# CYBERCAMP Santé #5

Paris Expo Porte de Versailles

26 mars 2026

*Cybersécuriser les établissements, protéger les patients*

# CYBERCAMP Santé #5

Paris Expo Porte de Versailles
26 mars 2026

**Cinq éditions.**
**Plus de 500 participants depuis 2020.**
**Et une conviction qui ne s'est jamais démentie :**
**la cybersécurité en santé n'est pas un sujet informatique**
**– c'est un sujet de gouvernance, de responsabilité,**
**et, fondamentalement, de soin.**
**Cette synthèse restitue l'essentiel de chaque séquence**
**du l'édition du 26 mars 2026.**

**Publication**
CyberCamp Santé #5 – Synthèse officielle de la 5e édition
26 mars 2026 – Paris Expo Porte de Versailles

Éditeur responsable
Doshas Consulting
128 rue La Boétie – 75008 Paris
RCS Paris 794 993 055
contact@doshas-consulting.com
www.cybercampsante.org

**Directeur de publication**
Didier AMBROISE, Fondateur Doshas Consulting

**Rédaction**
La synthèse a été rédigée à partir des interventions, keynotes et tables rondes du 26 mars 2026. Elle restitue fidèlement les propos tenus par chaque intervenant, dans le respect de leur pensée.
Intervenants cités : Thomas Aubin, Patrice Bigeard, Gilles Calmes, Émilie Danglades-Perez, Arthur Dauphin, Florence Eon-Jaguin, Steven Garnier, Quentin Le Thiec, Philippe Loudenot, Mireille Massot, Guillaume Mithieux, Daniela Parrot, Sandrine Roussel.

**Illustration et facilitation graphique**
Laëtitia Bernoux – Facilitatrice graphique
Photos : Tech4Health – Quinze mai

**Conception graphique & mise en page**
Studio Bleu Canari

**Copyright**
© CyberCamp Santé / Doshas Consulting – 2026.
Tous droits réservés.
Reproduction partielle autorisée sous réserve de mention explicite de la source :
« CyberCamp Santé #5 – Synthèse officielle, Doshas Consulting, mars 2026 »
Reproduction intégrale soumise à autorisation préalable de l'éditeur.

**Dépôt légal**
Mai 2026 – ISBN : 978-2-494611-02-3

**Prix**
10€

**Contact presse & partenariats**
contact@doshas-consulting.com
01 84 20 07 83

# Sommaire

# Les intervenants

Didier **Ambroise**

Thomas **Aubin**

Patrice **Bigeard**

Gilles **Calmes**

Émilie **Danglades Perrez**

Arthur **Dauphin**

Florence **Eon-Jaguin**

Steven **Garnier**

Quentin **Le Thiec**

Philippe **Loudenot**

Mireille **Massot**

Guillaume **Mithieux**

Danièla **Parrot**

Sandrine **Roussel**

# La situation l'exige

Didier AMBROISE — Doshas Consulting

Le CyberCamp Santé n'a jamais été conçu comme un colloque de plus. Depuis la première édition, l'ambition est la même : réunir celles et ceux qui subissent la menace, qui la documentent, qui la régulent, et qui en sortent – pour que les uns et les autres repartent avec quelque chose à faire différemment.

La cinquième édition s'ouvre dans un contexte qui n'a pas attendu le programme pour se détériorer. Depuis la précédente édition, des établissements ont été mis à genoux. Des patients ont vu leurs soins différés, leurs données exposées sur le dark web. Des directeurs généraux ont géré leur crise sans messagerie, sans accès aux dossiers, parfois sans téléphone. Des ingénieurs biomédicaux ont découvert que leur scanner dépendait d'un accès VPN jamais sécurisé.

Comprendre, débattre, décider : telle est la structure de la matinée. D'abord les chiffres et les faits – panorama des menaces, retour d'expérience opérationnel, cadre réglementaire. Puis les questions difficiles : qui est responsable quand tout tombe ? Qui paie ? Et comment, concrètement, on protège les patients ?

Un fil rouge traverse l'ensemble. La cybersécurité en santé n'est pas un sujet de DSI ou de RSSI. C'est un sujet de direction générale. C'est, fondamentalement, un sujet de soin. Tout le reste en découle.

