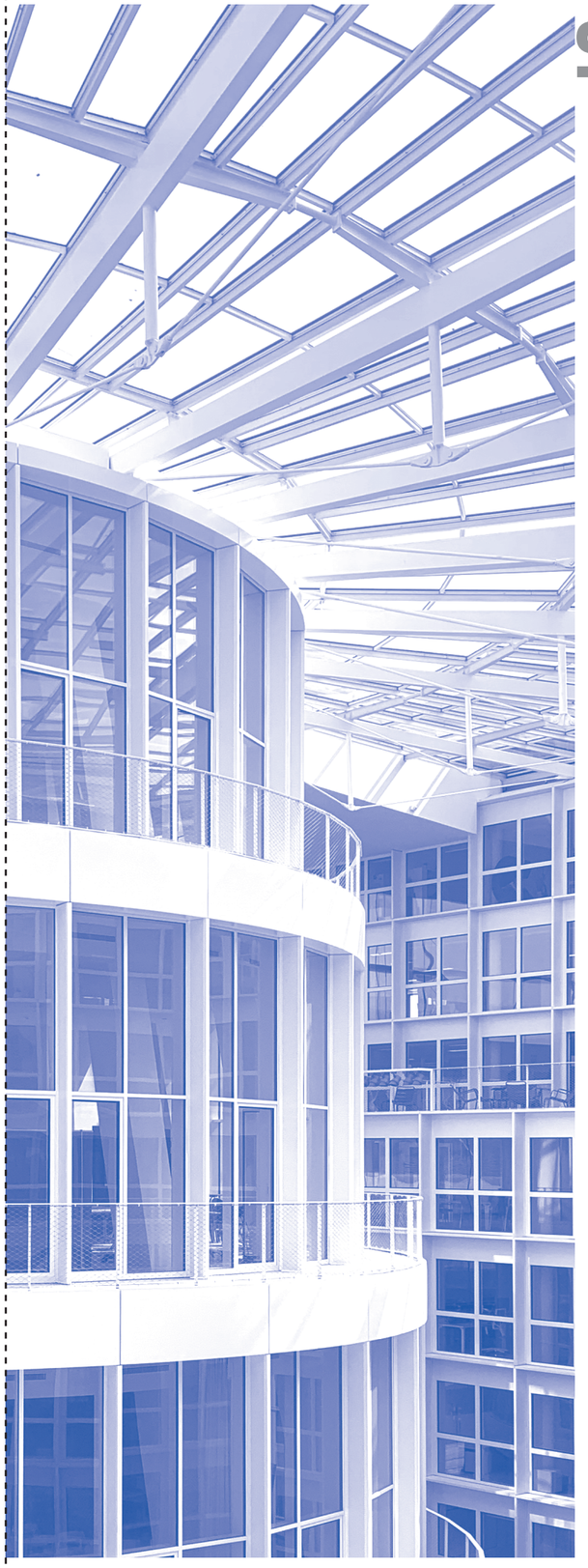
CYBERCAMP 2023

Santé

Éditeur : Doshas Consulting
Direction de la publication : Didier Ambroise & Cécile Jouanel
Rédaction : Doshas Consulting
Conception graphique : Studio Bleu Canari
Crédits photos : Arsedi, Pix'n Prod, Eugénie Martinez
et Doshas Consulting
Impression : L'Imprimeur - Mozac IMPRIM'VERT®
Dépôt légal : avril 2023
ISBN : 978-2-494611-01-6



sommaire

CyberCamp Santé #3

PariSanté Campus

2 février 2023

> **Le CyberCamp Santé est un rendez-vous important pour les acteurs de la cybersécurité en milieu hospitalier**
>
> François Braun, ministre de la Santé et de la Prévention

Au cœur du réacteur de la santé de demain !

Pour sa troisième édition, le CyberCamp Santé affichait complet et se déroulait, à PariSanté Campus, cœur du réacteur de la santé de demain. Jugée « pertinente », « très riche », et « essentielle » par la centaine de participants, cette matinée consacrée à la réflexion et aux retours d'expériences a marqué les esprits tant par son format que son contenu. Entre ateliers thématiques et discussions informelles, elle a répondu aux attentes de l'ensemble des acteurs de l'écosystème de la cybersécurité en santé, qui en ont apprécié le professionnalisme de l'organisation et la convivialité des échanges.

