PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

Network Vulnerability Assessment

Prepared for:
[redacted], a Third-Party Retailer for [redacted]

Prepared by:
Ken Sadorski
[redacted]

Confidentiality Notice

The information in this report is confidential and should only be disclosed between the testing organization and [redacted].

Table of Contents

PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

Executive Summary

This report provides a comprehensive security analysis of [redacted] network, focusing on vulnerabilities within the existing wireless and wired networks, physical security, user education, and other critical areas. The objective is to identify security gaps and recommend effective solutions to enhance network resilience and safeguard customer information.

Description

[redacted], a [redacted] retailer, operates a small office network comprising three desktop terminals and three printers on the sales floor, all wirelessly connected. With 20-25 simultaneous wireless connections, securing Customer Proprietary Information (CPI) is a priority.

Top-Five Security Concerns

- **Unsecured Wireless Devices:** Numerous devices on the sales floor pose a potential attack risk.
- **Physical Security Gaps:** Desktops and network equipment lack adequate physical security.
- **No Password Protection:** Desktop terminals are accessible without login credentials.
- **Backroom Security:** Network equipment is unsecured and easily accessible.
- **Lack of Device Restrictions:** Demo devices allow unrestricted access and installations.

Network and Wireless Security

- **Encryption**: WPA-2 encryption is in place for all wireless devices. Ensure all devices maintain WPA-2 encryption for optimal security.
- **Password Protection**: Default passwords pose a significant risk. Update all passwords to meet complexity standards (12-18 characters, including uppercase, lowercase, numbers, and symbols).
- **Firewall Configuration**: A properly configured hardware firewall is in place, effectively blocking unauthorized access. Regularly review the firewall settings to maintain security.

PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

System (PC/Server) Security

- **User Privileges:** Currently, employees can install and modify software at will, which is a security risk. Restrict user permissions to prevent unauthorized software installations.
- **Anti-virus:** All systems have anti-virus software installed and regularly updated. Ensure that only one anti-virus program runs on each system to prevent conflicts.
- **Updates:** All workstations are regularly updated. Continue to verify update cycles for Windows and other critical software.

Backups/Disaster Recovery

- **System Backups:** [redacted] relies on [redacted]'s Citrix platform, ensuring that critical data is secure and regularly backed up. Establish local backup solutions to safeguard internal data.
- **Power Failure Plan:** No Uninterruptible Power Supply (UPS) is installed. Recommend implementing UPS devices to prevent data loss during power outages.

Physical Security

- B**ackroom Security:** Networking equipment in the backroom lacks physical locks and is accessible during business hours. Implement locks on all networking equipment and secure the backroom.
- **Sales Floor Device Security:** All devices on the sales floor are secured with an alarmed locking mechanism. Regularly inspect these locks and ensure alarms are functional.

Authorization, Authentication, and Accounting (AAA)

- **Password Protection:** Sales floor desktops lack password protection, risking unauthorized access. Implement and enforce password policies across all workstations.
- **Employee Access Codes:** Each employee has a unique alarm code. Ensure terminated employees' access codes are promptly deactivated.

PDF-XChange Editor Click to BUY NOW! www.pdf-xchange.com

User Education

- **Acceptable Use Policies (AUP):** All employees sign an AUP during onboarding. Regularly reinforce this policy with periodic reviews or quizzes.
- **Phishing Awareness:** Current phishing training is limited. Provide ongoing education on identifying and avoiding phishing threats to safeguard company data.
- **Proper Disposal of CPI**: A secure shred bin is available for document disposal, but its location on the sales floor poses a risk. Relocate the bin to the backroom and enforce secure disposal practices.

Network Scan Analysis

- **Internal Scan:** All active SSIDs are accounted for, with no rogue networks detected. The firewall effectively blocks port scanning attempts.
- **External Scan:** The external IP address has appropriate filtering, preventing unauthorized probing. Maintain current firewall and network configurations to protect external access.

Action Plan

High-Priority Remediation

1. **Password Protection:** Implement mandatory passwords on all workstations and enforce screen locking when workstations are idle.
2. **User Restrictions:** Restrict installation permissions for employees to mitigate the risk of malware installation.
3. **UPS Installation:** Install UPS devices to protect against data loss from power failures.
4. **Physical Security Enhancements**: Secure networking equipment with locks and keep backroom doors closed during business hours.
5. **Regular User Education:** Increase user training on phishing, acceptable use, and secure handling of CPI.

By addressing these recommendations, [redacted] can greatly enhance its security posture, protect sensitive information, and improve operational resilience.