**FEVRE DAN TP 2 du 17/11/21**

**Question 1** -Identifiez, dans la description du contexte, les éléments permettant d’identifier les vulnérabilités liées au traitement des données à caractère personnel.

* CentreCall gère les 3 pôles liées à la collecte de données, l’infrastructure et serveurs et les applications. Il suffit d’un problème matériel, logiciel, une intrusion ou une erreur de paramétrage sur un de ces pôles pour avoir une fuite, un accès ou une perte de données sur les 3 pôles.
* Les données sont traitées par CentreCall sont ensuite mises à disposition des différents clients qui ont confiées l’externalisation de ces services. Il existe plusieurs risques pour ce fonctionnement car les données vont devoir transiter entre les serveurs de BDD et les clients qui vont les récupérer.
* Le temps des donnée conservées est de 1 an, ce qui peut sembler court mais cela laisse un certain temps pour être rapatrier par quelqu’un qui réussirait à s’introduire sur une de ces bases ou serveurs.
* Les données sont saisies par un opérateur humain sur un ordinateur de bureau pour les questionnaires avant d’être transférés. On ne peut exclure l’erreur humaine, une saisie malencontreuse, un vol de données par l’opérateur ou une erreur de transmission. On peut aussi envisager une vengeance d’un opérateur.
* Le stockage des réponses sont enregistrées sur plusieurs serveur de BDD redondants et un serveur de fichiers pour les enregistrements audio hébergées par CENTRECALL donc si il y a un problème de sécurité, toutes les données peuvent être récupérées.
* Appel par téléphone IP, peut-être écouté à la suite d’un piratage du poste.

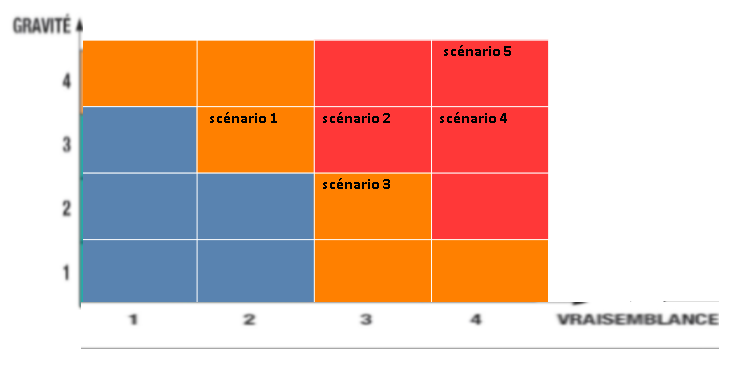
**Question 2**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Source de menace | Type de menace | Bien support | Niveau de vraisemblance | Critère de sécurité | | |
| Confidentialité | Disponibilité | Intégrité |
| Scénario de menace lié au risque 1 : Attaquant extérieur | Espionnage | Ordinateur de l’opérateur | 2 - Limité  (Les données ne sont présentes que sur le serveur de base de données) | L’authentification n’est plus assurée aux seules personnes habilitées |  |  |
| Scénario de menace lié au risque 2 : Salarié mécontent | Espionnage | Ordinateur de l’opérateur,  Accès aux bases de données et aux 3 pôles | 3 – Importante  L’authentification n’est plus assurée aux seules personnes habilitées, vol de données, transmission à une entreprise concurrente |  | Les données ne seront plus disponibles suite à un de ces actes |  |
| Scénario de menace lié au risque 3, consultation de données par utilisateur non-habilité | Espionnage | Ordinateur d’un des utilisateurs | 2-Limité  Périmètre habilitations restreint | L’authentification n’est plus assurée aux seules personnes habilitées |  |  |
| Scénario de menace lié au risque 4,  Altération base de données par attaque extérieur | Attaque | Serveur de BDD | 3 – Importante  Risque de pertes de données ou falsification |  |  | Crédibilités de l’entreprise pour les futurs collectes de données |
| Scénario de menace lié au risque 5, Arrêt du serveur suite attaque | Attaque | Serveur de BDD | 4 - Maximal |  | Les données ne seront plus disponibles à la suite de l’attaque | Crédibilités de l’entreprise mise à mal |

**Question 3**

|  |  |  |
| --- | --- | --- |
| **Exemple scénario 1** | **Usurpation d’identité** | **Niveau de gravité : 3 (important)**  **Les données confidentielles peuvent être exploitées par une entité malveillante** |
| **Exemple scénario 2** | **Suppression ou vol de données** | **Niveau de gravité : 3 (important)**  **Les données ne seront plus disponibles et l’entreprise perd en crédibilités** |
| **Exemple scénario 3** | **Consultation par un employé non-habilité** | **Niveau de gravité : 2 (limités)**  **Les données confidentielles peuvent être exploitées ou simplement consultés** |
| **Exemple scénario 4** | **Altération de bases de données** | **Niveau de gravité : 4 (maximal)**  **Perte de données et crédibilités** |
| **Exemple scénario 5** | **Attaque (DDOS ?)** | **Niveau de gravité : 4 (maximal)**  **Arrêt des services et perte de données** |

**Question 4**

****

**Question 5**

**Note de synthèse pour Mme AZRI :**

**Nous avons identifié 5 risques avec des plusieurs niveaux de gravités :**

**RISQUE 1 : Usurpation d’identité**

**C’est un risque tolérable sous contrôle.**

**Il faudra tout de même renforcer les mesures d’authentifications des opérateurs, en changeant régulièrement leurs moyens de connexions aux différents services de CenterCall pour éviter une récupération d’un mot de passe lors d’une opération de maintenance. On pourrait envisager une connexion par clefs ou carte privées.**

**RISQUE 2 : Suppression ou vol de données**

**C’est un risque inacceptable et qui doit être résolu très rapidement.**

**Il faut renforcer la surveillance et l’accès des employés en faisant attention aux données qu’ils peuvent récupérer. Mettre éventuellement une double sécurité entre l’employé et un superviseur pour le téléchargement de données ainsi que des logs toutes les heures pour vérifier les actions menées.**

**RISQUE 3 : Consultation par un employé non-habilité**

**C’est un risque tolérable sous contrôle.**

**Dans la mesure où la politique de sécurité mise en place est importante, car les habilitations de chaque utilisateur sont restreint, il suffit de maintenir un contrôle sur les moyens de connexions ainsi que les droits d’utilisation. La mise en plus d’une double authentification mentionnée plus haut peu également résoudre ce risque.**

**RISQUE 4 : Altération de bases de données**

**C’est un risque inacceptable et qui doit être résolu très rapidement.**

**Il faut renforcer les protections contre les attaques extérieures à l’organisation. Mettre en place des sauvegardes locales et externe réseau en plus de sauvegarde réseaux. Il faut mettre en place d’une surveillance constante des informations et leurs intégrités pour éviter une falsifications des données.**

**RISQUE 5 : Attaque (DDOS ?)**

**C’est un risque inacceptable et qui doit être résolu très rapidement.**

**Il faut mettre en place plusieurs mesures.**

**Avoir une architecture composée de plusieurs serveurs offrant le même service au client afin de répartir les points d’accès aux services et offres. En cas d’attaque, les clients subissent un ralentissement, plus acceptable qu’un arrêt de service.**

**Mettre en place un serveur tampon, appelé « cleaning center » pour filtrer et nettoyer le trafic de manière à ce que les menaces n’affectent pas le serveur.**

**(source trouvée sur le net pour la question 5, comment se protéger d’une attaque DDOS)**