À : Responsable informatique, parties prenantes

DE : Icecore013

DATE : 27/02/2024

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 :

L'audit informatique interne de Botium Toys a évalué l'ensemble du programme de sécurité de l'entreprise, y compris toutes les ressources numériques, les processus et procédures internes. Les éléments suivants ont été évalués :

\* Autorisations actuelles des utilisateurs dans les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outil de gestion des informations et des événements de sécurité (SIEM).

\* Contrôles actuellement mis en œuvre dans les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outil de gestion des informations et des événements de sécurité (SIEM).

\* Procédures et protocoles en vigueur pour les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outil de gestion des informations et des événements de sécurité (SIEM).

\* Conformité des autorisations, contrôles, procédures et protocoles en place aux exigences nécessaires.

\* Prise en compte des technologies actuelles pour l'accès au matériel et au système.

Objectifs :

Les objectifs de l'audit informatique interne de Botium Toys sont les suivants :

\* Adhérer au cadre de cybersécurité du Institut national des normes et de la technologie (NIST CSF).

\* Mettre en place un meilleur processus pour leurs systèmes afin de s'assurer qu'ils sont conformes.

\* Renforcer les contrôles du système.

\* Mettre en œuvre le concept des moindres autorisations dans le cadre 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) :

\* Absence de mise en œuvre du chiffrement pour protéger les informations confidentielles.

\* Manque de plans de reprise après sinistre pour assurer la continuité des activités en cas d'incident.

\* Manque de système de gestion des mots de passe pour faciliter la récupération, la réinitialisation et les notifications de verrouillage.

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

\* Nécessité d'améliorer la séparation des tâches pour éviter les abus de système à des fins personnelles.

\* Besoin de renforcer les politiques de contrôle d'accès pour améliorer la confidentialité et l'intégrité des données.

Résumé/recommandations :

L'audit a permis d'identifier plusieurs vulnérabilités et domaines à améliorer dans le programme de sécurité de Botium Toys. Pour adhérer au cadre de cybersécurité du NIST CSF et renforcer la posture de sécurité globale de l'entreprise, nous recommandons de :

1. Mettre en œuvre le chiffrement pour protéger les informations confidentielles.

2. Développer et mettre en œuvre des plans de reprise après sinistre pour assurer la continuité des activités en cas d'incident.

3. Mettre en place un système de gestion des mots de passe pour faciliter la récupération, la réinitialisation et les notifications de verrouillage.

4. Améliorer la séparation des tâches pour éviter les abus de système à des fins personnelles.

5. Renforcer les politiques de contrôle d'accès pour améliorer la confidentialité et l'intégrité des données.

Nous vous recommandons vivement de prendre en compte ces recommandations et de mettre en œuvre les mesures nécessaires pour améliorer la posture de sécurité de Botium Toys.

Cordialement,