JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

A Study of Cyber Security Threats and Mechanisms: A Review

Ranju Marwaha, Dr G N Verma, Amneet Kaur

ABSTRACT

This paper review the meaning of cyber security , types and threats. Cyber Security plays a significant role in today's digital world. Cyber crimes are increasing day by day posing a high risk for crucial data and information. Various steps can mitigate the impact of cyber threats and save the data.

Keywords : Cyber Security , Cyber Threats , Cyber Attacks

Cyber Security plays a critical role in protecting information systems, networks, and data from cyber threats. Importance of digital security is growing proportionate to increasing digital world rather more than that. Cyber Security is essential in areas like government, healthcare, finance, and education to protect sensitive data and prevent cyber attacks. Businesses rely on it to safeguard customer information and maintain operations. Critical infrastructure such as power grids and transportation systems also require strong security to avoid disruptions. Even individuals need cyber security to protect personal devices and online privacy.

Data presented to Parliament by the Ministry of Home Affairs and reported through the National Cybercrime Reporting Portal (NCRP) shows that in year 2024 cases of cyber attack rose to 42.08% over the previous years.

DEFINITION OF CYBER SECURITY

Cyber Security is the practice of protecting computer systems, networks, and data from unauthorized access, cyber attacks, and damage.

According to NIST (National Institute of Standards and Technology)

"The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentications, confidentiality, and non repudiation." [1]

As digital technology is rising , cyber risks are increasing , making cyber security more important than ever. It includes areas like network security, cloud security, application security, and endpoint protection. Cyber security also involves monitoring systems for potential threats and responding quickly to incidents. It ensures safe communication, secure financial transactions, and protected personal information.[2][3]

IMPORTANCE OF CYBER SECURITY

Cyber Security is very essential in today's digital age, as it saves the crucial data and systems from cyber threats. As the use of internet is accelerating , online services, and digital devices, individuals and organizations are more prone to attacks like hacking, phishing, and ransomware. Cyber Security ensures the safety of personal information, financial transactions, and confidential business data. It helps prevent data breaches that can lead to financial loss, legal consequences, and damage to reputation. In sectors like healthcare, finance, and government, It is critical for protecting public safety and national security. As remote work and cloud computing grow, secure networks and devices are essential. Cyber Security also builds faith between businesses and customers by safeguarding their data. It enables safe communication and supports the smooth operation of digital services. Without proper Cyber Security, systems can be compromised, leading to serious consequences. Therefore, strong Cyber Security is vital for a secure and reliable digital environment.[4][5][6]

PRINCIPLES OF CYBER SECURITY

The following principles form a base to cyber security

Confidentiality	It ensure that data is only accessible for authorized users. Data is given limited access
Integrity	Accuracy, trustworthiness and consistency of data is maintained.
Availability	It ensures that systems , data are available as and when required.
Authentication	Identity of the users and system is verified. Only legitimate users can access the data.
Authorization	It ensure right access privileges.
Non-repudiation	Proof of digital transaction is maintained
Accountability	Auditing, monitoring the users activity

TYPES OF CYBER THREATS

1. Malware

   Malware means malicious software designed to damage the computer, networs and other important peripherals. These malicious softwares are created and used by cyber attackers to gain access to important data or some financial gain. Their main purpose is to obtain sensitive information .

   Various Malware types includes Worms, Trojans, Ransomware, Spyware , Adware and Rootkit.

   Worms are types of malicious software that replicate themselves and spread the copies of itself to other computers. Worms do not require interference of the human being. Once worms are embedded it can modify and delete files.

   Trojan is a type of malware that disguises itself as legitimate software to trick users into downloading or installing it. They appear as useful programs, files, or software updates. Once activated, they can perform malicious activities such as stealing data, installing backdoors, or giving attackers control over the infected device. Trojans often open a "backdoor" for hackers to remotely access and control a system.[7]

   Ransomware The attacker encrypts the data and offers a decryption key in exchange of the payment. One of the most damaging and serious threat. It spreads through phishing emails, malicious downloads, or exploiting software vulnerabilities.It encrypts the files and demands payments from the users.

