Technical University of Denmark

Multiple Choice Question

02239 - Data Security

Author

Student Number:
s213685

Name:
Nikolaos Karavasilis

December 3, 2021

Question

Company A has decided to apply a full disk encryption on all of the computers. Which of the following security goals is the company trying to achieve:

1. **Integrity**.
2. **Availability**
3. **Non-Repudiation**
4. **Confidentiality**

Theory

One of the most important things, that organisations do, is to identify their information assets. Moreover, it is essential for a company to understand the potential threats in order to be able to know what needs to be protected and ,therefore, apply all the necessary defenses. Information assets are divergent and can be any type of information that holds some value for the company. Some of the most characteristic assets are computers, disks, hard drives and operating systems. Every company is responsible of tracking down their assets and afterwards analysing the vulnerabilities associated with them. For example, an asset can be lost, stolen or compromised by a third party. The threats compromise the confidentiality, availability and integrity of an asset and can either be intentional or fluky.

Confidentiality is to make sure that the information is not published to unauthorized entities. A failure to preserve confidentiality means that someone got access to information that was not supposed to access them. In many cases, confidentiality is ensured by using encryption.

Integrity involves maintaining the consistency of the information over its entire life cycle. Data should be kept accurate and complete and ,thus, avoiding any alternation from unauthorized parties. Security systems ensure integrity by designing controls that focus on eliminating threats from unauthorized entities aiming to modify the data.

Availability is to ensure that information assets are accessible from authorized users. This is usually associated with the system uptime. For instance, when the network crashes, users will not be able to use important applications. This phenomenon was captured recently when Facebook went down for many hours, while at the same time their employees were unable to use essential internal tools or even get physical access to the servers.

Examination goal

The question is designed to test the *Evaluation* cognitive domain according to Bloom's taxonomy. Specifically, the question is created to present to the reader a defensive mechanism that a company has used to prevent a possible threat is their asset. Then the reader is asked

to evaluate the mechanism and pick the security goal that the company is trying to achieve. Out of the four possible answers only one holds true. The correct choice depends on using judgments in terms of internal evidence as well as in terms of external criteria.

Stem

By using *Company A has decided to apply a full disk encryption on all of the computers* the reader is trying to understand the current policy. Knowledge is required concerning full disk encryption at this point of the stem. Then the question is aiming to force him in order to evaluate the above mechanism. In more detail, the reader needs to be able to know security risk analysis, since all of the possible answers characterize the key aspects of information assets. As mentioned in the theory section, confidentiality, integrity and availability not only ensure different things but also applying them requires different policies. Therefore, the user should first first evaluate the policy and then try to categorize in depending on the security goal that is trying to accomplish. Also, during the evaluation the reader need to be careful and pay attention to the word computers as well full disk encryption. These are the most important words in order to pick the right answer

Distractors

1st Choice - Integrity: Integrity is part of the three key aspects that most information security policies focus on protecting. This distractor is chosen to confuse the reader. The reader may be familiar with integrity and not pay attention to the phrase full disk encryption. Thus the word computer will confuse the reader to think that this is a classic vulnerability in hardware.

2nd Choice - Availability: Availability is also part of the three key aspects. This distractor is chosen to confuse the reader. Basic knowledge will confuse the reader to think that the policy is implemented only to prevent stolen or lost, since these are the most common vulnerabilities. However, paying attention to the phrase full disk encryption will erase the option of picking this distractor.

3rd Choice - Non-Repudiation: Non-Repudiation refers to a situation where a statement's author cannot successfully dispute its authorship or the validity of an associated contract. This distractor is chosen to confuse the reader, since non-repudiation is not part of the three key aspects used to characterize vulnerabilities.

4th Choice - Confidentiality: Confidentiality is the **correct** answer. The use of encryption protects the contents of the computer's hard disk in the event that it is lost or stolen. This is an example of a confidentiality control.