Intro To Security Concepts

AAA Framework And Cryptography Strategy

IT3358 - Unit 2 Assignment 1

Mary Le

Capella University

April 2021

**AAA Framework and Cryptography Strategy**

**Vulnerabilities and threats of data in storage, transit, and use**

All organizations are under constant threats from different malicious parties. Vulnerabilities are flawed/ weaknesses in a system that can be exploited to cause harm to the organization. Cybercriminals are always creating malware that they can use for their gain. There are different kinds of malware, and they can affect data stored in an organization in different ways (Delfs et al., 2002). Ransomware can be used to encrypt system files and make them inaccessible to the owner. The cybercriminals then ask for payment before they can release the encryption files. Other common types of malware are Trojans and Worms. Data may also be vulnerable to unpatched securities. The organization has to maintain constant updates to be able to protect its data from vulnerabilities. Apart from that, hidden backdoor programs may also give malicious parties access to organizational data.

**Cryptography tools and strategies**

Following technology advances, a lot of sensitive information is constantly being transmitted across the globe daily. Cryptography tools and strategies are vital for protecting information online (Delfs et al., 2002). Multiple tools can be used to protect data and information online. Security tokens can be used to protect data in storage, in transit, and use. A security token is a physical device that holds the information used to verify a person's identity. The token holder plugs the security token into a computer via a computer port to access a service in the network. Key-based authentication can also be used to protect the organization's data. Unlike the security token, key-based authentication employs complex algorithms to verify a client's identity. Each user is given a unique pair of asymmetric keys that they can store in the system they want access to. When a user tries to access data, he/ she will be required to decrypt it using the appropriate security key.

**Non-cryptography strategies for protection of data**

* Employee education and training

Research has shown that employees are some of the weakest links to an organization's data. When employees know how to detect an attack and the necessary steps to mitigate the effect of an attack, they can prevent walling, phishing, and other malicious attacks. Employees can be educated to reduce an organization's exposure to cyber-attacks.

* Tech Components

For an organization to protect its data from external attacks, it needs to have the right components in place; this applies both on-premises and in the cloud. The organization should introduce the various components uniformly so that operations can run smoothly.

* Mobile device management

Mobile device management is always a wise choice when addressing the security of data. It monitors mobile devices such as tablets and smartphones. It also allows an organization to wipe missing devices just if they landed in the wrong hands.

**Tools to support AAA framework in company's security solution**

Security information and event management tool

The tool can allow the organization to monitor a person's activity once the person logs into a network. The management can understand explicitly what the person is doing in the system (Indu et al., 2018); this can help manage data security.

Azure Active Directory

Azure Active Directory can be used in the organization to verify the identity of the users. It can allow users to give users role-based access control to access the information they need to accomplish specific tasks.

**Access control and identity management to protect data**

I can use adaptive multi-factor identification to protect the organization's data (Indu et al., 2018). The adaptive MFA can enable the administrators to set conditional access that verifies specific users and give them a risk rating in real-time. MFA can also enable the administrators to have a configured password experience.

**Policies**

1. All staff is required to treat all organization data confidentially and avoid sharing them with unauthorized personnel.
2. Employees are advised not to write down any of their passwords or leave their computers on and unattended.
3. All breached data will be assessed to determine the risk that it poses to the organization.

References

Delfs H., Knebl H. Knebl H. (2002). *Introduction to Cryptography*, Springer

Indu I., Anand P.R., Bhaskar V. (2018). *Identity and Access Management in Cloud Environment: Mechanisms and Challenges*, Engineering Science and Technology, an International Journal