CYBERSÉCURITÉ : UN ENJEU CRUCIAL

La cybermalveillance monte en puissance ces dernières années et concerne tous les secteurs, y compris celui de la santé. L'Ordre se mobilise pour assurer sa cybersécurité et accompagner les médecins.

Dr LEÏLA OURACI,
secrétaire générale adjointe

en collaboration avec **KEMAL OZCAN**, responsable sécurité des systèmes d'information

Au printemps dernier, le directeur adjoint de la CISA, l'équivalent américain de l'Anssi, alertait : la période est « *très inquiétante* » pour la sécurité informatique du secteur de la santé. Une situation qui nécessite une mobilisation importante. Au niveau mondial, on constate une augmentation des actes de piratage informatique de 38 % entre 2021 et 2022. En France, en trois ans, le nombre d'enquêtes ouvertes pour cyberattaque a été multiplié par 10 !

Un secteur particulièrement exposé

Concernant le secteur de la santé, la hausse des actes de piratage entre 2021 et 2022 est bien plus importante : +74 %. Cela s'explique par de multiples raisons, comme l'externalisation des services informatiques et numériques, leur obsolescence et leur vulnérabilité, l'importante surface d'exposition, mais aussi le manque de formation et de sensibilisation.

Le mode opératoire principal est le ransomware, ou rançongiciel. Ces programmes bloquent l'accès aux données. Une rançon est exigée pour les récupérer… mais cette récupération n'est pas garantie. C'est pourquoi il ne faut jamais accepter de payer la somme demandée. Les données personnelles sont également une cible privilégiée des hackers, ce qui peut conduire à de nombreuses usurpations d'identité. Plus rares, certaines cyberattaques sont menées pour des raisons idéologiques, avec comme objectif une perturbation de fonctionnement.

Des conséquences concrètes

En 2022 et 2023, de nombreux établissements de santé ont subi des cyberattaques, avec des conséquences variées. Des rançons ont ainsi été demandées, jusqu'à 1,2 million d'euros, ce qui constitue un manque à gagner conséquent pour des établissements souvent déjà en difficulté. D'autres attaques ont conduit à des fuites de données à caractère personnel, particulièrement dommageables pour les patients.

Les conséquences touchent aussi directement la santé des personnes hospitalisées, empêchant par exemple le transfert d'information lorsqu'une messagerie est coupée, bloquant des examens comme l'imagerie, ou même limitant l'accueil aux urgences. Certains patients ont vu leur accès à Internet coupé et donc la communication avec leurs proches fortement entravée.

Les actions de l'Ordre

L'Ordre a parfaitement conscience des conséquences s'il subissait une cyberattaque. Pour s'en prémunir, il met en place un certain nombre de mesures. Certaines sont de nature technique, comme des applications sécurisées ou bien la protection des e-mails et des identités. En effet, 90 % des cyberattaques passent par des e-mails. En 2022, sur les 16,8 millions d'e-mails reçus au sein de l'Ordre, seuls 20 % étaient légitimes. Les 80 % restants étaient des attaques ou des fraudes, qui ont été bloquées par les solutions de protection.
Le Cnom collabore étroitement avec les conseils départementaux afin de les sensibiliser à la cybersécurité. Le moment de l'inscription des médecins, notamment, doit susciter une grande vigilance pour éviter toute usurpation d'identité.

1er

LA FRANCE EST LE 1ER PAYS D'EUROPE en matière d'incidents de cybersécurité en santé (janvier 2021-mars 2023).

ADOPTER LES BONS GESTES POUR SE PROTÉGER

En médecine comme dans le domaine informatique, l'hygiène est la clé de la sécurité. Voici les 12 règles simples à appliquer au quotidien. Elles sont proposées par l'Agence nationale de la sécurité des systèmes d'information dans son *Guide des bonnes pratiques de l'informatique*.

1. CHOISIR AVEC SOIN SES MOTS DE PASSE
Idéalement, il faut un mot de passe pour chaque usage. Il doit être composé de 12 caractères de types différents, sans lien avec vous (ex. : date de naissance) et ne figurant pas dans le dictionnaire.

2. METTRE RÉGULIÈREMENT À JOUR SES LOGICIELS
Les mises à jour comblent les failles de sécurité. La vulnérabilité d'un logiciel est donc plus importante s'il n'est pas mis à jour.

3. BIEN CONNAÎTRE SES UTILISATEURS ET PRESTATAIRES
Il importe de connaître tous les utilisateurs d'un appareil et de réserver la session « administrateur » aux interventions sur le fonctionnement global de l'ordinateur.

4. EFFECTUER DES SAUVEGARDES RÉGULIÈRES
Cela vous permettra de récupérer vos données en cas d'attaque ou même de dysfonctionnement.

5. SÉCURISER SON ACCÈS WI-FI
Mal protégé, un réseau Wi-Fi peut être intégré par des personnes malveillantes pour intercepter des données ou participer à des cyberattaques.

6. ÊTRE PRUDENT AUSSI AVEC SON SMARTPHONE OU SA TABLETTE
Utilisez des codes de verrouillage, n'installez que les applications nécessaires et vérifiez les données auxquelles elles demandent accès.

7. PROTÉGER SES DONNÉES LORS DE SES DÉPLACEMENTS
Lorsque vous vous déplacez, votre appareil ne doit contenir que les données nécessaires qui doivent être sauvegardées par ailleurs. Surveillez votre appareil et évitez l'utilisation de Wi-Fi public.

8. ÊTRE PRUDENT LORS DE L'UTILISATION DE SA MESSAGERIE
Désactivez l'ouverture automatique de pièce jointe, ne cliquez pas sur un lien si vous n'êtes pas sûr à 100 % de l'adresse, ne répondez jamais à une demande de données confidentielles…

9. TÉLÉCHARGER SES PROGRAMMES SUR LES SITES OFFICIELS DES ÉDITEURS
Soyez vigilant au site sur lequel vous téléchargez vos logiciels (le premier résultat de recherche n'est pas forcément le bon), décochez les cases proposant l'installation de programmes complémentaires.

10. ÊTRE VIGILANT LORS D'UN PAIEMENT SUR INTERNET
Vérifiez la sécurité du site : cadenas, https://, orthographe de l'URL…

11. SÉPARER LES USAGES PERSONNELS ET PROFESSIONNELS
Il est tentant d'utiliser ses appareils personnels pour un usage professionnel. Or, ceux-ci sont souvent moins sécurisés.

12. PRENDRE SOIN DE SES INFORMATIONS PERSONNELLES, PROFESSIONNELLES ET DE SON IDENTITÉ NUMÉRIQUE
Vos données personnelles peuvent être utilisées pour vous nuire. Renseignez le minimum, vérifiez vos paramètres de sécurité, n'en dites pas trop sur les réseaux…

Nous rappelons aux médecins l'intérêt de l'utilisation de la messagerie sécurisée de leur espace médecin pour communiquer avec leur Ordre : https://messagerie.ordre.medecin.fr