Botium Toys Internal Security Audit

This repository contains an internal audit report conducted as part of a cybersecurity training exercise.

Overview

The audit follows the NIST Cybersecurity Framework and evaluates Botium Toys' current controls, compliance posture, and risk level.

Tools Used

- □ NIST CSF
- □ PCI DSS v4.0 guidelines
- □ GDPR compliance framework
- □ SOC 2 Trust Service Principles

1. Purpose and Scope

The purpose of this security audit is to evaluate the current security posture of Botium Toys, a toy manufacturing and e-commerce organization. The audit focuses on identifying security risks, vulnerabilities, and compliance gaps across the company's internal network, online systems, and operational processes.

The scope of this audit includes:

- Internal company network and connected systems.
- Employee access management and device security.
- Web application and customer data protection.
- Third-party services and vendor interactions.
- Physical and environmental security.

This audit does not include penetration testing or social engineering attacks, as the goal is to provide a policy- and procedure-level assessment.

2. Risk Assessment

The following risks have been identified based on the company's current operations and infrastructure:

1. Risk Area 2. Description 3. Potential Impact 4. Likelihood

- **Data Privacy** - Customer data stored without proper encryption or access control. *High Medium*
- **Access Control -** Lack of multi-factor authentication (MFA) for employee logins. *High High*
- **Network Security -** Insufficient firewall rules and network segmentation. *High Medium*
- **Vendor Management** - No standardized vetting process for third-party integrations. *Medium Medium*
- **Incident Response -** Absence of a formal incident response plan. *High High*
- **Physical Security -** Unrestricted access to server rooms or employee terminals. *Medium Low*

3. Audit Findings

After reviewing Botium Toys' operations and infrastructure, the following findings were noted:

1. **Access Control Gaps:**

- Employees reuse passwords across platforms.
- MFA is not enforced on key systems, increasing account compromise risk.

2. **Data Management Issues:**

- Customer payment data and PII are stored without encryption at rest.
- Backups are not regularly tested or secured offsite.

3. **Policy Deficiencies:**

- No documented incident response or disaster recovery plan.
- Lack of clear security awareness training for employees.

4. **Network Weaknesses:**

- Flat internal network structure with no segmentation.
- Outdated firewall configurations and missing intrusion detection systems.

5. **Vendor and Third-Party Risks:**

- Third-party services are used without consistent security reviews or contracts defining responsibility.

4. Recommendations

To improve Botium Toys’ overall security posture, the following actions are recommended:

1. **Access Control**

- Implement multi-factor authentication (MFA) across all systems.
- Enforce password rotation and complexity policies.
- Adopt role-based access control (RBAC) to minimize privilege abuse.

2. **Data Protection**

- Encrypt all sensitive customer and employee data both in transit and at rest.
- Use secure key management practices.
- Test and validate backup systems regularly.

3. **Network Security**

- Segment the internal network by department or sensitivity level.
- Deploy intrusion detection and prevention systems (IDS/IPS).
- Conduct regular vulnerability scans and patch management cycles.

4. **Policy and Awareness**

- Create an incident response plan with defined escalation procedures.
- Schedule quarterly security awareness training for all staff.
- Regularly review and update the organization’s information security policy.

5. **Vendor Security**

- Establish a vendor risk management process requiring annual security reviews.
- Include data protection clauses in all contracts with external vendors.

5. Conclusion

The security audit for Botium Toys reveals that while the company has a functional technology foundation, significant improvements are needed to ensure compliance with data protection best practices and modern cybersecurity standards.

Implementing the above recommendations will reduce the company’s exposure to data breaches, enhance resilience, and promote customer trust. Regular follow-up audits and continuous monitoring are advised to maintain a strong security posture.