Botium Toys : portée et objectifs de l'audit

**Portée**

L'audit informatique interne de Botium Toys évaluera les éléments suivants :

* 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).
* Veiller à ce que les autorisations, contrôles, procédures et protocoles en place pour les utilisateurs soient conformes aux exigences de conformité nécessaires.
* Veiller à ce que les technologies actuelles soient prises en compte. 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

**Questions mises en place lors de la lecture de l’évaluation des risques :**

* Quels sont les risques les plus importants pour l'entreprise ?
  + - Risque pouvant permettre une attaque :
      * Les réseau interne de l’entreprise sont il sécurisé ?
      * La gestion des accès au bâtiments sont ils correctes ?
      * La gestion des accès au matériel est elle correcte ? (code, double authentificationn badge….)
      * Le matériel est il suivie ? nominatif ? y a-t-il en place un système moindre privilège?
      * Les employer sont il formé à la sécurité ?
      * Y a til un moyen de vérifier l’intrusion de
    - En cas d’attaque, qu’est ce qui peut ‘amener à sa réussite
      * Y a-t-il des protocoles de sécurité ? une organisation et une équipe ? ou sont les playbook ?
      * Y a t’il un système de log ?
      * Quelles sont les ressource enregistrée ?   
        l’entreprise est elle en état de légalité (rgpd ect ?)
    - En cas de réussite, comment gérer les ressources.
      * Y a til un backend ?
      * Les ressources qui doivent être détruite après utilisation le sont elle bien ?
      * Y a-t-il un principe de ressource minimum appliqué ?
  + Dans l’entreprise
  + En télétravail
* Quels sont les contrôles les plus essentiels à mettre en œuvre immédiatement ou à l'avenir ?
* Quelle est la réglementation de conformité à laquelle Botium Toys doit se conformer pour garantir la sécurité des données des clients et des fournisseurs, éviter les amendes, etc. ?