IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 5, May 2024

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.423

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305185 |

Cyber Security and Threats

Saurabh Bobade, Prof. Lowlesh Yadav, Prof. Vijay Rakde

Department of CSE, Shri Sai College of Engineering and Technology, Chandrapur, India

Assistant Professor, Department of CSE, Shri Sai College of Engineering and Technology, Chandrapur, India

Assistant Professor, Department of CSE, Shri Sai College of Engineering and Technology, Chandrapur, India

ABSTRACT:The rapid development of technology has provided new opportunities and effective technology potential to organizations of all sizes. This new, but also brings with it an unprecedented threat. However, multimedia editing tools can be used to enhance and modify the content of digital data, compromising the reliability of the data. Cyber security is defined as the protection of systems, networks and information in cyberspace with the aim of preserving original information and eliminating all doubts regarding the truth. In business, this is an important and difficult topic in the online world. As more IoT devices connect to the internet, cybersecurity will become even more important. This article focuses on types of network security, types of vulnerabilities and threats in the network, and strategies to prevent threats. I finally took advantage of the online world.

KEY WORDS: Internet security, Internet threat, data mining, Internet crime, Internet crime. Introduction

I. INTRODUCTION

Nowadays, governments and organizations have become increasingly vulnerable to the security of information on the I nternet and computers. Cybersecurity is the process of protecting information and systems against unauthorized access. This has become riskier due to cyber attacks and threats. Cyber threats are threats that use various techniques to gain un authorized access to control networks and systems. Evidence suggests the threat is more serious than we thought. Onlin e blogs and mobile applications (such as WhatsApp, Hiking and instant messengers) are emerging very quickly and are being used to attack our information infrastructure. Cybercrime, cybercrime, cyberespionage, cyberwar. In cyberspace, cyber attackers exploit many vulnerabilities to carry out these operations. They exploit weaknesses in hardware and soft ware created using malware. DOSS attacks are used to flood target websites. Hacking is a way of breaking a computer's protection and interfering with its operation. Identity theft is also common. Everything changes very quickly. New tacti cs are constantly being published.

II. RELATED WORK

CYBER SECURITY

There are three core principles of cyber security. It involves Integrity, Confidentiality and Availability. Integrity means information unaltered from its original state without authorization. Information not to be shared with inappropriate users. Availability refers to system and information available and accessible to who need it essentially.

a) Types of Cyber Security 1. Physical Computer Security This is the simplest and most common type of computer security. In this case, anyone with physical access to the computer can control it. They are hire guards, use secure doors, and even put computers on military bases or deserted islands just to keep them safe. But ordinary people cannot protect their personal data on office computers or elsewhere. However, computer engineers are not aware of important information. 2. Internet security is a branch of computer security specifically related to the Internet.. The goal of network security is measures and establish rules to protect against attacks over the Internet and internet accessible resources. It is controlled by the network administrator. It is useful for private and public. It includes wired and wireless networks of Network Protocols, IP security, Email security, Web security, Intruders, Viruses and Firewalls. In firewall is a critical part of computer security. The main function of the firewall is to prevent unauthorized access to the network from your computer. Home computers can be easily protecting by firewalls.

b) Cyber security standards When identifying the most useful best-practice standards and guidance for implementing effective cyber security, it is important to establish the role that each fulfils, its scope and how it interacts with other standards and guidance.

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305185 |

CYBER THREATS

Cyber threats are the potential to damage or disrupt a system or computer network. The purpose of the attack depends on the cybercriminal's needs. These attacks affect many important areas such as the military, financial institutions, government, business, industry and hospitals, collecting, storing and processing sensitive information of computers, sharing information with other computers over the network.

a) Types of cyber threats and technologies Data and information security is a major problem for almost all organizations. Attackers are developing new technologies to capture patterns, signatures and messages in cyberspace. Here we will explain some of the threats and techniques in cyberspace.

1. Trojans - Trojans are unwanted programs or malicious programs that hide behind real programs and can cause physical damage or allow full access to the system, recording your keystrokes and monitoring on the webcam. Not easy to find and follow background

2. Root kits – A Root kit is a malicious software developed to hides certain programs or a process to a privilege to access a system and from regular anti-virus scan detection. Whenever booting a system that software which runs and gets activated each time and are difficult to install and detect various process and files in the system.

3. Spyware – Spyware refers to a hidden component of a freeware program which naturally gather and spy information from the system without the knowledge of users through an internet connection. Such spyware inundates with uncontrollable pop-up ads.

4. Scare ware – Scare ware is a type of threat which acts as an honest system message and guides to purchase and download potentially dangerous and useless. But actually they are harmful and take control of all software's running on certain computers control of all the software's running on certain computers.

1. **Spoofing –** It is a cyber-attack where a program or a person impersonate another by creating false data in order to gain illegal access to a system. These types of threats often appear in emails where the sender's address is spoofed..

