MILESTONE 5

Arturo Astorga

Purpose: Address recent security breach and present a new secure architecture

Goal: Protect customer data, support business continuity, and enable secure growth

OVERVIEW OF CURRENT INFRASTRUCTURE

- 3-layer wired network using Cisco Nexus and Catalyst switches
- Aruba wireless access with no login required (open network)
- Single Active Directory domain with default settings
- Weak password policy (no complexity, no history)
- External-facing servers use FTP and lack firewalls
- Point-of-sale systems use outdated PPTP VPN
- Symantec AV on workstations; 1/3 of users have local admin rights
- No antivirus on virtual servers; FTP used for file transfers

CRITICAL SECURITY VULNERABILITIES

- Password policy disabled; reuse and writing down passwords common
- Open wireless network with no user authentication or encryption
- Public-facing web and email servers have no perimeter firewall
- FTP enabled externally (unencrypted file transfers)
- No antivirus on virtual machines hosting critical systems
- Point-of-sale terminals used for browsing → malware risk
- Proofpoint spam filter updates inactive → increased phishing risk
- BYOD permitted with no access controls or MDM

RECOMMENDED SECURITY ENHANCEMENTS

- Enforce **Zero Trust Architecture** and network segmentation
- Enable **multi-factor authentication (MFA)** for remote and admin access
- Reinforce Active Directory policies (password complexity, minimal admin roles)
- Replace PPTP with **SSL VPN solutions**
- Update firewall configurations to control ingress/egress
- Disable public FTP, adopt **SFTP with IP restrictions**
- Deploy enterprise antivirus on all servers and endpoints
- Reactivate Proofpoint subscriptions; configure anti-spam rules
- Implement **Mobile Device Management (MDM)** for BYOD control

RECOMMENDED SECURE NETWORK ARCHITECTURE

- Suggested Visual Labels:
- Segmented internal zones (HR, POS, Finance, Admin)
- DMZ for external web/email servers with firewall protection
- Encrypted tunnels for remote access (SSL VPN)
- Secure wireless (WPA3, RADIUS authentication)
- SaaS integration with Cloud Access Security Broker (CASB)
- Centralized logging, SIEM, and monitoring solution

CONCLUSION & IMPLEMENTATION PROPOSAL

- Proposed architecture mitigates major vulnerabilities
- Supports PCI compliance, secure remote access, and scalable operations
- Enables a proactive cybersecurity posture
- Next Steps:

  Approve the proposal

  Engage our team to implement security solutions