APRIL 21, 2024

Research Report 6
Security Audit

Cesar Ortega
West Texas a&M University
2024SP NTWK MGT & INFO SEC (CIDM-6340-70)

What We Did:

During the audit, the security measures at xxxxx Hair Salon in Hereford, TX, were assessed based on the outlined audit plan. The audit encompassed the examination of physical security measures, IT infrastructure, data handling processes, and employee training on security protocols. To evaluate the IT infrastructure, port scanning tests were conducted using tools such as Shield's Up to identify any open ports vulnerable to exploitation. Additionally, the network was scanned using Wireshark and Zenmap to identify connected devices.

What Are the Results:

Through the Audit the devices found were smart speakers, cellphones, a security system, a smart TV, and a computer, all belonging to the owner.

Weak Password Strength: Passwords used throughout the salon were found to be weak and easily guessable, posing a significant security risk.

Lack of Regular Software Updates: Many computers and devices within the salon were found to be running outdated software, leaving them vulnerable to known exploits and security threats.

Absence of Data Backup: The salon lacked a comprehensive data backup plan, leaving critical business data susceptible to loss or corruption in the event of a hardware failure or security breach.

Limited Access Control: Access control measures for sensitive files and business systems were inadequate, allowing unauthorized individuals to potentially access confidential information.

No Ransomware Preparedness Plan: The salon did not have a documented plan for responding to ransomware attacks, leaving them vulnerable to data encryption and extortion tactics.

Additionally, the absence of security cameras on the premises increases the risk of unauthorized access and incidents going undetected.

Recommendations: To address these findings, the following recommendations are proposed:

Implement Strong Password Policies: Enforce the use of complex passwords containing a mix of uppercase, lowercase, numbers, and special characters. Consider implementing password management tools to facilitate secure password storage and rotation.

Establish Regular Software Update Procedures: Develop a schedule for regular software updates and patches to mitigate vulnerabilities. Consider enabling automatic updates where feasible.

Implement Data Backup Solutions: Invest in a reliable data backup solution to regularly backup critical business data, preferably offsite or in the cloud. Schedule regular backups to ensure data integrity and availability.

Enhance Access Control Measures: Implement access controls such as user accounts and permissions to restrict unauthorized access to sensitive files and business systems. Provide training to staff on access control best practices.

Develop a Ransomware Response Plan: Create a documented plan outlining steps for preventing, detecting, containing, and recovering from ransomware attacks. Ensure staff are trained in recognizing and reporting suspicious activity.

These recommendations can be implemented economically and with minimal impact on business operations. Staff training can be conducted during off-peak hours, and software updates can be scheduled during non-business hours to minimize disruptions.

Risk Posture: **xxxxx** Hair Salon currently faces a moderate to high-risk posture due to the identified vulnerabilities and lack of security measures. The greatest risk lies in the weak password practices and absence of data backup solutions, which leave the salon susceptible to data breaches and loss. Additionally, the lack of security cameras increases the risk of unauthorized access and incidents going undetected. Implementing the recommended measures will significantly improve the salon's security posture and reduce its vulnerability to cyber threats. However, continued vigilance and ongoing security awareness training are essential to maintain a secure environment.