SUSHANT UNIVERSITY ORGANIZED INTERNATIONAL CONFERENCE ON
"ADVANCES IN MULTIDISCIPLINARY RESEARCH AND INNVOATION" ICAMRI-2023
ON 28-29TH OCTOBER 2023
INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

Securing Digital Landscapes: Understanding Information Security Threats, the OSI Model, and Cyber Ethics

Neha Gupta, B.Tech Student – CSE, School of Engineering and Technology (SET), Sushant University, Gurugram, India
Aditya Minz, B.Tech Student – CSE, School of Engineering and Technology (SET), Sushant University, Gurugram, India
Yuvraj Gupta, B.Tech Student – CSE, School of Engineering and Technology (SET), Sushant University, Gurugram, India
Garv Lal, B.Tech Student – CSE, School of Engineering and Technology (SET), Sushant University, Gurugram, India

Abstract

This review paper explores the world of threats, vulnerabilities, and risk assessment in the context of organizational security. It highlights the importance of identifying and analyzing threats to effectively allocate resources and develop risk mitigation strategies. The paper also delves into the OSI model, providing insights into the vulnerabilities present at each layer and proposing corresponding solutions. Additionally, the concept of cyber ethics is discussed, emphasizing responsible online behavior and the promotion of a positive digital environment.By examining these key areas, organizations and individuals can enhance their understanding of security and ethics in the digital landscape.

Keywords - Threats, risk assessment, unintentional threats, intentional threats, internal attacks, external attacks, malware, Trojans, viruses, ransomware, worms, rootkits, botnets, vulnerabilities, cyber ethics, communication, OSI Model, cyberbullying, unauthorized access, personal information protection, authenticity, copyright compliance.

I. Introduction

In today's digital landscape, organizations face a myriad of threats that can disrupt their operations and compromise their assets. It is crucial for organizations to identify and analyze these threats to allocate resources effectively and develop appropriate risk mitigation strategies.This review paper aims to provide a comprehensive understanding of threats, threat vectors, vulnerabilities, the OSI model, and cyber ethics to assist organizations in safeguarding their assets and promoting responsible behavior in the digital realm. By exploring the different types of threats and their corresponding preventive measures, organizations can enhance their preparedness and resilience. Furthermore, understanding the various threat vectors and vulnerabilities helps organizations identify potential points of exploitation and implement effective security measures. The paper also delves into the OSI model, highlighting the vulnerabilities associated with each layer, which aids in comprehending the intricacies of network security. Lastly, the concept of cyber ethics is introduced, emphasizing the importance of responsible behavior, privacy protection, and compliance with ethical guidelines to foster a positive online environment.

II. Information Security Threats And Vulnerabilities

Threat: A threat is the potential occurrence of an undesirable event that can eventually disrupt and damage the operational & functional activities of an organization.Organizations must prioritize threat identification and analysis to effectively allocate resources and develop appropriate risk mitigation strategies.This involves conducting comprehensive risk assessments to identify potential threats specific to the organization's industry, location, and operational scope[1,2,4,6,7].The types include the following :-

- Natural - Natural threats are environmental events like earthquakes, floods, and storms that occur naturally and can damage infrastructure, disrupt operations, and jeopardize the safety of personnel. Organizations must have contingency plans and preventive measures in place to minimize the impact of natural threats and ensure the continuity of their business activities.

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

- Unintentional - Unintentional threats are risks caused by human actions or errors that are not intentional or malicious. They result from negligence, lack of awareness, or inadequate training. Examples include accidental data breaches, introduction of malware through email mishaps, or operational disruptions due to human errors. Organizations can mitigate unintentional threats through training, promoting security awareness, and implementing protocols to minimize human-related incidents.
- Intentional - Intentional threats can encompass a range of actions that are carried out with the deliberate intent to harm an organization, excluding cyber attacks. Here are two types of intentional threats:
- Internal - Internal intentional attacks, also known as insider threats, occur when individuals within an organization purposely engage in harmful activities or misuse their access privileges for personal gain, revenge, or other malicious purposes.
- External - External intentional attacks refer to deliberate actions targeted at an organization by individuals or groups from outside the organization. These attacks are typically driven by malicious intent and can have various objectives, including financial gain, disruption of operations, or damage to the organization's reputation.

2.1 What are Threat Vectors & Types of Threat vectors

Threat Vectors : It's a medium through which an attacker gains access to a System on exploiting identified vulnerabilities.

