CIS-481: Introduction to Information Security

InfoSec Chapter Exercise #2 - Option A

Team: 1

Participants: Zack Graas, Jacob Forcht, Trevor Hagel

Logistics

A. Get together with other students on your assigned team in person and virtually.

B. Review the two options available and decide on only one to pursue as a team.

C. Discuss and complete this assignment in a collaborative manner. Don't just assign different problems to each teammate as that defeats the purpose of team-based learning.

D. Choose a scribe to prepare a final document to submit via Blackboard for grading, changing the file name provided to denote the number of your assigned **Team**.

Problem 1 *(5 points)*

Why is information security a management problem? What can management do that technology alone cannot?

Employees are traditionally the weakest link in any security policy or plan. They are also one of the only variables in an information security plan that cannot be controlled by technology, only assisted by it. Management is extremely important for any info sec plan because good management is the key to maintaining employee integrity and consistency with data responsibility. Good management is one of the only things that keep employees, the weakest link in a data security plan, on the right track.

Problem 2 *(5 points)*

Why do employees constitute one of the greatest threats to information security that an organization may face?

Employees are one of the greatest threats to information security. This is not because they act maliciously, but rather they often are just forgetful or lax with following the strictly required info-sec protocols. If an employee feels that a security protocol is overbearing or preventing them from working efficiently, they are likely to just ignore it after some time. This is horrible for data security but also unavoidable. This is why an information security plan must take into account not just the technological factors of information access and security, but also the human side of information access and how employees will react to things that may be asked of them.

Problem 3 *(5 points)*

How can dual controls, such as two-person confirmation, reduce the threats from acts of human error and failure? Describe two other common controls that can also reduce this threat?

Dual control is a type of control that helps reduce human error and failures due to it. Dual control is also known as two-person control and is when two workers review and approve each other’s work. Each employee works on their specified task until finished and then submits their work to the other employee to be approved. Each employee double checks the work during the approval process to make sure there are no errors. Another human error threat reducing control is called job rotation. This control is to make sure that multiple employees can do each task. With every employee able to do each required task you can shuffle them around often. Doing this will increase the chances of employees catching misuse or abuse from another employee in the system. Another reason for this is so audits can be performed by another employee to again check for misuse or abuse of the system. Another control measure to reduce human error and failures is forced vacation. Requiring employees to take at least a one-week vacation allows for their work to be audited. Bad actors within the company are usually not willing to take a vacation due to fear of being found out a required vacation. This could even dissuade someone from misusing the system because they know they have to be gone for a week where they could get exposed for malpractice.

Problem 4 *(5 points)*

What is the difference between a regular denial of service (DoS) attack and a distributed denial of service (DDoS) attack? Which is harder to combat? Why?

The difference between a regular denial of service (DoS) attack and a distributed denial of service (DDoS) attack is that a regular denial deals with a single attacker flooding a target’s email with a bunch of requests. Whereas a distributed denial has multiple locations flooding a target’s emails with a bunch of requests. We believe that a distributed denial of service (DDoS) attack is harder to combat. This attack is dealing with multiple locations, and it would take a lot of time to figure out where these attacks are coming from.

Problem 5 *(5 points)*

Briefly describe the types of password attacks addressed in Chapter 2 of your text? Describe three controls a systems administrator can implement to protect against them?

The types of password attacks talked about in chapter 2 were brute force attacks, dictionary attacks, rainbow table attacks, and social engineering attacks. Brute force attacks are when every possible combination of characters and numbers is used to try to randomly guess a password. These attacks are unlikely at working against case-sensitive passwords that include numbers and special characters. A dictionary attack is when a brute force attack is conducted using a dictionary of commonly used passwords. This dictionary includes information related to the targeted user like names, dates, and pets. A rainbow table attack is when a bad actor gets ahold of a password file that is encrypted in hashes and they use a rainbow table to be able to get the plain text form of passwords from the hashed password file. The social engineering attack is when employees are taken advantage of in order to get their password information by bad actors. An example of this is attackers posing as tech support and asking the employee for user name and password information to fix their problems which give the attacker access to the system.

Controls to block the brute force attack would be not allowing passwords that are under a certain strength. For example, forcing people to create a password that is at least 10 characters have capitals, numbers and special characters would be a way to guarantee stronger passwords. Another control would be to limit the amount of failed password attempts so that this attack cannot occur. Another control to prevent the dictionary attack is creating a companies own dictionary that is used to prevent common passwords from being accepted during password creation.