



Office of Chief Information Officer
Department of Health and Human Services



Cybersecurity Essentials Training

Training Transcripts

Office of the Chief Information Officer

Assistant Secretary for Administration

U.S. Department of Health and Human Services

Table of Contents

[Section 1 - Introduction](#)

[Section 2 - Lessons](#)

[Lesson 1: General Cybersecurity Vulnerabilities.](#)

- Types of Vulnerabilities
 - User Vulnerabilities
 - Non-Malicious Employees
 - Insider Threats
 - Internal Processes and Vulnerabilities
 - Technology Failures
 - External Threats
 - External Attackers
 - Civil Unrest
 - Natural Disasters
 - Contingency Plans

[Lesson 2: Common Cyber-Attack Mechanisms and Motivations for Use.](#)

- Motivation for Attacks
- Types of Attacks
 - Denial-of-Service Attacks
 - Distributed Denial of Service Attack
 - Man in the Middle (MITM)
 - Social Engineering Attacks
 - Cross Site Scripting (XSS)
- Intrusion, Detection, and Prevention

[Lesson 3: Encryption](#)

- Encryption
 - Encryption definition
- Cryptographic algorithms
 - Public key (asymmetric) cryptographic algorithm

- Secret key (symmetric) cryptographic algorithm

Lesson 4: Firewalls and Virtual Private Networks (VPNs)

- Firewalls
- Virtual Private Networks (VPNs)
- SSL VPN
- Tunneling
- Split vs Single Tunneling

Lesson 5: Cloud Computing Vulnerabilities

- Cloud Computing
 - Public Cloud
 - Private Cloud
- Security Challenges
- Cloud Service Models
 - Infrastructure-as-a-Service (IaaS)
 - Software-as-a-Service (SaaS)
 - Platform-as-a-Service (PaaS)
- Cloud Security
- Virtualization

Lesson 6: Enterprise Performance Life Cycle

- Enterprise Performance Life Cycle Phases
 - Initiation
 - Concept
 - Planning
 - Requirements Analysis
 - Design
 - Development
 - Test
 - Implementation
 - Operations and Management
 - Disposition

Section 3 - Conclusion

- Training Wrap Up
- Feedback

Section 1 - Introduction

Welcome!

Cybersecurity Essentials training is designed to bridge the gap between awareness and role-based training. In this training, you will learn intermediate principles, procedures, practices and challenges of Cybersecurity. The Cybersecurity Essentials training provides a general summary of common vulnerabilities that can impact information and information systems along with common mitigation approaches. This training is designed for employees and contractors, who are involved in any way with IT systems. It provides the foundation for subsequent specialized or role-based training by providing a universal baseline of key security terms and concepts.

Section 2 - Lessons

Lesson 1: General Cybersecurity Vulnerabilities.

Overview

Welcome to Lesson 1! In this lesson we discuss general cybersecurity vulnerabilities and ways to minimize them.

Objectives

1. Recognize vulnerabilities from people and technology
2. Identify common system and technology failures
3. Understand internal process vulnerabilities and external threats
4. Discuss natural disasters

Topics

- Types of Vulnerabilities
 - User Vulnerabilities
 - Non-Malicious Employees
 - Insider Threats
 - Internal Processes and Vulnerabilities
 - Technology Failures
 - External Threats
 - External Attackers
 - Civil Unrest
 - Natural Disasters
 - Contingency Plans

Introduction

A vulnerability is a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. In this section, we take a look at common vulnerabilities HHS information systems may encounter.

Types of Vulnerabilities

User Vulnerabilities

Most cybersecurity vulnerabilities are caused by users of the information system. User vulnerabilities can occur inadvertently, deliberately, or merely by inaction. Any of these actions can create serious vulnerabilities in HHS Information systems or even create a security incident. Three types of user actions are:

- “Inadvertent actions” are actions done unintentionally and were not meant to do harm. Usually these actions are caused by omissions, errors, or mistakes.
- “Deliberate actions” are intentional actions that are designed to do harm. Insiders or outsiders could perform deliberate actions. Theft, vandalism, and/or fraud are all types of deliberate actions. These actions could take place via deleting or altering data, phishing, ransomware, hacking, or other types of sabotage.
- “Inaction” is a lack of action or failing to respond appropriately in a particular situation. Inaction may result from a lack of training, or from not having a skilled person available to take action.

Non-Malicious Employees

Information systems can also be harmed by non-malicious employees. Non-malicious employees are authorized users who make changes to a system, without knowing that the actions could cause problems in the information system.

Insider Threats

An insider threat is an individual with authorized access (i.e., within the security domain) that has the potential to harm an information system or enterprise through destruction, disclosure, modification of data, and/or denial of service. These threats can come from a disgruntled employee with intent to leak sensitive data, change or delete data, or create vulnerabilities within an information system. Insider threats can also destroy data using a logic bomb. A logic bomb is a piece of code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. Other ways malicious insiders can destroy or make information unusable include: installing malware; Denial of Service (DOS) attacks; and hardware or facility destruction.

Internal Processes and Vulnerabilities

Cybersecurity incidents can occur when internal processes fail. Common internal process failures include:

- Process Design or Execution vulnerabilities resulting from either poorly executed processes of a properly designed process; or from a process design that was not a good solution for a task. The desired outcome is not achieved as a result of improper creation of: process documentation, process flow, roles and responsibilities, information flow, task hand-off, escalation of issues, notifications and alerts, and service level agreements.
- Process Control vulnerabilities occur when the operation of a process does not include adequate controls. These controls may be found in: metrics, process ownership, periodic review, and status monitoring.
- Process Support refers to vulnerabilities that occur as a result of an organization's failure to deliver the appropriate human resources to complete training and development, staffing, accounting, and/or procurement.

Technology Failures

Let's now look at cybersecurity systems and technology vulnerabilities or weaknesses. Systems and technology vulnerabilities are technology problems or abnormalities, resulting from unexpected operational errors. Software, integrated systems, or hardware could all be sources of these failures. Additional information on failure types is listed below.

