Defending the Digital Realm: A Cybersecurity Initiative for The Accountability Partners

Arundhati Gadge
Department of Computer Science
New York Institute of Technology
Vancouver, Canada
agadge@nyit.edu

Deepansh Kumar
Department of Computer Science
New York Institute of Technology
Vancouver, Canada
dkumar08@nyit.edu

Gurpreet Gill
Department of Computer Science
New York Institute of Technology
Vancouver, Canada
ggill08@nyit.edu

***Abstract*—This report outlines the project aimed at enhancing cybersecurity measures for The Accountability Partners (TAP). Through comprehensive analysis and strategic planning, the project seeks to address vulnerabilities within TAP's infrastructure, particularly focusing on Microsoft 365 and business continuity procedures. Additionally, the project gives a way to include web application testing of TAP's websites to identify potential security risks.**

Keywords—Business Continuity, Web Application Security Testing

I. Introduction (*Heading 1*)

The project's overarching objective is to enhance The Accountability Partners' (TAP) cybersecurity framework by proactively identifying and mitigating potential risks inherent in their current infrastructure setup. Through the implementation of robust security measures and the refinement of business continuity procedures, our aim is to fortify TAP's defenses, safeguarding their sensitive data and ensuring the seamless continuity of business operations. The incorporation of web application testing for TAP's websites further amplifies our commitment to thorough security assessment and risk mitigation within the project's scope.

Problem Statement: TAP heavily relies on Microsoft 365 business standard license for crucial functions like data storage and communication. However, the absence of tailored security measures and a formalized business continuity plan leaves the organization vulnerable to an array of cybersecurity threats. These vulnerabilities, compounded by the pervasive risks of phishing attacks and potential data breaches, underscore the urgent necessity to bolster TAP's overall security posture. Moreover, the presence of potential vulnerabilities in TAP's websites accentuates the critical need for comprehensive cybersecurity measures to mitigate potential risks effectively.

II. Proposed Solution

The proposed solution comprises several key elements tailored to fortify The Accountability Partners' (TAP) cybersecurity framework:

- Implementation of security features within Microsoft 365.
- Development of a comprehensive business continuity plan tailored to TAP's operations, outlining protocols for incident response and recovery.
- Web application security testing of TAP's two websites to identify and address potential security vulnerabilities.

III. Methodology

The project adopts a systematic methodology aimed at fortifying The Accountability Partners' (TAP) cybersecurity framework. It commences with a meticulous assessment of TAP's existing security posture, involving an analysis of current policies, vulnerability scans, and risk identification. Subsequently, tailored security measures are proposed and implemented to address identified vulnerabilities and enhance overall security.

In addition to the foundational security measures, the project encompasses the development of a comprehensive plan for implementing a basic security setup customized to meet TAP's specific needs. This plan encompasses key configurations within Microsoft 365, including enabling multi-factor authentication (MFA), implementing idle session sign-out, blocking legacy authentication, setting user passwords to never expire, configuring a banned password list, managing external sharing settings, setting up account lockout thresholds, applying mobile application management policies, blocking client forwarding rules, and restricting user consent for unmanaged applications. Each configuration is accompanied by relevant guidance and best practices sourced from Microsoft documentation, ensuring thorough implementation and alignment with industry standards.

Furthermore, the project emphasizes the implementation of an email filtering policy to augment cybersecurity defenses. This policy involves the blocking of specific file extensions in email communications to mitigate the risk of malware, viruses, and other potential threats infiltrating the network. A comprehensive list of prohibited file extensions, including .exe, .bat, .cmd, .js,

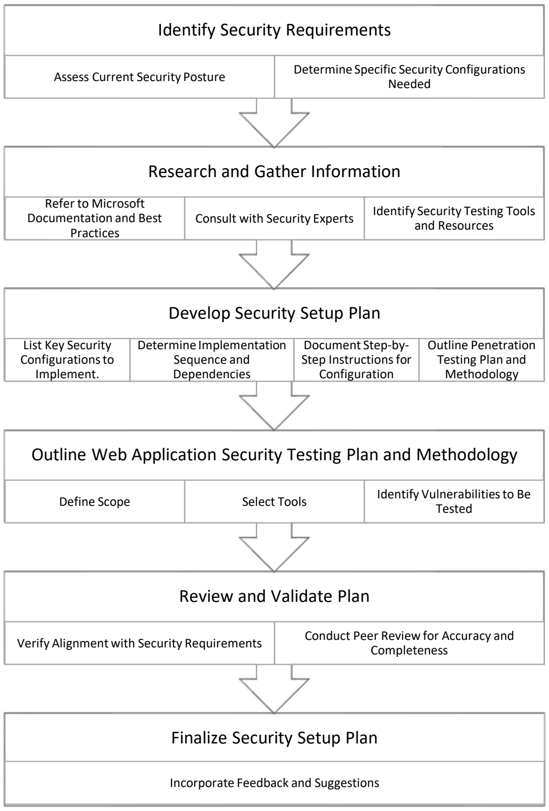
.vbs, .scr, .jar, .ps1, .com, .pif, and .msi, ensures a proactive approach to email security.

