CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 2

Names of team members: Shawn Nasr, Nicholas Cunningham, Timothy Mahan, Volody Bestiyanets

Logistics

A. Get into your regular team

B. Discuss and complete the assignment together. Don't just assign different problems to each teammate! That defeats the purpose of team-based learning.

C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

Problem 1

Why is information security a management problem? What can management do that technology alone cannot? (5 pts.)

Information security is a management problem because they facilitate the information security program that protects the organization's ability to function. Management influences and set the policies and procedures that protect information. Management can manage risk, policy, and enforcement of that policy will help to ensure a higher level of information security that technology cannot do alone.

Problem 2

Why do employees constitute one of the greatest threats to information security that an organization may face? (5 pts.)

Employees are one of the greatest threats to information security for an organization because they are the threat agents closest to the information. They use data and information in their activities, on a daily basis, making their human error a huge threat to the organization's confidentiality, integrity, and availability. Employee mistakes can lead to revelation of classified data, entry of erroneous data, accidental deletion/modification of data, storage of data in unprotected areas, and failure to protect information. Training, controls, and ongoing awareness activities can prevent human error.

Problem 3

How can dual controls, such as two-person confirmation, reduce the threats from acts of human error and failure? Describe two other controls that can also reduce this threat? (5 pts.)

Having a second individual confirming the accuracy of a fellow employee's action both increases the confidence in the accuracy of the act as well as incentivizes the first employee to pay closer attention to his work prior to submitting it for peer review as to avoid the tediousness of revising it.

Another control that provides similar effects includes a verification prompt immediately following the action of a user to reduce the likelihood of unintentional acts that could prove costly if there wasn't an opportunity present to confirm or rescind the action. A second dual control that could achieve this same effect includes having key recovery systems in place. This is to assure that there always exists some sort of log or backup version of an affected entity, such as a backup storage device that you could access in the a case of human error negatively affecting the state of the primary storage device, or having a failover server activate in the scenario that the primary one crashes, so as to not interrupt the functionality that these devices provide.

Problem 4

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? (5 pts.)

Denial of Service attacks are often a single computer or a set of computers on the same network segment that at used to request assets from a server or cluster of servers to the point where legitimate users cannot gain access to the resource in question. A Distributed Denial of Service attack is similar to the Denial of Service attack, only the Distributed Denial of Service utilizes zombies or bots from all over the internet to attack a resource. The distributed version of a DOS attack is more difficult to defend against, as a DOS attack can be thwarted by simply blocking the IP address(es) on the network segment from which the attack originates. If you were to try this protection technique when presented with a DDoS attack, your legitimate users would suffer.

Problem 5

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? (5 pts.)

Cracking - To reverse engineer, remove, or bypass a password. If you can guess the password, get rid of it or bypass the password mechanisms, you are cracking.

Brute Force - You essentially just try every possible combination of a password in order to gain access to a network or resource.

Dictionary - You select specific accounts to attack, and you use a dictionary of the most commonly used passwords in a dictionary you put together to guess with.

Rainbow Tables - Used to break hashed passwords. Their primary function is to create a hash table of every possible password for a user with the authentications system cryptographic function. The hashes for passwords are then compared to the table in order to determine the password a user has, which you can output as plain text and use to gain access to the resource in question.

Protections Methods:

Training - You want to make sure the people interacting with a resource or system are aware of it’s function, how it should and should NOT be used, and making sure this knowledge is disseminated prior to the implementation of the system (if new).

Ongoing Awareness Activities - By sending out periodic emails for example, you can keep users abreast of the latest threats, and provide useful reminders for your users to follow the best in security procedures.

Controls - Authentication and Authorization mechanisms (making sure the person trying to access the resource is a legitimate user, and making user that user has the rights to access said resource) can keep non-users with malicious intent, or keeping unintentional persons out of the system. This helps keep resources secure.