Security Risk Assessment Report: Network Hardening

By Lucio Rodrigues

Scenario

You are a security analyst working for a mid-sized financial services company that provides online banking and payment processing. Recently, the company experienced a network intrusion that exposed sensitive customer financial data, including account numbers and partial credit card details.

An internal review revealed that the attacker gained access through poorly secured remote connections and exploited several misconfigurations within the network. After inspecting the organisation's infrastructure, you identified four major vulnerabilities:

1. Remote Desktop Protocol (RDP) is enabled for all users without proper access restrictions.

2. Network devices (routers, switches) are running outdated firmware with known vulnerabilities.

3. The intrusion detection system (IDS) is not configured to send alerts in real-time.

4. Sensitive data is transmitted across the internal network without encryption.

If no action is taken, the organisation risks suffering another breach that could result in financial losses, regulatory penalties, and reputational damage. This report provides recommendations for strong and consistent network hardening practices to reduce these risks.

Part 1: Hardening Tools/Methods Implemented

---

1. **Implementing Network Segmentation and Access Control Lists (ACLs)**

By dividing the network into secure segments and using ACLs, sensitive systems can be isolated from general user access, ensuring only authorised personnel can connect to high-value assets like databases or payment systems.

2. **Regular Firmware Updates and Patch Management**

All network devices, including routers, switches, and security appliances, should have firmware updated to the latest secure versions. A patch management policy will ensure timely updates for both hardware and software components.

3. **Enabling End-to-End Encryption for Data in Transit**

By using encryption protocols such as TLS 1.3 for internal communications, sensitive financial and personal data remains protected even if intercepted by a malicious actor.

Part 2: Why These Tools/Methods Are Necessary

- **Network Segmentation and ACLs:**

Restricting access to sensitive areas of the network reduces the attack surface. In the event of a compromise, segmentation prevents attackers from easily moving laterally between systems. ACLs also provide granular control over who can connect to specific network resources.

- **Regular Firmware Updates and Patch Management:**

Attackers often target outdated systems because known vulnerabilities are easy to exploit. By maintaining updated firmware and applying security patches promptly, the organisation closes those known entry points and strengthens its defensive posture.

- **End-to-End Encryption:**

Encrypting data in transit prevents attackers from viewing or tampering with sensitive information, even if they manage to intercept network traffic. This is especially critical in a financial environment where customer trust and data confidentiality are paramount.

Part 3: Cybersecurity Implications

- RDP Without Access Restrictions:

Attackers can exploit exposed or weak RDP configurations to gain direct access to internal systems, often using brute-force or credential-stuffing attacks. Once inside, they can deploy ransomware, steal sensitive data, or move laterally. Network segmentation and strict ACLs limit access points, greatly reducing this risk.

- Outdated Firmware:

Legacy firmware often contains publicly known vulnerabilities. Threat actors can scan for these weaknesses using automated tools and exploit them without needing advanced skills. Regular firmware updates remove these “low-hanging fruit” vulnerabilities.

- Unconfigured IDS Alerts:

Without real-time alerts, attacks can progress undetected for hours or days, giving adversaries more time to entrench themselves. Enabling alerting ensures faster detection and response, reducing potential damage.

- Unencrypted Data in Transit:

Data traveling in plain text is vulnerable to interception via packet sniffing or man-in-the-middle (MITM) attacks. Implementing encryption ensures confidentiality and integrity, making stolen traffic useless to an attacker.