> « La cybersécurité en santé n'est pas un sujet informatique. C'est un sujet de gouvernance. C'est un sujet de direction. C'est, fondamentalement, un sujet de soin. »


## Allocution d'ouverture

# Ce qui progresse, ce qui inquiète

Steven GARNIER — Directeur cybersécurité, Agence du Numérique en Santé

La trajectoire du secteur sanitaire est « plutôt positive », reconnaît Steven Garnier. Le programme CaRE commence à porter ses fruits. La veille proactive du CERT Santé monte en puissance. Les exercices de crise se multiplient. Les établissements les plus avancés ont intégré la cybersécurité dans leur gouvernance.

Mais la trajectoire est inverse là où l'attention manque encore : le médico-social, les laboratoires d'analyse médicale, et surtout la médecine de ville. Ce sont désormais ces secteurs qui concentrent une part croissante des incidents graves – et la presse en a donné des exemples récents, trop nombreux.

Sur le plan réglementaire, la direction est claire. La vague 2 du Ségur Numérique impose pour la première fois des exigences de sécurité aux éditeurs – absence de vulnérabilités critiques, attestée par test d'intrusion. NIS2 va structurer un vocabulaire commun et des règles partagées entre toutes les entités du secteur et leurs sous-traitants. Le Cyber Resilience Act, avec ses étapes clés à l'automne 2026 et en 2027, doit enclencher une dynamique de security by design chez les éditeurs de logiciels.

> « Le port de la ceinture de sécurité, d'abord adopté pour éviter l'amende, est aujourd'hui un réflexe de survie. La réglementation cyber a vocation à jouer le même rôle dans les années qui viennent. »
>
> Steven Garnier, reprenant l'exemple du DG de l'ANSSI


**Le message de clôture de cette allocution est direct : n'attendons pas que le cadre s'impose. La menace est déjà là.**

# Les chiffres 2025 – en avant-première

Quentin LE THIEC — Expert cybersécurité, CERT Santé (ANS)

Chaque année, le CyberCamp Santé bénéficie d'une exclusivité : les chiffres du CERT Santé avant la publication officielle du rapport annuel (à lire ici). En 2025, le tableau est nuancé – et mérite d'être lu sans raccourci.

| Indicateur | Valeur / observation |
|---|---|
| **Déclarations totales** | 764 — en hausse (biais de surveillance : obligation légale de déclarer) |
| **Interventions réelles (vrais incidents)** | 71 — légère baisse vs 75 l'an passé |
| **Impact catastrophique sur le soin** | Environ 10 sur 71 |
| **Origine malveillante** | 53 % |
| **Compromission du SI** | 62 % |
| **Compromission de boîtes mail** | 46 % |
| **Audits réalisés (2024)** | 461 (pic JO 2024), stabilisation en 2025 avec le programme CaRE |

| | | | |
|---|---|---|---|
| **71** *interventions majeures* | **53** *d'origine malveillante* | **2** *à impact catastrophique sur le soin* | **461** *audits réalisés en 2024* |

Le nombre de déclarations progresse – biais de surveillance oblige : les établissements savent qu'ils doivent notifier, et ils le font davantage. Mais le nombre d'interventions réelles baisse légèrement, à 71, contre 75 l'année précédente. C'est à la fois un signe que la veille proactive du CERT Santé commence à stopper des attaques en amont – et un rappel que les chiffres reflètent avant tout ce qui est déclaré, principalement par le secteur sanitaire public.

L'évolution de la menace est plus préoccupante. Avant 2022, le vecteur principal était l'exploitation de logiciels non à jour. Depuis, c'est le vol de d'informations d'identification qui domine : des logins et mots de passe professionnels synchronisés sur un navigateur personnel, récupérés via un PC familial contaminé par un logiciel cracké et téléchargé par un adolescent. La chaîne est banale, le résultat est dévastateur. Quentin Le Thiec est sans détour sur les responsabilités : quelques éditeurs qui livrent des applications où un praticien peut accéder aux dossiers de tous les patients – pas seulement les siens – commettent une faute de conception. Certains établissements qui ne testent pas leurs solutions en production laissent des portes ouvertes. Et les soignants qui utilisent leur messagerie perso pour des données professionnelles peuvent constituer le maillon que les attaquants recherchent.

