CKISA, un projet innovant pour garantir la continuité des soins en cas de crise et renforcer la résilience des établissements hospitaliers

Face à la multiplication des cyberattaques et des pannes informatiques, le secteur de la santé est de plus en plus vulnérable. Le projet CKISA (Cyber Kit Santé), porté par le GCS AMEITIC et développé par Docaposte pour La Poste Santé & Autonomie, répond à cet enjeu crucial en proposant une solution innovante et globale. L'ambition est de déployer un dispositif standardisé, permettant de garantir la continuité des soins dans les établissements hospitaliers, quelles que soient leur taille et leurs ressources.

Sylvie Delplanque, directrice territoriale des services numériques et administratrice du GCS AMEITIC, et Sébastien Bachem, directeur des solutions santé chez Docaposte, apportent leurs éclairages sur cette initiative et son impact pour les établissements hospitaliers.

Pouvez-vous présenter le projet CKISA et expliquer ses enjeux pour les établissements de santé ?

Sylvie Delplanque : Le projet CKISA, porté par le GCS AMEITIC, a été sélectionné dans le cadre de l'appel à manifestation d'intérêt « Sécuriser les territoires » de France 2030. Pilotée par la Banque des Territoires pour le compte de l'État, l'initiative vise à renforcer la cybersécurité dans le secteur de la santé.

Notre objectif dépasse la simple prévention des cybercrises : il inclut également une capacité d'intervention rapide en cas de crise majeure impactant l'ensemble du système d'information. Le projet repose sur une approche intégrant des aspects humains, organisationnels et technologiques, visant à sécuriser les établissements tout en assurant la continuité des soins. L'enjeu est de détecter rapidement une attaque ou une panne majeure, d'assurer une réponse immédiate pour maintenir l'activité hospitalière en mode dégradé et de permettre une reprise rapide des systèmes.

Dans le cadre de cet appel à manifestation, nous devons également développer une solution innovante. Elle sera d'abord testée dans trois établissements pilotes : le Centre Hospitalier de Calais et deux hôpitaux du Groupement des Hôpitaux de l'Université Catholique de Lille (GHICL), Saint Philibert à Lomme et Saint Vincent de Paul à Lille. Ces établissements présentent des contextes variés du point de vue de la taille et des services cliniques, permettant de tester la solution dans différents environnements. À terme, nous souhaitons rendre cette solution accessible à tous les établissements de santé, quels que soient leur niveau de numérisation et leurs ressources informatiques.

Quels sont les principes d'organisation qui sous-tendent le projet ?

S.D. : Nous appliquons la méthodologie de l'ANSSI, qui inclut l'analyse des risques à travers le BIA (Bilan d'Impact d'Activité), le PCA (Plan de Continuité d'Activité) et le PRA (Plan de Reprise d'Activité). Le BIA permet d'identifier les données critiques et de déterminer combien de temps elles peuvent être inaccessibles sans perturber gravement l'activité (quelques heures, une journée, etc.). Le PCA définit les mesures à mettre en œuvre pour assurer la continuité des opérations en mode dégradé et pour revenir à la normale aussi rapidement que possible.En complément de cette documentation, le projet CKISA vise à développer une solution de repli pour assurer la continuité d'activité au travers d'un kit se composant de terminaux (valisettes), d'un réseau de secours et de deux applicatifs : la capsule Pilotage de crise destinée à la direction de l'établissement et sa cellule de crise ; la capsule Métier destinée au personnel soignant. Ces capsules disposent des informations vitales et stratégiques même en cas d'arrêt du système central. Hébergées sur une plateforme Cloud sécurisée et souveraine de Docaposte, elles restent accessibles via des équipements réseaux et terminaux spécifiques conçus pour les situations de crise (voir encadré).

Qu'en est-il de l'organisation en cas de crise ? Qu'est-ce qui change concrètement pour les équipes ?

S.D. : Le projet nous a conduits à repenser l'organisation de la gestion de crise. Nous avons mis en place une cellule dédiée, prête à intervenir immédiatement en cas de panne ou d'attaque. Elle est chargée de définir les priorités, d'organiser la communication et de mobiliser les équipes.

La formation du personnel est essentielle. Chaque professionnel doit savoir comment poursuivre son activité sans accès à l'informatique principale, qu'il s'agisse de prescrire sans dossier patient informatisé, de gérer la pharmacie sans outils informatiques ou de garantir la continuité des soins dans des conditions dégradées.

Nous avons aussi révisé les modes de communication interne et externe, en intégrant des solutions alternatives pour garantir les échanges entre services et partenaires, même en cas d'indisponibilité de la messagerie ou du réseau téléphonique.

Cette analyse a révélé des interdépendances souvent sous-estimées, notamment en matière de gestion économique et finan-

cière. Par exemple, si les commandes de médicaments ne peuvent être passées, les stocks s'épuisent rapidement, compromettant le bon fonctionnement de l'hôpital.

Vous utilisez un serious game pour tester la pertinence de CKISA, au fil de l'avancement du projet. Pouvez-vous nous en expliquer l'utilité ?

