LESSON GUIDE

INTRO TO CYBERSECURITY

Human Factor

2.2.4 - Mitigating the Human Risk

Lesson Overview:

Students will:

- Define ways in which humans present a risk to digital systems
- Examine use of policies, procedures, and security awareness as mitigation tools

Guiding Question: How can humans pose a risk to an organization?

Suggested Grade Levels: 8 - 12

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Mitigating the Human Risk

Slide 1 - Intro Slide

Slide 2 - Humans as Risk Factors

Define ways that humans can pose a risk to the organization - not following the Rules! many users consider security to be an inconvenience and will "go their own" way to make their life easier.

- Using a weak password or one that is used for many different logins
- Installing hardware or software without permission creates a situation where the organization's security features have been bypassed.
- Installing unauthorized software. Example: downloading a game app could include malware.

Here are a few more ways that the humans in an organization present a threat to the system.

- Reverse social engineering is a more sophisticated scam because it requires quite a bit of advance planning. Reverse social engineering is when the attacker finds a way to get the victim to make the initial contact. For example - the hacker sabotages a network, causing a problem to arise. That hacker then advertises that he is the appropriate contact to fix the problem, and then, when he comes to fix the network problem, he requests certain info from the employees such as passwords and gets what he really came for.
- Hoaxes are often discounted as being funny or harmless but in fact they can cause real harm. Hoaxes example = an email that says to delete a file if found on PC, but it was an important OS file and deleting it crashes the PC

Slide 3 - Mitigating Human Risk

Define "mitigate" - we will use that word a lot this year because the practice of cybersecurity isn't to STOP all possible risk, it is to minimize it to acceptable levels. When we "mitigate" a risk or vulnerability, we are reducing the likelihood that it will actually become a vector for an attack. As we saw at the beginning of this unit, the best way to mitigate the human factor risk is to educate the users about security awareness.

Slide 4 - Policies and Procedures

Define "policy" vs "procedure" – confirm that students understand we start with a Policy, we create Procedures as to how policy will be implemented and then we Train users so that they are more likely to follow the procedures. This is our best path to mitigating human risk factors.

1. First the organization has to decide generally how they want their users to behave – this will be a Policy

2. Then the organization will take that policy and create a series of steps that everyone is expected to follow - this will be a Procedure

3. Lastly, the users will receive formal training to understand the goal of the policy and the steps of the Procedure.

Slide 5 - Activity - Clean Desk Policy Test

POLICIES - These are some typical organization computer policies:

- Acceptable use
- Internet Usage
- Email Usage
- Clean Desk

Activity:

- Divide students into small groups of 2 - 3
- Distribute 1 copy of SANS Clean Desk Policy to each group
- Put Messy Desk image on the screen or share it online so that students can clearly see the details - CleanDesk_Image.jpg
- Based on their reading of the SANS Clean Desk Policy, the groups will attempt to find as many of the 10 security mistakes as they can.
- Then join back together as a class and review actual answers from the instructor answer sheet.

Slide 6 - Full picture of Clean Desk Test

Have groups read through the Clean Desk policy and allow the groups some time to identify the security mistakes.

Ask the student groups to report back - have someone write the list on the board. Once you have a list of about 8 - 10 items then compare with the teacher answer sheet to see what was missed or details on why items are against the policy.