International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

A Study of Threats, Detection and Prevention in Cybersecurity

Vijay Yadav[1]

[1]*Computer Engineering Department, Terna Engineering College, Nerul, Maharashtra, India*

Abstract - *Cybersecurity as the name suggests is a means to protect the sensitive data of business intellectuals as well as of naive users. As internet usage is increasing day by day, cybersecurity specialists have to implement various methods for the protection of the information. Securing the data has now become a major challenge in the field of cybersecurity. There are various kinds of threats which help the attackers to obtain the sensitive information of a user. Such acts are termed as cyber-crimes. Various organizations and Government intellectuals are taking measures to prevent the data breech. This paper mainly focuses on the types of modern threats and how they affect the organization or a personal user's system. This paper also includes detection of the threats and measures on how to prevent the system from being compromised.*

***Key Words*: Cybersecurity, cyber-crime, OWASP, SQL, logging, LINUX, XSS**

1. INTRODUCTION

In today's modern world we all use the internet to perform myriad number of activities such as booking tickets, shopping, digital marketing, transferring funds online, etc. Let's take an example, where a person tries to transfer a fund from one bank account to another does he/she think that his/her money is going into the right account.

What if the private data gets compromised or what if the money gets transferred into the hacker's account. There are 'n' number of problems that arise when we do any activity on the internet medium. We don't actually pay attention to the information that we share or we have on the Internet.

Well, first of all, we need to care about data protection. In the past, if we wanted to protect data, we protected the server, we protected the computer, and we protected our printed documents by locking everything up into a safe or something else that was considered safe. But today, we need to protect not just the computer, but also our tablets, smartphones, smart watches, etc. We have a lot of devices, and those devices carry the information that we shared and care. Today, it is much more important to protect the data our devices than any other day.

We need to be sure that the devices are secure with authentication methods that will increase or will have enough control mechanisms, to protect the data. Today, we're dealing with global businesses and not a single headquarter in one city. When we say global, we are dealing with a lot of offices and a lot of places in the world. Hence, for the protection of such sensitive data, every individual of the company must be trained to prevent the loss of any important information.

As of now, almost 70% of the total world population uses the internet for doing various activities. With such enormous number of users comes great responsibility. And thus, this is where cybersecurity comes into the picture. We will further discuss about the cyber threats, its detection and prevention measures.

2. THREATS, DETECTION AND PREVENTION

Cyber security can be defined as the body of technologies, processes, and practices designed to protect devices, networks, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology (IT) security.

Cyber security is the most vital field for the protection of data. The data or information which is being transmitted via Internet may contain some sensitive data which when stolen by the attacker may prove to be a huge loss to the organization. There are many hackers who are constantly looking for the information which is very important to the organization. The main motive of the hacker is to gain money or gain access to the sysadmin's account so that attacker can do whatever he/she desires.

There is a non-profit organization called OWASP(Open Web Application Security Project) which serves opulence amount of knowledge, papers and tools to help anyone involved in designing, developing, deploying or supporting a web application to ensure security is built in from the ground up and that the overall product is as secure as it can be.

The number of data breeches and fraud activities in the US is higher than any other country. The graph below illustrates the annual number of data breaches and exposed records that took place in USA from 2005 - 2019 (in millions).

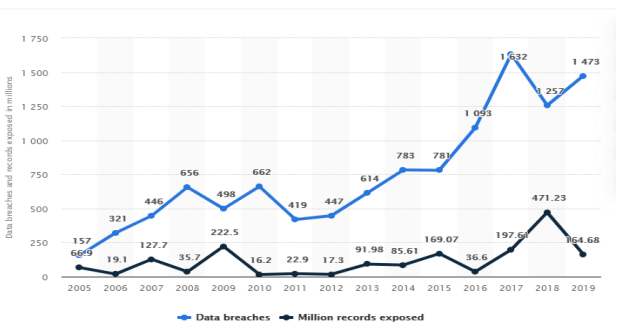

Figure 1: Annual number of data records in USA during 2005-2019 (in millions)

2.1 Trending Threats

Mentioned below are some major threats which have a great impact on the organization.