La 3e édition du CyberCamp Santé s'est ouverte par une intervention vidéo de **François Braun,** ministre de la Santé et de la Prévention dans laquelle il a rappelé les récents engagements pris en matière de cybersécurité pour les établissements de santé et l'objectif fixé que « 100% de ceux identifiés comme prioritaires aient réalisé, d'ici fin mai 2023, des exercices cyber. » Un exemple d'action pour que « les gestes barrières numériques » deviennent de véritables réflexes, sur le modèle des exercices incendie auxquels la population est désormais habituée. Saluant l'initiative de cette journée et toute sa pertinence, il a également annoncé l'élaboration d'un plan blanc numérique visant à mutualiser les ressources compétentes dans chaque région, afin de doter les établissements de pratiques à adopter, en cas d'incident cyber.

> **« L'enjeu est de trouver des solutions et de communiquer de façon intelligente, claire et positive vis-à-vis des citoyens. »**
>
> Antoine Tesnière, directeur général de PariSanteCampus

La matinée se déroulant à PariSanté Campus, son directeur général, le professeur **Antoine Tesnière** a tenu à accueillir les participants réunis dans la très belle salle de la rotonde, au deuxième étage de ce lieu dont la raison d'être est de « mélanger les compétences numériques et les compétences de santé, autour des enjeux de la transformation numérique du système de santé. » Il a souligné qu'au-delà des usages, de leur appropriation et de la dimension éthique, « le sujet de la sécurité est complètement central, les cybercriminels ayant un tropisme particulier pour les données de santé. »

Dernier intervenant de ce temps introductif, **Marc Loutrel,** directeur expertise, innovation, international de l'Agence du Numérique en Santé (ANS) est revenu sur la cyberattaque du Centre Hospitalier Sud Francilien (CHSF) de Corbeil-Essonnes en août 2022 comme point de départ d'annonces politiques importantes : enveloppe financière de 10 millions d'euros, *Task force cyber* mise en place en octobre 2022, construction du plan de renforcement cyber avec les ARS (Agences régionales de santé). Il a ensuite détaillé quelques chiffres clés du CERT Santé en matière d'incidents, demandes d'accompagnement, interventions en appui technique auprès d'établissements de santé et audits de cybersurveillance (voir infographie ci-dessous).

CERT Santé bilan 2022

592 / 733
incidents déclarés sur le portail des signalements

432 / 290
structures ont déclaré au moins un incident

Données 2022 / Données 2021

170 / 189
demandes d'accompagnement par le CERT Santé

101 / 80
interventions techniques d'appui (conseils techniques personnalisés, investigation numérique, remédiation, etc.)

Une clarification essentielle des textes européens

Des textes épars et fragmentés

Le Code de la cybersécurité dont la première édition est parue en juin 2022 rassemble des textes juridiques très différents en matière pénale, de défense nationale, de droit européen et de droit international.
L'approche européenne étant généraliste, il existe une juxtaposition de textes concernant les questions de santé :

- Le *Cybersecurity Act* de 2019
- La *Directive Network and Information Security* (NIS) 2 qui s'applique pour la cyberésilience des établissements de santé
- Le *Cybe Resilence Act,* proposition de règlement qui va concerner les objets connectés
- Deux règlements sur les dispositifs médicaux avec des spécifications précises
- Des dispositions dans le règlement sur l'intelligence artificielle, telles que des exigences de robustesse et de fiabilité, de gouvernance des données qui vont avoir un impact sur les questions de cybersécurité
- Le règlement sur l'Espace européen des données de santé qui comporte des mesures particulières sur le sujet.

Prise de conscience et pédagogie

À la base un travail de juristes, ce code a pour vocation de contribuer à une prise de conscience des professionnels concernés. En effet, on a tendance à associer l'idée de cybersécurité aux ingénieurs, aux informaticiens, aux cryptographes et pas forcément à des personnes travaillant dans le domaine de la justice ou de la santé, un des secteurs pourtant les plus attaqués par les cybercriminels et pour lequel le niveau de cyber-résilience est le plus faible.
Un travail de pédagogie doit donc être mené sur les réflexes d'hygiène numérique à acquérir, qui n'est pas facilité par le droit puisque on recense de nombreuses dispositions dans des textes extrêmement épars, au niveau national comme européen, avec des valeurs juridiques très différentes.
La compilation des textes s'accompagne de présentations et d'explications rédigées par plusieurs auteurs.
Pour coller à l'actualité, une seconde édition papier est à paraître en 2023 et une version en ligne est régulièrement mise à jour.

