Module 17: Cloud Security

Cybersecurity Essentials 3.0

Module Objectives

Module Title: Cloud Security

Module Objective: Recommend cloud security requirements based on a given cloud scenario.

Topic Title	Topic Objective
Virtualization and Cloud Computing	Describe ways to manage threats to the private and public cloud.
The Domains of Cloud Security	Explain the domains of cloud security.
Cloud Infrastructure Security	Explain mitigation of threats to the cloud platform infrastructure.
Cloud Application Security	Recommend cloud security applications.
Cloud Data Security	Explain how to secure cloud data.
Protecting VMs	Explain how to secure VM instances.

17.1 Virtualization and Cloud Computing

The Virtual Environment

Virtualization benefits an organization by decreasing the number of physical machines (e.g. servers and workstations) required in the IT environment.

Virtual machines

A hypervisor is a software or hardware program that allows you to run multiple independent operating systems on one physical system. It is a key component of virtualization. There are two virtualization methods:

- Hardware virtualization (type 1 hypervisor) — the guest operating system runs directly on a hardware platform, under the control of the host system.
- Hosted virtualization (type II hypervisor) — an application running on the host machine is used to create virtual machines that consist entirely of software and contain no hardware components.

Virtual machine environments use an operating system, so they need to be patched. Virtual machines share hardware and run with very high privileges. Be aware that an attacker that compromises a virtual machine may be able to compromise the host machine.

The Virtual Environment (Cont.)

Containers

- Unlike a virtual machine, a container consists of just the application and its dependencies. A container uses an engine for operating system emulation. Docker is an open platform that uses OS-level virtualization to deliver software in packages (containers). You can easily move containers around and the application will run. Specialized software such as Kubernetes allows you to manage your containers.

- If a user or application has elevated privileges within a container, the underlying operating system can be compromised.

Virtual Desktop Infrastructure (VDI)

- User desktop environments can be stored remotely on a server using thin client or virtual desktops. This makes it very easy to quickly create, delete, copy, archive, or download configurations over a network. Desktop virtualization requires high availability and storage capacity.

Cloud-Based Technology

Cloud-based technologies enable organizations like @Apollo to access computing, storage, software and servers through the Internet. It moves the technology component from the organization to the cloud provider.

Let's recap from Module 1 the three main computing service models, which are collectively known as XaaS ('anything as a service').

Software as a Service (SaaS) allows users to access application software and databases. Cloud providers manage the infrastructure while users store data on the cloud provider's servers.

Platform as a Service (PaaS) lets an organization remotely access the development tools and services used to deliver such applications, on a subscription basis.

Infrastructure as a Service (IaaS) provides virtualized computing resources over the Internet. The provider hosts the hardware, software, servers, and storage components, and the user pays for a subscription to use these resources.

Cloud Computing

Cloud computing classifications are based on how the service models are deployed.

Private Cloud:

- Also called an internal, corporate, or enterprise cloud, a private cloud is hosted on a private platform.
- A private cloud offers an organization more control over its data, but it may be more expensive than other cloud services due to infrastructure, maintenance, and administration costs.

Public Cloud:

- A public cloud is hosted by a service provider at an offsite facility.
- Users pay a monthly or yearly usage fee to access the cloud. This option costs the organization less for infrastructure, maintenance, and administration — however, the organization has less control over its data.

Cloud Computing (Cont.)

Hybrid Cloud:

- A hybrid cloud combines the private and public cloud by offering control of organizational data, which is still hosted in a public cloud.

Community Cloud:

- A community cloud is a collaborative effort in which more than one organization share and use the same platform.
- This type of cloud is geared toward the needs of an industry such as healthcare or energy.

Fog and Edge Computing

The explosion of IoT devices has led to fog and edge computing.

Fog computing distributes computing between the device and the cloud data center. It plays a critical role in applications where milliseconds matter, such as autonomous vehicles, airlines, and manufacturing applications.

- In fog computing, data is processed within an IoT gateway, or fog node, which is situated within the local area network.

- In edge computing, the data is processed on the device or sensor without being transferred to a data center.

Top Threats to Cloud Computing

Cloud computing is susceptible to many of the same threats that affect physical enterprise networks. However, the cloud environment also introduces unique threats.

For instance, if a threat actor successfully compromises a cloud resource, they could do the following:

- Use the cloud computing resources to target other online entities.
- Host malware on respected cloud providers that will appear harmless or even legitimate.
- Abuse the cloud services to launch DDoS attacks, host pirated contents, send email spam, and conduct phishing campaigns.

