ABOUT THE CONCEPTS OF CYBERSECURITY AND ITS KINDS

Erejepbaev Bekzat Muratbaevich
3rd year student of Tashkent University of Information Technologies, Nukus branch

B. Sh. Aytmuratov,
Scientific Advisor, Deputy Chairman, Deputy Director on Scientific affairs and Innovation of TUIT named after Muhammad-Al Khorezmi, Nukus branch

Annotation
This article provides information about the elements of cybersecurity and its methods of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. The article explains the basics of security, including security principles, critical security controls, and best practices in cybersecurity. Security programs provide a guide for potential malware to analyze user behavior and learn how to better detect new infections.

Keywords: electron, security, protocols, virus, mobile, information, cybersecurity, mail, technology, business, cybercrime, emotet, trojans.

Cybersecurity is the practice of protecting computers, servers, mobile devices, electronic systems, networks and data from malicious attacks. It is also known as information technology security or electronic information security. This term is used in various contexts, from business to mobile computing, and can be divided into several general categories.

Network security is the practice of protecting a computer network from intruders, whether targeted intruders or opportunistic malware.

Application security is aimed at protecting software and devices from threats. Hacked software can provide access to data intended for protection. Successful security begins at the design stage, long before the application or device is launched.

Information security protects the integrity and confidentiality of information, both during storage and transmission. Operational security includes processes and solutions for processing and protecting data assets. The permissions that users have when accessing the network, and the procedures that determine how and where data can be stored or transmitted, fall under this umbrella.

Disaster recovery and business continuity determine how an organization reacts to a cybersecurity event or other event that could result in loss of operations or data. The disaster recovery policy defines how the organization will restore its operations and data so that they can return to their ability to function the same as before the incident. Business continuity is a plan by which an organization retreats, trying to work without certain resources.

End-user training focuses on the most unexpected factor of cybersecurity: people. Anyone can accidentally inject a virus into another protected system if they don't follow the security rules. Teaching users to delete suspicious email attachments, prevent unknown USB drives from connecting, and other important lessons is crucial for the security of any organization.

The scale of cybersecurity. Global cyberattack continues rapidly develop with the number of data breaches increasing every year. The Risk Based Security report showed that in the first nine months of 2019, 7.9 billion terrible records were revealed as a result of data hacking. This figure is more than twice the number of open records for the same period in 2018 (112%). Medical services, retailers and community structures faced the greatest number of violations, while malicious criminals were responsible for the majority of incidents. In the USA, the National Institute of Standards and Technology (NIST) has created a cybersecurity system. In order to help combat the spread of malicious code and detect it at an early stage, the system recommends constant monitoring of all electronic resources in real time. There are three types of threats faced by cybersecurity:

1. **Cybercrimes** involve individuals or groups that target systems to gain financial gain or cause violations.
2. **Cyberattacks** often involve gathering information for political reasons.
3. **Cyberterrorism** is aimed at hacking electronic systems to cause panic or fear. So, how do attackers gain control on computer systems? Some common methods that may pose a threat to cybersecurity:

Malware means a harmful software. One of the most common cyber threats is malware, which is software created by a cybercriminal or hacker to break into or damage a legitimate user's computer. Malware, which is often distributed through an unsolicited email application or a legal download, can be used by cybercriminals for cyberattacks to make money or for political reasons. There are several types of malware, including:

Virus: This is a self-replicating program that attaches to a clean file and spreads throughout the computer system, infecting files with malicious code.

Trojans: A type of malware disguised as legitimate software. Cybercriminals deceive users by uploading Trojans to their computers, where they cause damage or collect data.

Spyware: Software that secretly records what a user is doing so that cybercriminals can use this information. For example, spyware can capture credit card data.

Ransomware: malicious software that blocks files and user data with the threat of deleting them if the fee is not paid.

Adware: Advertising software that can be used to distribute malware.

Botnets: networks of computers infected with malware that cybercriminals use to perform online tasks without the user's permission.

SQL Injection: SQL injection (Structured Language Query) is a type of cyber attack used to control and steal data from a database. Cybercriminals exploit vulnerabilities in data-driven applications to inject malicious code into a database using a malicious SQL statement. This gives them access to confidential information in the database.

Fishing is when cybercriminals target victims with emails that appear to request confidential information from a legitimate company. Fishing attacks are often used to trick people into transmitting credit card information and other personal information.

Bibliogrpahy

1. Akbarov D.Y. Cryptographic methods for ensuring information security and their application. – Tashkent, “O’zbekiston markasi” nashriyot, 2009 - p432
2. Russian – Uzbek Explanatory Dictionary of information security terms. 2nd edition. Under general edit of X.P.Xasanov. Tashkent, 2016 – p 733.
3. D.Y.Akbarov, P.F.Xasanov, X.P.Xasanov, O.P.Axmedova, U.Xolimtayeva. Mathematical foundations of cryptography. Training guide. T: M.Ulug’bek UzNU named after M.Ulugbek, 2018- p144.
4. Rakhimjon, H. (2022). 6 NEW PROGRAMMING LANGUAGES TO LEARN. Academicia Globe: Inderscience Research, 3(04), 126-135.