- ➔ Malware (Malicious Software) - Damages or disables computer systems & gives limited or full access of the system to the attacker.These vectors can be diverse and can encompass various methods or channels through which attacks can occur
- ➔ Trojan (or Trojan Horse) - is a type of malware that appears harmless or legitimate on the surface but contains malicious code hidden within. The name "Trojan horse" is derived from the Greek myth where a giant wooden horse was used to conceal soldiers who then attacked from within. Similarly, a Trojan operates by deceiving users into believing it is a legitimate program or file while carrying out malicious activities in the background.
- ➔ Virus - A virus is a malicious software that can self-replicate and spread by attaching itself to other files or programs. It requires an executable file or program to activate its replication process. Once executed, the virus can infect other files or systems, causing damage, stealing information, or disrupting operations. Effective antivirus measures and user education are essential to prevent virus infections and mitigate their impact.
- ➔ Ransomware - Ransomware is a form of malware used by cybercriminals to encrypt data and demand a ransom for its release. Attackers exploit vulnerabilities or trick users into downloading infected files, making it a lucrative money-making scheme. Organizations must implement strong cybersecurity measures, regular backups, and educate employees to mitigate the financial and operational impact of ransomware attacks.
- ➔ Worms - Worms are self-replicating malware that spread automatically across networks. They exploit vulnerabilities to move from one system to another without user interaction. Worms can cause widespread damage, disrupt network operations, and lead to data breaches. To protect against worms, organizations should maintain updated security measures, such as patching and strong firewalls, while users should exercise caution to prevent infections.
- ➔ Rootkits - Rootkits are malicious software that hide within active processes, often at the kernel or system file level. They evade detection by concealing themselves and can persistently control a compromised system. They exploit vulnerabilities to install themselves and can intercept system calls and modify files. Detecting and removing rootkits require specialized tools, and protection involves maintaining updated systems,

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

strong access controls, and behavior-based security solutions. Monitoring system logs and network traffic is essential for early detection and response.

➔ Botnets - Botnets are networks of infected computers controlled by an attacker. They exploit vulnerabilities to infect machines, creating a network of bots. These botnets can be used for various malicious activities like DDoS attacks, spam distribution, and data theft. To counter botnets, keep systems updated, use reliable antivirus software, and practice safe browsing. Network monitoring and collaboration with security organizations are essential in fighting botnet threats.

➔ Fileless Malware - Fileless malware is a type of malicious software that injects its code directly into the memory of running applications, bypassing traditional file-based detection. It doesn't leave traces on the computer's file system, making it difficult to detect and remove. By residing in the RAM, it can persist even after system reboots, posing a significant threat to cybersecurity. Advanced detection and prevention techniques are necessary to effectively defend against fileless malware attacks.

➔ Vulnerability - A vulnerability is a weakness or flaw in an asset, such as software or hardware, that can be exploited by threat agents. It can result from programming errors, design flaws, or misconfigurations. Vulnerabilities need to be identified and addressed through measures like patching, updates, and security audits to reduce the risk of exploitation and enhance overall security. These include the following :-

- Software Vulnerability: Buffer Overflow Vulnerability - A programming error that occurs when a program stores more data in a buffer than it can handle, leading to memory corruption. Attackers exploit this to execute malicious code or gain unauthorized access.
- Hardware Vulnerability: Spectre and Meltdown - Flaws in modern processors that allow attackers to access sensitive data by exploiting speculative execution.
- Misconfiguration Vulnerability: Weak Passwords - Using easily guessable passwords creates a vulnerability, enabling attackers to gain unauthorized access through brute-force or password-cracking techniques.

2.2 The Formula of "Risk = Asset + Threat + Vulnerability"

In risk assessment, the formula "Risk = Asset + Threat + Vulnerability" captures the key factors involved. Assets are valuable resources within an organization, including physical and intangible elements. Threats encompass potential events that can harm the organization, originating from natural disasters, cyber attacks, human error, or malicious actions. Vulnerabilities represent weaknesses in systems or controls that could be exploited by threats. By understanding and addressing these components, organizations can better manage and mitigate risks to their assets.[1,2,4,7,9,10]

★ Asset: Assets are valuable resources within an organization, including physical and intangible elements like infrastructure, data, and reputation. They are vulnerable to compromise, damage, or loss, making their protection essential in risk management.

★ Threat: Threats are potential events that can cause harm or disruption to an organization. They can originate from natural disasters, cyber attacks, human mistakes, or intentional malicious actions. Threats pose risks to an organization's assets, including physical resources, data, intellectual property, and reputation. Understanding and addressing threats is essential for effective risk management and safeguarding the organization's well-being.

