Controls

While frameworks are used to create plans to address security risks, threats, and vulnerabilities, controls are used to reduce specific risks. If proper controls are not in place, an organization could face significant financial impacts and damage to their reputation because of exposure to risks including trespassing, creating fake employee accounts, or providing free benefits.

Let's review the definition of controls. Security controls are safeguards designed to reduce specific security risks. In this video, we'll discuss three common types of controls: encryption, authentication, and authorization.

Encryption is the process of converting data from a readable format to an encoded format. Typically, encryption involves converting data from plaintext to ciphertext. Ciphertext is the raw, encoded message that's unreadable to humans and computers. Ciphertext data cannot be read until it's been decrypted into its original plaintext form. Encryption is used to ensure confidentiality of sensitive data, such as customers' account information or social security numbers.

Another control that can be used to protect sensitive data is authentication. Authentication is the process of verifying who someone or something is. A real-world example of authentication is logging into a website with your username and password. This basic form of authentication proves that you know the username and password and should be allowed to access the website. More advanced methods of authentication, such as multi-factor authentication, or MFA, challenge the user to demonstrate that they are who they claim to be by requiring both a password and an additional form of authentication, like a security code or biometrics, such as a fingerprint, voice, or face scan.

Biometrics are unique physical characteristics that can be used to verify a person's identity. Examples of biometrics are a fingerprint, an eye scan, or a palm scan. One example of a social engineering attack that can exploit biometrics is vishing. Vishing is the exploitation of electronic voice communication to obtain sensitive information or to impersonate a known source. For example, vishing could be used to impersonate a person's voice to steal their identity and then commit a crime.

Another very important security control is authorization. Authorization refers to the concept of granting access to specific resources within a system. Essentially, authorization is used to verify that a person has permission to access a resource. As an example, if you're working as an entry-level security analyst for the federal government, you could have permission to access data through the deep web or other internal data that is only accessible if you're a federal employee.

The security controls we discussed today are only one element of a core security model known as the CIA triad. Coming up, we'll talk more about this model and how security teams use it to protect their organizations.

Revision #2
Created 5 June 2023 16:46:07 by naruzkurai
Updated 5 June 2023 16:48:23 by naruzkurai