ENSURING CYBER SECURITY IN INFORMING THE SOCIETY

Rustamov Alisher Bahodirovich

Associate Professor, University of Information Technologies and Management Gmail: arustamov_88@mail.ru

Abstract: *Today, internet technologies have reached a sophisticated level of cybercrime, which seems almost impossible to prevent. Security areas in cyberspace have increased dramatically as the sophistication of cybercrime continues to worry many organizations. While we cannot prevent every incident, we can control how we manage the outcome so that we are prepared and competent in our response process. Every day, people, organizations, and governments not only need to protect their infrastructure, but also require new platforms and intelligence, the latest and most disruptive technologies, and new cyber tools and threats that emerge with each.*

Keywords: *Resources, threats, privacy, integrity, information, vulnerabilities, communication tools, potential, confidentiality*

As demand for digital technology grows, so do security concerns. As information technology becomes more complex, it becomes more difficult to prevent errors and vulnerabilities, creating new opportunities for cybercrime. The ease of cybercrime is possible for those who take security measures by using sophisticated technology, building on secure operating systems, and installing hardware devices designed to protect their computer systems. However, organizations are more at risk of facing cyber terrorism than individuals. Cyber criminals are not chosen; where there is a weakness, they try to exploit it. Therefore, all organizations need to understand and protect against the cyber threats they face. While cyber warfare and cyber warfare threaten national security and the economy, organizations and individuals are placing great importance on developing cyber security.

Cybersecurity refers to protecting everything accessible from the internet; These include computers, networks, personal devices, personal data, privacy, smartphones and people. Policy makers at the national level have a responsibility to bear the brunt of the risk in responding to cyber threats at the expense of protecting privacy. In this view, a cybersecurity policy can enable what he describes as "securing cyberspace." This is not to say that cybersecurity efforts should not limit surveillance to the detriment of individual privacy or other democratic values. Necessary checks and controls should be established to reflect community-approved privacy standards. Cybersecurity issues are no longer limited to computer systems such as desktop computers and laptops. Rather, they appear everywhere, from electricity and water systems to healthcare, from public transport to smart cars, from implants to supply chains, from banking and logistics to emergency services. There is no perfect solution to cybercrimes, but we must try to minimize them to have a safe and secure future in cyberspace. By applying the best cybersecurity strategy to such processes, a strong security infrastructure includes multiple layers of protection spread across a company's computers, software, and networks. Cyber security tools and professionals act as the last line of defense between our most important data and digital chaos.

Networking organized through the Internet can be divided into the following classes**:**

– packet sniffer (sniffer - meaning filtering) - an application program that works in promiscuous mode using a network card (indiscriminately sends all information packets sent through a physical channel to a special program for processing);

– IP-spoofing (spoof - deception, mystification) - when a hacker pretends to be an expert authorized to access the network from within the corporation where the network is located or from outside it;

– denial of service (Denial of Service - DoS). Access of authorized users to the network system is restricted as a result of violation of network functions or operating system organizers or related programs through DoS network;

– actions aimed at passwords - actions aimed at obtaining the password information specified for accessing the network by an authorized user;

– events organized during the program operation;

– network espionage (reconnaissance) - collection of information on network operation based on relevant data and programs;

– by gaining trust within the network, abusing it;

– network attacks organized for unauthorized access;

– virus and trojan program attacks.

Given the above attack types, a cyber security risk assessment identifies the information assets that could be affected by a cyber attack (eg hardware, systems, laptops, customer data and intellectual property). It then identifies the risks that may affect these assets.

Basic steps in threat assessment:

– Defining the scope of threat assessment.

– Identify vulnerabilities that could lead to threats.

– Assign any threat analysis and rating.

– Determination of measures according to the results of the threat analysis.

Digital technologies contribute to the cybersecurity process in development in the following ways:

– Raising awareness: Mentoring raises awareness of the importance of cybersecurity in digital transformation projects and educates stakeholders on protecting digital assets

– Providing guidance: Mentors provide guidance on cybersecurity best practices and help organisations take a proactive approach to security rather than reacting to threats

– Sharing experiences: Mentors can share their experience of implementing cybersecurity measures in similar projects and provide insight on common pitfalls and effective strategies

– Identifying and mitigating risks: Mentors can help organisations to identify and mitigate cybersecurity risks and help them implement tailored security measures

In conclusion, mentoring is a crucial step in ensuring the success and security of digital transformation. By sharing experiences, providing guidance, and raising awareness, mentoring can equip organisations with the knowledge and tools necessary to protect their digital assets and data, build a culture of organisational resilience, and embrace the future of cyber security with confidence.

REFERENCES:

1. Cybersecurity Curricula 2017 – Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8) (Crosscutting concepts).
2. M.Stamp. Information security. Principles and Practice. Second Edition. ISBN 978-0-470-62639-9. 2011.
3. CISSP Official Study Guide (Mike Chapple, James Michael Stewart, Darril Gibson) (2018, Sybex)
4. Official ISC2 Guide to the CSSLP CBK
5. Sitorabonu , A. Va Gulmira, P. (2024). KAPARATIV TARMOQLARDA AXBOROT XAVFSIZLIGINI TA'MINLASHDA YANGI TEXNOLOGIYALARNING ROLI. Efiopiya xalqaro multidisipliner tadqiqotlar jurnali, 11(06), 169-171.
6. Qodirov, B. K. (2022). Kredit-modul tizimida ma'lumotlar bazasi fanini o'rganishda muammolarning istiqbollari va ularning echimlari. Xalqaro rasmiy ta'lim jurnali, 2(1), 16-22.
7. Rustamov, A., & Amirov, A. (2022). TARMOQLARDA AUTENTIFIKASIYA PROTOKOLLARIGA QO’LLANILADIGAN NAMUNAVIY HUJUM TURLARI. Прикладные науки в современном мире: проблемы и решения, 1(31), 12-14.
8. Rustamov, A., & Amirov, A. (2022). TARMOQLARDA RANSOMWARENI OLDINI OLISHDA VEB XAVFSIZLIKNING MUHIMLIGI. Прикладные науки в современном мире: проблемы и решения, 1(31), 15-18.
9. Shukrullaevna, N. D., & Bahodirivich, R. A. (2017). MOOC bilan liniyada o'qitish jarayonining sifatini oshirish. Akademiya, 2(6 (21)), 21-24.