SYNTHÈSE DU PLAN D'ACTION CaRE : CYBER ACCÉLÉRATION ET RÉSILIENCE DES ÉTABLISSEMENTS

Élodie Chaudron
Directrice de programme
chez Agence du numérique
en santé

Crédit photo : DR

Comme dans tous les secteurs, la santé connaît un essor du numérique. Ce dernier est partout : dans les cabinets libéraux, à l'hôpital, à la maison, son usage est devenu quotidien pour tous les soignants et les patients. De fait, les opportunités de cybermalveillance augmentent aussi. Selon l'ANSSI, le secteur santé est le troisième secteur le plus touché par les cyberattaques, après les collectivités territoriales et les TPE/ PME et les signalements réalisés auprès du CERT Santé par les établissements ne faiblissent pas avec le temps.

Cette menace cible des systèmes d'information hospitaliers vastes et complexes, ce qui les rend particulièrement vulnérables. Les établissements souffrent pour nombre d'entre eux d'une grande dette technologique et rencontrent des difficultés structurelles à mobiliser durablement les équipes en capacité de rattraper ce retard.

Ces derniers mois, plusieurs cyberattaques majeures ont touché des établissements de soins, avec des conséquences importantes et durables. Ces attaques provoquent en premier lieu une bascule des services en mode dégradé, pouvant aller jusqu'à l'interruption des activités, mais au-delà de cette période aigüe, les perturbations s'installent pour des mois, avec un impact sur la prise en charge des patients et des coûts de remédiation très importants.

Cette accélération de la menace sur notre système de santé a conduit à réagir avec la mise en place d'un programme sans précédent, à la hauteur des enjeux, nommé CaRE (Cybersécurité accélération et Résilience des Établissements), d'ores et déjà doté d'un budget de 250 M€ de 2023 à 2025 et avec un objectif total de 750 M€ investis d'ici 2027.

Dès 2023 de premières actions concrètes ont été déployées :
Près de **1 500 exercices de crise cyber** auront été réalisés en 2023, soit 30% des établissements.

Les établissements touchés se sont largement mobilisés pour constituer des retours d'expérience et les partager.

Des critères numériques ont été ajoutés à la certification HAS et plus de 150 experts visiteurs numériques ont été recrutés. Ils démarrent les premières évaluations des établissements pilotes.

Une formation socle au numérique a été rendue obligatoire dans tous les cursus de santé, avec une forte valence cybersécurité, avec une mise en oeuvre au plus tard à la rentrée universitaire 2024.

Plusieurs outils ont été réalisés et mis à disposition des établissements : kits d'exercice de crise cyber, guide d'élaboration du plan blanc numérique, kit d'élaboration des plans de continuité et de reprise de l'activité, catalogue des offres cyber.

Les instances de gouvernance du programme se sont mises en place avec tous les acteurs : ministères, agences nationales, régions, fédérations hospitalières et du médicosocial.

Le programme s'est construit avec tout l'écosystème, réunis au sein d'une "taskforce", avec le double objectif :

- Éviter autant que faire se peut que les attaques aboutissent
- Permettre aux établissements de s'en relever le plus rapidement possible.

Le programme s'articule autour de quatre axes de travail, détaillés ci-dessous.

GOUVERNANCE DE LA CYBERSÉCURITÉ ET LA RÉSILIENCE DES ÉTABLISSEMENTS

Au niveau **national**, la gouvernance se traduit d'une part par la mise en place d'un comité de pilotage CaRE qui réunit mensuellement les acteurs impliqués : ministériels (DNS, DGOS, HFDS, FSSI), agences nationales (ANSSI et ANS), acteurs régionaux (ARS et GRADeS), et d'autre part par des groupes de travail spécialisés.
Les travaux de ces différents groupes sont la base du programme CaRE, publiée en décembre 2023, et qui sera mise à jour annuellement.

Cette gouvernance doit également s'inscrire au niveau des établissements. Les équipes internes doivent être consolidées. L'inscription de la cybersécurité dans la stratégie locale sera matérialisée par la mise en place d'objectifs dédiés dans les contrats pluriannuels d'objectifs et de moyens conclus entre les ARS et les établissements, et par **l'inscription par la HAS de critères sur le numérique et la cybersécurité dans le manuel de certification des établissements**. Une instruction sera produite en 2024 pour synthétiser les différentes obligations et exigences. Enfin, un groupe de travail va être constitué pour inclure les usagers dans la démarche.

Sur le plan de la résilience des établissements, **la préparation a été identifiée comme le vecteur essentiel de progression**, et a été outillée à travers la mise en place de kits d'exercice de crise par l'ANS, dont la réalisation a été financée dès 2023, la diffusion d'un guide d'élaboration du plan blanc numérique par la DGOS, et un kit de plan de continuité et de reprise d'activité par la taskforce. Le déploiement opérationnel de ces outils est suivi par les ARS, l'ANS et la DGOS.

Dans l'objectif d'autonomiser les établissements dans la mise en place des actions de sécurisation nécessaires, un référentiel d'autoévaluation va être constitué, et devra être suivi par les établissements.

