Information Security and Network Security

Chapter – 2

Threats and attacks Modes

Information systems security is the integrity and safety as its resources and activities. In cyber world it can be almost impossible to trace sophisticated attacks to their true source.

Need for Security

- New Technologies open door to the threats
- e-business increases online threats
- use of integrated of technologies such as networks of computers company intranet or internet access to communicate and transmit information for rapid business decisions which opens organization to the external world.
- Threats from outside the organization must be addressed becomes the damages from non-secured information system can result in catastrophic consequences for the organization.

Information -level Threats vs network level Threats

A threat is possible event that can harm an information system. Information level threats are threats that involve the (purposeful) dissemination in such a way that organizations their operation and their repetitions may be affected.

N/W based threats we mean that in order to become effective potent as attackers require network access to corporate computer systems to networks used by corporate computer systems. e.g. sending fake inquiries to service accounts.

Revenge website

Information systems security- Threats and attacks

Security Threats have four principle sources that include

1. Human error: e.g. Inadvertent (accidently) disclosure of confident as information.
2. Computer abuse (misuse) or crime e.g. person intends to be malicious (intended to do harm) and starts to steal information from sites or cause damage to a computer or computer network. An internet-based computer fraud can happen.
3. Natural and political disasters this can happen in the form of natural calamities and wars, riots etc.
4. Failures of hardware or software server manufacturing software errors etc.

Security Threats or Attack Modes

Related (misuse) to computer crime or abuse include:

1. **Impersonation** – An act of pretending to be another person/user for the purpose of fraud. Attackers poses as a known or trusted person to dupe an employee into transferring money to fraudulent account, sharing sensitive information (Such as intellectual property, financial data or payroll information), or revealing login credentials that attackers used to hack into a company's computer network.

   Stopping an impersonation attack requires strong security policies and vigilance on the part of employees. But these attacks are designed to take advantage of human error.
2. **Trojan horse method** – Concealing within an authorized program a set of instructions that will cause unauthorized actions. A computer program that appears to have useful function, but also has hidden and potentially malicious function that evades security mechanisms, sometimes by exploring legitimate authorizations of a system entity that invokes the program.
3. **Logic Bomb** - unauthorized instruction often introduced with the trojan horse technique its program downloaded and installed on a computer the appears harmless but is in fact malicious. It is type of malware that contains malicious code that is discreetly installed into software, a computer network, or an operating system with goal of causing harm to a network when certain conditions met.
4. **Computer Viruses** - segments of code that are able to perform malicious acts and insert copies of themselves into other program in the systems and onto the diskettes placed in the computer.
5. **DOS** (Denial of Service) - Rendering the system unusable by legitimate users. Attack meant to shutdown (legal/ valid) a machine or network making it inaccessible to its uses. Dos attacks often target web servers of high – profile.

   Denial of service (DOS) can be carried out by:

   - Starting a number of programs on computer or server simultaneously.
   - Overloading a network by consuming a disproportionately large amount of bandwidth
   - Continuously pinging a server
   - Over loading server with many server applications some vulnerabilities that aid the threat of Dos are
   - Lack of firewall

- Inadequate network administration personnel with malicious intents.

6. **Dial Diding** – Changing data before or during input often to change the contents of a data base. It is done by data entry operator or computer virus.
7. **Salami Technique** – Diverting small amounts of money from a large number of accounts maintained by the system. It occurs when an attacker uses an online database to obtain customer information, such as bank/ credit card details. Over time, over the time, the attacker deducts insignificant amounts from each account.
8. **Spoofing** – Configuring a computer system to masquerade (Rules show) as another system over the network in order to gain unauthorized access to the resources the system being mimicked is entitled. Attack that appears like a legitimate one that traps people to fall into their hands and gives way to steal information or data.
9. **Super – Zopping** – using a system's program that can by parts regular system controls to perform unauthorized acts. The term derived from super zap program, valuable program developed by IBM which allowed mainframe computer administrators to override normal security measures in way to respond to any emergency. Illegal use of super zap programs can result in alteration of data files that are generally updated only by manufacturers programs.
10. **Scavenging** – unauthorized access to information by searching through the residue after a job has been run on a computer. Techniques range from searching waste baskets or dumpsters (large container for rubbish) for printouts to scanning the contents of a computer's memory.
11. **Data leakage** – there are a variety of methods for obtaining the data stored in a system. The data may be encoded into an innocuous (Offensive/ not harmful) report in sophisticated ways e.g. as the number of characters per line**.**
12. **Wiretapping -** tapping computer TC wines to obtain information
13. **Theft of mobile devices -** This is a new dimension that is coming up scaring the increase in mobile work force.
14. **Application attacks** – consists of cyber criminals gains access start with application layer hunting for applications where availabilities written with code. Attacks target certain programming languages.
15. **Web Application attack** serious weakness or vulnerabilities allow criminal to gain daren't and public access to database in order to churn sensitive data many at these data bases contain valuable

information (e.g. personal data and financial details) making them frequent target of attacks websites depends on database to deliver the required information to visitors

16. **Malware attacks** – Can cause significant damage to organizations and their employees.

