Botium Toys : portée et objectifs de l'audit

Il s'agit d'une entreprise fictive :

Botium Toys est une petite entreprise américaine qui développe et vend des jouets. L'entreprise dispose d'un seul site physique, qui lui sert de bureau principal, de vitrine et d'entrepôt pour ses produits. Cependant, la présence en ligne de Botium Toy s'est développée, attirant des clients aux États-Unis et à l'étranger. Par conséquent, le service informatique est de plus en plus sollicité pour soutenir le marché en ligne dans le monde entier.

La responsable du service informatique a décidé qu'un audit informatique interne devait être réalisé. Elle s'inquiète de ne pas disposer d'un plan d'action solide pour assurer la continuité et la conformité de l'entreprise au fur et à mesure de son développement. Elle pense qu'un audit interne peut contribuer à mieux sécuriser l'infrastructure de l'entreprise et l'aider à identifier et à atténuer les risques potentiels, les menaces ou les vulnérabilités des actifs critiques. La responsable souhaite également s'assurer que l'entreprise respecte les réglementations relatives au traitement interne et à l'acceptation des paiements en ligne, ainsi qu'à la conduite des affaires dans l'Union européenne (U.E.).

Le responsable informatique commence par mettre en œuvre le cadre de cybersécurité du National Institute of Standards and Technology (NIST CSF), définit le champ d'application et les objectifs de l'audit, dresse la liste des actifs actuellement gérés par le service informatique et procède à une évaluation des risques. L'objectif de l'audit est de fournir une vue d'ensemble des risques et/ou des amendes que l'entreprise pourrait encourir en raison de l'état actuel de son dispositif de sécurité.

Votre tâche consiste à examiner le champ d'application, les objectifs et le rapport d'évaluation des risques du responsable informatique. Ensuite, vous effectuerez un audit interne en remplissant une liste de contrôle et de conformité.

Botium Toys : évaluation des risques

Ressources numériques actuelles

Les ressources numériques gérées par le service informatique sont les suivantes :

- Équipements sur place pour les besoins de l'entreprise
- Équipements des employés : appareils des utilisateurs (ordinateurs de bureau/portables, smartphones), postes de travail à distance, casques, câbles, claviers, souris, stations d'accueil, caméras de surveillance, etc.
- Gestion de systèmes, de logiciels et de services : comptabilité, télécommunications, bases de données, sécurité, e-commerce et gestion des stocks
- Accès Internet
- Réseau interne
- Gestion des accès des fournisseurs
- Services d'hébergement de centres de données
- Conservation et stockage des données
- Lecteurs de badge
- Maintenance des systèmes anciens : systèmes en fin de vie qui nécessitent une surveillance humaine

Description des risques

Actuellement, la gestion des ressources est inadéquate. Par ailleurs, Botium Toys n'a pas mis en place les contrôles appropriés et peut ne pas être en conformité avec les réglementations et les normes américaines et internationales.

Les bonnes pratiques en matière de contrôle

La première des cinq fonctions du NIST CSF est Identifier. Botium Toys devra se consacrer à la gestion des ressources. De plus, ils devront déterminer l'impact de la perte de ressources existantes, notamment des 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 à un manque de contrôles et d'adhésion aux réglementations et normes de conformité nécessaires.

Commentaires supplémentaires

L'impact potentiel de la perte d'une ressource est jugé moyen, car le service informatique ne sait pas quelles ressources seraient perdues. La probabilité d'une perte de ressources ou d'amendes de la part des instances gouvernementales est élevée car Botium Toys n'a pas mis en place tous les contrôles nécessaires et n'adhère pas aux réglementations et aux normes requises en matière de confidentialité des données des clients.

Audit de sécurité Botium Toys

Botium Toys est une petite entreprise américaine qui développe et vend des jouets. L'entreprise n'a qu'un seul emplacement physique. Cependant, sa présence en ligne a augmenté, attirant des clients aux États-Unis et à l'étranger. Son service informatique est soumis à une pression croissante pour soutenir son marché en ligne dans le monde entier.
La responsable du service informatique a décidé qu'un audit informatique interne devait être réalisé. Elle s'inquiète de l'absence d'un plan d'action solide pour assurer la continuité des activités et la conformité de l'entreprise au fur et à mesure de son développement. Elle estime qu'un audit interne peut contribuer à mieux sécuriser l'infrastructure de l'entreprise et l'aider à identifier et à atténuer les risques potentiels, les menaces ou les vulnérabilités des ressources critiques. La responsable souhaite également s'assurer que l'entreprise respecte les réglementations relatives à l'acceptation des paiements en ligne et à la conduite des affaires dans l'Union européenne (U.E.).
La responsable informatique commence par mettre en œuvre le Cybersecurity Framework de l'Institut national des normes et de la technologie (NIST CSF), en définissant le champ d'application et les objectifs de l'audit et en procédant à une évaluation des risques. L'objectif de l'audit est de fournir une vue d'ensemble des risques auxquels l'entreprise peut être confrontée en raison de l'état actuel de sa posture de sécurité. La responsable informatique souhaite utiliser les résultats de l'audit comme preuve pour obtenir l'autorisation de développer son service.
Votre tâche consiste à examiner le champ d'application, les objectifs et l'évaluation des risques de la responsable informatique. Ensuite, réalisez un audit interne pour compléter l'évaluation des contrôles et la liste de contrôle de la conformité.

