Cybersécurité

MOURANCHON Mattéo
SIO 1

1)

Les risques de vulnérabilité peuvent survenir aux données à titre de donnée personnelle, en particulier :

– Trop de collecte en grande quantité
– Donnés collectés pas assez protéger
– Les données enregistrées il y a 1 ans peuvent être compromise à la sécurité

-Trop de membre qui ont accès aux données
-risque de surveillance des données insuffisante

2)

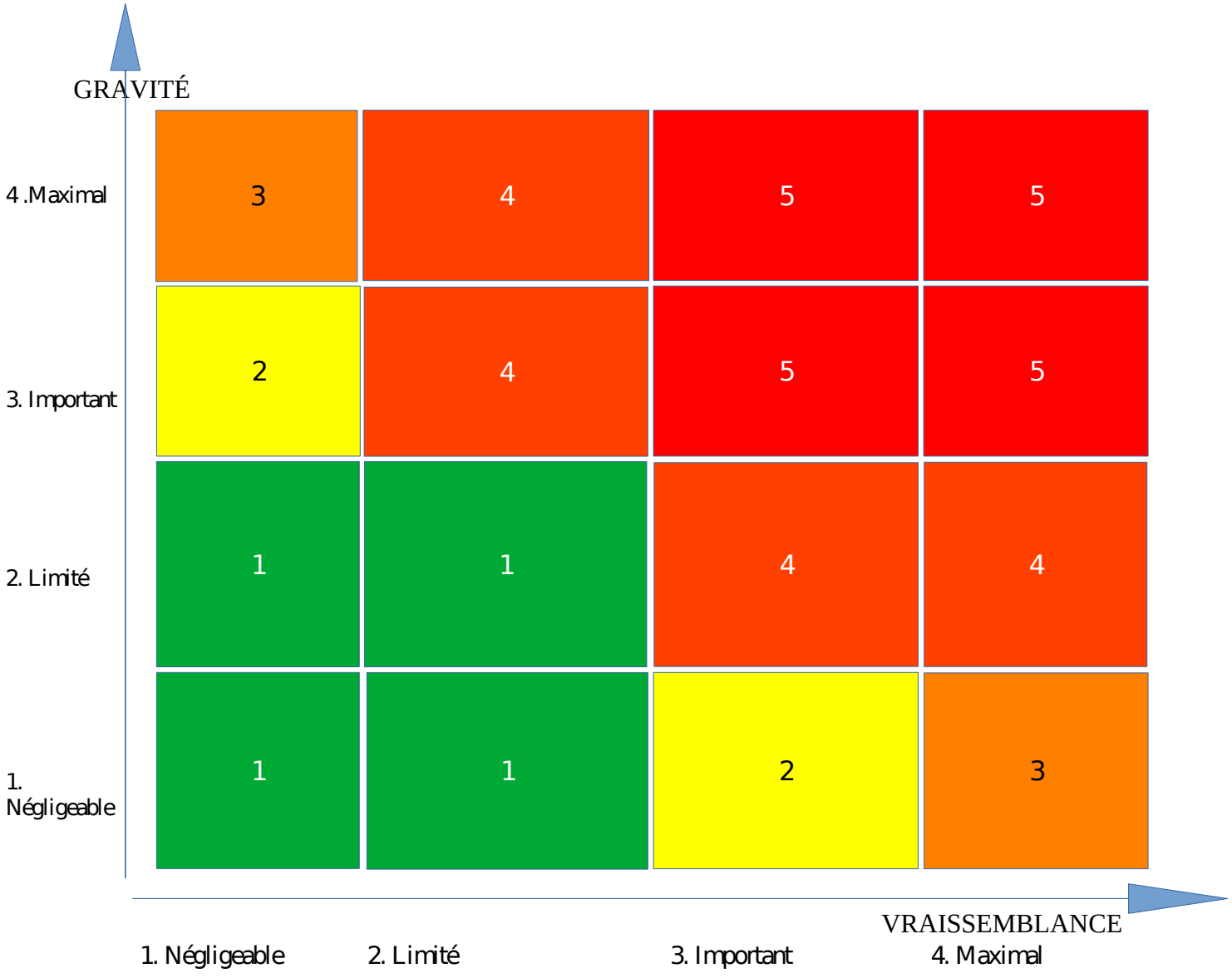
Source de menace	Type de menace	Bien support	Niveau de vraisemblance	Confidentialité	Disponibilité	Intégralité
Scénario de menace lié au risque 1 : attaquant extérieur	Espionnage	Ordinateur de l'opérateur	2 : limité (les données ne sont présentes que sur le serveur de base de données	L'authentification n'est pas aux seules personnes habilitées.		
Scénario de menace lié risque 2 : Salarié malveillant	Malveillance interne	Base de données	4 : Maximal (action facile à exécuter et grave conséquence)	Le salarié peut copier ou effacer les données sensibles facilement		Objectif est de nuire à call center
Scénario de menace lié risque 3 : Consultation par un employé non habilité	Accès non autorisé aux données	Base de données	2 : limite (accès non autorisé à une base de données, habilité insuffisante)	L'employé consulter des infos qu'il ne devrait pas voir et sans autorisation		
Scénario de menace lié risque 4 : Altération des données par un attaquant	Sabotage/ attaque extérieur	Base de données	1 : négligeable (Les données changées faussent toute l'étude)			Conséquence sur la crédibilité des futures synthèses d'études de marché
Scénario de menace lié risque 5 : Arrêt du serveur de la base de données	Déni de service (DDoS)	Serveur base de données	4 : Maximal (attaque extérieur dans le but de DDoS le serveur de Call Center		Les opérateurs de call Center ont besoin de l'accès au serveur pour travailler	

