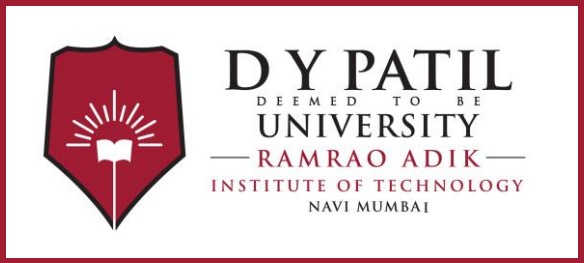


Information Security

Module: 5

•Faculty: Mrs. Bhavana Alte
Mr. Prathmesh Gunjgur

Contents

Module 5:

Lecture 28: Network Security

Network Security

- Network Security refers to the measures taken by any enterprise or organization to secure its computer network and data using both hardware and software systems. This aims at securing the confidentiality and accessibility of the data and network.

Benefits of Network security

- Network Security helps in protecting clients' information and data which ensures reliable access and helps in protecting the data from cyber threats.
- Network Security protects the organization from heavy losses that may have occurred from data loss or any security incident.
- It overall protects the reputation of the organization as it protects the data and confidential items.

Network Security

- The basic principle of network security is protecting huge stored data and networks in layers that ensure the bedding of rules and regulations that have to be acknowledged before performing any activity on the data.

These levels are:

- Physical Network Security
- Technical Network Security
- Administrative Network Security

Network Security

- Physical Network Security: This is the most basic level that includes protecting the data and network through unauthorized personnel from acquiring control over the confidentiality of the network. These include external peripherals and routers that might be used for cable connections. The same can be achieved by using devices like biometric systems.

- Technical Network Security: It primarily focuses on protecting the data stored in the network or data involved in transitions through the network. This type serves two purposes. One is protected from unauthorized users, and the other is protected from malicious activities.

- Administrative Network Security: This level of network security protects user behavior like how the permission has been granted and how the authorization process takes place. This also ensures the level of sophistication the network might need for protecting it through all the attacks. This level also suggests necessary amendments that have to be done to the infrastructure.

Types of Network Security

Firewalls

- A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.
- Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.
- Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.
- Firewalls are commonly used in private networks or intranets to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.
- An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Types of Network Security

Hardware and Software Firewalls

•Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

•Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus

•An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

•Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Types of Network Security

Content Filtering

•Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

•Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

•Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

Types of Network Security

Content Filtering

•Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

•Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

•Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

Types of Network Security

Virtual Private Networks:

Virtual private networks (VPNs) create a connection to the network from another endpoint or site. For example, users working from home would typically connect to the organization's network over a VPN. Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network. Forcepoint's Secure Enterprise SD-WAN allows organizations to quickly create VPNs using drag-and-drop and to protect all locations with our Next Generation Firewall solution.

Network Access Control:

To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices. Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

Types of Network Security

Virtual Private Networks:

Virtual private networks (VPNs) create a connection to the network from another endpoint or site. For example, users working from home would typically connect to the organization's network over a VPN. Data between the two points is encrypted and the user would need to authenticate to allow communication between their device and the network. Forcepoint's Secure Enterprise SD-WAN allows organizations to quickly create VPNs using drag-and-drop and to protect all locations with our Next Generation Firewall solution.

Network Access Control:

To ensure that potential attackers cannot infiltrate your network, comprehensive access control policies need to be in place for both users and devices. Network access control (NAC) can be set at the most granular level. For example, you could grant administrators full access to the network but deny access to specific confidential folders or prevent their personal devices from joining the network.

Types of Network Security

Access Control:

Not every person should have a complete allowance for the accessibility to the network or its data. One way to examine this is by going through each personnel's details. This is done through Network Access Control which ensures that only a handful of authorized personnel must be able to work with the allowed amount of resources.