> « En 2025, les incidents commencent encore par des erreurs basiques : comptes VPN ouverts, mots de passe triviaux, absence de MFA. L'outillage progresse – la surface humaine reste la principale vulnérabilité. »
>
> Quentin Le Thiec, CERT Santé

**Pour 2026, le CERT Santé annonce une évolution de son offre de services, avec des micro-services d'audit en remplacement du format traditionnel – pour mieux s'adapter à la diversité des établissements et à la réalité de leurs contraintes.**

# Armentières : bilan deux ans après l'attaque

Thomas AUBIN — RSSI GHT Hôpitaux Publics Grand Lille · Président Club RSSI Santé


Il est rare qu'un retour d'expérience soit présenté deux ans après l'événement. C'est précisément ce qui lui donne sa valeur.
Thomas Aubin ne parle pas de ce qu'il a vécu dans le feu de l'action – il parle de ce à quoi Armentières ressemble aujourd'hui, de ce qui reste ouvert, de ce qui ne reviendra jamais tout à fait comme avant.
La nuit du 10 au 11 février 2024, un dimanche, les imprimantes du Centre Hospitalier d'Armentières se mettent à cracher en boucle le même message : la revendication de l'attaquant.
95 % du parc informatique est chiffré en quelques heures, via une GPO qui a circulé sur l'Active Directory sans que personne ne la voie passer.
La porte d'entrée ? Un compte VPN compromis en décembre 2023, jamais détecté, jamais fermé.

**CHIFFRAGE DU COÛT TOTAL : 2,9 M€**

| Poste | Montant |
|---|---|
| Perte de recettes (activité réduite) | 1 400 000 € |
| Surcoûts informatiques et IT (forensic, reconstruction) | 850 000 € |
| Surcoûts RH (heures sup, renforts CHU Lille, gardes) | 640 000 € |

**2,9 M€** *coût total de la crise*

**57 h** *fermeture des urgences*

**230 000** *patients concernés par la fuite de données*

**6 mois** *pour reconstruire le SI*

La gestion de crise a mobilisé une équipe SI passée de 6 à 30 personnes en quelques heures, avec un couloir sécurisé par des agents de sécurité aux deux extrémités pour filtrer les accès. 546 actions ont été référencées dans le plan post-crise. La cellule de crise s'est réunie deux fois par jour au plus fort de l'incident, avant de se cadencer progressivement jusqu'à devenir mensuelle.
Thomas Aubin insiste sur la gestion du temps long. On ne sort pas d'une cyberattaque en deux semaines. Armentières a officiellement fermé sa cellule de crise en janvier 2025 – onze mois après l'attaque. Certains sujets sont encore ouverts aujourd'hui.

Les équipes ont tenu pendant la crise – absentéisme en baisse, turnover stoppé, solidarité totale. Puis, au premier trimestre 2025, les arrêts maladie ont remonté. La fatigue, le stress post-traumatique, ont eu leur temps de latence.

L'établissement a choisi une transparence totale sur les causes : une documentation interne volée avait permis à l'attaquant de comprendre le plan de sauvegarde et de le saborder dix jours avant le déclenchement. Il lisait les docs. Il avait le temps. Le cas d'Armentières, lui, n'avait pas de système de détection capable de l'identifier.

> « Il y a un avant cyberattaque et un après cyberattaque. Ce marqueur-là, on ne l'efface pas. On reconstruit – pas à l'identique, parce qu'on en a profité pour corriger ce qui aurait dû l'être depuis longtemps. Mais ça ne revient jamais exactement comme avant. »
>
> Thomas Aubin, RSSI GHT Grand Lille

**Le message pour la salle est sans ambiguïté : évaluer, investir, cartographier. Ne pas attendre l'attaque pour savoir ce qu'il y a dans son SI. Et ne pas mésestimer la cinétique de crise – ni pour l'organisation, ni pour les hommes et les femmes qui la traversent.**

