Botium Toys : Portée, objectifs et rapport d'évaluation des risques

Portée et objectifs de l'audit

Portée: La portée de cet audit est définie comme l'ensemble du programme de sécurité de Botium Toys. Cela inclut leurs actifs tels que les équipements et appareils des employés, leur réseau interne et leurs systèmes. Vous devrez examiner les actifs de Botium Toys ainsi que les contrôles et les pratiques de conformité qu'ils ont mis en place.

Objectifs: Évaluez les actifs existants et complétez la liste de contrôle des contrôles et de la conformité pour déterminer les meilleures pratiques de contrôle et de conformité qui doivent être mises en œuvre pour améliorer la posture de sécurité de Botium Toys.

Actifs courants

Les actifs gérés par le service informatique comprennent :

- Équipement sur site pour les besoins professionnels au bureau
- Équipements des employés : appareils des utilisateurs finaux (ordinateurs de bureau/portables, smartphones), postes de travail distants, casques, câbles, claviers, souris, stations d'accueil, caméras de surveillance, etc.
- Produits en vitrine disponibles à la vente au détail sur place et en ligne ; stocké dans l'entrepôt attenant à l'entreprise
- Gestion de systèmes, logiciels et services : comptabilité, télécommunications, bases de données, sécurité, commerce électronique et gestion des stocks
- accès Internet
- Réseau interne
- Conservation et stockage des données
- Maintenance des systèmes existants : systèmes en fin de vie qui nécessitent une surveillance humaine

L'évaluation des risques

Description du risque

Actuellement, la gestion des actifs est inadéquate. De plus, Botium Toys ne dispose pas de tous les contrôles appropriés et peut ne pas être entièrement conforme aux réglementations et normes américaines et internationales.

Contrôler les bonnes pratiques

La première des cinq fonctions du NIST CSF est l'identification. Botium Toys devra consacrer des ressources pour identifier les actifs afin de pouvoir les gérer de manière appropriée. En outre, ils devront classer les actifs existants et déterminer l'impact de la perte des actifs existants, y compris les systèmes, sur la continuité des activités.

Score de risque

Sur une échelle de 1 à 10, le score de risque est de 8, ce qui est assez élevé. Cela est dû au manque de contrôles et au manque de respect des meilleures pratiques en matière de conformité.

Commentaires supplémentaires

L'impact potentiel de la perte d'un actif est jugé moyen, car le service informatique ne sait pas quels actifs seraient à risque. Le risque pour les actifs ou les amendes de la part des organes directeurs est élevé car Botium Toys ne dispose pas de tous les contrôles nécessaires et n'adhère pas pleinement aux meilleures pratiques liées aux réglementations de conformité qui maintiennent la confidentialité et la sécurité des données critiques. Consultez les puces suivantes pour plus de détails :

- Actuellement, tous les employés de Botium Toys ont accès aux données stockées en interne et peuvent accéder aux données des titulaires de carte et aux PII/SPII des clients.
- Le cryptage n’est actuellement pas utilisé pour garantir la confidentialité des informations de carte de crédit des clients qui sont acceptées, traitées, transmises et stockées localement dans la base de données interne de l’entreprise.
- Les contrôles d'accès relatifs au moindre privilège et à la séparation des tâches n'ont pas été mis en œuvre.
- Le service informatique a assuré la disponibilité et intégré des contrôles pour garantir l’intégrité des données.

- Le service informatique dispose d'un pare-feu qui bloque le trafic sur la base d'un ensemble de règles de sécurité correctement définies.
- Un logiciel antivirus est installé et surveillé régulièrement par le service informatique.
- Le service informatique n'a pas installé de système de détection d'intrusion (IDS).
- Il n’existe actuellement aucun plan de reprise après sinistre et l’entreprise ne dispose pas de sauvegarde des données critiques.
- Le service informatique a établi un plan pour informer l'UE. clients dans les 72 heures en cas de faille de sécurité. De plus, des politiques, procédures et processus de confidentialité ont été élaborés et sont appliqués parmi les membres du service informatique/autres employés, afin de documenter et de conserver correctement les données.
- Bien qu'il existe une politique de mot de passe, ses exigences sont nominales et ne correspondent pas aux exigences minimales actuelles en matière de complexité des mots de passe (par exemple, au moins huit caractères, une combinaison de lettres et au moins un chiffre ; caractères spéciaux).
- Il n'existe pas de système centralisé de gestion des mots de passe qui applique les exigences minimales de la politique de mot de passe, ce qui affecte parfois la productivité lorsque les employés/fournisseurs soumettent un ticket au service informatique pour récupérer ou réinitialiser un mot de passe.
- Bien que les systèmes existants soient surveillés et entretenus, aucun calendrier régulier n'est en place pour ces tâches et les méthodes d'intervention ne sont pas claires.
- L'emplacement physique du magasin, qui comprend les bureaux principaux, la devanture du magasin et l'entrepôt de produits de Botium Toys, dispose de serrures suffisantes, d'une surveillance par télévision en circuit fermé (CCTV) à jour, ainsi que de systèmes de détection et de prévention des incendies fonctionnels.