ETHICAL CYBERSECURITY PRACTICES IN NETWORK TECHNOLOGIES

Abdullajonov Davronjon
Teacher of the department of Kokan University,
Usmanov Husanboy
Kokan University KI-1-22 group, student,

Annotation: This article discusses the application of ethical Cyber Security in network technologies and cyber threats and their types and locations in the system.

Cybersecurity: Cybersecurity is a set of practices, technologies, and processes aimed at protecting computer systems, networks, and data from cyber threats and unauthorized access. Cyber Security includes measures to ensure the confidentiality, integrity and availability of data.

Keywords: ethics, Cyber Security, hacker, phishing, malware, DDos attacks, hacks, injections, Ed ids/ips, siem, mfa, vpn

Introduction:

Introduction to Ethics and Cybersecurity

Hacking: Hacking is the process of accessing, analyzing and attempting to modify computer systems and networks. Hackers can work for a variety of purposes, including security testing, security enhancements, and malicious activities such as unauthorized access to data and attacks on systems.

Legal Compliance: Ethics helps cybersecurity professionals comply with laws and regulations related to the use of information systems and data.

Trust and reputation: Being ethical helps build trust between users and customers, which is critical for organizations and cybersecurity professionals.

Professional Responsibility: Adherence to ethical standards and regulations demonstrates the professional responsibility and competence of cybersecurity professionals.

In general, ethics is an integral part of Cyber Security, emphasizing the importance of following rules and standards when dealing with computer systems and data. Types of Hacking and Cyber Threats

Main part:

Importance of ethics and rules in Cyber Security:

Privacy Protection: Cybersecurity ethics help protect personal data and privacy, which is especially important in today's world where large amounts of personal data are stored and transmitted digitally.

Preventing Cyber Attacks: Ethics educates both conscientious cybersecurity professionals and users to follow best practices for preventing cyber-attacks and unauthorized access.

There are different types of hacking attacks, each aimed at achieving specific goals. Some of the more common types are:

Buffer overflow: Buffer overflow attacks occur when an attacker loads more data into the buffer than it can hold, which can cause the program to crash or even execute malicious code. Ethical Hacking and Unethical Hacking difference between practices:

Ethical Hacking: Ethical hackers, also known as white hat hackers or vulnerability researchers, have the authority to test and assess the security of systems or networks with the consent of the owners. Their goal is to identify vulnerabilities and improve overall security.

Education and Training of Cyber Professionals: Ethical education and training of cyber professionals will become an integral part of their professional development. This includes understanding the consequences of one's actions, as well as the principles of using one's skills responsibly.

International Cooperation on Cyber Security: Given that cyber threats transcend borders; ethics calls for increased international cooperation. A concerted effort to share information and develop common standards can strengthen cybersecurity globally.

How ethical hacking is changing cybersecurity

The rise of cybercrime in recent years has increased the importance for businesses and organizations to take measures to protect their networks from attackers. As a result, the practice of ethical hacking has become popular. Ethical hacking involves using the same methods and techniques as attackers, but the goal is to identify and eliminate potential security vulnerabilities.

Ethical hacking is one of the most effective ways to assess potential security vulnerabilities and identify potential solutions to improve network security. By using the same tactics as malicious hackers, ethical hackers can discover vulnerabilities that would otherwise go undetected. In addition, ethical hacking can provide valuable information about the behavior of attackers. By studying the tactics used by hackers, organizations can better understand their potential threats and develop strategies to prevent and respond to cyberattacks.

The practice of ethical hacking is becoming increasingly important in the world of Cyber Security. This allows organizations to better protect their networks and stay ahead of attackers. As the threat of cybercrime continues to grow, ethical hacking can become an important tool for organizations seeking to keep their networks secure.

Ethical Hacking and Cyber Security Challenges The digital age has created a number of challenges in the areas of ethical hacking and Cyber Security. With the rise of malicious cyber-attacks, organizations are under increasing pressure to protect their data and systems from potential breaches. Ethical hacking and Cyber Security is a complex but important field. As the digital age continues to evolve, ethical hackers and Cyber Security professionals will be needed to protect systems and data from attackers.

Network security

Network security protects your network data from security breaches that could lead to data loss, sabotage, or illegal use. The goals of the system are to ensure the security of the stored data and to ensure that network users have constant access to this data. Network security solutions also help organizations provide information, services and products to their customers in a safe and secure manner.

An organization must implement network security as an important component to protect its interests and operate effectively.

Today, the financial success of an organization is not only based on sophisticated marketing methods and revenue streams. Businesses are increasingly relying on the Internet for fast communication and lightning-fast transactions.

Network security in Cyber Security.

