Research Journal of Computer and Information Technology Sciences ________________________ISSN 2320 – 6527
Vol. **11(1),** 12-15, June **(2023)** *Res. J. Computer and IT Sci.*

Short Review Paper

Cyber Security: Threats and its prevention

Prince Pratap Singh Banjare and Sunita Soni
Bhilai Institute of Technology, Durg, CG, India
princeb65@gmail.com

Available online at: www.isca.in
Received 3rd September 2021, revised 28th January 2023, accepted 16th April 2023

Abstract

The term "Cyber Security" is very important nowadays. This two-letter word Cyber Security in which Cyber means anything which is related to Internet & Security means protection. We can say that whenever we try to protect our E-Systems i.e., computers, mobile devices, servers, networks, databases, etc. from malicious attacks then it is known as Cyber Security. Many organizations deal with ecommerce applications with their fragile network. Vital web security services are intent to cyber-attacks so it is very important for the organizations to improve their performance & security of E-Systems to make sure that the data of users follow integrity & confidentiality. There are many techniques of prevention of cyber-attack suggested or proposed by many people from which we can protect our E-Systems from these types of malicious attacks. But unfortunately, no single solution can work for all E-Systems devices & services although we can use some techniques i.e., Network security techniques, Application security techniques, Information security techniques, Operational security techniques, etc. to overcome the cyber threats. We can use many safety tips from which we can protect our E-Systems from cyber threats. In this era, we need such tools of protection against these cyber-attacks. For example, we can use Anti-viruses, strong passwords; avoid using public Wi-Fi network connections, updating our systems frequently, etc. The objective of this research is that how we can protect our E-Systems from doing simple changes in our habits while using E-System's computers or devices that work with the help of the internet.

Keywords: E-Systems, cyber-attacks, cyber security, network security, malicious attacks, cyber threats, malwares, spywares, denial of service (DoS), Trojans, Emotet, Adware, Phishing, Brute-force, Cross-site scripting, Zero-day exploit, cloud breaches, Strong password, Firewalls.

Introduction

Nowadays, the Internet captures a major part of our lives. Without the internet most of our tasks are incomplete. It not only enables smooth operations but also improves the management processes. The evolution of E-Systems has made our society more independent on their services than ever. Just imagine a story that you are using your computer. In the background, some cyber criminals mainly known as hackers are stealing some data from your system. The information is that much sense that the hacker sells it to someone demanding some profit in exchange for that particular data.

For me, it is like a scene in a movie but nowadays it is very common. Sometimes, someone is watching us from our web camera and we don't have any idea about that therefore some people hide their camera with some physical stickers. In this research, we will see & learn that how cyber security threats can be pulled off from our lives by just making small changes in our habits of using E-Systems i.e., computer systems or devices[1].

Cyber security was originally designed for the protection of networks & devices from external threats or cyber-attacks. This cyber security world revolves around the industry standard of the CIA which stands for Confidentiality, Integrity, and Availability. All three have their own functions. Such as Confidentiality or we can say privacy grants access only to the authorized users. Integrity is that the information can be manipulated (add, remove, change, alter, etc.) by authorized users and Availability means the information or functions must be available on-demand according to the user's need.

Cyber security mainly uses authentication mechanisms i.e., some users can use to identify an account that a user wants to access, while a password is a mechanism that proves the user is who he claims to be[2].

Types of Cyber security Threats

Malwares: Malwares are most common cyber threats which are generally known as malicious software. Malware activates when a user clicks on a malicious links or attachments which were generally come with the unfaithful email attachments or admit-table looking downloads. Once it is activated it can do many things, such as blocking access to key network components (ransom ware), transmitting data from hard drives (spywares), and installing additional harmful software's without user's proper permission, making our system idle or useless. Cyber criminals can make money by using malwares[3].

There are many types of Malwares, they are as follows:
Virus: It is a self-replicating program that spreads throughout computer system which infects files with the malicious codes. It generally attaches itself to clean the files of our computers.

Trojans: It is a type of malware that looks like appropriate software. The hackers do fakement to we users to upload Trojans onto our systems where they can damage or collect our data from our hard drives.

Spyware: Spying on something means secretly collecting the information of any user without permission. Spyware does the same thing. These programs secretly record what we users were doing. For example, it can record our credit/debit card details, internet banking details etc.

Ransom-ware: We saw in movies that someone took something personal belongings and then they ask for money in return of that. Ransom-ware does the same thing. It locks down user's files with the threat of expunging it unless a ransom is paid to them.

Adware: These are generally advertising software which can be used to spread malwares.

Botnets: Botnets are a type of distributed denial of service (DDoS) attacks. These are the networks or organizations of malware infected systems/computers which is used by cyber criminals to perform any tasks without any prior permissions of user. It is also known as zombie systems. It overcomes the target's processing capabilities. They are generally present on different a geographic location that's why they are hard to trace[4].