★ Vulnerability: Vulnerability refers to weaknesses in an organization's systems, processes, or controls that can be exploited by threats. These weaknesses can be technical (outdated software, misconfigured systems) or human-related (lack of training, poor security practices). Vulnerabilities increase the likelihood and impact of threats causing harm to the organization's assets. Addressing vulnerabilities is essential to minimize risk and protect valuable assets.

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

III. OSI Model

The OSI model is a conceptual model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer. It consists of seven layers, and each layer performs a particular network function. The OSI model was developed by the International Organization for Standardization (ISO)in 1984, and it is now considered as an architectural model for intercomputer communications[3,5,7,8,9].The seven network functions are :-

- Physical layer: This is the lowest layer of the OSI model and is responsible for transmitting individual bits from one node to another node. It defines the physical characteristics of the network, such as the cables, connectors, voltages, frequencies, etc. It also defines the line configuration, data transmission mode, topology, and signals.
- Data link layer: This layer is responsible for the error free transfer of data frames from one node to another. It defines the format of the data on the network and provides reliable and efficient communication between two or more devices. It also handles the addressing, flow control, error control, and media access control.
- Network layer: This layer is responsible for routing packets from one network to another. It defines the logical addressing scheme, such as IP addresses, and determines the best path for data transfer. It also handles congestion control, fragmentation, reassembly, and network security.
- Transport layer: This layer is responsible for end to end delivery of data segments from one process to another. It defines the service type, such as connection oriented or connectionless, and provides reliable and efficient data transfer. It also handles segmentation, reassembly, flow control, error control, and multiplexing.
- Session layer: This layer is responsible for establishing, maintaining, and terminating sessions between two or more applications. It defines the rules and procedures for communication, such as synchronization, dialog control, authentication, etc. It also handles session recovery and session security
- Presentation layer: This layer is responsible for translating data between different formats and encoding schemes. It defines the syntax and semantics of the data exchanged between applications. It also handles data compression, encryption, decryption, etc.
- Application layer: This is the highest layer of the OSI model and is responsible for providing services to user applications. It defines the protocols and interfaces for communication, such as HTTP, FTP, SMTP, etc. It also handles user authentication, file transfer, email, web browsing, etc.

3.1 Each layer of the OSI model has different vulnerabilities while a normal person is using the network[2,4,5,6]. Here are some examples of possible threats and solutions for each layer:

- Physical layer: This layer can be vulnerable to unauthorized access, damage, environmental issues, or disconnection of physical links. To prevent these threats, physical security measures such as locks, alarms, firewalls, backup power, etc. should be implemented
- Data link layer: This layer can be vulnerable to ARP spoofing, MAC flooding, VLAN hopping, or STP attacks. To prevent these threats, switch security measures such as port security, MAC filtering, private VLANs, DHCP snooping, etc. should be implemented
- Network layer: This layer can be vulnerable to IP spoofing, ICMP attacks, routing attacks, or DoS attacks. To prevent these threats, network security measures such as IPsec, firewalls, IDS/IPS, routing protocols authentication, etc. should be implemented
- Transport layer: This layer can be vulnerable to TCP hijacking, SYN flooding, port scanning, or session hijacking. To prevent these threats, transport security measures such as SSL/TLS, encryption, authentication, firewall rules, etc. should be implemented

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

- Session layer: This layer can be vulnerable to session fixation, session replay, or session termination attacks. To prevent these threats, session security measures such as cookie management, session tokens, session timeouts, etc. should be implemented

- Presentation layer: This layer can be vulnerable to data manipulation, data encryption attacks, or data compression attacks. To prevent these threats, presentation security measures such as data integrity checks, encryption algorithms, compression algorithms, etc. should be implemented.
- Application layer: This layer can be vulnerable to SQL injection, XSS, CSRF, phishing, malware, or logic bombs. To prevent these threats, application security measures such as input validation, output encoding, secure coding practices, antivirus software, etc. should be implemented.