- *Hardware failures* may include performance issues related to broken or faulty physical equipment, such as hard drive crashes; PIV card reader not reading the card when inserted; and/or keyboard not registering the keystroke when a key is pressed.
- *Software failures* result from risks relating to operating systems, applications, programs, and/or other software assets. Configuration management, security settings, compatibility, change control, coding practices, and testing are normally where software failures are located.
- *Systems failures* occur when integrated systems do not perform as expected. These failures may be a result of complexity, integration, design elements, or specifications.

External Threats

External threats are typically outside the control of HHS personnel. External attackers, civil unrest, and natural disasters are external threats. Let's take a closer look at each.

External Attackers

External attackers are hackers. A hacker is an unauthorized user who attempts to or gains access to an information system. They are not authorized users or employees and seek to steal information for identity theft or for some other financial crime.

Civil Unrest

Civil unrest is also seen as an attack on an information system. Civil unrest can refer to a riot, terrorist act, or some other civil disorder that may lead to a disruption of IT operations.

Natural Disasters

Natural disasters may include: pandemic, fire, earthquakes, flooding, and other weather events. These events can cause havoc to any business. Review each term below to find out more.

- Weather event such as severe rain, tornados, snow, and/or hurricanes could all cause adverse reactions within an organization and cause service delay.
- Fires may occur outside of a facility or within a facility and cause organizational disruptions.
- Flooding could happen outside or within a facility, and water damage could cause organizational disruptions.
- Earthquakes outside can cause organizational operations to be disrupted.
- Pandemic refers to a widespread medical issue or condition that could disrupt organizational operations.

Contingency Plans

It's important to plan for all types of attacks and natural disasters. A contingency plan includes management policy and procedures used to guide an enterprise response to a perceived loss of mission capability. When a natural disaster or major system failure occurs, a contingency plan is activated by the enterprise risk managers to determine what happened, why, and how to resolve the problem. It may point to the Continuity of Operations Plan (COOP) or Disaster Recovery Plan

for major disruptions. Having contingency plans in place helps to prevent **incidents** and system failures at HHS.

Lesson Summary

In Lesson 1, we discussed cybersecurity threats; system and technology failures; and external threats. Understanding how these threats and failures occur is critical in determining the best way to limit points of vulnerability.

Knowledge Check

1- If a HHS systems administrator accidentally changes or deletes information within the HHS information system, **is this considered to be a cybersecurity incident?**

- A. Yes
- B. No

Answer: A. Yes.

Explanation: While this may have been done unintentionally, the act of changing or deleting information within the HHS information system is definitely considered a cybersecurity incident.

2- A disastrous glitch affecting hospitals throughout the southeast originated while security patches designed to counter potential future cyber-attacks were being uploaded. It took hospitals more than two weeks to recover their electronic medical record systems. Risks stemming from software assets of all types, including programs, applications, and operating systems is defined as what?

- A. Software failure
- B. Configuration management
- C. Hardware failure
- D. All of the above

Answer: A. Software failure

Explanation: Software failure is risk stemming from software assets of all types.

Lesson 2: Common Cyber-Attack Mechanisms and Motivation for Use.

Overview

Welcome to Lesson 2! In this lesson, we take an in depth look at denial-of-service attacks. We will also investigate intrusion attacks and what motivates hackers to use cyber-attack mechanisms like cross site scripting.

Objectives

1. Identify motivation for using intrusion attacks
2. Explain denial-of-service attacks and their consequences
3. Study social engineering attacks
4. Discuss cross site scripting (XSS)
5. Define intrusion attacks and explore ways to detect them

Topics

- Motivation for Attacks
- Types of Attacks
 - Denial-of-Service Attacks (DoS)
 - Distributed Denial of Service Attacks (DDoS)
 - Man in the Middle (MITM)
 - Consuming Server Resources
 - Saturating Network Resources
 - Social Engineering Attacks
 - Cross Site Scripting (XSS)
- Intrusion, Detection, and Prevention

Introduction

Hackers use a variety of tools to gain unauthorized access to information stored on HHS computer systems. These efforts are called Intrusion Attacks. Let's take a look at common ways attackers attempt to compromise information systems.

Motivation for attacks

Hackers are motivated by:

- *Revenge*: An employee can cause harm to the Department because of being fired or laid off.
- *Money*: The employee may leak sensitive information to cybercriminals for financial gains.
- *Idealism or Hacktivist*: The employee who uses computer hacking to achieve a political or social agenda.
- *Espionage or Political*: HHS's Information and information systems are an attractive target to other countries around the world that lack comparable health related information. Some citizens of other countries consider theft of any type of government information as an act of patriotism or activism for the cause or Government they support.
- *Business Advantage*: An employee who just moved to another employer may still carry the records and intellectual property of the first employer to the second.

Types of Attacks

Denial-of-Service Attacks

A Denial-of-Service (DoS) attack is the prevention of authorized access to resources or the delaying of time-critical operations. This is when an attacker is able to prevent authorized users from gaining access to a network or service where they are normally granted access. This is accomplished by consuming valuable server resources like system memory and/or bandwidth. An intruder may be able to consume all the available bandwidth or system memory by generating a large number of requests to the system or network.

Distributed Denial of Service Attack

A Distributed Denial of Service (DDoS) attack is a denial of service technique that uses numerous hosts to perform the attack. This type of attack may include:

- Ping of Death (POD)

- A DoS attack in which an attacker attempts to crash, destabilize, or freeze the targeted computer or service by sending malformed or oversized packets using a simple ping command.
- Botnet
 - A botnet (or zombie army) is a group of computers connected in a coordinated fashion for malicious purposes. Each computer in a botnet is called a bot. These bots form a network of compromised computers, which is controlled by a third party and used to transmit malware or spam, or to launch attacks.
- TCP SYN Flood
 - Flooding is an attack that attempts to cause a failure in a system by providing more input than the system can process properly.
- Tear Drop
 - A DoS attack in which the attacker sends IP data packets in the form of fragments to the victim system. However, when the victim system tries to reconstruct the fragments into the original packets, it is unable to do so and ends up crashing.
- Smurf
 - Smurfs are attacks that make the task of gaining more flooding resources easier, and allow an attacker to amplify his flooding resources a hundred or even a thousand-fold. The goal is to create a tremendous amount of traffic. In this case, the target continues to function but cannot process any legitimate network requests because the attacker has consumed all of the network bandwidth.