BRUNESSEN BERTRAND

Professeure agrégée des facultés de droit, en poste à l'Université de Rennes 1, Brunessen Bertrand dirige le Centre de recherches européennes de Rennes (CEDRE) et le laboratoire de droit européen. Spécialisée depuis plusieurs années en politique européenne du numérique, elle est également en charge de la chaire Jean-Monnet sur la gouvernance des données (DataGouv).

« Aider les professionnels à adopter les bons réflexes »

La cybercriminalité, un risque systémique

Aujourd'hui la question n'est pas de savoir si vous allez être attaqués, la question qui se pose c'est quand cela va-t-il vous arriver ! La cybercriminalité est devenue, au fil du temps, un risque systémique.
Une fois qu'on a fait ce constat, on adopte des postures pour travailler sur la résilience. C'est la raison pour laquelle le Code de la cybersécurité propose tout un ensemble de textes et de réflexions de plusieurs auteurs pour aider les professionnels à adopter les bons réflexes. Sachant que l'idée n'est pas de leur faire peur. Elle est de renforcer la prévention pour pouvoir anticiper et adopter les bons réflexes en matière de notifications. Par exemple, éviter tout retard dans les signalements d'incidents aux autorités administratives ou judiciaires.
Le message à faire passer consiste à dire qu'en cas d'infractions, les services de gendarmerie ou de police se tiennent prêts à intervenir aux côtés des victimes. Elles ne sont pas seules et ne doivent pas hésiter à composer le 17 !

Des données de santé qui valent de l'or

Aujourd'hui, les données de santé sont celles qui ont le plus de valeur car elles contiennent le plus d'informations à caractère personnel sur un individu (nom, prénom, date et lieu de naissance), le numéro NIR valant de l'or sur le *dark web.*
À partir d'elles, les cybercriminels peuvent générer une fraude à l'identité puis des fraudes au moyen de paiement comme une souscription à différents crédit, etc...
Avec la numérisation des données de santé, force a été de constater la mise en place de mécanismes d'escroquerie ciblée. Au-delà de la réception de tentatives quotidiennes sur nos boîtes mail qui sont générées aléatoirement et envoyées de manière massive, il se développe des essais d'extorsion en fonction de la pathologie des victimes potentielles (traitements, maladies...).
Le geste d'hygiène numérique de base est bien sur de ne cliquer sur aucun lien contenu dans un SMS et un courriel suspects.
Pour les signaler, il existe le 33 700, une plateforme qui transmet ensuite une liste noire de numéros aux opérateurs téléphoniques.

MATTHIEU AUDIBERT

Chef d'escadron, Matthieu Audibert est à la tête du département des coopérations et des partenariats cyber du commandement de la gendarmerie dans le cyberespace (ComCyberGend).

« Un objectif ambitieux et opportun pour les établissements de santé »

Élaboration et mise en place

En 2021, les Agences Régionales de Santé (ARS) et les Groupements Régionaux d'Appui au Développement de la e-Santé (GRADeS) ont rejoint le conseil d'administration de l'ANS et ont fait remonter, lors des premières réunions collégiales, le besoin de travailler sur la cybersécurité, notamment sur la continuité d'activité. C'est pour cette raison que la décision a été prise de produire ces kits d'exercices de crise et de les mettre à disposition des structures sanitaires et médicosociales.
Ils représentaient également une réponse aux enjeux de la feuille de route du Fonctionnaire Sécurité des Systèmes d'Information (FSSI) sur le renforcement de la cyber-sécurité des ARS. Ce sont elles qui ont été mandatées pour accompagner les établissements et contrôler qu'ils fassent bien leurs exercices. Un objectif très ambitieux et opportun !

Contenu des kits

Les kits sont des ensembles documentaires, composés de trois parties.
La première est dédiée à la communication afin d'aider l'animateur en amont de l'organisation de l'exercice. Une autre s'adresse aux participants, qui vont avoir des profils très différents, pour leur donner les règles du jeu. En effet, une cellule de crise d'un établissement de santé réunit l'ensemble de la direction générale et les directions métiers et techniques. Cette partie regroupe des documents supports comme un relevé de décisions, un glossaire pour les aider à utiliser un vocable commun et surtout des fiches réflexes, qui vont leur permettre d'acquérir certaines bonnes pratiques, en termes de gestion de crise, quelle que soit son origine.
Le dernier élément, le plus important, est l'ensemble qui est destiné à l'animateur. Il contient un livret qui récapitule les éléments à suivre, un support de briefing pour le lancement de l'exercice et un support de débriefing pour recueillir les premiers retours, à chaud, des participants : intérêt, rôle, canevas de rapport, etc...
Le cœur de chaque kit c'est le chronogramme, avec des événements prenant la forme de mails ou d'appels téléphoniques simulés.

