NOTE DE VULNÉRABILITÉ SECTORIELLE

Exposition cyber du secteur santé

Panorama des vulnérabilités 2026 -- Risques, incidents et recommandations pour les établissements de santé, EHPAD et structures médico-sociales

Référence	Date	Périmètre	Diffusion
L70C-NVS-2026-01	Avril 2026	France -- Secteur santé & médico-social	**Libre -- Reproduction autorisée avec mention de source**

Le secteur de la santé est devenu en 2025-2026 la cible prioritaire des groupes cybercriminels en France et en Europe. La combinaison de données à haute valeur (dossiers patients, données génomiques, informations financières), de systèmes informatiques vieillissants et de contraintes opérationnelles qui rendent les interruptions intolérables crée un profil de vulnérabilité structurellement attractif pour les attaquants.

Cette note dresse un panorama objectif de l'exposition cyber du secteur, à destination des directeurs d'établissement, responsables informatiques, RSSI et assureurs. Elle ne constitue pas un audit de sécurité mais une synthèse analytique fondée sur les incidents documentés et les données publiques disponibles en avril 2026.

01 Le secteur santé en chiffres -- État de la menace 2026

83
établissements de santé cyberattaqués en France en 2025
+31% vs 2024

22j
durée moyenne de perturbation après incident ransomware
jusqu'à 6 mois dans les cas graves

4,2M€
coût moyen d'un incident majeur (France, 2025)
hors préjudice patients

68%
des établissements sans RSSI dédié (enquête FSSI 2025)
PME & structures < 500 lits

Sources : ANSSI Panorama de la cybermenace 2025, CERT Santé, FSSI -- Bilan annuel 2025. Chiffres illustratifs construits à partir de données publiques agrégées.

02 Paysage des menaces -- Acteurs et modes opératoires

Trois types de menaces dominent le paysage cybercriminel ciblant le secteur santé en 2026. Leur compréhension est indispensable pour dimensionner les investissements de protection.

Type	Acteurs	Objectif	Fréquence

Ransomware double extorsion	Groupes criminels (LockBit 3.0, Medusa, BlackBasta)	Rançon, blocage, revente données	Hebdomadaire en Europe
Exfiltration données patients	Groupes APT (Chine, Russie) + revendeurs	Espionnage, revente (dossiers = 250 EUR/unité)	Continue, souvent non détectée
Attaque infrastructure critique	Groupes hacktivistes, APT étatiques	Déstabilisation, signal politique	Pics lors de contexte géopolitique
Fraude interne et social engineering	Acteurs opportunistes, initiés	Détournement financier, accès	Permanente, sous-estimée

03 Cartographie des vulnérabilités sectorielles

Les établissements de santé présentent un profil de vulnérabilité structurellement défavorable, combinant contraintes techniques héritées et pression opérationnelle permanente. Les sept vulnérabilités suivantes sont classées par niveau de criticité observé dans les incidents de 2025-2026.

V1 Équipements biomédicaux non patchés connectés au réseau — CRITIQUE

Les dispositifs médicaux connectés (scanners, pompes à perfusion, moniteurs) tournent sur des OS non maintenus (Windows XP, 7) et ne peuvent être mis à jour sans validation fabricant -- procédure longue et coûteuse. Ils constituent des points d'entrée persistants sur le réseau de soins.

Vecteur : Exploitation directe depuis le LAN ou via un équipement bureautique compromis

V2 Absence de segmentation réseau IT/OT médical — CRITIQUE

Dans la majorité des structures auditées, le réseau administratif, le réseau de soins et les équipements biomédicaux partagent le même segment réseau. Un ransomware pénétrant par un poste bureautique peut atteindre les équipements de soins en quelques minutes.

Vecteur : Propagation ransomware, accès non autorisé aux équipements de soins

V3 Accès distants VPN sans MFA pour les praticiens et prestataires — CRITIQUE

La télémédecine et la maintenance à distance des équipements ont multiplié les accès distants. La majorité de ces accès ne sont protégés que par un mot de passe, sans second facteur. Les comptes prestataires (infogérance, maintenance biomédicale) sont particulièrement exposés.

Vecteur : Phishing ciblé, credential stuffing, attaque sur comptes prestataires

V4 Sauvegardes insuffisantes ou non testées — ELEVEE

Les plans de sauvegarde existent mais ne respectent pas la règle 3-2-1 dans 60% des cas. Les sauvegardes sont souvent sur le même réseau que la production et chiffrées simultanément lors d'une attaque ransomware. Les tests de restauration sont rarement conduits.

Vecteur : Chiffrement simultané lors d'attaque, incapacité de restauration

V5 Messagerie et pièces jointes non filtrées — ELEVEE

Le phishing reste le vecteur d'entrée numéro un. Les solutions de filtrage des pièces jointes et des URLs malveillantes sont absentes ou insuffisantes dans de nombreuses structures. La formation des utilisateurs est ponctuelle et non évaluée.

Vecteur : Phishing, spearphishing ciblé sur personnels soignants ou administratifs

V6 **Gestion des identités et accès privilégiés insuffisante** ELEVEE

Les comptes partagés (médecins de garde, infirmières de nuit) sont courants pour faciliter la continuité des soins. Les comptes à privilèges (administrateurs SI) ne sont pas gérés par une solution PAM. Les mots de passe par défaut restent présents sur certains équipements.

Vecteur : Mouvement latéral, élévation de privilèges, persistance attaquant

V7 **Dépendance à des prestataires informatiques de petite taille** MODEREE

De nombreux EHPAD et petites cliniques externalisent totalement leur informatique à des prestataires locaux dont la maturité cyber est variable. Une attaque sur le prestataire (attaque supply chain) peut se propager à l'ensemble de ses clients simultanément.

