Botium Toys – Internal Security Audit

Executive Summary

This report presents the findings of an internal IT security audit conducted for Botium Toys, a fictional U.S.-based company. The purpose of this audit was to evaluate existing security controls, compliance practices, and risks related to the company's IT infrastructure.

The audit identified several critical gaps in Botium Toys' security posture, including lack of encryption for sensitive data, inadequate access control policies, absence of an intrusion detection system, weak password requirements, and no disaster recovery plan.

Given the risk score of 8/10 (High), Botium Toys faces potential data breaches, compliance fines, and operational disruptions if immediate improvements are not implemented.

Scope

The scope of this audit included:
- Employee equipment and workstations
- Internal network and internet access
- On-premises equipment (storefront, office, warehouse)
- Systems and services (accounting, telecom, database, ecommerce, inventory)
- Data retention and storage practices
- Legacy systems

Findings

1. Administrative Controls

- ❌ No least privilege access controls (all employees can access sensitive data)
- ❌ Weak password policy (does not meet modern complexity standards)
- ❌ No centralized password management system
- ❌ No disaster recovery plan in place
- ✅ Privacy policies exist (GDPR notification plan included)

2. Technical Controls

- ✅ Firewall implemented with defined rules
- ✅ Antivirus deployed and monitored
- ❌ No IDS/IPS in place
- ❌ No encryption for customer credit card data
- ❌ No system backups or recovery procedures
- ❌ Legacy systems not regularly maintained

3. Physical Controls

- ✓ Locks, CCTV, and fire detection systems in place
- ✓ Storefront and warehouse have adequate physical protections

Recommendations

1. Implement Access Control (Least Privilege & Separation of Duties): Restrict employee access to only the data they require.
2. Encrypt Sensitive Data: Immediately secure all payment card and customer PII data in compliance with PCI DSS.
3. Improve Password Security: Adopt stronger policies (minimum 8–12 characters, mix of uppercase, lowercase, numbers, and special characters) with a centralized password manager.
4. Deploy IDS/IPS: Implement network monitoring to detect and prevent intrusions.
5. Establish Backup & Disaster Recovery Plans: Ensure data resilience and business continuity.
6. Legacy System Maintenance: Create a formal schedule for monitoring and updating legacy systems.
7. Compliance Enforcement: Strengthen GDPR and PCI DSS adherence to avoid legal fines.