Top Threats to Cloud Computing

The following lists some threats associated with cloud computing.

Threat	Description
Data breaches	These occur when protected sensitive data is accessed by an unauthorized entity.
Cloud misconfiguration	This occurs when the cloud computing resource is set up incorrectly, making it vulnerable to attacks.
Poor cloud security architecture strategy	Private cloud security is the responsibility of the organization. However, security for public clouds, hybrid clouds, and community clouds becomes a shared responsibility between the organization and the provider. This can introduce vulnerabilities if the cloud security architecture is not fully understood or correctly implemented.
Compromised account credentials	This occurs when user accounts or access privileges are not properly secured and are hijacked by threat actors. This can lead to a major security threat if the account has high privileges. For example, in public clouds a service account has the highest privilege for accessing and managing cloud assets. A hijacked service account would enable a threat actor to control all cloud resources.

Top Threats to Cloud Computing (Cont.)

The following lists some threats associated with cloud computing.

Threat	Description
Insider threat	This occurs when an employee, contractor, or business partner maliciously or unintentionally compromise the cloud service.
Insecure software user interface (UI) or application programming interface (API)	Cloud computing uses software UIs and APIs for customers to interact with their cloud services. These interfaces are the most exposed points to the internet and therefore, they are targets for threat actors.
Limited cloud usage visibility	This occurs when the cloud client does not have full visibility into the cloud service, making the identification of safe or malicious files more difficult.

17.2 The Domains of Cloud Security

Domains of Cloud Security

There are many resources available promoting cloud computing security.

- A widely respected and referenced resource is the Security Guidance for Critical Areas of Focus in Cloud Computing v4 document.
- Developed by the Cloud Security Alliance (CSA), it promotes best practices to provide security assurance within the cloud computing domains.
- Specifically, the document covers 14 domains of cloud security.

Domains of Cloud Security

Domain Title	Description
Cloud Computing Concepts and Architectures	The domain defines cloud computing terminology and details the overall logical and architectural frameworks used in the Security Guidance document.
Governance and Enterprise Risk Management	The domain describes four areas impacted by cloud computing: • Governance • Enterprise Risk Management • Information Risk Management • Information Security
Legal Issues, Contracts, and Electronic Discovery	The domain describes legal issues associated with cloud computing including the moving of data to the cloud, contracting with cloud service providers, and handling electronic discovery requests in litigation.
Compliance and Audit Management	The domain describes challenges of delivering, measuring, and communicating compliances when organizations migrate from traditional data centers to the cloud.
Information Governance	The domain describes the need to ensure that the use of data and information complies with organizational policies, standards, and strategy including regulatory, contractual, and business objectives.

Domains of Cloud Security (Cont.)

Domain Title	Description
Management Plane and Business Continuity	The domain describes the need to secure the cloud computing management plane (i.e., the protocols and resources used to manage the cloud). It also describes business continuity and disaster recovery procedures to be used by the cloud provider and the cloud client.
Security as a Service	The domain covers the continually evolving security services delivered from the cloud.
Infrastructure Security	The domain describes cloud-specific aspects of infrastructure security and the foundation for operating securely in the cloud.
Virtualization and Containers	The domain describes the need to secure the virtualization technology and virtual assets which are the foundation for cloud computing.
Incident Response	The domain describes the critical aspects of incident response (IR) including the Incident Response Lifecycle and considerations for responders as they work in a cloud environment.
Application Security	The domain provides guidance on how to securely build and deploy applications in cloud computing environments, specifically for PaaS and IaaS.

Domains of Cloud Security (Cont.)

Domain Title	Description
Data Security and Encryption	Data Security should be risk-based since it is not appropriate to secure everything equally. The domain describes those controls related to securing the data itself, of which encryption is one of the most important.
Identity, Entitlement, and Access Management (IAM)	The domain describes how cloud identity is different than traditional identity management.
Related Technologies	The domain provides background and recommendations for technologies that rely nearly exclusively on cloud computing to operate and for technologies that do not necessarily rely on cloud but are commonly seen in cloud deployments.

