

À Marseille, les hôpitaux s'entraînent à faire face à une cyberattaque grandeur nature

Dans les Bouches-du-Rhône, plusieurs établissements de santé ont participé à un exercice de gestion de crise simulant une cyberattaque.

Objectif : tester leur capacité à réagir, maintenir les soins et coordonner les équipes en situation dégradée.



Texte **Thibault Demeneix**

Dans une salle de crise, l'alerte tombe : un poste informatique de réanimation est compromis. Rapidement, la décision est prise d'isoler l'ensemble du service. Les équipes informatiques alertent la direction, contactent les autorités compétentes et enclenchent les premières procédures d'urgence.

Mais ici, pas de véritable attaque. La scène est simulée dans le cadre d'un exercice coordonné à l'échelle du GHT 13, qui regroupe plusieurs établissements des Bouches-du-Rhône.

À l'origine de cette simulation, la société Tilwit, fondée en 2021 par Pierre-Yves Boyeau, spécialisée dans la résilience des organisations. « Nous avons été sollicités pour réaliser un exercice de gestion de crise sur l'ensemble des établissements du groupement », explique Stéphane Bouchut, directeur opérationnel. Pendant six mois, ses équipes ont analysé les infrastructures, les systèmes d'information et l'organisation de chaque hôpital afin de construire un scénario au plus proche de la réalité.

Une crise simulée, des réactions bien réelles

Dès le déclenchement de l'exercice, les équipes doivent réagir comme en situation réelle. Isolement des systèmes, remontée d'information, activation des cellules de crise : chaque décision compte.

À l'AP-HM, les équipes de sécurité informatique identifient rapidement une attaque de type ransomware. « On ne va pas prendre de risques », explique Pierre-Alain Jullien, responsable de la sécurité opérationnelle, qui décide de déconnecter l'ensemble des postes concernés. Les autorités nationales, comme l'ANSSI et les dispositifs de cyberveille, sont immédiatement alertés.

Côté médical, la priorité reste la continuité des soins. « Dès qu'on a une suspicion de cyberattaque, on déconnecte le réseau et on bascule sur des procédures papier », explique le Pr Velly, Directeur Médical de la crise de l'APHM. Chaque service dispose de « crash box » permettant de continuer à suivre les patients sans outil informatique, avec dossiers médicaux, prescriptions et historiques imprimés.

Nombre d'établissements ayant joué la simulation : 13

Nombre de services de soins impactés : 9

Nombre d'EHPAD impactés : 2

Nombre de personnes mobilisées : 280

Nombre d'animateurs : 5

Nombre d'observateurs : 33

Nombre de stimuli envoyés : +1 200

Durée de l'exercice : 7 h



Stéphane Bouchut, directeur opérationnel de Tilwit



Pierre-Alain Jullien, responsable sécurité opération



Odile Guigue, cadre de santé d'un service pilote du CH d'Arles



Katia Azri, cadre supérieur de santé à Aix-en-Provence

Assurer la continuité des soins en mode dégradé

Dans les établissements, les équipes doivent s'adapter rapidement. Au centre hospitalier d'Arles ou à Aix-en-Provence, les soignants activent des procédures dites « dégradées » pour maintenir l'activité malgré la perte des outils numériques.

« On peut assurer la continuité des soins sans problème grâce au dossier papier », explique Odile Guigue, cadre de santé au CH d'Arles, qui insiste sur l'importance de la traçabilité des traitements et des transmissions entre équipes.

Pour les directions hospitalières, l'exercice met en évidence la nécessité d'une coordination étroite entre les services médicaux, techniques et administratifs. « Les stimuli étaient très réguliers, ce qui a rendu la cellule de crise particulièrement active », souligne Florian Mormon, directeur des affaires médicales au CH d'Arles.

S'entraîner pour mieux anticiper les crises

Au-delà de la simulation elle-même, l'objectif est avant tout pédagogique. « L'exercice, c'est le nerf de la guerre »,



Florian Mormon, directeur des affaires médicales au CH d'Arles

insiste Katia Azri, cadre supérieur de santé à Aix-en-Provence, qui évoque la difficulté d'organiser ce type de formation sans perturber les services, mais aussi l'adhésion des équipes lorsqu'elles y participent.

Pour Tilwit, ces exercices s'inscrivent dans une logique de « formation-action ». Les équipes sont accompagnées en temps réel pour appliquer leurs procédures et mieux comprendre les situations auxquelles elles pourraient être confrontées.

Les premiers résultats sont jugés encourageants : les cellules de crise se sont mises en place en moins de 40 minutes en moyenne, un délai considéré comme satisfaisant.

L'exercice permet également de mesurer l'impact du temps sur la gestion d'une crise. En simulant une situation à J+10, avec un changement de responsable, les organisateurs ont pu observer les écarts dans la prise de décision et l'organisation.

Un enjeu stratégique pour les hôpitaux

Face à la multiplication des cyberattaques dans le secteur de la santé, ces simulations deviennent un outil stratégique. Elles permettent d'identifier les failles organisationnelles, d'améliorer la coordination et de préparer les équipes à des situations critiques où chaque minute compte.

Pour les organisateurs, la prochaine étape sera de multiplier les exercices à l'échelle de chaque établissement afin de renforcer les compétences locales.

Car si l'attaque était fictive, les enjeux, eux, sont bien réels : garantir la continuité des soins, protéger les données des patients et assurer la résilience d'un système hospitalier de plus en plus dépendant du numérique.