DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Cybersécurité au cabinet

Se protéger contre le piratage informatique

Alors que plusieurs cabinets médicaux romands ont été pris pour cible par des logiciels de rançon en mars dernier, la Société Vaudoise de Médecine recommande l'application de 9 mesures concrètes aux médecins soucieux-ses de se prémunir au mieux contre toute attaque informatique.

Publication d'informations privées liées aux patient-es, atteinte au bon fonctionnement du cabinet et à sa réputation, les risques que représente une cyberattaque pour les structures médicales sont multiples et potentiellement lourds de conséquences. Or, comme le rappelle la FMH,

> chaque cabinet médical est chargé de garantir la protection et la sécurité des données qu'il traite [1].

S'il n'existe pas de protection parfaite face aux pirates informatiques, il est possible de leur compliquer sensiblement la tâche en appliquant quelques principes simples, exposés ci-dessous. Nous vous recommandons de faire appel à votre prestataire informatique qui pourra personnaliser ses conseils selon les spécificités de votre infrastructure.

9 conseils pour renforcer son « immunité » informatique

1. **Installer un antivirus ou un pare-feu** (dispositif de sécurité qui surveille le trafic entrant et sortant de votre réseau) **sur tous ses appareils** et effectuer les mises à jour dès leur parution (si possible de manière automatique) afin de pallier au plus vite les fragilités du système.

2. **Sauvegarder régulièrement ses données** sur un dispositif « hors-ligne » (comme un disque dur portable) et un dispositif « hors site » (par exemple un disque dur externe stocké en dehors des locaux ou une solution « Cloud », c'est-à-dire de stockage en ligne) pour disposer de deux copies en cas d'attaque. Tester au minimum 1 à 2 fois par an la fonctionnalité du système en procédant à des restaurations.

3. **Effectuer les mises à jour du système et des logiciels** présents sur ses ordinateurs.

4. **Utiliser des mots de passe sûrs**, différents pour chaque compte, d'au moins 12 caractères incluant majuscules, minuscules, chiffres et caractères spéciaux pour éviter de donner accès à toutes vos interfaces aux hackeur-ses. Avoir recours à un **gestionnaire de mot de passe** peut s'avérer utile. Procéder à une

authentification à deux facteurs (double vérification de l'identité, par ex. via un mot de passe et un code reçu ensuite par SMS ou sur une application mobile dédiée) permet encore de réduire les risques d'intrusion.

5. **Se méfier des courriels d'expéditeurs/trices inconnu-es** et ne jamais cliquer sur une pièce jointe ou un lien y relatif. Ne jamais transmettre de noms d'utilisateur/trice ou de mots de passe par e-mail ou téléphone et **sensibiliser ses employé-es** aux dangers encourus.

6. **Vérifier que ses disques durs soient chiffrés** (codage informatique empêchant la lecture des données à quiconque ne possède pas la clé de déchiffrement) par le système d'exploitation utilisé et/ou demander à son informaticien-ne.

7. **Envisager d'éteindre son serveur** durant les périodes d'inactivité pour réduire le temps d'exposition aux tentatives de hacking (à effectuer en collaboration avec votre informaticien-ne).

8. **Se renseigner sur les conditions de souscription à une cyberassurance** pour bénéficier d'une couverture en cas de dommages causés au cabinet ou à des tiers (perte de données, responsabilité civile, etc.). A noter que le paiement des rançons n'est pas toujours inclus.

9. **Vérifier la fiabilité des connexions à distance** établies dans le cadre du télétravail.