17.3 Cloud Infrastructure Security

Infrastructure Security

- The Infrastructure Security domain describes cloud-specific aspects of infrastructure security and the foundation for operating securely in the cloud.
- Cloud infrastructure is the foundation on which virtualized cloud resources such as computing, networking, and data storage are built and deployed.
- There are two major layers to infrastructure in cloud computing:
    - The physical and logical compute (CPU, memory, etc.), networks, and storage are combined to create a cloud.
    - The virtual infrastructure managed by a cloud user, that is, the compute, network, and storage assets they access from the resource pools.

Infrastructure Security (Cont.)

- Due to the nature of cloud computing, traditional infrastructure security measures based on the control of physical communication paths and insertion of security appliances do not work.
- Custom cloud security tools include virtual appliances and software agents that are used to secure virtual environments. However, these tools may introduce bottlenecks when accessing resources, or lead to processor overloading. Therefore, the use of virtual appliances should be carefully evaluated and deployed.
- Software-defined networks (SDN) enable new types of security controls and provide an overall gain for network security including:
    - Easy network isolation without constraints of physical hardware
    - SDN firewalls (security groups in cloud computing) applied to assets based on more flexible criteria than hardware firewalls

Cloud Security Responsibilities

- Cloud computing involves cloud clients and Cloud Service Providers (CSPs). Therefore, cloud security works in a shared responsibility model.
- A CSP is responsible for the cloud services to the client, but the client is responsible for the rest of services. The sharing of responsibilities varies according to the type of cloud deployment.
- The following table displays the security implementation responsibility between a client and a CSP in different cloud service models.

Cloud Security Responsibilities (Cont.)

The following table displays the security implementation responsibility between a client and a CSP in different cloud service models.

Security Responsibility	On-premise	IaaS	PaaS	SaaS
Data	Client	Client	Client	Client
Endpoints	Client	Client	Client	Shared
Identity Management	Client	Client	Shared	Shared
Application	Client	Client	Shared	CSP
Network Control	Client	Client	Shared	CSP
Operating System	Client	Client	CSP	CSP
Physical Infrastructure	Client	CSP	CSP	CSP

Other Cloud Infrastructure Security Considerations

Company Security Policies:

- An organization may permit users to download unknown software tools.
- Un-sanctioned apps may increase employee productivity by permitting them to download and use their favorite software tools.
- Unmonitored apps can create security gaps and blind spots.
- Established, well-defined company security policies and educating users are effective ways to manage unknown apps.

Other Cloud Infrastructure Security Considerations (Cont.)

Layered Security:

- Cloud resources can be viewed in four layers, hardware, infrastructure, platform, and application layers. Defense-in-depth strategies can be applied to each of these layers.

- Some layered security options are:
  - Cloud platforms typically have built-in security at the platform level to protect client cloud resources. For example, some CSPs provide built-in DDoS service that clients do not need to configure.
  - A virtual private cloud allocates private subnets that are logically isolated from the internet.
  - While clients will not have access to configure physical firewall devices, CSPs typically provide equivalent firewall functions, or virtual firewalls, such as deny and allow rules and host-level security groups.
  - Flow logs are used to monitor traffic that crosses individual network interfaces.
  - VPNs are used to provide remote user access to the cloud resources, as well as site-to-site connections used in multi-cloud scenarios, or connections between a cloud and on-premises data centers.
  - Identity and access management (IAM) services provide user credential management and user authentication and authorization management. Proper use of IAM is critical to protect cloud resources from being abused.

Other Cloud Infrastructure Security Considerations (Cont.)

Microsegmentation:

- Also referred to as hypersegregation, microsegmentation leverages virtual network topologies to run multiple, smaller, and more isolated networks without incurring additional hardware costs.
- Because the networks are entirely defined in software without many of the traditional addressing issues, it is far more feasible to run these multiple, software-defined environments.
- Microsegmentation techniques allow for more granular control of security for traffic and workflows within the cloud.

17.4 Cloud Application Security

Application Development (Cont.)

To maintain security at all stages of application development, the following robust process needs to be followed.

Developing and testing:

- Software is developed and updated in a development environment, where it can be developed, tested, and debugged before being deployed.
- A development environment is less restrictive than the live environment and has a lower security level.
- Version control software helps track and manage changes to the software code.
- Developers may also work in a sandbox environment so that code is not overwritten as they develop it.
- During testing, developers look at how the code interacts with the normal environment.
    - Quality assurance (QA) can find defects in the software. It is much easier to fix any defect found at this phase.

