Network Security Plan & Flowchart
For
Deerfield Beach Police Department
By

Cyber Security Intern Team

Aadith Preetham (C0902681)

Submission: 21 Feb 2025

Table of Contents

Introduction

Over the past few weeks, DeerGuard Defenders have gained valuable insights into the infrastructure and policies followed by the Deerfield Beach Police Department. While developing an Incident Response Plan was crucial for managing security breaches, it is equally important to establish a Network Security Plan to proactively prevent incidents.

To address existing gaps in Deerfield Beach Police Department's network security architecture, DeerGuard Defenders have formulated a comprehensive security plan outlining procedures for maintaining and deploying network security solutions. This plan is designed to enhance Deerfield Beach Police Department's cybersecurity framework by identifying vulnerabilities, implementing industry best practices, and ensuring continuous security improvements. The document provides risk mitigation strategies and ongoing maintenance protocols to safeguard sensitive law enforcement data and maintain the integrity of Deerfield Beach Police Department's operations.

Identified Security Issues

A recent cybersecurity audit of the Deerfield Beach Police Department identified multiple critical vulnerabilities in the network infrastructure. These security weaknesses pose significant risks to data integrity, confidentiality, and overall law enforcement operations. Below is a detailed breakdown of each vulnerability and its potential impact:

1. Outdated Systems (Unpatched or Expired Software)

- Several servers and workstations within Deerfield Beach Police Department's network are running on outdated operating systems and software versions that are no longer receiving security patches or vendor support.
- Risk:
    - Unpatched vulnerabilities can be exploited by cybercriminals to gain unauthorized access.
    - Attackers can deploy malware, ransomware, or zero-day exploits targeting known software weaknesses.
    - Outdated systems may also fail to support modern encryption standards, weakening overall data security.

2. Weak & Repeated Passwords (Poor Credential Management)

- Many Deerfield Beach Police Department staff members reuse passwords across multiple systems, making them vulnerable to credential stuffing attacks.
- Risk:
    - Easy-to-guess passwords increase the risk of brute force attacks.

    - Reusing credentials across systems means that a single compromised password can grant attackers access to multiple systems.
    - Without Multi-Factor Authentication (MFA), even a minor credential leak can lead to a major security breach.

3. Misconfigured Firewalls (Lack of Proper Traffic Filtering)

- Deerfield Beach Police Department's firewall rules are not properly configured, leaving gaps in traffic monitoring and access control. The default setting allows outbound traffic without restrictions, increasing exposure to external threats.
- Risk:
    - Attackers can exploit open ports to infiltrate Deerfield Beach Police Department's internal network.
    - Unauthorized data transfers may go unnoticed, leading to potential data exfiltration.
    - Lack of strict outbound traffic control can result in malware infections spreading across police systems.

