FAKULTI TEKNOLOGI MAKLUMAT
DAN KOMUNIKASI
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
BITS 3363 – NETWORK SECURITY
PROJECT MANAGEMENT

MEETING 2

Title: Network Security Project Integration

INSTRUCTIONS

- Brainstorm with your team members on how to perform project management tasks to provide for data security and quality data assurance. Which task and sub task in your project that protect the data and quality of data assurance in the organization. Just list down the answer. For example, Implementation stage – Surveillance System – CCTV with IP, optical camera, zooming and artificial intelligence mechanism embedded.
- Discuss what is the security measures to govern the network from harmful attacks and threats.
- Meeting 2 is part of the Project Report Documentation.

The purpose of meeting 2 is to look at the progress of the project integration to completion. The Project Manager needs to discuss with team members on how to protect the data and quality assurance of the organization.

MEETING 2: PROGRESS REPORT

Group KeepAlive – Car Manufacturer – Proton

GROUP MEMBERS (MAXIMUM 6 PERSONS IN A GROUP)

1. Muhammad Izham Bin Norhamadi (B032020039)
2. Ahmad Sha Herizam Bin Tahir (B032020009)
3. Muhammad Imran Bin Rosli (B032020043)
4. Affendy Elyas bin Azhari Sharidan (B032020024)
5. Muhammad Firdaus Hafizi Bin Sabri (B032020037)
6. Muhammad Rifqi Bin Ramlan (B032020028)

Date: 16/12/2021

1.0 INTRODUCTION

In this modern era of technology, the topic of security has been a common hot conversation among IT pioneers and technology enthusiast across all platforms like media social and IT forum. Day by day, a lot of security attacks and malware have been introduced and keep growing with different each time it has been discovered. That's why security measures are essential to make sure all projects and businesses are safe and sound from these malicious cyber and network attacks that will potentially bring dangerous harm to our assets. As we know, every business or project has its own management phase to make sure the project runs smoothly. Little did we know that every phase requires set amounts of security measure to be implemented according to its phase as every phase has different security approaches. Implementing a suitable security approach to its phase will utilize fully the security provided and eventually will reduce the risk of network attacks drastically.

1. Initiation Phase
   - Having a well-organized plan for the security measure either physically or digitally
   - Prepare physical security tools such as CCTV and software security such as Antivirus properly and make sure all of it is in good condition to use

2. Planning Phase
   - Determine the best place to place surveillance system – place CCTV at the entrance of the server room – how many CCTV to be put into the server room.
   - Determine what type of access control to use to verify user data for access into the system.
   - Determine what type of Intrusion Detection System (IDS) to use in the network.

3. Execution Phase
   - Intrusion Detection System (IDS) – Implement IDS to monitor network traffic for anomalies

- Setting User Account Policies and Group Policies – Make sure to configure policies to match business needs and provide employees with enough permissions to work

4. Control Phase
   - Server Hardening - Perform server hardening with industry security standards to make sure no vulnerabilities were left undetected
   - Employee permission checkup – Perform a regular checkup on employees’ role and permission to resources and make sure employee does not accumulate more permission than necessary
   - Backup – Schedule a recurring backup for sensitive data to business operation
   - Update – Make sure sensitive systems are up to date to patch out vulnerabilities

5. Closing Phase
   - Hardware Maintenance – Perform a recurring maintenance to servers and hardware that required replacements
   - System review – Review and document the running operation everything ran smoothly and lessen resource waste

(10 Marks)

2.0 Discuss what is the security measures your project team need to provide for safeguarding the network from harmful attacks and threats. Is there any standard of security measures?

- Put up a firewall

  A firewall is a network security device that monitors and filters incoming and outgoing network traffic according to security regulations set by an organization. A firewall can help protect your computer and data by managing your network traffic. It accomplishes this by filtering out unwanted and undesirable network traffic. A firewall verifies access by scanning incoming communication for dangerous elements such as hackers and malware that could infect your machine.

- Use security software (Anti-virus)

  We all know the danger of viruses and malware that can destroy any system or network. To protect our networks against this virus and malware, we need to install and use antivirus software. If dangerous malware infiltrates your network, anti-virus software can assist in detecting and removing it by detecting spam, malware and virus attacks.

- Update programs and systems regularly

  Security improvements are included in updates, which help defend against known problems and vulnerabilities. To avoid becoming a victim of cybercriminals, make sure that software and gadgets are up to date.

- Access Control

  Minimize the security risk of unauthorized access to physical and logical systems. This system works by identifying or verifying the person that is authorized access that includes username and password, PINs, biometric scan and security tokens. Access control also keeps confidential information from falling into the wrong hands.

- Use strong passwords

  Strong passwords are essential for internet security. Make your password tough to guess by using a combination of capital and lower-case letters, numbers and symbols, making it between eight and 12 characters long, avoiding the use of personal data, always changing it regularly, never using it for multiple accounts and using two factor authentication.

- Monitor for intrusion

  Intrusion detectors can be used to keep track of system and network activity. Based on the sort of behaviour it has detected, a detection system can generate an alarm, such as an email notice, if it suspects a potential security breach.

- Use VPN

  VPN can hide IP address to let network going through the configured remote server run by the VPN host.

(10 Marks)

Assessment: [Meeting 2] – (5%) – [PO6, CS3]
CS means Communication