Application Development

Provisioning and deprovisioning:

- Provisioning is the creation or updating of software.
- Deprovisioning is its removal.
- An organization can use a self-service portal to automate software provisioning and deprovisioning.

Staging and production:

- Staging environments should closely match the organization's production environment.
- By testing in a staging environment, developers can verify that the software runs under the required security settings.
- After the developer runs and tests security, the program can be deployed to production.

Securing Coding Techniques

When coding applications, developers use several techniques to validate that all security requirements have been met.

Normalization is used to organize data in a database and help maintain data integrity. Normalization converts an input string to its simplest known form to ensure that all strings have unique binary representations and that any malicious input is identified.

Stored Procedure: A stored procedure is a group of precompiled SQL statements stored in a database that execute a task. If you use a stored procedure to accept input parameters from clients using different input data, you will reduce network traffic and get faster results.

Securing Coding Techniques (Cont.)

Obfuscation and camouflage

A developer can use obfuscation and camouflage to prevent software from being reverse engineered. Obfuscation hides original data with random characters or data. Camouflage replaces sensitive data with realistic fictional data.

Code reuse means using existing software to build new software, saving time and development costs. Care must be taken, though, to avoid the introduction of vulnerabilities.

SDKs: Third-party libraries and software development kits (SDKs) provide a repository of useful code to make application development faster and cheaper. The downside is that any vulnerabilities in SDKs or third-party libraries can potentially affect many applications.

Input Validation

Controlling the data input process is key to maintaining database integrity. Many attacks run against a database and insert malformed data. Such attacks can confuse, crash, or make the application divulge too much information to the attacker.

Automated input attack example:

- Customers fill out a web application form to subscribe to a newsletter.
- A database application automatically generates and sends email confirmations back to the customers.
- When customers receive the email with a URL link to confirm their subscription, attackers have modified the URL link.
- These modifications can change the username, email address or subscription status of the customers when they click to confirm their subscription.
- Hackers can automate this attack to flood the web application with thousands of invalid subscribers to the newsletter database.

Validation Rules

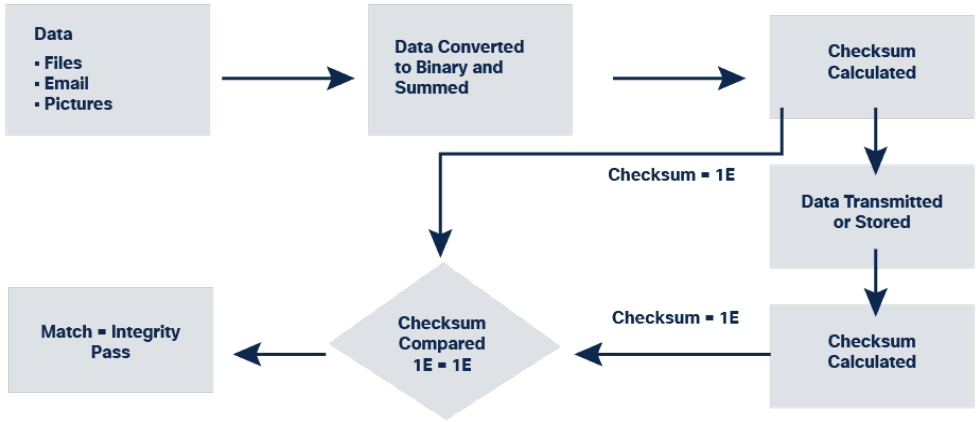
A validation rule checks that data falls within the parameters defined by the database designer. A validation rule helps to ensure the completeness, accuracy, and consistency of data. The criteria used in a validation rule include the following:

- **Size** – checks the number of characters in a data item
- **Format** – checks that the data conforms to a specified format
- **Consistency** – checks for the consistency of codes in related data items
- **Range** – checks that data lies within a minimum and maximum value
- **Check digit** – provides for an extra calculation to generate a check digit for error detection

Integrity Checks

Compromised data can threaten the security of your devices and systems.

An **integrity check** can measure the consistency of data in a file, picture, or record to ensure that it has not been corrupted. The integrity check performs a **hash function** to take a snapshot of data and then uses this snapshot to ensure data has remained unchanged. A **checksum** is an example of a hash function.



Integrity Checks (Cont.)

The checksum process includes:

- **How a checksum works:** A checksum verifies the integrity of files, or strings of characters, before and after they transfer between devices across a local network or the Internet.
  - Checksums convert each piece of information to a value and sum the total.
  - To test the data integrity, a receiving system repeats the process.
  - If the two sums are equal, the data is valid.
  - If not, a change has occurred somewhere along the line.