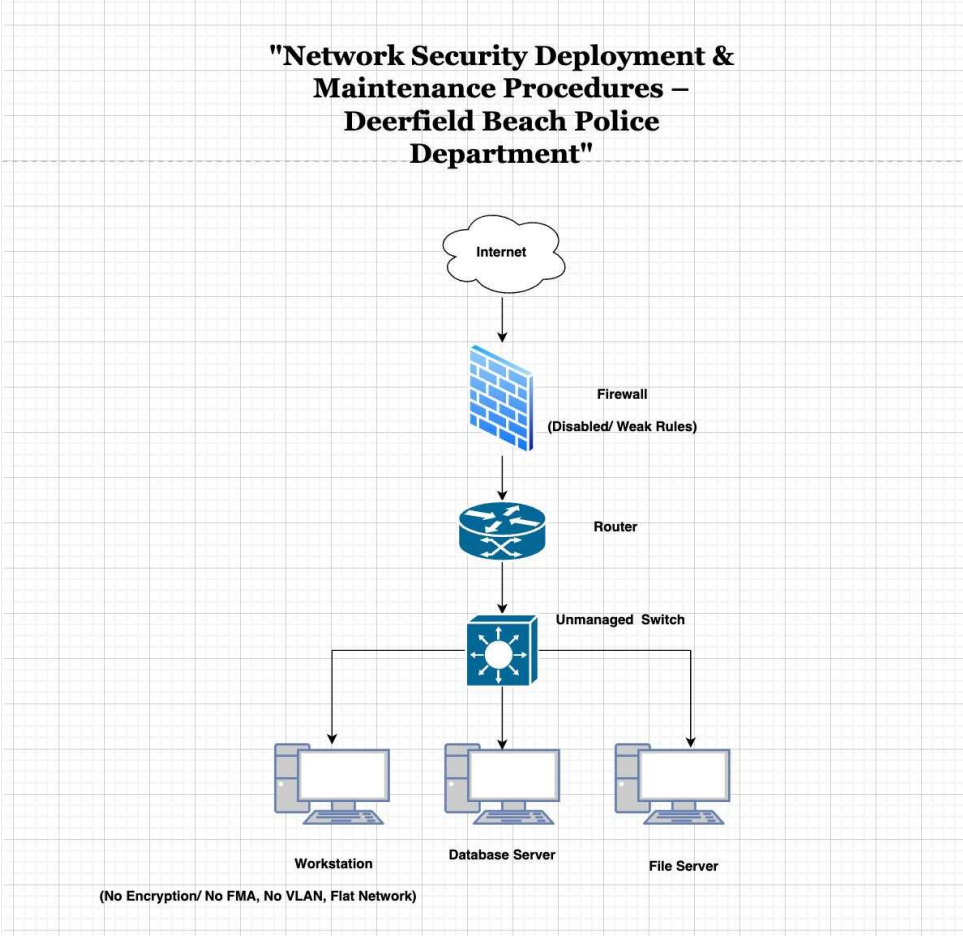
4. Web & Email Server Weaknesses (Phishing Susceptibility)

- Phishing simulations conducted in Week 4 revealed that many employees failed to recognize fraudulent emails, making them highly susceptible to social engineering attacks.
- Risk:
    - Attackers can send spoofed emails pretending to be Deerfield Beach Police Department leadership or IT staff, tricking employees into clicking malicious links.
    - Successful phishing attacks can result in stolen credentials, malware installation, or unauthorized access to law enforcement databases.
    - Deerfield Beach Police Department's email server lacks advanced filtering, allowing a significant amount of malicious emails to bypass defenses.

5. Misconfigured Cloud Storage (Exposure of Sensitive Police Records)

- During a recent security audit, it was discovered that certain sensitive police records stored in cloud storage were publicly accessible due to improper access control settings.
- Risk:
    - Unrestricted access allows unauthorized individuals to view, download, or modify confidential case files.
    - If these records contain personally identifiable information (PII) or ongoing investigation details, public exposure could compromise legal proceedings and officer safety.

- Attackers may use open cloud storage vulnerabilities to upload malicious files, creating backdoors into the network.



Network Diagram (Unsecured)

Vulnerability	Key Risks	Potential Consequences
Outdated Systems	Lack of security updates, zero-day exploit risk	Ransomware infections, unauthorized access
Weak & Repeated Passwords	Credential reuse, brute force attacks	Data breaches, unauthorized system access
Misconfigured Firewalls	Unrestricted outbound traffic, open ports	Data exfiltration, malware spread
Web & Email Server Weaknesses	Phishing attacks, social engineering	Stolen credentials, unauthorized access
Misconfigured Cloud Storage	Publicly accessible police records	Data leaks, legal violations, operational disruption

Network Security Implementation Plan

The plan is divided into 5 key phases to ensure proper security deployment and continuous maintenance.

Phase 1: Security Assessment & Risk Identification

Objective: Identify and prioritize security risks across Deerfield Beach Police Department's network.