Vecteur : Attaque supply chain, compromission prestataire

04 Incidents marquants -- France et Europe 2025-2026

Les incidents suivants sont représentatifs des typologies observées. Les noms ont été anonymisés ou modifiés à des fins de démonstration.

Période	Type de structure	Nature de l'incident	Impact opérationnel
Jan. 2026	CHU régional (1 200 lits)	Ransomware LockBit -- 340 serveurs chiffrés	Déprogrammation 3 semaines, retour au papier 47
Nov. 2025	Réseau EHPAD (12 établissements)	Compromission prestataire infogérance -- propagation simultanée	Paralysie simultanée, données de 4 200 résidents
Sep. 2025	Clinique privée (180 lits)	Exfiltration silencieuse données patients (6 mois non détectée)	Notification CNIL, 8 200 patients concernés, plainte
Mar. 2025	GHT interdépartemental	Phishing DRH -- compromission AD -- ransomware 72h plus tard	Paie bloquée 3 mois, données RH de 1 400 agents
Juil. 2025	Laboratoire d'analyses (réseau régional)	Attaque supply chain via logiciel métier de l'éditeur	23 laboratoires simultanément paralysés, résultats

05 Recommandations prioritaires

Face à ce panorama, les recommandations suivantes sont classées par ordre de priorité et d'impact. Elles sont dimensionnées pour être réalistes dans le contexte budgétaire contraint des établissements de santé français.

R1

Segmenter immédiatement le réseau médical du réseau administratif

C'est la mesure à impact le plus élevé pour le coût le plus bas. Un VLAN dédié aux équipements de soins avec un firewall en coupure empêche la propagation d'une attaque bureautique vers les équipements critiques. Peut être réalisé en 1 à 3 semaines.

IMMEDIATE

R2

Déployer le MFA sur tous les accès distants sans exception

VPN praticiens, accès prestataires, messagerie web, applications métier en mode SaaS. Le MFA neutralise 99% des attaques sur les credentials volés. Coût marginal, déploiement en moins d'une semaine sur la majorité des solutions modernes.

IMMEDIATE

R3

Mettre en oeuvre la sauvegarde 3-2-1 avec copie hors réseau

3 copies, 2 supports différents, 1 hors site ET hors réseau de production. La sauvegarde connectée en permanence n'est pas une sauvegarde -- c'est une copie supplémentaire que le ransomware va chiffrer. Budget estimé : 5 000 à 20 000 EUR selon le volume de données.

IMMEDIATE

R4

Former l'ensemble du personnel aux risques phishing annuellement

Le phishing reste le vecteur numéro un. Une formation annuelle d'une heure, accompagnée d'un exercice de phishing simulé, réduit significativement le taux de clics malveillants. Coût : 5 à 15 EUR par personne. ROI immédiat.

COURT TERME

R5

Inventorier et isoler les équipements biomédicaux non patchables

Établir l'inventaire exhaustif des dispositifs médicaux connectés et leur version OS. Les équipements non maintenables doivent être isolés sur un segment réseau dédié sans accès Internet et avec accès entrant restreint aux seuls flux nécessaires.

COURT TERME

R6

Désigner un référent cybersécurité et souscrire une assurance cyber

Un RSSI à temps partiel ou mutualisé entre plusieurs établissements, combiné à une assurance cyber adaptée (couverture sinistre, frais de remediation, pertes d'exploitation), constitue le minimum viable pour une structure de taille moyenne. Coût combiné : 15 000 à 40 000 EUR/an selon la taille.

MOYEN TERME

06 Horizon 2027 -- Tendances à surveiller

IA offensive : les outils de génération de contenu permettent des campagnes de spearphishing ultra-personnalisées à grande échelle. Les personnels soignants, cibles de premier choix, recevront des emails indiscernables d'une communication hospitalière légitime.

Réglementation NIS2 : les hôpitaux et grandes cliniques entrent dans le périmètre NIS2 (entités essentielles). Des obligations de déclaration d'incident sous 24h et de mise en conformité s'imposent d'ici fin 2026. Les sanctions peuvent atteindre 2% du chiffre d'affaires annuel mondial.

Convergence IT/OT médicale : la montée en puissance des dispositifs médicaux connectés (IoMT -- Internet of Medical Things) va multiplier les surfaces d'attaque. Les robots chirurgicaux, perfusions intelligentes et équipements de surveillance deviendront des cibles privilégiées.

Tensions assurantielles : les assureurs cyber renforcent leurs critères d'éligibilité. Un établissement sans segmentation réseau, sans MFA et sans backup isolé se verra refuser la couverture ou se verra appliquer des primes prohibitives d'ici 2027.

À PROPOS DE CETTE NOTE

Cette note sectorielle est produite par Louis70 Conseil SAS dans le cadre de sa mission de sensibilisation aux enjeux de cybersécurité. Elle est fondée sur des sources ouvertes, des données publiques agrégées et l'expérience opérationnelle de ses consultants. Les chiffres cités sont illustratifs -- leur exactitude doit être vérifiée auprès des sources primaires (ANSSI, CERT Santé, FSSI).

Louis70 Conseil accompagne les établissements de santé, EHPAD et structures médico-sociales dans leurs démarches de diagnostic cyber, de mise en conformité et de formation. Premier échange toujours confidentiel, sans engagement.

L. Bonjean
Capitaine de frégate (h) -- Gérant Louis70 Conseil SAS -- SIREN 989 600 481