Trois niveaux de maturité

Pour toucher le plus grand nombre d'établissements possible, l'idée de s'adapter à leur niveau de maturité cyber et de gestion de crise s'est concrétisée par la publication de trois kits différents.

ÉLODIE CHAUDRON

Élodie Chaudron est responsable du développement territorial à l'Agence du numérique en santé (ANS).

Kit débutant : pour partager les bonnes pratiques autour de la gestion de crise, notamment en matière de communication, et sensibiliser les directeurs aux enjeux de la cybersécurité et aux investissements nécessaires. L'objectif est de faire comprendre qu'une crise cyber, ce n'est pas qu'une problématique technique et que le travail le plus important est celui à mener sur les procédures dégradées.

Kit intermédiaire : pour tester la coordination interne entre la cellule de crise décisionnaire et les équipes IT, entre lesquelles la communication permanente est indispensable et doit être la plus claire possible.

Kit niveau avancé : pour se rapprocher le plus possible d'un événement réel, avec un périmètre technique plus large, des échanges simulés avec le CERT Santé et la mise en place d'une communication intégrant les dimensions interne et externe.

Selon le niveau de difficultés, les durées de jeu varient entre 1h30, 2h30 et 3 heures.

Mesures prioritaires

« La réalisation de ces exercices de crise cyber fait aujourd'hui partie des mesures prioritaires de renforcement qui sont demandées à toutes les structures. Les établissements sanitaires ont récemment reçu une instruction du Haut fonctionnaire de défense et sécurité (HFDS), la rendant obligatoire, avec une cible à 100 % d'ici mai 2023, pour les établissements identifiés comme prioritaires.
Un financement dédié de 10 millions d'euros a par ailleurs été octroyé. Il décline toute une stratégie régionale pour accompagner les établissements dans la réalisation d'exercices de crise sur la base de ces kits.

> **“Une crise cyber, ce n'est pas qu'une problématique technique”**

STEVEN GARNIER

Steven Garnier est référent technique eSanté à l'Agence Régionale de Santé (ARS) Bourgogne-Franche-Comté.

Accompagner les établissements de santé dans leur maturité

Un risque immatériel, complexe et très évolutif…

L'une des difficulté dans le milieu hospitalier est que la cybersécurité peut être perçue comme complexe, technique et peu compréhensible pour les directions qui allouent les budgets et accompagnent les équipes. Inversement, il est parfois compliqué pour un RSSI ou un DSI de parvenir à les engager.
Le niveau de résilience des établissements de santé étant malheureusement encore insuffisant pour pouvoir les rendre assurables, ou du moins durablement assurables, l'enjeu est donc de passer de la notion de difficulté à celle de maturité. Pour les accompagner dans la gradation de leur maturité, il faut parvenir à créer, collectivement, les briques manquantes dans le renforcement de leur sensibilisation, leur compréhension et leur capacité à prendre des décisions tenant compte de contraintes humaines et budgétaires.

… possible à identifier et à quantifier

Pour que les établissements de santé soient en capacité de choisir leurs actions prioritaires, nous souhaitons leur apporter de nouveaux outils d'identification et de quantification des risques, à partir d'un axe « protection sécurité des patients et des données » / « maturité » dont les étapes sont :

- La sensibilisation (je connais)
- La compréhension (je comprends)
- L'identification (j'identifie des risques)
- La quantification (je mesure mes expositions)
- Les actions (j'optimise mes décisions).

Une solution souveraine, experte et innovante

Ce CyberCamp Santé est l'occasion d'annoncer le lancement d'une solution de pilotage du risque cyber, dédiée aux établissements de santé, conçue et développée par Relyens et Citalid, une jeune pousse française de la cybersécurité.
Cette solution 100 % française et souveraine possède deux composantes :

- un modèle de quantification et de recommandation du risque cyber, dont le fondement est une analyse de la menace en continu, combinant des informations techniques, du ciblage sectoriel, un contexte géopolitique et des mises à jour en continu.