1. Conduct a Comprehensive Security Audit (Tool to be used: **Nessus**)
    - Identify outdated software, weak authentication methods, and vulnerable systems.
    - Perform penetration testing on Deerfield Beach Police Department's external-facing infrastructure.
    - Review cloud storage permissions to detect misconfigurations.
2. Analyze Phishing & Social Engineering Risks (Tool to be used: **Blackeye** and **LocalTunnel**)
    - Assess the effectiveness of Deerfield Beach Police Department's phishing awareness training.
    - Monitor email click rates during phishing simulations (Week 4 findings).
3. Firewall & Network Traffic Analysis (Tool to be used: **Wireshark**)
    - Evaluate firewall rules and ensure outbound traffic control is enforced.
    - Conduct log analysis to detect anomalies.

Phase 2: Security Deployment & Hardening

Objective: Implement security solutions to mitigate identified risks.

1. Patch & Upgrade Systems (Tool to be used: OS Dependent)
    - Deploy automated patch management for operating systems and applications.
    - Upgrade all outdated servers and workstations.
2. Implement Strong Authentication & Password Policies
    - Enforce Multi-Factor Authentication (MFA) across all Deerfield Beach Police Department systems.
    - Implement a password manager to prevent password reuse.
3. Firewall Hardening & Network Segmentation (Tool to be used: **UFW**)
    - Restrict outbound traffic and enforce strict access controls.
    - Implement role-based access controls (RBAC).
4. Secure Web & Email Servers
    - Deploy email filtering solutions to block phishing attempts.

    - Encrypt all police records and sensitive data at rest.
5. Restrict Public Access to Cloud Storage
    - Enforce zero-trust access controls for cloud storage.
    - Encrypt all law enforcement files stored in the cloud.

Phase 3: Continuous Monitoring & Threat Detection

Objective: Maintain ongoing security through proactive monitoring.

1. Deploy Intrusion Detection Systems (IDS)
    - Implement real-time network monitoring to detect suspicious activity.
    - Use AI-based threat intelligence for early attack detection.
2. Security Information & Event Management (SIEM) (Tool to be used: **Graylog**)
    - Set up log monitoring for all critical systems.
    - Alert incident response teams in case of anomalies.
3. Incident Response Plan (IRP) Execution
    - Follow incident handling procedures defined in Deerfield Beach Police Department's IRP (Week 3 findings).
    - Conduct bi-annual security drills.

Phase 4: Security Awareness & Employee Training

Objective: Educate employees to reduce human-error-related breaches.

1. Mandatory Phishing Awareness Training (Tool to be used: **PhishSim**)
    - Conduct quarterly phishing simulations (Week 4 findings).
    - Reward employees who correctly identify phishing attempts.
2. Cybersecurity Gamification
    - Implement interactive learning methods (e.g., Cybersecurity Poker Game from Week 5).
    - Encourage engagement through team-based competitions.
3. Security Policy Enforcement
    - Regularly update password policies and access control rules.
    - Enforce strict data handling protocols for police records.