Man in the Middle (MITM)

Man in the Middle (MITM) is an attack on the authentication protocol run in which the Attacker positions himself or herself in between the Claimant and Verifier so that he can intercept and alter data traveling between them.

- Session hijacking
 - Border Gateway Protocol (BGP) is a routing protocol, which means that it is used to update routing information between major systems. Without BGP, email, Web

page transmissions, and other Internet communications would not reach their intended destinations. Session hijacking involves intrusion into an ongoing BGP session, i.e., the attacker successfully masquerades as one of the peers in a BGP session, and requires the same information needed to accomplish the reset attack. The difference is that a session hijacking attack may be designed to achieve more than simply bringing down a session between BGP peers. For example, the objective may be to change routes used by the peer, in order to facilitate eavesdropping, blackholing, or traffic analysis.

- IP spoofing
 - “IP spoofing” refers to sending a network packet that appears to come from a source other than its actual source.
- Phishing and spear phishing
 - Phishing is tricking individuals into disclosing sensitive personal information through deceptive computer-based means. Other definitions include: Deceiving individuals into disclosing sensitive personal information through deceptive computer-based means; and a digital form of social engineering that uses authentic-looking—but bogus—emails to request information from users or direct them to a fake Web site that requests information. **If you receive an unexpected email with a link or an attachment, verify that it came from a legitimate sender by speaking directly to the sender using a telephone number in the HHS Microsoft Outlook address book or your business records, not the number in the email as it could be a phishing/vishing attempt. Forward all suspected phishing attempts to spam@hhs.gov instead of replying to message.**
 - Spear phishing is a variation on phishing in which hackers send emails to a specific organization or individual; or specific groups of people with specific common characteristics or other identifiers. Normally they are orchestrated to obtain trade secrets or military information.

Social Engineering Attacks

Social engineering is a way for hackers to use social skills and/or human interaction to compromise a computer system or network. Review the terms below to reveal ways hackers use social engineering, along with how to prevent it.

- Email (or phishing) attacks are emails sent by hackers in an effort to infiltrate and obtain information from a computer system or network. These emails appear to be legitimate or from someone that the user is familiar with. The email may ask the user to open an attachment or click a link so that information can be updated or validated. These emails also may include a sense of urgency for the user to respond.
- Hackers may use password guessing as another form of social engineering. The personal interests, hobbies, and/or connections of a user can be used by a hacker to guess a user's password. Normally this information can be obtained from social media sites; and unfortunately can be used to harm the user.
- "Shoulder surfing" is commonly used by hackers that have access to a legitimate user of the targeted computer system. They may use this close proximity to watch a user as they type in a password.

Cross Site Scripting (XSS)

Cross Site Scripting (XSS) is a vulnerability that allows attackers to inject malicious code into an otherwise benign website. These scripts acquire the permissions of scripts generated by the target website and can therefore compromise the confidentiality and integrity of data transfers between the website and client. Websites are vulnerable if they display user supplied data from requests or forms without sanitizing the data so that it is not executable.

Intrusion, Detection, and Prevention

Common ways to mitigate intrusion attacks are through the use of Intrusion Detection Systems and Intrusion Prevention Systems. An Intrusion Detection Systems (IDS) is a hardware or software product that gathers and analyzes information from various areas within a computer or a network to identify possible **incidents** which include both intrusions (attacks from outside the organizations) and misuse (attacks from within the organizations). IDSs can be installed on either a physical or a virtual server. An Intrusion Prevention System (IPS) is a system(s) which can detect an intrusive activity and can also attempt to stop the activity, ideally

before it reaches its targets. Intrusion Detection and Prevention System (IDPS) is software that automates the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents and attempting to stop detected possible incidents.

Lesson Summary

In Lesson 2 we took an in-depth look at denial-of-service attacks and social engineering. We also investigated intrusion attacks, and what motivates hackers to use cyber-attack mechanisms and cross site scripting.

Knowledge Check

1- The HHS network security team installed a system that monitors network traffic and alerts network administrators upon the detection of suspicious activity. The system also has the ability to respond to abnormal or malicious traffic by blocking the user or source IP address from accessing the network altogether. Intrusion Prevention Systems (IPS) are used to prevent which of the following types of attacks?

- A. Denial-of-service attacks
- B. Intrusion attacks
- C. Mail bombing attacks
- D. All of the above.

Answer: B. Intrusion attacks

Explanation: Intrusion attacks can be detected by analyzing network changes and abnormalities.

2- Sandy works at HHS and is greeted by her co-worker, John, at her cubicle. John sits down next to Sandy and fills her in on a meeting Sandy missed. Sandy's computer goes into "sleep" mode as they chat. Sandy quickly remembers that she must complete the email she was composing for her manager. She turns around and types her password on her computer right in front of John. Just as Sandy finishes typing her password, she realizes that John may have been watching her. Sandy normally trusts John, but she doesn't know if she should trust that he wouldn't steal her password. What should Sandy do if John was shoulder surfing?

- A. Report as a possible cybersecurity breach

- B. Quickly change her password
- C. Ask John to forget her password
- D. Forget about it. Sandy is being too suspicious

Answer: B. Quickly change her password.

Explanation: "Shoulder surfing" is common among hackers and users who wish to learn someone's password. John may have been hanging around Sandy's desk, talking and waiting for her to type her password. If this is true, John was "shoulder surfing" while at Sandy's desk. While this may appear to be a cybersecurity **incident**, because Sandy isn't positive that John is not trust-worthy, changing her password is the best option. If the incident is reported, she will be advised to change her password.

Lesson 3: Encryption

Overview

Welcome to Lesson 3! In this lesson we look at how encryption can be used to prevent cybersecurity attacks. By defining cryptographic algorithms, and the differences between symmetric and asymmetric algorithms, we can get a closer look at how encryption actually works.