1. SQL Injection
SQL injection is a type of attack in which the malicious code is fed in to the website using Structured Query Language(SQL). After the injection of the code system will behave in an aberrant manner. A SQL injection attack targets the entire website if the website is programmed using a SQL database. Attackers can inherently run SQL commands that allow them to drop/delete website data, copy it, modify it, and run other malicious commands.

2. Cross site scripting
Cross-site scripting, or XSS attack, is a type of injection attack where the attacker can add malicious code and exploit the user of the service. XSS attacks are a frequent method to obtain a session hijacking. It would be as simple as adding a malicious script in a website, and the user unknowingly runs the script in their browser. The script could then do malicious things like steal a victims cookies, can have access to a log in to a website and can also modify the sensitive data which is useful for a victim.

3. Password attacks
Passwords are the most secure common safeguards. Unfortunately, our passwords might not be as secured as they need to be. A most ordinary attack that takes place to gain access to an account is a password attack. Password attacks utilize software like password crackers or rainbow tables that try and guess your password. A common password attack is a brute force attack, which just continuously tries different combinations of characters and letters until it gets success. Since this attack requires testing a lot of combinations of passwords, it usually takes a more time than the rainbow table attack .Another type of password attack is a dictionary attack. A dictionary attack doesn't test out brute force combinations like abc1 or ABC1. Instead, it tries out words that are most frequently used in passwords, like password, donkey, and volleyball.

4. Sensitive data Exposure
As we know that there are many small organizations or personal users who possess the sensitive data. But, this sensitive data is not being preserved properly or let say not encrypted properly which helps attackers to gain the access of the system and cause damage to the organization. Some examples of sensitive data such as Credentials, Credit card numbers, Social Security Numbers, Medical information, Personally identifiable information (PII), Other personal information.

5. Broken Access Control
A system administrator has the overall access to the every system present in the organization. Sometimes, a bad guy (attacker) tricks the system admin and gains the access of the sysadmin's system and further can change the settings of the whole working of the organization. Hence, this is known as Broken Access. For an example if a third party is given an access to the software he/she may change the configuration of the software which can result to the loss of huge data. Examples of Broken Access are Access to a hosting control / administrative panel, Access to a server via FTP / SFTP / SSH, Access to a website's administrative panel, Access to other applications on your server, Access to a database.

6. Using Components With Known Vulnerabilities
There are many software or hardware devices which we don't update at regular intervals. Therefore, when we don't update our devices it may lead to some vulnerability which is not known by the user but it is known to the attacker. And hence, the attacker exploits that vulnerability and gains the access to the remote system. Sometimes the sysadmin willingly does not update the software/hardware claiming that it might happen that software won't work or some vulnerability will born. Thus, the advantage of such situations is being taken by the attackers.

7. DNS Cache Poisoning Attack
As we have studied that DNS works by getting information about IP addresses and names to make it easier for us to find a website. A DNS Cache Poisoning attack works by misleading a DNS server to accept a fake DNS record that will point victim to a compromised DNS server. It then gives you the fake DNS address when you try to ingress legitimate websites.

8. Rogue Access Point Attack
A rogue AP is an access point that is installed on the network without known to the network administrator. Sometimes, in corporate world, someone may plug a network router into their corporate network to create a simple wireless network to gain high speed or for any other trivial reasons. Sounds innocent, right? Wrong. This can actually be pretty dangerous, and could allow unauthorized access to an authorized secure network. Instead of an attacker having to gain access to a network by plugging directly into a network port, they can just stand outside the office and can easily navigate through your wireless network.

9. Evil twin Attack
Evil Twin Attack is similar to the rogue AP attack but has a small but important difference. The main aim of an evil twin attack is for a victim to connect to a network that is identical to victim's network. This identical network is the network of evil twin and is controlled by attacker. Once a victim connects, attackers are able to monitor sufferer's traffic.

