Mémo pour les parties prenantes

À : Responsable informatique, parties prenantes
DE : Tyana
DATE : 30 mai 2024
OBJET : Résultats et recommandations de l'audit interne d'informatique

Chers collègues,

Je vous prie de bien vouloir 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 concernés par cet audit incluent : la comptabilité, la détection des endpoints, les pare-feux, le système de détection d'intrusion (IDS) et l'outil SIEM. Ces systèmes ont été évalués selon les critères suivants :

- Les autorisations des utilisateurs actuels,
- Les contrôles en place,
- Les procédures et protocoles actuels.

L'objectif est de vérifier que les autorisations des utilisateurs, les contrôles, les procédures et les protocoles respectent les exigences de conformité aux normes PCI DSS et RGPD, tout en prenant en compte les technologies actuelles, qu'il s'agisse du matériel ou de l'accès au système.

Objectifs :

- Adopter le cadre de sécurité NIST CSF.
- Améliorer les processus pour assurer la conformité des systèmes.
- Renforcer les contrôles existants.
- Mettre en œuvre le principe du moindre privilège pour la gestion des identifiants utilisateurs.
- Élaborer et formaliser les politiques et procédures, y compris les playbooks.

- Garantir le respect des exigences de conformité.

Constatations critiques (à traiter immédiatement) :

Plusieurs contrôles doivent être mis en place pour atteindre les objectifs de l'audit, notamment :

- Contrôle du moindre privilège et séparation des tâches,
- Plans de reprise après sinistre,
- Politiques de mots de passe, contrôle d'accès et gestion des comptes (y compris un système de gestion des mots de passe),
- Chiffrement (pour sécuriser les transactions sur les sites web),
- Système IDS,
- Sauvegardes,
- Logiciel antivirus,
- Vidéosurveillance,
- Verrous,
- Surveillance et maintenance 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 RGPD, ainsi qu'aux directives SOC1 et SOC2 concernant les politiques d'accès des utilisateurs et la sécurité des données.

Constatations (à aborder, mais non urgentes) :

Les contrôles suivants devraient 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 de traiter rapidement les constatations critiques relatives à la conformité aux normes PCI DSS et RGPD, car Botium Toys accepte des paiements en ligne de clients du monde entier, y compris de l'Union européenne. De plus, afin de respecter le principe du moindre privilège, il est conseillé de suivre les orientations SOC1 et SOC2 pour élaborer des politiques d'accès des utilisateurs et des mesures de sécurité des données adéquates.

La mise en place de plans de reprise après sinistre et de sauvegardes est cruciale pour assurer la continuité des activités en cas d'incident. L'intégration d'un IDS et d'un logiciel antivirus renforcera la capacité à détecter et à atténuer les risques, étant donné que les systèmes actuels nécessitent une surveillance manuelle. Enfin, pour sécuriser les ressources hébergées sur le site physique de Botium Toys, il est important d'installer des verrous et des systèmes de vidéosurveillance pour protéger l'équipement et surveiller d'éventuelles menaces.

Bien que non urgente, l'utilisation du chiffrement, l'ajout d'un coffre-fort temporisé, d'un éclairage adéquat, d'armoires verrouillables, de systèmes de détection et de prévention des incendies, ainsi que d'une signalisation indiquant le fournisseur de services d'alarme, renforceront encore la sécurité globale de Botium Toys.