Andrew Plum

Mr. Alves-Foss

Cyb 110

10/15/21

Ch. 8 Homework

1) People are the weakest link in the security program because no matter what security measures are put in place, there is little control over people that are a part of the security program. Because of this lack of control, they may participate in unknowingly dangerous activities that jeopardize the effectiveness of the security program. People make mistakes by doing things like clicking on dangerous links, handing over passwords, sending sensitive information through unprotected channels, posting important data in conspicuous places, and trusting people who shouldn't be trusted. Attackers know people are the weakest link in the security program and take advantage of this by conducting social engineering attacks whose success is dependent on how well the attacker can manipulate these people. Because of this, in order to have an effective security program, good training is often required for people to help strengthen their sense of security awareness.

3) You can more effectively reach users in your security awareness and training efforts by presenting the information in an engaging and varied way. For example, in lecture during the training, you might want to highlight the key points to them rather than flooding them with information as they will be more likely to retain the important information then. After the lecture, you could have them engage in some sort of activity like a game where they are quizzed with incentives to do well. This will be a more engaging and interesting environment created for people to partake in. In general, if you present the information in as varied and repeated avenues as possible, people will likely be more engaged in at least one of the avenues than if they just read a lengthy policy which further means they will be better off in retaining the information in the course of the long term.

4) Employees shouldn't attach personal items to your organization's network because allowing them to connect to the organizations network would enable circumventing a lot of the security measures you should have in place. This would mean your security system would be a lot more vulnerable to attacks. If a malicious figure were to install malware on your one of your employee's devices and if they then connected one of these devices to the organization's network, it would make it much easier for the attacker to be successful in the attack they want to do because they could circumvent a lot of the security measures in place. Employees shouldn't connect their devices to the organization's network because it is a security concern.

5) You want to train users to recognize phishing email attacks by training them to pay attention to details big and small. They should look for things like poor imitations of company logos especially that of your own company, poor grammar, and other things which make the website or email or link or file or whatever in question seem illegitimate. Tell them they should act very cautious if they have any doubt about an email, website, file, etc. They should also be very cautious if they don't know who sent them the email, website, link, file, etc. Training your employee users to be more aware of details goes a long way in staving off phishing attacks.

8) Using a wireless network in a hotel with a corporate laptop would be dangerous because these networks likely aren't secure. Because these networks aren't secure, it is much easier for an attacker to get unauthorized access to your data than if the network were secure. If there was a data breach and the data that was leaked was sensitive, it could be disastrous for the company or organization as it could entail bad consequences. The risk simply outweighs the reward of using the unsecure hotel network which is why it would be better to just not use it.