CSC116 Project Proposals

Date: January 3rd, 2025

To: Professor Wu Yusen

Fr: Caden Radojevich Headrick, CSC116 Teaching Assistant

Re: CSC116 Project Proposals

Introduction

Healthcare's increasing reliance on technology makes strong cybersecurity absolutely vital. These projects explore critical vulnerabilities and practical solutions within the medical field, offering valuable insights for future healthcare professionals. Let's dive into these fascinating challenges and real-world applications of cybersecurity.

Project 1: Analyzing a Cyberattack Against Healthcare

- **Objective:** Groups select a specific cyberattack that targeted a healthcare organization, analyze its methods and impact, and propose preventative measures.
- **Tasks:**
    - Attack Selection: Each group will select a real-world cyberattack that targeted a healthcare organization. Examples could include ransomware attacks, data breaches, denial-of-service attacks, or other significant incidents.
    - Attack Analysis: Thoroughly research the chosen attack, focusing on:
        - The attacker's methods (e.g., phishing, exploitation of vulnerabilities, social engineering).
        - The specific vulnerabilities exploited (if known).
        - The impact of the attack on the organization (e.g., financial losses, disruption of services, damage to reputation, patient safety implications).
        - The organization's response to the attack.
    - Preventative Measures: Based on the analysis, propose at least two specific preventative measures that the targeted organization could have implemented to mitigate the attack. These measures should be practical and feasible, considering the organization's size and resources. Consider both technical controls (e.g., strong passwords, multi-factor authentication, intrusion detection systems) and non-technical controls (e.g., employee training, security awareness campaigns, incident response planning).

    - Presentation Development: Develop a clear and well-structured presentation that outlines:
        - A brief overview of the chosen cyberattack.
        - A detailed analysis of the attack methods, vulnerabilities, and impact.
        - The proposed preventative measures, with justifications for each.
    - Presentation Delivery: Present the findings to the class, demonstrating a thorough understanding of the cyberattack and the proposed mitigation strategies.
- **Outcome:** A well-structured and informative presentation demonstrating a comprehensive understanding of a specific cyberattack against a healthcare organization, along with practical and feasible preventative measures. The presentation should show critical thinking skills, effective research, and strong communication abilities.

Project 2: Strengthening Data Security in a Small Medical Practice

- **Objective:** To analyze the data security posture of a fictional small medical practice and develop a comprehensive and financially feasible security improvement plan.
- **Tasks:**
    - Scenario Development: Create a detailed scenario for a fictional small medical practice (e.g., a family doctor's office, a dental practice, a small physiotherapy clinic). Describe its size, the types of patient data it handles (electronic health records, billing information, etc.), and its current IT infrastructure (computers, networks, storage). Consider both physical and digital security aspects.
    - Vulnerability Assessment: Identify at least two potential vulnerabilities in the practice's data security, considering risks from internal and external threats (e.g., unauthorized access, data breaches, malware, physical theft, loss of devices). Justify each vulnerability with a brief explanation.
    - Mitigation Strategies: For each identified vulnerability, propose at least two specific mitigation strategies. These strategies should be practical and feasible for a small medical practice. Consider technical (e.g., strong passwords, access controls, encryption) and non-technical (e.g., staff training, security policies, physical security measures) approaches.
    - Prioritization and Implementation Plan: Prioritize the vulnerabilities based on their potential impact and likelihood. Develop a concise implementation plan, outlining the steps needed to implement the chosen mitigation

strategies, including a timeline and resource allocation (this can be hypothetical).

- **Outcome:** A well-structured presentation demonstrating a thorough understanding of data security risks in a small medical practice. The presentation should effectively communicate the identified vulnerabilities, proposed mitigation strategies, and a realistic implementation plan. The analysis should be supported by clear reasoning and evidence. The presentation itself should be clear, concise, and professional.

Project 3: Cybersecurity Awareness Training Program for Healthcare Staff

- **Objective:** To design and present a cybersecurity awareness training program for healthcare staff.
- **Tasks:**
  - Identify common cybersecurity threats relevant to healthcare (e.g., phishing, malware, social engineering).
  - Research effective methods for delivering cybersecurity awareness training (e.g., online modules, workshops, simulations, gamification).
  - Develop a training program with clearly defined learning objectives, activities, and assessment methods. The program should be tailored to the specific needs and technical literacy of healthcare staff.
  - Create a presentation that outlines the training program, justifying the chosen methods and demonstrating a clear understanding of adult learning principles.
- **Outcome:** A comprehensive cybersecurity awareness training program plan and an engaging presentation that effectively communicates the training's content and methods, demonstrating an understanding of adult learning principles and the specific cybersecurity threats faced by healthcare workers.

Group Contract Proposal

I understand that group projects can sometimes lead to conflicts or unequal workloads. To proactively address these potential issues, I propose a group contract that will clearly outline group responsibilities, communication strategies, and a plan for resolving disagreements fairly and efficiently. Outlined in this contract would be consequences for violating the group agreement. This ensures a positive and productive group experience.

Conclusion

These projects offer a unique opportunity for the students to develop crucial cybersecurity skills within a relevant healthcare context. By tackling real-world challenges, they'll gain invaluable experience, fostering a new generation of healthcare professionals equipped to navigate the increasingly complex digital landscape. Their work will directly contribute to a safer and more secure healthcare environment.