# MedinLux

THE MAGAZINE ABOUT HEALTH, MEDICINE & PHARMACY IN LUXEMBOURG

Numéro 50

MENSUEL
20 DÉCEMBRE 2025 - 20 JANVIER 2026

WWW.MEDINLUX.LU


Editeur responsable: FédérationMedical Network - 3 rue des Frères - 1541 Luxembourg

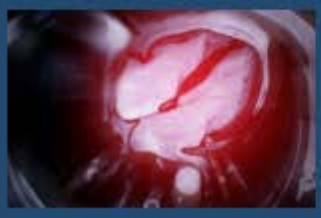
## Cybersécurité hospitalière: entre complexité technologique et mutualisation stratégique

Rencontre avec le Dr Paul Wirtgen

8

HWL 2025
**L'intelligence artificielle: une position pragmatique**

12



**Une étude sous la loupe STEMI avec atteinte pluritronculaire: faut-il traiter les lésions non coupables immédiatement ou attendre?**

23

# CYBERSÉCURITÉ HOSPITALIÈRE: ENTRE COMPLEXITÉ TECHNOLOGIQUE ET MUTUALISATION STRATÉGIQUE

INTERVIEW RÉALISÉE
PAR JEAN-POL LEBLON

**Dans un environnement de santé de plus en plus connecté, la protection des données patients et la continuité des soins reposent sur des infrastructures informatiques robustes. Le Dr Wirtgen, Directeur général du Centre Hospitalier du Nord (CHdN) et Président de Luxith, nous éclaire sur les défis uniques de la cybersécurité dans les hôpitaux luxembourgeois, de la mise en œuvre de la directive NIS2 aux impératifs budgétaires et humains.**

**PAUL WIRTGEN**
(CHDN – LUXITH)

## UN ENVIRONNEMENT IT D'UNE COMPLEXITÉ UNIQUE

**Pourquoi la cybersécurité représente-t-elle un défi si particulier pour le secteur hospitalier par rapport à d'autres secteurs critiques?**

En tant que président de Luxith, je suis heureux de pouvoir participer à la mutualisation de nombreux projets de cybersécurité pour les hôpitaux luxembourgeois. Parallèlement, en tant que directeur général du CHdN, je porte évidemment une responsabilité importante pour l'environnement IT et la digitalisation en général de notre hôpital.

Je tiens à souligner particulièrement que la cybersécurité ne peut être prise en charge que par une équipe constituée d'experts, internes et externes à l'hôpital! La digitalisation du secteur hospitalier est extrêmement complexe. Elle associe les éléments classiques de toute digitalisation (softwares, hardwares, réseaux) à des équipements médicaux techniques extrêmement nombreux et sophistiqués, qui comprennent des liens de plus en plus fréquents vers le réseau et la documentation hospitalière.

D'autre part, les différents types de prise en charge des patients varient beaucoup d'une spécialité à l'autre et demandent très souvent des softwares adaptés et spécifiques. L'environnement administratif est tout aussi complexe, allant de la logistique et la gestion des stocks à la facturation, sans oublier l'analyse de données via la BI (*Business Intelligence*). La multiplicité des systèmes IT est donc un challenge particulier pour assurer une cybersécurité la plus efficiente possible.

## STRATÉGIE, CONFORMITÉ ET MENACES ACTUELLES

**La directive NIS2 renforce les obligations de cybersécurité. Quels sont les défis prioritaires pour les hôpitaux luxembourgeois afin de se conformer à cette directive?**

La directive NIS2 exige de toutes les entités essentielles de réaliser de façon répétée des analyses de risque couvrant l'ensemble des systèmes d'information, et d'en déduire les priorités pour les actions de renforcement.

Les hôpitaux collaborent déjà depuis la directive NIS1 avec l'ILR (Institut Luxembourgeois de Régulation), qui est l'autorité compétente en matière de cybersécurité au Grand-Duché pour notre secteur. Dans ce cadre, Luxith favorise les échanges entre les spécialistes des différents hôpitaux, notamment grâce à ses groupes de travail réunissant les RSSI et les CIO. La mise en place de projets mutualisés est décidée par le Conseil de gérance de Luxith, et leur financement est assuré par la CNS après acceptation d'un contrat d'objectifs et de moyens.

**Concernant les menaces, quels types d'attaques sont les plus fréquents aujourd'hui? Avez-vous noté une recrudescence liée au contexte géopolitique?**

Le *phishing* constitue le type d'attaque principal auquel nous sommes confrontés. Quant au contexte géopolitique actuel, c'est une réponse difficile, mais je n'ai pas connaissance d'augmentation récente d'attaques spécifiques contre les hôpitaux du Grand-Duché en raison des tensions internationales.

**La rapidité d'accès aux données est vitale. Comment concilier cet impératif avec une sécurité maximale, notamment pour l'imagerie ou le dossier patient?**

Les exigences de disponibilité des examens médicaux obligent en effet à mettre en place des systèmes complexes de transmission de données par des voies sécurisées. Cela inclut des données cryptées, hébergées sur des systèmes redondants et les mieux sécurisées possible.

Un exemple concret est l'archive nationale de l'imagerie médicale, appelée ANIM, dont les images peuvent également être accédées de manière sécurisée à partir du DSP (Dossier de Soins Partagé) national.

**Comment la résilience de ces systèmes est-elle testée?**

Des tests ou simulations d'attaques sont généralement organisés par l'ILR ou le HCPN (Haut-Commissariat à la Protection Nationale), parfois en coordination avec des tests «grandeur nature» menés à l'échelle européenne.

## LE FACTEUR HUMAIN ET LES MOYENS

**La sophistication des menaces exige des compétences pointues. Le Luxembourg dispose-t-il de ressources suffisantes et comment gérez-vous la formation des équipes?**

Les équipes de Sécurité de l'Information des hôpitaux sont en général sous la responsabilité d'un RSSI (Responsable de la Sécurité des Systèmes d'Information) ou CISO, qui dirige son équipe d'experts. Ces équipes internes réalisent des actions de sensibilisation régulières auprès du personnel médico-soignant et administratif (séances d'information, newsletters dédiées, etc.).

Cependant, les dotations des hôpitaux pour les professionnels IT et cybersécurité proviennent du budget hospitalier négocié avec la CNS. La croissance nécessaire de ces budgets pour répondre aux besoins du terrain est difficilement compatible avec la maîtrise des coûts imposée par l'enveloppe budgétaire globale.

## PERSPECTIVES D'AVENIR

**Pour conclure, quels sont, selon vous, les défis majeurs pour les 2 à 5 prochaines années en matière de cybersécurité hospitalière?**

Je résumerais les perspectives d'avenir et les besoins en innovation par quatre axes majeurs:

- Le défi des ressources humaines: les besoins sont importants et nécessiteront des budgets RH accrus pour attirer et retenir les talents.
- L'évolution des coûts technologiques: les nouvelles technologies demandent des budgets annuels de plus en plus élevés, notamment parce qu'elles se présentent souvent sous forme de «locations» de services (*Software as a Service*).
- La mutualisation accrue: les technologies seront développées de plus en plus de façon mutualisée afin de progresser de manière concertée et cohérente pour l'ensemble du secteur.
- L'intégration de l'innovation: de nouvelles technologies, comme l'Intelligence Artificielle (IA) et le Cloud, sont désormais intégrées dans les stratégies du secteur de la santé et doivent être sécurisées. ◘