L'hôpital et l'intelligence ordinaire

Société éditrice
Special Partner
Siège social
84 Avenue de la République
75011 Paris
Directeur de publication
Xavier Lebranchu
xavier.lebranchu@dsih.fr
Rédaction
redaction@dsih.fr
Coordinatrice générale
Hassania Ahrad
hassania.ahrad@dsih.fr
Rédacteurs
Fabrice Deblock
Pierre Derrouch
Pauline Nicolas
Contributeurs
Marguerite Brac de La Perrière
Christophe Cantin
Cédric Cartau
Félix Mamoudy
Nicolas Schneider
Omar Yahia
Direction artistique
François Jaccard
Pour nous contacter
02 99 46 24 43
contact@dsih.fr
Abonnement
Tel. 02 99 46 24 43
Courrier :
84 avenue de la République
75011 Paris
Courriel : abonnement@dsih.fr
Tarif d'abonnement France
3 numéros par an, 64 euro TTC
Étranger : nous consulter
Cnil : 1436001
Inpi : 113813102
Dépôt légal : à parution
Impression : Corlet
Tirage : 4 000 ex
Issn : 2110-6827
Périodicité : Quadrimestrielle
Imprimé en France

PEFC 10-31-1510
FABRIQUÉ EN FRANCE

Le 31 mars 2026, le centre hospitalier Stell de Rueil-Malmaison a pris de plein fouet un ransomware. Trois jours plus tôt, le réseau de laboratoires Cerballiance et ses 700 sites annonçaient une fuite de données sensibles, la deuxième en moins d'un an.

Ces attaques récentes rappellent que la santé reste une cible privilégiée des hackers. Le Panorama de la cybermenace 2025 de l'ANSSI, publié le 11 mars 2026, l'atteste : 3e rang des secteurs les plus attaqués en France, hausse de 51 % des exfiltrations de données. Pour Vincent Strubel, directeur général de l'agence, la menace ne faiblit pas : «on est sur une marée haute qui perdure», tout en réfutant l'idée de «raz-de-marée».

Comme si cela ne suffisait pas, les hackers ont ouvert un autre front qui prend la forme d'une partie de poker menteur : l'ANSSI n'a confirmé que 80 revendications d'exfiltration de données, pour 196 incidents recensés.

Un coup de bluff peu rassurant en définitive : ces bravades révèlent en creux les fragilités des établissements, suffisamment vulnérables pour qu'on n'ait même plus besoin de les attaquer pour les compromettre ; il suffit de prétendre l'avoir fait pour provoquer une onde de choc réputationnelle.

Certes, le programme CaRE avait déjà montré de premiers résultats en 2025. Sur plus de 1 000 établissements audités au titre du premier volet, la part de ceux présentant une vulnérabilité majeure d'Active Directory avait chuté de 20 points entre mai 2024 et février 2025, tandis que l'exposition Internet critique reculait de 35 points entre août 2024 et janvier 2025.

Malgré ces progrès, la dette de fond demeure. Elle a été chiffrée par le rapport de la Cour des comptes du 3 janvier 2025 : 1,7 % du budget d'exploitation des établissements de santé publics et privés à but non lucratif était consacré en moyenne au numérique, contre 9 % dans la banque ; dans les hôpitaux publics, près de 20 % des postes de travail ont plus de sept ans ou un système d'exploitation hors maintenance ou obsolète, et 23 % des équipements réseau ne peuvent plus être mis à jour ou réparés en cas de panne. Le sous-investissement y est qualifié de chronique.

Et c'est dans ce paysage que l'IA générative fait son nid. Selon le baromètre FHF « IA en santé : qui est le maître ? », 65 % des établissements publics déclarent déjà y recourir. Elle s'installe alors que les socles restent friables et que les obligations s'enchaînent : article 84 de la LFSS 2026 sur les systèmes d'aide à la décision médicale et à la dispensation pharmaceutique ; 6e cycle de certification HAS, qui intègre désormais des critères dédiés à l'IA ; règlement européen sur l'IA, dont une large part s'applique à compter du 2 août 2026.

Greffer de l'IA là-dessus, c'est un peu comme mettre un turbo sur une 4L.

Nettoyer les bases, documenter les flux, retirer les serveurs fantômes, durcir les annuaires, conditionner les projets neufs à la maîtrise de l'existant : avant l'intelligence artificielle, il faudrait peut-être retrouver l'intelligence ordinaire.

Bonne lecture

Pierre Derrouch