Section Quiz

Candidate: Dunkan Gibson (dunkan.gibson)
Date: 4/4/2022 7:21:25 pm • Time spent: 03:06

Score: 60%

Passing Score: 80%

Question 1: ✔ Correct

Which of the following is a technology that tries to detect and stop sensitive data breaches, or data leakage incidents, in an organization?

- Data loss prevention
- Data transmission security
- Public key cryptography
- Data hashing

EXPLANATION

Data loss prevention (DLP) is a technology that tries to detect and stop sensitive data breaches, or data leakage incidents, in an organization. DLP is used to prevent sensitive data from being disclosed to an unauthorized person, whether it is deliberate or accidental.

Data transmission security is the use of secure protocols to encrypt data when it is transmitted. Hashing takes a variable-length string (message) and compresses and transforms it into a fixed-length value. When received, a hash is decrypted into the actual output so the recipient can understand the message.

Public key infrastructure uses certificates, which are electronic documents that use a digital signature, to bind a public key with an identity.

REFERENCES

10.2.2 DLP Facts

q_dlp_dlp_secp7.question.fex

Question 2: ✕ Incorrect

Which rights management category is applied to music, videos, and software that is sold to consumers?

- ~~IRM~~
- DRM
- Static
- Dynamic

EXPLANATION

Digital Rights Management (DRM) is file-level management applied to rich media like music, videos, and software. This strategy uses security technologies such as encryption, permissions, product keys, limited install applications, and persistent online authentication to prevent editing, sharing, and unauthorized copying.

Dynamic data masking replaces original information with a mask that mimics the original in form and function, making it useful for data that is in use or processing.

Static data masking is helpful for data at rest in a database. Masking this way can be specified by field or column.

Information Rights Management (IRM) focuses on business-to-business transfers for files such as documents, emails, spreadsheets, and financial data.

REFERENCES

10.2.2 DLP Facts

q_dlp_drm_secp7.question.fex

Question 3: ✔ Correct

Your organization is having a third party come in and perform an audit on the financial records. You want to ensure that the auditor has access to the data they need while keeping the customers' data secure. To accomplish this goal, you plan to implement a mask that replaces the client names and account numbers with fictional data.

Which masking method are you implementing?

- Dynamic
- Encryption
- Static
- Tokenization

EXPLANATION

Dynamic data masking replaces original information with a mask that mimics the original in form and function, making it useful for data that is in use or processing.

Tokenization replaces actual data with a randomly generated alphanumeric character set called a token.

Static data masking is helpful for data at rest in a database. Masking this way can be specified by field or column.

Encryption happens when plaintext data is changed into unreadable ciphertext using an algorithm.

REFERENCES

10.2.2 DLP Facts

q_dlp_dynamic_01_secp7.question.fex

Question 4: ✔ Correct

Which of the following BEST describes dynamic data masking? (Select two.)

- [ ] It is good to use when making copies of a database for testing.
- [ ] Original data is made irretrievable through reverse-engineering.
- [x] It can be used to control which users can see the actual data.
- [x] It replaces original information with a mask that mimics the original in form and function.
- [ ] It is helpful for data at rest in a database and can be specified by field or column.

EXPLANATION

Dynamic data masking:

- Replaces original information with a mask that mimics the original in form and function, making it useful for data that is in use or processing. For example, someone's name would be replaced with another random name, or credit card numbers would be replaced with random numbers that contain the same number of characters.
- Can be used to control which users can see the actual data.
- Allows original data to be retrieved.

Static data masking:

- Is helpful for data at rest in a database and can be specified by field or column.
- Is good to use when making copies of a database for testing, development, or reporting.
- Makes original data irretrievable through reverse-engineering. A mask copy is made rather than masking the original database.

REFERENCES

10.2.2 DLP Facts

q_dlp_dynamic_02_secp7.question.fex

Question 5: ✕ Incorrect

Which of the following DLP implementations can be used to monitor and control access to physical devices on workstations or servers?

- Endpoint DLP
- Cloud DLP
- Network DLP
- ~~File-level DLP~~

EXPLANATION

Endpoint data loss prevention (DLP) runs on end user workstations and servers. Endpoint DLP is also referred to as a Chinese Wall solution. This could be something as simple as restricting the use of USB devices. Many endpoint-based systems also provide application controls to prevent confidential information transmission and also provide some type of immediate feedback to the user. Giving feedback to the user is based on the concept that not all data leakage incidents are malicious. The employee might not realize that the security-policy violation is inappropriate. The intent is to deter the employee from a similar action in the future.