- Malware attacks can exfiltrate (Unauthorized transfer of information) sensitive data such as email addresses, passwords and other business assets.
- Look up organizations network's and PC's making them in operable.
- Cause operational issue like disrupted productivity and catastrophic (consume sudden great damage) data loss.
- Encrypt information that can be opened by key known only by the attackers it is also called ransomware attack Attacker demand for money to give key.
- Compromise the confidentiality integrity or availability of organizations data and assets.

17. Clickjacking – The malicious (intended to do harm) practice of marinating a website user's activity by concealing (wide) hyperlinks beneath legitimate while content there by causing the user to perform actions of which they are unaware.
18. Email spoofing- It threat that involve sending email messages with take sender address. E-mail protocols cannot on their own authenticate the source of an email. Email spoofing takes advantage of fact that email, in many ways, is not very different from regular email.

    Each email has three elements an envelope a message header message body. An email spoofer puts whatever they want into each of those fields, not just the body and to: fields. When the email hits target inbox the email program reads What is in these fields and generates what the end -reader sees. If certain information is entered in the right fields what they see will be different from what is real, such as from where the email originated. In some attacks the target in thoroughly researched enabling attackers to add specific details and use the right wording to make the attack more successful.

    Email spoofing protection. Use antimalware software. Send emails writing subdomain. E.g. use help your company .com instead of your company .com

    Use email signing certificates to protect outgoing emails.
19. Eavesdropping –

    Eavesdropping or stiffing is process of accessing in a network by using certain software. An attacker through eavesdropping can capture data and misuses it. This threats the integrity,

availability and confidentiality of data. Some vulnerabilities that avoid the threat of eavesdropping are

- Lack of physical security over data communications closets of hubs.
- Leaving confidential information such as login password, in open.
- Leaving the system that has sensitive data unlocked.
- Sending data over the network in an unencrypted form.

❖ Some of the above-mentioned crime techniques may be used for a direct gain of industrial espionage curing spices while yet others simply for destructive purpose.

❖ Computer viruses –

A computer virus is a piece of program code that attacks copies of itself to other programs and thus replicates itself.

❖ Characteristics of computer viruses

1. The attacked program may work properly but at some point, will perform a malicious or destructive act intended by the attacker who has written by the attacker who has written the virus.
2. Viruses are best known for their rapid spread in performed computer environment they proliferated (multiply- in- crease rapidly in numbers)
3. Through infected diskettes or programs downloaded from the internet or other networks.
4. Two principal types of viruses are boot infectors and program infectors. The boot infectors replace the content of the first sector of the diskettes or hard disk. Program infectors copy themselves into extendable files stored on the hard disk.

Classification of threats and assessing damages –

Threats is an indication of a potential undesirable event. Threats consist of the following properties –

1. Asset – something of value to the organization.
2. Actor who or what may volute the security requirements CIA of an asset. Actors can be from inside or outside the organization.
3. Motive (optional) – indication of whether the actor's information is deliberate or accidental
4. Access (Optional) – how the asset will be accessed by the actor (n/w access or physical access)

The major categories of damages resenting from threats to IS are

- Destruction of information and /or other resources
- Theft, removal or loss of information and/or other resources

- Insources of information (confidential data)
- Mobilizational of important or sensitive information
- Interruption of access to important information software, application or services. Prior to assessing damage (caused by security incidents) use need to identity assets.

  Categories of logical and physical assets.

1. Information – Documented (paper or electronic) data or intellectual property used to meet the mission of an organization.
2. Software – Show application services that process store or transit information.
3. Hardware – Its physical devices considering their replacement costs.
4. People – the people in an organization who process skills, competencies, knowledge and experience that are difficult to replace.
5. System – Is that process and store information.

Protecting information systems security - The aim of information systems securing is to protect corporate assets or at lease to limit their loss.

Good infuses starts with threat modes- what the system is designed to protect, from whole and for how long.

Information systems controls play important role ensure secure operations of IS and thus to safeguard assets and the data stored in these systems.

Information systems controls are classified as follows –

1. Preventive controls prevent an error omission or unauthorized intrusion.
2. Defective controls – detect violation These controls exist to detect and report when errors, omissions and unauthorized of entry occur.
3. Corrective controls – Defect and correct an exceptional situation.

   These controls are designed to correct errors, omissions and unauthorized users and instructions once they are classified as:

   1. General controls – controls applying to the entire is activity in the organization
   2. Application controls – controls that are specific to a given application controls are employed at application security layer.