Cloud Security:

Now a day, a lot of many organizations are joining hands with cloud technology where a large amount of important data is stored over the internet. This is very vulnerable to the malpractices that few unauthorized dealers might pertain to. This data must be protected and it should be ensured that this protection is not jeopardized by anything. Many businesses embrace SaaS applications for providing some of their employees the allowance of accessing the data stored in the cloud. This type of security ensures creating gaps in the visibility of the data.

Types of Network Security

Intrusion Prevention System(IPS):

An intrusion Prevention System is also known as Intrusion Detection and Prevention System. It is a network security application that monitors network or system activities for malicious activity. The major functions of intrusion prevention systems are to identify malicious activity, collect information about this activity, report it, and attempt to block or stop it.

Module 5:

Lecture 29: Operating System Security

Operating System Security

- The process of ensuring OS availability, confidentiality, integrity is known as operating system security. OS security refers to the processes or measures taken to protect the operating system from dangers, including viruses, worms, malware, and remote hacker intrusions. Operating system security comprises all preventive-control procedures that protect any system assets that could be stolen, modified, or deleted if OS security is breached.

Operating System Security

Threats to Operating System

- Malware: It contains viruses, worms, trojan horses, and other dangerous software. These are generally short code snippets that may corrupt files, delete the data, replicate to propagate further, and even crash a system. The malware frequently goes unnoticed by the victim user while criminals silently extract important data.
- Network Intrusion: Network intruders are classified as masqueraders, misfeasors, and unauthorized users. A masquerader is an unauthorized person who gains access to a system and uses an authorized person's account. A misfeasor is a legitimate user who gains unauthorized access to and misuses programs, data, or resources. A rogue user takes supervisory authority and tries to evade access constraints and audit collection.
- Buffer Overflow: It is also known as buffer overrun. It is the most common and dangerous security issue of the operating system. It is defined as a condition at an interface under which more input may be placed into a buffer and a data holding area than the allotted capacity, and it may overwrite other information. Attackers use such a situation to crash a system or insert specially created malware that allows them to take control of the system.

Operating System Security

There are various ways to ensure operating system security. These are as follows:

- Authentication: The process of identifying every system user and associating the programs executing with those users is known as authentication. The operating system is responsible for implementing a security system that ensures the authenticity of a user who is executing a specific program. In general, operating systems identify and authenticate users in three ways.

    - Username/Password: Every user contains a unique username and password that should be input correctly before accessing a system.
    - User Attribution: These techniques usually include biometric verification, such as fingerprints, retina scans, etc. This authentication is based on user uniqueness and is compared to database samples already in the system. Users can only allow access if there is a match.
    - User card and Key : To login into the system, the user must punch a card into a card slot or enter a key produced by a key generator into an option provided by the operating system.

Operating System Security

- One Time passwords: Along with standard authentication, one-time passwords give an extra layer of security. Every time a user attempts to log into the One-Time Password system, a unique password is needed. Once a one-time password has been used, it cannot be reused. One-time passwords may be implemented in several ways.
    - Secret Key: The user is given a hardware device that can generate a secret id that is linked to the user's id. The system prompts for such a secret id, which must be generated each time you log in.
    - Random numbers: Users are given cards that have alphabets and numbers printed on them. The system requests numbers that correspond to a few alphabets chosen at random.
    - Network password: Some commercial applications issue one-time passwords to registered mobile/email addresses, which must be input before logging in.

Operating System Security

- Firewalls: Firewalls are essential for monitoring all incoming and outgoing traffic. It imposes local security, defining the traffic that may travel through it. Firewalls are an efficient way of protecting network systems or local systems from any network-based security threat.

- Physical Security: The most important method of maintaining operating system security is physical security. An attacker with physical access to a system may edit, remove, or steal important files since operating system code and configuration files are stored on the hard drive.

