Cyber Security Review and Recommendations for a Small to Medium Sized Organisation

Create the Project Scope Statement

Identify and Meet with Key Stakeholders

- Confirm Final Scope Inclusions and Exclusions
- Identify Project Scope Deliverables
- Identify Stakeholders Engagement

Key Project Implementation Requirements

- Good End-User / Customer Involvement
- Good Executive Management Support
- Clear Statements of Requirements

Organisational Objectives

- To reduce the level of exposure to fraudulent or damaging web, email and internal attacks or unsolicited use..
- To Identify the current Cyber Security status and vulnerabilities within the Organisation
- To identify and recommend new processes, procedures and infrastructure modifications that would enhance the Cyber Security status of the Organisation.

Detail Image of Business Processes within the Scope and their Interactions

- This project will require discussions with the administrators and end users of the network.
- Network access will be required as requested
- Administration documentation such as current policies or procedures will be reviewed.
- A project liaison / project manager will be required from he client to enable clear and up to date communications during the project.
- All physical equipment and network access will be for review purposes only, no alterations to any network data or configurations will be undertaken during this project.

SWOT Analysis of Existing Cyber Security Stature

Project Restraint's are Identified

- This project will not undertake any modifications to network equipment, applications or software systems. This project assumes all actionable deliverables will be undertaken out of this scope.

Assumptions on the Project are Clarified

- It is assumed all relevant data and information will be provided by the client and bound by a confidentiality agreement prior to its provision.
- It is assumed the client will be available and helpful in completing the project with the suggested project timeframe.

Critical Project Outcomes

- This project will provide a snapshot of the organisations present Cyber Security status and will document any provide recommendations to harden the Cyber Security organisational status.

Product and Service Statement

Project Scope

Personelle Review

- Email Vulnerability Awareness Campaign
  - Employee Cyber Awareness Training (Recommendation)
- Network User Policy Review
  - External / Portable Devices
    - Creation of Policies and Procedures (Recommendation)
  - Fixed in Office Devices
    - Creation of Policies and Procedures (Recommendation)
- User Authentication and Information Classification Review
  - Data Access Management Review
    - Creation of Folder Authority Matrix (Recommendation)
    - Implementation of Data Access Restrictions (Recommendation)
- Identification of the Person In Charge
  - Review Network Cyber Security Maintenance Procedures
    - Creation of a Network Maintenance Matrix (Recommendation)
  - Identify the Cyber Security Management Capabilities within the Organisation
    - Ongoing Training and Resource Allocation for Continued Cyber Security Practices (Recommendation)

Infrastructure Review

- Password Control Systems
  - Network and Operating System Password Management Review
    - Implementation of Password Management Procedures (Recommendation)
  - Individual User Password Management Review
    - Implementation of Password Management Procedures (Recommendation)
- Operating System and Application
  - Patching and Security Updates
    - Review of Patching and Security Management Process
  - Application Management Review
- Data Management
  - Data Collection Review
    - Identification of Critical and Private Data
  - Processing of Data Review
  - Data Encryption Requirements Review
  - Storage of Data Review
    - Data Backup Review
      - Data backup Recommendations (Recommendation)
  - Legal Status Acknowledgement
- Firewall
  - Firewall Selection
    - Firewall Hardening (Recoommendation)
      - Application Restrictions
      - Whitelisting
  - Wireless Network Configuration
    - WAN Security Infrastructure Review
      - WAN Security Hardening (Recommendations)

Network Review

- VPN
  - VPN Provider and Information Review
- IDS
  - Identifying Present IDS Management and Implementation
    - Create an IDS Account and Ensure organisational wide account usage (Recommendation)
- SIEM
  - Review the Appropriateness of a SIEM
    - Review Network Monitoring and Incident Logging and Review (Recommendations)
- Honeypot
  - Review the Appropriateness of Honeypot Implementation

Reporting

- Current Cyber Security Status
  - Personnel Report
    - Competency
    - Knowledge
    - Willingness
  - Infrastructure Report
    - Network Infrastructure Life Cycle Stage
  - Network Report
    - IDS Review
    - Monitoring / Patching / Updating Management Practices
- Recommendations Report
  - Personnel Recommendations
  - Infrastructure Receommendations
  - Network Reccommendations

AUSTRALIA ECU EDITH COWAN UNIVERSITY

Cyber Security Review and Recommendations for a Small to Medium Sized Organisation