10. Denial of Service (DOS) Attack
A Denial-of-Service, or DoS attack, is an attack that tries to prevent access to a service for legitimate users by overwhelming the network or server. DoS attacks try to take up resources of a service, and prevent legitimate users from accessing it.

The Ping of Death or POD, is a simple example of a DoS attack. It works by sending a malformed ping to a computer. The ping would be so huge in size that the internet protocol cannot handle it. Thus results in a buffer overflow. This can make the system vulnerable and potentially allow the execution of malicious code. Another example is a ping flood, which sends tons of ping packets to a system. More specifically, it sends ICMP echo requests, since a ping expects an equal number of ICMP echo replies. If a computer can't keep up with this, then it's prone to being overwhelmed and taken down.

OWASP TOP 10 - 2013 (New)
A1 - Injection
A2 - Broken Authentication and Session Management
A3 - Cross-Site Scripting (XSS)
A4 - Insecure Direct Object References
A5 - Security Misconfiguration
A6 - Sensitive Data Exposure
A7 - Missing Function Level Access Control
A8 - Cross-Site Request Forgery (CSRF)
A9 - Using Known Vulnerable Components
A10 - Invalidated Redirects and Forwards

Table 1: Top 10 cyber threats in the year 2013

2.2 Threat Detection

Some of the threat detection methods are as follows:

1. Cloud access and security brokers (CASB)
As we know that in today's modern generation we are using cloud services for many purposes. The main purpose of using cloud services if for storage of large amount of information. Cloud access and security brokers (CASB) technology helps to detect the unauthorized entry to cloud applications. It can easily view the cloud access patterns which help to find the attacker, when an attack occurs.

2. Endpoint detection and response
Endpoint detection and response mainly deals with the combination of collection of endpoint data and real-time continuous monitoring. Further analyses these patterns to detect the threat that might occur. If threat detection is successful then it will automatically respond and delete that threat or will inform the security personnel.

3. Intrusion detection systems
Intrusion can also be referred to as threat. Intrusion detection systems are the type of software or application which is able to detect the threats by monitoring network traffic. It can easily detect the malicious activity that takes place in network by monitoring the traffic. Limitation of IDSs is that they cannot detect endpoint or cloud based threats.

4. Network Firewalls
Firewalls can be defined as the physical or virtual application which acts as a safeguard by inspecting every packet which comes from the external network. There are two main types of firewalls stateful and stateless firewalls. Stateless firewalls are only meant to detect invalid packets whereas stateful firewalls are able to detect as well as discard the packet which subsumes malicious information.

5. Log files
Log files are the files which contain the information about every packet that is being passed from our network to the external network or vice-versa. A security personnel can view the files for the threat detection.

6. Threat Intelligence Platforms
Threat Intelligence Platforms are the platform where the information of previous attacks or threats that damaged the system is maintained. Hence if any threat is detected on the system, a user can easily know what kind of threat it is and can also judge which part of the system is going to be compromised.

2.3 Threat Prevention

Here are some of the frequent threat prevention techniques which can mitigate the risk of threats caused to a system:

1. Regular Backups
There are various kinds of information such as personal information, sensitive information, trivial information, credential details, etc. Backup of the most important data must be carried out at regular interval of time. So, if the sensitive data gets compromised it can be reverted back with the help of backups maintained.

2. Auditing and Logging
A security personnel must always maintain the log information and do auditing on the regular basis. This will help to prevent the attack by monitoring the traffic in the network. There are mainly two types of software called tcpdump and Wireshark which helps the security personnel to analyze the packets for threat prevention.

3. Intrusion Prevention Systems
Intrusion Prevention Systems are the type of appliance or software that helps to detect the threat and also to prevent the threat causing a attack by discarding the suspicious IP packets.

