AXE 5 : Gérer, anticiper et prévenir les risques

Chapitre 3 : Renforcer la cyber résilience du système de santé

1 Contexte et enjeux

Les acteurs du système de santé sont la cible de nombreuses attaques de leurs systèmes d'information (SI), par la nature des données qu'ils détiennent et traitent. Rien qu'en 2022, plusieurs établissements de santé d'Île-de-France ont subi des cyber attaques majeures (Centre Hospitalier Sud Francilien, Clinique des Bluets, Centre Hospitalier de Versailles).

L'impact sur l'activité de ces établissements a nécessité le déclenchement du plan blanc et une réorganisation importante de l'offre de soins. Ces attaques ont mis en exergue la vulnérabilité du système de santé à l'égard de la menace cyber et le besoin de mieux s'y préparer.

En effet, les outils numériques sont devenus incontournables pour le bon fonctionnement des établissements de santé (SI métiers ou administratifs ou financiers Mon Espace Santé/ Dossier médical partagé, outils de télésanté, etc). **Leur indisponibilité rend très difficile, voire impossible, la poursuite des activités de soins**. En cas de cyberattaque massive, la remise en fonctionnement des SI, et plus généralement de l'établissement, peut prendre plusieurs mois.

Les **impacts financiers sont souvent majeurs**, compte tenu d'une part, des coûts de gestion de crise et de reconstruction des SI, d'autre part en raison des pertes de recettes engendrées par la baisse d'activité et l'impossibilité de la retracer dans le PMSI. Enfin, les cyberattaques peuvent donner lieu à des vols de données particulièrement sensibles (exemple des données de santé). Par ailleurs, les impacts ne se limitent pas au seul établissement attaqué et **peuvent déstabiliser l'organisation de l'offre de soins au niveau de tout un territoire**, *a fortiori* si l'établissement victime de l'attaque est un établissement de recours.

Améliorer la résilience du SI constitue un enjeu pour les directions générales des établissements et pas uniquement pour les services supports en informatique. Par ailleurs, cet enjeu ne se limite pas au secteur sanitaire, puisque le médico-social et les professionnels de ville, ne disposant pas nécessairement d'équipes informatiques ou d'experts en cybersécurité, sont également la cible des cyberattaquants.

Conscient de ces enjeux de protection de la donnée sensible d'une part, et de maintien en activité du système de santé d'autre part, le gouvernement a renforcé ses moyens d'action dans le cadre de sa stratégie nationale de cybersécurité, dans un **contexte de menace cyber très élevé**, En effet, les plans d'actions et mesures nationales et régionales n'ont cessé de s'étoffer au cours des dernières années et continueront à le faire sur la durée du PRS3, pour s'adapter au niveau de menace grandissant.

Un cadre d'actions, des référentiels et des programmes de financement cyber à destination des établissements sanitaires et médico-sociaux sont définis au niveau national et portés par le ministère en charge de la santé, le CERT Santé et l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Ces actions ne seront pas décrites dans le détail dans le cadre de la présente fiche mais ont bien sûr vocation à être déployées en Île-de-France.

Les actions envisagées par l'ARS visent à répondre à trois enjeux :

- **La prévention :** accroître la sécurisation et la résilience des établissements aux attaques et incidents majeurs cyber ;
- **La gestion de crise :** en cas de cyber-attaque, assurer la sécurité et la continuité des prises en charge en soins, éviter la déstabilisation et la saturation régionale ;
- **La réparation post-cyberattaque :** accompagner l'établissement dans sa reconstruction et sa sécurisation, sur plusieurs mois voire années, avec des impacts pouvant être conséquents sur les prises en charges des patients, sur la gestion des ressources humaines, et sur l'axe financier.

2 Objectifs stratégiques et opérationnels à 5 ans

- ***Volet « préventif » : améliorer le niveau de maturité des établissements et professionnels de santé en matière cyber et réduire les vulnérabilités***
- ***Un accompagnement de l'ensemble des acteurs du système de soins (sanitaire, médico-social, ville) est nécessaire afin de réduire les vulnérabilités et améliorer la résilience du système vis-à-vis de la menace cyber, ce qui passera par les actions suivantes :Volet « gestion de crise » : se préparer à la gestion des attaques et incidents cyber***

L'année 2022 est marquée par une évolution du guide méthodologique ORSAN qui doit se traduire, en 2023 par une mise à jour de la documentation ORSAN. Dans ce cadre, il a été fait le choix à l'ARS IDF de créer un nouveau plan ORSAN CYBER qui, en interface avec les dispositions spécifiques transversales devra permettre d'organiser la réponse à des incidents majeurs ou des cyber-attaque d'ampleur.

- ***Volet « reconstruction post-cyberattaque » : soutenir la reconstruction du système d'information***

Suite à une cyber-attaque, l'établissement se retrouve face à un dilemme : redémarrer sur sa configuration ancienne, mais pas forcément stable, ou partir sur de nouvelles options au risque de fonctionner en mode dégradé durant une période longue. Par ailleurs, la reconstruction nécessite la plupart du temps des ressources matérielles, techniques et humaines supplémentaires.

