THREATS TO INFORMATION SECURITY AND OPPORTUNITIES TO PREVENT THEM

Rakhmonova Saodat Djurayevna
Teacher of informatics at Angor District Vocational School No. 1
https://doi.org/10.5281/zenodo.10464783

Abstract: In the center of information security is the activity of protecting information - ensuring its confidentiality, availability and integrity, as well as the issue of not allowing any compromise in a critical situation. This article discusses the rapid development of Internet services and its security.

Key words: regulator, cybercriminal, methodology, criminalistics, cyber attack, man-made, Internet products, hacking

Threats to information security can take many forms. The most serious threats for 2018 were "Crime-as-a-Service", Internet products, supply chains and the complexity of regulatory requirements. Crime as a Service is an example of a darknet marketplace for large criminal communities to provide a package of criminal services at low cost to emerging cybercriminals. This enables hacking attacks that were previously unattainable due to high technical complexity or high cost. This makes cybercrime a mass phenomenon. Many organizations are actively implementing Internet products. These devices are often designed without security requirements in mind, creating additional opportunities for cyberattacks. In addition, the rapid development and complexity of Internet services reduces its transparency, which, combined with vaguely defined legal rules and conditions, allows organizations to use the personal data of customers collected by devices at their discretion, without their knowledge. In addition, it is difficult for organizations themselves to monitor which of the data collected by IoT devices is transferred out. The threat to supply chains is that organizations share a variety of valuable and sensitive information with their suppliers, resulting in the loss of direct control over them. Thus, the risk of compromising the confidentiality, integrity or availability of this information is greatly increased. Today's ever-increasing number of new regulatory requirements are making the management of organizations' vital information assets significantly more complex. The process of ensuring information security begins with the assessment of the property, the information assets of the organization, the factors that threaten this information and its vulnerability, and the significance of the overall risk for the organization. Depending on the property, a program will be created to protect these assets. After the risk is identified and quantified, cost-effective countermeasures can be selected to reduce this risk. For example, the General Data Protection Regulation (GDPR), which was adopted in the European Union in 2018, requires any organization to control the content of personal data, its processing methods, storage and requires the indication of the manner of protection and the purposes for which it is served. In addition, this information must be provided not only during the inspection by the competent authorities, but also at the first request of the owner of this information. Maintaining such compliance requires diverting significant budgets and resources from other information security tasks of the organization.

Although simplifying the processing of personal data implies improvement of information security in the long term, the risks of the organization increase significantly in the short term. Information security (English: Information Security, also English: InfoSec) is the practice of preventing unauthorized access, use, disclosure, destruction, modification, research, recording or destruction of information. At the heart of information security is the activity of protecting information - ensuring its confidentiality, availability and integrity, as well as the issue of not allowing any compromise in a critical situation. Such situations include natural, man-made and social disasters, computer failure, physical theft, etc. Although the work processes of most organizations in the world are still based on paper-based documents and require appropriate information security measures, the number of initiatives to introduce digital technologies in enterprises is steadily growing. And this information requires the involvement of information technology (IT) security specialists for protection. These professionals provide information security technology (often a type of computer systems). In this context, a computer refers not only to a household personal computer, but to digital devices of any complexity and purpose, ranging from primitive and isolated ones such as electronic calculators and household appliances to industrial control systems and supercomputers connected via computer networks. Because of the vital importance and value of information to their business, large enterprises and organizations typically hire information security professionals for their employees. Their mission is to protect all technologies from malicious cyber-attacks aimed at stealing sensitive information or controlling internal systems of the organization.

Information security as an employment field has developed and grown significantly in recent years. He has developed many professional specialties including network and related infrastructure security, software and database protection, information systems auditing, business continuity planning, electronic records discovery and computer forensics. Information security specialists have high stable employment and high demand in the labor market. According to extensive research conducted by several organizations (ISC), in 2017, 66% of information security leaders recognized a critical workforce shortage in their departments, and by 2022, there will be a shortage of 1,800,000 professionals worldwide. predicted that it would In order to standardize this activity, scientific and professional communities work on the basis of continuous cooperation aimed at developing basic methodology, policy and network standards in the field of technical information security measures, legal liability, as well as user and administrator training standards. This standardization is largely influenced by a wide range of laws and regulations governing the access, processing, storage and transmission of data. However, if the culture of continuous improvement is not properly formed in the organization, the introduction of any standards and methodologies can have a superficial effect.

In short, it is a multidisciplinary research and professional activity aimed at developing and implementing various security mechanisms (technical, organizational, human-oriented, legal) to protect information from threats, regardless of where it is located (both inside and outside the organization's perimeter). sector and, accordingly, the employees of the sector should create an excellent program on the information systems where information is created, processed, stored, transmitted and destroyed.

References:

Interagency or Internal Report 7298 Glossary of Key Information Security Terms (en). Gaithersburg, MD, USA: Revision 2, 2013.
Aktualnye voprosy nauchnoy i nauchno-pedagogicheskoy deyatelnosti molodyx uchenyx. M.: IIU MGOU, 2016. ISBN 978-5-7017-2532-2.
https://uz.wikipedia.org/wiki/Axborot_xavfseziligi#CITEREFOlavsrud2017