# Le millefeuille réglementaire – ce qui arrive, ce qui tarde

Me Émilie DANGLADES-PEREZ — Simmons & Simmons

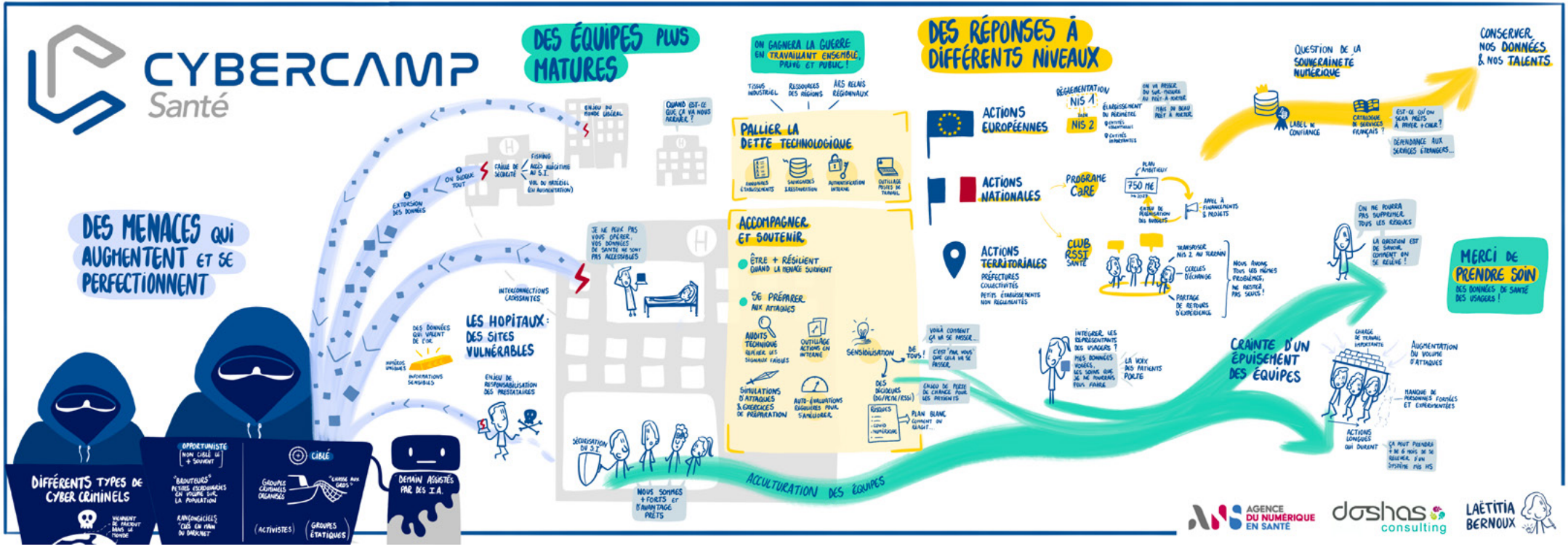
La comparaison s'impose d'elle-même : il y a quelques années, les acteurs de santé ont traversé la mise en conformité RGPD. Aujourd'hui, c'est la conformité cybersécurité qui s'impose – avec quatre textes majeurs qui se superposent, chacun avec ses délais, ses autorités et ses sanctions. NIS2 est le texte central. Il élargit le périmètre des entités concernées — hôpitaux, laboratoires d'analyse, certains fabricants de dispositifs médicaux – et impose une obligation de moyens continue : analyse des risques renouvelée, plan de gestion des incidents testé, sécurisation de la chaîne fournisseurs. Les amendes peuvent atteindre 10 millions d'euros, et la directive prévoit une mise en cause personnelle du dirigeant en cas de manquement grave. La transposition française n'est pas encore publiée – mais l'argument du « pas encore obligatoire » a une date d'expiration très proche.

Le Cyber Resilience Act change les règles pour les éditeurs : security by design, gestion obligatoire des vulnérabilités, patches à disposition des clients. Le Digital Omnibus simplifie les notifications d'incidents en créant un point de contact unique, ce qui devrait considérablement soulager les DPO qui jonglent aujourd'hui entre CNIL, ANSSI et autorités sectorielles.

> « La conformité, ça ne se fait pas le jour où le texte est transposé. Ça se prépare maintenant, avec une équipe multidisciplinaire, autour de la table, en se demandant par quoi on commence. »
>
> Me Émilie Danglades-Perez

L'Espace Européen des Données de Santé (EEDS), enfin, est l'horizon 2029 – l'interopérabilité des systèmes à l'échelle du continent, la réutilisation des données de santé pour le soin et la recherche. La France, avec sa plateforme des données de santé, a une longueur d'avance, qu'il convient de conserver.


**Conseil pratique, répété tout au long de l'intervention : lire les contrats des sous-traitants. Les faire auditer. Et si on ne comprend pas ce qui est écrit, trouver quelqu'un qui comprend.**


