ISSN No:-2456-2165

Investigation on Data Security Threats & Solutions

B P Patil
Nowrosjee Wadia College, Pune, India

K G Kharade
Assistant Professor, Department of Computer Science
Shivaji University, Kolhapur, India

R K Kamat
Professor, Department of Electronics
Shivaji University, Kolhapur, India

Abstract:- Data security is now became major concern for companies, organizations, government authorities and even personal users also. Data security is basically prevention of data from being misused by unauthorised parties for fraud. In other words, it means keeping users personal, financial, confidential information safely, so no one can access it. Moreover, there are many ways by which data loss can occur, accidental deletion, computer virus attack, system failure, natural calamities, etc. Knowing these ways data loss can helps to prevent data from data loss. The network structure itself has some vulnerabilities by which attacker can access user's data. To secure data user should first know about how data can be lost. There are simple ways that can be undertaken to remain secured at all time in cyber world, which we are going to discuss in this article.

Keywords:- *Cyber Security, Data Loss, Hacking, Malware.*

I. INTRODUCTION

A massive amount of data is being created with every passing second. The rate of data creation is growing faster than even before. As per the study, about 90% of data has been created in last two years than the entire previous history of human data creation. By 2020, about 1.7 megabytes of new data will be generated every second for every human being that means total amount of data in world will 44 Zettabytes. In simple words, one zettabyte is equal to one trillion gigabytes. This huge amount of data is critical for businesses as well as personal users, making lucrative to attackers.

Data is valuable whether it is contact details, financial details, payment details, private pictures & videos or any other sensitive information. This data needs to be stored properly and securely. The term Cybersecurity knocked up in year 1988 when the first ever online virus: Morris Worm was registered. This worm slowed down many computers which connected to the internet until they becomes unusable.

As cyberattacks are growing day by day users must know about how they function and how to secure data from attacks before they could damage/steal user's data and misuse it.

II. DATA GENERATION STEPS

Data is defined as collection of facts and figures which represents ideas or object. Data can be in form of characters, symbols, numbers and pictures.

Data can be generated explicitly and implicitly:-

- *Explicit Data:* The information provided intentionally and purposefully is called explicit data. Creating user account, saving contact details, credit card details etc. are examples of explicit data.
- *Implicit Data:* The information provided unintentionally and unknowingly is called implicit data. Leaving browser history uncleared, leaving transaction receipts at public places, call logs on mobile phones, details of last login on computers, etc. are some of the examples of implicit data.

A. Secure Data

There are few things that should be kept in mind to prevent data from loss or theft. They are

- *Confidentiality*

Confidentiality means only authorised users can access to particular data. For example, only bank account holder can access his bank transaction details.

- *Authenticity*

Authenticity is nothing but a verification of a data which is not modified or changed during data sharing. For example, if a user receives email containing his bank details as an attachment, it must be coming from his bank only. And if any other source sends same attachment it can't be considered authentic.

- *Integrity*

Integrity is accuracy, reliability and originality of the data. If a user receives incomplete, incorrect data that can be harmful to user. For example, if a customer receives more amount of bill than he bought things from store, then it shows that the database of store is corrupted.

B. Implementation of Data Security

To reduce risk of data loss user should follow three steps,

- *Precaution*

Precaution means action taken before any data loss. Which contains installing a strong antivirus in a system to detect any malicious things, keeping windows firewall on, using strong password (consists of uppercase and lower

case letters, numbers, special symbols), download the data from trusted websites only, etc.

➢ *Maintenance*

Maintenance means keeping device or system up-to-date regularly. Which includes taking backup of data regularly, update antivirus and firewall regularly, deleting unwanted memory (browser cache and history), keeping system clean to prevent from overheating, etc.

➢ *Reaction*

Reaction means instantly action taken after a data breach occurs. How quickly user responds after a data breach, lowers the risk of more data loss.

It includes immediately disconnect the affected computer from network so that other computers remains safe, reinstalling all system software and application.

❖ *Network Security*

Security plays important role in preventing computer networks that are connected to many people. Data sharing between computers are based on network and it is vulnerable to hacking techniques. Due to which security of network is important to protect data from hackers and malicious activities.

In last few years there are many number of hacking attacks are increased. Moreover, many threats are being created to do hacking attacks and other malicious activities.