LES RESSOURCES ET LEUR MUTUALISATION

En effet, le manque de ressources dédiées au numérique au sein des établissements et en particulier sur la cybersécurité a été identifié comme un frein majeur à la mise en œuvre des actions de sécurisation. Dans cette optique, des recommandations vont être émises concernant le dimensionnement des équipes et les compétences nécessaires. En lien avec la feuille de route du numérique en santé, **les dépenses dédiées au numérique devront s'élever à 2% du budget des établissements**, dont 10% dédiés au cyber, pour soutenir à la fois l'attractivité des postes et le financement des outils. La fidélisation est également un enjeu, qui a déjà été pris en compte en 2023 avec **la revalorisation de la grille des ingénieurs hospitaliers**.

En parallèle, il faudra renforcer la mutualisation de certaines ressources, tout d'abord à l'échelle des établissements, et notamment en s'appuyant sur la **convergence au sein des GHT**, mais également au niveau régional, où les ARS et les GRADeS devront développer une offre de service et s'assurer de sa visibilité pour les établissements. La mobilisation des industriels sera également essentielle pour disposer d'une palette d'outils efficaces sans imposer de dérive budgétaire trop importante.

LA SENSIBILISATION

Elle est essentielle à plusieurs titres. Tout d'abord, au niveau des décideurs, qui doivent prendre conscience que la cybersécurité n'est plus une option, mais un composant essentiel de la sécurité de la prise en charge et de la continuité des soins. Les retours d'expérience terrain sont un outil de choix pour l'illustrer.

Au niveau des équipes informatiques, la sensibilisation vise à s'assurer de la compréhension des enjeux, des objectifs et des moyens mis à disposition, notamment à travers la constitution de groupes de travail nationaux et régionaux.

Enfin, cette sensibilisation doit être réalisée pour **l'ensemble des professionnels de santé**, dans le cadre de leur formation initiale ou continue (un module obligatoire « numérique et cyber » a ainsi été intégré à tous les cursus), mais aussi dans le cadre de leur exercice professionnel.

Le programme s'attache à livrer les outils pédagogiques et méthodologiques qui permettront d'aider les décideurs et leurs équipes, et à mettre à disposition des lieux d'échange et de partage qui leur permettront de trouver les réponses à leurs questions.

LA SÉCURITÉ OPÉRATIONNELLE DES ÉTABLISSEMENTS

Celle-ci repose sur des éléments techniques, identifiés pour leur rôle dans les chaînes d'attaque observées, qui ont été rassemblés par la taskforce au sein de 5 domaines, chacun d'entre eux donnant lieu à des objectifs particuliers et bénéficiant d'un financement adapté à ceux-ci.

Le premier domaine va démarrer fin 2023 et concerne l'exposition internet des établissements et la sécurité des annuaires d'entreprise, qui constituent une source importante de failles exploitables par les attaquants.

Quatre autres domaines sont d'ores et déjà identifiés : « Continuité d'activité et stratégie de sauvegarde », « Sécurisation des accès de télémaintenance », « Poste de travail et détection », « Identification électronique des professionnels (HospiConnect) ». L'objectif de ce dernier domaine est d'accélérer l'adoption par les établissements de solutions d'identification électronique sécurisées pour l'accès des professionnels aux services numériques sensibles (authentification forte, gestion des identités et des accès, Single Sign On). Doté d'un budget de 50 M€, le programme sera initié par des appels à projets d'expérimentations de plusieurs solutions au sein de quelques établissements candidats début 2024, avant une généralisation en 2025.

Les dépendances avec HOP'EN 2, le programme de financement de la transition numérique des établissements de santé, seront prises en compte sur l'ensemble des domaines pour faciliter la programmation des travaux au sein des établissements. Les travaux de la taskforce se poursuivant, et la maturité des établissements étant naturellement amenée à progresser suite à la mise en oeuvre des premiers domaines, de **nouveaux domaines** vont probablement émerger dans le futur. Un budget total de 250M€ est d'ores et déjà défini.

Un budget complémentaire viendra prolonger les efforts d'investissement sur la cyber jusqu'en 2027.

Enfin, la pérennisation de ces actions sera construite à travers deux dispositifs : les réflexions sur le financement pérenne du numérique à l'hôpital, et l'inscription de la cybersécurité dans les référentiels sectoriels.

Lien vers la page CaRE avec la Feuille de route intégrale.
https://esante.gouv.fr/strategie-nationale/cybersecurite

Membres de la task force :

Patrice BIGEARD (FSSI),
Elodie CHAUDRON (ANS),
Laure DUHESME (ANSSI),
Alain ESPINOUX (ANS),
Matthieu FAURE (DNS),
Steven GARNIER (ARS BFC),
Jean-Baptiste LAPEYRIE (ANS),
Auriane LEMESLE (GRADeS PDL),
Christophe MATTLER (DNS),
Clara MORLIERE (DNS),
Thierry NAVARETTE (GRADeS ARA),
Jean-François PARGUET (FSSI),
Christophe PICHOT MEUGER (ANS),
Fabian RICHARD (ARS Normandie),
Silvère RUELLAN (ANSSI),
Rémi TILLY (GRADeS IDF),
Djamil VAYID (ARS Réunion),
Nicolas VOSS (DGOS),
Mehdi ZINE (ANS).