Botium Toys Security Audit Report

Table of contents

1. Audit Scope and Objectives

Scope:
The scope of this audit covers a comprehensive review of Botium Toys' security program, including:

- Technological assets (employee equipment and devices).
- Internal network and critical systems.
- Data management systems and storage.

Objectives:
The objective is to evaluate the company's current technological assets and complete a compliance and control checklist. This will help identify which controls and best practices need to be implemented to improve Botium Toys' security posture and ensure compliance with international regulations.

2. Evaluated Technological Assets

The primary assets managed by Botium Toys' IT Department include:

- Local equipment: Computers, servers, and other devices used in the office for business activities.
- Employee devices: End-user equipment such as desktop computers, laptops, smartphones, remote workstations, and peripherals (headsets, cables, keyboards, mice, surveillance cameras, etc.).
- Showcase products: Merchandise available for sale both in the physical store and on the e-commerce platform.
- Management systems: Software for accounting, telecommunications, databases, security, e-commerce, and inventory management.

- Internal network: The network infrastructure supporting all IT operations.
- Data storage: Systems used to store critical and confidential data.
- Legacy systems: Systems that have reached the end of their lifecycle and require manual monitoring for proper operation.

3. Risk Assessment

Risk Description:
Ineffective asset management has been identified. Botium Toys has not implemented all necessary security controls and does not comply with various national and international regulations.

Controls and Best Practices:
The first function of the NIST Cybersecurity Framework (NIST CSF) is "Identify." Botium Toys needs to allocate resources to identify and classify critical assets, determining the impact their loss would have on business continuity.

Risk Score:
The assigned risk score is 8/10, representing a high level of vulnerability due to the lack of controls and non-compliance with security best practices.

Potential Impact:
The potential impact of asset loss is considered medium as the IT Department is unclear about which specific assets would be at risk. However, the risk of regulatory sanctions is high because Botium Toys does not meet the necessary requirements for data privacy and security protection.

4. Key Vulnerabilities Identified

- Uncontrolled access: All employees have access to internal data, including sensitive customer data (credit card information and PII/SPII).
- Lack of encryption: Stored, processed, and transmitted credit card information is not encrypted.
- Insufficient access controls: Controls related to the principle of least privilege and segregation of duties are not implemented.
- Network security: While the company has a firewall to block unauthorized traffic, it does not have an Intrusion Detection System (IDS).
- Missing contingency plans: There are no disaster recovery plans, nor are there regular backups of critical data.
- Weak passwords: The password policies are weak, with no requirement for minimum complexity.
- No centralized password management system: This affects productivity when employees or suppliers need to reset passwords.
- Irregular maintenance of legacy systems: There is no regular schedule or clear procedures for monitoring and maintaining critical end-of-life systems.

- Physical controls: Although the physical infrastructure is protected with CCTV, appropriate locks, and fire prevention systems, it is recommended to strengthen these measures.

5. Control Checklist

Control	Yes	No
Principle of least privilege	✔	
Disaster recovery plan		✔
Secure password policies		✔
Segregation of duties		✔
Firewall	✔	
Intrusion Detection System (IDS)		✔
Data backups		✔
Antivirus software	✔	
Legacy system maintenance		✔
Data encryption		✔
Password management system		✔
Physical access control (locks, CCTV)	✔	
Fire prevention systems	✔	

6. Compliance Checklist

Payment Card Industry Data Security Standard (PCI DSS)

Best practices	Yes	No
Only authorized users have access to customers' credit card information	✔	
Credit card information is stored, accepted, processed, and transmitted securely	✔	
Implement data encryption procedures to better protect credit card data and transaction touchpoints		✔
Adopt secure password management policies		✔

General Data Protection Regulation (GDPR)

Best Practices	Yes	No
EU customer data is kept private/secure	✔	
There is a plan to notify the EU and customers within 72 hours if data is compromised or breached	✔	
Ensure that data is properly classified and inventoried		✔
Enforce privacy policies, procedures, and processes to properly document and maintain data		✔

System and Organization Controls (SOC Type 1, SOC Type 2)

Best Practices	Yes	No
User access policies are established	✔	
Confidential (PII/SPII) data is private	✔	
Data integrity ensures that information is consistent, complete, accurate, and validated	✔	
Data is available to authorized personnel	✔	

7. Recommendations for Improving Botium Toys' Security Posture

- Implement the Principle of Least Privilege: Limit access to critical data and systems to authorized employees only. Review and update access permissions periodically.
- Adopt Secure Password Management Policies: Implement stricter password policies, including complexity requirements (minimum number of characters, inclusion of letters, numbers, and special characters) and the need for periodic changes. Additionally, it is recommended to install a centralized password management system.
- Encrypt Sensitive Data: Implement encryption procedures for credit card information both at rest and in transit. This includes encrypting all confidential data stored in databases and transactions involving this data.
- Develop a Disaster Recovery Plan: Establish a formal disaster recovery plan to ensure business continuity in case of incidents. The plan should be regularly tested and reviewed.
- Adopt a Comprehensive Backup Strategy: Perform regular backups of all critical data and store them in secure locations. It is recommended to test backups periodically to ensure data can be correctly restored.
- Implement an Intrusion Detection and Prevention System (IDS/IPS): Install and configure an IDS/IPS to monitor and detect suspicious activities on the network. Ensure the system is up to date and fully operational.
- Strengthen Compliance with Privacy Policies: Review and update privacy and data protection policies to comply with international regulations such as GDPR. Implement proper data classification and documentation processes.
- Reinforce Physical and Operational Controls: Ensure sensitive areas, such as offices and warehouses, are properly secured with locks, CCTV, and fire detection systems. Limit physical access to critical assets.

- Monitor and Regularly Maintain Legacy Systems: Establish a continuous monitoring and preventive maintenance plan for legacy systems, and implement vulnerability management tools.

These recommendations will help Botium Toys reduce security risks, ensure data integrity, and improve compliance with international standards.