IT Security and Risk Management

Risk Management

ا.د. حنان الطاهر الداقيز

h.dagez@uot.edu.ly

ربيع 2024

https://t.me/+xavNMXu7DyM5Yjc0

Three principles are commonly recognized in the field as being essential

- There are three principles that will influence many facets of security standards, guidelines, and control designs:

- ✓ Least Privilege الامتياز الأقل
  Defense in Depth الدفاع في العمق
- ✓ Separation of Duties فصل المهام

Least Privilege

- This principle specifies that no communications or activities should be permitted unless there is an explicit need for that transaction or access.
- Least privilege can be applied at any level of design and operation.

Role-based access controls (RBAC) is Least Privilege technique

- A common application of this principle is the use of role-based access controls **(RBAC)** to define the privileges associated with a particular job function; a user is then assigned to that role for authorization purposes.

Defense in Depth

- This principle recommends the use of multiple security techniques or layers of controls to help reduce the exposure if one security control is compromised.
- This may include several layers of defense using different types of protections or could even include vendor diversity.

Defense in Depth Techniques

A simple example of this principle is the implementation of firewalls to protect against external attacks, used along with Intrusion Detection Systems (IDS) to detect any attacks that get past the perimeter controls. Each layer of protection doesn't need to perform the same function. In fact, many layered security controls may look at communications at a network level with one control and then inspect the traffic again at an application level.

Separation of Duties

- The principle of Separation of Duties is intended to minimize errors and make it more difficult to exploit access privileges for personal gain.
- This principle requires the system to be built or process to be implemented so that no one person or group has authority to perform all privileged functions, especially all functions related to the creation and handling of sensitive or critical information.

Threats to Information

- About securing data, we need to think of the controls in terms of three information states:
- **In Transit**: This refers to the data that is being electronically transmitted between systems or physically transported. Usually, this includes your network security and physical security controls.
- **In Process**: This refers to the protection of data as it is being used by the system or application. For instance, when a user inputs data into a form, how is that data filtered and parsed, how is it stored in memory while being processed, and how is it made available to other users?
- **At Rest**: These protections usually focus on protecting data where it is stored,
- whether that be a database or a backup tape. Typical controls for this state
- include Access Controls, Encryption, and Physical Protections.

Threats to Information

For every state that data can take, there is a long list of threats to that information. The major categories are:

- Unauthorized Disclosure, such as a data breach.
- Corruption, such as an accidental modification of a data record.
- Denial of Service, such as an attack that makes a resource unavailable.
- Inability to Prove the Source of an Attack, such as the use of a shared account to perform an unauthorized activity.

Modern Information Security Challenges

There are several challenges with today's dynamic business environments that can make it difficult to adequately protect the organization's resources. Among these many challenges, the following are worth highlighting:

- ✓ Blending of corporate and personal lives
- ✓ Inconsistent enforcement of policies
- ✓ IT doesn't own and control all devices
- ✓ Attacks are no longer obvious