Objectives

1. Define encryption
2. Understand cryptographic algorithms
3. Analyze and explain the differences between symmetric and asymmetric encryption

Topics

- Encryption
 - Encryption definition
- Cryptographic algorithms
 - Public key (asymmetric) cryptographic algorithm
 - Secret key (symmetric) cryptographic algorithm

Introduction

Let's take a closer look at encryption, and how encryption protocols work.

Encryption

Encryption Definition

Encryption is the conversion of plaintext to cipher text through the use of a cryptographic algorithm. This means that information is converted from normal text to something that a hacker cannot interpret. Because of the need to secure information, cryptographic algorithms are used to encrypt email messages, in an attempt to prevent interception.

Cryptographic Algorithms

Cryptographic algorithms are used to alter data in a readable form (plaintext) to protected or non-readable form (ciphertext) and back to readable form. Deciding the best way to encrypt data will help to prevent **incidents**. In this training, cryptographic algorithms are placed into two categories or classifications: Public Key and Secret (Private) Key.

Public Key (Asymmetric) Cryptographic Algorithm

Asymmetric cryptography, also known as public-key cryptography, is a process that uses a pair of related keys— one public key and one private key—to encrypt and decrypt a message and protect it from unauthorized access or use. A public key is a cryptographic key that can be used by any person to encrypt a message so that it can only be deciphered by the intended recipient with their private key. A private key — also known as a secret key—is shared only with key's initiator.

When someone wants to send an encrypted message, they can pull the recipient's public key, most often stored in the Global Address List, to encrypt the message before sending it. The recipient of the message can then decrypt the message using their related private key stored in their PIV card. This is why you're prompted to enter your PIN to unlock your PIV whenever you open an encrypted email. It's also why your old private encryption keys are stored on your PIV: so they can be used to open old emails that were encrypted using your old public encryption key. These encryption and decryption processes happen automatically; users do not need to physically lock and unlock the message.

Secret Key (Symmetric) Cryptographic Algorithm

A secret key (symmetric) cryptographic algorithm is a cryptographic algorithm that uses a single secret key for both encryption and decryption. Symmetric algorithms or "shared-key" algorithms work by allowing two authorized parties to use shared keys between them when sending encrypted information. A key is used by the sender to send encrypted information, and the same key is used to decrypt the information by the recipient.

Lesson Summary

In Lesson 3, you learned about encryption, cryptographic algorithms, and reviewed the differences between symmetric and asymmetric algorithms.

Knowledge Check

1- What technology both authenticates and keeps information transmitted across a network private so that unauthorized people cannot access it?

- A. Cryptographic algorithm.
- B. Encipher algorithm.
- C. None of the above.
- D. A and B.

Answer: A. Cryptographic algorithm

Explanation: Cryptographic algorithms are sequences of processes, or rules, used to encipher and decipher data.

2- Which type of cryptographic algorithm is a type of encryption where the key used to encrypt the information is not the same as the key used to decrypt the information?

- A. Symmetric encryption
- B. Asymmetric encryption
- C. Encipher
- D. None of the above.

Answer: B. Asymmetric encryption

Explanation: In an asymmetric encryption, a public key and a private key are used. The public key can be revealed, but, to protect the data, the private key must be concealed.

Lesson 4: Firewalls and Virtual Private Networks (VPNs)

Overview

In this lesson we will take a look at how firewalls are used to prevent intrusion; and how VPNs are also used to prevent cyberattacks. Split vs single tunneling is also discussed.

Objectives

1. Define firewall.
2. Discuss the ways that firewalls are used to prevent intrusion.
3. Examine virtual private networks (VPNs).
4. Explore split vs. single tunneling.

Topics

- Firewalls
- Virtual Private Network (VPNs)
- SSL VPN
- Tunneling
- Split vs Single Tunneling

Introduction

There are many ways to prevent network intrusions. Firewalls and VPNs will be reviewed in detail to gain an understanding of which solution may work best in different environments.

Firewalls

What is a Firewall? A firewall is a gateway that limits access between networks in accordance with local security policy. Other definitions include: a hardware/software capability that limits access between networks and/or systems in accordance with a specific security policy; and a device or program that controls the flow of network traffic between networks or hosts that employ differing security postures. A private firewall is a utility on a computer that monitors network activity and blocks communications that are unauthorized. HHS cybersecurity operations teams manage HHS Firewalls.

Virtual Private Networks (VPNs)

A VPN is a virtual network, built on top of existing physical networks that can provide a secure communications mechanism for data and other information transmitted between networks. Like cryptographic algorithms are used to encrypt email, VPN is used to encrypt the Internet. Because a VPN can be used over existing networks, and the Internet, it can facilitate the secure transfer of sensitive data across public networks. This is often less expensive than alternatives such as dedicated private telecommunications lines between organizations or branch offices.

VPNs can also provide flexible solutions, such as securing communications between remote telecommuters and the organization's servers, regardless of where the telecommuters are located. A VPN can even be established within a single network to protect particularly sensitive communications from other parties on the same network.

SSL VPN

Per the NIST Guide to Secure Socket Layer (SSL) VPN document, an SSL tunnel VPN network extension provides a secure connection from the user's system to an organization's network. This host-to-gateway tunnel can handle arbitrary traffic, much like a host-to-gateway IPsec VPN can. SSL tunnel VPN devices can support full or split tunneling.

Tunneling

Tunneling is a technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network. Full tunneling causes all network traffic to go through the tunnel to the organization. Split tunneling routes organization-specific traffic through the SSL VPN tunnel, but other traffic uses the remote user's default gateway.

Split vs Single Tunneling

Per NIST Special Publication 800-53, split tunneling might be desirable by remote users to communicate with local information system resources such as printers/file servers. However, split tunneling would in effect allow unauthorized external connections, making the system more vulnerable to attack and to exfiltration of organizational information. The use of VPNs for remote connections, when adequately provisioned with appropriate security controls, may provide the organization with sufficient assurance that it can effectively treat such connections as non-remote connections from the confidentiality and integrity perspective. VPNs thus provide a means for allowing non-remote communications paths from remote devices. The use of an adequately provisioned VPN does not eliminate the need for preventing split tunneling.