PIERRE-YVES ANTIER

Pierre-Yves Antier
est directeur stratégie, innovation, transformation du groupe Relyens.

> **« L'objectif est de comprendre l'état de la menace, afin de le transformer en un risque et une quantification financière. »**

- une plateforme de pilotage pour comprendre, modéliser et quantifier les risques ainsi que prioriser une roadmap. Ses principes sont de pouvoir renseigner le niveau de défense de l'établissement de santé, son organisation en matière de cybersécurité et ses impacts financiers comme opérationnels.

Retrouver « les chemins de la confiance »

Véritable course contre la montre, cette évolution des réponses face à la menace cyber permettra d'engager un cercle vertueux, à condition d'être capable de diffuser le plus largement et le plus rapidement possible cette solution. C'est pourquoi Relyens s'est associé à HOSPIVISION®, un outil de référence bien connu des établissements de santé, développé par le groupe PSIH. Un premier set d'indicateurs en mode gratuit est désormais accessible. Il comporte un scénario sur un rançongiciel et un scénario sur une fuite de données.
Cette résilience permettra de préserver la confiance des citoyens envers leur système de santé, des patients dans leur établissement de santé et celle du personnel soignant, soumis à rude épreuve en cas de cyberattaque !

Intervenir dans l'analyse du risque

« La définition originelle de l'assurance, qui est d'éviter le risque de ruine, implique la condition d'identifier un aléa. Or, aujourd'hui les cyberattaques n'en sont plus un puisqu'on sait qu'elles vont arriver. La seule incertitude (aléa) reste la date.
Cette situation rend difficile l'assurabilité des établissements de santé, en matière de cybercriminalité. Les articles annonçant que la menace cyber est devenue inassurable sont d'ailleurs nombreux et réguliers. Pour autant, le travail des assureurs n'est pas seulement de verser une indemnité en cas de sinistre ou d'essayer d'accompagner les victimes. Il est d'intervenir dans l'analyse du risque et la prévention, au travers de solutions intelligentes servant à en identifier les caractéristiques, en cerner la fréquence et l'intensité, puis à le sérier pour tenter de le cantonner. L'objectif étant de permettre, aux assurés couverts, d'éviter le risque de ruine. »

David Bigot, délégué général de ROAM

« Dialoguer, réfléchir et trouver des solutions avec les usagers »

Voir la réalité en face

Depuis l'instauration de la démocratie en santé, il y a 20 ans, les usagers participent à l'amélioration des soins pour tous et à la mise en œuvre des politiques de santé. Ils ont des droits qu'ils font valoir par l'intermédiaire de leurs représentants, dans des commissions et des directoires, au sein des établissements de santé.
Premiers concernés par la fuite et l'utilisation frauduleuse de leurs données personnelles, ils veulent voir la réalité en face. C'est notamment le cas des bénévoles impliqués dans les associations de patients qui œuvrent au quotidien pour écouter, dialoguer, réfléchir, trouver des solutions et faire progresser les pratiques qui seront aussi, demain, celles de la cybersécurité en santé.
De nombreux discours alarmistes sont portés par les médias, alors que beaucoup d'usagers identifient très naturellement que le numérique est un vecteur de progrès pour la santé. Il est donc important que les acteurs de terrain s'approprient les clés du narratif de la cybersécurité en santé pour retrouver les « chemins de la confiance ».

Identifier les risques réels

Les patients au sens large ont du mal à identifier les risques réels pesant sur leurs données de santé. Ce qui ressort des enquêtes et de nos échanges de terrain avec les associations de santé, c'est la crainte qu'elles soient envoyées à leur banque, leur assureur, leur employeur pour être utilisées à leur détriment.
Il est donc très important de les sensibiliser à la question de l'hygiène numérique. Cette acculturation, ce changement de modèle ne peuvent se faire sans prendre en compte leur vision et leur perception de la réalité.
Ce CyberCamp Santé est l'occasion pour nous tous d'apprendre les uns des autres, comme nous pouvons apprendre des représentants des usagers à améliorer les exercices de gestion de crise et la transparence de l'information.
Si les citoyens ont conscience que le risque zéro n'existe pas, ils veulent savoir que les meilleurs efforts sont mis en action pour les résoudre et qu'on ne leur cache rien !