3)

Scénario 1	Usurpation d’identité	Niveau de gravité : 3 (important) Les données confidentielles peuvent être exploitées par une entité malveillante
Scénario 2	Suppression ou vol de données par un salarié malveillant	4 (maximal) Le salarié peut supprimer les données dans la base de données sans problème
Scénario 3	Consultation non autoriser par un employé avec l’habilité insuffisante	2 (limite) Accès et consultation d’un dossier non autoriser par l’employer
Scénario 4	Altération des données par une attaque extérieure dans la base de données	3 (important) Sabotage des données pour l’étude de marché
Scénario 5	Arrêt des serveurs par une attaque extérieure	4 (maximal) Attaques des serveurs par déni de DDoS

4)
Les risques principaux liés au traitement des données sont l'usurpation de compte, la suppression ou le vol de données par un salarié, la consultation par un employé non habilité, l'altération des données et l'arrêt du serveur par une attaque externe. Les plus graves concernent le vol interne et l'arrêt du serveur, car ils peuvent entraîner une fuite massive d'informations ou une indisponibilité totale du service. Pour réduire ces risques, il est conseillé de sécuriser les serveurs, de limiter les accès aux seules personnes autorisées, de chiffrer les données, de réaliser des sauvegardes régulières et de sensibiliser les employés à la protection des informations.

CARTOGRAPHIE DES RISQUES



5)

A l’attention de Mme Azri

L’analyse montre 5 risques : usurpation de compte, vol ou suppression de données, consultation non autorisée, altération, sabotage ou arrêt des serveurs.
Les plus graves sont le vol interne et l’arrêt des serveurs, parce qu’ils entraînent une fuite de données ou une indisponibilité total pour le service.
L’usurpation et l’altération ont aussi eu un impact majeur en cause des consultations non autorisée due aux habilitations insuffisantes, qui reste limite.

Pour réduire ces risques ou plutôt les menace, voici des suggestions :

– Sécuriser les serveurs
– Limiter les accès plus stricts
– Sensibiliser les employés
– chiffrer les données
– Sauvegarder régulièrement