Enterprise Network Security Implementation & Hardening

Client Environment: Small Law Firm Handling Sensitive Legal Data

Overview

This project involved designing and implementing a comprehensive cybersecurity infrastructure upgrade for a small law firm with significant security vulnerabilities. The existing environment lacked network segmentation, centralized endpoint protection, automated backups, and formal security policies, exposing the organization to risks such as data breaches, unauthorized access, and data loss.

The objective was to transform the environment into a secure, resilient, and scalable infrastructure using industry best practices.

Objective

- Strengthen network security through segmentation and perimeter defense
- Implement centralized endpoint protection and monitoring
- Ensure data availability through automated backup solutions
- Reduce human-related risks through cybersecurity awareness and policy enforcement

Environment (Before Implementation)

- Flat network with shared access between employees and guests
- No firewall-based traffic control or segmentation
- Inconsistent or missing antivirus protection across endpoints
- Manual or unreliable backup processes
- No formal cybersecurity policies or employee training

This environment created high risk for:

- Lateral movement attacks
- Data exfiltration
- Ransomware impact
- Compliance and confidentiality failures

Implementation & Methodology

The project followed a structured implementation approach based on the Systems Development Life Cycle (SDLC), including planning, analysis, design, implementation, testing, and maintenance phases.

Key implementations included:

Firewall Deployment (pfSense)

- Configured perimeter firewall with rule-based traffic control
- Blocked unauthorized access and monitored network activity

Network Segmentation (VLANs)

- Separated guest, employee, and server networks
- Restricted lateral movement across network segments
- Configured managed switches to support VLAN tagging

Endpoint Protection (Microsoft Defender for Business)

- Deployed centralized antivirus and threat monitoring
- Enabled real-time detection and automated remediation

Automated Cloud Backup System

- Implemented daily encrypted backups
- Conducted regular restoration testing to verify data integrity

Security Policies & Training

- Developed policies (acceptable use, password, Wi-Fi access)
- Conducted employee cybersecurity training sessions
- Simulated phishing attacks to assess awareness

Key Challenges & Problem Solving

- Identified hardware limitation where existing switches did not support VLAN tagging

Procured and configured managed switches to enable segmentation

- Detected misconfigured firewall rules during validation

Adjusted rules to enforce proper isolation between network segments

Results & Security Impact

The implementation significantly improved the organization's security posture:

- 100% of endpoints protected with centralized antivirus monitoring
- 100% success rate in automated daily backups, with successful recovery validation
- Full network segmentation achieved, preventing unauthorized cross-VLAN access
- All unauthorized access attempts blocked, confirmed through firewall logs
- Phishing susceptibility reduced to <10%, down from an estimated ~25% baseline
- Over 90% employee participation in cybersecurity training

These improvements reduced risk exposure and established a foundation for long-term security and compliance.

Security Relevance (SOC Perspective)

This project demonstrates practical experience in:

- Network segmentation and access control
- Firewall configuration and traffic monitoring
- Endpoint detection and response
- Incident prevention and risk mitigation
- Security awareness and human risk reduction

In a SOC environment, these implementations directly relate to:

- Monitoring firewall logs and alerts
- Investigating endpoint threats
- Identifying misconfigurations and vulnerabilities

Tools & Technologies

- pfSense Firewall
- VLAN Configuration (Managed Switches)
- Microsoft Defender for Business
- Cloud Backup Solutions (Veeam / Acronis concepts)
- Network Monitoring & Logging Tools