ARTHUR DAUPHIN

Titulaire d'un master
en santé publique,
après avoir soutenu
sa thèse de doctorat
en pharmacie consacrée
à la démocratie sanitaire,
il a rejoint France Assos santé,
en tant que chargé de mission
Numérique en santé.

Évolutions réglementaires et mesures de prévention

1- Évolutions réglementaires

Quelques textes clés en matière juridique régulent le monde numérique et les risques qui y sont associés. Publiée dans le Journal Officiel de l'Union Européenne en décembre 2022, la directive NIS2 prendra effet en France au plus tard au second semestre 2024, afin d'apporter une meilleure protection contre les acteurs malveillants. Certaines de ses exigences seront immédiatement applicables, tandis que d'autres auront un délai de mise en conformité. L'ANSSI (Agence nationale de la sécurité des systèmes d'information) recommande aux entreprises de se préparer dès maintenant et de ne pas relâcher leur effort en matière de cybersécurité. Les exigences de NIS 1 resteront applicables jusqu'à l'entrée en vigueur de NIS 2 qui prendra en compte les efforts déjà entrepris par les opérateurs.

Le Parlement européen examine en ce moment l'*Artificial Intelligence Act,* un projet de règlement visant à renforcer la robustesse et la cybersécurité des dispositifs d'intelligence artificielle, afin que leur utilisation, leur fonctionnement et leur performance ne soient ni compromis ni altérés. Il s'agit aussi d'éviter que les données d'entrée ne soient manipulées pour tromper le système et changer son comportement.

Problématiques remontées

- La multiplication des textes et leur adaptation au contexte cyber lui-même en constante évolution ;
- Le manque de moyens pour la mise en place sur le terrain ;
- Durcissement des sanctions, manque de visibilité sur les mesures à mettre en œuvre pour respecter les exigences NIS ;
- L'appréhension du risque de manipulation des systèmes d'IA ;
- Les exigences de gouvernance de données dans l'IA Act, pour éviter l'impact sur les producteurs de soins, les fabricants, etc…
- L'articulation des règlements dispositifs médicaux/objets connectés en lien avec la durée de vie de ces objets.

2 - Les mesures de prévention et de réaction face aux cyberattaques

Les actions à mettre en place face à une cyberattaque par rançongiciel

Adopter les bons réflexes

- Ouvrir une main courante pour tracer les actions et les évènements liés à l'incident ;
- Déconnecter au plus tôt les supports de sauvegardes après vous être assurés qu'ils ne sont pas infectés ;
- Isoler les équipements infectés en les déconnectant du réseau ;
- Laisser éteints les équipements non démarrés ;
- Conserver les données chiffrées ;
- Mettre en place une cellule de crise ;
- Établir une stratégie de communication interne comme externe et les éléments à fournir en vue de la judiciarisation (dépôt de plainte) ou de la notification réglementaire (avis à la CNIL).

Trouver de l'assistance technique

- La plateforme cybermalveillance.gouv.fr permet d'entrer en contact avec des prestataires de proximité ;
- Le cas échéant, faire appel à des prestataires spécialisés dans la réponse aux incidents de sécurité.

Communiquer au juste niveau

- Communication interne adaptée : rassurer les collaborateurs et leur rappeler qu'ils sont soumis à une clause de confidentialité ;
- Communication externe adaptée : centraliser la communication vers l'extérieur en étant transparent vis-à-vis des entités institutionnelles.

Ne pas payer la rançon

- Le paiement ne garantit pas l'obtention d'un moyen de déchiffrement ;

- Il incite les cybercriminels à poursuivre leurs activités et entretient donc ce système frauduleux ;
- Il n'empêchera pas votre établissement d'être à nouveau la cible de cybercriminels.

Déposer plainte

- Déposer plainte auprès des services de police ou de gendarmerie.

Restaurer les systèmes depuis des sources saines

- Réinstaller le système sur un support connu et restaurer les données depuis les sauvegardes effectuées, de préférence, avant la date de compromission du système ;
- Vérifier que les données restaurées ne sont pas infectées par un rançongiciel.