3 Moyens d'y parvenir / leviers pour l'atteinte des objectifs de l'axe

- ***Volet « préventif »***

  - **Encourager les établissements à faire de la cybersécurité** une priorité, notamment en incluant des objectifs cyber dans les objectifs des chefs d'établissements ou dans les contrats pluriannuels d'objectifs et de moyens conclus entre l'ARS et les établissements ;
  - **Renforcer les actions de sensibilisation** pour les directions générales d'établissements, membres du comité de direction, présidents de commission médicale d'établissement (CME), mais aussi pour tous les professionnels : promouvoir les outils de sensibilisation disponibles au catalogue du SESAN, les outils de sensibilisation disponibles auprès de l'Agence nationale de sécurité (ANS), formations gratuites de l'ANSSI, les formations disponibles via l'ANFH… ;
  - **Favoriser le partage sur les bonnes pratiques, retours d'expériences** pour les DSI, RSSI, utilisateurs du SI, directions d'établissements, notamment via l'organisation de journées régionales ou de webinaires, la diffusion de newsletters ;
  - S'assurer de la **réalisation par les établissements des audits annuels cyber obligatoires** (service Active directory security - ADS et cybersurveillance), **ainsi que des exercices de cybercrise**, et promouvoir la mobilisation des programmes de financements dédiés pour la réalisation de ces audits et exercices ; s'assurer de la **définition et de la mise en œuvre d'un plan d'actions** par les établissements intégrant les axes d'amélioration mis en lumière par les audits et les exercices ;
  - Promouvoir le remplissage par les établissements de l'**Observatoire national dédié à la cyber** (OPSSIES), afin notamment de disposer d'une vision d'ensemble du niveau de préparation des établissements vis-à-vis du risque cyber, identifier les éventuels points de vulnérabilité et les actions complémentaires à mettre en œuvre ;
  - Promouvoir et poursuivre l'enrichissement de **l'offre du GIP SESAN dédiée à la cybersécurité** à destination des ES, ESMS et professionnels franciliens : tests d'intrusion, cybersurveillance, scan de vulnérabilité, cartographies et analyse de risques, exercices de cybercrise, …
  - Poursuivre, en lien avec le GIP SESAN, les **actions de sensibilisation et d'accompagnement** des directeurs des SI (DSI) et responsables de la sécurité des systèmes d'information (RSSI) régionaux : expertise SSI, animation du réseau régional des RSSI et des délégués à la protection des données (DPO), formations en ligne... ;
  - Réaliser des audits sécurité des SI SAMU ou autres audits cyber ciblés ;
  - S'appuyer sur les outils, **programmes de financements et acteurs nationaux** spécialisés (ANSSI et CERT Santé).

- ***Volet « gestion de crise »***

Il s'agit tout d'abord de **co-construire le plan ORSAN Cyber avec les acteurs régionaux et définir un ainsi les dispositifs et stratégies de réponses** pour ensuite **les déployer avec les parties prenantes.**

Une partie de ces dispositifs et les actions qui en découlent est déjà pré-identifiée et leur construction à débuter sans attendre l'achèvement des travaux ORSAN (mais y sont intégrés) compte tenu de l'état de la menace, notamment :

- La mise en œuvre d'un cadre permettant l**e recours à des ressources d'expertises, RH ou matériels** pilotées par l'agence. Ceci suppose les préalables suivant :
  - Identifier **des moyens RH, experts et techniciens** sur l'ensemble des champs techniques, **mobilisables à tout moment** en cas de cyberattaque et définir les modalités de cette mobilisation ;
  - Organiser **l'entraide inter-établissements** (dans le département, dans la région et selon la filière de prise en charge) ;
  - Identifier et adapter les moyens immédiatement projetables sur le terrain ;
  - Disposer d'une capacité de mobilisation rapide de **moyens matériels informatiques permettant une première reconstruction d'urgence** (ex : ordinateur, serveurs, système de messagerie…) et permettre de pérenniser le mode dégradé le temps de la reconstruction ;
- La réalisation de **procédures et d'outils de réorganisation de l'offre** de soins non programmée (également utilisable sur d'autres risques tel que le risque de crue majeur de la Seine) ;
- La mise à disposition **par le GIP SESAN d'une prestation de « réponse à Incident »** permettant à un établissement attaqué de bénéficier sans délai d'un appui à la gestion de crise cyber.

- ***Volet « reconstruction »***

Le soutien à la reconstruction peut prendre plusieurs formes :

- Renforcer le pilotage stratégique SI ;
- Compléter l'offre SESAN pour faciliter le recours à des moyens supplémentaires durant la période de reconstruction :
  - Accompagnement méthodologique pour la définition de la reconstruction, voire le suivi de l'avancement ;
  - Accompagnement pour migrer vers de nouvelles architectures, voire passer en mode SaaS (solution logicielle applicative hébergée dans le Cloud) ;
- Proposer des mises à niveaux (formation) et des partages d'expérience.