Nouvelles technologies

avec Caduciel informatique en partenariat avec Le Pharmacien de France

Pour protéger efficacement l'informatique de votre officine, vous devez agir sur plusieurs composantes.

La sécurité informatique en pharmacie

La sécurité du réseau informatique de votre officine est un tout formé de plusieurs composantes. Que penseriez-vous d'une maison protégée par une porte blindée, des barreaux aux fenêtres, et dont la petite porte de derrière resterait ouverte en permanence ? Il en est de même pour votre réseau informatique.

Les 5 règles d'or de la sécurité informatique en officine :

1. Utiliser un logiciel antivirus mis à jour régulièrement et automatiquement.
2. Installer un Firewall avec mise à jour des règles de sécurité.
3. Mettre à jour votre système d'exploitation pour éviter les failles de sécurité.
4. Sauvegarder sur support externe (copies de secours des données importantes).
5. Gérer les contrôles d'accès.

La protection contre les attaques externes.

A l'heure des réseaux et des connexions haut débit, la sécurité informatique de votre officine constitue un enjeu important. Plusieurs centaines de nouveaux virus apparaissent chaque mois et beaucoup d'emails échangés en contiennent. Les actes de piratage sont de plus en plus fréquents et les dégâts causés coûtent de plus en plus chers. Imaginez qu'un programme malveillant (virus, trojans, vers...) ou qu'un hacker (pirate informatique) accède à vos fichiers personnels, aux données de vos clients, à l'ensemble de vos écritures comptables ; rien ne l'empêcherait de détourner, de modifier ou bien d'effacer l'ensemble de vos fichiers...

Aujourd'hui les protections contre ce type de malveillance sont au minimum : le Firewall, l'Antivirus et l'Antispyware.

• Qu'est-ce qu'un Firewall ?

Un firewall, également appelé pare-feu, est un dispositif matériel ou logiciel interdisant certains trafics Internet malveillants. Un virus informatique est un programme capable de se reproduire et qui, une fois activé, est destiné à endommager les données. Un vers (ou Worm) est quant à lui un code malicieux qui utilise les failles de sécurité ainsi que les technologies de messagerie pour se propager plus rapidement.

Le firewall est le moyen le plus efficace pour maîtriser ce qui rentre et sort de votre ordinateur (couches 3, 4 et 7 du modèle OSI).

• Qu'est-ce qu'un Antivirus ?

Le logiciel antivirus est le complément idéal du firewall. Il est le "gardien" de votre ordinateur et de son contenu. Pour être efficace, votre logiciel anti-virus doit être tenu à jour très régulièrement. Sans mise à jour, votre logiciel antivirus ne pourra pas détecter et désinfecter votre poste des dernières générations de virus connus. Il doit également comporter un module résident, pour pouvoir surveiller l'activité de l'ordinateur pendant que vous travaillez.

• Qu'est-ce qu'un Antispyware ?

Le logiciel Antispyware permet de détecter et d'éradiquer ces programmes malicieux dont le pouvoir de nuisance est très important. Spyware ou trojan (chevaux de Troie) sont des logiciels espions qui réalisent diverses opérations sur l'ordinateur infecté, à l'insu de l'utilisateur. Ils peuvent détruire vos données sur le disque dur, voler vos informations confidentielles et aller jusqu'au "crash" de votre système.

En ayant une mise à jour régulière et automatique de votre solution de sécurité, comme celle proposée par Caduciel Informatique (voir schéma), vos données seront bien protégées.

La protection de votre réseau informatique en cas de panne

La perte de vos données causée par une panne de votre système est toute aussi importante. Pour ce faire, une architecture de type NSPOF (No Single Point Of Failure) évite de laisser un seul point critique au sein de votre système informatique. Il permet ainsi de maintenir votre activité même si votre système rencontre une panne. Afin d'augmenter la sécurité et de fiabiliser votre solution, l'utilisation de deux cartes réseau, d'une base de donnée répliquée et synchronisée, d'un montage de disques durs en RAID (Redundant Array of Inexpensive Disks) sont des techniques professionnelles efficaces. Le système possède alors une grande tolérance aux pannes, principe dit "de haute disponibilité". Les sauvegardes externes restent également des moyens efficaces avec toutefois des temps de restauration plus longs.

L'utilisateur, facteur déterminant dans une politique de sécurité...

L'utilisateur est un acteur important de la sécurité. Le facteur humain est même déterminant dans une politique de sécurité. En effet, il accède à l'ensemble des informations de l'officine sans restriction. Il peut décider ou non de tenir compte des alertes ou des informations du système informatique. Un système de contrôle d'accès avec une authentification et une identification de l'utilisateur par un mot de passe ou par reconnaissance d'une empreinte digitale permet de réserver l'accès aux postes informatiques et à leurs logiciels uniquement aux personnes habilitées.

La sécurité absolue n'existe pas ! Cependant pour faire face à ces risques et à leurs conséquences, quelques règles d'or s'imposent, aujourd'hui mises en place par Caduciel au travers de ses solutions informatiques.

Un exemple de réseau informatique officinal bien protégé.