   Spyware is type of malicious software that secretly monitor and collect information from a user's device without their knowledge or consent. It often operates in the background, tracking activities like browsing habits, keystrokes, passwords, and other sensitive data

Adware is not malicious but can affect the functionalities of the system. It downloads or display the advertisements on users device.It can track the behavior of the users activity and can pose a risk at later stage.

Rootkit is a malicious software that gain root level control of the network .It maintains unauthorized access and it cannot be detected. Rootkit can allow the full access to data or steal the data. [8]

2. Denial of Service attack (DoS)

A DoS attack forbids the legitimate user to access the data. It is done by putting excessive traffic on the network so that the user cannot access the services or the resources. Websites of Financial institutions, defence or other crucial areas are its main targets. A large amount of useless data is sent so that traffic on server increases. Lot of requests are put on servers so that it will consume a lot of resources , once resources are exhausted, the network becomes slow , This causes denial of service to legitimate users.

Various DoS attack are

Volume-Based Attacks : In this types of attack, the server is flooded with large amount of traffic and thus making services unavailable.

Protocol Attacks : In this types of attack, many requests are sent to the server and handshake never completes , thus all traffic struck with half-open connections examples SYN flood , Ping of Death

Application Layer Attacks: In this types, application layer is made the target.functionality of the application is interrupted with seemingly legitimate requests.

Distributed Denial-of-Service (DDoS) Attacks: The server is flooded with malicious traffic, thus results in slow performance of the server and downtime in providing services to the users.

Resource Exhaustion: lots of requests is send to the server for a number of resources.Thus actual users unable to get access.

Reflective Attacks: A request is sent to server using third party IP.A server send responses not knowing that malicious act.

3. Phishing Attack : In this type of attack, the attackers create a fake email or phone call to victim to share his personal credentials or other sensitive information. It might contain some link for the users to use and thus all sensitive information is leaked.

Various types of phishing attacks are

Deceptive phishing : sending of large number of emails to the victim
Spear phishing : malicious emails sent to the individuals and steal sensitive data.
Whaling : High rank individual are made the target so that crucial informationcan be extracted.
Angler phishing: the attacker disguised himself as customer care executive and steals sensitive information.
Clone phishing: legitimate emails is copied and resend to the user so that passwords etc can be stolen. [9]

4. Man in the Middle Attack (MITM) In this type of attack, the attackers put himself into the ongoing communication between users and server. Silently it listens to the entire communication and data that is exchanged . It can then modify that data . the user assumes that connection is secure and reliable.

5. Pass – the –Hatch Attack (PtH): The attacker first gain the access to the OS and extract passwords etc. It uses the stolen hash to make request to other systems. The target system authenticates the request and thus gain the access to the new system. Thus session starts.

6. Credential Stuffing: Attackers get the list of compromised password and they uses bots to use these credentials on different financial websites , thus gain access to the sensitive information and steal the money. It is common practice that people often uses same password on different websites. Brute force attack uses trial and error way to gain access to the credentials.

7. Code injection Attacks : In this type of attack, the sensitive application interprets the code as the malicious information is given by the attacker. Now attacker got access to the program and it can alter the program. This process is called as code injection.

   SQL Injection (SQLi) : the attacker injects the malicious SQL queries into the database and use these queries to gain access to the information . Now once access gained, it can modify the information.

   Cross-Site Scripting (XSS) : The attacker injects malicious code into the website. Thus the code posted by users become risky and more prone to XSS attacks.

   Server-Side Template Injection (SSTI): Now this time, template is injected thus allowing to to execute arbitrary code on the server.

   CRLF injection: Carriage return, line feed characters are inserted into the input , thus can be used later to enter malicious code or execute the attack.

8. Data Poisoning : In this type of attack, the data is given poison that is misleading data in inserted into the training dataset and thus corrupting the model's learning process. Main motive is to degrade the model thus lowering its performance. Once deployed , the faculty behavior is triggered and thus sensitive information becomes vulnerable to attack.

9. Tunneling DNS: In this type of attack the network security is bypassed. The attacker uses DNS queries and response to send the information. Hacker becomes free to gain access , to perform commands and control the system. When user downloads the malware , a hacker gain access to the system. Attacker need to set up a tunnel that is a way to send and receive data from the compromised system.

