Challenges in Cyber Security and a review of Security Technologies for Network Applications

Sharada B.T, Sunitha K

Lecturer, Department of Computer Science, FMKMC College, Madikeri, India.

Abstract: A number of challenges have been developed in the field of cyber security as a result of the ever-evolving dynamics of technology and communication. It provides an overview of these challenges as well as a review of security solutions that are commonly utilized to protect network applications

Keywords: ***Encryption, APTs, IoT, SAST, Penetration evaluation, Fuzzing, SDLC***

I. INTRODUCTION

Cyber security is protecting computer networks. The primary goal of cyber security is confidentiality, availability, and integrity of information in the digital era. Cyber security tools are used to avoid unauthorized activities and various types of cyber-attacks. Cyber security encloses many more technologies, processes, practices, and measures framed to avoid various illegal activities [1].

It uses various key aspects are included in cyber security.

- **Protection**: The process of protecting the data from corruption, theft, or unauthorized access by using some of the encryption methods.
- **Detection**: To identify and recognize any doubtful or unauthorized activities in real-time by using tools and techniques. It responds quickly for the threat activities
- **Response**: When the occurrences of cyber incidents it takes a proper procedure and plans to address the system find the effect of those incidents and respond to them.
- **Recovery**: By using proper procedures and plans to restore systems to their normal state by minimizing downtime and data loss.
- **Prevention**: Preventing the system means updating the software regularly, using patches to secure the system, and giving guidelines on how to operate the network to minimize vulnerabilities.
- **Authorization and Authentication**: To allow using of only authorized access to sensitive information and resources through the use of strong authentication methods like two-way authentication or biometric verification.
- **Encryption**: Using encryption techniques to encode data, if they are authorized persons with the decryption keys can access and understand it.
- **Security Audits and Assessments**: Regularly check system evaluations, and networks for weaknesses, malicious unwanted code, and compliance with security standards and regulations.
- **Security Policies and Training**: To train the organization's employees how to use a safe computer network and develop security policies, guidelines, and procedures. [2]

II. CHALLENAGES ON CYBER SECURITY

There are many challenges in the field of cybersecurity due to the landscape of technology, improved networks, and elegant cyber threats. Some of the challenges are

- **Sophisticated Cyber Threats**: For cyber security professionals to defend against cybercriminals who are continuously developing cyber-attack techniques. This is one of the main challenges for cybersecurity professionals.
- **Quick developing Technology**: The adoption of new tools and platforms in the developing technology without efficient knowledge of security considerations, which creates vulnerabilities that attacker, can utilize the networks.
- **Insider Threats**: Employees in organizations with negligent actions can lead to data breaches and security issues. It affects the sensitive information of the organizations.
- **Unaware of Security**: Without the basic knowledge of how to handle cybersecurity practices, People become more vulnerable to common threats like phishing attacks.
- **Resource Constraints**: In small-scale organizations the establishment of necessary resources that are not available to implement robust cybersecurity measures, which are open to any attacks.
- **Dependency on Third Parties**: The organization will face security issues from third-party vendor services and any security weakness in their system

DOI : 10.35291/2454-9150.2023.0196

- **IoT and Connected Devices**: Usage of more internet of things IoT devices introduces a number of entries for attackers traditional computing devices have more security methods compared to these devices' security issues
- **Cloud Security**: As more data and services move to the cloud it is crucial to prevent data loss and unauthorized access by properly configuring cloud services
- **Data Privacy**: Organizations must have stricter data protection regulations to handle sensitive information by giving required robust security methods
- **Advanced Persistent Threats (APTs):** APTs are remaining undetected for long periods and are not able to identify the behavior of attackers APTs are a long-term process
- **Lack of Cyber Security Professionals**: To successfully handle cyber threats professionals are required lack of this knowledge could cause organizational problems.
    - **Human mistake**: When security standards and procedures are not followed properly human mistakes can result in security lapses inadvertent data failure and data disclosure patches are created and released.
    - **Zero-Day Vulnerabilities**: Attackers occasionally make use of flaws that the software vendor is not yet aware of making it difficult to protect against these attacks until patches are created and released.
    - **Regulatory Compliance**: That operate across many jurisdictions complying with the requirements of numerous cyber security rules and standards can be difficult and resource-intensive.
    - **Cyber security Complexity**: Managing several security tools technologies and solutions can make it more difficult to monitor examine and react to risks [3].

Not only these challenges along with some other challenges also faced in the period of 2018 to 2022

Cyber security has changed between 2018 and 2022 in response to emerging threats, shifting technological landscapes, and a growingly interconnected digital world. There are a few significant difficulties during this time [4].

Different 5G slices can be securely connected with the help of 5G and mobile security. Forbes has adopted a hybrid cloud model whereby sensitive data is saved locally and less sensitive data is stored in the cloud, in line with Nokia's strategy of hiding privacy through design and service orientation. The use of AI and machine learning in nation-state cyber operations and cyber-attacks is subject to international cyber security standards and has the potential to escalate.

Deep fakes and Man-made Content It produce false audio and visual content, which can lead to false information and hazards to confidence. It will be easier to reduce risks if there is a greater demand for cyber security education and awareness at all levels, among individuals and in organizations. The COVID-19 pandemic has brought forth new cyber security issues pertaining to patient data privacy and the safety of the healthcare system.

