Subject: Stakeholder Memorandum – Key Findings of the Security Audit of Botium Toys

Date: 29th January, 2024

To: 3MTT TedPrimeHub

From: MATANMI OLUMUYIWA OLATUNDE

Dear Cybersecurity Fellows,

I am writing to communicate the key findings of the recent security audit conducted on behalf of Botium Toys. The purpose of this memorandum is to assess the effectiveness of the existing security measures, identify vulnerabilities/risks, and propose recommendations to enhance the overall security posture.

**A. Executive Summary**

The security audit was conducted to assess the information security measures in place at Botium Toys and identify potential vulnerabilities that could compromise the confidentiality, integrity, and availability of sensitive information.

**B. Scope of the Security Audit**

**The audit covered the following key areas:**

1. Network Security/Infrastructure

2. Application Security

3. Data Security/Handling and Storage

4. Physical Security Measures

5. Incidence Response and Management

* **Network Security/Infrastructure**: Evaluation of the company’s network architecture, firewalls, Intrusion Detection/Prevention Systems (IDS/IPS) and the overall resilience of the network.
* **Application Security**: Assessment of the security of Botium Toys’ web and mobile applications, including authentication mechanisms, data input validation, and protection against common web application vulnerabilities.
* **Data Security**/**Handling & Storage**: Examination of how sensitive data is stored, transmitted, and processed within the organization, with a focus on compliance with data protection regulations.
* **Physical Security Measures:** Review of the physical security measures in place to protect the company’s facilities, servers, and other critical assets.
* **Incidence Response and Management:** Evaluation of the company's incident response plan, including how security incidents are detected, reported, and mitigated.

The audit methodology included penetration testing, vulnerability scanning, code review, policy review, and interviews with key personnel.

**C. Key Findings**

The audit identified several areas requiring improvement in Botium Toys’ security posture. The most critical findings include:

1. **Unpatched Vulnerabilities in critical systems:** Several critical systems were found to be running outdated software with known vulnerabilities, this significantly increases the risk of successful cyberattacks.
2. **Weak Password Policies:** Password complexity requirement were insufficient, and password sharing practices were observed. The authentication mechanisms in place for certain applications were found to be weak, increasing the risk of unauthorized access.
3. **Inadequate Data Encryption:** Sensitive data, such as customer information and financial records was found to be transmitted without proper encryption, posing a potential risk to data confidentiality.
4. **Limited Security Awareness Training:** Employees lacked awareness of cybersecurity best practices, increasing the risk of phishing attacks and social engineering scams.
5. **Incomplete Incident Response Plan:** A comprehensive incident response plan was not in place, potentially hindering the company’s ability to effectively respond to security incidents.

**D. Recommendations**

Based on the identified findings, the following recommendations are made:

1. Patch all critical systems immediately, ensure that all systems are regularly updated with the latest security patches and software versions. Implement a process for regular vulnerability scanning and patching.
2. Strengthen password policies and Enhanced Authentication. Enforce strong password complexity requirements and prohibit password sharing, implement multi-factor authentication (MFA) for critical applications to strengthen access controls.
3. Implement data encryption at rest and in transit. Use industry-standard encryption algorithms to protect sensitive data.
4. Intrusion detection system is highly recommended to help identify possible intrusions by threat actors.
5. Provide comprehensive security awareness training to all employees. Educate employees on cyber threats, best practices, and reporting procedures.
6. Develop and implement a comprehensive incident response plan. Define roles, responsibilities, and procedures for incident response.
7. Backups and disaster recovery plans of critical data should be in place to ensure business continuity in the case of a breach.
8. Provide a time-controlled safe, locking cabinets, fire detection and prevention systems and signage indicating alarm service provider, and adequate lightning will further improve Botium Toys’ Security Posture.

**E.** Next Steps

Botium Toys' management should be committed to addressing the identified vulnerabilities and implementing the recommended actions. A detailed action plan with specific timelines and assigned responsibilities should be developed and shared with stakeholders within a specified timeframe. Regular updates on the progress of the remediation efforts should be provided.

Conclusion

While Botium Toys should implement some security measures, there are significant vulnerabilities that need to be addressed to ensure the security of its systems, data, and customers. By implementing the recommendations outlined in this memorandum, Botium Toys can significantly improve its security posture and mitigate the risk of cyberattacks.

We encourage all stakeholders to take an active role in supporting Botium Toys' security initiatives. Together, we can create a more secure environment for Botium Toys and its customers.

Best Regards

**Matanmi Olumuyiwa Olatunde**

**Fellow Cybersecurity (3MTT 1ST COHORT)**

**09060405365/08030695080**

[**matanmi2003@gmail.com**](mailto:matanmi2003@gmail.com)