New York Tech - Vancouver
20/02/2024

Project Proposal: Enhancing Security Measures for The Accountability Partners

Team: DeViLsFiRe

Members: Arundhati Gadge (1323117), Deepansh Kumar (1321000), Gurpreet Gill (1315782)

Problem Statement:

The proposal aims to address the security concerns of The Accountability Partners, a company relying on Microsoft 365 Enterprise standard for their data storage, communications, and virtual collaboration, alongside maintaining security for their two websites. The central argument revolves around implementing comprehensive security measures, particularly focusing on securing their Microsoft 365 environment, websites, and Zoom meetings, to mitigate risks associated with constant phishing attacks, data security breaches, and develop process for business continuity.

Review of Related Work:

In assessing the current state of The Accountability Partners' cybersecurity measures, it is evident that they lack robust policies and procedures to safeguard their data and communications. Existing literature highlights the significance of implementing tailored cybersecurity policies and utilizing advanced features offered by Microsoft 365 subscriptions to enhance organizational security. However, there is limited research specifically addressing the security concerns of small businesses using Microsoft 365 Enterprise standard version data storage and communication purposes.

This project seeks to build upon existing research by proposing practical solutions tailored to the needs of The Accountability Partners. By evaluating the effectiveness of Microsoft 365 E3 license features in bolstering security and aligning with recognized cybersecurity frameworks such as CIS Critical Security Controls v8 Mapping to NIST CSF, this project aims to provide actionable recommendations to mitigate identified security risks. Developing a process to backup and restore data to drive business continuity in case of disaster.

Project Objective:

The major objectives of the project include:

- Assessing the current/default security policies of The Accountability Partners.
- Evaluating the effectiveness of upgrading to Microsoft 365 E3 license in enhancing security.
- Mapping security considerations based on CIS Critical Security Controls v8 to NIST CSF to provide comprehensive security guidelines.
- Proposing and implementing tailored security measures to address identified vulnerabilities, encompassing their Microsoft 365 environment from phishing email attacks.

Description and Methodology of the Proposed Project:

This project aims to enhance The Accountability Partners' security measures, focusing on their use of Microsoft 365 Business, and the security of their two websites. The primary objective is to mitigate security risks such as constant phishing attacks, data breaches, and unauthorized access.

The project starts with a thorough assessment of the organization's current security posture, including Microsoft 365, and website security. Based on the findings, tailored security measures will be proposed and implemented. This includes configuring advanced settings in Microsoft 365, implementing multi-factor authentication, and enhancing endpoint security.

Additionally, the project will evaluate the potential benefits of upgrading to a Microsoft 365 E3 license to enhance security capabilities. Furthermore, it will provide a comprehensive security framework based on industry standards such as CIS Critical Security Controls v8 mapped to NIST CSF.

Overall, the project will take a systematic approach to identify, mitigate, and manage security risks, aiming to strengthen The Accountability Partners' security posture and mitigate potential threats effectively.

Contribution to Knowledge:

This project will contribute to knowledge by:

- Providing practical insights into enhancing cybersecurity for small businesses utilizing Microsoft 365 for data storage and communication, while incorporating the principles outlined in CIS Critical Security Controls for comprehensive risk mitigation strategies.

- Demonstrating the effectiveness of Microsoft 365 E3 license features in mitigating security risks, particularly in small business environments, thereby highlighting the value of investing in advanced security solutions.

- Offering a comprehensive security framework based on industry best practices, recognized standards, and the principles outlined in CIS Critical Security Controls, providing organizations with a structured approach to addressing cybersecurity challenges and bolstering their security posture effectively.

Resources:

- Access to the administrative account of Microsoft 365 for configuration and implementation of security measures.

- Provision of a test account for Microsoft 365 to conduct evaluations and testing of proposed security measures without impacting production systems.

- A comprehensive list of endpoints used within the company’s infrastructure, including laptops, desktops, mobile devices, and servers, to assess security implications and ensure compatibility with proposed security solutions.

Project Schedule and Milestone Description:

	Description of Work	Estimated Time
Phase One	Initial Assessment and Requirement Gathering	3 - 4 weeks
Phase Two	Proposal Development and Approval	1 week
Phase Three	Implementation of Security Measures	2 - 3 weeks
Phase Four	Evaluation and Testing	2 weeks
Phase Five	Documentation and Reporting	1 week

References/Bibliography:

- Microsoft. Basic Security Set Up for Microsoft 365. https://learn.microsoft.com/en-us/microsoft-365/community/basic-security-set-up-for-microsoft-365#security-within-microsoft-365
- Microsoft. Find the right Microsoft 365 enterprise plan for your organization. https://www.microsoft.com/en-ca/microsoft-365/enterprise/microsoft365-plans-and-pricing
- CIS Critical Security Controls v8 Mapping to NIST CSF document.

This proposal outlines a structured approach to address the security concerns of The Accountability Partners, focusing on enhancing security measures within their Microsoft 365 environment. By leveraging advanced features offered by Microsoft 365 E3 license and aligning with established cybersecurity frameworks, this project aims to provide actionable recommendations to strengthen the organization's security posture.

Need Changes:

Approval Signature

____
Sara Khanchi, Professor