ACSS

Le dispositif de traitement des incidents graves de sécurité des systèmes d'information dans le secteur santé

#1 De quoi parle-t-on ?

La sécurité numérique est au cœur des préoccupations du ministère des solidarités et de la santé.
L'interconnexion, la multiplication des échanges et le partage des données entre la ville et l'hôpital multiplient les risques liés à la sécurité : piratage, vols ou détournements de données, blocage des systèmes etc.
Au regard de l'augmentation du nombre d'attaques sur les systèmes numériques des établissements de santé, l'amélioration des actions de prévention et d'assistance portée devient prioritaire.

La sécurité des systèmes d'information de santé permet que les données de santé soient disponibles, confidentielles, fiables, partagées et traçables.
La protection des données de santé est indispensable pour assurer une meilleure coordination des soins et une prise en charge optimale des patients.

#2 Le contexte règlementaire

Au travers de l'article 110 de la loi n° 2016-41 du 26 janvier 2016 de modernisation de notre système de santé, le Ministère des Solidarités et de la Santé introduit l'obligation de signalement des incidents de sécurité pour :

- les établissements de santé,
- les hôpitaux des armées,
- les centres de radiothérapie,
- les laboratoires de biologie médicale.

Le décret d'application n°2016-1214 du 12 septembre 2016 précise que les incidents graves de sécurité des systèmes d'information du secteur santé devront être signalés sans délai à compter du 1er octobre 2017.

#3 Les objectifs

- **Renforcer l'analyse et le suivi** des incidents pour le secteur santé ;
- **Alerter et informer** l'ensemble des acteurs de la sphère santé en cas de menaces ;
- **Partager les bonnes pratiques** sur les actions de prévention, ainsi que sur les réponses à apporter suite aux incidents, afin de réduire les impacts et de mieux protéger les systèmes.

La mise en place du dispositif est guidée par les principes suivants :

- **Une logique de sensibilisation et d'accompagnement** afin de favoriser les déclarations spontanées des établissements hospitaliers ;
- **Un rôle de conseil** ou d'orientation vers les acteurs adéquats, mais en aucun cas une prise en charge de l'incident à la place de la structure victime ;
- Une attention particulière portée sur la sécurité du dispositif pour **assurer la confidentialité** des informations communiquées par les établissements.

#4 Un portail unique pour déclarer les incidents de sécurité

Les structures de santé concernées doivent déclarer leurs incidents de sécurité via le portail de signalement des évènements sanitaires indésirables depuis l'espace dédié aux professionnels de santé :
www.signalement.social-sante.gouv.fr/

Celles-ci devront signaler toute action ou suspicion d'action malveillante causant une indisponibilité partielle ou totale de leurs systèmes d'information, une altération ou une perte de leurs données et plus généralement des incidents ayant un impact sur le fonctionnement normal de l'établissement.

#5 Une cellule d'accompagnement opérationnelle pour aider les structures de santé

Afin d'apporter un accompagnement aux organismes concernés par la déclaration de ces incidents, les services du Haut Fonctionnaire de Défense et de Sécurité du ministère des solidarités et de la Santé, en lien avec les agences régionales de santé (ARS) et l'ASIP Santé, met en place un dispositif d'Accompagnement Cybersécurité des Structures de Santé (la cellule ACSS).
Elle traite les signalements d'incidents de sécurité de leurs systèmes d'information.

Elle propose un Portail de veille et d'échanges :

cyberveille-sante.gouv.fr

Ce portail informe sur l'actualité SSI (Sécurité des Systèmes d'information), les vecteurs de menaces et les bonnes pratiques en matière de sécurité numérique.
Il présente des bulletins de veille sur certaines vulnérabilités logicielles critiques ou des menaces sectorielles, des fiches réflexes et des guides pour répondre à différents types d'incidents.
Ce portail met également à disposition de la communauté SSI en santé un espace privé pour le partage entre spécialistes de la cybersécurité.