidelines is adequately monitored, for example through audits. It is equally important that the instructions can be implemented in practice and that employees do not find themselves in situations where the performance of work and information management instructions conflict. This may be the case, for example, when working remotely, people may be tempted to save files from the organization's system environment to their own devices so that they can work even with a poor network connection. Although individual cases do not in themselves pose a problem for information management as a whole, continuous incorrect operating models can cause additional and unnecessary risks.

In Finland, public administration actors are obliged by the Information Management Act, which defines the minimum requirements for data processing and protection. The Act can also be used as a guideline by organisations that are not directly affected by it. However, when reading legal texts, it is good to remember that they usually define the minimum requirements, i.e. the level that must at least be reached. When planning on company's own information management, one should aim higher, as it can not only differentiate from competitors but also help limit damage in the event of a cyberattack.

3. SPAM MESSAGES REMAIN POPULAR

Spam and scam messages are a common everyday nuisance. They make up a significant portion of all sent emails. According to general estimates, they account for between 40% and 50% of all messages sent, although higher estimates have also been made. Scam messages are also sent on social media services, in addition to which scam calls are a notable phenomenon. Although spam and scam messages are often thought of as an obvious and minor security threat, because of their large number, someone always ends up as a victim. At the end of February, technology company IBM published an article about 2023 trends in spam and scam messages. Several cyber security companies have also published their own reports on the subject. Based on reports it seems that scam messages are alive and well.

The aim of spam messages may be, for example, to establish contact with the victim through social engineering and later scam money or online banking credentials. Another goal may be to sneak malware into the victim's or victim organisation's information systems, through which valuable information can be accessed. This can be done, for example, through attachments in an email or by getting the victim to click on links in the email. According to a report by the US cybersecurity company Vipre, 71 percent of cases originate from links, attachments are involved in 22 percent of cases, and the rest involve other forms of attack, such as QR codes. Links often redirects the victim to a malicious website. They can also be located in places and contexts that interest people. These include, for example, advertisements. The aim is to get the victim to enter personal and other information on the site behind the link, which can later be exploited by a malicious actor.

Among the malware delivered with attachments, Vipre highlights the popularity of html files as a form of attack. On the other hand, according to IBM, the most popular method of delivering malware to a victim's computer is a zip compression file. More important than the file format, however, is the awareness that vague attachments or attachments from unknown senders should under no circumstances be opened.

When looking at common trends in spam and scam messages, attention is also drawn to the acceleration of attack cycles. For example, the IBM article highlights a large spike in malware distributed through OneNote files in mid-2023 and a dramatic decline thereafter. Threat actors seem to be more agile than before to exploit vulnerabilities and also quick to change their actions if a certain form of attack loses its effectiveness. One form of attack that has lost its effectiveness is the use of macro files in cyberattacks. A macro is a set of commands that are used to automate a repetitive task, and using macros that come with Excel files, for example, has been a common attack method in the past. According to IBM, the popularity of this method of attack fell by as much as 93 percent in 2023 compared to the previous year.

In the future, the number and quality of spam and scam messages are likely to increase. One of the factors behind this is the development of artificial intelligence. It has been speculated to make scam messages more credible. The development of deep fakes also forces us to think more carefully about the reliability of messages received. There are many ways to protect from spam and scam messages. Organizations can implement technical measures to avoid spam and scam messages. This includes, but is not limited to, enabling spam filters or changing their security level. It would be advisable to neutralize the threat even before it reaches its target. People have traditionally been the weakest link in cybersecurity. In addition to technical measures, general threat awareness, staff training and good general cyber hygiene practices play a key role in preventing and preparing for threats.

REFERENCES

1. EU reached political agreement on Cyber Solidarity Act

https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52023PC0209

https://therecord.media/europe-cyber-solidarity-act-agreement

https://www.consilium.europa.eu/en/press/press-releases/2024/03/06/cyber-solidarity-package-council-and-parliament-strike-deals-to-strengthen-cyber-security-capacities-in-the-eu/

https://www.infosecurity-magazine.com/news/eu-cyber-solidarity-incident/

https://www.tivi.fi/uutiset/tv/d1a95a5a-e33e-40f8-a9b7-551cb045f3ea?ref=newsletter:d2ae&utm_source=Postiviidakko&utm_medium=email&utm_campaign=Tivi_Uutiskirje_ilta

2. Successful information management helps in cyber incidents

https://www.cybersecuritydive.com/news/lastpass-cyberattack-timeline/643958/

https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/

https://betanews.com/2022/12/30/lastpass-accused-of-lying-in-security-breach-announcements/

https://www.cshub.com/attacks/news/iotw-lastpass-facing-class-action-lawsuit-following-data-breach

https://www.hs.fi/kotimaa/art-2000010073301.html

https://yle.fi/a/74-20063927

https://vm.fi/tiedonhallintalaki

3. Spam messages remain popular

https://cybersecurity-magazine.com/phishing-in-2024-heres-what-to-expect/

https://securityintelligence.com/x-force/spam-trends-campaigns-senior-superlatives-2023/

https://vipre.com/resources/email-security-in-2024-an-expert-look-at-email-based-threats/?ref=hackernoon.com

https://www.emailtooltester.com/en/blog/spam-statistics/

Pictures: Pixabay