Emotet: Emotets are an intricate Trojan that can load other malware and also can steal data. It blooms on ingenious or easy password. We should create a secure and strong password in order to protect ourselves from this cyber threat. Emotes are most costly & destructive malwares.

Denial of Service: It is also known as DoS attack which stands for Denial of Service. In this cyber-attack floods a computer network so it can't respond to requests. The cyber criminal blocks a computer system from achieving its aim or requests by sending traffic to the servers, networks and databases so that the computer system (E-Systems) did not get used hence the organization could not get the vital information. Cyber attackers often use flood attacks to sabotage the "handshake" process and carry out a DoS[4].

Man in the Middle: MITM attack is a cyber threat in which in order to steal information exchanging between any individuals, cybercriminal interrupts or intercepts communication between those two individuals and then use malware to install software and use their data or information maliciously. For example, while we are using a public Wi-Fi network, any attacker inserts themselves between our device & network and they can install any malicious software without our permission[4].

Phishing: This attack uses factitious communication techniques such as emails or messages in which it seems like any reputed company is asking for your sensitive information such as credit/debit card details, OTP, CVV, etc. It generally tricks a receiver to open the mail or message whatever they sent and carrying out the process present in that particular message so that they can steal the user's sensitive information or install malicious software on our machine[4].

SQL Injection: A structured Query Language (also known as SQL) injection is a cyber-attack in which an intruder can insert a SQL code into the server or database and took control and steal the information or data from the server or database. When the server got infected, it easily releases information. Inserting the infected code into the server or database is as simple as entering it into the website search box[5].

Password Attacks: When an attacker knows the password then they have access to a wealth of information about the user. Password attackers can use endless methods to identify the password of any person inclusive of gaining access to password databases, dealing with social engineering, or simply by guessing.

Brute-Force Attacks: This attack uses all the possible combinations to guess the passwords.

Dictionary Attack: When a set of many common passwords are used to gain access to the computer system then it is known as the dictionary attack.

To prevent these password attacks we can use the 2-factor authentication method because this method adds up an extra security layer.

Cross-site Scripting: This attack can send malicious scripts from reliable websites. That infected code joins the dynamic content that is sent to the prey's browser. Generally, this infected code contains JavaScript code but it can also include HTML and XSS, etc[5].

Rootkits: These are the threats that are installed inside legal software which can gain remote control access of the system over the administration level. Since rootkits are hidden in the legal software, once you allow the program to manipulate the operating system, the rootkits install themselves in that system and remain inoperative until the attacker triggers it through any mechanism[6].

IoT Attacks: Internet of things (IoT) is very common nowadays. It provides nearly endless access points to the intruders to trade upon the E-System/Networks. The interconnection of things makes possibilities for attackers to breach an entrance and use it as a gate to exploits other E-Systems in the network. Keeping the Operating system up to date and using strong passwords can reduce the possibilities of attacks using IoT devices or platforms[6].

Drive-by Downloads: A drive-by download is generally picked by us unknowingly from any web page. We the user visits any web pages and in that, a malicious program gets implanted in our E-Systems without our permission. Later on, it caused us to like our information. We can avoid this attack by using anti-viruses which are designed to identify the threats and segregate them from our E-Systems[7].

Spear Phishing: In this attack, the attacker's goal is to attack those who are privileged users who are mainly system administrators or C-suite users.

Zero-day Exploit: It generally occurs when the vulnerability of software & hardware is announced. The attacker already exploits the system before the implementation of the solution or patch.

Advanced Persistent Threats (APT): This attack occurs when a malicious code started availing the unauthorized access to our E-Systems and at that time, we as a user can not detect it for some extended time. Our computer systems could also not detect the same.

DNS Attack: In this attack, the intruder's main target is to exploit vulnerabilities present in the domain name system (DNS). The intruder took advantage of our system's vulnerabilities and recurve the visitors to some malicious pages (which is also called DNS Hijacking) and then the filtered data is being sent to compromised systems (which is also called DNS Tunnelling)[7].

Cloud Breaches: Nowadays, approx. all companies are shifting towards the cloud to support remote work. In this covid scenario, all companies following remote work. They all shifted from physical to digital thus, cyber-attackers also aiming towards the cloud very frequently. There are many issues a company can face if any intruder gains its cloud database. i.e., they can misconfigure their database, can delete their data from the cloud, and many things they can do with the same data to make you & your company suffer[8].

Prevention from Cyber security Threats

We can easily prevent our E-Systems from cyber-attacks. We just need to be careful with some useful strategies of our devices and systems. Here are some prevention techniques from which we can save our system and overcome cyber-attacks.

End-user Protection: It is also called endpoint security. This software scans our E-Systems/computers for checking that if there is any malicious code is present in our system or not. If present then it'll encapsulate that code and then eliminate it from our machine. Cryptographic protocols are used by these endpoint techniques to encrypt emails, attached files, or any of our data to protect it against any malicious attacks. End-point protection not only protects our data from erasing but also protects data from loss or theft[8].