Ressources numériques actuelles

Les ressources numériques gérées par le service informatique sont les suivantes :

- Équipements sur place pour les besoins de l'entreprise
- Équipements des employés : appareils des utilisateurs (ordinateurs de bureau/portables, smartphones), postes de travail à distance, casques, câbles, claviers, souris, stations d'accueil, caméras de surveillance, etc.
- Gestion de systèmes, de logiciels et de services : comptabilité, télécommunications, bases de données, sécurité, e-commerce et gestion des stocks
- Accès Internet
- Réseau interne
- Gestion des accès des fournisseurs
- Services d'hébergement de centres de données
- Conservation et stockage des données
- Lecteurs de badge
- Maintenance des systèmes anciens : systèmes en fin de vie qui nécessitent une surveillance humaine

Contrôles administratifs			
Nom du contrôle	**Type de contrôle et explication**	**Doit être mis en œuvre**	**Priorité**
Moindre privilège	Préventif: permet de limiter l'accès des vendeurs et du personnel non autorisé uniquement aux ressources informatiques et données nécessaires pour accomplir leurs tâches.	Oui	Élevée
Plans de reprise après sinistre	Correctif: assure la continuité des activités en cas d'incident, en minimisant ou éliminant les pertes de productivité dues aux temps d'arrêt. Cela couvre : les conditions environnementales (climatisation, alimentation électrique), le matériel (serveurs, équipements), la connectivité réseau, les applications (e-mail, données électroniques), ainsi que la	Oui	Élevée

Contrôles administratifs			
	sauvegarde et restauration des données.		
Politiques de mots de passe	Préventif: établit des règles pour renforcer les mots de passe afin d'améliorer la sécurité et réduire le risque de compromission des comptes par des attaques par force brute ou dictionnaire.	Oui	Élevée
Politiques de contrôle d'accès	Préventif: renforce la confidentialité et l'intégrité des données en contrôlant l'accès.	Oui	Élevée
Politiques de gestion des comptes	Préventif: réduit la surface d'attaque et minimise l'impact des employés mécontents ou des anciens employés.	Oui	Élevée
Séparation des tâches	Préventif: assure que personne ne dispose d'un accès pouvant lui permettre d'abuser du système à des fins personnelles.	Oui	Élevée

Contrôles techniques			
Nom du contrôle	**Type de contrôle et explication**	**Doit être mis en œuvre**	**Priorité**
Pare-feu	Préventif: des pare-feux sont déjà en place pour filtrer le trafic indésirable ou malveillant qui tente de pénétrer dans le réseau interne.	S.O.	S.O.
Système de détection	Détectif: permet à l'équipe informatique d'identifier	Oui	Élevée

d'intrusion (IDS)	rapidement des intrusions potentielles (par exemple, un trafic anormal).		
Chiffrement	Dissuasif: assure la protection des informations sensibles (comme les transactions de paiement en ligne).	Oui	Élevée
Sauvegardes	Correctif: permet de maintenir la productivité en cas d'événement imprévu et s'aligne avec le plan de reprise après sinistre.	Oui	Élevée
Système de gestion des mots de passe	Correctif: permet la récupération, la réinitialisation et la gestion des mots de passe, avec des notifications de verrouillage.	Oui	Élevée
Logiciel antivirus (AV)	Correctif: permet de détecter et de mettre en quarantaine les menaces connues.	Oui	Élevée
Surveillance, maintenance et intervention manuelles	Préventif/Correctif: nécessaire pour les systèmes actuels afin d'identifier et d'atténuer les menaces, les risques et les vulnérabilités.	Oui	Élevée

Contrôles physiques			
Nom du contrôle	**Type de contrôle et explication**	**Doit être mis en œuvre (X)**	**Priorité**
Coffre-fort temporisé	Dissuasif: réduit l'impact des menaces physiques.	Oui	Moyenne
Éclairage adéquat	Dissuasif: réduit les cachettes	Oui	Moyenne

	pour dissuader les menaces.		
Surveillance par télévision en circuit fermé (CCTV)	Préventif/Détectif: réduit le risque de certains événements et peut servir à des fins d'enquête après un incident.	Oui	Élevée
Armoires verrouillables (pour les équipements de réseau)	Préventif ; améliore l'intégrité en empêchant l'accès non autorisé aux équipements réseau.	Oui	Moyenne
Panneau indiquant le fournisseur de services d'alarme	Dissuasif: réduit la probabilité d'une attaque réussie.	Oui	Faible
Verrous	Préventif: protège les ressources physiques et numériques en renforçant la sécurité.	Oui	Élevée
Détection et prévention des incendies (alarme incendie, système de gicleurs, etc.)	Détectif/Préventif: détecte un incendie pour éviter d'endommager les stocks, serveurs…	Oui	Moyenne