To create a secure network that can be free from attacks, the following things should be considered-

➢ Back up data regularly
➢ Save data on reliable hardware
➢ Keep system software up-to-date
➢ Install security certificates to stay protected from attacks
➢ Upgrade firewall with ACL, proxy and routers regularly
➢ Network Security Threats

Anything that can be harmful to computer system comes under Network Security Threat. Network security threats are of two types:

➢ *Passive Threats:*

Passive threats involves attempt by attacker on two user's communication system and stealing or getting access to data without any of the user's permission. During passive attack attacker does not changes or modifies the communication. File sharing, messaging are the examples of communication that can be monitored by attacker.

➢ *Active Threats:*

Active threats involves some changes or modification of data during communication and attempt of gaining unauthorised access to computer by attacker. In this attacker directly involves in malicious activities which user may notice. For example, ransomware attack, Data Theft, etc.

❖ *Types of Network Security Threats and Its Solutions*

There are many threats that can be done no network. Some of them are mentioned below with their security solutions:

➢ *Unauthorised Access:*

Accessing someone other's computer or network without their proper permission is unauthorised access. This is done intentionally by breaking system security measures. It is most damaging threat of network security. A hacker can access all of the data illegally and may steal confidential and sensitive data of the user.

Solution:

- Implement a strong authentication process.
- Protect login with strong password containing uppercase and lower case letters, numbers, special symbols.
- Do not share login ID and password with anyone.

➢ *Eavesdropping:*

Eavesdropping is act of monitoring user communication without permission. It can be conducted on emails, messaging, social media, calls or any other internet communication services. The aim of doing this is to gain sensitive information like password, session packets, etc. that are transferred over the network. During eavesdropping attacker intercepts packets of data sharing over an HTTP connection, modifies it and misuse it so that network may get damaged.

Solution:

- Use strong encryption policy using SSL certificates to reduce risk.
- Create network segments so that if someone attacks on system that attack will be limited only on that segment.
- Authenticate every device before connecting to the network.

➢ *DoS & DDoS:*

These treats are very difficult to detect. It makes online service unavailable by sending huge amount of traffic which server can't handle.

In Denial of Service, an attacker send a lot of requests on server which server is not capable to handle. For example, if a server can handle 100 requests per second, the attacker sends 250 requests per second. Due to which there is most chances of server getting down or inaccessible. And due to this a legitimate user request is unacceptable as there are already lot of pending requests. In DoS, attacker sends request from one source only.

A Distributed Denial of Service attacks the particular business website or machine and make its network resource unavailable to access temporarily or indefinitely disrupting services of a host connected to the internet. In DDoS, attacker sends requests from multiple sources. The main goal of doing this attack is to prevent a website from working properly and stops their functions due to website may have financial loss.

Solution:
- Regularly upgrade security patches of the server.
- Monitor the packets to save server from the entrance of harmful packets.
- Keep a response plan ready.
- Maintain strong network architecture.
- Keep look on any type of warning.

➢ *IP Spoofing:*

Attackers usually hides their identity and takes other's identity to do malicious activities. IP spoofing is most common form of hiding own IP. Act of IP spoofing to distract target computer to think that the data is he receiving is coming from trusted source(IP address). If attacker wants to hide their identity they changes the source address.

Solution:
- Use firewall on every computer on network.
- Filter data packets entering and leaving the internal network.
- Use access control list to detect any external network entries in the internal network.
- Use SSL certificates to reduce the risk.

➢ *Man-in-the-Middle Attack (MITM):*

MITM is a type of eavesdropping attack where hacker establishes a private connection with sender and receiver on which all communication between sender and receiver goes through a hacker's private connection not with the original connection they had.

Solution:
- Use strong encryption on access points.
- Use time testing techniques.
- Use VPNs.
- Use Public Key Pair based authentication.

❖ *Wireless Network Security Threats and Control Measures*

Like wired network, wireless network has its own vulnerabilities. Wired network has built-in physical security options which wireless network doesn't has. Therefore, they have more risk to get attacked.

In 21st century wireless LANs are present almost everywhere. With the growth in use of wireless networks, the number of threats has also increased. Here are the few security threats:

➢ *Rouge Wi-Fi Networks:*

In this a hacker creates a Wi-Fi networks that pretends to be genuine. And if user connects to that network then hacker can have access to all of user's communication through network.

