Un plan d'action est un document qui décrit les actions à entreprendre pour remédier à des problèmes ou vulnérabilités identifiées lors d'un audit de la sécurité des systèmes d'information. Le plan d'action doit être établi en commun accord avec l'audité, c'est-à-dire l'organisme qui a fait l'objet de l'audit. Il doit prendre en compte les objectifs, les projets en cours et les perspectives de l'audité, ainsi que les résultats de l'appréciation des risques déjà établie.

Le plan d'action doit être organisé par projets, en regroupant les actions et recommandations associées aux différentes vulnérabilités décelées. Il doit également tenir compte des estimations proposées par l'auditeur, qui doivent être données sur la base d'un dimensionnement adéquat des besoins de l'audité, de ses capacités humaines et financières et de l'offre sur le marché Marocain.

Le modèle de rapport d'audit de la sécurité des systèmes d'information prévoit l'utilisation d'un modèle de plan d'action proposé (voir annexe 7). Ce modèle peut être utilisé pour structurer le plan d'action et faciliter sa mise en œuvre. Il comprend généralement les informations suivantes:

* La vulnérabilité ou le problème à remédier
* L'action ou la recommandation proposée pour remédier à la vulnérabilité
* Le responsable de la mise en œuvre de l'action ou de la recommandation
* La date de début et de fin prévue pour la mise en œuvre de l'action ou de la recommandation
* Le coût estimé de la mise en œuvre de l'action ou de la recommandation
* Le statut de l'action ou de la recommandation (en cours, terminée, etc.)

Il est important de suivre de manière régulière l'avancement du plan d'action et de faire des ajustements si nécessaire pour s'assurer que les vulnérabilités sont adéquatement traitées et que la sécurité des systèmes d'information est améliorée.

**Annexe 1**

|  |  |
| --- | --- |
| Nom de l’organisme | Uber Dubai |
| Acronyme | n'a pas d'acronyme officiel |
| Statut | privée |
| Secteur d’activité | Service |
| Catégorie | une entreprise de transport ou de technologie de l'information |
| Site web | [https://www.uber.com/en-AE/cities/dubai](https://www.uber.com/en-AE/cities/dubai/) |
| Adresse Email | N’a pas d’adresse email spécifique |

Voici un exemple de désignation de processus et d'exigences de confidentialité, d'intégrité et de disponibilité des données traitées :

**Annexe 1**

|  |  |  |  |
| --- | --- | --- | --- |
| Désignation du  processus | exigences des données traitées en (1) | | |
| Confidentialité | ntégrité | Disponibilité |
| Processus 1 | 2 | 3 | 3 |
| Processus 2 | 3 | 2 | 2 |
| Processus 3 | 1 | 1 | 4 |

(1) Classement en 4 niveaux : faible (1), moyen (2), fort (3) et très fort (4).

Selon cet exemple, le processus 1 requiert une exigence moyenne en matière de confidentialité, une forte exigence en matière d'intégrité et une forte exigence en matière de disponibilité. Le processus 2 requiert une forte exigence en matière de confidentialité, une exigence moyenne en matière d'intégrité et une exigence moyenne en matière de disponibilité. Enfin, le processus 3 requiert une faible exigence en matière de confidentialité, une faible exigence en matière d'intégrité et une très forte exigence en matière de disponibilité.

Cette désignation peut être utilisée pour établir un plan d'action qui prenne en compte les exigences de chaque processus en matière de sécurité de l'information.

***Annexe 3 : Description du SI Uber Dubai***

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

Haut du formulaire

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| Applications | | | | | | | |
| Nom | Modules | Description | Environnement  de développement | Développée  par /Année | Noms ou @IP des  serveurs  d’hébergement | Nombre  d’utilisateurs | Incluse au  périmètre  d’audit (6) |
| Gestion de  la  production | Suivi de la chaîne d'approvision-  nement,  planification  des tâches,  gestion  des stocks | Logiciel de  gestion de la  production  permettant de  suivre  l'approvisionn  -ement  en matières  premières, de  planifier les tâches  de production et  de gérer les stocks  de produits finis. | JAVA,MySQL | 2021 | IRIC.company.com | 200 | OUI |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Serveurs (par plateforme) | | | | | |
| Nom | @IP | Type | Système d’exploitation | Rôle/métier | Inclus au périmètre  d’audit |
| Server1 | 192.168.1.1 | Machine  virtuelle (MV) | Windows  Server 2016 | Contrôleur de  domaine, messagerie,  application métier | Oui |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Infrastructure Réseau et sécurité | | | | | |
| Nature | Marque | Nombre | Administré par | Observations | Inclus au périmètre  d’audit |
| Szitch | Cisco | 10 | Société ABC | Switches de niveau 3  pour une meilleure  performance | OUI |

|  |  |  |
| --- | --- | --- |
| Postes de travail | | |
| Système d’exploitation | Nombre | Inclus au périmètre d’audit |
| Windows 10 | 100 | OUI |

Voici comment un processus de gestion des incidents de sécurité de l'information pourrait être modélisé pour une organisation comme Uber:

1. Détection: La première étape consiste à détecter l'incident de sécurité de l'information. Cela peut être fait en utilisant des outils de surveillance et de détection des menaces, en analysant les journaux de sécurité et en recevant des notifications de partenaires de sécurité ou de membres du personnel.
2. Évaluation: Une fois que l'incident a été détecté, il est important de l'évaluer rapidement pour déterminer sa gravité et son impact potentiel sur l'organisation. Cela peut être fait en utilisant des méthodologies d'évaluation des risques et en collaborant avec les équipes de sécurité et les responsables de l'information.
3. Réponse: Une fois que l'incident a été évalué, il est important de mettre en place une réponse rapide et efficace. Cela peut inclure des mesures telles que la mise en quarantaine de systèmes ou de comptes compromis, la mise à jour de logiciels de sécurité ou la notification de parties prenantes clés.
4. Correction: Après avoir pris des mesures pour contenir l'incident, il est important de corriger les vulnérabilités qui ont permis l'incident et de mettre en place des mesures de prévention pour éviter qu'un incident similaire ne se produise à l'avenir.
5. Suivi: Une fois que l'incident a été géré et résolu, il est important de suivre l'incident et de documenter les leçons apprises pour améliorer les processus de gestion des incidents à l'avenir. Cela peut inclure la création de rapports d'incidents et la mise en place de processus de révision et d'amélioration continue.