Focus sur la loi d'orientation et de programmation du ministère de l'intérieur (LOPMI)

Les trois points clés de ce texte

- La création d'une nouvelle infraction (article 323-3-2 du Code pénal) : la gestion d'une plateforme en ligne pour permettre des transactions illégales de produits, contenus ou services (ex : base de données volée).
- L'aggravation des peines : les sanctions pour les actes de piratage de données informatiques (article 323-1 du Code pénal) sont renforcées si la cyberattaque entraîne un risque immédiat de mort ou de blessures graves, ou empêche les secours. Dans ce cas, la peine maximale est de 10 ans d'emprisonnement et 300 000 euros d'amende (article 323-4-2 du Code pénal). Cette nouvelle réglementation s'applique spécifiquement aux cyberattaques commises contre les établissements de santé et les services de secours.
- L'encadrement du versement de rançons en cas de cyberattaque : si une assurance a été souscrite pour indemniser une victime de pertes causées par une cyberattaque, le paiement d'une rançon ne sera possible que si la victime a déposé plainte au plus tard 72 heures après la connaissance de l'attaque (article L. 12-10-1 du Code des assurances).

Animateur *:*
Maitre Florence Eon-Jaguin,
avocate associée
Withlaw Avocats

Problématiques remontées

- L'existence ou non d'une politique interne de gestion de crise au sein des organisations ;
- L'importance de la communication en cas de gestion de crise ;
- Le positionnement par rapport au fait de payer ou non une rançon ;
- Le positionnement vis-à-vis du dépôt de plainte ;
- L'opportunité de réaliser ou non des actions de prévention / sensibilisation au profit des salariés de la structure ;
- L'existence ou non d'une redondance dans les systèmes aux fins de résilience.

Vers une meilleure assurabilité des établissements de santé français ?

Deux questions ont été posées en début d'atelier :

- **Quels apports vous intéressent-ils le plus dans l'assurance cyber ?**
- **À quel moment l'assureur cyber vous aide-t-il le plus ?**

Concernant la première question, l'apport plébiscité est l'expertise, suivi de l'aspect financier.
Concernant la deuxième question, un accompagnement en amont est plébiscité, suivi de l'accompagnement pendant l'incident cyber.
Par conséquent, l'image « ancienne » de l'assureur qui indemnise un sinistre avéré est révolue, la bascule se faisant vers un modèle d'accompagnement en amont, mobilisant des experts et susceptible d'apporter davantage de « prévention ».

1 - État des lieux de l'assurabilité des établissements de santé français

Les participants devaient réfléchir à la question suivante :
« que pensez-vous des prérequis d'assurance dans le cadre de votre politique de prévention de l'extorsion ? »

Les remarques formulées ont été les suivantes :

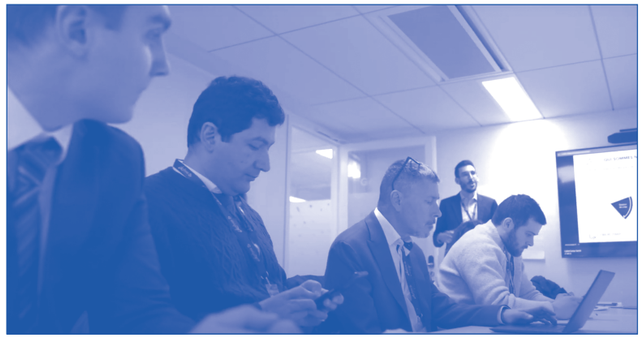
- Les questionnaires d'assurance sont trop complexes et demandent très souvent un niveau de maturité que les établissements de santé n'ont pas. Il faudrait simplifier ces questionnaires en les axant sur des démarches d'engagement cyber, sans forcément demander que les actions soient déjà en place. Car à date, ces prérequis sont inatteignables pour la plupart des établissements de santé.
- D'autre part, ces questionnaires sont très souvent issus de la réglementation anglo-saxonne. Il faudrait les adapter au contexte français pour davantage de pertinence et de souveraineté.
- Enfin, pour faire écho à la première remarque, il faut accentuer la communication vers les établissements de santé pour leur faire comprendre que le risque cyber est assurable car aujourd'hui, de nombreux établissements de santé ne cherchent même plus à se faire assurer.

2 - Complexité de la gouvernance

Les participants devaient réfléchir à la question suivante :
« Comment gérez-vous les relations avec les tiers mainteneurs et fabricants de dispositifs médicaux ? ».