4. Disk Encryption
Disk Encryption is a mechanism of the encrypting the disk containing the most valuable data of the organization. Let us suppose there is an internal attacker which tries to steal the physical disk, but further the attacker would need the encryption key to decrypt it and access the information contained in it.

5. To Prevent Injection Attacks
The best way to prevent the XSS or SQL injection attacks is to use safe APIs. Another way to prevent such attacks is using

input validations. We can use LIMIT and other SQL commands within queries to mitigate mass disclosure of records in case of SQL injection.

6. Passwords
A user must be made aware of using long passwords rather than short passwords which is easily vulnerable. Minimum length of the password must be 8 characters long and it must contain combination of a char symbol, capital letter, small letter and numbers. By setting such passwords it is very difficult for the hacker to decode the password by brute force or using Rainbow tables.

7. Hashing
Hashing is a technique which is used to encrypt the information using algebraic functions which makes the data inaccessible for the attackers. There are various hashing algorithms such as MD5 , SHA, etc. Advance level of hashing can be made by using of salt i.e using equal number of characters on the end or front of the message, which is to be transmitted via insecure channel.

8. Access Control Lists (ACLs)
Access Control Lists are the lists of the employees of the organization which are able to access the particular information based on their job role. Access Control Lists can prevent the internal attacker from the data being exploited. Hence, it is necessary to maintain the Access Control Lists by the system administrator.

9. Use of safe LINUX commands
There are various kinds of LINUX commands which the user feels safe but can give a birth to new vulnerabilities causing a damage to the system. For example, Never login directly as root unless necessary. Use "sudo" to execute commands. sudo are specified in /etc/sudoers file also can be edited with the "visudo" utility which opens in VI editor. This could be a good advantage for an attacker to gain the access of your linux machine.[1]

10. Antivirus
Antivirus is a software which keeps the information about the threats and which when detected can easily destroy them. Hence, antivirus must be kept updated because in cyber world there are many new attacks are being emerging. Therefore, to detect and prevent such new attacks it is recommended that we must update our antivirus software regularly.

3. CONCLUSION

Cyber security is vast topic. We encountered the most frequent attacks, its detection and its prevention techniques. As the number of cyber threats are increasing day by day and every year many companies or organizations gets affected due to poor knowledge of their employees. Hence, it is necessary to provide knowledge about the threats and proper training to the employees. We cannot stop the cyber-crimes completely but we can mitigate it by applying different strategic efforts which may cause less damage to the organizations.

REFERENCES

1. Razzaq, Abdul, et al. "Cyber security: Threats, reasons, challenges, methodologies and state of the art solutions for industrial applications. "Autonomous Decentralized Systems (ISADS), 2013 IEEE Eleventh International Symposium on. IEEE, 2013.

2. Byres, Eric, and Justin Lowe. "The myths and facts behind cyber security risks for industrial control systems." Proceedings of the VDE Kongress. Vol. 116. 2004.

3. "Common Cyber Attacks: Reducing The Impact Gov.uk", https://www.gov.uk/...data/.../Common_Cyber_Attacks-Reducing_The_Impact.pd

4. "Cyber security: risks, vulnerabilities and countermeasures to prevent social Engineering attacks", International Journal of Advanced Computer Research, Vol 6(23) ISSN (Print): 2249-7277, ISSN (Online): 2277-7970 http://dx.doi.org/10.19101/IJACR.2016.623006

5. Ten, Chee-Wooi, Chen-Ching Liu, and Govindarasu Manimaran. "Vulnerability assessment of cyber security for SCADA systems." IEEE Transactions on Power Systems 23.4 (2008): 1836-1846.

6. "Cyber Crime-Its Types, Analysis and Prevention Techniques", Volume 6, Issue 5, May 2016, ISSN: 2277 128X (www.ijarcsse.com)

[1] Cyber Security: Understanding Cyber Crimes- Sunit Belapure Nina Godbole

[2] Computer Security Practices in Non Profit Organisations – A NetAction Report by Audrie Krause.