Integrity Checks (Cont.)

The checksum process includes:

- **Hash functions:** Common hash functions include MD5, SHA-1, SHA-256, and SHA-512. These use complex mathematical algorithms to compare data to a hashed value.
- **Version control:** Organizations use version control to prevent authorized users from making accidental changes. Version control means that two users cannot update the same object, such as a file, database record or transaction, at the exact same time.
- **Backups:** Accurate backups help to maintain data integrity if data becomes corrupted. An organization needs to verify its backup process to ensure the integrity of the backup.
- **Authorization** determines who has access to an organization's resources based on a need-to-know basis.

Other Application Security Practices

How can you be sure that a piece of software you are installing is authentic or that information is secure when browsing the Internet?

- **Code signing** helps prove that a piece of software is authentic.
  - Executables designed to install and run on a device are digitally signed to validate the author's identity and provide assurance that the software code has not changed since it was signed.

- **Secure cookies:** Using secure cookies protects information stored in cookies from hackers.
  - When your client system interacts with a server, the server sends an HTTP response that instructs your browser to create at least one cookie.
  - The cookie then stores data for future requests while you are browsing that website.
  - Web developers should use cookies with HTTPS, to secure cookies and prevent them from being transmitted over unencrypted HTTP.

Lab - Recommend a Cloud Security Solution

In this lab, you will complete the following objectives:

- Part 1: Research and recommend a cloud model and a cloud service model.
- Part 2: Identify shared responsibility for cloud services and cloud security.
- Part 3: Identify five security threats related to cloud computing.
- Part 4: Identify five security measures for deploying ecommerce in cloud.

17.5 Cloud Data Security

States of Data

The States of Data Domain describes controls related to securing the data itself, of which encryption and hashing are of the most important.

Customer data should be protected in the following three states:

- **Data at rest:** This refers to data that is in storage.
  - Data is in this state when no user or process is accessing, requesting, or amending it.
  - Data at rest can be stored on local devices such as a hard disk in a computer, or a centralized network, such as an organization's server.
  - In cloud computing, data at rest can be stored in a cloud and is accessible from any computer connected to the internet, usually with subscription.
  - All data that is not in transit nor in process is considered data at rest.

States of Data (Cont.)

- **Data in transit:** This refers to data which is being transmitted.
  - The data is not at rest, nor is it being processed.
  - The transmission could be within a single server along its motherboard's bus lines, between devices on a single network, or between networks and possibly across the internet.
  - Using cryptography and hashing to protect data in transit is critical for cloud computing.

- **Data in process:** This refers to data during initial input, modification, computation, or output.
  - Data is in this state when it is neither in transit nor at rest.
  - It is data that is being processed.

Cryptography

- **Cryptography** is the science of making and breaking secret codes.
  - By storing and transmitting encrypted data, only the intended recipient can read or process it, and only if they have proper knowledge of the secret used in the encryption algorithm.

- **Encryption** is the process of scrambling data so that unauthorized people cannot easily read it.
  - When enabling encryption, readable data is called plaintext, while the encrypted version is encrypted text or ciphertext.
  - Encryption converts the plaintext readable message to ciphertext, which is the unreadable, disguised message. Decryption reverses the process.
  - Encryption requires a key, which plays a critical role in encrypting and decrypting a message. The person possessing the key can decrypt the ciphertext to plaintext.

Cryptography (Cont.)

There are two classes of encryption algorithms:

- **Symmetric encryption algorithms** use the same pre-shared key to encrypt and decrypt data, a method also known as private key encryption.
  - The Advanced Encryption Standard (AES) is a symmetric encryption algorithm that has a fixed block size of 128 bits with a key size of 128, 192, or 256 bits.
  - The U.S. government uses AES to protect classified information.

- **Asymmetric encryption algorithms** use one key for encryption that is different from the key used for decryption.
  - Asymmetric encryption algorithms include Rivest-Shamir-Adleman (RSA), Diffie-Hellman, ElGamal, and Elliptic curve cryptography (ECC).

Hashing

- **Hashing** is a tool that ensures data integrity by taking binary data (i.e., the message) and producing a fixed-length representation called the hash value (i.e., message digest).

