CIS-481: Introduction to Information Security

Module 2 - The Need for Information Security

Exercise #2

Team: 5
Participants: Abril Beascoechea, Nicholas Zhang, Ricardo Portillo, Charles Degboe, and Sam M

Logistics

A. Get together with other students on your assigned **Team** in person and/or virtually.
B. 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 and may impact your performance on assessments, especially with respect to the essay questions.
C. 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?

Information security is a management problem because oftentimes the human factor can be the weakest link in a security system. Management has the responsibility of training employees to ensure that they follow correct procedures and protocols to protect information. This means continuously making sure employees are up to date with security standards and are educated on potential threats and methods for bad actors to access private information.

Furthermore, management has the power to delegate resources and funding to specific areas such as information security. If a company does not provide the effective resources to manage information security, then no matter how good a certain technology is, it may not be enough. This means allocating enough employees and budget to identify and fix any potential vulnerabilities in the system.

Problem 2 *(5 points)*
Why do employees constitute one of the greatest threats to information security that an organization may face?

-Employees are among the greatest threats of an organization's data primary due to human error. Mistakes made by employees can lead to revelation of classified data, entry of erroneous data, accidental data elimination/modification, among other issues. Despite how advance an organization's security technology is, its still vulnerable to social engineering. "People are the weakest link", and cybercriminals can easily deceive and exploit employees who haven't been properly trained or simply made a mistake.

Problem 3 *(5 points)*
How can dual controls, such as two-person confirmation (sometimes referred to as the two-person rule) , reduce the threats from acts of human error and failure? [You've probably seen

an example of this in a movie that shows how a nuclear weapon requires two keys, held by two different people, to be launched.]

Describe two other common controls that can also reduce this threat.

Dual Control is important in keeping safe sensitive informations, systems and networks as they required à second person confirmation. This essentially will help companies or organization reduce the threat on any data breaches, any unauthorized access to informations. The integrity of the system is very important, thats why dual control is in place, that way no person by themselves can authorize or access à data that can bring threat or compromise the system. It also ensure to not let any other user to be more powerful into making critical error that jeopardize the system. Other two common of controls could be user control access and automated control. With user control access only certain individual can access certain data limiting each authorized user to certain informations which reduced any risk of data loss. Automated control limit human from authorizing the system, reducing any human error threat.

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?

-Regular Denial of Service (DoS) occurs when an attacker sends a large number of connection or information requests to a target with the purpose of overloading the target's system, making it unable to respond to legitimate requests for service. This can result in the system crashing or being unable to perform its ordinary functions.
A Distributed Denial of Service (DDoS) attack, on the other hand, consists of a flood of requests being launched to the target simultaneously from many different directions. This involves many machines, making the attack much larger and harder to block. For this reason, a DDoS attack is harder to combat since its way more complex, and currently there are no controls that any single organization can apply. DDoS is considered a weapon of mass destruction on the Internet.

Problem 5 *(5 points)*
Briefly describe the types of password attacks addressed in Module 2 of the text. Describe three controls a systems administrator can implement to protect against one or more of these types of password attacks.

The types of password attack referenced in module 2 are:

Brute Force Attacks: Involves attempting all possible combinations of characters until the right combination is found, effective against weak passwords.

Dictionary Attacks: This attempt lists of common passwords to try and access faster than brute force because it attempts known common passwords.

Rainbow Table Attacks: This is if the password has gets compromised, once the attacker obtains the hash it is easier for them to translate it into the password used.

Social Engineering Attacks: This involves the manipulation of people to try and have an individual give the password to the attacker without the individual knowing. This is human error or failure.

Systems that can be implemented to protect against these password attacks can be Multi-Factor Authentication (MFA) ; this requires the user to set two or more verification methods to gain access to the system. MFA includes password, security tokens and biometric verification, MFA is helpful in protecting against all of the attacks mentioned above.

Another method is password policies, by doing this you can prevent users from setting simple passwords and enforce them to use complex passwords. By doing this you will be better protected against Brute Force attacks and Dictionary attacks

Lastly account lockout mechanisms help prevent brute force and dictionary attacks. This is locking out accounts when there have been multiple failed attempts signing in, this can be either temporarily and it will unlock after a certain time or by administrator unlocking account. This stops attackers from trying thousands of times from trying to access.