Marshall Eddy

CS332-002

Vincent Skimmer

12 April 2017

Breaching Webservers

First and foremost, as a general statement, most people working in an organization (the end user’s) do not know about cyber attacks and how to defend against them; they might not even know what they are in the first place. Honestly it is not their fault, they are just ignorant. For example, an IT guy might not be great at spelling or grammar, because that it not what they practiced and learned in school, but someone with a business degree (or more so and English degree) might have better grammatical skills than the IT guy because they had to learn that stuff for what they were going in to. Thus, these people un-educated in information security frankly just need to be educated.

Generally speaking, there are two main ways for an end-user to be targeted and lead to a breach: Spear Phishing and via a USB (or thumb) drive. USB is more physical, as the attacker would need to physically drop off the USB and the end user would need to physically insert the device into a device connected to the company’s server. Then, there is spear phishing, which is an email directly targeted to an end-user in hopes to trick them into downloading malicious code. In my opinion, there are multiple steps to informing an end-user on how to recognize and handle these situations.

First off, one should inform them of the most common risks, what they are, how often they are used, and how they would harm the company. Hopefully, this will help them realize that this is something they should worry about and something that could potentially happen to them. Once they have a general idea of what the most common attacks, talk to them about how they can prevent this from happening.

For instance, with USB’s they should be told to never use a USB drive unless someone within the company has handed it to them personally, or they have brought it from home. Tell them to never pick up a USB that is not theirs. Then with spear phishing, I think there are several precautions to implement. First, inform them about a junk filter, and ensure they either have that set up or know how to set it up, because junk filters help a decent bit. Next, if they are reading an email and it does not sound like something the sender would say, give the sender a call before doing anything else, if they say they did not send the email, then delete it. If they do not answer, then inspect the email address and ensure it is the correct one, if it is, then wait to speak with the sender in person, or on the phone, if it is not, then delete the email. If any emails look suspicious, delete it.

These are some simply and easy things to teach end-users about and will hopefully help minimalize the risks of a breach to the company. There are several things people can do to prevent breaches, but these are simply ways to avoid the most common and will hopefully stick with the end-user’s in the long run.

References

Class

Textbook