DOMS | Page No.
Date / /

Some Important terms :

- **Piggybacking:** It refers to a situation where an unauthorized party gains access to some system in connection with an authorized party. This can happen in several ways, including piggybacking on public wireless networks and piggybacking into a password protected system. One primary type of piggybacking deals with a user session. If an authorized user enters a password and initiates the use session, and then steps away from the workstation, an unauthorized party can get access.

Eavesdropping Attacks :

Eavesdropping is secretly listening to a conversation you shouldn't be part of. Businesses and individuals who want to protect their conversation should actively look to improve their security. Eavesdropping attacks can occur in various forms, targeting different communication channels such as phone calls, text messages, emails, instant messages or even physical conversations. This knowledge can then be used later for a wide range of purposes such as

demanding a ransom, disrupting operational activity or selling it to competitors.

Eavesdropping Methods :
Physical, on-premise eavesdropping devices & transmission links
These can be anything like secret microphones placed inside a telephone receiver for recording, devices hidden within the room. To get these devices in place, the hacker must have physical access to the premises to install them. Criminals will install these in unsuspecting areas such as inside a book on a bookcase, behind a picture frame, inside phone handsets. Other devices, known as transmission links, operate on a similar basis. However, they utilize existing communication channels. Instead of installing the device or bug itself, the hacker will intercept telephone lines and other links to listen the conversation.

Listening Post : Eavesdropping attacks may also make use of something called a listening post. These stations are placed near the victim to monitor and process the information collected through eavesdropping devices and transmission links. When a telephone is picked up to make or take a

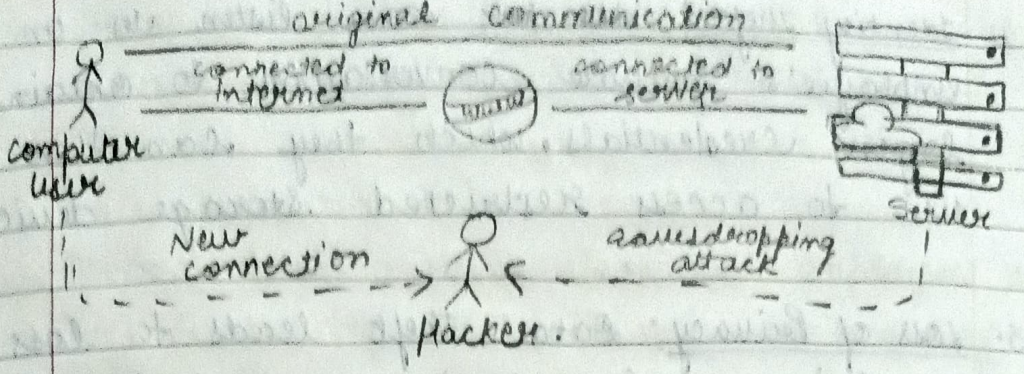
call, it triggers a recorder that is automatically turned off when the call is ended.

Weak Passwords: Weak passwords make it easier for attackers to gain access of users account, which gave them a route into corporate systems & networks. This include hackers being able to compromise confidential communication channels, intercept activities and conversations between colleagues, and steal sensitive or valuable business data.

Open Networks: Users who connect to open networks that do not require passwords & do not use encryption to transmit data, provide an ideal situation for attackers to eavesdrop. Hackers can monitor user activities that take place on the network. Alternatively, cyber security hackers can carry out eavesdropping attack if a user has connected to an unsecured network. These networks are usually in cafes, public transport and other communal places. The hacker is free to monitor any information passed through communication channels over the unsecured network.

Eavesdropping Attack

2015 | Page No. | Date / /



How can an eavesdropping attack hurt your business?

Eavesdropping attacks can result in the loss of critical business information, users privacy being intercepted and lead to wider attacks & identity theft.

A good example of the impact eavesdropping attacks can have increasing use of digital assistants like Amazon Alexa & Google Home. These assistants make users lives easier but also easy for attackers to eavesdrop on and gain private information.

The impact of eavesdropping can include:

- Financial loss: Attackers with sensitive data can access critical business applications anytime They can threaten to reveal the information unless the victim pays a large sum or sells it to competitors.

2. Identity Theft: Attacker can listen in on any employee's private conversation to obtain login credentials, which they can then use to access restricted storage devices.

3. Loss of Privacy: Data theft leads to loss of privacy for businesses and people working in the organization. The attacker can intercept important business information and conversations by injecting an eavesdropping attack on cell phones that causes privacy loss for businesses.

How to prevent Eavesdropping Attacks

The increasingly digital world makes it easier for hackers to intercept corporate information & user conversations. However, it also presents opportunities for organizations to prevent attacker malicious intent. Common methods that help to prevent eavesdropping attacks include:

1. Military grade encryption: One of the best ways to prevent eavesdropping attacks is to encrypt data in transmission & private conversations. Encryption blocks attackers ability to read data & exchange between two parties. For eg. military

grade encryption provides 256-bit encryption which is impossible for an attacker to decode.

