WEB OF SYNERGY:
International Interdisciplinary Research Journal
Volume 2 Issue 12, Year 2023 ISSN: 2835-3013
https://univerpubl.com/index.php/synergy

Cyber Security Threat Management

Maxkamova Shalolaxon Yusufjonovna
Teacher of Dangara multidisciplinary technical school of Fergana region

Article Information

Received: Oct 23, 2023
Accepted: Nov 24, 2023
Published: Dec 25, 2023

Keywords: *information, information security, cybersecurity, cybercrime, privacy, integrity, presence, cyber threats, cyber defense.*

ABSTRACT

This article fully covers the concepts of Information Security, cyber security. Important recommendations are given on how important cybersecurity is for our lives, on how they fight cybercrime.

In the world market, all countries in the 21st century began to move directly from an "Industrial society" to an "informed society". Inevitably, the future of the world economy, along with natural resources (oil, gas, coal, metals, etc.), information factors determine, and in the first development of the information sphere, it becomes important to place forces within the world. In an informed society, information is increasingly becoming a strategic resource. The improvement of information technology is an important factor in the informatization of society. In the modern world, based on technology, security is of the greatest importance. Cyber security and information security are commonly used synonymously in security terminology, causing many misunderstandings among security professionals. So here I want to dispel the misconception between cyber security and information security.

The difference between cyber security and information security.

Cyber security - or computer security-includes a number of practices, processes, and technologies designed to protect devices, networks, programs, and data from attacks and unauthorized access. Cyber security protects not only data, but also resources and technologies related to the storage of this data. Part of cyber security is also engaged in the protection of information and communication technologies, which are called ICT (information and communication technologies) security.

Information security-information that is interpreted in a certain context and has a meaning or a certain meaning, can be defined as information. Information security is concerned with the protection of information and usually focuses on aspects of the confidentiality, integrity and

availability of information. The cyber and Information Security Center defines information security as the process of protecting information, as well as information systems, from unauthorized access, disclosure, hacking, destruction, modification, or use, all to ensure privacy, integrity, and availability. These three terms are defined as follows:

Privacy refers to the maintenance of permitted restrictions on access and disclosure, including means to protect personal privacy as well as proprietary information.

Integrity refers to the protection of information from improper destruction or modification, including ensuring the authenticity and non-rejection of information.

Availability implies reliable and timely use of data, as well as ensuring its use.

However, an alternative definition of cyber security became the basis for the definition of ICT security. According to him, anything that is not protected by ICT security is controlled by cyber security. Thus, information is also present in the cyber sphere, and therefore the part of the cyber sphere with information will also be under Information Security. In conclusion, cybersecurity is the security of anything and everything related to the cyber sphere, and information security is related to information security, regardless of the sphere. Thus, you can conclude that in a certain sense, Information Security is a high set of cybersecurity.

Why is Cyber Security important?

Cybersecurity is now one of the newly introduced concepts, with different definitions given to it. Specifically, the CSEC2017 Joint Task Force source defines cybersecurity as: **cybersecurity** is an area of knowledge based on computations that embodies technology, human, information, and processes in itself to guarantee proper execution of actions in the context in which the disruptors exist. It includes the creation, implementation, analysis and testing of secure computer systems. Cybersecurity is an embodied field of knowledge of education and involves the management of legal aspects, politics, the human factor, ethics and risks.

In contrast, Cisco, a network-based organization, has defined cybersecurity as: cybersecurity – the practice of protecting systems, networks, and applications from digital attacks. These cyberattacks usually aim to manage, exchange or destroy confidential information, extort money from users, disrupt normal performance. Currently, the implementation of effective cybersecurity measures is becoming more complicated from the practical side as a result of an increase in the number and type of devices and the potential of intruders than in humans.

The necessity of the cybersecurity field of knowledge began to emerge from the development of the first mainframe computers. In this case, multi-layer security measures have been implemented to protect these devices and their functions. The increasing need to ensure national security has led to the emergence of complex and technologically complex reliable security measures. Every professional currently in the field of information technology is required to have fundamental knowledge of cyber security.

Recently, many cases such as hacking sites in social networks, distributing viral programs are desperately sucked. Cybercrime has become one of the serious problems in our current era of globalization. Cybercriminals mainly carry out these activities with the aim of earning a modest income.

To protect this information, it is very important to have advanced cyber defense programs and mechanisms, and everyone is interested. Everyone in the community relies on critical infrastructure such as hospitals and other health care facilities, financial services programs, and power plants. We need these to continue our society. On an Individual level, cybersecurity attacks can lead to identity theft and extortion attempts, which can seriously damage an individual's life. We all rely on the security of our data and personal information. For example, when accessing an application or filling out more sensitive information in digital health systems.