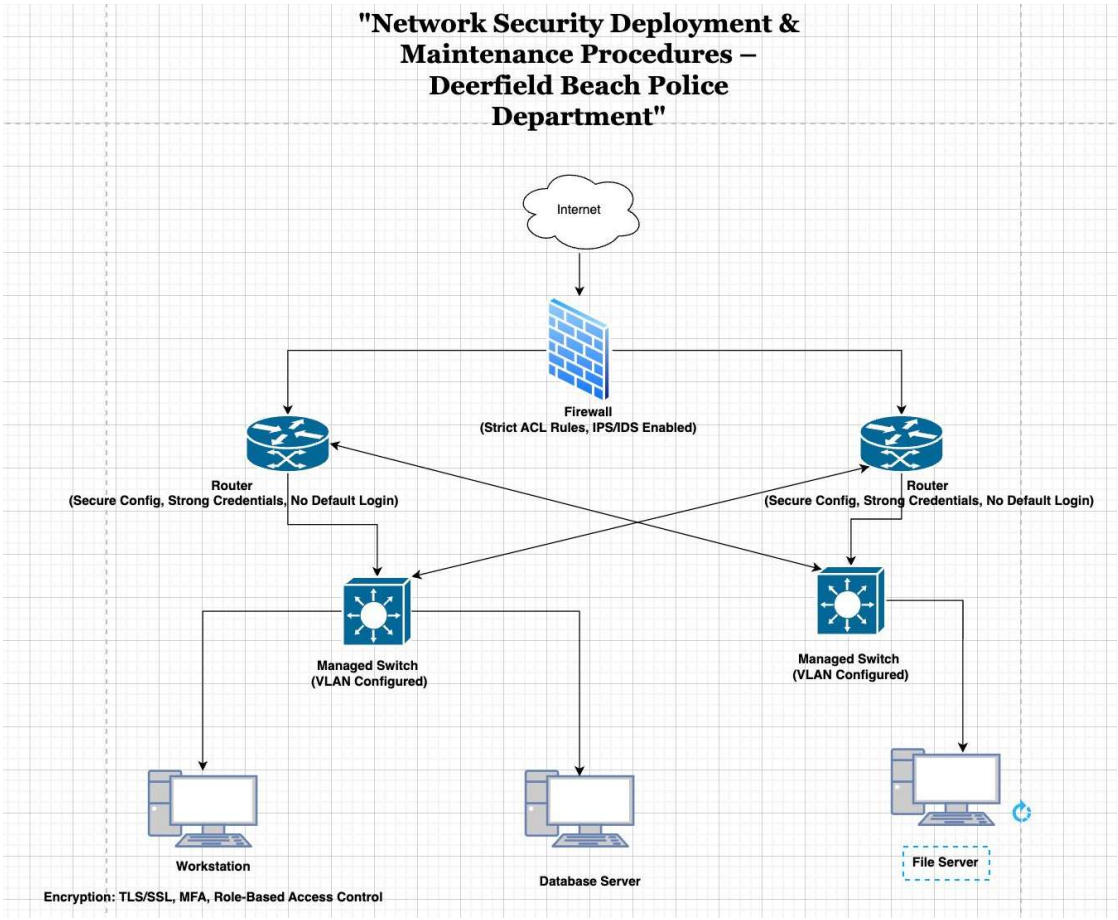
Phase 5: Ongoing Security Review & Continuous Improvement

Objective: Ensure that Deerfield Beach Police Department's network security remains resilient over time.

1. Bi-Annual Security Audits
    - Review firewall configurations, email security, and password management policies.
    - Assess compliance with industry standards.
2. Update Incident Response Procedures