Lesson Summary

In Lesson 4 we discussed the ways firewalls prevent intrusion; how virtual private networks (VPNs) are also used to prevent cyberattacks; and single vs split tunneling.

Knowledge Check

1- Firewalls are used to prevent phishing attacks.

- A. True
- B. False

Answer: False.

Explanation: Firewalls cannot prevent phishing attacks. Firewalls determine whether or not permission should be granted to gain entry into a computing device. Hackers are denied access based on configuration rules. A hacker only needs an email address to send a phishing email to a potential victim. The prevention of phishing attacks must first come from the user of the email account. The user must be educated to prevent phishing attempts from being successful. Phishing attacks are also prevented by report phishing emails to your OpDiv or HHS Incident Response Team.

2- A VPN is needed to create a secure connection on your computer prior to accessing the HHS network.

- A. True
- B. False

Answer: True.

Explanation: A VPN is a virtual network that can provide a secure communications mechanism for data and control information transmitted between networks. This allows email and information systems resources on a network to be connected securely.

Lesson 5: Cloud Computing Vulnerabilities

Overview

Welcome to Lesson 5! In this lesson, we analyze the significant security challenges involving virtual computing environments, such as cloud services.

Objectives

1. Analyze security challenges within virtual environments.
2. Understand cloud service models.
3. Discuss cloud security.

4. Describe virtualization.

Topics

- Cloud Computing
 - Public Cloud
 - Private Cloud
- Security challenges
- Cloud Service Models
 - Infrastructure-as-a-Service (IaaS)
 - Software-as-a-Service (SaaS)
 - Platform-as-a-Service (PaaS)
- Cloud Security
- Virtualization

Introduction

In this section, we will explore security challenges government agencies may experience when using cloud computing services and introduce ways to work securely within virtual computing environments.

Cloud Computing

So, what is cloud computing? Cloud computing has been defined by NIST as a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or cloud provider interaction. The security challenges cloud computing presents are formidable, including those faced by public clouds whose infrastructure and computational resources are owned and operated by an outside party that delivers services to the general public via a multi-tenant platform.

Public Cloud

A public cloud is one in which the infrastructure and computational resources that it comprises are made available to the general public over the Internet. It is owned and operated by a cloud

provider delivering cloud services to consumers and, by definition, is external to the consumers' organizations.

Private Cloud

A private cloud is one in which the computing environment is operated exclusively for a single organization. It may be managed by the organization or by a third party, and may be hosted within the organization's data center or outside of it. A private cloud has the potential to give the organization greater control over the infrastructure, computational resources, and cloud consumers than can a public cloud.

Security challenges

The most significant challenge to a virtual computing environment is security. Creating a secure environment composed of many users while accessing a shared server is difficult; yet it is critical for cloud computing. Meeting the security needs of different applications within a public cloud can also be challenging. Using public clouds may not be suitable for all applications. However, many highly sensitive applications related to critical infrastructure management, health-care applications, etc. are hosted by private clouds.

Cloud Service Models

The service model to which a cloud conforms dictates an organization's scope and control over the computational environment, and characterizes a level of abstraction for its use. Cloud service models may include:

- *Infrastructure-as-a-Service (IaaS)* is a model of service delivery whereby the basic computing infrastructure of servers, software, and network equipment is provided as an on-demand service upon which a platform to develop and execute applications can be established. Its main purpose is to avoid purchasing, housing, and managing the basic hardware and software infrastructure components, and instead obtain those resources as virtualized objects controllable via a service interface. The cloud consumer generally has broad freedom to choose the operating system and development environment to be hosted. Security provisions beyond the basic infrastructure are carried out mainly by the cloud consumer.
- *Software-as-a-Service (SaaS)* is a model of service delivery whereby one or more applications and the computational resources to run them are provided for use on

demand as a turnkey service. Its main purpose is to reduce the total cost of hardware and software development, maintenance, and operations. Security provisions are carried out mainly by the cloud provider. The cloud consumer does not manage or control the underlying cloud infrastructure or individual applications, except for preference selections and limited administrative application settings.

- *Platform-as-a-Service (PaaS)* is a model of service delivery whereby the computing platform is provided as an on-demand service upon which applications can be developed and deployed. Its main purpose is to reduce the cost and complexity of buying, housing, and managing the underlying hardware and software components of the platform, including any program and database development tools. The development environment is typically special purpose, determined by the cloud provider and tailored to the design and architecture of its platform. The cloud consumer has control over applications and application environment settings of the platform. Security provisions are split between the cloud provider and the cloud consumer.

Cloud Security

Three main security and privacy issues relevant to outsourcing public cloud computing services include:

1. **Inadequate Policies and Practices:** The security policies and practices of the cloud provider might not be adequate or compatible with those of HHS.
2. **Weak Confidentiality and Integrity Sureties:** Insufficient security controls in the cloud provider's platform could affect negatively the confidentiality and privacy, or integrity of the system.
3. **Weak Availability Sureties:** Insufficient safeguards in the cloud provider's platform could negatively affect the availability of the system.

FedRAMP provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services used by the US government. Because its goal is to protect US citizen data in the cloud, it's the government's most rigorous security compliance framework.

Before FedRAMP, vendors were faced with different requirements for each Agency they worked with, which meant they had to prepare authorization packages for each one. FedRAMP implemented standard security baselines and processes to provide both an initial authorization

of a cloud service and a mechanism for a consistent security package to be reused across the federal government. This saves time, money, and effort for both Agencies and Cloud Service Providers (CSPs).

Virtualization

Virtualization is the simulation of the software and/or hardware upon which other software runs. This simulated environment is called a virtual machine (VM). There are many forms of virtualization, distinguished primarily by computing architecture layer. For example, application virtualization provides a virtual implementation of the application programming interface (API) that a running application expects to use, allowing applications developed for one platform to run on another without modifying the application itself. Virtualization security should include:

- Security on the physical device that's hosting the virtual environment;
- Keeping control of each virtual machine;
- Creating and implementing security policies for the environment and infrastructure; and
- Creating security controls for each virtual machine.

