Feuille de travail sur les fuites de données

Résumé de l'incident : Lors d'une réunion, un responsable des ventes a donné accès à un dossier contenant des documents internes à son équipe. Ce dossier comprenait des fichiers relatifs à un nouveau produit non encore annoncé publiquement, ainsi que des analyses clients et des supports promotionnels. Après la réunion, le responsable n'a pas révoqué l'accès au dossier, mais a demandé à son équipe d'attendre une autorisation avant de partager les supports promotionnels.

Lors d'un appel vidéo avec un partenaire commercial, un membre de l'équipe des ventes a oublié l'avertissement de son responsable. Ce commercial souhaitait partager un lien vers des supports promotionnels afin que le partenaire puisse les diffuser à ses clients. Cependant, il a partagé par erreur un lien vers un dossier interne. Par la suite, le partenaire a publié ce lien sur la page des réseaux sociaux de son entreprise, croyant qu'il s'agissait des supports promotionnels.

Contrôle	Le moins privilégié
Problèmes)	***Quels facteurs ont contribué à la fuite d'informations ?*** *L'accès au dossier interne n'était pas limité à l'équipe commerciale et au responsable. Le partenaire commercial n'aurait pas dû être autorisé à diffuser les informations promotionnelles sur les réseaux sociaux.*
Revoir	***Qu'aborde la norme NIST SP 800-53 : AC-6 ?*** *La publication spéciale 800-53 du NIST (AC-6) explique comment une organisation peut protéger la confidentialité de ses données en appliquant le principe du moindre privilège. Elle propose également des améliorations des contrôles afin d'en accroître l'efficacité.*
Recommandation(s)	***Comment le principe du moindre privilège pourrait-il être amélioré au sein de l'entreprise ?*** ● *Limiter l'accès aux ressources sensibles en fonction du rôle de l'utilisateur.* ● *Auditez régulièrement les privilèges des utilisateurs.*

Justification	***Comment ces améliorations pourraient-elles résoudre les problèmes ?*** *Les fuites de données peuvent être évitées si l'accès aux fichiers internes est limité aux seuls employés. De plus, exiger des responsables et des équipes de sécurité qu'ils auditent régulièrement l'accès aux fichiers de l'équipe contribuerait à limiter la divulgation d'informations sensibles.*

Aperçu du plan de sécurité

Le cadre de cybersécurité du NIST (CSF) utilise une structure hiérarchique arborescente pour organiser l'information. De gauche à droite, il décrit une fonction de sécurité générale, puis se précise en se ramifiant en catégories, sous-catégories et contrôles de sécurité individuels.

Fonction	Catégorie	Sous-catégorie	Référence(s)
Protéger	PR.DS : *Sécurité des données*	PR.DS-5 : *Protections contre les fuites de données.*	NIST SP 800-53 : AC-6

Dans cet exemple, les contrôles mis en œuvre par le fabricant pour se protéger contre les fuites de données sont définis dans la norme NIST SP 800-53, un ensemble de lignes directrices pour la sécurisation de la confidentialité des systèmes d'information.

Remarque : Les références contiennent généralement des hyperliens renvoyant aux lignes directrices ou aux règlements auxquels elles se rapportent. Cela facilite l'accès à des informations complémentaires sur la mise en œuvre d'un contrôle particulier. Il est fréquent de trouver plusieurs liens vers différentes sources dans la colonne des références.

NIST SP 800-53 : AC-6

Le NIST a élaboré la norme SP 800-53 pour fournir aux entreprises une solution personnalisable. Plan de protection des données personnelles. Il s'agit d'une ressource complète décrivant un large éventail de catégories de contrôle. Chaque contrôle fournit quelques informations clés :

- **Contrôle :** Définition du contrôle de sécurité.
- **Discussion :** Description de la manière dont le contrôle devrait être mis en œuvre.
- **Améliorations du contrôle :** Liste de suggestions pour améliorer l'efficacité du contrôle.

AC-6	**Le moindre privilège**
	Contrôle: Seuls les accès et autorisations minimaux requis pour accomplir une tâche ou une fonction doivent être fournis aux utilisateurs.
	Discussion: Les processus, les comptes utilisateurs et les rôles doivent être appliqués de manière à garantir le principe du moindre privilège. L'objectif est d'empêcher un utilisateur d'exercer des privilèges supérieurs à ceux nécessaires à la réalisation des objectifs de l'entreprise.
	Améliorations des commandes : ● Limiter l'accès aux ressources sensibles en fonction du rôle de l'utilisateur. ● Révoquer automatiquement l'accès aux informations après un certain délai. ● Conservez les journaux d'activité des comptes utilisateurs provisionnés. ● Auditez régulièrement les privilèges des utilisateurs.

Remarque : Dans la catégorie des contrôles d'accès, SP 800-53 liste le sixième contrôle de moindre privilège, c'est-à-dire AC-6.