CYBERCAMP
Santé
DES ÉQUIPES PLUS MATURES
ON GAGNERA LA GUERRE EN TRAVAILLANT ENSEMBLE, PRIVÉ ET PUBLIC !
TISSU INDUSTRIEL
RESSOURCES DES RÉGIONS
ARS RELAIS RÉGIONAUX
PALLIER LA DETTE TECHNOLOGIQUE
ACCOMPAGNER ET SOUTENIR
ÊTRE + RÉSILIENT QUAND LA MENACE SURVIENT
SE PRÉPARER AUX ATTAQUES
AUDITS TECHNIQUE
OUTILLAGE ACTIONS EN INTERNE
SENSIBILISATION
SIMULATIONS D'ATTAQUES & EXERCICES DE PRÉPARATION
AUTO-ÉVALUATIONS ESSENTIELLES POUR S'AMÉLIORER
DES DISCOURS (DG/PCME/RSSI)
PLAN BLANC
DES RÉPONSES À DIFFÉRENTS NIVEAUX
ACTIONS EUROPÉENNES
RÉGLEMENTATION
NIS 1
NIS 2
ÉLARGISSEMENT DU PÉRIMÈTRE
ENTITÉS ESSENTIELLES
ENTITÉS IMPORTANTES
ON VA PASSER DU SUR-MESURE AU PEUT-ÊTRE TROP À FAIRE
TROP DE BLEU PEUT À FAIRE
ACTIONS NATIONALES
PROGRAMME CaRE
PLAN AMBITIEUX
750 M€
CENTRE DE RÉALISATION DES BUDGETS
APPEL À FINANCEMENTS & PROJETS
ACTIONS TERRITORIALES
PRÉFECTURES
COLLECTIVITÉS
PETITS ÉTABLISSEMENTS NON RÉGLEMENTÉS
CLUB RSSI SANTÉ
TRANSPOSER NIS 2 AU TERRAIN
CERCLES D'ÉCHANGE
PARTAGE DE RETOURS D'EXPÉRIENCE
NOUS AVONS TOUS LES MÊMES PROBLÈMES, NE RESTEZ PAS SEULS !
QUESTION DE LA SOUVERAINETÉ NUMÉRIQUE
LABEL DE CONFIANCE
CATALOGUE DE SERVICES FRANÇAIS ?
EST-CE QU'ON SERA PRÊTS À PAYER + CHER ?
DÉPENDANCE AUX SERVICES ÉTRANGERS...
CONSERVER NOS DONNÉES & NOS TALENTS
DES MENACES QUI AUGMENTENT ET SE PERFECTIONNENT
ENJEU DU MONDE LIBÉRAL
QUAND EST-CE QUE ÇA VA NOUS ARRIVER ?
FAILLE DE SÉCURITÉ
FISHING
ACCÈS MALVEILLANTS AU S.I.
VOL DU MESSIEL (EN AUGMENTATION)
1 ON BLOQUE TOUT
2 EXTORSION DES DONNÉES
JE NE PEUX PAS VOUS OPÉRER, VOS DONNÉES DE SANTÉ NE SONT PAS ACCESSIBLES
INTERCONNECTIONS CROISSANTES
LES HOPITAUX : DES SITES VULNÉRABLES
DES DONNÉES QUI VALENT DE L'OR
NUMÉROS UNIQUES
INFORMATIONS SENSIBLES
ENJEU DE RESPONSABILISATION DES PRESTATAIRES
SÉCURISATION DU S.I.
NOUS SOMMES + FORTS ET D'AVANTAGE PRÊTS
VOILÀ COMMENT ÇA VA SE PASSER...
C'EST CRA VOUS QUE CELA VA SE PASSER
BE TOUS !
ENJEU DE PIÈCE DE CHANCE POUR LES PATIENTS
INTÉGRER LES REPRÉSENTANTS DES USAGERS ?
MES DONNÉES VOLÉES, LES SOINS QUE JE NE RECEVRAI POUR FAIRE
LA VOIX DES PATIENTS PORTE
ON NE POURRA PAS SUPPRIMER TOUS LES RISQUES
LA QUESTION EST DE SAVOIR COMMENT ON SE RELÈVE !
MERCI DE PRENDRE SOIN DES DONNÉES DE SANTÉ DES USAGERS !
CRAINTE D'UN ÉPUISEMENT DES ÉQUIPES
CHARGE DE TRAVAIL IMPORTANTE
AUGMENTATION DU VOLUME D'ATTAQUES
MANQUE DE PERSONNELS FORMÉS ET EXPÉRIMENTÉS
ACTIONS LONGUES QUI DURENT
ÇA PEUT PRENDRE + DE 6 MOIS DE SE RELEVER, S'EN SYSTÈME PAS HS
ACCULTURATION DES ÉQUIPES
DIFFÉRENTS TYPES DE CYBER CRIMINELS
OPPORTUNISTE
NON CIBLÉ LE + SOUVENT
"BOUTEURS" PETITES ESCROQUERIES EN MASSE SUR LA POPULATION
RANSOMWARES "CLÉS EN MAIN" DU DARKNET
CIBLÉ
"CARRIÈRE AUX GOGOS"
GROUPES CRIMINELS ORGANISÉS
(ACTIVISTES)
(GROUPES ÉTATIQUES)
DEMAIN ASSISTÉS PAR DES I.A.
AGENCE DU NUMÉRIQUE EN SANTÉ
doshas consulting
LAËTITIA BERNOUX

