Audit de sécurité de Botium Toys

Mémo pour les parties prenantes

A : Responsable informatique, parties prenantes
De : Garance Defrel
Date : 10/03/2024
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 :

L'audit a porté sur les systèmes suivants :

- Système de comptabilité
- Système de gestion des endpoints
- Pare-feu
- Systèmes de détection d'intrusion (IDS)
- Outil SIEM

L'audit a évalué :

- **Autorisations des utilisateurs** : Les droits d'accès de chaque utilisateur.
- **Contrôle en place** : L'efficacité des contrôles de sécurité implémentés.
- **Procédures et protocoles** : La conformité des procédures et protocoles avec les meilleures pratiques.
- **Conformité réglementaire** : La conformité aux normes PCI DSS et au RGPD
- **Technologies et accès au système** : L'utilisation et la sécurité des technologies et des systèmes.

Objectifs :

Les objectifs de l'audit étaient :

- S'aligner sur le NIST CSF (National Institute of Standards and Technology Cybersecurity Framework).
- Garantir la conformité des systèmes de Botium Toys aux normes de sécurité et aux réglementations en vigueur.

- Renforcer les contrôles de sécurité des systèmes.
- Mettre en œuvre le principe du moindre privilège pour la gestion des identifications des utilisateurs.
- Élaborer et/ou réviser les politiques et procédures de sécurité de l'entreprise.
- Confirmer que Botium Toys adhère à toutes les exigences réglementaires et de conformité applicables.

Constatations critiques :
L'audit a révélé des non-conformités aux normes PCI DSS et au RGPD. Botium Toys doit prendre des mesures pour se conformer à ces réglementations.

- **Manque de contrôle d'accès** : Des contrôles d'accès insuffisants exposent les systèmes de Botium Toys à des risques de compromission.
- **Absence de système de détection d'intrusion (IDS)** : L'absence d'un IDS rend Botium Toys vulnérable aux attaques.
- **Manque de sauvegarde des données** : L'absence de sauvegarde de données régulières met en péril la continuité des activités.
- **Non-conformité au RGPD** : Le non-respect des exigences du RGPD expose Botium Toys à des sanctions.

Constatations
- **Manque de formation des employés** : Les employés de Botium Toys ne sont pas suffisamment formés aux bonnes pratiques de sécurité informatique.
- **Système de gestion des mots de passe faibles** : Le système de gestion de mot de passe de Botium Toys ne respecte pas les normes de sécurité minimales.
- **Absence de politique de sécurité pour les appareils mobiles** : Botium Toys n'a pas de politique de sécurité spécifique pour les appareils mobiles utilisés par les employés.

Résumé/Recommandations :

Voici les quelques recommandations proposées :

- **Prioriser la mise en œuvre des contrôles critiques** : Mettre en place les contrôles d'accès, le système IDS, les sauvegardes de données et se conformer aux exigences du RGPD en priorité.
- **Former les employés** : Organiser des formations sur les bonnes pratiques de sécurité informatique pour tous les employés.

- **Renforcer le système de gestion des mots de passe** : Implémenter un système de gestion des mots de passe plus sécurisé, en utilisant des mots de passe forts et la multi-factorisation d'authentification.
- **Élaborer une politique de sécurité pour les appareils mobiles** : Définir les règles d'utilisation des appareils mobiles par les employés.

L'audit a révélé des lacunes importantes dans la sécurité informatique de Botium Toys. La mise en œuvre des recommandations formulées dans ce mémo ci-dessus, est essentielle pour protéger les données, garantir la continuité des activités et se conformer aux réglementations.

Cordialement,

Garance Defrel