Free Questions for Cybersecurity-Audit-Certificate by certsdeals

Shared by Rosario on 04-10-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

Which of the following is the MOST cost-effective technique for implementing network security for human resources (HR) desktops and internal laptop users in an organization?

Options:

A- Fortified demilitarized zone

B- Software defined perimeter

C- Layer 3 virtual private network

D- Virtual local area network

Answer:

D

Explanation:

The MOST cost-effective technique for implementing network security for human resources (HR) desktops and internal laptop users in an organization is using avirtual local area network (VLAN). A VLAN is a logical grouping of network devices that share the same

broadcast domain regardless of their physical location or connection. A VLAN can enhance network security by isolating different types of traffic or users from each other and applying different security policies or rules based on the VLAN membership. For example, an organization can create a VLAN for HR desktops and internal laptop users that restricts their access to only HR-related systems or resources. A VLAN can also reduce network costs by saving bandwidth, improving performance, and simplifying management.

Question 2

Question Type: MultipleChoice

An IS auditor has learned that a cloud service provider has not adequately secured its application programming interface (API). Which of the following is MOST important for the auditor to consider in an assessment of the potential risk factors?

Options:

A- Resource contention

B- Identity spoofing and phishing

C- Confidentiality, integrity, and availability

D- Denial of service

Answer:

C

Explanation:

The MOST important thing for an IS auditor to consider in an assessment of the potential risk factors when a cloud service provider has not adequately secured its application programming interface (API) is the impact on theconfidentiality, integrity, and availabilityof the cloud service. An API is a set of rules and protocols that allows communication and interaction between different software components or systems. An API is often used by cloud service providers to enable customers to access and manage their cloud resources and services. However, if an API is not adequately secured, it can expose the cloud service provider and its customers to various threats, such as unauthorized access, data breaches, tampering, denial-of-service attacks, or malicious code injection.

Question 3

Question Type: MultipleChoice

Which of the following is the GREATEST risk pertaining to sensitive data leakage when users set mobile devices to "always on" mode?

Options:

A- An adversary can predict a user's login credentials.

B- Mobile connectivity could be severely weakened.

C- A user's behavior pattern can be predicted.

D- Authorization tokens could be exploited.

Answer:

D

Explanation:

The GREATEST risk pertaining to sensitive data leakage when users set mobile devices to "always on" mode is thatauthorization tokens could be exploited. Authorization tokens are pieces of data that are used to authenticate users and grant them access to certain resources or services. Authorization tokens are often stored on mobile devices to enable seamless and convenient access without requiring users to enter their credentials repeatedly. However, if users set their mobile devices to "always on" mode, they increase the risk of losing their devices or having them stolen by attackers. Attackers can then access the authorization tokens stored on the devices and use them to impersonate the users or access their sensitive data.

Question 4

Question Type: MultipleChoice

Using a data loss prevention (DLP) solution to monitor data saved to a USB memory device is an example of managing:

Options:

A- data in use.

B- data redundancy.

C- data availability.

D- data at rest.

Answer:

D

Explanation:

Using a data loss prevention (DLP) solution to monitor data saved to a USB memory device is an example of managingdata at rest. Data at rest is data that is stored on a device or media, such as hard disks, flash drives, tapes, or CDs. Data at rest can be exposed to unauthorized access, theft, or loss if not properly protected. A DLP solution is a tool that monitors and controls the movement and usage of data across an organization's network or endpoints. A DLP solution can prevent users from saving sensitive data to removable devices or alert on any violations of data policies.

Question 5

Question Type: MultipleChoice

Which of the following is a feature of a stateful inspection firewall?

Options:

A- It tracks the destination IP address of each packet that leaves the organization's internal network.

B- It is capable of detecting and blocking sophisticated attacks

C- It prevents any attack initiated and originated by an insider.

D- It translates the MAC address to the destination IP address of each packet that enters the organization's internal network.

Answer:

B

Explanation:

A feature of a stateful inspection firewall is that it iscapable of detecting and blocking sophisticated attacks. A stateful inspection firewall is a type of firewall that monitors and analyzes the state and context of network traffic. It keeps track of the source, destination, protocol, port, and session information of each packet and compares it with a set of predefined rules. A stateful inspection firewall can detect and

block attacks that exploit the logic or behavior of network protocols or applications, such as fragmentation attacks, session hijacking, or application-layer attacks.

Question 6

Question Type: MultipleChoice

Which of the following devices is at GREATEST risk from activity monitoring and data retrieval?

Options:

A- Mobile devices

B- Cloud storage devices

C- Desktop workstation

D- Printing devices

Answer:

A

Explanation:

The device that is at GREATEST risk from activity monitoring and data retrieval is mobile devices. This is because mobile devices are devices that are portable, wireless, and connected to the Internet or other networks, such as smartphones, tablets, laptops, etc. Mobile devices are at greatest risk from activity monitoring and data retrieval, because they can be easily lost, stolen, or compromised by attackers who can access or extract the data stored or transmitted on the devices. Mobile devices can also be subject to activity monitoring and data retrieval by third-party applications or services that may collect or share the user's personal or sensitive information without their consent or knowledge. The other options are not devices that are at greatest risk from activity monitoring and data retrieval, but rather different types of devices that may have different levels of risk or protection from activity monitoring and data retrieval, such as cloud storage devices (B), desktop workstations C, or printing devices (D).

Question 7

Question Type: MultipleChoice

Which of the following is the MOST important consideration when choosing between different types of cloud services?

Options:

A- Emerging risk and infrastructure scalability

B- Security features available on demand

C- Overall risk and benefits

D- Reputation of the cloud providers

Answer:

C

Explanation:

The MOST important consideration when choosing between different types of cloud services is the overall risk and benefits. This is because choosing between different types of cloud services involves weighing the trade-offs between the risk and benefits of each type of cloud service, such as Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS). For example, SaaS may offer more benefits in terms of cost savings, scalability, and usability, but also more risks in terms of security, privacy, and compliance. On the other hand, IaaS may offer more benefits in terms of flexibility, customization, and control, but also more risks in terms of complexity, management, and maintenance. The other options are not the most important consideration when choosing between different types of cloud services, but rather different aspects or factors that affect the choice of cloud services, such as emerging risk and infrastructure scalability (A), security features available on demand (B), or reputation of the cloud providers (D).