Operating System Security

OS security policies and procedures cover a large area, there are various techniques to addressing them. Some of them are as follows:

- Installing and updating anti-virus software
- Ensure the systems are patched or updated regularly
- Implementing user management policies to protect user accounts and privileges.
- Installing a firewall and ensuring that it is properly set to monitor all incoming and outgoing traffic.

Module 5:

Lecture 30: User Security

User Security

- User Security consists of the platforms which protect your organization's users, endpoints and their online activity to more efficiently correlate threats.
- As users are increasingly logging in to networks via their personal devices, securing these is just as important as securing company owned devices.

User Security

Implementation of security for users:

- Specifying passwords for new users : If you provide a user name and email address, you can specify or generate the initial system password for a new user.

- Changing system and database passwords for users: For security purposes, you can change a system password and also change their database password to synchronize with the new system password. Authorized users can change their own passwords.

- Specifying password hints for users: You can specify password hints to check if the person requesting a new password is the user.

- Specifying security groups for users: To grant users the privileges that are associated with a security group, you can specify a security group for that user.

User Security

- Specifying security profiles for users: When you specify a security profile for multiple users, you assign the users to groups and set other security attributes. The groups and security attributes include the default insert site, the use default insert site as a display filter, the storeroom site, and the default storeroom.

- Specifying security profiles for multiple users: When you specify a security profile for multiple users, you assign the users to groups and set other security attributes. These groups and security attributes include the default insert site, the use default insert site as a display filter, the storeroom site, and the default storeroom.

- Granting user access to Oracle and Structured Query Language server databases: You can grant a user authorization to read, insert, update, and delete specific objects that define a set of fields and business rules, and that update one or more database tables.

User Security

- Changing user access to Oracle and Structured Query Language server databases: To manage database access for users, you can change their existing access. You can remove rights to objects, and add, delete, or change existing rights.

- Removing user access to Oracle and Structured Query Language server databases: You can remove access for a user to read, insert, update, and delete specific objects. These objects define a set of fields and business rules, and update one or more database tables.

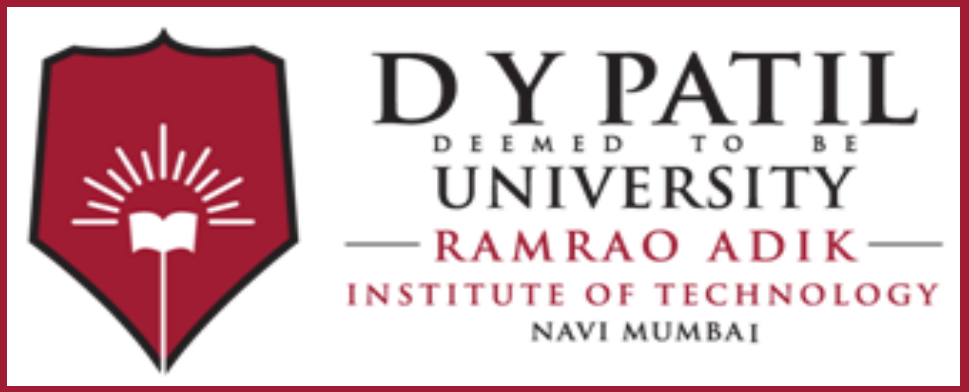
- Logging out and blocking users: You can manage the ability of a user to log in. For users who are currently logged in, you can either log them out or block them.

- Enabling login tracking: You use the Security Controls action in the Security Groups and Users applications to enable login tracking. Login tracking enhances security by limiting the number of incorrect passwords a user can enter when attempting to sign in.

User Security

- Setting user defaults: You use the Security Controls action to specify the defaults for user records. You can access the Security Controls action from either the Security Groups application or the Users application.

- Changing a database password without restarting the application server: When you implement a database password change, you can reduce downtime by performing a live refresh of the application server.


D Y PATIL
DEEMED TO BE
UNIVERSITY
RAMRAO ADIK
INSTITUTE OF TECHNOLOGY
NAVI MUMBAI

Thank You