Link: https://www.mindmeister.com/1813750801

1. Project Scope

1.1. Personelle Review

1.1.1. Email Vulnerability Awareness Campaign

1.1.1.1. Employee Cyber Awareness Training (Recommendation)

1.1.2. Network User Policy Review

1.1.2.1. External / Portable Devices

1.1.2.1.1. Creation of Policies and Procedures (Recommendation)

1.1.2.2. Fixed in Office Devices

1.1.2.2.1. Creation of Policies and Procedures (Recommendation)

1.1.3. User Authentication and Information Classification Review

1.1.3.1. Data Access Management Review

1.1.3.1.1. Creation of Folder Authority Matrix (Recommendation)

1.1.3.1.2. Implementation of Data Access Restrictions (Recommendation)

1.1.4. Identification of the Person In Charge

1.1.4.1. Review Network Cyber Security Maintenance Procedures

1.1.4.1.1. Creation of a Network Maintenance Matrix (Recommendation)

1.1.4.2. Identify the Cyber Security Management Capabilities within the Organisation

1.1.4.2.1. Ongoing Training and Resource Allocation for Continued Cyber Security Practices (Recommendation)

1.2. Infrastructure Review

1.2.1. Password Control Systems

1.2.1.1. Network and Operating System Password Management Review

1.2.1.1.1. Implementation of Password Management Procedures (Recommendation)

1.2.1.2. Individual User Password Management Review

1.2.1.2.1. Implementation of Password Management Procedures (Recommendation)

1.2.2. Operating System and Application

1.2.2.1. Patching and Security Updates

1.2.2.1.1. Review of Patching and Security Management Process

1.2.2.2. Application Management Review

1.2.3. Data Management

1.2.3.1. Data Collection Review

1.2.3.1.1. Identification of Critical and Private Data

1.2.3.2. Processing of Data Review

1.2.3.3. Data Encryption Requirements Review

1.2.3.4. Storage of Data Review

1.2.3.4.1. Data Backup Review

1.2.3.4.1.1. Data backup Recommendations (Recommendation)

1.2.3.5. Legal Status Acknowledgement

1.2.4. Firewall

1.2.4.1. Firewall Selection

1.2.4.1.1. Firewall Hardening (Receommendation)

1.2.4.1.1.1. Application Restrictions

1.2.4.1.1.2. Whitelisting

1.2.4.2. Wireless Network Configuration

1.2.4.2.1. WAN Security Infrastructure Review

1.2.4.2.1.1. WAN Security Hardening (Recommendations)

1.3. Network Review

1.3.1. VPN

1.3.1.1. VPN Provider and Information Review

1.3.2. IDS

1.3.2.1. Identifying Present IDS Management and Implementation

1.3.2.1.1. Create an IDS Account and Ensure organisational wide account usage (Recommendation)

1.3.3. SIEM

1.3.3.1. Review the Appropriateness of a SIEM

1.3.3.1.1. Review Network Monitoring and Incident Logging and Review (Recommendations)

1.3.4. Honeypot

1.3.4.1. Review the Appropriateness of Honeypot Implementation

1.4. Reporting

1.4.1. Current Cyber Security Status

1.4.1.1. Personnel Report

1.4.1.1.1. Competency

1.4.1.1.2. Knowledge

1.4.1.1.3. Willingness

1.4.1.2. Infrastructure Report

1.4.1.2.1. Network Infrastructure Life Cycle Stage

1.4.1.3. Network Report

1.4.1.3.1. IDS Review

1.4.1.3.2. Monitoring / Patching / Updating Management Practices

1.4.2. Recommendations Report

1.4.2.1. Personnel Recommendations

1.4.2.2. Infrastructure Receommendations

1.4.2.3. Network Reccommendations

2. Create the Project Scope Statement

2.1. Organisational Objectives

2.1.1. To reduce the level of exposure to fraudulent or damaging web, email and internal attacks or unsolicited use..

2.1.2. To Identify the current Cyber Security status and vulnerabilities within the Organisation

2.1.3. To identify and recommend new processes, procedures and infrastructure modifications that would enhance the Cyber Security status of the Organisation.

2.2. Detail Image of Business Processes within the Scope and their Interactions

2.2.1. This project will require discussions with the administrators and end users of the network.

2.2.2. Network access will be required as requested

2.2.3. Administration documentation such as current policies or procedures will be reviewed.

2.2.4. A project liaison / project manager will be required from he client to enable clear and up to date communications during the project.

2.2.5. All physical equipment and network access will be for review purposes only, no alterations to any network data or configurations will be undertaken during this project.

2.3. SWOT Analysis of Existing Cyber Security Stature

2.4. Project Restraint's are Identified

2.4.1. This project will not undertake any modifications to network equipment, applications or software systems. This project assumes all actionable deliverables will be undertaken out of this scope.

2.5. Assumptions on the Project are Clarified

2.5.1. It is assumed all relevant data and information will be provided by the client and bound by a confidentiality agreement prior to its provision.

2.5.2. It is assumed the client will be available and helpful in completing the project with the suggested project timeframe.

2.6. Critical Project Outcomes

2.6.1. This project will provide a snapshot of the organisations present Cyber Security status and will document any provide recommendations to harden the Cyber Security organisational status.

2.7. Product and Service Statement

3. Key Project Implementation Requirements

3.1. Good End-User / Customer Involvement

3.2. Good Executive Management Support

3.3. Clear Statements of Requirements

4. Identify and Meet with Key Stakeholders

4.1. Confirm Final Scope Inclusions and Exclusions

4.2. Identify Project Scope Deliverables

4.3. Identify Stakeholders Engagement