To highlight this, network security is a branch of Cyber Security that focuses on protecting computer networks from cyber-attacks. Network security has three primary goals: preventing unauthorized access to network resources, detecting and stopping ongoing cyber-attacks and security breaches, and ensuring that authorized users have secure access to network resources when needed.

The risk of cyber-attacks increases as networks grow in size and complexity. According to IBM's Cost of Data Breach 2022 report, 83 percent of surveyed firms have experienced multiple data breaches. These attacks were costly. The average cost of a data breach worldwide is $4.35 million, while the average cost of a data breach in the US is more than double that at $9.44 million.

Network security device

In addition to the many network devices that every organization should have, a variety of network security tools and devices can help protect your network.

Malware
MALWARE
Man In the Middle
Phishing
Drive-By Downloads
Password Attacks
Malvertising
DDoS
Rogue Software

While most security solutions are proprietary, there are some open source options. Below is a list of the most common types of network security devices that can help protect your network from the ever-changing threat landscape.

Firewall

A firewall is an important security measure for medium and large businesses. A perimeter firewall protects the network from the Internet and is well known to many. A firewall can be a standalone system or embedded in other devices such as routers or servers. Some firewalls, available in hardware and software formats, are specifically designed as devices to separate two networks.

Their main task is to filter incoming network traffic and prevent access to organization systems. Firewall behavior is controlled by policies, which take one of two forms.

Allow list: Only traffic marked as safe is allowed and all other traffic is denied.

Blacklist: All movement is permitted unless otherwise noted as dangerous.

Proxy server

Proxies work between remote users and servers at the application layer of the OSI model. They hide the identity of both parties, ensuring that each party recognizes only the trusted party. This configuration provides strong security between public and private networks. Proxies can effectively protect sensitive applications by operating at the application layer. They support advanced authentication methods such as passwords and fingerprints for enhanced security.

Network access control

As businesses embrace Bring Your Own Device (BYOD) policies, it's critical to have a solution that provides the visibility, access control, and compliance you need to strengthen your network security infrastructure.

Network Access Control (NAC) is a network solution that restricts access to network resources and infrastructure to only compliant, authenticated, and trusted endpoint devices.

Application security

The process of creating, adding, and testing security controls in software to prevent security vulnerabilities from threats such as unauthorized access and modification is known as software security.

The Vera code State of Software Security study found that 83 percent of the 85,000 applications evaluated had at least one security issue. Many had a lot, because their analysis revealed ten million problems, XNUMX% of all applications have at least one critical flaw. Organizations should regularly conduct application security testing to identify and resolve code issues.

Cyber attackers lose the ability to compromise or exploit critical web applications.

Administration of weakness

Vulnerability management is the continuous process of finding, prioritizing, fixing, and reporting system security flaws.

Network assets are discovered, classified and reported to address security vulnerabilities in target systems.

Vulnerability management is critical today because attackers are constantly searching the Internet for vulnerabilities and exploiting previously unpatched vulnerabilities in corporate systems.

Network access test

Network penetration testing is an attempt to analyze and evaluate the security of IT infrastructure by safely exploiting vulnerabilities.

These failures can occur in operating systems, services and applications, firewall misconfigurations, or unsafe end-user behavior.

One of the biggest reasons why penetration testing is important to a company's cybersecurity program is to teach employees how to combat hostile cyberattacks.

Penetration testing can also determine whether a company's security policies are working and whether they are effective in preventing attacks.

Antivirus protection

Antivirus software prevents, detects and removes viruses from your computer.

Most antivirus programs run automatically in the background after installation and provide real-time protection against virus threats.

Many new viruses are discovered regularly; Therefore, in order to stay ahead of the mass of dangerous codes that are widespread on the Internet, it is necessary to install an antivirus program and configure it to automatically update the latest detection files.

Today, malware authors are well versed in exploiting holes in computer systems.

Antivirus software can be used as a first line of defense to prevent viruses from damaging computer systems.

Endpoint Detection and Response (EDR)

Endpoint detection and response technology is a solution that continuously monitors endpoint system activity and events.

In addition, EDR gives security professionals the visibility they need to detect undetected events.

EDR is useful because it shows how an attacker got into the system and what they did inside it.

EDR can detect malicious endpoint behavior caused by zero-day exploits, complex, persistent threats, and fileless or malware attacks that leave no signature, and thus avoid legacy antivirus.

Network security key

The network security key is your password to access the Wi-Fi network. Connects the router to devices connected to the Wi-Fi network. A network security key protects your Wi-Fi network and its users from attackers trying to use your connection.

Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), Wi-Fi Protected Access 2 (WPA2), and Wi-Fi Protected Access 3 (WPA3) are some of the network security switches used in most Wi-Fi networks. There are four types. networks - Fi. networks.