REFERENCES

10.2.2 DLP Facts

q_dlp_end_dlp_secp7.question.fex

Question 6: ✔ Correct

DLP can be used to identify sensitive files in a file system and then embed the organization's security policy within the file.

Which of the following DLP implementations travels with sensitive data files when they are moved or copied?

- Network DLP
- Cloud DLP
- Endpoint DLP
- File-level DLP

EXPLANATION

File-level DLP is used to identify sensitive files in a file system and then to embed the organization's security policy within the file. This way, the policy travels with the file when it is moved or copied. Since the security policy travels with that file if it's moved or copied, you can continue to control access to the file. For example, you can restrict who it can be transmitted to, even when the file is no longer on your system.

REFERENCES

10.2.2 DLP Facts

q_dlp_file_dlp_secp7.question.fex

Question 7: ✕ Incorrect

You have been offered a position as a security analyst for Acme, Inc. The position will be remote. Acme Inc. has sent you your employment contract using a system that only allows you to open and digitally sign the contract.

Which rights management method is being used?

- ~~Static~~
- IRM
- Dynamic
- DRM

EXPLANATION

Information Rights Management (IRM) focuses on business-to-business transfers for files such as documents, emails, spreadsheets, and financial data. Information rights management utilizes encryption and permissions to create rules for the files. These rules could allow or deny copying and pasting, editing, forwarding, and printing.

Digital Rights Management (DRM) is file-level management applied to rich media like music, videos, and software.

Dynamic data masking replaces original information with a mask that mimics the original in form and function, making it useful for data that is in use or processing.

Static data masking is helpful for data at rest in a database. This type of masking can be specified by field or column.

REFERENCES

10.2.2 DLP Facts

q_dlp_irm_secp7.question.fex

Question 8: ✔ Correct

Which DLP method works by replacing sensitive data with realistic fictional data?

- File-level DLP
- ➡ Masking
- Tokenization
- Encryption

EXPLANATION

Masking works by replacing sensitive data with realistic fictional data. The two types of masking are dynamic data masking and static data masking.

Tokenization replaces actual data with a randomly generated alphanumeric character set called a token.

File-level DLP is used to identify sensitive files in a file system and then to embed the organization's security policy within the file. This way, the policy travels with the file when it is moved or copied.

Encryption happens when plaintext data is changed through an algorithm into unreadable ciphertext.

REFERENCES

10.2.2 DLP Facts

q_dlp_masking_secp7.question.fex

Question 9: ✔ Correct

DLP can be implemented as a software or hardware solution that analyzes traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.

Which of the following DLP implementations analyzes traffic for data containing such things as financial documents, social security numbers, or key words used in proprietary intellectual property?

- File-level DLP
- Endpoint DLP
- Network DLP
- Cloud DLP

EXPLANATION

Network DLP is a software or hardware solution that is typically installed near the network perimeter. Network DLP analyzes network traffic in an attempt to detect sensitive data that is being transmitted in violation of an organization's security policies.

REFERENCES

10.2.2 DLP Facts

q_dlp_net_dlp_secp7.question.fex

Question 10: ✕ Incorrect

Tokenization is another effective tool in data loss prevention. Tokenization does which of the following? (Select two.)

- ~~Identifies sensitive files and embeds them within your security policies~~
- Protects data on its server with authentication and authorization protocols
- Allows continued control access to the file, even when it's no longer in your system
- Replaces actual data with a randomly generated alphanumeric character set
- ~~Allows a security policy to travel with a specific file, even when copied or moved~~

EXPLANATION

Tokenization is another effective tool in data loss prevention. Tokenization does the following:

- Replaces actual data with a randomly generated alphanumeric character set called a token
- Stores original data on a server
- Protects data on its server with authentication and authorization protocols
- Allows authorization only when the correct token is presented

Another data protection tool is rights management. Rights management does the following:

- Protects data at the file level
- Identifies sensitive files and embeds them within your security policies
- Allows a security policy to travel with a specific file, even when copied or moved
- Allows continued control access to a file, even when it's no longer in your system

REFERENCES

10.2.2 DLP Facts

q_dlp_token_secp7.question.fex