2. Spread Awareness: Ensuring that employees are aware of the risks & dangers. Cybersecurity is a crucial first line in protecting organizations from any cyberattack. Organizations must provide training that how the attackers launch their attack. Employees need to understand the methods that attackers use to listen the conversations, follow best practices to limit the risk. They should also avoid downloading insecure applications or Software & never connect to weak or open networks.

3. Network Segmentation: Organizations can limit the possibilities of attackers eavesdropping on networks by restricting their availability. Network segmentation enables organizations to limit resources to only the people that require access to them. For eg. people on a marketing team do not require access to HR Systems & people on the IT team do not need to view financial information.

4 Avoid Shady links: Related to awareness is the need to avoid shady or untrusted links. Eavesdropping attackers can spread malicious software that includes eavesdropping malware through shady links. Users should only download official software from trusted resources.

5. Update & Patch Software: Attackers can also exploit vulnerabilities in software to target organizations & users. This makes it crucial to turn on automatic updates & ensure all software is patched immediately as a new release or update is available.

6. Physical Security: Organizations can also protect their data & users through physical security measures in their office spaces. This is crucial to protecting the office from unauthorized people who may drop physical bugs on desks, phones & more.

Muskan

Operational and organizational Security Policies, Procedure, standards, guidelines:

Policies are high-level, broad statements of what the organization wants to accomplish. They are made by management when laying out the organization's position on some issue. Procedures are the step-by-step instructions on how to implement policies in the organization. They describe exactly how employees are expected to act in a given situation or to accomplish a specific task. Standards are mandatory elements regarding the implementation of a policy. They are accepted specifications that provide specific details on how a policy is to be enforced. Some standards are externally driven. Regulations for banking and financial institutions, for example, require certain security measures be taken by law. Other standards may be set by the organization to meet its own security goals. Guidelines are recommendations relating to a policy. The key term in this case is recommendations—guidelines are not mandatory steps.

These documents guide how security will be implemented in the organization:

Policies: High-level, broad statements of what the organization wants to accomplish

Procedures :Step-by-step instructions on how to implement the policies

Standards :Mandatory elements regarding the implementation of a policy

guidlines

Standards : Recommendations relating to a policy. Guidelines

This operational process and policy lifecycle roughly consist of four steps in relation to your security policies and solutions: 1. Plan (adjust) for security in your organization. 2. Implement the plans. 3. Monitor the implementation. 4. Evaluate the effectiveness.

Security Policies

In keeping with the high-level nature of policies, the security policy is a high-level statement produced by senior management that outlines both what security means to the organization and the organization's goals for security. The main security policy can then be broken down into additional policies that cover specific topics. Statements such as "this organization will exercise the principle of least access in

its handling of client information" would be an example of a security policy. The security policy can also describe how security is to be handled from an organizational point of view (such as describing which office and corporate officer or manager oversees the organization's security program). In addition to policies related to access control, the organization's security policy should include the specific policies described in the next sections. All policies should be reviewed on a regular basis and updated as needed. Generally, policies should be updated less frequently than the procedures that implement them, since the high-level goals will not change as often as the environment in which they must be implemented. All policies should be reviewed by the organization's legal counsel, and a plan should be outlined that describes how the organization will ensure that employees will be made aware of the policies. Policies can also be made stronger by including references to the authority who made the policy (whether this policy comes from the CEO or is a department-level policy, for example) and references to any laws or regulations that are applicable to the specific policy and environment.

Change Management Policy :

The purpose of change management is to ensure proper procedures are followed when modifications to the IT infrastructure are made. These modifications can be prompted by a number of different events, including new legislation, updated versions of software or hardware, implementation of new software or hardware, or improvements to the infrastructure. The term "management" implies that this process should be controlled in some systematic way, and that is indeed the purpose. Changes to the infrastructure might have a detrimental impact on operations. New versions of operating systems or application software might be incompatible with other software or hardware the organization is using. Without a process to manage the change, an organization might suddenly find itself unable to conduct business. A change management process should include various stages, including a method to request a change to the infrastructure, a review and approval process for the request, an examination of the consequences of the change, resolution (or mitigation) of any detrimental effects the change might incur, implementation of the change, and documentation of the process as it related to the change.

Data Policies :

System integration with third parties frequently involves the sharing of data. Data can be shared for the purpose of processing or storage. Control over data is a significant issue in third-party relationships. There are numerous questions that need to be addressed. The question of who owns the data, both the data shared with third parties and subsequent data developed as part of the relationship, is an issue that needs to be established.