So with all of this said, is virtualization secure? According to NIST, migrating computing resources to a virtualized environment has little or no effect on most of the resources' vulnerabilities and threats. However, the use of virtualization may help reduce the impact of such exploitation—but virtualization may also provide additional attack vectors, thus increasing the likelihood of successful attacks. Many of the features of virtualization offer both benefits and disadvantages to security.

Lesson Summary

In Lesson 5, we analyzed the significant challenge of security; examined cloud service models; discussed cloud security; and defined virtualization.

Knowledge Check

- 1- HHS is utilizing a cloud service for some network applications. However, when a problem arises at the headquarters of their cloud service provider, HHS does not have control over restoring services to its customers. When will the organization be able to regain access to their cloud and restore services to their customers and employees?

- A. Once the cloud service provider resolves the problem on their end, the organization can then restore services to their customers and employees.
- B. The following day, the organization can restore services to their customers and employees.
- C. Never
- D. The organization can restore services to their customers and employees on their end right away, before the cloud service provider has resolved the problem.

Answer: A. Once the cloud service provider resolves the problem on their end, the organization can then restore services to their customers and employees.

Explanation: Because the organization relies on the cloud service provider for their application services, unfortunately they must wait for the cloud service provider to resolve the issues prior to restoring services to their employees and customers. This is one downside to using cloud services.

2- Cloud computing is a way to simulate software and/or hardware upon which other software runs.

- A. True
- B. False

Answer: A. False.

Explanation: Virtualization is the simulation of the software and/or hardware upon which other software runs.

Lesson 6: Enterprise Performance Life Cycle

Overview

Welcome to Lesson 6! In this lesson, we describe and review the different components of the HHS Enterprise Performance Life Cycle (EPLC).

Objectives

1. Identify Enterprise Performance Life Cycle (EPLC).
2. Examine the phases of the HHS EPLC.

Topics

- EPLC Phases
- Initiation
- Concept
- Planning
- Requirements Analysis
- Design
- Development
- Test
- Implementation
- Operations and Management
- Disposition

Introduction

In this section, we will investigate the phases of the EPLC. The Enterprise Performance Life Cycle is the HHS version of systems development life cycle (SDLC). EPLC incorporates best practices for planning, managing, and overseeing IT investments throughout the investment life cycle within a government environment.

Enterprise Performance Life Cycle Phases

Instructions: Review each EPLC phase below for more information.

Note: The EPLC Policy and EPLC Framework for your OpDiv may vary to ensure OpDiv needs are met.

Initiation

Identifies the business need, develops a Rough Order of Magnitude (ROM) cost and preliminary schedule, and basic business and technical risks. The outcome of the Initiation Phase is the decision to invest in a full business case analysis and preliminary project management plan.

Concept

Identifies the high level business and functional requirements required to develop the full business case analysis and preliminary Project Management Plan for the proposed project. The goals of the Concept Phase are:

- Selection to the HHS IT project portfolio;
- Approval of initial project cost;
- Schedule and performance baselines; and
- Issuance of a Project Charter.

Planning

Completes development of a full Project Management Plan and if applicable, refinement of project cost, schedule, and performance baselines. The goals of the Planning phase is to produce a complete and adequate project plan with sufficient requirements development to validate the planning and project baselines.

Stage Gate Reviews

Ensure that projects, as they move through their life cycles, are fully complying with relevant IT project management requirements and other applicable Critical Partner policies.

Requirements Analysis

Develops detailed functional and non-functional requirements and the Requirements Traceability Matrix (RTM), and awards contracts if needed. The outcome of the Requirements Analysis Phase is award of contracts if needed and approval of the requirements.

Design

Create the Design Document **with careful consideration of privacy requirements and risk management**. The goal of the Design Phase is to complete the Business Product design and successful completion of Preliminary and Detailed Design Reviews with physical Enterprise Architecture diagrams as needed.

Development

Develops code and other deliverables required to build the Business Product and conduct an Independent Verification & Validation Assessment. The purpose of the Development Phase is

complete all coding and associated documentation; user, operator, and maintenance documentation; and test planning.

Test

Thorough testing and audit of the Business Product's design, coding, and documentation occurs in the testing phase. The goal of the Test Phase is to resolve or accept all issues identified during acceptance testing and prepare for training and implementation.

Implementation

Conducts user and operator training, determines readiness to implement, and executes the Implementation Plan, including any phased implementation. The goal of the Implementation Phase is successful establishment of full production capability and completion of the Post-Implementation Review.

Operations and Management

Operates and maintains the production system and conducts annual operational analyses. The goal of the Operations and Maintenance Phase is successful operation of the asset against current cost, schedule, and performance benchmarks.

Disposition

Retires an asset when operational analysis indicates that it is no longer cost-effective to operate the asset. The goal of the Disposition Phase is to deliberate the systematic decommissioning of the Product, with appropriate consideration of data archiving and security, **data disposal according to applicable records schedules**, migration of data or functionality to new assets, and incorporation of lessons learned over the project life cycle.

Important terms to remember include:

Templates - standardized documents with a preset format.

Practices Guides - brief documents describing the background, requirements, and best

practices. Checklists - brief documents listing the items to be noted, checked, remembered, and delivered when completing the accompanying template.

Lesson Summary

In Lesson 6, we investigated the components of the HHS Enterprise Performance Life Cycle (EPLC).

Knowledge Check

1- Which of the following is not a goal of the concept phase?

- A. Selection to the HHS IT project portfolio;
- B. Spending the entire budget;
- C. Schedule and performance baselines;
- D. Issuance of a Project Charter.

Answer: B. Spending the entire budget

Explanation: Budget expenditure is not a goal of the concept phase.

2- Rob works in IT management at HHS and needs a reliable project management plan to integrate best known practices from both the government and commercial sectors, to utilize a process that is dependable and duplicative, and also offers a standard structure for preparing, managing, and supervising IT projects over their life cycle. Rob decides to use the EPLC. Which of the following is the definition of EPLC?