10. Inside Threats : Such threats originate from within the organizations . It can be in form of malicious insiders or careless insiders or even compromised insiders. Malicious insiders might sale the data for some kind of financial gain. Careless insiders might disclose the credentials unintentionally. Compromised insiders might fall prey to hackers.

11. IoT Based Attack: In this attack the susceptibility of the devices connected to the internet are targeted. Attackers steal the data or can cause damage to the resources. [10]

MECHANISM TO CONTROL THREATS

Protecting data and information is very essential to save it from cyber threats.

Technical controls [11]

Encryption : Protecting the data in transit by encrypting the data , thus it will become useless for the attacker.

Firewalls : Firewall can be installed so that filtered data is received. It blocks the malicious data and thus saving from cyber attack.

Malware scanners: This software scans the files and documents for malicious attack.

2FA : Another method is to use second form of verification besides the password.

Network Segmentation : It divides the network into smaller parts. This will limit the cyber attack if it occurs.

Anti virus software: It prevents the malicious software programs to disrupt the data. Update versions of the antivirus protects the data from attack.

IDS: Another system to monitor the networks for malicious attacks. It warns the system if any malignant attack found.[12]

Administrative Practices

Strong Passwords : Combination of alphabets, numbers and special characters can form a strong password that becomes difficult to crack.

Regular Updates : regular updates of software are crucial for protecting system from attacks. They provide updated security features.

Data Backups : Regular backups of data can be helfpful . If data is lost due to some cyber attack, it can be recovered.

Access Control : It enables individuals or organizations to manage the data and data can be accessed by authorized persons only.

Digital signatures : It can be another method to prevent data from corrupting. [13]

Physical controls

Surveillances : Modern and updated physical security and traditional methods can prevent data from physical attacks.

Fire Extinguishers : it can protect data from intentional or unintentional fire breaks.[14]

CONCLUSION

This paper reviewed the papers on cyber security types and threats. Various types of cyber attacks are coming up day by day. Cyber threats are biggest challenges that this digital world is facing. By understanding the nature of various threats, we can reduce the effect of these threats. Although these cannot be eradicated completely, we can only alleviate the dangers of the attack. Staying acquainted, employing strong security measures, and inculcating a culture of cyber awareness are essential steps toward reducing vulnerabilities and safeguarding sensitive information from cyber attackers.

REFERENCES

1. https://csrc.nist.gov/glossary/term/cybersecurity
2. " A study of cyber security challenges and its emerging trends on latest technologies by G Nikhita , GJ Ugander Reddy
3. Cybercrime and Cybersecurity in India: Causes, Consequences and Implications for the Future By: Nir Kshetri Springer Netherlands
4. " A study of cyber security threats , challenges in different field and its prospective solutions : A ReviewVal Hyginus U Eze, Chinyere Nneoma Ugwu and Ifeanyi Cornelius Ugwuanyi INOSR publications
5. Research Paper on cyber security challenges and threats Atul Arun Patil IJARSCT
6. Cyber Security Threats on the Internet and Possible Solutions B. A. Obotivere1, A. O. Nwaezeigwe2 IJARCCE
7. CYBER SECURITY: THREATS AND CHALLENGES Niteesh Kumar*1
   *1BE, CSE Fourth Year Student, Brindavan College of Engineering, Bangalore
8. A Research Paper on Cyber Security Ansh Singh1, Gulshan Kumar2 International Journal of Research Publication and Reviews Journal homepage: www.ijrpr.com ISSN 2582-7421
9. Evolution Cybercrime—Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data
10. An analytical study on challenges and gaps in India's cyber security framework Anuradha Chakraborty and Sanyogita Tiwari ~ 4 ~ International Journal of Criminal, Common and Statutory Law 2025; 5(1): 04-07
11. G N Redyy and GJU Reddy "A study of cyber security challenges and its emerging trends on latest technologies
12. A study of cyber security challenges and its Emerging trends on latest technologies G.nikhita reddy1 , g.j.ugander reddy2
13. The study on legal and ethical issues in cyber security in india IJRAR June 2024
14. Physical Security to Cybersecurity (Challenges and Implications in the Modern Digital Landscape) April 2024 Journal of Electrical Systems 20(4s):692-702