# Cyberattaque : qui est responsable, qui paie ?

**Modération : Maitre Florence EON-JAGUIN**
**Gilles CALMES · Guillaume MITHIEUX · Patrice BIGEARD · Laure HELENE-DUHESME**

La question du titre est volontairement abrupte. Elle l'est d'autant plus quand on a vécu la situation. Gilles Calmes, ancien directeur général du Centre Hospitalier Sud-Francilien de Corbeil-Essonnes, ouvre la table ronde avec un témoignage qui dit tout de la réalité d'une crise cyber en milieu hospitalier.

## Ce que ça fait, concrètement

C'est un dimanche matin à 6h. Tous les écrans sont noirs. 800 patients sont dans l'hôpital. Le plan blanc numérique est déclenché – mais le système d'alerte automatique ne fonctionne pas. Pendant quinze jours, une seule obsession : la sécurité des soins. Et puis, quand on relève la tête, les questions commencent à surgir. Les données de 700 000 patients sont dans la nature. Les données personnelles des 5 000 agents aussi. Il faut retrouver les adresses – parce que le SI est mort, y compris les annuaires. Il faut écrire à un million de personnes pour leur permettre de déposer plainte à titre conservatoire. Ce qui a nécessité la mise sous pli d'un courrier et affranchissement timbre par timbre. Quinze jours après le début de la crise, le directeur des finances frappe à la porte. Comment on paie le personnel ? Comment on règle les fournisseurs ? L'activité est en chute libre, la trésorerie ne suit pas. Une avance de la CPAM – dix-sept million d'euros sur cinq mois – a dû être négociée en urgence. Dispositif à prévoir en amont, dit Gilles Calmes avec le recul. Tout comme la procédure de « service fait » pour le trésorier public, qui ne peut pas payer sans attestation – et dont l'attestation informatique n'existe plus.

## Le secteur médico-social : des dommages collatéraux invisibles

Guillaume Mithieux, DSI de l'ORSAC – soixante établissements médico-sociaux – apporte un éclairage complémentaire. Dans ce secteur, les incidents ne font pas les journaux. Mais ils ont un coût réel : 55 000 euros virés vers un compte frauduleux suite à un mail piraté, dont une partie définitivement perdue. Des boîtes mail utilisées pour envoyer 10 000 messages de phishing en Europe, le temps que quelqu'un s'en aperçoive. Des sauvegardes insuffisantes, des données perdues sans bruit. Le levier, pour lui, est clair : la gouvernance SSI doit être portée par la direction générale. Pas déléguée à la DSI. Pas traitée comme un sujet technique. La création d'un poste de RSSI, d'une feuille de route, d'une stratégie – c'est à ce niveau que ça se joue.

> « Ceux qui paient d'abord, c'est les 5 000 professionnels de cet hôpital. Pas pendant un jour, pas pendant une semaine. Pendant deux ans. »
>
> Gilles Calmes, ancien DG du CHSF

## La répression : possible, mais géopolitiquement contrainte

Patrice Bigeard, FSSI des ministères sociaux, nuance l'idée reçue d'impunité totale des hackers. Les enquêtes aboutissent – quand elles sont menées avec les moyens nécessaires. Des groupes ont été identifiés, des individus interrogés. Mais une partie significative des opérateurs malveillants opère depuis la Crimée ou l'Ukraine dans une zone juridiquement inextricable. Les enquêteurs se déplacent. Les hackers restent libres. C'est frustrant, mais ce n'est pas une raison pour ne pas déposer plainte – c'est même la seule façon de permettre à la machine judiciaire de tourner.

Laure Hélène-Duhesme, pour l'ANSSI, rappelle que NIS2 va doter l'agence de pouvoirs de contrôle et de sanction qu'elle n'a pas aujourd'hui – et que la mise en cause du dirigeant est expressément prévue par la directive en cas de manquement grave ou de refus de coopérer.