- A. Enterprise Performance Life Cycle
- B. An investment framework developed by representatives of the HHS Optics through the EPLC Workgroup.
- C. None of the above.
- D. A and B.

Answer: D. A and B. A is Enterprise Performance Life Cycle and B is an investment framework developed by representatives; and B is an investment framework developed by representatives of the HHS Optics through the EPLC Workgroup.

Explanation: EPLC stands for Enterprise Performance Life Cycle. EPLC is an investment framework developed by representatives of all HHS Optics through the EPLC Workgroup.

Section 3 - Conclusion

Training Wrap Up

In this training, you learned to:

- Reviewed cybersecurity challenges; including common information and security systems vulnerabilities and cyber-attack mechanisms.
- Discuss security principles and technologies; including intrusion, techniques, and motivation.
- Identify cyber-attack mechanisms; and vulnerabilities within virtual computing environments.
- List and understand the steps of the EPLC.

Training Review

Welcome to the Training Review!

Please read each point below to review the Cybersecurity Essentials Training.

- Phishing attempts: **If you receive an unexpected email with a link or an attachment, verify that it came from a legitimate sender by speaking directly to the sender using a telephone number in the HHS Microsoft Outlook address book or your business records, not the number in the email as it could be a phishing/vishing attempt. Forward all suspected phishing attempts to spam@hhs.gov instead of replying to message.**
- Denial of service attacks: "Denial-of-service attacks" are used to prevent legitimate users of a service from using that service. These attacks can come in the form of mail bombing, saturating network resources, and/or consuming server resources.
- The Enterprise Performance Life Cycle is the HHS version of systems development life cycle (SDLC). EPLC incorporates best practices for planning, managing, and overseeing IT investments throughout the investment life cycle within a government environment.
- Encryption: Cryptographic algorithms are sequences of processes, or rules, used to encipher and decipher messages in a cryptographic system. In asymmetric encryption, a public key and a private key are used. The public key can be revealed, but to protect the data, the private key must be concealed.
- Virtual Private Networks (VPNs): A VPN is a virtual network that can provide a secure communications mechanism for data and control information transmitted between

networks. This allows email and information systems resources on a network to be connected securely. VPNs do not prevent phishing attempts.

- Intrusion Detection System (IDS): Intrusion attacks can be isolated by using an IDS to detect changes and variants that may take place within systems and networks.

Thank you for taking the Cybersecurity Essentials training. You may exit the training at this time. We would love to hear your Feedback.

Feedback

What do you think?

Welcome to the feedback section of the training! We cannot do better without your feedback. Once you have completed the training, you will have the opportunity to provide your feedback in the following form. Feedback is optional, but needed for the continuous improvement of the training. If you decide to complete the form, please send it to OIS_Training@hhs.gov. Thank you for your attention!

Training References

1. NIST SP 800-16, Revision 1, Third Draft, Federal Information Technology/Cybersecurity Training: <https://csrc.nist.gov/publications/detail/sp/800-16/rev-1/draft>
2. A Taxonomy of Operational Cyber Security Risks, Version 2: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf
3. A Taxonomy of Operational Cyber Security Risks, Version 2: http://resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf
4. Security and Privacy Language for Information and Information Technology Procurements, Ver. 2.0: <https://intranet.hhs.gov/it/cybersecurity/policies/security-privacy-language.pdf>
5. Tech-FAQ, Logic Bomb: <http://www.tech-faq.com/logic-bomb.html>
6. Concise Courses, Intrusion Detection Systems Recommended IDS Solutions for 2017: <https://www.concise-courses.com/hacking-tools/intrusion-detection-systems/>
7. LeaseWeb Reliable Hosting, DDoS attacks: <https://www.leaseweb.com/faq/ddos-attacks>
8. Concise Courses, Intrusion Detection Systems Recommended IDS Solutions for 2017: <https://www.concise-courses.com/hacking-tools/intrusion-detection-systems/>
9. SANS Technology Institute, Security Laboratory, Methods of Attack Series: <https://www.sans.edu/cyber-research/security-laboratory/article/denial-of-service>
10. US-Cert, Security Tip (ST04 -014), Avoiding Social Engineering and Phishing Attacks: <https://www.us-cert.gov/ncas/tips/ST04-014>
11. LifeWire, What are WEP, WPA, and WPA2: <https://www.lifewire.com/what-are-wep-wpa-and-wpa2-which-is-best-2377353>
12. Special Publication (NIST SP) - 800-77: <https://csrc.nist.gov/publications/detail/sp/800-77/final>
13. Special Publication (NIST SP) - 800-77: <https://csrc.nist.gov/publications/detail/sp/800-77/final>
14. Special Publication (NIST SP) - 800-113: <https://csrc.nist.gov/publications/detail/sp/800-113/final>
15. TechTarget, SearchCloudProvider, Definition cloud provider: <http://searchcloudprovider.techtarget.com/definition/cloud-provider>
16. NIST SP 800-125 - Guide to Security for Full Virtualization Technologies: <https://csrc.nist.gov/publications/detail/sp/800-125/final>
17. HealthIT.gov, Health Information Exchange (HIE): <https://www.healthit.gov/providers-professionals/standards-interoperability>
18. Enterprise Performance Life Cycle Framework – HHS.gov: <https://www.hhs.gov/ocio/eplc-lifecycle-framework.pdf>
19. Enterprise Performance Life Cycle Framework – HHS.gov: <https://www.hhs.gov/ocio/eplc-lifecycle-framework.pdf>

20. EPLC Artifacts – Life Cycle Phases: <https://intranet.hhs.gov/it/strategy-policy-governance/eplc/artifacts.html#InitiationPhase>

Rules of Behavior for Privileged Users v. 3.0

The following *HHS/OpDiv Rules of Behavior (RoB) for Privileged Users* is an addendum to the *Rules of Behavior for General Users* and provides mandatory rules on the appropriate use and handling of HHS/OpDiv information technology (IT) resources for all HH privileged users, including federal employees, interns, contractors, and other staff who possess privileged access to HHS/OpDiv information systems.¹ Privileged users have network accounts with elevated privileges that grant them greater access to IT resources than non-privileged users. These privileges are typically allocated to system, network, security, and database administrators, as well as other IT administrators.² The compromise of a privileged user account may expose HHS/OpDiv to a high-level of risk; therefore, privileged user accounts require additional safeguards.

