Connaître les techniques de gestion de la sécurité d'une base de données

**I. Partie sécurité**

**Identifiez les comptes d’utilisateur et Réexaminez régulièrement les droits d’accès.**

Les droits (appelés "**privilèges**") sont accordés à : Un utilisateur ou groupe d'utilisateur

**Les "privilèges" concernent :** Le créateur d'un schéma possède tous les privilèges pour ce schéma. L'utilisateur est identifié lors de sa connexion au serveur. Des privilèges pourront être accordé à un module (programme d'application, session interactive, code SQL incorporé dans un texte du langage hôte, fonction ou procédure stockée) ou à un ensemble d'utilisateurs. Une transaction ne peut être exécutée que si toutes les opérations possèdent les privilèges requis

**Établir et maintenir un modèle d’accès basé sur le principe du moindre privilège.**

A fait de réduire les dommages qu’un utilisateur peut causer délibérément ou accidentellement, si un attaquant prend le contrôle d’un compte d’utilisateur le dommage sera aussi réduit.

**Analysez notre environnement à la recherche de fichiers potentiellement nuisibles.** Recherchez régulièrement les exécutables, les programmes d’installation et les scripts, et supprimer ces fichiers afin que personne ne puisse accidentellement ouvrir des fichiers contenant des rançongiciels ou d’autres logiciels malveillants. (Il excite plusieurs antivirus qui peuvent scanner les serveurs, comme *Kaspersky Endpoint Security.*

# Avec du monitoring : **Recherchez les pics suspects d’activité.** **Recherchez les activités en dehors des heures de travail.**

# ****II. Partie Sauvegarde****

# Nous pouvons compter sur différents types de backup pour construire notre stratégie de sauvegarde.

## Les types de backups sont :

**Base de données complète**ou backup full. Ce type de backup inclut tous les objets de la base de données, les tables systèmes, les données, et les transactions qui ont eu lieu pendant le backup. Les backups full permettent une restauration complète d’une base de données à l’état où elle se trouvait avant le backup

**Backup différentiel**. Ce type de backups contient seulement les données qui ont changé depuis le dernier backup full ainsi que les transactions qui ont eu lieu pendant le processus de sauvegarde. Un backup différentiel est utilisé avec le dernier backup full effectué sur la base de données. Les backups différentiels pris antérieurement au dernier backup différentiel, mais consécutifs à un même backup full, peuvent être considérés comme obsolètes car ce dernier backup différentiel contient toutes les modifications effectuées sur la base de données depuis le dernier backup full et de facto l’ensemble des informations reprises dans les backups différentiels antérieurs.

**Backup du journal des transactions** (transaction log) ou backup log. Ce type de backup contient l’ensemble des transactions effectuées pour une base de données depuis le backup log précédent et tronque le contenu du transaction log. Un **backup log** permet d’assurer la restauration d’une base de données à un moment spécifique comme par exemple, le moment avant la perte d’une donnée.

**Backup de fichier ou de groupement de fichiers**. Cette option convient principalement pour la sauvegarde de bases de données de taille importante. Un backup de fichier contiendra toutes les données d’un ou plusieurs fichiers ou d’un groupement de fichiers. Un **backup log** doit également être effectué pour couvrir tous les backups de ce type en cas de restauration où les sauvegardes de l’ensemble des fichiers, prises à des moments différents, doivent être utilisées

**Backups copie seule** ou backups copy-only. C’est le type de backup le plus utilisé pour effectuer une sauvegarde sans affecter le plan de sauvegarde mis en place pour une base de données. On peut créer des backups full et des backups log de ce type. Ainsi, un backup full copy-only est fonctionnellement équivalent à un backup full. Cependant, un backup log copy-only contiendra toutes les transactions effectuées depuis le dernier backup full, ce qui signifie qu’un backup full copy-only est ignoré pour la prise d’un backup log copy-only.

## J’opte pour une stratégie de **Backup différentiel, avec une planifier des backups** à l’aide d’un système de planification*. ( par ex : avec un job SQL Server Agent ou autre tout dépend de l’hébergeur)*

Il est conseillé que les sauvegardes **(backups)** ne soient pas effectuées au même endroit (même disque physique) que celui où se trouvent les bases de données. Ainsi, lorsqu’un disque physique qui contient des bases de données est en panne, nous pouvons utiliser l’autre disque ou le partage réseau utilisé pour restaurer les bases de données perdues.

**En conclusion, Les stratégies de sauvegarde et restauration ne peuvent être complètes si les sauvegardes qui sont prises ne peuvent être restaurées avec succès sur un serveur de test et que nous nous sommes assurés que les backups que nous prenons permettent de remplir toutes les exigences et toutes les conditions pour toutes les combinaisons définies dans nos stratégies de restauration. Il y a plusieurs facteurs qui entrent en ligne de compte la politique de la société ainsi que le budget alloué.**