La sécurité des bases de données

Par 29a.ca

Sécurité des bases de données : parce que ton mot de passe mérite mieux qu'un champ VARCHAR (20). Ou comment éviter que ta base devienne un buffet à volonté pour hackers affamés.

Ah, les bases de données. Ces petits coffres-forts numériques qui contiennent **tes clients**, **tes mots de passe**, **ta facturation**, et parfois... **la recette secrète de ta sauce à spag**.

Mais attention. Mal protégée, ta base peut vite passer de "système robuste" à "passoire en ligne".

Et deviens un classique du genre : *"1 million de comptes exposés suite à une mauvaise configuration MongoDB."*. (Oui, c'est déjà arrivé. Plein de fois. 😅 à beaucoup d'entreprises)

📚 Que contient une base de données typique?

- Des **infos sensibles** : noms, courriels, mots de passe (parfois en clair, oups);
- Des **données métiers** : stocks, ventes, plans secrets de domination mondiale;
- Des **choses que personne n'aurait dû écrire là** : genre "Mon oncle Paul est nul en *Excel*" dans un champ "commentaires internes".

Bref, c'est un festin de données. Et les hackers ? Ils **ont faim**.

💀 Les pires erreurs (vues dans la nature...)

1. Mot de passe admin : "admin"

C'est presque de la poésie. Minimaliste. Aussi efficace qu'un cadenas en sucre sur une valise une trottinette à 3 000$.

2. Aucune restriction IP

Accès à distance ouvert à *tout l'internet*. Autant dire : "Bonjour, ceci est ma base. Servez-vous, c'est open bar."

3. Pas de chiffrement

Tout en clair. Comme un journal intime laissé sur le banc d'un parc, avec une flèche qui dit "Lisez à partir de la page 5".

4. Injection SQL? Bah, c'est vintage et avec les *framework* je suis protégé (il n'y a pas plus faux) !

Et pourtant, encore en 2025, beaucoup de sites sont vulnérables à

```
' OR 1=1 --
```

🧠 Bonnes pratiques (avec humour, mais sérieux quand même)

✅ 1. Mots de passe forts et hashés

- Stocke-les **hashés avec un sel**;
- PAS de MD5. Pas de SHA1;
- Utilise **bcrypt**, **argon2**, ou mieux : demande à un expert de sécurité… ou à ta cafetière connectée, si elle a un bon *firewall*.

✅ 2. Moins de privilèges, plus de paix

- Donne à chaque utilisateur *le strict minimum de permissions*. Ta fonction de facturation n'a pas besoin de DROP DATABASE.

✅ 3. Chiffre les données sensibles

- Même dans la base. Parce qu'un admin malveillant, ça existe. Oui, même Kevin du support IT.

✅ 4. Sauvegardes chiffrées et isolées

- Et surtout pas sur le même serveur que la base. Sinon, c'est comme cacher la clé du coffre **dans le coffre**.

✅ 5. Logs + surveillance + alertes

- Utilise un SIEM ou au minimum un outil d'audit. Tu veux savoir si quelqu'un télécharge *toute* ta base à 2 h du matin… surtout s'il s'appelle "anonymous_user".

🧘 En résumé :

Les bases de données sont précieuses mais entre de mauvaises mains, elles deviennent :

- Un jackpot pour les pirates;
- Une enquête pour les journalistes;
- Un cauchemar pour ton département légal

Alors sécurise-les. Et rappelle-toi :

Une base bien protégée dort la nuit. Une base mal protégée se réveille sur *HavelBeenPwned*.
