Nim : 1210651223

Nama : Eko Setiawan

Kelas : C

OPERATIONS SECURITY

ADMINISTRATIVE SECURITY

A fundamental aspect of operations security is ensuring that controls are in place to inhibit people either inadvertently or intentionally compromising the confidentiality,integrity, or availability of data or the systems and media holding that data.

Label

Objects have labels and subjects have clearances.According to Executive Order 12356—National Security Information,

- "top secret"
- "secret"
- "confidential"

Clearance

Clearances must determine the subject's current and potential future trustworthiness; the latter is harder (and more expensive) to assess. Some higher-level clearances include access to compartmented information. Compartmentalization is a technical method for enforcing need to know.

Separation of duties

Separation of duties (also called segregation of duties), each person involved is supervising the other when access is granted and used. No one person should have total control of a sensitive transaction.
For example,
administration of a nuclear weapons system should require many people's oversight and completion of duties.

Rotation of duties

Rotation of duties describes a process that requires different staff members to perform the same duty.Rotation of duties can serve as a either detective or deterrent control: the fear of being caught may deter someone from committing fraud; the rotation may detect fraud that has already occurred.

Mandatory leave/forced vacation

An additional operational control that is closely related to rotation of duties is that of mandatory leave, also known as forced vacation.

Nondisclosure agreement

A nondisclosure agreement (NDA) is a work-related contractual agreemen.Job candidates, consultants,or contractors often sign nondisclosure agreements before they are hired. Nondisclosure agreements are largely a directive control.

Background checks

Background checks (also known as background investigations or preemployment screening) are an additional directive control. Some organizations perform cursory background investigations that include a criminal record check.

SENSITIVE INFORMATION/MEDIA SECURITY

This section discusses concepts that are an important component of a strong overall information security posture.

Sensitive information

Sensitive information requires protection, and that information physically resides on some form of media. It is also likely that sensitive information is transferred, whether internally or externally, for use.

Labeling/marking

Perhaps the most important step in media security is the process of locating sensitive information and labeling or marking it as sensitive.

Handling

People handling sensitive media should be trusted individuals who have been vetted by the organization.Policies should require the inclusion of written logs detailing the person responsible for the media.

Storage

Physical storage of the media containing sensitive information should not be performed in a haphazard fashion, whether the data is encrypted or not.

Retention

Media and information have a limited useful life.Keep in mind there may be regulatory or other legal reasons that may compel the organization to maintain such data for keeping data beyond its time of utility.

Media sanitization or destruction of data

While some data might not be sensitive and not warrant thorough data destruction measures, an organization will have data that must be verifiably destroyed or otherwise rendered nonusable in case the media on which it was housed is recovered by a third party. The

process for sanitization of media or destruction of data varies directly with the type of media and sensitivity of data.

-Data remanence
-Wiping, overwriting, or shredding
-Degaussing
-Physical destruction
-Shredding

ASSET MANAGEMENT

Systems security is another vital component to operations security, and there are specific controls that can greatly help system security throughout the system's life cycle.

Configuration management

Basic configuration management practices associated with system security will involve tasks such as disabling unnecessary services; removing extraneous programs; enabling security capabilities such as firewalls, antivirus, and intrusion detection or prevention systems; and the configurating security and audit logs.

Baselining

Security baselining is the process of capturing a point in time understanding of the current system security configuration.

Vulnerability management

Vulnerability scanning is a way to discover poor configurations and missing patches in an environment.The remediation or mitigation of vulnerabilities should be prioritized based on both risk to the organization and ease of remediation procedures.

Zero-day vulnerabilities and zero-day exploits

A zero-day vulnerability is a vulnerability that is known before the existence of a patch.
A zero-day exploit, rather than vulnerability, refers to the existence of exploit code for a vulnerability that has yet to be patched.

Change management

The purpose of the change control process is to understand, communicate, and document any changes with the primary goal of being able to understand, control, and avoid direct or indirect negative impact that the change might impose.

FAST FACTS

The general flow of the change management process includes:
• Identifying a change
• Proposing a change

• Assessing the risk associated with the change
• Testing the change
• Scheduling the change
• Notifying impacted parties of the change
• Implementing the change
• Reporting results of the change implementation

CONTINUITY OF OPERATIONS

Continuity of operations is principally concerned with the availability portion of the confidentiality, integrity, and availability triad.

