**INFT 1202 Capstone Project Report**

**<Team Number: 2 & Team name: 2>**

**A close-up of a logo

Description automatically generated**

**Title of the Project:**

**Proposal 1: Hardening BYOD: Implementing Critical Security Control 3 in a bring your own device (BYOD) Architecture**

**Proposal 2: Technologies to combat spam.**

**Group Members:**

|  |  |  |
| --- | --- | --- |
| **S.No.** | **Student Name** | **Student Id** |
| **1.** | **Bhudev Nevaniya** | 100848467 |
| **2.** | **Meet Brahmbhatt** | 100899436 |
| **3.** | **Maisha Khatoon** | 100899259 |
| **4.** | **Shreeraj Shah** | 100848468 |

**Submitted to Dr. Sk Md Mizanur Rahman**

Contents

[Capstone Project Report 3](#_Toc142304328)

[Proposal 1-Hardening BYOD: Implementing Critical Security Control 3 in a bring your device (BYOD) Architecture. 3](#_Toc142304329)

[Introduction 3](#_Toc142304330)

[Prerequisites 3](#_Toc142304331)

[Network Diagram 3](#_Toc142304332)

[Methodology (Steps) of the project (along with screenshots) 3](#_Toc142304333)

[Challenges Faced 4](#_Toc142304334)

[Conclusion 5](#_Toc142304335)

[Project Management 5](#_Toc142304336)

[References 5](#_Toc142304337)

[Proposal 2- Technologies to combat spam. 5](#_Toc142304338)

[Introduction 5](#_Toc142304339)

[Prerequisites 5](#_Toc142304340)

[Network Diagram 6](#_Toc142304341)

[Methodology (Steps) of the project (along with screenshots) 6](#_Toc142304342)

[Challenges Faced 7](#_Toc142304343)

[Conclusion 7](#_Toc142304344)

[Project Management 7](#_Toc142304345)

[References 8](#_Toc142304346)

# Capstone Project Report

## Proposal 1-Hardening BYOD: Implementing Critical Security Control 3 in a bring your device (BYOD) Architecture.

## Introduction

Bring your device (BYOD) policies allow employees to use personal mobile devices like smartphones and laptops for work. This provides flexibility but also introduces security risks if the devices are not properly secured.

To mitigate these risks, we proposed implementing Critical Security Control 3 (CSC 3) for mobile device security in a BYOD environment. CSC 3 covers establishing secure configurations for systems including mobile devices to prevent exploitation of vulnerable services and settings.

## Prerequisites

* The components required for implementing CSC 3 for BYOD security are:
* Network access control (NAC) system: To enforce access restrictions and device compliance policies.
* Mobile device management (MDM) system: To enroll, configure and manage mobile devices remotely.
* Wireless network infrastructure: To provide secure Wi-Fi connectivity with WPA2-Enterprise authentication.
* Firewalls and intrusion prevention systems: To monitor traffic and detect threats.
* Endpoint security solutions: Antivirus, antimalware tools to protect devices.
* Employee training programs: To educate on BYOD security best practices.

## Network Diagram

The network diagram shows the systems implemented for securing BYOD devices:

* BYOD devices connect via secure Wi-Fi provided by WLAN controllers and access points.
* Traffic is inspected by firewalls and intrusion prevention systems.
* NAC authenticates/authorizes devices and ensures compliance before granting network access.
* MDM manages mobile devices and can take actions like remote wipes.
* Endpoint security solutions like antivirus are installed on devices.

## Methodology (Steps) of the project (along with screenshots)

We implemented CSC 3 in a phased manner through these steps:

**Defined BYOD Security Policy:**

* Documented allowed device types, OS versions, required apps, etc.
* Specified password, encryption, and malware protection requirements.
* Outlined acceptable usage and data security rules.
* Identified remediation actions for non-compliant devices.

**Implemented Network Access Control:**

* Deployed NAC solution with required network integration and endpoints.
* Configured NAC policies based on defined BYOD security rules.
* Set up NAC to authenticate users/devices and check compliance.
* Enabled dynamic access controls to allow, deny or limit network access.

**Deployed Mobile Device Management:**

* Evaluated and selected suitable MDM platform.
* Enrolled employee BYOD devices into MDM.
* Applied secure configuration profiles to devices as per policy.
* Used MDM to regularly audit devices and take remote actions.

**Secured Wireless Network:**

* Implemented WPA2-Enterprise authentication on Wi-Fi.
* Set up separate SSID and VLAN for BYOD devices.
* Enabled wireless intrusion prevention and anomaly detection.

**Installed Endpoint Security Software:**

* Deployed antivirus, antimalware tools on BYOD devices.
* Configured automated scanning and signature updates.
* Enabled firewalls and remote management capabilities.

**Conducted Security Awareness Training:**

* Educated employees on BYOD security best practices through training.
* Communicated BYOD policy requirements.
* Shared information on the latest mobile threats.

**Performed Regular Security Assessments:**

* Audited BYOD devices using MDM for compliance.
* Conducted penetration testing and vulnerability assessments.
* Reviewed logs/events for anomalies.
* Updated security measures based on findings.

