

Cybersécurité, actions et positionnement de l'ARS

Pierre LEROUX, *PhD*

Responsable Service Systèmes d'Information de Santé & Cybersécurité

Direction Stratégie et Parcours

241 rue Garibaldi | CS 93383 | 69418 Lyon CEDEX 03

pierre.Leroux@ars.sante.fr Tél. 04 2786 5620 – 07 7863 2734

Le contexte

Etablissement + données de santé = cible parfaite !

Chaque établissement de santé est une cible potentielle avec une probabilité d'être attaqué quasi-certaine :

- En 2023, 11,4% des attaques traitées par l'ANSSI (Agence Nationale de Sécurité des systèmes d'information) concernaient le secteur de la santé
- Majoritairement pour des **demandes de rançon**
- Risque dans le contexte international tendu de subir des attaques massives à des fins de **désorganisation des services publics** (ex. mise en alerte JOP 2024)

Pour un hôpital victime de cyberattaque, c'est :

- Entre 6 semaines et 6 mois (voire ++ ex.) avant de reprendre une activité « normale »
- Entre 300k€-3M€ (voire ++) de coût (remise en état, perte d'exploitation, ...)
- Une charge mentale très forte sur le personnel (informaticiens comme soignants)
- Des risques juridiques par perte de chance des patients
- Une image de marque dégradée créant la défiance des usagers

Les risques pesant sur les établissements

- **Obsolescence des systèmes :**
83 % d'entre eux utilisent des logiciels dépassés, plus vulnérables aux attaques.
- **Multiplication des terminaux :**
Prolifération des dispositifs médicaux et non médicaux connectés = prolifération de ces terminaux, fait de chaque appareil une cible potentielle pour les cybercriminels
→ intégration du biomédical dans les processus de la DSI (achat/installation, intégration de la sécurité dans les projets, etc.) et gouvernance commune.
- **Contraintes budgétaires et pénurie de talents :**
Peut entraîner un temps de réponse aux menaces plus important ou une découverte tardive d'une menace déjà nichée dans le réseau
- **Essor des soins à distance**
Ce passage à des modèles de prestation de soins décentralisés élargit la surface d'attaque et rend la sécurisation de l'ensemble du réseau beaucoup plus fastidieuse
- **Complexité croissante des environnements informatiques médicaux :**
Approche par solutions en silos, *best-of-breed*, empilant des solutions de sécurité pas entièrement intégrées

