Cybersecurity Fundamentals

Contents

Core principles
- The Principle of Least Privilege
- The Core of All Security (CIA, AAA and PPT)
- Prevent / Detect / Respond
- Security by Thirds
- Security Roles and Responsibilities
- The Nature of the Threat

Risk Management
Information Security Governance

Next

Core principles

The Principle of Least Privilege

This principle restricts how privileges are granted.
The principle of least privilege states that a subject should be given only those privileges that it needs in order to complete its task.
In other words, Only the **minimum access** necessary to perform an operation should be granted, and that access should be granted only for the **minimum** amount of **time** necessary.

The Principle of Least Privilege

Least privilege requires isolation to restrict access of the component to other parts of the system
If a component follows least privilege, then any privilege that is further removed from the component removes some functionality.

For example, in an online shopping application, the frontend used by public user shouldn't be allowed to access account reconciliation API, which can only be accessed by finance frontend.

The Principle of Least Privilege

A good real-world example appears in the security clearance system of the U.S. government -- the policy of "need to know".

If you have clearance to see any classified document, you still won't be able to see *any* secret document that you know exists.
If you could, it would be very easy to abuse the secret clearance level.
Instead, people are only allowed to access documents that are relevant to those tasks that apply to them.

The Principle of Least Privilege

Famous violations of the principle of least privilege exist in UNIX systems.
For example, you need to have root privileges to run a service on a port number less than 1024.

So, to run a mail server on port 25 (SMTP port) a program needs the privileges of the root user.

However, once a program has set up shop on port 25, there is no need for it to use root privileges again.

A security-conscious program would give up root privileges and let the operating system know that it should never require those privileges again (at least, not until the next run of the program).

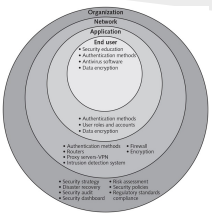
CIA Security Triad

CIA security triad: The confidentiality, integrity, and availability of systems and data
IT security practices focus on the CIA security triad:
Confidentiality ensures only those individuals with proper authority can access sensitive data

Integrity ensures data can only be changed by authorized users

Availability ensures data can be accessed when and where needed
CIA security must be implemented at the organization, network, application, and end-user levels

CIA Security Triad



CIA Security Triad

CIA security triad: The confidentiality, integrity, and availability of systems and data
IT security practices focus on the CIA security triad:
Confidentiality ensures only those individuals with proper authority can access sensitive data

Integrity ensures data can only be changed by authorized users

Availability ensures data can be accessed when and where needed
CIA security must be implemented at the organization, network, application, and end-user levels

The AAA

Vital pillars of **a good security program**.
The better you implement these three principles, the more secure your organization will be:

Authentication:
The process of verifying someone's identity.
Is Keith really Keith?

Authorization:
The process of giving the user permission to access a specific resource or function.
While we know Keith is Keith, what *can* Keith do?

Accountability:
Accountable to what he is authorized to do and to what he is not authorized to do
While we know Keith is Keith, what *did* Keith do?

The PPT

If you do not have these three things in place, you **do not have a security program**, or, you likely don't have a program that has any possibility of being **effective**.

Policy:
Broad general statement of management's intent
It is a legal document that spells out the general sense of how management expects the assets of the organization to be protected.
Example: strong password for all accounts

Procedure:
The detailed steps to make policy happen
The description and the step-by-step procedures to implement the policies
Example:

1. Combination of numbers, letters and characters
2. Not less than 10 digit

Training:
Users must know what policies and procedures say in order to follow them
You can create the best policies and procedures in the world but not telling anyone what they say.

Prevent/Detect/Respond (PDR)

Prevent as much as you can

Detect for anything you can not prevent:
Or if the preventive measures fail

Respond to what is detected

Security by Thirds

A security professional needs to be:

1/3 technologist

1/3 manager

1/3 lawyer

Roles and Responsibilities

Senior Manager (e.g. CEO, Director etc.):
Has legal responsibility to protect the assets of the organization

Authority can be delegated – responsibility cannot be
They can delegate the authority to implement security to the Chief Information Security Officer

Roles and Responsibilities

Data Owner:
Person with primary responsibility for data
Owners determine classification, protective measures, and more

Data Custodian:
The person/group that makes
the decisions of the owners happen

Users:
Use data
Are also automatically Data Custodians (provide advice)

The Nature of the Threat

Disgruntled Insider:
An employee/user from inside the organization who have already granted some level of access to do his work and become unhappy, angry or dissatisfied with the organization.

Accidental Insider:
A employee/user on our network that has no intention of causing damage, but does so by accident. For example, a user clicks a link or opens the email attachment

External Insider:
Individual or group that has **gained remote control access** to at least one computer inside the network of the organization. The most common attack is that the accidental insider opens the gate for External insider.

Next…

Risk Management

Risk Management

Basic Definitions

Threat: Anything that can do anything bad to our stuff

Vulnerability: Anything that allows the threat to happen

Likelihood: How likely is it to happen

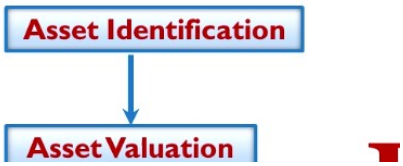
Impact: How bad will it be?

Countermeasure/safeguard: Anything to lessen or mitigate a vulnerability

Gap Analysis: Here is our risk; here are our countermeasures. What is the gap between?

And how can we close the gap both effectively and cost-effectively

Risk Management



Next…

Information Security Governance

Information Security Governance

It is an integral part of enterprise governance

Consists of the **leadership, organizational structures** and **processes** that ensures that the organization's information security sustains and extends the organization's strategies and objectives.

Information security **governance provides a structure for aligning** information security **strategy with business strategy.**

Directing and controlling information security of the organization

Information Security Governance

Directing: creating directives, policies and procedure of **information security** from the strategic down to the operational level

Controlling: measure, monitor and report compliance and performance of **information security** from operational level up to strategic level

Exercise (10 minutes)

- What do you think can be the two most common mistakes by security team for implementing the principle of least privilege?

References

www.sans.org

Questions/Comments?

Thank You