Service-Level Agreements

Service-Level Agreements will dictate what is considered acceptable regarding things such as bandwidth, time to delivery,response times, etc.

Fault tolerance

Availability not only is solely focused on system uptime requirements but also requires that data be accessible in a timely fashion.

Backup

The three basic types of backups are: full backup, incremental backup, and differential backup.
-full
-Incremental and differential

Redundant Array of Inexpensive Disks

The goal of a Redundant Array of Inexpensive Disks (RAID) is to help mitigate the risk associated with hard disk failures.

FAST FACTS

Three critical RAID terms are: mirroring, striping, and parity.
• Mirroring achieves full data redundancy by writing the same data to multiple hard disks.
• Striping focuses on increasing read and write performance by spreading data across multiple hard disks. Writes can be performed in parallel across multiple disks rather than serially on one disk. This parallelization provides a performance increase and does not aid in data redundancy.
• Parity achieves data redundancy without incurring the same degree of cost as that of mirroring in terms of disk usage and write performance.

System redundancy

Though redundancy and resiliency of data, provided by RAID and backup solutions, are important, further consideration needs to be given to the systems themselves that provide access to this redundant data.
-Redundant hardware and redundant systems
-High-availability clusters

INCIDENT RESPONSE MANAGEMENT

A security incident is a harmful occurrence on a system or network. All organizations will experience security incidents. Incident response management is a regimented and tested methodology for identifying and responding to these incidents. A Computer Security Incident Response Team (CSIRT) is the group tasked with monitoring, identifying, and responding to security incidents. The goal of the incident response plan is to allow the organization to control the cost and damage associated with incidents and to make the recovery of impacted systems quicker.

Methodology

1. Preparation
2. Detection and analysis
3. Containment, eradication, and recovery
4. Postincident activity

Many incident handling methodologies treat containment, eradication, and recovery as three distinct steps, as we will in this book.

Other names for each step are sometimes used; here is the six-step life cycle we will follow, with alternate names listed:

1. Preparation
2. Detection and analysis (aka identification)
3. Containment
4. Eradication
5. Recovery
6. Lessons learned (aka postincident activity, postmortem, or reporting)

Preparation

These include training, writing incident response policies and procedures, and providing tools such as laptops with sniffing software, crossover cables, original OS media, removable drives, etc.

Detection and analysis

An event is any auditable action on a system or network (such as a server reboot or a user logging in to check e-mail). An incident is a harmful event (such as a denial of service attack that crashes a server).

Containment

Containment might include taking a system off the network, isolating traffic, powering off the system, or other items to control both the scope and severity of the incident.

Eradication

The eradication phase involves two steps: removing any malicious software from a compromised system and understanding the cause of the incident. In order for an organization to reliably recover from an incident, the cause

must be determined so that the systems in question can be returned to a known good state without risk of compromise persisting or reoccurring.

Recovery

The recovery phase involves cautiously restoring the system or systems to operational status. For this reason, close monitoring of the system after it is returned to production is necessary.

Lessons learned

This fact is unfortunate because the lessons learned phase, if done right, is the phase that has the greatest potential to effect a positive change in security posture. The goal of the lessons learned phase is to provide a final report on the incident, which will be delivered to management.

Types of attacks

This section will provide basic information on the types of attacks more commonly experienced and responded to in organizations.

Session hijacking and MITM

Older protocols such as Telnet may be vulnerable to session hijacking. A Man-in-the-Middle (MITM, also called Monkey in the Middle) attack places the attacker between the victim and another system.

Malware

Malware, or malicious code/software, represents one of the best-known types of threats to information systems.

Denial of Service and Distributed Denial of Service

(DDoS) is a many-to-one availability attack. DoS attacks come in all shapes and sizes, ranging from those involving one specially crafted packet and a vulnerable system to see that packet to DDoS attacks that leverage tens of thousands (or more) of bots to target an online service provider with a flood of seemingly legitimate traffic attempting to overwhelm their capacity.

Types of Malware

-Virus
-Macro virus
-Worm
-Trojan horse
-Rookit

Denial of Service Examples

-Land
-Smurf
-SYN Flood
-Teardrop
-Ping of Death

-Fraggle
-DNS Reflecktion