Fonctions et dépendances critique d'un hôpital

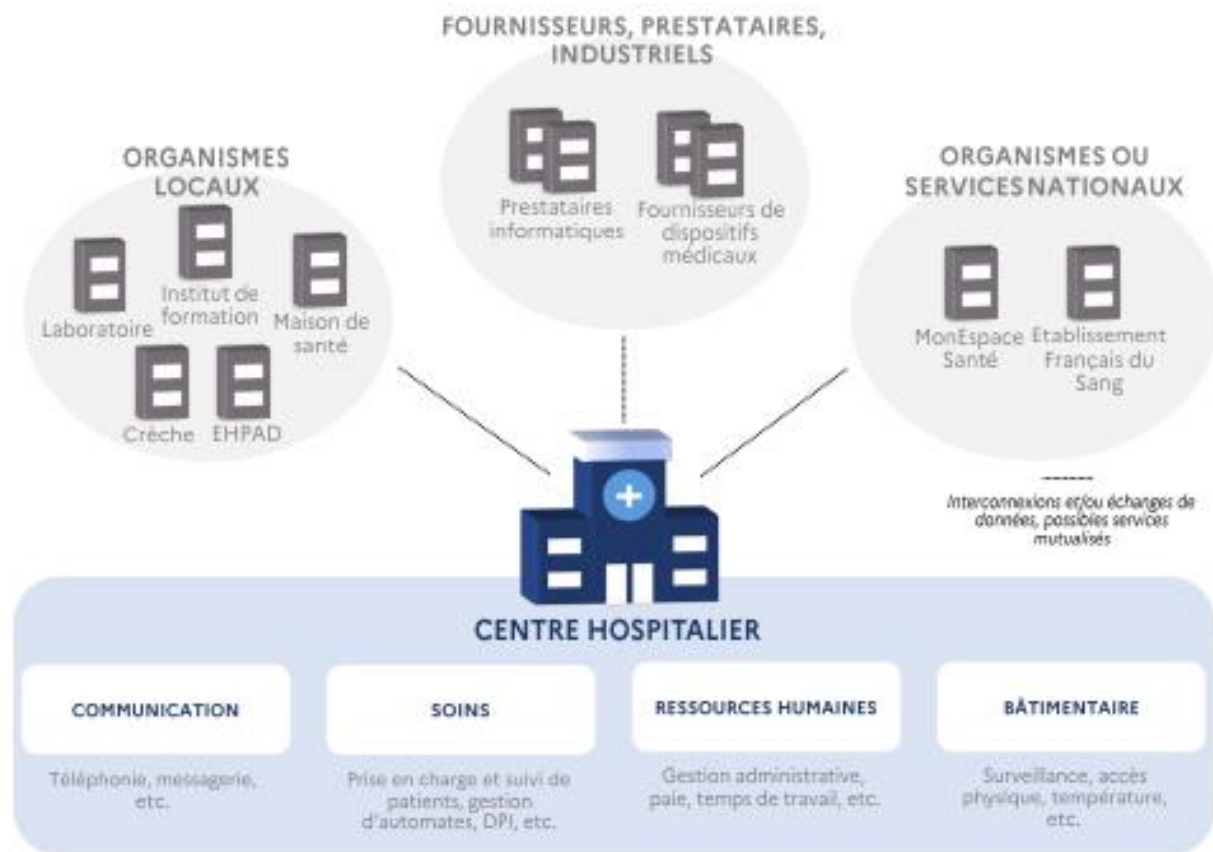


FIGURE 2 – Quelques fonctions et dépendances critique d'un Centre Hospitalier typique

La feuille de route fixée aux ARS

L'ARS doit superviser les actions des ES

Suite à plusieurs attaques majeures médiatisées : Dax, Villefranche s/ Saône, ...

→ Prise de conscience politique sur la nécessité d'agir

→ feuille de route fixée aux ARS par le HFDS du MSS le 30 juillet 2021 ;

Fixe environ 25 mesures aux ARS.

Il s'agit essentiellement de coordonner et de contrôler les actions relevant de la **responsabilité des établissements** (présenté ci-après).

Les ES **sanitaires** sont prioritairement impliqués, puis dans un 2nd temps, le secteur médico-social est concerné.

Une attention particulière est à porter aux CH supports de GHT désignés par décret « **Opérateurs de Services Essentiels (OSE)** » (Directive européenne NISV1). Elle leur impose des obligations particulières dont un parcours cybersécurité piloté par l'ANSSI.

Les actions prioritaires pédagogiques

Sensibiliser le Comité de direction

- Faire intervenir en CoDir le Responsable sécurité de l'ES pour faire prendre conscience des menaces et de leurs conséquences
- Définir et adopter un plan d'actions interne

Sensibiliser les utilisateurs : acculturation aux bonnes pratiques

- Inclure des clauses de vigilance dans la charte interne d'usage du SI
- Afficher les flyers du kit national « TousCyberVigilants » aux endroits stratégiques
- Organiser des actions de formation, jeux de rôles, ...
- Organiser des campagnes de tests (simulation de phishing, ...)



Les actions prioritaires préventives en ES

- Rédiger le **Plan de Continuité et Reprise d'Activité** (PCRA)
- Réaliser des exercices de continuité d'activité : passage en mode procédures dégradées simulant une indisponibilité du SI
- Atteindre le niveau de maturité des prérequis HOP'EN/SUN-ES et en particulier
 - Désigner un Responsable sécurité des SI opérationnel (formation, certification, ...)
 - Réaliser une analyse de risques actualisée associée à un plan de traitement
- Faire réaliser les audits proposés par l'ANSSI et de cyber surveillance du Cert-Santé
- Connaître / diffuser la procédure de signalement (EIG)
- Rédiger les procédures de passage en cellule de crise et mise en sécurité, validées par le CoDir
- Constituer les équipes d'intervention (interne et/ou prestataires) de réponse à incident (PRIS)
- Déployer un mode de communication sécurisé

Les principaux freins recensés

- ✓ Constat général : les Directions générales des ES
 - ne prennent pas la mesure du risque et du rôle de pilotage qu'elles devraient jouer
 - laissent le responsable sécurité se débattre dans ses difficultés et n'affectent pas les budgets a minima estimés nécessaires.
- ✓ Les responsables sécurité SI sont un vivier quantitativement faible :
 - marché de l'emploi très **concurrentiel**,
 - **manque d'attractivité** des emplois hospitaliers (1 RSSI/GHT).
- ✓ Pas de budgets fléchés sur ce champ d'intervention par le ministère, malgré les priorités énoncées... sauf ...

