Lab #5

Matthew Langlois - 7731813

Dec. 4

Objective

In this lab we were tasked with playing a security game called CyberCIEGE to help us gain an overall understanding of cyber security in the workplace. This laboratory serves attempts to demonstrate what could potentially happen in an insecure workplace with uneducated staff members.

Scenarios & Objectives

A)

In this game we were observing from the point of a security officer. By observing from this point of view we are able to understand the challenges that security officers face on a daily basis. It helps us understand the constant struggle that the person in charge of security faces. CyberCEIGE allows us to play multiple scenarios to lock down the system further, showing us what could happen if we don't lock down the system.

Often security can be thought of as "what happens WHEN we get hacked" not "what happens IF we get hacked" because in todays world hackers have become so advanced making use of exploits before there are even patches out. So in this game we needed to consider the constraint of how much information we actually store on the system. For example, do we really need to be storing credit card information or can we just pass that along to our payment processor?

In this game, and the real world, a common task required to be performed by the security lead would be to improve existing infrastructure through the use of third party products such as an antivirus software, a secure email server, or even the possibility of a stable version of a certain software needed by the company.

The Security Officer would be responsible for evaluating different products to fill a certain objective in order to calculate the best possible method to protect the system. In CyberCEIGE performing these upgrade were as simple as clicking a button, provided you had enough money. However in the real world there would be complex RFPs done through a bidding process over many months. Obviously this game had to constrain this by removing the whole time line of bidding on a new security product.

In order to balance the game slightly the security officer makes money for uptime and loses money for downtime. The game is over when the user has no money left or the systems have been compromised. Thus the security officer needs to make responsible and educated decisions on what to purchase for the company. If the wrong purchase was made it could lead to the system going down or even being hacked!

B)

I believe that CyberCIEGE did an okay job at teaching the user about security in a workplace from an overall standpoint. It lacked some major things such as specific configuration details, though mimicking something like that in a game would be quite difficult. It was very successful at showing what could happen if a system wasn't secure. Both physical and cyber attacks were conducted in this game, both of which are a reality. Furthermore the game was successful at demonstrating how cost applies to cyber security.
However, the CyberCIEGE user interface was quite confusing an not very intuitive. I believe the game could be made better if the UI had a major overhaul to match more recent games. Perhaps there could even be AI to better react to invalid security choices. Right now the game lets you spend money on anything, even if it doesn't help. It would be nice if there was some AI to demonstrate why the choice made was incorrect.

C)

As stated earlier the game doesn't really take into account time, just money. I believe the game could be made better if the attacks took place over weeks or potentially months within the game. This could take into account for the time it takes to implement policy in the real world. Furthermore it could be adjusted slightly to take into account what a security officer might see on a more daily basis such as scanning for vulnerabilities, ensuring systems are patched, etc...
Obviously a game cannot 100% mimic a real world scenario since there are just too many areas of security to cover. However with these improvements I believe the game will be closer to a real world scenario.

D)

In the first scenario "Stop Worms and Viruses", we learned was to always apply updates regularly. We need to make sure that the antivirus and email scanners are up to date, sometime even requiring manual patching. If updates cannot be performed automatically then we need to make sure our users are trained on how to determine if an email is safe to open.
In the second scenario "Link Encryptors", the lesson learned was to protect sensitive communications between employees using industry standard tools such as VPN and secure channels.
In the third scenario named "Identify Theft", we learned that we should get users to always use strong passwords. They also need to ensure that they log out of systems which contain sensitive information when they are not around otherwise someone might steal their information.
In the fourth scenario named "BortSoft", we learned how to use network and security policies to protect the company from hackers. It built upon the idea of having private subnetworks, and implementing rules as to which macros and such can be opened.
In the fifth scenario named "Life with Macros", we learned that the best way to prevent malicious macros is to disable running macros in the office software. However if you can guarantee that you know the document is from a trusted person then it would be okay to

open the document. The best practice is to disable macros by default and then only run them if they come from a trusted source.
In the sixth scenario named “Passwords”, we learned that a strong rule set for passwords is important. It also shows why it is critical to teach users about secure passwords. Finally, it is best to keep servers on private networks so that they aren’t exposed externally unless absolutely necessary.

Conclusion

Overall, CyberCIEGE served as a decent introductory tool to cyber security practices in the real world. However it lacked the ability to manually configure "real" systems. It also eliminates the entire aspect of time by allowing the player to just immediately purchase upgrades/training. It also doesn’t offer much insight into the data actually being compromised, for example it may have been better allowing the security officer to determine how information is store such as choosing not to store credit card information. This laboratory provided a good insight into what a security officer may face on a daily basis.