What is network security?

Network security includes everything you do to keep your network and data safe and secure. It includes both hardware and software. It pursues many types of threats. They cannot network or spread. Good network security controls network access.

How does network security work?

Network security includes multiple layers of protection at the network edge and within the network. Policies and controls are activated at each level of network security. Authorized users can access network resources, but attackers cannot perform attacks or threats.

The four basic principles of security are access, authentication, authorization, and accounting. Use physical and software security measures to prevent unauthorized access to your device or data. Hardware access restrictions usually refer to physical access restrictions. Access restrictions in software generally apply to both physical and virtual modes.

Summary: In this article, we have considered Cyber Security and network technologies, hackers and cyber attacks

In general, ethics is an integral part of Cyber Security and emphasizes the importance of compliance. It helps protect personal information, prevent cyber-attacks, comply with legal requirements, build trust and reputation, and demonstrate professional responsibility.

In Cyber Security, there are several types of hacking and cyber threats such as phishing attacks, denial of service (DDoS) attacks, malware, injection attacks, and buffer overflows. Each of them is aimed at achieving specific goals and poses a threat to information systems and data.

The difference between ethical hacking and unethical practices is legality, consent, and intent. Ethical hacking is done with consent and within the law to improve overall security, while unethical hacking is illegal and ethically unacceptable.

References:

1. Iqboljon, X. (2023). MATEMATIKA FANIDA FUNKSIYALARNI SAMARALI O ‘QITISH ISTIQBOLLARI. International Multidisciplinary Journal of Universal Scientific Prospectives, 1(2), 64-69.
2. Ilyosjon o'g'li, X. I. (2023). THE IMPORTANCE OF CREDIT IN THE MARKET ECONOMY. Open Access Repository, 9(6), 265-267.
3. Ilyosjon o'g'li, X. I. (2023). CREDIT COUNT METHODS. Open Access Repository, 9(6), 271-273.
4. Ilyosjon o'g'li, I. X. (2023, May). TENGLAMALAR SISTEMASI. In Proceedings of Scientific Conference on Multidisciplinary Studies (Vol. 2, No. 5, pp. 49-52).
5. Ilyosjon o'g'li, X. I. (2023). KREDITNING BOZOR IQTISODIYOTDAGI AHAMIYATI. In Proceedings of International Conference on Educational Discoveries and Humanities (Vol. 2, No. 1, pp. 33-39).
6. Iqboljon, X. (2024). SYSTEM OF LINEAR ALGEBRAIC EQUATIONS AND METHODS OF THEIR SOLUTION. Multidisciplinary Journal of Science and Technology, 4(1), 39-44.
7. Meliboev A, Alikhanov J, Kim W. Performance Evaluation of Deep Learning Based Network Intrusion Detection System across Multiple Balanced and Imbalanced Datasets. Electronics. 2022; 11(4):515. https://doi.org/10.3390/electronics11040515
8. Davronjon, A., & Gulmiraxon, K. (2022). WIDESPREAD INTRODUCTION OF DIGITAL TECHNOLOGIES IN THE REAL SECTOR OF THE ECONOMY, AS WELL AS IN AGRICULTURE AND WATER MANAGEMENT. World Economics and Finance Bulletin, 9, 167-172.
9. Abdullajonov, D. S. O., & Kasimova, G. K. Q. (2022). DEVELOP A TRAINING PROGRAM FOR YOUNG PROFESSIONALS IN EDUCATIONAL INSTITUTIONS, WHICH IS THE CORE OF CYBERSECURITY. Academic research in educational sciences, 3(6), 185-192.

10. Shokirjon oʻgʻli, A. D. (2023). AXBOROT TEXNOLOGIYALARI SOHASIDA ILMIY IZLANISHLAR OLIB BORISH TENDENSIYALARI. QO ‘QON UNIVERSITETI XABARNOMASI, 1223-1227.

11. Otto, M., & Thornton, J. (2023). JAHON IQTISODIYOTI VA XALQARO MUNOSABATLAR. QO ‘QON UNIVERSITETI XABARNOMASI, 216-219.

12. Abdullajonov, D., & Qosimova, G. (2022). OZBEKISTONDA KIBERXAVSIZLIK VA RAQAMLI IQTISODIYOT RIVOJLANISHINING AXBOROT JAMIYATI SHAKLLANISHIDAGI ORNI. Евразийский журнал математической теории и компьютерных наук, 2(13), 29-37.

13. Shokirjon oʻgʻli, A. D., & Solijon oʻgʻli, T. U. (2022). The Application of Digital Technologies to Enterprises and Organizations Will Help Reduce Social and Economic Costs. Eurasian Journal of Learning and Academic Teaching, 4, 131-140.