2. **Malware –** Malware is a malicious software that are designed to do unwanted actions into the system or to damage the system. Malware is of many types like Trojans, viruses, etc., which can behalf and Take control of your computer and all the software running on it.

3. **Adware –** Adware is a software will collect all your data without our consent. That would come in the form of installed automatically or a free download and send your passwords, usernames, surfing habits, settings, downloaded applications to third parties. It redirects you to unwanted websites or bombards you with uncontrollable ads. These are difficult to remove and may infect your computer with viruses

b) Techniques to Avoid Cyber Threats

The innovation of technology tosses up new online risks. To identify and eradicate the security holes from system that makes vulnerable to cyber threats. There are some of the steps to help our systems and information's.

1. Properly configure and patch operating systems, browsers, and other software programs.
2. Use and regularly update firewalls, anti-virus, and anti-spyware programs.
3. Use strong passwords (combination of upper and lower case letters, numbers and special characters) and do not share passwords.
4. Be cautious about all communications; think before you click. Please use common sense when communicating with users you know and those you do not know.
5. Do not open e-mail or related attachments from un-trusted sources and don't access questionable web locations.

III.METHODOLOGY

Reconnaissance refers to gathering information about the target for the ex-Domain name, IP, Target personal information, Email, Sub-domains, Job information, etc. Reconnaissance is also known as Foot-Printing., open ports, and services in the target network. Usually in this phase, hacker tries to prepare a blueprint of the target. We have many tools to collect information about the target device; these include Net craft, HTT monitoring for mirror location,

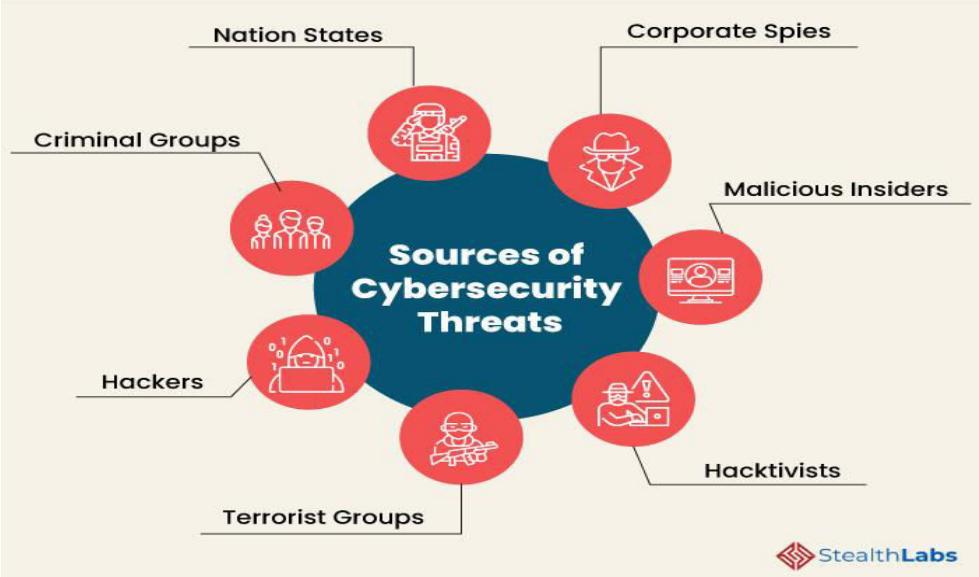
|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305185 |

Firebug - data extractor, Know - network discovery, sublist3r for subdomains, etc. It is located. Host, IP address, running service, open port and services on the target network

By using strong passwords, controlling access, installing firewalls, using secure software, regularly updating programs and systems, and monitoring access, security measures are in place to give you a basic level of security against most IT risks. Strong passwords are essential for good online security. Make your password hard to guess. Ensure people can only access information and services for which they are authorized. Firewalls are effective protectors of computers and the Internet and are one of the main barriers to preventing online infections such as viruses and malware. You should use security software such as anti-spyware, anti-malware, and anti-virus programs to help detect and remove malware that has infiltrated your network. Updates contain important informationsecurity upgrades that help protect against known bugs and vulnerabilities. You can use intrusion detectors to monitor system and unusual network activity



Here are some of the common sources of cyber threats:

1) Nation States Cyber attacks launched by nations can cause harm by disrupting communications, military operations, and daily lives.

2) Criminal Groups Criminal groups gain access to systems or networks for financial gain. These groups use phishing, spam, spyware and malware for theft, online fraud and physical abuse.

3) Hackers Hackers explore various network technologies to intervene by protecting and exploiting vulnerabilities in computer systems or networks. Their motivations are personal gain, revenge, money-making and political activities. Hackers create new threats to competition or pride in the hacker community.

4) Terrorist organizations use cyber attacks to destroy, access or use critical systems, undermine national security, destroy military equipment, disrupt business and cause harm to many people.

