# Mémo pour les parties prenantes

À : Responsable informatique, parties prenantes Société XXXXX

DE : David Chardon  
DATE : 25-02-2024  
OBJET : Résultats et recommandations de l'audit interne d'informatique

Chers/Chères collègues,

Veuillez prendre connaissance des informations suivantes concernant la portée, les objectifs, les principales conclusions, le résumé et les recommandations de l'audit interne de Botium Toys.

**Portée :**

* Les systèmes suivants sont concernés : comptabilité, détection des endpoints, pare-feux, système de détection d'intrusion, outil SIEM. Les systèmes seront évalués en fonction des critères suivants :
  + Autorisations de l'utilisateur actuel
  + Contrôles actuels mis en œuvre
  + Procédures et protocoles actuels
* S'assurer que les autorisations des utilisateurs, les contrôles, les procédures et les protocoles en place s'alignent sur les exigences de conformité aux normes PCI DSS et au RGPD.
* S'assurer que la technologie actuelle est prise en compte, tant pour le matériel que pour l'accès au système.

Objectifs :

* Adhérer au NIST CSF.
* Mettre en place un meilleur processus pour leurs systèmes afin de s'assurer qu'ils sont conformes.
* Renforcer les contrôles du système.
* S'adapter au concept des moindres autorisations lorsqu'il s'agit de la gestion des informations d'identification des utilisateurs.
* Établir leurs politiques et procédures, y compris leurs playbooks.
* Veiller à ce qu'ils respectent les exigences en matière de conformité.

**Constatations critiques** (à traiter immédiatement) :

* De multiples contrôles doivent être élaborés et mis en œuvre pour atteindre les objectifs de l'audit, notamment :
  + Contrôle du moindre privilège et séparation des tâches
  + Plans de reprise après sinistre
  + Politiques en matière de mots de passe, de contrôle d'accès et de gestion des comptes, notamment la mise en œuvre d'un système de gestion des mots de passe
  + Chiffrement (pour sécuriser les transactions sur les sites web)
  + IDS
  + Sauvegardes
  + Logiciel antivirus
  + Vidéosurveillance
  + Verrous
  + Surveillance, maintenance et intervention manuelles pour les systèmes existants
  + Systèmes de détection et de prévention des incendies
* Des politiques doivent être élaborées et mises en œuvre pour répondre aux exigences de conformité aux normes PCI DSS et au RGPD.
* Des politiques doivent être élaborées et mises en œuvre pour s'aligner sur les directives SOC1 et SOC2 relatives aux politiques d'accès des utilisateurs et à la sécurité générale des données.

**Constatations** (à aborder, mais il n'y a pas de besoin immédiat) :

* Les contrôles suivants doivent être mis en œuvre dans la mesure du possible :
  + Coffre-fort temporisé
  + Éclairage adéquat
  + Armoires verrouillables
  + Panneau indiquant le fournisseur de services d'alarme
  + Systèmes de détection et de prévention des incendies

**Résumé/recommandations :** il est recommandé que les constatations critiques relatives à la conformité aux normes PCI DSS et au RGPD soient rapidement prises en compte étant donné que Botium Toys accepte les paiements en ligne de clients du monde entier, y compris de l'Union européenne. De plus, étant donné que l'un des objectifs de l'audit est de s'adapter au concept de moindre autorisation, les orientations de SOC1 et SOC2 relatives aux politiques d'accès des utilisateurs et à la sécurité globale des données devraient être utilisées pour élaborer des politiques et des procédures adéquates. Il est également essentiel de disposer de plans de reprise après sinistre et de sauvegardes, car ils permettent d'assurer la continuité des activités en cas d'incident. L'intégration d'un IDS et d'un logiciel AV dans les systèmes actuels renforcera notre capacité à identifier et à atténuer les risques potentiels, et pourrait contribuer à la détection des intrusions, étant donné que les systèmes existants requièrent une surveillance et une intervention manuelles. Pour sécuriser davantage les ressources informatiques hébergées sur le site physique unique de Botium Toys, des verrous et des systèmes de vidéosurveillance doivent être utilisés pour sécuriser les ressources physiques (notamment l'équipement) et pour surveiller et enquêter sur les menaces potentielles. Bien que cela ne soit pas nécessaire dans l'immédiat, l'utilisation du chiffrement et l'existence d'un coffre-fort temporisé, d'un éclairage adéquat, d'armoires verrouillées, de systèmes de détection et de prévention des incendies et d'une signalisation indiquant le fournisseur de services d'alarme amélioreront encore la posture de sécurité de Botium Toys.