Update your Software's and Operating systems: When we update our software, we get the latest security patches and they cover all the previous flaws of that particular software. The latest updates are better than previous updates in the case of E-Systems, so it is necessary to update the systems and software on regular basis[9].

Use Anti-virus Software's: For the best level of protection, we should use anti-virus software. It detects the threat and sometimes warns us too and then removes it automatically.

Use strong passwords: What is the use of a lock if it'll get open with any key? We should always use strong passwords. For strong password creation, we should use at least one small case letter, one upper case letter, one numeric value, and one special character in our passwords. For example, if I create a password for myself, I use something related to some sentence[10].

Sentence: My car doesn't like Vanilla ice cream at the parlor and Gym. Password: M2354dlVic@p&G

NOTE: Remember that the sentences can be an abstract sentence. Do not find meaning in that. So, the password should not be easy that anyone could guess it.

Do not open email attachments from unknown senders: In the era of cyber-crimes, one should not trust any unknown sender because there are 99% chances that the attached file is infected with malicious software i.e., malware or code which can damage or systems or devices only after downloading it[10].

Do not use public Wi-Fi: Using unsecure Wi-Fi network which is generally open network can be very harmful for us as it is mainly used for man-in-the-middle attacks. While using this public network the attacker gain access to our systems and then they can manipulate it the way they want. So avoid using it and if using then do not grant permission for any suspicious things on your system[10].

Make Backup of your Data: It is a part of personal online security. Just in case if you get attacked by ransome-ware then the only way to get your data back is from the backup. For making backup we should follow 3-2-1 rule. i.e., We should make three copies of our data on two different type of media

(Local drive and external hard drive) and one copy at cloud storage. In this manner we can easily recover lost data[11].

Install Firewalls: Using some additional layer of security to protect our system can be termed as firewall. The idea behind installing a firewall is to provide an additional security layer which is very effective way of defending the system from cyber attacks. A firewall system blocks any Brute force attack before damaging or changing something of our system[11].

If you've seen a movie named Avengers: Age of Ultron[12]. In that the AI known as JARVIS was working there as a firewall who is continuously changing the nuclear codes and protecting it from ultron so that it cannot launch the nuclear weapon and cause a war.

Conclusion

Cyber security is in every part of our lives. Our day starts with the internet and also ends with the internet. It is like oxygen for we humans nowadays. Every information is in our finger tips. Day by day it is getting common of facing the cyber threats. We have seen many types of attacks so far. We needed to take care of whatever we are using like internet or E-systems etc. All we need to do is a little change in our daily lives while using the internet or e-systems. Timely updating the systems and changing passwords on a daily basis etc can make us secure from these attacks.

References

1. Mbelli, T. M., & Dwolatzky, B. (2016). Cyber security, a threat to cyber banking in South Africa: An approach to network and application security. In 2016 IEEE 3rd International Conference on Cyber Security and Cloud Computing (CSCloud), pp. 1-6. IEEE.

2. Al Shaer, D., Al Musaimi, O., De la Torre, B. G., & Albericio, F. (2020). Hydroxamate siderophores: Natural occurrence, chemical synthesis, iron binding affinity and use as Trojan horses against pathogens. *European Journal of Medicinal Chemistry*, 208, 112791.

3. Sneed, H. M. (2005). Testing an e-government Web site. In Seventh IEEE International Symposium on Web Site Evolution (p. 3). IEEE.

4. Meszaros, J., & Buchalcevova, A. (2017). Introducing OSSF: A framework for online service cyber security risk management. *Computers & Security*, 65, 300-313.

5. Stevens, C. (2020). Assembling cyber security: The politics and materiality of technical malware reports and the case of Stuxnet. *Contemporary Security Policy*, 41(1), 129-152.

6. Kuznetsov, D. I., & Ryabchina, L. S. (2019). Information security of the Internet of Things systems. *Bulletin of Kryvyi Rih National University*, 49, 80-83.

7. G. Immerman, (2020). The importance of edge computing for the iot. URL: https://www. machinemetrics.com/blog/edge-computing-iot.

8. Jamal, A. A., Majid, A. A. M., Konev, A., Kosachenko, T., & Shelupanov, A. (2023). A review on security analysis of cyber physical systems using Machine learning. *Materials Today: Proceedings*, 80, 2302-2306.

9. Alghamdi, M. I. (2021). WITHDRAWN: Determining the impact of cyber security awareness on employee behaviour: A case of Saudi Arabia.

10. Al-Ghamdi, M. I. (2021). Effects of knowledge of cyber security on prevention of attacks. *Materials Today: Proceedings*.

11. Paulsen, C. (2016). Cyber securing small businesses. *Computer*, 49(8), 92-97.

12. Ventura, R. A. (2015). Avengers: Age of Ultron. *Philosophy Now*, 111, 46-47.