IV. Cyber Ethics

Cyber ethics encompasses the principles and guidelines that dictate ethical behavior in the digital realm. By adhering to cyber ethics, individuals ensure the responsible and safe utilization of the internet[3,6,9,10].This paper reviews various aspects of cyber ethics and emphasizes their importance in promoting a positive online environment.These include the following :-

- Communication and Interaction: Responsible communication is the foundation of healthy online interactions. Individuals should engage in respectful and constructive conversations, fostering cultural exchange and collaboration. Through email and instant messaging, people can connect with others across geographical boundaries, enhancing global connectivity.
- Avoid Cyberbullying: Cyberbullying poses a significant threat to individuals' psychological and emotional well-being. It is essential to refrain from using derogatory language, spreading false information, or sharing embarrassing content with the intent to harm others. Cultivating a safe and respectful online environment is crucial in preventing cyberbullying incidents.
- Responsible Information Use: The internet serves as a vast source of information, and individuals must use it responsibly and legally. Proper citation and referencing of sources are essential to respect copyright laws and intellectual property rights. By acknowledging the efforts and creativity of content creators, individuals contribute to a fair and ethical digital ecosystem.
- Unauthorized Access: Respecting others' privacy and security is paramount in cyber ethics. Unauthorized access to someone else's accounts violates their trust and breaches ethical boundaries. Upholding ethical standards requires refraining from engaging in such activities, fostering a culture of trust and integrity in online interactions.
- Malware and Hacking: Malicious activities like spreading malware or attempting to hack into systems are clear violations of cyber ethics. Such actions compromise the security and integrity of digital assets, leading to financial loss, data breaches, and other detrimental consequences. Reporting potential threats and vulnerabilities contributes to a safer online environment.
- Protect Personal Information: The internet poses risks related to identity theft, phishing, and online scams. Individuals must prioritize safeguarding their personal information and exercise caution when sharing it. By maintaining privacy settings and being mindful of the information they disclose, individuals can protect themselves from malicious intent.
- Authenticity and Impersonation: Maintaining honesty and authenticity in online interactions is essential. Creating fake accounts or impersonating others undermines trust and can have legal repercussions. Upholding integrity and trustworthiness ensures a genuine and reliable online community.

INTERNATIONAL ADVANCE JOURNAL OF ENGINEERING, SCIENCE AND MANAGEMENT (IAJESM)
July-December 2023, Submitted in October 2023, iajesm2014@gmail.com, ISSN -2393-8048
Multidisciplinary Indexed/Peer Reviewed Journal. SJIF Impact Factor 2023 =6.753

- Copyright Compliance: Respecting copyright laws and intellectual property rights is crucial in the digital age. Individuals should obtain proper permissions or use authorized platforms to download or share copyrighted materials. Encouraging ethical practices supports content creators and discourages piracy, fostering a fair and sustainable digital ecosystem.

V. Conclusion

As technology continues to advance, the risks and challenges in the digital realm become more complex. This review paper has provided a concise exploration of threats, vulnerabilities, risk assessment, the OSI model, and cyber ethics. By prioritizing threat identification, implementing robust security measures, and adhering to ethical guidelines, organizations and individuals can safeguard their assets and contribute to a safer digital landscape. It is crucial to continuously adapt and stay informed about emerging threats and ethical considerations to ensure the long-term security and well-being of all stakeholders involved.

References

(1) TUSHAR P. PARIKH, DR. ASHOK R. PATEL, Cyber security: Study on Attack, Threat, Vulnerability, Vol. 5, Issue: 6
(2) Nikander, Jussi & Manninen, Onni & Laajalahti, Mikko. (2020). Requirements for cybersecurity in agricultural communication networks. Computers and Electronics in Agriculture. 179. 105776. 10.1016/j.compag.2020.105776.
(3) Gade, Nikhita Reddy & Reddy, Ugander. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends On Latest Technologies.
(4) Saloni Khurana, 2017, A Review Paper on Cyber Security, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT) VIMPACT – 2017 (Volume 5 – Issue 23
(5) Obaidat, M.A.; Obeidat, S.; Holst, J.; Al Hayajneh, A.; Brown, J. A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers **2002**, 9, 44
(6) Bekkali, A.; Essaaidi, M.; Boulmalf, M.; Majdoubi, D. Systematic Literature Review of Internet of Things (IoT) Security. Adv. Indynamical Syst. Appl. (ADSA) **2022**, 21, 25–39.
(7) Albalawi, A.M.; Almaiah, M.A. Assessing and reviewing of cyber-security threats, attacks, mitiga tion techniques in iot environment. J. Theor. Appl. Inf. Technol. **2022**, 100, 2988–3011.
(8) Ghazal, T.M.; Afifi, M.A.; Kalra, D. Security vulnerabilities, attacks, threats and the proposed countermeasures for the Internet of Things applications. Solid State Technol. **2020**, 63, 31–45.
(9) Dange, S.; Chatterjee, M. IOT botnet: The largest threat to the IOT Network. Advances in Intelligent Systems and Computing **2019**, 22, 137–157.
(10) Gerodimos, A.; Maglaras, L.; Ayres, N. IOT: Communication protocols and security threats. Preprints **2021**, 25, 2021110214.