DOSSIER ÉLECTRONIQUE DU PATIENT ET SÉCURITÉ DES DONNÉES AU CABINET MÉDICAL

Caroline Gallois-Viñas, responsable de la cellule Cybersanté, directrice opérationnelle de la Structure Porteuse DEP Neuchâtel

Les informations médicales des patients étant des données sensibles et confidentielles, il est essentiel de mettre en place des mesures visant à assurer une protection optimale et garantir leur intégrité.

Ces dernières années, le nombre de cyberattaques a augmenté en Suisse et les cabinets médicaux sont de plus en plus pris pour cible, avec pour exemple malheureux le piratage de certains cabinets médicaux de la Chaux-de-Fonds en mars 2022.

Les principaux types de cyberattaques observés sont :

PHISHING : Les attaquants créent des e-mails, des messages texte ou des sites Web qui semblent légitimes pour inciter les destinataires à divulguer des informations sensibles telles que des mots de passe, des numéros de carte de crédit, des informations bancaires, etc.

RANSOMWARE : Il s'agit d'une forme d'attaque où des logiciels malveillants chiffrent les fichiers d'un système ou d'un réseau, puis demandent une rançon en échange de la clé de déchiffrement. Les victimes sont souvent confrontées à des menaces de suppression définitive et/ou de publication sur le Dark Web de leurs données si la rançon n'est pas payée. Il n'y cependant aucune garantie que les pirates disposent effectivement de la clé de déchiffrement.

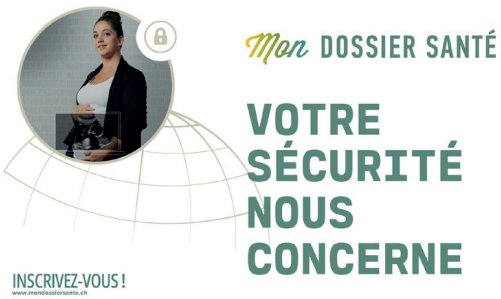
MALWARE (logiciels malveillants) : Le terme «malware» englobe divers types de logiciels malveillants tels que virus, vers, chevaux de Troie, spywares, adwares, etc., conçus pour endommager, compromettre et/ou ralentir les systèmes informatiques.

ATTAQUES PAR DÉNI DE SERVICE (DDoS) : Les attaques DDoS consistent à submerger un serveur ou un réseau avec un trafic excessif de connexions, rendant ainsi les services inaccessibles pour les utilisateurs légitimes.

Comment prévenir ces attaques en cabinet médical et assurer la sécurité des données des patients ?

- Il est tout d'abord essentiel de **former et sensibiliser** le personnel du cabinet médical aux risques et aux bonnes pratiques à respecter.
- Utiliser **un antivirus et un pare-feu**.
- **Effectuer les mises à jour et appliquer les correctifs régulièrement** pour les systèmes d'exploitation, les applications, les logiciels et les équipements réseaux, afin de corriger les vulnérabilités connues. Ce point doit faire partie du contrat que vous avez avec votre prestataire informatique.
- **Utiliser un mot de passe complexe** pour accéder à l'ordinateur et penser à verrouiller/fermer la session lorsque l'on quitte le poste de travail. Ne pas divulguer le mot de passe et ne pas le noter à un endroit facilement accessible.
- **Effectuer des sauvegardes régulières** de toutes les données médicales et stocker ces sauvegardes dans un endroit sécurisé, hors ligne (p. ex. disque dur externe).

ET LE DOSSIER ÉLECTRONIQUE DU PATIENT (DEP) DANS TOUT ÇA ? CONSTITUE-T-IL UN RISQUE POUR LA SÉCURITÉ OU AU CONTRAIRE LA RENFORCE-T-IL ?



La plateforme DEP en tant que telle est hautement sécurisée. Elle répond à la loi sur le dossier électronique du patient (LDEP) et a été certifiée par un organisme indépendant, sur la base de plus de 440 critères techniques et organisationnels.

Les principales mesures mises en place au niveau de la plateforme elle-même et de la communauté de référence sont les suivantes :

• **Authentification forte à 2 facteurs** : L'accès à la plateforme est uniquement possible pour un utilisateur détenant un Moyen d'Identification Électronique (MIE) à 2 facteurs, fourni par un éditeur certifié. Ceci s'applique aux patients, à leurs représentants, aux professionnels et auxiliaires de santé ainsi qu'aux administrateurs de Mon Dossier Santé.

Caroline Gallois-Viñas, responsable de la cellule Cybersanté, directrice opérationnelle de la Structure Porteuse DEP Neuchâtel

- **Données cryptées et stockées en Suisse** : Les données médicales des patients doivent légalement être stockées sur des serveurs installés en Suisse. C'est par conséquent la nouvelle loi fédérale sur la protection des données (nLPD) et ses ordonnances qui s'appliquent. Les données médicales sont cryptées en transit (entre les terminaux) et au repos (sur les serveurs), grâce aux dernières technologies disponibles sur le marché. De plus, les données cryptées et les clés cryptographiques sont stockées sur des environnements totalement séparés auprès du fournisseur de plateforme, qui est certifié selon la norme EN ISO/IEC 27001.

- **Tests d'intrusion** : La plateforme DEP a subi plusieurs tests d'intrusion exécutés par différents prestataires distincts avant ouverture. Le fournisseur de la plateforme mène également de nouveaux tests d'intrusion à chaque mise à jour majeure sous la forme d'un « Bug Bounty program » récompensant la découverte de bugs et/ou failles de sécurité. De plus, des tests visant à empêcher le social engineering et à mettre en application le plan de reprise d'activité sont régulièrement effectués.

- **Audits réguliers** : La communauté de référence proposant le DEP est auditée régulièrement. Un audit complet a lieu tous les 3 ans et un audit de suivi a lieu chaque année pour assurer la conformité à la LDEP. Les prestataires de soins sont également audités par échantillonnage.

La LDEP édicte également des exigences de sécurité envers les prestataires de soins et c'est en ce sens que **le DEP va permettre d'augmenter la sécurité au sein des cabinets médicaux**. Ces exigences sont les suivantes :

- **Formation** de tous les utilisateurs (professionnels et auxiliaires) au DEP et sensibilisation à la sécurité de l'information
- Utilisation d'un **antivirus** / **pare-feu avec mise à jour** régulière
- **Annonce** à la communauté de référence **en cas d'incident de sécurité** ou de départ d'un collaborateur
- **Gestion restrictive des droits administrateurs du système**
- Utilisation d'un Moyen d'Identification Électronique (**MIE**) à **2 facteurs certifié**

Pour plus d'informations sur Mon Dossier Santé, le dossier électronique du patient neuchâtelois, et les modalités d'affiliation, n'hésitez pas à consulter notre site internet https://www.mondossiersante.ch/prestataires-de-soins/.