Our files, data, and complete device are being taken over by ransomware attacks until we pay a ransom payment. Our system will be attacked by a variety of random malware techniques, such as WannaCry and Not Petya. Because it spread among devices by taking advantages of the Windows Server Message Block (SMB) protocol, it is more potent and very successful. It is conversed with mutually on the network. According to estimates, the attack compromised over 300,000 systems across more than 100 nations, causing damages estimated to be in the hundreds of millions to billions of dollars. WannaCry was initially launched in 2017 and accepts payments in bitcoins or crypto currency Attackers quickly moved to most of the countries, but they initially targeted enterprises in Ukraine. Their primary goal is to destroy ports, disable businesses, and freeze government institutions globally.

III. TYPES OF CYBER SECURITY

1. Application security
2. Network security
3. Cloud security
4. Critical infrastructure security
5. IoT security
6. Data security

Application Security refers to defending against many forms of theft and dangerous attacks on system software applications. By using these techniques, software placed on a system is covered from potential attacks that service different types of techniques to identify possible risks before they can make use of application faults.

By using some specialized tools, processes, and techniques the users of e-commerce detect the vulnerability of their software application before hackers can find and attack them.

During the phases of software development it is necessary for the administrator to check various cyber security policies, standards, and tools to prevent hackers can accessing applications through a network.

Tools and Techniques are

- Static code inspection
- Dynamic Testing
- Penetration evaluation
- Fuzzing

If the software developer uses these tools then it is helpful to identify entire potential faults in their code or

DOI : 10.35291/2454-9150.2023.0196

development stage. This will prevent unauthorized access to software and private data.

Static code inspection is used to static application security testing (SAST) [5] to analyse the source code of program before executing it. It identify security vulnerabilities, errors in code, failure in identifying the operational problems before running or deploying may lead to security breaches.

In the concepts of cyber security code inspection in the code base it detects the weakness and vulnerabilities of the application before running it. For potential issues occurred in a code can quickly scanned by some automated static code analysis tools. When dealing with complicated applications, which are challenging to examine manually, scalability impacts are present. This reduces the security risks at the time of development stage by enabling developers to fix issues before the production. While secure code practices static code inspection integrated into SDLC [6] (Software Development Life Cycle). This tools performs in continuous integration or continuous deployment pipeline (CI/CD). This also identifies the common security vulnerabilities are SQL injection [7], cross-site scripting (XSS), buffer overflows, weak authentication methods and other security flaws.

By providing organizations custom rules and policies based on specific security requirements at the time of coding practices which allow developing most relevant code their application and organizations. By improving the quality of code, adhering to recommendations, developer can implement more reliable and maintainable code. It also gets feedback which is helpful to the developers improve their coding skills and security awareness.

Dynamic application security testing means securing the software application while running in real time environment. It interacts with the application to identify vulnerabilities for the attackers.

Dynamic testing are performed with real-world scenarios, where testing phase done by interacting with the application to identify vulnerabilities not only in the code but also in the run time. It identifies the input validation issues, leakage in data transfer problems occurring while maintaining the session etc. It is also known as block-box testing. It uses only in external point of view. It verifies the authentication authorization and authorization mechanisms, encryption etc. dynamic testing can also identify input related attacks like SQL injection, command injection. It unwraps the risks might occur in web forms, URLs, cookies etc. This evaluates the attack surface of an application. It also has a challenge to identify the design level vulnerabilities which has occurred at the core of the development cycle. Static and dynamic testing approach provides comprehensive security assessments.

A pen-test called a penetration [8] evaluation is an estimate the nature of the security system, network, application and other digital assets are protected. Authorized testing is conducted here to make use that using organizational devices or data without harm or accidentally created no harm.

Fuzzing [9] is used to find vulnerabilities when a system is put through automated testing. Fuzzing analysis is an automated software testing technique that finds problems in libraries, software programs, random or incorrect inputs, and potential security flaws. It is used to identify flaws and memory corruption that are missed by standard testing methods. This utility automatically generates a wide range of valid and invalid inputs using randomised input. When certain applications get unexpected or wrong inputs, it might lead to software vulnerabilities. Fuzzing is a highly efficient and automated way to find these problems.

IV. CONCLUSION

The challenges in cyber security are constantly evolving, necessitating proactive measures and the adoption of advanced security technologies to protect network applications effectively. Organizations must remain vigilant, stay updated on emerging threats, and implement a multi-layered security strategy to mitigate risks and safeguard their digital assets.

REFERENCES

[1]. http://www.kaspersky.com/resource-center/definitions/what-is-cyber-security.html
[2]. Security aspects-NCERT https://ncert.nic.in/textbook/pdf/lecs112.pdf
[3]. Russell Anthony Tantillo, Network Security through Open Source Intrusion Detection Systems, May 2012.
[4]. http://www.bing.rsisecurity.com | RSI Security
[5]. http://www.synopsys.com/glossary/what-is-sast.html
[6]. Software Engineering: A Practitioner's Approach By Roger S Pressman.
[7] Software Security: Building Security In" by Gary McGraw and "Hacking: The Art of Exploitation" by Jon Erickson.
[8]. The Hacker playbook 3: practical guide to penetration testing- Peter Kim
[9]. Fuzzing for Software Security Testing and Quality Assurance, Second Edition by Art Takanen, Jared D. DeMOTT, Charlie Miller, Atte Kettunen

DOI : 10.35291/2454-9150.2023.0196