Moreover, the project includes the creation of a disclaimer banner for external email defender systems. This process typically involves configuring settings within the email security solution to display a disclaimer banner for external emails. While specific steps may vary depending on the platform utilized, a general guide is provided to facilitate the creation of the disclaimer banner, thereby enhancing awareness and ensuring compliance with organizational policies regarding external email communications.

A. *Experiment/Simulation detail*

The experiment involved simulating the implementation of the identified security configurations within a controlled environment. We utilized Microsoft 365 administrative tools and resources to configure each security measure according to the established plan.

B. *Test Procedure Design*



Identify Security Requirements
Assess Current Security Posture
Determine Specific Security Configurations Needed
Research and Gather Information
Refer to Microsoft Documentation and Best Practices
Consult with Security Experts
Identify Security Testing Tools and Resources
Develop Security Setup Plan
List Key Security Configurations to Implement.
Determine Implementation Sequence and Dependencies
Document Step-by-Step Instructions for Configuration
Outline Penetration Testing Plan and Methodology
Outline Web Application Security Testing Plan and Methodology
Define Scope
Select Tools
Identify Vulnerabilities to Be Tested
Review and Validate Plan
Verify Alignment with Security Requirements
Conduct Peer Review for Accuracy and Completeness
Finalize Security Setup Plan
Incorporate Feedback and Suggestions

C. *Analysis of Test Procedure*

As we proceed with the planning and implementation stages, we are conducting preliminary tests and analyses to assess the potential impact and effectiveness of the planned security configurations. These initial tests involve evaluating the functionality of each proposed security measure and its compatibility with The Accountability Partners existing infrastructure.

D. *Discussion of Project*

At this stage, our project has provided initial insights into the security posture of The Accountability Partners. Preliminary results indicate successful progress in planning and implementing key security configurations within Microsoft 365 existing license. Early observations suggest improvements in areas such as authentication, data protection, and threat mitigation.

E. *Future Development and Improvement Initiatives*

- Continued monitoring and assessment of security measures to ensure ongoing effectiveness and compliance with evolving threats and regulations.
- Implementation of user awareness training and education programs to enhance understanding and adoption of security protocols.
- Collaboration with external security experts or consultants to further strengthen security defenses and address identified vulnerabilities.

IV. Conclusion

In conclusion, the project aims to significantly enhance The Accountability Partners' (TAP) cybersecurity posture by implementing a multifaceted approach tailored to their specific needs. Through the deployment of advanced security features within Microsoft 365, the development of a comprehensive business continuity plan, integration of industry-standard security frameworks like CIS and NIST, and thorough web application testing of TAP's websites, the project seeks to fortify TAP's defenses against evolving cyber threats.

By addressing key vulnerabilities and implementing proactive security measures, TAP can better safeguard their sensitive data, ensure uninterrupted business operations, and mitigate potential risks effectively. The proposed solution not only enhances TAP's resilience to cyber threats but also fosters a culture of cybersecurity awareness and preparedness within the organization.

In essence, the project endeavors to empower TAP with the necessary tools and strategies to navigate the complex cybersecurity landscape, thereby enhancing their overall security posture and enabling them to thrive in an increasingly digital world.

REFERENCES

[1] 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

[2] Microsoft. Find the right Microsoft 365 enterprise plan for your organization.https://www.microsoft.com/en-ca/microsoft-365/enterprise/microsoft365-plans-and-pricing

[3] CIS Critical Security Controls v8 Mapping to NIST CSF document.

V. APPENDICES

A. *Manual/ Implementation*

- Implementation Detail of Email Policy for Blocking File Extensions - https://github.com/Arundhati-NYIT/Project-1-/blob/main/Implementation%20Detail%20of%20Email%20Policy%20for%20Blocking%20File%20Extensions.docx

B. *Data sheets of critical components*

Phase	**Description**	**Estimated Time**
One	Initial Assessment and Requirement Gathering	28th Feb
Two	Proposal Development and Approval	6th March
Three	Implementation of Security Measures	27th March
Four	Web Application Testing (if approved)	10th April
Five	Evaluation and Testing	15th April
Six	Documentation and Reporting	22th April

C. *Initial proposals containing advisor comments.*

Project Proposal Report - https://github.com/Arundhati-NYIT/Project-1-/blob/main/Project%20Proposal%20Report%20-%20DevilsFire.doc

D. *Progress reports with advisor comments*

- Microsoft 365 E3 licensing - https://github.com/Arundhati-NYIT/Project-1-/blob/main/Microsoft%20365%20E3%20licensing.docx
- CIS Controls Framework Recommendations – https://github.com/Arundhati-NYIT/Project-1-/blob/main/CIS_Conrols_Framework_Recommendations.xlsx
- Configurations Planning - office 365 - https://github.com/Arundhati-NYIT/Project-1-/blob/main/Configurations%20Planning%20-%20%20office%20365.docx