## Challenges Faced

Some challenges faced during this project:

* Getting employee buy-in for enrolling devices and installing security software. Clear communication of benefits was needed.
* A variety of devices/platforms made centralized configuration and management difficult.
* Regular security assessments required significant time and expertise, impacting costs.
* Keeping pace with evolving mobile OS versions, new vulnerabilities, and attack methods.
* Limited control over employee-owned devices. Security depended on voluntary compliance.
* Privacy concerns regarding monitoring personal devices, though policies helped mitigate this.

## Conclusion

Implementing CSC 3 establishes strong mobile device security practices crucial for BYOD adoption. Key lessons:

* Defining the BYOD policy upfront with all stakeholders is essential.
* Solutions like MDM and NAC are critical for managing and securing devices at scale.
* Training and transparency are key for employee adoption.
* Must budget for expert resources to create/manage configurations, assessments, etc.
* Security requires continuous improvement as threats evolve.

Overall, a layered strategy with access controls, centralized management, network security, training, and assessments enables secure BYOD.

## Project Management

* Bhudev Nevaniya: Researched BYOD security frameworks and best practices. Documented draft BYOD security policy.
* Meet Brahmbhatt: Evaluated NAC and MDM solutions. Provided network architecture recommendations and design.
* Maisha Khatoon: Planned endpoint protection rollout. Conducted employee awareness training.
* Shreeraj Shah: Defined wireless network security controls. Set up compliance monitoring and assessment programs.

## References

## Proposal 2- Technologies to combat spam.

## Introduction

Spam emails containing malicious links, attachments, and phishing attempts can significantly impact an organization's security and productivity.

This project focused on implementing a layered anti-spam strategy including technologies like email gateways, authentication protocols, and user education to defend against unwanted and dangerous emails.

## Prerequisites

The main requirements for deploying anti-spam controls are:

* Email gateway solution for filtering and analyzing emails.
* Tools for content-based filtering, sender reputation analysis, and machine learning to detect spam.
* Email authentication mechanisms like SPF, DKIM, and DMARC
* Anti-malware and anti-phishing capabilities
* Email encryption solutions such as TLS and PGP
* Security awareness training for employees
* Monitoring capabilities to track the effectiveness of controls.

## Network Diagram

The network diagram shows the anti-spam systems implemented:

* Emails pass through the gateway which scans for spam using different techniques.
* Suspicious emails can be quarantined.
* Emails are authenticated using SPF, DKIM, and DMARC.
* Encryption can be applied to sensitive emails.
* Anti-malware tools analyze attachments/links.
* Logs are sent to SIEM for monitoring and analytics.

## Methodology (Steps) of the project (along with screenshots)

We implemented anti-spam controls using a phased approach:

**Assessed Email Security:**

* Analyzed current email protection for gaps in spam filtering, phishing prevention, etc.
* Identified high-risk users needing additional safeguards.

**Deployed Email Gateway:**

* Evaluated solutions based on advanced spam filtering capabilities.
* Integrated selected gateway with mail server via SMTP.

**Configured Spam Filters:**

* Enabled different techniques like reputation checks, content analysis, and machine learning.
* Created allow/block lists and whitelists for approved senders.
* Set up a quarantine to isolate suspicious messages.
* Fine-tuned filters to achieve high accuracy and minimize false positives.

**Implemented Email Authentication:**

* Configured SPF, DKIM, and DMARC using DNS records.
* Enforced strict DMARC policies to block unauthenticated emails.

**Installed Anti-Malware and Anti-Phishing:**

* Deployed malware prevention tools to scan attachments/links.
* Implemented anti-phishing capabilities to identify and reject phishing scams.
* Customized rules based on observed phishing techniques.

**Enabled Email Encryption:**

* Implemented TLS for encrypting communication between mail servers.
* Allowed users to encrypt sensitive emails via PGP.

**Ongoing Monitoring:**

* Continuously monitored performance using SIEM and analytics.
* Periodically tested systems using simulated phishing and spam attacks.
* Adjusted configurations to improve the accuracy of controls.

**Security Awareness Training:**

* Educated employees on identifying spam/phishing emails and reporting threats.
* Sent regular simulated phishing emails for training.

## Challenges Faced

Some challenges faced with implementing anti-spam controls:

* Ongoing tuning of filters is required due to evolving spamming techniques.
* Occasional false positives incorrectly classify legitimate emails as spam.
* User awareness and social engineering attacks are unpredictable.
* Encrypted spam messages avoided content inspection.
* Lack of adoption of authentication protocols by many external domains.
* Additional overhead on IT teams to monitor and maintain multiple systems.

## Conclusion

Deploying anti-spam defenses requires a layered model combining technology and policies. Key takeaways:

* Email gateways provide efficient protection using diverse spam identification techniques.
* Authentication mechanisms like DMARC block spoofing and improve visibility.
* User security training is vital to identify advanced phishing attempts.
* Controls need constant vigilance as spammers rapidly change tactics/technologies.
* A coordinated effort across infrastructure, software, policies, and people is essential rather than a single solution.

Overall, this project helped safeguard against constantly evolving spam, phishing, and malware threats.

## Project Management

* Bhudev Nevaniya: Researched anti-spam solutions and best practices. Conducted email infrastructure assessment.
* Meet Brahmbhatt: Architected email gateway deployment and integration. Evaluated filtering techniques.
* Maisha Khatoon: Planned and conducted security awareness training for users. Set up simulations for testing.
* Shreeraj Shah: Implemented email authentication and encryption technologies. Coordinated monitoring.

## References