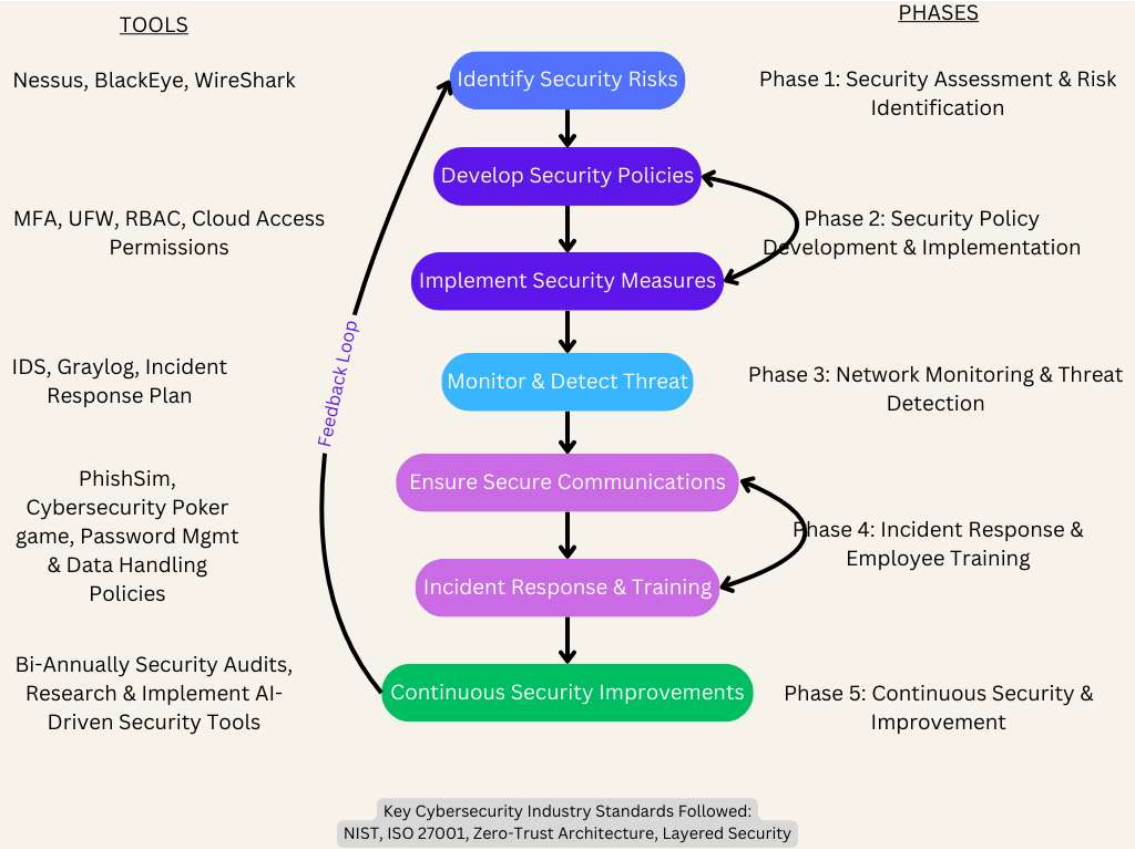
- Improve IRP based on past security incidents.
- Document lessons learned from security events.

3. Adopt New Security Technologies
    - Research and implement AI-driven security tools.
    - Upgrade to next-generation endpoint protection solutions.



Network Diagram (Secured)

Flowchart for Network Security Plan for DBPD



Conclusion

Thus, the Network Security Implementation Plan for the Deerfield Beach Police Department is designed to proactively address vulnerabilities and strengthen cybersecurity across the department. By tackling key risks—like outdated systems, weak passwords, misconfigured firewalls, phishing threats, and cloud security gaps—this plan lays out a clear, structured approach to keeping DBPD's network and sensitive data safe.

Following a five-phase strategy, the plan ensures strong authentication, encryption, continuous monitoring, and staff training, making security a shared responsibility rather than just a technical task. The flowchart provides a straightforward guide, helping the IT team and leadership navigate security measures with confidence.

Cybersecurity isn't a one-time fix—it's an ongoing effort. Regular audits, policy updates, and security drills will help DBPD stay ahead of threats and adapt to new challenges. With this plan in place, the department is well-equipped to protect its digital assets, support its officers, and serve the community safely in an increasingly digital world.

References

National Institute of Standards and Technology (NIST). (2020). *Zero Trust Architecture (SP 800-207)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

National Institute of Standards and Technology (NIST). (2018). *Guide to Enterprise Password Management (SP 800-118)*. U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-118

Arabo, A., Brown, I., & El-Moussa, F. (2012). Cyber security in modern critical infrastructure: Threats and challenges. *Journal of Cyber Security and Mobility, 1*(1), 1-20. https://doi.org/10.13052/jcsm2245-1439.121

Tariq, M., & Ehsan, N. (2021). Cybersecurity risk management for law enforcement agencies: A case study approach. *Journal of Information Security and Applications, 58*, 102774. https://doi.org/10.1016/j.jisa.2021.102774

Microsoft. (2022). *Best practices for securing Active Directory*. https://learn.microsoft.com/en-us/security/

Wireshark. (2022). *Wireshark user guide*. https://www.wireshark.org/docs/