Scénario :

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

---

Portée et objectifs de l'audit

Portée: Cet audit couvre l'ensemble du programme de sécurité de Botium Toys. Il inclut ses actifs, tels que les équipements et appareils des employés, son réseau interne et ses systèmes. Vous devrez examiner les actifs de Botium Toys, ainsi que les contrôles et les pratiques de conformité 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 département 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 ; stockés dans l'entrepôt attenant de l'entreprise
- Gestion des systèmes, logiciels et services : comptabilité, télécommunication, base de données, sécurité, commerce électronique et gestion des stocks
- accès Internet
- Réseau interne
- Conservation et stockage des données
- Maintenance des systèmes hérités : systèmes en fin de vie nécessitant 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 n'est peut-être pas entièrement conforme aux réglementations et normes américaines et internationales.

Meilleures pratiques de contrôle

La première des cinq fonctions du CSF du NIST est l'identification. Botium Toys devra consacrer des ressources à l'identification des actifs afin de pouvoir les gérer de manière appropriée. De plus, l'entreprise devra classer les actifs existants et déterminer l'impact de leur perte, 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 s'explique par un manque de contrôles et de respect des bonnes pratiques de conformité.

Commentaires supplémentaires

L'impact potentiel de la perte d'un actif est jugé moyen, car le service informatique ignore quels actifs seraient menacés. Le risque pour les actifs ou les amendes des autorités compétentes est élevé, car Botium Toys ne dispose pas de tous les contrôles nécessaires et ne respecte pas pleinement les bonnes pratiques liées aux réglementations de conformité garantissant la confidentialité et la sécurité des données critiques. Consultez les points suivants pour plus de détails :

- Actuellement, tous les employés de Botium Toys ont accès aux données stockées en interne et peuvent être en mesure d’accéder aux données des titulaires de cartes 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 principe du 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 en fonction d'un ensemble de règles de sécurité définies de manière appropriée.
- 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 sauvegardes de données critiques.
- Le service informatique a mis en place un plan pour informer les clients de l'UE dans les 72 heures en cas de faille de sécurité. De plus, des politiques, procédures et processus de confidentialité ont été élaborés et appliqués par les membres du service informatique et les autres employés afin de documenter et de conserver correctement les données.
- Bien qu'une politique de mot de passe existe, ses exigences sont nominales et ne sont pas conformes aux exigences actuelles de complexité minimale 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, il n'existe pas de calendrier régulier pour ces tâches et les méthodes d'intervention ne sont pas claires.
- L'emplacement physique du magasin, qui comprend les bureaux principaux de Botium Toys, la devanture du magasin et l'entrepôt de produits, dispose de suffisamment de serrures, d'une surveillance par télévision en circuit fermé (CCTV) à jour, ainsi que de systèmes de détection et de prévention des incendies fonctionnels.

Exercice:

Liste de contrôle des contrôles et de la conformité

Liste de contrôle d'évaluation des contrôles

Oui	Non	Contrôle
☐	☑	moindre privilège
☐	☑	Plans de reprise après sinistre
☐	☑	Politiques de mot de passe
☐	☑	Séparation des tâches
☑	☐	Pare-feu
☐	☑	Système de détection d'intrusion (IDS)
☐	☑	Sauvegardes
☑	☐	Logiciel antivirus
☑	☐	Surveillance, maintenance et intervention manuelles pour les systèmes existants
☐	☑	Cryptage
☐	☑	Système de gestion des mots de passe
☑	☐	Serrures (bureaux, vitrine, entrepôt)
☑	☐	Surveillance par télévision en circuit fermé (CCTV)
☑	☐	Détection/prévention incendie (alarme incendie, système de gicleurs, etc.)

Liste de contrôle de conformité

Norme de sécurité des données de l'industrie des cartes de paiement (PCI DSS)

Oui	Non	Meilleures pratiques
☐	☑	Seuls les utilisateurs autorisés ont accès aux informations de carte de crédit des clients.

☑	☐	Les informations de carte de crédit sont stockées, acceptées, traitées et transmises en interne, dans un environnement sécurisé.
☐	☑	Mettre en œuvre des procédures de cryptage des données pour mieux sécuriser les points de contact et les données des transactions par carte de crédit.
☐	☑	Adoptez des politiques de gestion des mots de passe sécurisées.

Règlement général sur la protection des données (RGPD)

Oui	Non	Meilleures pratiques
☐	☑	Les données des clients de l'UE sont conservées de manière privée et sécurisée.
☑	☐	Un plan est en place pour informer les clients de l'UE dans les 72 heures si leurs données sont compromises ou s'il y a une violation.
☐	☑	Assurez-vous que les données sont correctement classées et inventoriées.
☑	☐	Appliquer les politiques, procédures et processus de confidentialité pour documenter et conserver correctement les données.

Contrôles des systèmes et des organisations (SOC type 1, SOC type 2)

Oui	Non	Meilleures pratiques
☐	☑	Des politiques d'accès des utilisateurs sont établies.
☐	☑	Les données sensibles (PII/SPII) sont confidentielles/privées.
☑	☐	L'intégrité des données garantit que les données sont cohérentes, complètes, exactes et ont été validées.
☐	☑	Les données sont accessibles aux personnes autorisées à y accéder.

Recommandations :L'organisation doit se conformer à la législation américaine en vigueur et adopter toutes les règles du RGPD pour se protéger des poursuites judiciaires en cas d'attaque.

L'entreprise doit s'appuyer sur des référentiels pour construire sa politique de sécurité, comme le NIST CSF.

De plus, l'entreprise doit renforcer sa sécurité en adoptant une politique de moindre privilège, en renforçant son accès aux données personnelles et privées sensibles, ainsi qu'en adoptant une politique de mots de passe robuste et en adoptant une authentification multifacteur pour les données les plus sensibles. Le chiffrement des données doit être déployé pour garantir leur intégrité.

De plus, l'entreprise doit se doter d'un système de détection d'intrusion (IDS) et établir des procédures pour gérer les processus en cas d'attaque malveillante sur ses actifs. Un plan général de réparation et de reprise d'activité doit être mis en œuvre pour assurer la continuité des activités en cas d'attaque. Un processus de sauvegarde et de préservation des données doit également être mis en place.

L'organisation doit identifier et classer les données afin de réaliser une évaluation plus précise des risques et des menaces et des contrôles efficaces à mettre en œuvre.

Par ailleurs, une politique de formation et de sensibilisation des salariés aux bonnes pratiques pourrait être mise en place.

Enfin, il est important de s’assurer que le matériel utilisé n’est pas obsolète et que son matériel et ses logiciels sont à jour.