Risk

Risk = Threats x Vulnerabilities

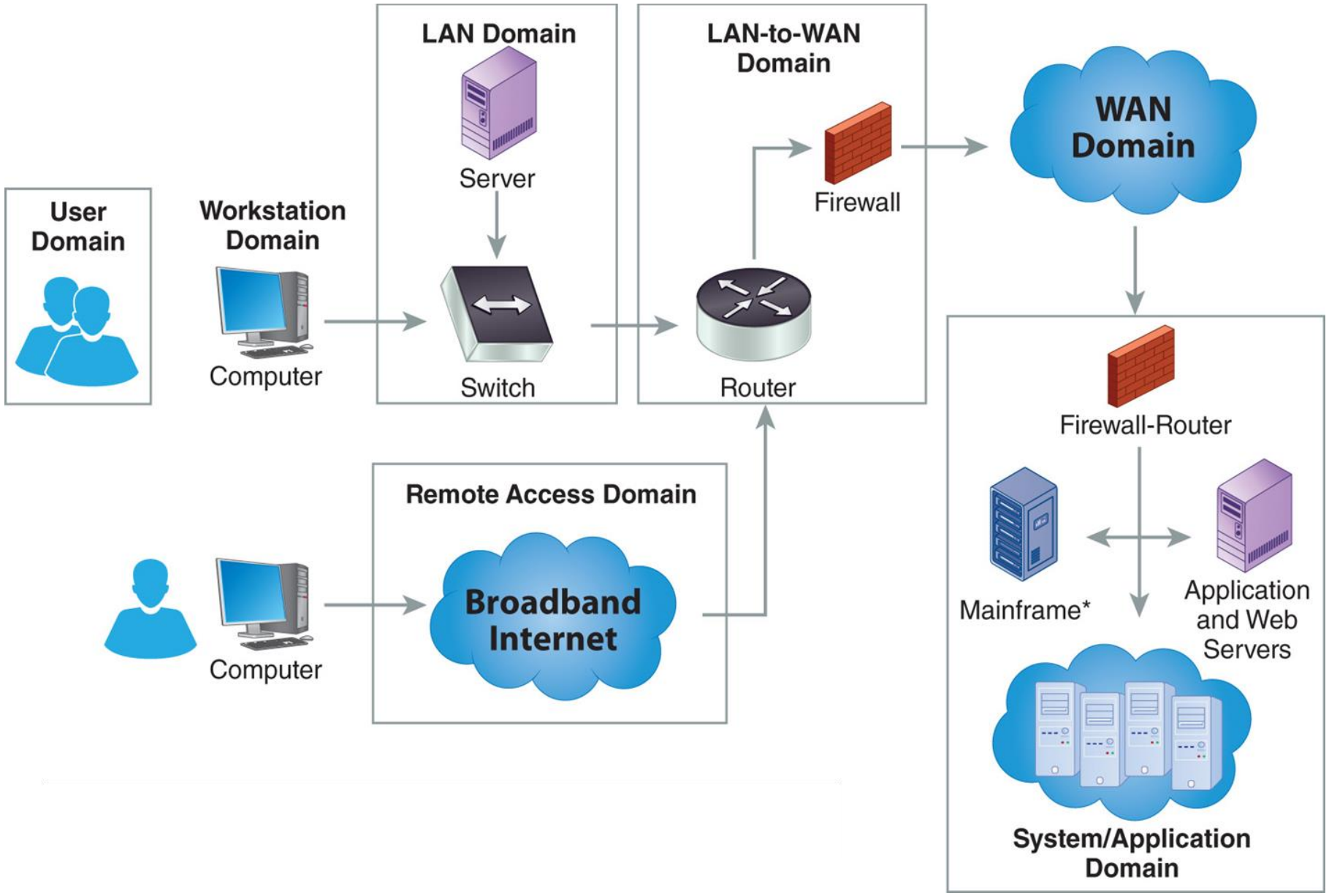
Risk Management Fundamentals

- Information technology (IT) systems contribute to the success of most companies. If you don't properly manage IT risks, they can also contribute to your company's failure.
- Effective risk management starts by understanding threats and vulnerabilities.
- You build on this knowledge by identifying ways to mitigate the risks. Risks can be mitigated by reducing vulnerabilities or reducing the impact of the risk.
- You can then create different plans to mitigate risks in different areas of the company
  - A company typically has several risk mitigation plans in place.

Risk Management

- Risk management isn't intended to be risk elimination. That isn't a reasonable goal.
  - Risk management attempts to identify the risks that can be minimized and implement controls to do so.
- A company doesn't need to manage every possible risk. Some risks are reasonable to manage while others are not.
  - Consider both the cost to implement the control and the cost of not implementing the control.

Seven domain of typical IT infrastructure



Seven domain of typical IT infrastructure

- An attacker only needs to be able to exploit vulnerabilities in one domain.
- A business must provide protection in each of the domains.
- A weakness in any one of the domains can be exploited by an attacker even if the other six domains have no vulnerabilities.
- Some attackers have the skill and aptitude to con users so they focus on the User Domain. Other attackers may be experts in specific applications so they focus on the System/Application Domain.

User Domain

User Domain covers all the users (of any rank) that have access to the other six domains.

- **RISKS**:

1. User can destroy data in application(intentionally or not) and delete all
2. User can find that his friend cheated on him and use his password to delete all of his work so that he would be fired.
3. User can insert infected CD or USB flash drive into the work computer

User Domain..

- The User Domain includes people. They can be users, employees, contractors, or consultants. The old phrase that a chain is only as strong as its weakest link applies to IT security too.
- People are often the weakest link in IT security.
- **Example**:
  - Technical security can require strong, complex **passwords** that can't be easily cracked. However, a social engineer can convince an employee to give up the password.
    - Additionally, users may simply write their password down. Some users assume that no one will ever think of looking at the sticky note under their keyboard.
  - **Users can visit risky Web sites**, and download and execute infected software. They may unknowingly bring viruses from home via universal serial bus (USB) thumb drives. When they plug in the USB drive the work computer becomes infected. This in turn can infect other computers and the entire network.