Data Ownership:

Data requires a data owner. Data ownership roles for all data elements need to be defined in the business. Data ownership is a business function, where the requirements for security, privacy, retention, and other business functions must be established. Not all data requires the same handling restrictions, but all data requires these characteristics to be defined. This is the responsibility of the data owner.

Unauthorized Data Sharing :

Unauthorized data sharing can be a significant issue, and in today's world, data has value and is frequently used for secondary purposes. Ensuring that all parties in the relationship understand the data-sharing requirements is an important prerequisite. Equally important is ensuring that all parties understand the security requirements of shared data.

Data Backups :

Data ownership requirements include backup responsibilities. Data backup requirements include determining the level of backup, restore objectives, and level of protection requirements. These can be defined by the data owner and then executed by operational IT personnel. Determining the backup responsibilities and developing the necessary operational procedures to ensure that adequate backups occur are important security elements.

Classification of Information:

A key component of IT security is the protection of the information processed and stored on the computer systems and network. Organizations deal with many different types of information, and they need to recognize that not all information

is of equal importance or sensitivity. This requires classification of information into various categories, each with its own requirements for its handling. Factors that affect the classification of specific information include its value to the organization (what will be the impact to the organization if it loses this information?), its age, and laws or regulations that govern its protection. The most widely known system of classification of information is that implemented by the U.S. government (including the military), which classifies information into categories such as Confidential, Secret, and Top Secret. Businesses have similar desires to protect information and often use categories such as Publicly Releasable, Proprietary, Company Confidential, and For Internal Use Only. Each policy for the classification of information should describe how it should be protected, who may have access to it, who has the authority to release it and how, and how it should be destroyed. All employees of the organization should be trained in the procedures for handling the information that they are authorized to access. Discretionary and mandatory access control techniques use classifications as a method to identify who may have access to what resource.

Data Labeling, Handling, and Disposal:

Effective data classification programs include data labeling, which enables personnel working with the data to know whether it is sensitive and to understand the levels of protection required. When the data is inside an information processing system, the protections should be designed into the system. But when the data leaves this cocoon of protection, whether by printing, downloading, or copying, it becomes necessary to ensure continued protection by other means. This is where data labeling assists users in fulfilling their responsibilities. Training to ensure that labeling occurs and that it is used and followed is important for users whose roles can be impacted by this material. Training plays an important role in ensuring proper data handling and disposal. Personnel are intimately involved in several specific tasks associated with data handling and data destruction/disposal and, if properly trained, can act as a security control. Untrained or inadequately trained personnel will not be a productive security control and, in fact, can be a source of potential compromise.

Need to Know:

Another common security principle is that of need to know, which goes hand-in-hand with least privilege. The guiding factor here is that each individual in the organization is supplied with only the absolute minimum amount of information and privileges he or she needs to perform their work tasks. To obtain access to any piece of information, the individual must have a justified need to know. A policy spelling out these two principles as guiding philosophies for the organization should be created. The policy should also address who in the organization can grant access to information and who can assign privileges to employee.

Disposal and Destruction Policy:

Many potential intruders have learned the value of dumpster diving. An organization must be concerned about not only paper trash and discarded objects, but also the information stored on discarded objects such as computers. Several government organizations have been embarrassed when old computers sold to salvagers proved to contain sensitive documents on their hard drives. It is critical for every organization to have a strong disposal and destruction policy and related procedures. Important papers should be shredded, and important in this case means anything that might be useful to a potential intruder. It is amazing what intruders can do with what appear to be innocent pieces of information. Before magnetic storage media (such as disks or tapes) is discarded in the trash or sold for salvage, it should have all files deleted, and should be overwritten at least three times with all 1's, all 0's, and then random characters. Commercial products are available to destroy files using this process. It is not sufficient simply to delete all files and leave it at that, since the deletion process affects only the pointers to where the files are stored and doesn't actually get rid of all the bits in the file. This is why it is possible to "undelete" files and recover them after they have been deleted. A safer method for destroying files from a storage device is to destroy the data magnetically, using a strong magnetic field to degauss the media. This effectively destroys all data on the media. Several commercial degaussers are available for this purpose. Another method that can be used on hard drives is to use a file on them (the sort of file you'd find in a hardware store) and actually file off the magnetic material from the surface of the platter. Shredding floppy media is normally sufficient, but simply cutting a floppy disk into a few pieces is not enough—data has been successfully recovered from floppies that were cut into only a couple of pieces. CDs and DVDs also need to be disposed of appropriately. Many paper

shredders now have the ability to shred these forms of storage media. In some highly secure environments, the only acceptable method of disposing of hard drives and other storage devices is the actual physical destruction of the devices. Matching the security action to the level of risk is important to recognize in this instance. Destroying hard drives that do not have sensitive information is wasteful; proper file scrubbing is probably appropriate. For drives with ultra-sensitive information, physical destruction makes sense. There is no single answer, but as in most things associated with information security, the best practice is to match the action to the level of risk.