



GOUVERNEMENT

*Liberté
Égalité
Fraternité*

22 février 2021

COMMUNIQUE DE PRESSE

Sécurité des réseaux informatiques des établissements de santé : le Gouvernement renforce sa stratégie.

Depuis deux ans, le Ministère des Solidarités et de la Santé a engagé un travail complet de mise à niveau de la sécurité des systèmes d'information des établissements de santé. Les attaques récentes sur nos établissements de santé démontrent la nécessité d'aller plus loin. Dans le cadre de la stratégie Cyber présentée le 18 février dernier par le Président de la République Emmanuel Macron, le Gouvernement renforce sa stratégie de cybersécurité à destination des établissements sanitaires et médico-sociaux pour un montant d'au moins 350 M€.

Le Ministre des Solidarités et de la Santé, Olivier Véran et le Secrétaire d'État chargé de la Transition numérique et des Communications électroniques, Cedric O se sont rendus aujourd'hui à Villefranche-sur-Saône pour détailler la mise en œuvre concrète de ces annonces.

« Depuis le début de l'année, un établissement de santé est victime chaque semaine d'une cyberattaque. C'est pourquoi nous faisons le choix d'investir massivement dans la sécurité des systèmes d'information de santé à travers le Ségur de la Santé. L'ensemble des services du Ministère des solidarités et de la santé seront mobilisées pour améliorer cette prise en compte des enjeux de cybersécurité », commente Olivier Véran, Ministre des Solidarités et de la Santé.

« Si aujourd'hui la situation est maîtrisée à Villefranche et Dax, il faut malheureusement s'attendre à d'autres attaques. Face à l'urgence nous renforçons notre action et complétons les travaux engagés depuis deux ans. Ainsi, nous mettons en place un accompagnement renforcé des établissements de santé face à la menace. La réalisation d'audits par l'ANSSI pour permettre la montée en sécurité des systèmes d'information des établissements de santé est essentielle. La prévention et la construction d'une réponse adaptée sont au cœur de notre stratégie nationale pour la cybersécurité », déclare Cédric O, Secrétaire d'État chargé de la Transition numérique et des Communications électroniques.

Un investissement massif dans la cybersécurité des systèmes d'information de santé

Le Ségur de Santé a prévu une enveloppe de 2 milliards d'euros d'investissements pour accélérer la numérisation des établissements de santé et médico-sociaux. Ils doivent notamment permettre d'accompagner leur transition numérique, de moderniser les systèmes d'information existants, et de renforcer leur interopérabilité, leur convergence et leur sécurité. Dans ce cadre, **350 M€ seront spécifiquement dédiés au renforcement de la cybersécurité de ces structures.**

Dès aujourd'hui, un accompagnement renforcé pour les établissements de santé

En plus des 350M€ prévus dans le cadre du Ségur de la Santé, la stratégie nationale pour la cybersécurité annoncée le 18 février a attribué à l'ANSSI une enveloppe budgétaire de 136 M€ pour renforcer la cybersécurité de l'Etat. **Sur cette enveloppe déjà dédiée à la cybersécurité, 25 M€ seront spécifiquement consacrés à la sécurisation des établissements de santé pour la réalisation d'audits** pour les accompagner dans leur démarche de cybersécurisation.

Ce financement permettra également d'accélérer le déploiement du « service national de cyber surveillance en santé » en partenariat avec l'Agence du Numérique en Santé (ANS) et à développer les moyens du dispositif « cyber veille en santé » pour augmenter les capacités de réaction et d'appui aux structures de l'ANS en cas d'incidents ou de cyberattaques.

Une meilleure prise en compte de la cybersécurité dans tous les projets de systèmes d'information des établissements de santé

Face à l'augmentation de la menace, il n'est plus possible de faire de la cybersécurité une variable d'ajustement des projets informatiques des établissements de santé. Ainsi, aucun projet ne pourra désormais faire l'objet d'un soutien de la part de l'Etat si une part de à **5 à 10% de son le budget informatique n'est pas dédiée à la cybersécurité.**

Un renforcement de la formation, de l'information et de la sensibilisation des acteurs intervenants dans le champ de la santé en matière de sécurité des pratiques numériques.

La sensibilisation à la cyber sécurité sera intégrée dans tous les cursus de formation des acteurs en santé afin conforter les pratiques « d'hygiène numérique » dans un contexte de renforcement de la convergence et de l'interopérabilité des systèmes d'information comme de la fluidité du parcours ville-hôpital. (2022)

Des exigences renforcées de sécurité informatique pour l'ensemble des établissements supports des 135 groupements hospitaliers territoriaux

D'ici 3 mois, **135 groupements hospitaliers français seront intégrés à la liste des « opérateurs de service essentiels »**. Ce classement implique des règles de sécurité informatique plus strictes et la contrainte d'appliquer aux systèmes d'information les meilleures pratiques de cybersécurité. L'ANSSI sera chargée de contrôler le bon respect de ces règles. Les Agences Régionales de Santé accompagneront les établissements pour les aider à se conformer à ces nouvelles obligations.

Contacts presse

Cabinet d'Oliver Véran	01.40.56.60.60	sec.presse.solidarites-sante@sante.gouv.fr
Cabinet de Cédric O	01 53 18 43 10	presse@numerique.gouv.fr
ANSSI	06 49 21 63 80	Margaux.vincent@ssi.gouv.fr