PROTECTION AGAINST DIGITAL ATTACKS IN CYBER SECURITY SYSTEMS

Mahmudova S.
Nakhchivan State University
https://doi.org/10.5281/zenodo.11094873

Abstract
We always feel the need to protect the security of our personal information that belongs to us in the Internet world, as well as our valuable things in real life. There are many ways to ensure this. In our daily lives, we can reduce risks by installing cameras to protect physical objects or by being more careful. As in real life, in the virtual world, both individuals and growing businesses take advantage of technology to protect themselves from internal and external cyber attacks. At such moments, professionals are needed - cyber security specialists

Keywords: information security, cyber security, cyber attacks, network attacks, software attacks, system security.

Due to the significant increase in the use of the Internet and social media, all topics related to information began to be taken more seriously. Specializations, professions, courses, seminars, etc., especially starting with the word Cyber. The Greek word "kubernan" which means "to direct" first entered the English language in 1948 as "cybernetics". In 1958, it was used by Lois Couffignal as "Cyber" to describe the relationship between living things and robots. The word Cyber is also a translated version of the word Cyber into Azerbaijani.[1]

Just as our security is important in real life, security is also important in the virtual world and this is called as Cyber Security. Cyber security generally includes computer security, transaction security, data protection, personal data security, internet network security, and even security of any signal transmitting devices. The reason these topics have branched out and gained importance are the cyber attacks and threats faced. As the number and type of cyber attacks have increased, so have the branches of cyber security. Since the 1980s, concepts such as Cyber Criminals, Ethics in the Cyber World, and Ethical Cyber Piracy have emerged.[3]

Cyber security is the practice of protecting computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. Also known as information technology security or electronic information security. The term is used in a variety of contexts, from business to mobile computing, and can be divided into several general categories.

• Network security is the protection of a computer network from intrusions by targeted attackers or random malicious programs.

• Software security is the protection of software and devices from threats. A compromised application may allow access to protected data. Successful security starts in the design phase, long before any software or device is used.

• Information security protects the integrity and confidentiality of data both stored and transmitted.

• Operations security consists of processes and decisions to manage and protect information assets. The permissions granted to users when accessing a network and the procedures that determine how and where data can be stored or shared are all included in this definition.

• Disaster recovery and business continuity for any organization's cyber security incident. or determine how it responds to any other event that results in the loss of operations or data. A disaster recovery strategy dictates how an organization restores its operations and data to return to the same operational capability as before the incident. Business continuity is a plan that an organization uses when trying to operate without certain funds.

• Education of end users addresses the most unknown factor in cyber security - people - what to do in advance. Anyone can accidentally introduce a virus into a secure system by not following proper security practices. Teaching users how to delete suspicious email attachments, not plugging in unidentified USB drives, and other important lessons is critical to the security of any organization.[2]

Why is cyber security important? The world relies on technology more than ever before. As a result, the creation of digital data has accelerated. Today, businesses and governments store large amounts of such data on computers and transfer it to other computers over networks. Devices and their underlying systems have vulnerabilities that can compromise the health and goals of any organization when exploited. A data breach can have a number of devastating consequences for any enterprise. This can discredit the company by losing the trust of consumers and partners. Losing important data, such as source files or intellectual property, can cost a company a competitive advantage. In addition, data breaches can affect corporate revenues due to non-compliance with data protection regulations. It has been found that the average data breach costs an affected organization $3.6 million. Due to the amount of critical information being leaked in the press, it is imperative that organizations adopt and implement a robust cyber security approach.[4]

Malicious persons who infiltrate information systems, steal data, and conduct cyber attacks on networks are usually called "hackers," "crackers," black hat hackers, or cybercriminals. These people are usually people who can write code to an excellent degree, with reverse engineering skills. An example of this type of person is Kevin Mitnick. He is the only person in the history of

the world who was forbidden to stand near the coffee machine. The reason is that he has the ability to write and use his own codes by "hacking" the coffee machine.

There are many research organizations on cyber threats and threats. These institutions investigate various risks and provide information about which types of attacks are more frequent during the year. Among the types of cyber attacks, money laundering and cybercriminals' attacks to demonstrate their skills are prominent. Cyber security has become extremely important for states and companies due to the significant increases in cyber attacks. Examples of the largest cyber attacks in world history include:

• I Love You - this virus infected 45 million computers globally and caused a total loss of 10 billion dollars.

• Nimda – this worm-type malware caused a total of $3 billion in damage.

• Love Bug – this virus brought down many networks in total and caused 10 billion dollars in damage.

It can be seen from the listed cases that 100% protection from cyber attacks is not possible. In order to ensure cyber security, you need to make constant investments and work with various cyber security experts. [4]

So how do cyber security measures protect users and systems? Primarily, cyber security relies on cryptographic protocols to encrypt emails, files and other important data. This not only protects data in transit, but also protects against loss or theft. In addition, end-user security software scans computers for pieces of malicious code, quarantines the code, and then removes it from the computer. Security programs can even detect and remove malicious code hidden in the Master Boot Record (MBR) that is designed to encrypt or erase data from a computer's hard drive. Electronic security protocols also focus on real-time detection of malware. Many use heuristics and behavioral analysis to control the behavior of a program and its code to protect against viruses or trojans (polymorphic and metamorphic malware) that change their shape each time they are executed. Security software can confine potentially malicious programs to a virtual bucket separate from the user's network to analyze their behavior and learn how to better detect new infections. Security programs are evolving as cybersecurity professionals discover new threats and new ways to combat them.

References:

1. Alizade Matlab Nurush, Bayramov Hafiz Maharram, Mammadov Alovsat Suliddin. Information security. Baku-2016.
2. Cyber security | Arif Hasanov. Baku-2020
3. Alizade-C.Sh.-Aliyev-B.A.-Cyber security. Baku-2019.
4. http://sia.az/az/news/politics/450260-web-cameras-installed-in-nazir-secki-mentegelerin-kiber-tehlukesizlik-teminati-yaradilib