Sébastien Bachem : Le serious game permet de simuler une situation de crise fictive – cyberattaque majeure ou panne étendue – afin de confronter les équipes hospitalières (soignants, informaticiens, direction) à des scénarios réalistes.
Dans la première phase, les participants doivent gérer la crise sans aucun outil de secours. Ils prennent alors conscience des difficultés majeures : absence d'accès aux dossiers patients, indisponibilité de l'imagerie, interruption des communications internes, etc.
Dans la seconde phase, nous réintroduisons les solutions du projet CKISA ce qui permet de tester la valisette et les capsules, et d'en mesurer l'impact sur la réactivité des équipes et la continuité de l'activité.
Ce serious game, mis en place à chaque version majeure de la solution, permet d'identifier les fonctionnalités à améliorer ainsi que les domaines où des formations supplémentaires sont nécessaires. La méthodologie Agile employée facilite l'ajustement rapide de la solution en fonction des retours d'expérience.

Qu'en pensent les équipes hospitalières ? Les retours sont-ils positifs ?

Sylvie Delplanque : Oui, les retours sont très positifs. Les soignants et le personnel technique prennent véritablement conscience des défis qu'une cyberattaque ou une panne de réseau complète représente. Nous avons observé des situations de stress extrême, par exemple, lorsque l'on ne peut plus envoyer les analyses vitales au laboratoire ou lorsqu'on ne sait plus quel patient se trouve dans quelle chambre.
Les équipes sont impliquées à toutes les étapes du projet, depuis les ateliers de conception, où elles définissent les données critiques et les priorités fonctionnelles, jusqu'aux phases d'expérimentation.

Sébastien Bachem : La mobilisation est forte, nourrie par des exemples récents de cyberattaques ayant touché des hôpitaux français, comme celui de Corbeil-Essonnes. La menace est bien réelle, et les équipes voient enfin émerger une solution concrète.

Quelles sont les grandes étapes à venir pour finaliser le projet ?

Sylvie Delplanque : D'ici la fin de l'année 2025, la solution devrait être validée et testée sur les établissements pilotes. Puis nous entrerons dans une phase d'accompagnement élargie, où nous ajusterons les outils en fonction des retours des établissements. Le GCS prévoit d'étendre l'expérimentation à d'autres hôpitaux de la région. L'objectif est que chaque établissement puisse s'approprier la méthodologie et, si les résultats sont concluants, adopter également la solution technique.
À terme, notre ambition est de disposer d'une solution reproductible pour tout établissement de santé.

Sébastien Bachem : Une fois le pilote validé, nous envisageons d'industrialiser la solution afin qu'elle puisse être déployée dans n'importe quel établissement de santé, quelle que soit sa taille. Cela inclura notamment la formation du personnel, l'accompagnement au changement et la mise en réseau des établissements pour partager les bonnes pratiques et assurer une montée en compétences progressive. L'objectif est de pérenniser la démarche CKISA.
Il est important que les hôpitaux ne développent pas des systèmes indépendants, mais qu'ils se basent sur une solution commune, sécurisée et validée. Cela s'inscrit directement dans la stratégie de Docaposte et de La Poste Santé & Autonomie qui portent une vision à long terme de la santé, basée sur des services numériques de confiance et des solutions souveraines.

Les deux capsules de CKISA : principe et utilité

Le projet CKISA repose sur deux capsules complémentaires, interagissant en permanence, conçues pour répondre aux besoins spécifiques des crises sanitaires :
● **La capsule pilotage de crise :** destinée à la direction de l'établissement et sa cellule de crise, elle centralise les informations stratégiques remontant de l'ensemble des services et permet une coordination rapide grâce à des tableaux de bord en temps réel et un système de messagerie sécurisé.
● **La capsule métier :** dédiée aux soignants, ellefacilite l'accès sécurisé aux données essentielles des patients, prescriptions et plans de soins, tout en permettant une communication instantanée et la mise à jour continue des données critiques.

Les partenaires du projet

Plusieurs expertises de Docaposte, pilier numérique de La Poste Santé & Autonomie, sont mobilisées pour répondre aux différents enjeux stratégiques du projet :

● **Maincare,** éditeur de logiciels santé, et Weliom, cabinet de conseil en santé, (tous deux filiales de Docaposte) associent leurs expertises pour les travaux de conception fonctionnelle avec les établissements pilotes. En outre Maincare apporte ses composantes techniques et logicielles déjà éprouvées dans les établissements de santé et Weliom apporte son savoir-faire en exercice de crise pour les serious game et phases d'expérimentation.

● **Docaposte**, expert dans le traitement de données sensibles et dans le développement et intégration de solutions numériques en santé, est en charge des développements, front et back-end, de l'intégration des composantes Maincare ainsi que de l'interopérabilité avec les systèmes d'information hospitaliers.

Des partenaires externes reconnus pour leur expertise en matière de cybersécurité et en gestion des crises sont également parties prenantes :

● **Crisalyde** : expert en gestion de crise, ayant accompagné des hôpitaux lors d'attaques cybernétiques et apportant son expertise pour le pilotage de crise.

● **Advens** : spécialisé en cybersécurité, apportant son expertise sur la sécurisation des systèmes d'information.