## Ce que la table ronde a convergé

Unanimité sur la rançon : on ne paie pas. Ni légalement obligatoire, ni recommandé par l'ANSSI – et payer, c'est laisser la porte ouverte à celui qui garde les clés. Sur les habilitations : un seul compte compromis ne doit pas permettre d'accéder à la totalité des données d'un établissement. Ce n'est pas une exigence technique sophistiquée. C'est un principe élémentaire que trop d'établissements n'ont pas encore appliqué. Sur la certification HAS enfin : la cybersécurité est désormais dans le référentiel de visite – c'est un levier d'action concret auprès des directions, que les RSSI seraient bien inspirés d'utiliser.

Table ronde

# Comment protéger concrètement les patients ?

Modération : Arthur DAUPHIN — France Assos Santé
Mireille MASSOT · Sandrine ROUSSEL · Danièla PARROT · Philippe LOUDENOT

La deuxième table ronde aborde la même réalité par l'autre bout : non plus la crise vue depuis la direction ou le RSSI, mais la crise vécue par les patients, par les ingénieurs biomédicaux, par les DPO, et par ceux qui, depuis des années, tirent la sonnette d'alarme sur la cohérence d'ensemble du système.

## La voix des patients : la dernière informée

Mireille Massot, présidente de France Assos Santé Bretagne et représentante des usagers au CHU de Rennes, témoigne de la cyberattaque du 21 juin 2023. Son constat est sans fard : les représentants des usagers ont été au même niveau d'information que la presse au moment des faits. Aucune communication interne ne leur a été adressée d'emblée. Pourtant, le patient a une vie au-delà de l'hôpital. Il attend des bilans. Il a des rendez-vous programmés. Il a parfois besoin d'une téléconsultation, d'une télésurveillance, d'un compte-rendu envoyé à son médecin de ville. Quand tout tombe, ces fils-là se coupent aussi. Le CHU de Rennes a géré la crise avec sérieux – cellule quotidienne, communiqués de presse, page intranet dédiée, accompagnement des équipes. Mais le retour de Mireille Massot est clair : les représentants des usagers doivent être intégrés en amont dans les plans de sécurité, dans les exercices de crise, dans la gouvernance. Pas informés après coup.

## Les dispositifs médicaux : une exclusion réglementaire qui interroge

Sandrine Roussel, présidente de l'AFIB, apporte un éclairage technique souvent absent des débats cyber. Les dispositifs médicaux – scanners, moniteurs de soins intensifs, équipements de dialyse, systèmes de biologie – sont explicitement exclus du Cyber Resilience Act. Régis par le règlement européen 2017/745, ils obéissent à un cycle de développement spécifique, de quatre à dix ans, qui les rend structurellement en retard sur l'état de l'art logiciel au moment de leur mise en service.
La grille de lecture proposée est utile : en cas de cyberattaque, le bloc opératoire peut fonctionner sans réseau – la connectivité est utile, pas indispensable. Les consultations, idem. En revanche, les soins intensifs – avec leurs reports d'alarmes centralisés – et surtout les plateaux techniques dépendent de la connectivité de façon critique. 70% du diagnostic médical repose sur la biologie, rappelle un rapport de la Cour des comptes de 2015. Ce chiffre n'a fait qu'augmenter depuis.

> « La question n'est pas « est-ce qu'on va se faire attaquer ? ». La vraie question, c'est : jusqu'où ? Quels dégâts ? Et comment on réduit la surface d'exposition ? »
>
> Philippe Loudenot, CyberCercle

Le risque réel aujourd'hui n'est pas tant l'attaque directe via un dispositif médical que l'intégrité des données : une valeur erronée, une transposition fausse entre deux logiciels, un résultat modifié – pire, potentiellement, que l'absence de résultat.

## La sous-traitance : maillon faible, maillon contractuel

Daniela Parrot, DPO des ministères sociaux, place la question de la responsabilité exactement où elle doit l'être : le responsable de traitement, c'est l'établissement. C'est lui qui gère, qui arbitre, qui décide – et qui se retourne ensuite vers le sous-traitant. Pas l'inverse.
Le conseil pratique qu'elle répète, c'est de cartographier tous les sous-traitants, savoir où chacun intervient, et lire les contrats. Pas déléguer la lecture des contrats. Les lire. Vérifier ce qui est écrit sur la notification des incidents, sur les audits, sur les pénalités. Et quand un sous-traitant ne respecte pas ses engagements contractuels, activer les pénalités – pas par vengeance, mais pour que ça change.