5) Hacktivists Hacktivists carry out cyber attacks for political gain rather than financial gain. They target businesses, organizations or individuals that do not align with their thinking and processes.

6) Malicious Insiders 97% of surveyed IT managers expressed concern about insider threats to cybersecurity. Insiders may include employees, third-party vendors, contractors or other business partners who have access to intellectual property rights but do not use them properly.accesses to steal or destroy information for financial or personal gain.

7) Corporate Spies

Corporate spies conduct industrial or business espionage to either make a profit or disrupt a competitor's business by attacking critical infrastructure, stealing trade secrets, and gaining access.

IV. CONCLUSION

In the event of a cyber security incident, such as an attack, studies show that the greatest defence is a PC-savvy customer . To consider is by far the most vulnerable, who are identified in this investigation as new employees inside an organization, as specifically, with the adversary seeking for personally identifiable information from people

|e-ISSN: 2319-8753, p-ISSN: 2347-6710| www.ijirset.com | Impact Factor: 8.423| A Monthly Peer Reviewed & Refereed Journal |

|| Volume 13, Issue 5, May 2024 ||

| DOI:10.15680/IJIRSET.2024.1305185 |

involved. Mental issues that con-tribute to customer and organization vulnerability are also addressed in this investigation. This study finds that cyber security threats and approaches have a role to play in reducing the impact of digital attacks, risk, and vulnerability, while creativity has a role to play in reducing the influence of digital attacks, threat, and lack of strength. Cyber-attacks can be mitigated, but there does not appear to be an absolute solution for overcoming such network security threats at this time. Later, when the company implements the system security design, the operation of the cyber attack, threat, and vulnerability decreases

REFERENCES

1. . Lowlesh Yadav and Asha Ambhaikar, “IOHT based Tele-Healthcare Support System for Feasibility and perfor-mance analysis,” Journal of ElectricalSystems, vol. 20, no. 3s, pp. 844–850, Apr. 2024, doi: 10.52783/jes.1382.
2. L. Yadav and A. Ambhaikar, "Feasibility and Deployment Challenges of Data Analysis in Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-5, doi: 10.1109/ICAIIHI57871.2023.10489389.
3. L. Yadav and A. Ambhaikar, "Approach Towards Development of Portable Multi-Model Tele-Healthcare System," 2023 International Conference on Artificial Intelligence for Innovations in Healthcare Industries (ICAIIHI), Raipur, India, 2023, pp. 1-6, doi: 10.1109/ICAIIHI57871.2023.10489468.
4. Lowlesh Yadav and Asha Ambhaikar, Exploring Portable Multi-Modal Telehealth Solutions: A Development Approach. International Journal on Recent and Innovation Trends in Computing and Communication (IJRITCC), vol. 11, no. 10, pp. 873–879, Mar. 2024.11(10), 873–879,DOI: 10.13140/RG.2.2.15400.99846.
5. Lowlesh Yadav,Predictive Acknowledgement using TRE System to reduce cost and Bandwidth, March 2019. International Journal of Research in Electronics and Computer Engineering (IJRECE), VOL. 7 ISSUE 1 (JANUARY- MARCH 2019) ISSN: 2393-9028 (PRINT) | ISSN: 2348-2281 (ONLINE).
6. H. Suryotrisongko and Y. Musashi, "Review of Cybersecurity Research Topics, Taxonomy and Challenges: Interdisciplinary Perspec-tive," 2019 IEEE 12th Conference on Service-Oriented Computing and Applications (SOCA), Kaohsiung, Taiwan, 2019, pp. 162-167, doi: 10.1109/SOCA.2019.00031.
7. Y. Liu, H. Qin, Z. Chen, C. Shi, R. Zhang and W. Chen, "Research on Cyber Security Defense Technology of Power Generation Acquisition Terminal in New Energy Plant," 2019 IEEE International Conference on Energy Internet (ICEI), Nanjing, China, 2019, pp. 25-30, doi: 10.1109/ICEI.2019.0001
8. F. Alkhudhayr, S. Alfarraj, B. Aljameeli and S. Elkhdiri, "Information Security:A Review of Information Security Issues and Tech-niques," 2019 2nd International Conference on Computer Applications & Information Security (ICCAIS), Riyadh, Saudi Arabia, 2019, pp. 1-6, doi: 10.1109/CAIS.2019.8769504.
9. Lowlesh Nandkishor Yadav, “Predictive Acknowledgement using TRE System to reduce cost and Bandwidth” IJRECE VOL. 7 ISSUE 1 (JANUARY-MARCH 2019) pg no 275-278
10. C. Ten, G. Manimaran and C. Liu, "Cybersecurity for Critical Infrastructures: Attack and Defense Modeling," in IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans, vol. 40, no. 4, pp. 853-865, July 2010, doi: 10.1109/TSMCA.2010.2048028.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details