➢ *Packet Analyser:*

It is also known as Packet Sniffers. These are small computer programs that monitors traffic on a network. They can also intercept and modify some data packages, and provide details to hacker.

➢ *Evil Twins:*

Evil twin is a wireless network access point that same as Rouge networks but it looks more legitimate than rouge networks. Hackers create Evil twins to attract the users who are looking for free Wi-Fi connections.

➢ *War Drivers:*

The act of searching unsecure Wi-Fi connection by individual in a moving way is call war driver. This is to gain unauthorized access to computers or devices on that non-secure network. This attack can be done by attacker within the range of Wi-Fi network only.

➢ *Endpoint Attacks:*

Each user present in a same network is known as endpoint. While there can be many devices in a network if hacker can access any of the endpoint using fake websites that can allows hacker to get access of device as well as all devices present in the same network.

➢ *Mishandled Wi-Fi Security Setups:*

With all advanced hacking techniques if a user does some error while securing his network or device there can be a lot of chances of getting hacked are increases. While using configuring public network it is not necessary to be ensure about security. Many employees just leaves the default user Id and password on Wi-Fi router through which hacker can access it more easily.

➢ *Soft Apps:*

It is more common that users leave there hotspots on, so when user connects to the public Wi-Fi network, hotspot makes a vulnerable way through which hackers can attack.

➢ *Threat Control Measures:*

To reduce risk of these threats following things should be kept in mind:
- *Turn off Wireless Network when it is not in use or you are away from Home:*

  This will reduce possibility of getting hacked.
- *Set up a Security Key for Network:*

  Due to which unauthorised users can't access to the network. Routers comes with default username and password that are already known to hackers and they may have access to network. Therefore it is important to change the username and password of router in regular interval of time.
- *Enable Encryption:*

  User can configure router in which user can allow access of network to only devices who enters the correct password. And by adding filter to router user can allow only trusted devices to connect the network. If an attacker got the password somehow still he can't get access to network.
- *Use Firewall:*

  Firewall gives an additional layer of security and can remarkably reduce the chance of attackers gaining access to private wireless network. It keeps logs of attempts to access of network and blocks unauthorized attempt to access the network.

❖ *Other Security Threats and its Solution*

In addition to above threats, there are many other common threats that can affect computers and may be harmful to system. These are software threats and called as Malware (Malicious Software). These are designed to steal,

damage or any illegal action on user's personal information. Following are the few common threats:

➢ *Computer Viruses and Worm:*

Virus is a program which is saved or installed on victim's computer with his permission. This program can damage computer system like slowing down computer, showing various advertises, data loss, etc. The virus can spread on entire computer network by propagating himself.

Worm is a software that increases rapidly to infect computers by replicating himself over the network. Worm creates multiple copies of himself. Due to which computer system gets slower.

Solution:
- Install a powerful antivirus which can detect any kind of these viruses and worms.
- Upgrade antivirus regularly.

➢ *Trojan Horse:*

Trojan horse is a piece of malware that contains harmful code. It is hidden inside another genuine software or file. Which installs unwittingly when user installs other software or saves file from untrusted source.

Solution:
- Download files and software's from trusted websites only.
- Use antivirus that can detect if there is any malicious attachment or not.

➢ *Spams:*

Normally spams means junk emails that are send to people without their permission. These mails contains advertisement of various services and products. Spams can do less damage to computer but it is irritating to users.

Solution:
- Use spam filters, most of the email service providers has spam filters inbuilt. Spam filter separates spam mails from important mails.
- User can also purchase spam filter to function more effectively depending on user's requirement.

➢ *Phishing:*

Phishing technique is used to obtain personal information in fraudulent manner. Which contains sending emails to people and proposing that these mails are from reputed companies or website in order to induce individuals to reveal their personal details.

Solution:
- Use phishing filters.
- Do not reveal personal information unless website has security mode.(Look for padlock icon at the left side of URL)

➢ *Maliciously Coded Websites:*

Some websites contain malicious code. When user visit these website, they may install any malicious code or Trojan horse on computer without user's permission. These websites are mainly designed to get bank details, passwords or any other sensitive information of user.

Solution:
- Use internet security antivirus which shows warning if a user tries to access malicious website.

➢ *Zombies and Botnets:*

Zombie computer is also called as bot. It is a networked computer infected by a virus or malware. Hacker controls this computer remotely and performs malicious activities. From zombie computer hacker can get access of all computers present on same network and this network of infected computer is called as Botnet. Through botnet all infected computers can remotely controlled once by hacker and performs malicious acts.