- **Hash functions** are one-way functions used to verify and ensure data integrity.
  - A hash tool can also verify authentication.
  - It works by using a cryptographic hashing function to replace plaintext passwords or encryption keys.
  - A cryptographic hash function has the following properties:
    - The input can be any length.
    - The output has a fixed length.
    - The hash function is one-way and is not reversible.
    - Two different input values will almost never result in the same hash.

17.6 Protecting VMs

Protecting Virtual Machines

- Virtual Machines (VMs or VM instances), just like a physical computer, require patches, updates, and antimalware measures to protect them from external threats.

- The cloud offers additional security options, depending on the specific tools available in a cloud platform, to protect VMs including:

  Plan subnet placement: Carefully choose the subnet for each instance so that it has only the necessary access to the outside world.

  Disable unneeded ports and services: Only enable ports and services that are needed to reduce unnecessary exposure to outside.

Protecting Virtual Machines (Cont.)

Enforce account management and policies: The OS in a VM has default user accounts. Deactivate any default user accounts and create user accounts with best-practice account management policies such as password complexity and least privilege access.

Install antivirus/antimalware software and keep it updated: This can be accomplished through the VM OS, or it might be available as a service from the cloud platform.

Install host-based/software firewall and IDP/IPS: This can be accomplished through the VM OS, or it might be available as a service from the cloud platform.

Protecting VMs from VM Sprawl Attacks

- Creating VM instances in a cloud is a relatively easy process.
  - This may lead to a VM Sprawl issue, where an organization has many VM instances that are not properly managed.
  - If these running instances are not monitored and maintained, they eventually become outdated and vulnerable to attacks.

- A cloud computing client should implement policies to log and audit cloud resources being used.
  - VM sprawl not only presents potential risks, but it also consumes cloud services unnecessarily, such as VM instances, storage, and unassigned public IP addresses.
  - By logging the use of cloud resources, monitoring the running VMs, and auditing the actual usage, an organization can better manage and protect the VMs they really need.

17.7 Cloud Security Summary

What Did I Learn in this Module?

- A hypervisor is a software or hardware program that allows for multiple, independent OSs to run on a single physical system.
- There are two types of hypervisors: Type 1 is hardware virtualization and Type 2 is hosted virtualization.
- Cloud-based technologies let organizations access computing, storage, software, and servers through the internet.
- The three main cloud computing service models are SaaS, PaaS, and IaaS.
- Cloud computing classifications include private, public, hybrid, and community clouds.
- Cloud environment threats include data breaches, cloud misconfiguration, poor security architecture, compromised account credentials, insider threats, insecure software UI or API, and limited cloud usage.
- To protect VMs: plan subnet placement, disable unneeded ports and services, enforce account management policies, install antivirus/antimalware software and keep it updated, and install host-based/software firewalls and IDS/IPS.
- VM Sprawl is where an organization has many VM instances that are not properly managed.
- The Infrastructure Security domain describes cloud-specific aspects of infrastructure security and the foundation for operating securely in the cloud.

What Did I Learn in this Module? (Cont.)

- Two major layers of infrastructure in cloud computing are the physical and logical compute and the virtual infrastructure.
- Cloud resources can be viewed in four layers: hardware, infrastructure, platform, and application.
- Microsegmentation leverages virtual network topologies to run multiple, smaller, and more isolated networks without incurring additional hardware costs.
- The Application Development Domain provides guidance on how to securely build and deploy applications in cloud computing environments such as PaaS and IaaS.
- Techniques for validating security requirements when coding applications include: normalization, stored procedure, obfuscation and camouflage, code reuse, and SDKs.
- Controlling the data input helps to maintain database integrity.
- Validation rules help ensure the security of databases by checking to see if data meets certain rules when it is entered into a field.
- Integrity checks measure the consistency of data in a file, picture, or record to ensure it has not been corrupted.
- The States of Data Domain describes controls related to securing the data itself, of which encryption and hashing are the most important.

What Did I Learn in this Module? (Cont.)

- A checksum is an example of a hash function.
- States of data are data at rest, data in transit, and data in process.
- Cryptography is the science of making and breaking codes.
- There are two classes of encryption algorithms: symmetric and asymmetric.
- Hashing is a tool that ensures data integrity by taking binary data and producing a fixed-length representation called the hash value.
- To protect VMs: Plan subnet placement, disable unneeded ports and services, enforce account management policies, install antivirus/antimalware software and keep it updated, and install host-based/software firewalls and IDS/IPS.