THE MAIN ASPECTS OF CYBERSECURITY

Qurbonmurodov Diyorbek Ulugbek o'g'li
Tashkent University of Information Technologies
named after Muhammad Al- Khwarizmi, Tashkent, Uzbekistan

Cybersecurity (sometimes called computer security) is a set of methods and practices of protection against malicious attacks for computers, servers, mobile devices, electronic systems, networks and data. Cybersecurity finds application in a variety of fields, from the business sphere to mobile technologies. There are several main categories in this direction.

Network security – actions to protect computer networks from various threats, such as targeted attacks or malware [1].

Application security is the protection of devices from threats that criminals can hide in programs. An infected application can give an attacker access to the data it is supposed to protect. The security of the application is provided at the development stage, long before its appearance in open sources.

Information security – ensuring the integrity and privacy of data both during storage and during transmission.

Operational security – handling and protection of information assets. This category includes, for example, the management of network access permissions or rules that determine where and how data can be stored and transmitted.

Disaster Recovery and business continuity – responding to a security incident (the actions of intruders) and any other event that may disrupt the operation of systems or lead to data loss. Disaster recovery is a set of rules describing how an organization will deal with the consequences of an attack and restore workflows. Business continuity is an action plan in case an organization loses access to certain resources due to an attack by intruders.

Awareness raising– user training. This direction helps to reduce the influence of the most unpredictable factor in the field of cybersecurity – human. Even the most secure system can be attacked due to someone's mistake or ignorance. Therefore, each organization should conduct trainings for employees and tell them about the main rules: for example, that it is not necessary to open suspicious attachments in e-mail or connect questionable USB devices [1].

The scale of the spread of cyber threats

Year after year, there are more and more threats in the world and there are more and more data leaks. The statistics are shocking: according to the RiskBased Security report, 7.9 billion cases of data leakage were recorded in the first nine months of 2019

alone. These figures exceed the figures for the same period in 2018 by more than twice (by 112%).

Most often, medical and government institutions or organizations from the retail sector are exposed to data leakage. In most cases, the reason is the actions of criminals. Some organizations attract intruders for an understandable reason – financial and medical data can be stolen from them. However, any company can become a target, because criminals can hunt for customer data, spy or prepare an attack on one of the customers.

International Data Corporation predicts that if the number of cyber threats continues to grow, the amount of spending on cybersecurity solutions will reach US$ 133.7 billion by 2022. Governments of different countries are fighting criminals, helping organizations to implement effective cybersecurity methods.

Thus, the US National Institute of Standards and Technology (NIST) has developed the principles of secure IT infrastructure. NIST recommends constant monitoring of all electronic resources in real time in order to identify malicious code before it causes harm and prevent its spread [1].

The National Cyber Security Centre of the UK government has released a guide 10 steps to cyber security (10 steps to cybersecurity). It talks about how important it is to monitor the operation of systems. In Australia, recommendations on combating the latest cyber threats are regularly published by the Australian Cyber Security Centre (ACSC).

REFERENCE:

1. Practical Reverse Engineering: x86, x64, ARM, Windows Kernel, Reversing Tools, and Obfuscation, Bruce Dang; 2014