Solution:
- Use antivirus which has NIP (Network Intrusion Prevention).
- Upgrade security patches regularly.

❖ *Preparing for Unexpected Threats*

Data is valuable to organisations and companies and has importance in their business growth, if some data may loss they may have big trouble in their business. Therefore protection of data is necessary. Here are some ways by which data may be lost unexpectedly:

➢ *Human Error:*

This is biggest cause of data loss. It is bigger than any malicious activity. Deleting files unintentionally, not checking warning signs, not taking backup regularly, etc. are the examples of human error.

➢ *System Malfunction:*

System Malfunction can be in many ways, such as power failure, system defects while manufacturing, dropping accidently, etc. to avoid such things users should handle system hardware with care. Users should keep it in safe place. Use of UPS (Uninterrupted Power Supply) is useful in sudden power failure.

➢ *Hardware Theft:*

Users may leave their laptop, mobile unattended and lose it while travelling or thieves may steal devices from home. Due to which user may loss his data if proper backup is not taken.

➢ *Natural Disaster:*

Natural disaster like cyclones, floods, earthquake, fire can be harmful to the data. The best way of keeping data secured against natural disaster is storing data securely on cloud storage.

➢ *Water Damage:*

Users use their portable devices such as mobiles and laptop carelessly. So that spilling drinks on electronic devices have become more frequently. Electronic devices may not have any covers to safeguard its internal parts, so any liquid can damage these devices more easily.

➢ *Software Crash:*

If an operating system is not properly installed by user, system has more chances to get crashed or not

working properly. In this case user can't operate computer neatly and may not have proper access to their data.

❖ *Data Backup and its Need*

Data backup is basically a process of securing important data in any other external source data storage. If in case, original data is damaged due to some threats these backed up data can be used and it will not hurt to user. User should keep their duplicate copy of data in external hard drives, USB drives, CD/DVD or cloud. The main intention of data backup is to be able to restore data easily in case of any of the data loss threats.

With the huge amount of data creating everywhere every day, data is very important to businesses as well as individuals also. Due to all vulnerabilities in network chances of data loss can takes place any time and if this occurs user may be in big trouble. Physical security is the key to safe and confidential data.

Data backup is time consuming and requires lot of storage space. Therefore, user should know which data is important that only should be backed up. Backing up unimportant data will costs user more as well as user have to give more time to backup. By knowing the frequency of change of data user can determine in how much interval of time he should backup his data. For example, if data is changes weekly, then it should be backed up weekly. There is no need of data backup daily. User should backup his data incrementally. There is no need of taking full backup of data every time. Due to which less storage space will be required for data backup.

III. CONCLUSION

Computer security endeavours to guarantee the privacy, trustworthiness, and accessibility of processing and their components. Usually, Software, Hardware, and Data are the most important components of computer science. To secure the data in the computer system, the user must have taken the utmost care to prevent it from the intruders. Proper knowledge of data security can prevent the user from being victim of the intruder. In this paper we have mentioned various techniques to keep the data safe and secure

REFERENCES

[1]. Daya, B. (n.d.). Network Security: History, Importance, and Future. *Network-Security-article*.
[2]. Dobran, B. (2018, 09 10). *7 Tactics To Prevent DDoS Attacks & Keep Your Website Safe*. Retrieved from https://phoenixnap.com/: https://phoenixnap.com/blog/prevent-ddos-attacks
[3]. Gollmann, D. (n.d.). Computer Security 3e. *Computer Security 3e*.
[4]. Jonas, M. (2018, 10 10). *10 Public Wi-Fi Security Threats You Need to Know*. Retrieved from https://www.safervpn.com/: https://www.safervpn.com/blog/10-public-wi-fi-security-threats/
[5]. *Network Security Threats: 5 Ways to Protect Yourself*. (n.d.). Retrieved from https://www.theamegroup.com/: https://www.theamegroup.com/network-security-threats/
[6]. Safe BACKUP Consult Ltd. (n.d.). *7 Greatest Causes of Data Loss*. Retrieved from www.databackuponlinestorage.com/: https://www.databackuponlinestorage.com/7_Causes_of_Data_Loss
[7]. Star Certification. (n.d.). *Star Cyber Secure User*.