If these systems, networks and infrastructures do not have the right protection, our data can fall into the wrong hands. In this sense, we are talking about protection in the form of technology and politics. The same applies to organizations and businesses, governments, the military and other socially critical organizations. They store very large amounts of data in data repositories, computers, and other devices. Most of this information contains sensitive information. The disclosure of this information can be very harmful in many cases - to the confidence of citizens in institutions, business competitiveness, personal reputation and consumer confidence in companies. Privacy is a fundamental human right and is protected by law. Previously, this meant that people had to live their lives within the walls of their homes without government intervention. TODAY, Personal Life means making free choices without being affected, communicating freely and looking for what you like on the Internet. You should do all this without having to face the consequences of your actions that affect your daily life. Although it is a human right, many people do not have information about how to collect, use and share their information on the Internet. In 2018, changes were made to the GDPR (General Data Protection Regulation) in the European Union to strengthen data protection for us individuals. At the same time, important initiatives are carried out every year aimed at raising awareness and knowledge about cyber security. Two such annual events are Cybersecurity Awareness Month and Data Protection day. "Data Protection" Day is an international event held annually on January 28. The purpose of the day is to promote personal immunity and raise awareness for individuals, businesses and consumers. Thus, everyone will learn about how, better protect our personal data in digital space. Cybersecurity Awareness Month (ECSM) is an annual company held by the European Union throughout the month of October. The company promotes cybersecurity among EU citizens and organizations and provides up-to-date information on online security. What is Data Protection Day?

Social networks are one of the places where we leave the most information and information. To show this, a team of researchers from Cambridge and Stanford University looked at how much information they could find about a person only by viewing the likes of that person on Facebook. Based on just 10 likes, researchers have found that they can get to know you better than your colleagues. Based on the 70 likes on Facebook, they can get to know you better than your friends. For this: based on only 300 likes, they can get to know you better than your spouse. In addition, based solely on your public online activities, they could accurately predict whether you are suffering from depression or are taking drugs. This shows how important such an event and companies are. We still need to continue to raise awareness among people about how their information is collected, used and shared. We should also inspire them to take steps to better protect their digital personal data. How can information about employees, customers and other information of enterprises ensure their safety?

Companies have a lot of valuable information, such as business concepts and financial information, as well as information about their customers and employees. Companies must make sure that their and customers ' information is protected and kept in accordance with current regulations. This also applies to the partners and sellers of the company. A security breach in which customer data leaks can lead to financial losses. But this can lead to the loss of customer loyalty, trust and brand reputation. All companies must be transparent about how to collect, use and Share end-user data. They must also introduce security technology, security policies and risk management and cybersecurity, which are important for data protection.

How can I be better at protecting my data as a person?

As a consumer, you are responsible for making conscious decisions when sharing your personal information. All information about you, such as your age and gender, location and shopping history, is of great importance. So are the digital tracks you leave when browsing the internet. This is not only about how you provide information, but also about what you allow companies and applications. This can happen, for example, when downloading an application. Before you

start using the application, you are often required to give its owner access to certain information about you. This can be your microphone, contact list, location, photos, and access to health information. Often times, this information is not very relevant for the app you are downloading, and you may not feel comfortable sharing this information either. Almost everything about you can be viewed as information - so you need to have full control over the information you are constantly sharing. Review the terms of the apps you are downloading and manage your privacy settings. Always keep in mind which information you share and with whom. Cyber security is important because it protects all categories of information from theft and damage. These include classified information, identifiable information (PII), protected health information (PHI), personal information, intellectual property, data, government and industrial information systems. Without a cybersecurity program, your organization will not be able to protect itself from data hacking companies, making it an irresistible target for cybercriminals. Due to Global connectivity and the use of cloud services such as Amazon Web Services to store confidential information and personal information, there is an increasing inherent risk and residual risk. The widespread poor configuration of cloud services associated with increasingly sophisticated cybercriminals means that your organization suffers from a successful cyberattack or is at increased risk of data corruption. Business leaders can no longer rely solely on ready-made cybersecurity solutions such as antivirus software and firewalls, cybercriminals are becoming smarter and their tactics are becoming more resistant to traditional cyberbullying. Cyber threats can come from any level of your organization . Cybersecurity training should be conducted at workplaces to educate employees about common cyber threats such as social engineering fraud, phishing, Pay-Per-View attacks (think WannaCry), and other malware designed to steal intellectual property or personal information. The increase in data corruption means that cybersecurity applies not only to tightly regulated areas such as health care.

Cybersecurity is closely linked to all the technological advances that are taking place in our time, especially. Imagine a country that has no military to protect its resources from other places it controls. Is it true that the country is weak. Would you like to live in such a country?

Even with the technology and the internet that you are using now, every day, so, without cybersecurity, your personal data, Location, Photos, Camera, and much more would not be protected, and as a result, important information about your personal life will be turned into ready-made prey by cybercriminals. Another example is if you have a personal business that relies on computers and data, and you have worked hard to build this company. But in the absence of cybersecurity, your company can get out of business and lose all the money, data and company reputation overnight.

Above, we have given examples of why cyber security is important. But in today's virtual life we can give many examples of this. In general, we can think of cyber security as a military part of the internet.

Do you need to know programming to get into the cybersecurity industry?

It is not necessary to know the science of programming when you are just stepping into the field of cybersecurity. But if you start working hard with this area, you will definitely be required to learn and know programming. Because so, there are complex cybercrime that you must be a professional programmer to combat those cybercrime.

REFERNCES

1. A. U. Anorboyev, “Cybercrime, the problems of combating it and the prospects for ensuring cybersecurity”. Monograph. - T: National Guard Institute. 2020
2. S. K. Ganiyev, S. T. Xudoyqulov, “The basics of cybersecurity”. Tutorial-T: Tashkent 2020
3. N.S. Salayev, R. N. Roziev, “National and international standards for combating

cybercrime", Monograph. – T: TDYU, 20182.

4. www.lex.uz
5. www.iiv.uz