

COMMUNIQUE DE PRESSE

LA FHF SALUE LE PLAN POUR LA CYBERSECURITE ET ATTEND DES REPONSES CONCRETES ET IMMEDIATES POUR PROTEGER NOS HOPITAUX

En réponse aux cyberattaques qui ont notamment touché les hôpitaux de Dax (Landes) et de Villefranche-sur-Saône (Rhône), le Président de la République a présenté jeudi 18 février un plan à hauteur d'1 milliard d'euros visant à renforcer la cyber sécurité du pays et de ses institutions d'ici 2025. La Fédération hospitalière de France (FHF), qui alertait déjà lors du Ségur sur la nécessité de se prémunir contre ces menaces, salue cette annonce et attend des réponses concrètes déployées à court terme face aux risques identifiés.

Dans une contribution sur le numérique en santé adressée au gouvernement dans le cadre du Ségur de la santé, en juillet 2020, nous l'écrivions déjà : le prochain virus qui neutralisera la planète pourrait bien être numérique.

En plus de la bataille sanitaire menée depuis presque un an, l'hôpital public a en effet dû livrer une seconde bataille informatique ces derniers mois, causée par une série de cyberattaques. Ces agressions pour l'heure souvent inédites pour l'hôpital public ont mis à l'épreuve les hospitaliers dans une période déjà tendue. La FHF tient ainsi à souligner la forte mobilisation et la capacité de résilience des professionnels de santé qui ont su s'adapter et poursuivre leur activité malgré ces attaques. Face à ces atteintes, la FHF salue également la capacité de réponse de l'ANSSI et d'Orange Cyber Défense ainsi que l'excellent travail mené en lien étroit avec les équipes hospitalières.

Alors que les hackers profanent le caractère sacré de l'hôpital et avec le risque que la fréquence de ces attaques se démultiplie, il est donc urgent et nécessaire que l'État renforce rapidement la sécurité des hôpitaux.

Le plan financé à hauteur d'1 milliard d'euros annoncé par le Chef de l'État est ainsi une mesure positive qui permettra de développer et d'adopter les outils de riposte nécessaires.

Il est essentiel d'engager immédiatement le travail avec les hôpitaux pour définir les orientations stratégiques à mettre en œuvre :

- Les **besoins immédiats de lignes directrices** données aux hôpitaux, fondées sur le retour d'expérience et prévenir de nouvelles attaques ;
- Les **besoins à moyens termes** : de coordination des équipes cybersécurité hospitalières, de formation, de méthodes partagées, de recrutement d'expertises, de financement des technologies, de développement d'un écosystème cybersécurité spécialisé santé.

Un pilotage interministériel de la cybersécurité permettrait également de positionner la santé au rang d'autres secteurs d'activités (économie, défense, diplomatie, ...) et ainsi de bénéficier d'un haut niveau de pratiques et de financements dédiés.

La FHF rappelle son souhait de voir tous les hôpitaux reconnus d'importance stratégique pour le bon fonctionnement du pays et désignés OSE (opérateurs de services essentiels). Il est temps d'engager les moyens à long terme qui permettront de s'adapter au niveau de menace toujours croissant.

« L'hôpital, qui joue dans cette crise son rôle de « bouclier sanitaire », a lui aussi besoin d'être protégé à la hauteur des menaces qui pèsent sur sa sécurité et celles des données de millions de patients. Le Plan annoncé par le Chef de l'État est en cela une bonne mesure qui mérite d'être précisée, en lien avec les hospitaliers, pour répondre concrètement et à court terme à leurs besoins et se prémunir contre de nouvelles attaques. »

Frédéric Valletoux, Président de la FHF

Contacts presse : Havas – communicationfhf@havas.com