## Seize ans de retard et le syndrome des vingt kilomètres

Philippe Loudenot, senior advisor au CyberCercle, ne pratique pas la langue de bois. En 2009, il fermait neuf hôpitaux à cause du virus Conficker. Des guidelines pour les fabricants biomédicaux avaient été produites à l'époque – elles ont été balayées d'un revers de main. Seize ans plus tard, les mêmes failles existent. Le syndrome des vingt kilomètres : après un accident de la route, tout le monde ralentit. Vingt kilomètres plus loin, tout le monde est reparti à cent quatre-vingts.
Sa critique porte aussi sur le fonctionnement en silos – sanitaire, libéral, médico-social, associations, collectivités territoriales – alors que le patient, lui, circule entre tous ces espaces. Et sur la conformité « check-list » : cocher une case en disant « c'est fait » n'est pas une démarche qualité. La cybersécurité est un processus continu, pas un état.

| Secteur | Impact si réseau coupé |
|---|---|
| **Bloc opératoire** | Faible — connectivité utile mais non indispensable à l'acte |
| **Consultations** | Faible — diagnostic médical reste possible sans SI |
| **Soins intensifs** | Modéré — reports d'alarmes centralisés dépendent du réseau |
| **Plateaux techniques (labo, radio)** | Critique — 70 % du diagnostic médical dépend de la biologie (rapport Cour des comptes 2015) |

Conclusion

# Cinq priorités pour 2026-2027

Didier AMBROISE — Doshas Consulting

Une liste de vingt priorités n'engage à rien.
En voici cinq – les cinq que cette matinée a rendues incontournables.

## 1 La gouvernance d'abord

Le risque cyber n'est pas un sujet de DSI ou de RSSI. C'est un sujet de direction générale, de conseil de surveillance, de COMEX. Si votre DG n'a pas signé la politique SSI de votre établissement, commencez par là.
Tout le reste – budget, ressources, formation, exercices – découle de ce signal politique.

## 2 Les sous-traitants dans la boucle

Le clausier du RSSI Santé existe (à retrouver ici).
Utilisez-le. Notification en 48 heures, logs conservés six mois minimum, contacts opérationnels identifiés avant la crise.
Ces clauses ne valent rien si elles ne sont pas dans vos contrats. Et vos contrats ne valent rien si vous ne les avez pas lus.

## 3 Le médico-social ne peut plus attendre

Programme CARE, structures autonomes, médecine de ville : le trou entre les ambitions affichées et ce qui arrive sur le terrain est béant. Ce n'est pas une question de moyens abstraits – c'est un risque patient concret, documenté, qui s'aggrave à mesure que l'informatisation progresse sans que la sécurité suive.

## 4 La plainte dans les 72 heures

C'est une obligation légale depuis la loi LOPMI. C'est la condition d'activation de votre assurance cyber.
C'est le seul moyen de permettre aux enquêteurs de travailler. Si vous n'êtes pas prêts à le faire en situation de crise, préparez la procédure maintenant – sur papier, avec les coordonnées imprimées.

## 5 S'entraîner

PCA, PRA, exercices de crise : pas une fois tous les cinq ans. Les établissements qui s'en sortent le mieux sont ceux qui ont répété. Imprimer l'annuaire. Allumer les PC de secours. Tester physiquement que le matériel de secours fonctionne. Simuler la décision en condition de brouillard – comme on répète les gestes d'urgence en médecine.

# Remerciements

Le CyberCamp Santé existe parce que des organisations publiques, institutionnelles et privées font le choix d'investir dans la diffusion de la culture cyber en santé.
Doshas Consulting remercie chaleureusement l'ensemble des partenaires et soutiens qui ont rendu possible la cinquième édition de cet événement.

## Partenaires institutionnels

## Sponsors & partenaires technologiques

## Partenaire média & événementiel

Un remerciement particulier à l'ensemble des intervenants, modérateurs et experts qui ont accepté de partager leur expérience, leurs analyses et leurs convictions avec les participants : Thomas Aubin, Patrice Bigeard, Gilles Calmes, Émilie Danglades-Perez, Arthur Dauphin, Florence Eon-Jaguin, Steven Garnier, Thomas Jan, Quentin Le Thiec, Laure Hélène-Duhesme, Philippe Loudenot, Mireille Massot, Guillaume Mithieux, Danièla Parrot, Sandrine Roussel.

CYBERCAMP Santé

doshas consulting

ISBN : 978-2-494611-02-3

10 €