Team Meeting

Date: April 16, 2024  
Time: 10:00 AM  
Location: Campus center  
Meeting called by: Omar  
Type of meeting: Project Analysis  
Facilitator: Omar  
Note taker: Adriel  
Timekeeper: Rohan

Attendees:

Omar

Shadath

Rohan

Adriel

Please read:

Project brief on cyber threats in healthcare

Please bring:

Laptops or tablets for note-taking

Minutes

Agenda item: Project Overview  
Presenter: Omar

Discussion:  
Omar provides an overview of the project scope, objectives, and deliverables. He emphasizes the importance of understanding the current digital security threats faced by the hospital system and how to prepare for them. The team discusses the key points and clarifies any questions.

Conclusions:  
The team agrees to focus on analyzing the current threat landscape, identifying various modes of cyber attacks, and formulating recommendations for enhancing the health system's security posture.

Action items

⎫ Develop a detailed project plan outlining tasks, timelines, and responsibilities.

Person responsible: Omar

Deadline: April 20, 2024

⎫ Gather relevant resources and literature on cyber threats in healthcare for further analysis.

Person responsible: Shadath

Deadline: April 18, 2024

⎫ Schedule a meeting with the hospital system's IT team to gather insights into their current security measures and challenges.

Person responsible: Adriel

Deadline: April 22, 2024

Agenda item: Current Threat Landscape  
Presenter: Shadath

Discussion:  
Shadath presents an analysis of the current threat landscape in healthcare, highlighting recent trends in malware, ransomware, and other cyber attacks targeting hospitals and medical facilities. The team discusses the potential impact of these threats and identifies areas of vulnerability within the health system.

Conclusions:  
The team acknowledges the severity of the threats facing the healthcare industry and the urgent need for proactive measures to mitigate risks and protect patient data.

Action items

⎫ Conduct a deeper dive into specific malware and ransomware incidents targeting healthcare organizations.

Person responsible: Shadath

Deadline: April 25, 2024

⎫ Research best practices for strengthening cybersecurity defenses in healthcare settings.

Person responsible: Rohan

Deadline: April 28, 2024

⎫ Prepare a summary report of the current threat landscape findings for presentation to the hospital system's stakeholders.

Person responsible: Adriel

Deadline: May 2, 2024

Agenda item: Modes of Attacks  
Presenter: Rohan

Discussion:  
Rohan discusses various modes of cyber attacks commonly used against healthcare organizations, including social engineering, phishing, and insider threats. The team explores case studies and examples to understand the tactics employed by attackers and their potential impact on the health system.

Conclusions:  
The team recognizes the importance of implementing multi-layered security measures to defend against different modes of cyber attacks and prevent unauthorized access to sensitive healthcare data.

Action items

⎫ Assess the vulnerability of the health system's network infrastructure to social engineering and phishing attacks.

Person responsible: Omar

Deadline: May 5, 2024

⎫ Develop a training program for healthcare staff to raise awareness about common cyber threats and best practices for mitigating risks.

Person responsible: Adriel

Deadline: May 8, 2024

⎫ Review the organization's access control policies and procedures to minimize the risk of insider threats.

Person responsible: Rohan

Deadline: May 10, 2024

Agenda item: Preparation for Health Systems  
Presenter: Adriel

Discussion:  
Adriel presents recommendations for preparing the health system to defend against cyber threats, including implementing robust cybersecurity policies and procedures, conducting regular security assessments, and investing in employee training and awareness programs. The team discusses the feasibility and potential challenges of implementing these recommendations.

Conclusions:  
The team agrees on the importance of taking proactive steps to strengthen the health system's cybersecurity posture and protect patient information from unauthorized access or disclosure.

Action items

⎫ Draft a cybersecurity policy document outlining best practices and guidelines for protecting sensitive healthcare data.

Person responsible: Shadath

Deadline: May 15, 2024

⎫ Schedule a follow-up meeting with the hospital system's stakeholders to present the project findings and recommendations.

Person responsible: Omar

Deadline: May 20, 2024

⎫ Prepare a comprehensive report summarizing the project findings, recommendations, and action plan for the health system's leadership team.

Person responsible: Adriel

Deadline: May 25, 2024

Other Information

Observers: None

Resources: Project brief, cybersecurity literature

Special notes: None

***MEETING WAS 90 MINUTES***