Ethical Hacking Technical Report

Client: Trion Corporation

Date: May 10, 2024

Prepared by: Hernaliza Cañada

Executive Summary: This report details the technical findings of an ethical hacking assessment conducted for Trion Corporation. The assessment aimed to uncover vulnerabilities in the organization's network infrastructure, applications, and systems. Through various testing methodologies, including penetration testing and vulnerability scanning, critical and high-risk issues were identified. This report presents a comprehensive overview of these findings, along with actionable recommendations for mitigation.

Vulnerability Summary:

1. **Unrestricted File Upload:**
    - High: The operating system of several servers has not been updated with the latest security patches.
2. **Software Security:**
    - High: Several application including the web server and the database server are running outdated version with known vulnerabilities.
3. **Wireless Networks:**
    - Critical: Use of an outdated WEP version of an encryption on Wi-Fi networks responsive to any interception.
    - High: Allowing any devices to connect on Wi-Fi networks. Used open authentication in Wi-Fi.
4. **Network Infrastructure:**
    - High: Misconfigured of the firewall rules that cause into permitting unrestricted access.
5. **Web Applications:**

   Critical: Unvalidated Web Portal, enablement attackers to redirect users to malicious sites.
6. **Physical Security:**
    - High: Lack of CCTV coverage in sensitive areas within the premises.
7. **Operating Systems:**
    - High: Unsecured server room access with default lock, that expose critical infrastructure to physical breaches.
8. **Security Patches:**
    - High: Many of the operating systems of several servers have not been updated with the latest security patches.
9. **Email Security:**

   - **High:** Accessing information thru mails, pretending to be legitimate account to fish information, providing the credentials and many sensitive information.

10. **Implement two-factor authentication:**
    - **High:** Critical systems do not require 2FA, increasing the risk of unauthorized access

Recommendations:

1. **Unrestricted File Upload:**
   - Validated file types and sizes before allowing uploads and implement antivirus scanning for all uploaded files in the system.
2. **Software Security:**
   - Regularly update all the software version with the latest version and implement a patch for the management process in insuring timely updates.
3. **Wireless Networks:**
   - Upgrade Wi-Fi network encryption to WPA2 or WPA3 to ensure confidentiality and integrity of wireless communications.
   - Implement authentication on Wi-Fi connection.
4. **Network Infrastructure:**
   - Immediately apply patches to address the command in execution the vulnerability.
5. **Web Applications:**
   - Implement input validation and output encoding to prevent Unvalidated Redirects and Forwards.
6. **Physical Security:**
   - Install CCTV cameras in all areas and ensure proper monitoring and recording of the CCTV’s.
   - Change access lock and restrict the access control in the server room.
7. **Operating Systems:**
   - Upgrade Windows 10 systems to supported versions or implement compensating controls
8. **Security Patches:**
   - Make a schedule for the regular maintenance of windows to monitor the advisories for the update and apply a security patches.
9. **Email Security:**
   - Conduct regular security awareness training for employees to educate them about the risks of phishing attacks and how to identify and report suspicious emails
10. **Implement two-factor authentication:**
    - Use of multi-factor authentication methods in enhancing the security in all critical system and user account**.**

Conclusion: The findings of this ethical hacking assessment underscore critical vulnerabilities and security weaknesses within Trion Corporation infrastructure. By implementing the recommended remediation measures, Trion Corporation can strengthen its security posture and reduce the risk of cyber threats and unauthorized access.

Signature: Hernaliza Cañada