Audit de Sécurité : Botium Toys

Réalisé selon le cadre NIST CSF - [Date du rapport]

---

1. Évaluation des Contrôles

Réponse à : "Botium Toys dispose-t-il actuellement de ce contrôle ?"

Contrôle	Présent	Justification
Least Privilege	❌ Non	Tous les employés accèdent aux données sensibles (rapport section "Additional comments").
Disaster recovery plans	❌ Non	Aucun plan existant (rapport : "no disaster recovery plans").
Password policies	✅ Oui	Existe mais critères faibles ("requirements are nominal").
Separation of duties	❌ Non	Non implémenté ("separation of duties not implemented").
Firewall	✅ Oui	Configuré avec règles de sécurité ("firewall blocks traffic").
Intrusion detection system (IDS)	❌ Non	Absent ("not installed").
Backups	❌ Non	Aucune sauvegarde critique ("no backups of critical data").
Antivirus software	✅ Oui	Installé et surveillé ("monitored regularly").
Monitoring manuel des systèmes hérités	⚠ Partiel	Maintenance sans planning ("no regular schedule").
Encryption	❌ Non	Non utilisé ("encryption is not currently used").
Système de gestion des mots de passe	❌ Non	Absent ("no centralized password management system").
Verrous (bureaux, magasin, entrepôt)	✅ Oui	Suffisants ("sufficient locks").
Surveillance CCTV	✅ Oui	À jour ("up-to-date CCTV").
Détection/prévention incendie	✅ Oui	Fonctionnel ("functioning systems").

---

2. Évaluation de la Conformité

PCI DSS

"Botium Toys respecte-t-il cette pratique ?"

Exigence	Conforme	Justification
Accès restreint aux données cartes de crédit	❌ Non	Tous les employés y accèdent.
Traitement sécurisé des données de paiement	❌ Non	Pas de chiffrement, stockage local non sécurisé.
Mise en œuvre du chiffrement	❌ Non	Non appliqué.
Politiques de mots de passe robustes	❌ Non	Politique faible, pas de système centralisé.

GDPR

Exigence	Conforme	Justification

Exigence	Conforme	Justification
Confidentialité des données clients UE	❌ Non	Données PII accessibles à tous les employés.
Notification des clients UE sous 72h en cas de violation	✅ Oui	Plan existant ("plan to notify within 72 hours").
Classification et inventaire des données	❌ Non	Mauvaise gestion des actifs ("inadequate asset management").
Application des politiques de confidentialité	✅ Oui	Politiques appliquées ("privacy policies enforced").

SOC (Type 1/2)

Exigence	Conforme	Justification
Politiques d'accès utilisateur définies	❌ Non	Pas de moindre privilège.
Confidentialité des données sensibles (PII/SPII)	❌ Non	Exposition généralisée.
Intégrité des données	✅ Oui	Contrôles assurés ("ensured data integrity").
Disponibilité pour les personnes autorisées	❌ Non	Accès non restreint.

---

3. Recommandations Prioritaires

⚠️ Contrôles Critiques (Risque Élevé)

1. **Implémenter le moindre privilège**
   - *Objectif* : Restreindre l'accès aux données cartes de crédit et PII.
   - *Délai* : 1 mois
2. **Chiffrement des données sensibles**
   - *Objectif* : Conformité PCI DSS/GDPR.
   - *Solution* : Chiffrement AES-256 pour les données au repos/en transit.
3. **Sauvegardes automatisées + Plan de reprise**
   - *Objectif* : Protéger contre la perte de données critiques.
   - *Fréquence* : Sauvegardes quotidiennes hors-site.

📋 Conformité (Risque Moyen)

- **PCI DSS** :
  - Segmenter le réseau (isoler les données de paiement).
  - Audit trimestriel des accès.
- **GDPR** :
  - Former les employés à la manipulation des données PII.
  - Désigner un DPO (Data Protection Officer).
- **SOC** :
  - Documenter les politiques d'accès.
  - Mettre en place un système de journalisation (logging).

---

4. Annexe : Évaluation des Risques

- **Score de risque** : 8/10 (Élevé)
- **Raisons clés** :
  - Absence de contrôles d'accès (exposition des données clients).
  - Non-conformité PCI DSS/GDPR (risque d'amendes jusqu'à 4% du CA annuel).
  - Aucune stratégie de reprise après sinistre.

> *"La croissance non contrôlée de Botium Toys expose l'entreprise à des risques opérationnels et juridiques majeurs. Les recommandations ci-dessus réduiront le score de risque à ≤3/10 sous 6 mois."*