A privileged user is authorized (and therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform. System accounts and level of privilege vary dependent upon the role being fulfilled. A privileged user has the potential to compromise the three security objectives of confidentiality, integrity, and availability. Such users include, for example, security personnel or system administrators who are responsible for managing restricted physical locations or shared IT resources and have been granted permissions to create new user accounts, modify user privileges, as well as make system changes. Examples of privileged users include (but are not limited to):

1. Application developer
2. Database administrator
3. Domain administrator
4. Data center operations personnel
5. IT tester/auditor
6. Helpdesk support and computer/system maintenance personnel
7. Network engineer
8. System administrator
9. Security Stewards

Privileged users must read, acknowledge, and adhere to the RoB for Privileged User and any other HHS/OpDiv policy or guidance for privileged users, prior to obtaining access and using HHS/OpDiv information, IT resources and information systems and/or networks in a privileged role. The same signature acknowledgement process followed for the Appendix D, General User RoB, applies to the privileged user accounts. Each OpDiv must maintain a list of privileged users, the privileged accounts those users have access to, the permissions granted to each privileged account, and the authentication technology or combination of technologies required to use each privileged account³.

¹ Per NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, privileged roles include, for example, key management, network and system administration, database administration, and Web administration.

² OMB-16-04 available at [Review-Doc-2015-ITOR-315-1.docx \(whitehouse.gov\)](#), October 30, 2015.

³ Per NIST White Paper, *Best Practices for Privileged User PIV Authentication*, April 21, 2016, available at <https://csrc.nist.gov/publications/detail/white-paper/2016/04/21/best-practices-for-privileged-user-piv-authentication/final>.

Following is the RoB for a privileged user.

I understand that as a privileged user, I must:

1. Use privileged user accounts appropriately for their intended purpose and only when required for official duties.
2. Comply with all privileged user responsibilities in accordance with the HHS Policy for Information Security and Privacy Protection (IS2P) and any other applicable HHS and OpDiv policies.
3. Notify system owners immediately when privileged access is no longer required.
4. Properly protect all information, including media, hard copy reports and documentation as well as system information in a manner commensurate with the sensitivity of the information and securely dispose of information and GFE that are no longer needed in accordance with HHS/OpDiv sanitization policies.
5. Report all suspected or confirmed information security incidents and privacy breaches to the OpDiv Helpdesk, HHS/OpDiv CSIRC, or OpDiv CSIRT as soon as possible, without unreasonable delay and no later than within **one (1) hour** of occurrence/discovery.
6. Complete any specialized role-based security or privacy training as required before receiving privileged system access.

I understand that as a privileged user, I must **not**:

1. Share privileged user account(s), password(s)/passcode(s)/PIV PINs, and other login credentials, including to other system administrators.
2. Conduct official HHS/OpDiv business using personal email or personal online storage account.
3. Use privileged user access to log into any system for non-elevated duties.
4. Install, modify, or remove any system hardware or software unless it is part of my job duties and the appropriate approvals have been obtained or with official written approval.
5. Access the internet for any reason while using my privileged account. This includes downloading of files (including patches or updates), etc.
6. Remove or destroy system audit logs or any other security, event log information unless authorized by appropriate official(s) in writing.
7. Tamper with audit logs of any kind. Note: In some cases, tampering can be considered evidence and can be a criminal offense punishable by fines and possible imprisonment.
8. Acquire, possess, trade, or use hardware or software tools that could be employed to evaluate, compromise, or bypass information systems security controls for unauthorized purposes.
9. Introduce unauthorized code, Trojan horse programs, malicious code, viruses, or other malicious software into HHS/OpDiv information systems or networks.
10. Knowingly write, code, compile, store, transmit, or transfer malicious software code, to include viruses, logic bombs, worms, and macro viruses.
11. Use privileged user account(s) for day-to-day communications and other non-privileged transactions and activities.
12. Elevate the privileges of any user without prior approval from the system owner.
13. Use privileged access to circumvent HHS/OpDiv policies or security controls.

14. Access information outside of the scope of my specific job responsibilities or expose non-public information to unauthorized individuals.
15. Use a privileged user account for web access except in support of administrative related activities.
16. Use any unknown website(s) which may be infected with malware and responding to phishing emails. If I use, I will report to OpDiv Helpdesk, HHS/OpDiv CSIRC, or OpDiv CSIRT as soon as possible, without unreasonable delay and no later than within **one (1) hour** of occurrence/discovery.
17. Use any file sharing program without HHS/OpDiv's permission.
18. Modify security settings on system hardware or software without the approval of a system administrator and/or a system owner.
19. Use systems (either government issued or non-government) without the following protections in place to access sensitive HHS/OpDiv information:
 - Antivirus software with the latest updates
 - Anti-spyware and personal firewalls
 - A time-out function that requires re-authentication after no more than 30 minutes of inactivity on remote access
 - Approved encryption to protect sensitive information stored on recordable media, including laptops, USB drives, and external disks; or transmitted or downloaded via e-mail or remote connections.

SIGNATURE

I have read the above *Rules of Behavior (RoB) for Privileged Users* and understand and agree to comply with the provisions stated herein. I understand that violations of these RoB or HHS/OpDiv information security policies and standards may result in disciplinary action and that these actions may include reprimand, suspensive of access privileges, revocation of access to federal information, information systems, and/or facilities, deactivation of accounts, suspension without pay, monetary fines, termination of employment; removal or debarment from work on federal contracts or projects; criminal charges that may result in imprisonment. I understand that exceptions to these RoB must be authorized in advance in writing by the designated authorizing official(s).

User's Name: _____
(Print)

User's Signature: _____

Date Signed: _____