Considérations relatives à la sécurité des données, à l'éthique et à la conformité

En tant qu'administrateur de base de données (DBA), l'une des tâches les plus importantes de votre rôle consiste à protéger les données du système. Vous contrôlez le système, vous êtes donc responsable de la sécurité des données et de leur conformité à toutes les normes en vigueur. Vous devez également vous conformer aux normes éthiques les plus strictes. Certaines organisations incluent un rôle spécifique d'administrateur de sécurité de base de données qui se concentre sur ces tâches, mais tous les administrateurs de base de données doivent les garder à l'esprit.

::page{title=”Éthique fondamentale”}

Une base de concepts éthiques de base permet de soutenir de bonnes pratiques en matière de sécurité des données. Ces concepts devraient vous aider à orienter les politiques et les flux de travail que vous créez ainsi que les actions que vous entreprenez. Voici quelques concepts importants :

- **Transparence** : Lorsque vous collectez des informations, vous devez indiquer aux propriétaires de ces informations exactement quelles données vous allez collecter et ce que vous en ferez. Expliquez-leur comment vous utilisez les données, comment vous les stockez, qui y aura accès et comment vous les éliminerez une fois que vous aurez fini de les utiliser.
- **Consentement** : Vous devez obtenir le consentement explicite des propriétaires de données avant de collecter leurs données. Ce consentement doit détailler les données que vous serez autorisé à collecter et la manière dont vous serez autorisé à les utiliser.
- **Intégrité** : Soyez toujours clair sur vos procédures et politiques et suivez-les toujours de manière cohérente. Dans la mesure du possible, assurez-vous que les autres membres de votre organisation suivent également les procédures et politiques appropriées.

Envisagez de créer un code d’éthique, c’est-à-dire une déclaration écrite des normes et des intentions liées à la sécurité. Vous pouvez y inclure les priorités, les meilleures pratiques, les personnes responsables et tout ce qui est important à comprendre clairement. Cela créera des attentes communes pour vous-même et pour les autres, ce qui contribuera à instaurer la confiance et permettra à chacun de suivre plus facilement les procédures correctes.

Conception de systèmes sécurisés

La structure de votre système est un outil puissant pour protéger vos données. Si votre système est conçu pour maintenir la sécurité, il est beaucoup plus facile d'empêcher les violations. Pour vous assurer que votre système fonctionne pour vous, tenez compte des facteurs suivants.

- **Protection contre les accès malveillants** : la première ligne de protection de vos données est la sécurité logicielle de base. Votre pare-feu et vos autres outils de cybersécurité doivent empêcher activement le piratage et l'installation de logiciels malveillants, et vous alerter des menaces. Veillez à mettre à jour régulièrement ces logiciels pour que les listes d'analyse soient à jour. Informez également les utilisateurs sur le phishing et les autres moyens par lesquels ils peuvent permettre involontairement un accès malveillant.
- **Stockage sécurisé** : Le stockage que vous choisissez pour vos données doit être sécurisé non seulement contre les accès malveillants, mais aussi contre les pannes matérielles et même les catastrophes naturelles. Sélectionnez soigneusement vos services et assurez-vous de bien comprendre leurs pratiques de sécurité et leurs plans de préparation aux catastrophes. Sauvegardez vos données régulièrement et de manière fiable pour minimiser la perte de données en cas d'urgence.
- **Accès précis** : seules les personnes ayant besoin de certaines données doivent pouvoir y accéder. Établissez un système d'attribution et de suivi des privilèges qui attribue à chaque utilisateur uniquement les privilèges nécessaires et contrôle ce qu'il peut faire avec les données. Assurez-vous que votre politique est conforme à tous les accords d'utilisation des données que vous avez conclus.

- **Déplacement sécurisé** : les données peuvent être particulièrement vulnérables à l'interception lorsque vous les déplacez vers ou hors du stockage. Assurez-vous de considérer les méthodes de transfert sécurisées avec autant de soin que vous planifiez la sécurité du reste de votre système.
- **Archivage sécurisé** : À un moment donné, vous souhaiterez peut-être déplacer des données d'un stockage actif vers une archive. Cela peut les protéger contre tout accès accidentel et rendre votre système plus efficace. Assurez-vous que votre système d'archivage est aussi sécurisé que le reste de votre stockage. Les accords de données précisent souvent la durée pendant laquelle vous pouvez utiliser les données. Assurez-vous donc que les données archivées sont régulièrement éliminées pour les droits expirés et ne conservez pas plus de données que nécessaire pour respecter la politique de l'organisation. Éliminez vos données supprimées de manière sûre et complète.

Problèmes de conformité

Il est essentiel de se conformer à toutes les lois et normes en vigueur. Tout manquement peut entraîner une insécurité des données, une censure professionnelle pour votre organisation et même des poursuites judiciaires. Cette liste comprend certains des types de normes les plus courants, mais elle n'est pas exhaustive. Renseignez-vous toujours sur les réglementations et les normes qui s'appliquent à votre organisation.

- **Réglementations nationales/internationales** : De nombreux secteurs doivent se conformer à des normes juridiques importantes au niveau national ou international. Citons par exemple la réglementation HIPAA relative aux informations relatives à la santé aux États-Unis, le RGPD en Europe et la loi sur les technologies de l'information de 2000 en Inde.
- **Normes sectorielles** : certaines normes de données ne sont pas imposées par la loi, mais peuvent néanmoins avoir des répercussions sur la réputation et la réputation de votre organisation si elles ne sont pas respectées. Citons par exemple la norme de sécurité des données du secteur des cartes de paiement (PCI DSS), qui s'applique à toute organisation qui collecte, stocke ou transmet des données de titulaires de carte.
- **Bonnes pratiques organisationnelles** : chaque organisation formulera des normes pour la gestion de ses données internes. En tant qu'administrateur de base de données, vous pouvez travailler sur ce sujet dans le cadre de votre travail. La confidentialité des employés est souvent un élément important de ces politiques, tout comme la protection de la propriété intellectuelle détenue par l'organisation.

Si vous construisez votre système et vos procédures de manière réfléchie et que vous les maintenez avec cohérence et vigilance, vous pouvez garantir la sécurité et la productivité des données de votre système.