Le Pharmacien de France
en partenariat avec
Caduciel informatique
www.caduciel.com

Nos conseils pour sécuriser vos données, éviter les piratages et prévenir les bugs informatiques.

Travailler en toute sécurité

© Miguel Medina

La sécurité informatique est un élément essentiel au bon fonctionnement de votre officine. Elle a pour but de prévenir les conséquences d'une panne matérielle mais aussi d'éviter toute perte ou utilisation frauduleuse des données.

La mise en œuvre d'une bonne politique de sécurité informatique à l'officine passe par :

- l'identification et l'analyse des risques encourus,
- la mise en adéquation des moyens et des dispositifs visant à sécuriser l'exploitation de l'officine, en fonction de la probabilité que le problème se produise et des dommages encourus.

Elle doit, au minimum, intégrer :

- l'environnement « applicatif », le risque majeur étant la perte ou l'utilisation frauduleuse des données de l'officine (vol ou incendie, utilisateur malveillant, accès aux données depuis Internet, etc.),
- l'environnement « physique », le risque majeur étant une panne matérielle (alimentation, disque dur, serveur....) pouvant entraîner la perte d'utilisation partielle ou totale de l'informatique officinale.

Voici quelques exemples de solutions de sécurité préconisées en fonction de l'environnement et du risque encouru. Celles-ci pourront vous servir de référence pour bâtir votre propre politique de sécurité interne, qui dépend de la configuration de votre officine.

Risques liés à l'environnement « applicatif »

« Crash » de votre base de données
Quelles solutions ?

- Sauvegarde régulière sur des supports amovibles (disque dur externe, clé USB...).
- Réplication de la base de données sur différents PC.

Accès à vos données depuis Internet
Quelles solutions ?

- Firewall physique au travers de matériel spécifique ou de votre routeur de connexion ADSL (attention : le firewall doit être systématiquement accompagné de la mise en place d'une solution antivirus).
- Solution de connexion sécurisée type VPN (Virtual Private Network) avec cryptage et authentification forte pour les utilisateurs nomades.

Incendie, vol de matériel, inondation, etc.
Quelles solutions ?

- Sauvegarde de vos données essentielles sur un support amovible transportable (petit disque dur, etc.).
- Sauvegarde à distance et automatique de vos données sensibles (envoi des données sur un serveur distant par liaison ADSL).

Utilisateur malveillant
Quelle solution ?

Controle d'accès des utilisateurs et restriction des droits d'accès aux fonctionnalités du logiciel par la mise en place de solution d'authentification et d'identification (mot de passe, capteur d'empreinte digitale, lecteur de badge, etc.).

Risques liés à l'environnement « physique »

Panne du serveur dédié
Quelles solutions ?

- Disques durs montés en technologie RAID (Redundant Array of Independent Discs : permet une duplication des données sur un ou plusieurs disques).
- Double alimentation électrique.
- Double serveur (pour éviter les conséquences d'un problème sur la carte mère).
- Architecture en "peer-to-peer" (de poste à poste, sans serveur dédié) ou chaque poste est autonome (division du risque).

Panne du disque dur
Quelles solutions ?

- Disques durs montés en technologie RAID, SATA (Serial Advence Technology Attachent : protocole d'échange).
- Applicatif permettant de répliquer les données sur un autre poste en temps réel.

Perte de connexion Internet (plus de commandes, plus de tiers payants, plus de mises à jour, plus de télémaintenance, plus d'accès aux applications ASP (Active Server Pages)...)
Quelles solutions ?

- Redondance de la liaison par l'utilisation d'un modem RTC.
- Redondance de la liaison ADSL.

Rupture réseau
Quelles solutions ?

- Eviter le matériel « tout en un » (ex : routeur + swich pour répartir les connexions réseau).
- Matériels de rechange (duplication carte réseau, switch, etc.).

Problème d'alimentation électrique
Quelle solution ?

- Mise en place d'onduleur pour éviter les problèmes liés au secteur (central ou individuel).

Une politique de sécurité reste efficace à la condition d'un suivi régulier réalisé par le biais de mises à jour (base antivirus, système d'exploitation, etc.) et de vérification maintenance des matériels.

Claire Grevot