Workstation Domain

A computer of an individual user where the production takes place

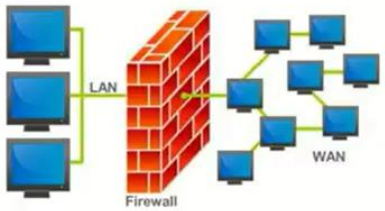
- RISKS:

1. The workstation's OS can have a known software vulnerability that allows a hacker to connect remotely and steal data.
2. A workstation's browser can have a software vulnerability which allows unsigned scripts to silently install malicious software.
3. A workstation's hard drive can fail causing lost data.

Workstation Domain

- The workstation is the end user's computer. If antivirus software isn't installed, the workstation is also vulnerable.
- Antivirus companies regularly update virus definitions as new malware is discovered.
  - If the antivirus software is installed and up to date, the likelihood of a system becoming infected is reduced.
- Bugs and vulnerabilities are constantly being discovered in operating systems and applications.
- Software vendors regularly release patches and fixes that can be applied. When systems aren't updated, the threats can become significant.

LAN Domain



- The LAN Domain is the area that is inside the firewall. It can be a few systems connected together in a small home office network.
  - It can also be a large network with thousands of computers.
- Each individual device on the network must be protected or all devices can be at risk.
- The internal LAN is generally considered a trusted zone. Data transferred within the LAN isn't protected as thoroughly as if it were sent outside the LAN.
- **Example:** attacks occur when an attacker uses a protocol analyzer to capture data Sniffing packets. A protocol analyzer is also known as a sniffer. An experienced attacker can read the actual data within these packets.
- If hubs are used instead of switches, there is an increased risk of sniffing attacks.
  - An attacker can plug into any port in the building and potentially capture valuable data.
- If switches are used instead of hubs, the attacker must have physical access to the switch to capture the same amount of data.
- Most organizations protect network devices in server rooms or wiring closets.

LAN Domain

Contains all of the work stations, hubs, switches, and routers. The LAN is a trusted zone

- RISKS:

1. A worm can spread through the LAN and infect all computers in it.
2. LAN server OS can have a known software vulnerability.
3. An unauthorized user can access the organization’s workstations in a LAN.

LAN \ WAN Domain

- The LAN-to-WAN Domain connects the local area network to the wide area network (WAN).
  - The LAN Domain is considered a trusted zone since it is controlled by a company.
  - The WAN Domain is considered an untrusted zone because it is not controlled and is accessible by attackers.
- The area between the trusted and untrusted zones is protected with one or more firewalls. This is also called the **boundary**, or the **edge**. Security here is referred to as **boundary protection or edge protection**.
- The public side of the boundary is often connected to the Internet and has public Internet Protocol (IP) addresses.
  - These IP addresses are accessible from anywhere in the world, and attackers are constantly probing public IP addresses.
  - They look for vulnerabilities and when one is found, they pounce.
- A high level of security is required to keep the LAN-to-WAN Domain safe.

LAN \ WAN Domain

The boundary between the trusted and un-trusted zones. The zones are filtered with a firewall.

- RISKS:

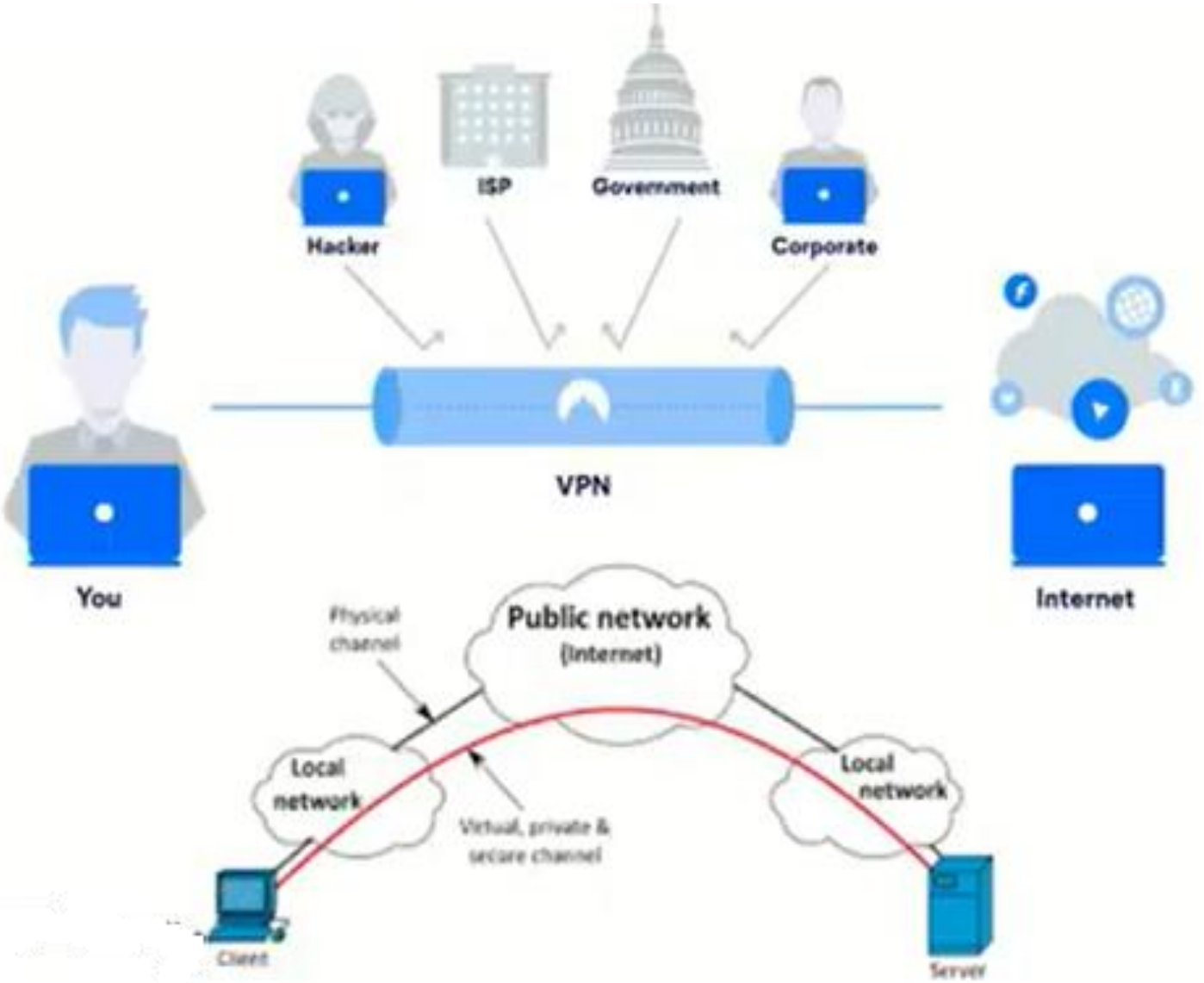
1. A hacker can attack your IT infrastructure and gain access to your internal network.
2. A firewall with unnecessary ports open can allow access from the Internet

-

Remote Access Domain

- **Example:**
  - **Mobile workers** often need access to the private LAN when they are away from the company.
  - Remote access can be granted via a virtual private network (VPN) connection.
- VPNs have their vulnerabilities, even they are examples of a control to lessen the risk!
- Vulnerabilities exist at two stages of the VPN connection:
  - **First stage is authentication:** Authentication is when the user provides credentials to prove identity. If these credentials can be discovered, the attacker can later use them to impersonate the user.
  - **Second stage is when data is passed** between the user and the server. If the data is sent in clear text, an attacker can capture and read the data.

Remote Access Domain



Remote Access Domain

The domain in which a mobile user can access the local network remotely, usually through a VPN.

- RISKS:

1. Communication circuit outage can deny connection.
2. Remote communication from office can be unsecured.
3. VPN tunneling between remote computer and ingress/egress router can be hacked.

WAN Domain

- For many businesses, the WAN is the Internet.
- As mentioned in the LAN-to-WAN Domain, the Internet is an untrusted zone.
- Any host on the Internet with a public IP address is at significant risk of attack.
- Moreover, it is fully expected that any host on the Internet will be attacked.
- Semiprivate lines aren't as easily accessible as the Internet.
- However, a company rarely knows who else is sharing the lines. These leased lines require the same level of security provided to any host in the WAN Domain.
- A significant amount of security is required to keep hosts in the WAN Domain safe.

WAN Domain

1. Stands for Wide Area Network and consists of the Internet and semi-private lines

- RISKS:

1. Service provider can have a major network outage.
2. Server can receive a DOS or DDOS attack.
3. A FTP server can allow anonymously uploaded illegal software

System / Application Storage Domain

- The System/Application Domain refers to servers that host server-level applications.
  - Mail servers receive and send email for clients.
  - Database servers host databases that are accessed by users, applications, or other servers.
  - Domain Name System (DNS) servers provide names to IP addresses for clients.
- You should always protect servers using best practices:
  - Remove unneeded services and protocols.
  - Change default passwords.
  - Regularly patch and update the server systems.
  - Enable local firewalls.
- **One of the challenges with servers in the System/Application Domain is that the knowledge becomes specialized.**
  - **For example**, common security issues with an email server would likely be known only by technicians who regularly work with the email servers.

System / Application Storage Domain

This domain is made up of user-accessed servers such as email and database.

- **RISKS:**

1. A DOS attack can cripple the organization's email.
2. A database server can be attacked by SQL injection, corrupting the data.

Thank you