Les remarques formulées ont été les suivantes :

- Les établissements de santé sont aujourd'hui « dépendants » des éditeurs de dispositifs médicaux en matière de cybersécurité. En effet, ils « subissent » le niveau de maturité cyber des solutions numériques utilisées, sans pouvoir contraindre les fabricants car la réglementation ne prévoit rien en termes d'exigences minimales cyber. Par conséquent, les établissements de santé ont deux possibilités :
  - > Ne plus utiliser la solution présentant des risques cyber et donc abandonner certains soins ;
  - > Continuer à pouvoir soigner et donc conserver le dispositif médical avec les risques cyber associés.
- Quelques pistes de solutions ont été évoquées en réunion :
  - > Conditionner l'Autorisation de Mise sur le Marché (AMM) à un niveau minimum de sécurité numérique du produit ;
  - > Éduquer le marché en ajoutant aux critères de choix d'une solution numérique, un aspect cyber ;
  - > Vérifier et challenger les contrats déjà signés avec les fabricants de solutions numériques sur cette thématique de gestion du risque cyber.



3 - Politique de gestion du risque

Les participants devaient réfléchir à la question suivante :
« comment priorisez-vous les investissements en prévention par rapport au transfert du risque résiduel ? ».

Les remarques formulées ont été les suivantes :

- À date, il n'y a pas de doctrine / méthode / outil permettant d'aiguiller les décideurs sur cette question. Chacun fait comme il veut / peut.
- D'autre part, la question posée en fait émerger une autre : comment mesurer le risque résiduel, sachant que la plupart des établissements de santé sont incapables de le faire, notamment avec la « boîte noire » des dispositifs médicaux.
- Enfin, la notion d'investissements ne doit pas être vue comme uniquement financière, mais doit également prendre en compte l'aspect ressources humaines.

4 - Pistes de travail pour une meilleure assurabilité

Les participants ont été encouragés à suivre de près les thématiques suivantes :

- Savoir déployer une politique de « patch management » très stricte pour tous les systèmes ouverts (exposés à Internet notamment) ;
- Maitriser les sauvegardes/restauration et savoir les protéger ;
- Disposer d'un antivirus de flux de messagerie renforcée par une « sandbox » ;
- Il faut rajouter à cette liste la segmentation des réseaux, ainsi que la dimension humaine/organisationnelle pour ne pas traiter que l'aspect technique.

Animateur :
Christophe Millet,
cyber risk manager Relyens

Qu'est-ce qu'une cyber crise et comment la définir ?

Les échanges au cours des ateliers ont montré qu'il existait un champ lexical propre à chacun avec un ressenti commun.

CHOC URGENCE PANIQUE
RAPIDE STRESS SOLITUDE
MALVEILLANT
TENSION SOUDAIN cohésion de groupe
SUBI IMPREVU CONTAGIEUX

Constat : Une cybercrise touche TOUT LE MONDE. Il est donc fondamental de s'y préparer et d'anticiper sa survenue.

***Animateurs** : Anthony Sbong et Arthur Chedeville (ITEC Security)*

Quels sont les impacts potentiels et les piliers de la gestion de crise ?

Les impacts sont à la fois techniques, humains et financiers.

- **Arrêt de l'activité**
- **Prise en charge du patient dégradée :** localisation, distribution de repas, radios, téléphonie, ventilation, ascenseurs, climatisations, badges, facturation sont à l'arrêt ;
- **Plans blancs :** surcharge pour les soignants, difficultés à gérer la crise ;
- **Coûts réels**
- **Notoriété**
- **Comment tenir sur la durée ?**

« Ça a été soudain, même si on s'y attendait »

« Quand vous êtes dans la crise réelle il y a une urgence »

Pour autant la criticité n'est pas toujours comprise immédiatement ni correctement.

Qu'est-ce qu'il faut faire ?

- Sensibiliser et mettre en place des bonnes pratiques ;
- S'assurer du cloisonnement du SI ;
- Tester les processus de crise : PRA/PCA, sauvegardes régulières ;
- Définir des solutions de communication alternatives (chats sécurisés, etc …)
- Anticiper la communication : auprès des patients, des professionnels, de l'extérieur (image) ;
- Anticiper les impacts humains :
  > définition des personnes/expertises à mobiliser
  > identification des montées en charge
- Réfléchir à la gestion du temps long : penser à la santé des collaborateurs impliqués ;
- Définir des responsabilités pour la prise de décisions ;
- Être dans une démarche d'entraînement en continu ;
- « **Venir au CyberCamp Sante tous les ans** »

En conclusion

De l'avis des participants, des intervenants et des animateurs d'ateliers, cette matinée a été un temps fort, riche en échanges, en apprentissages et en retours d'expérience. L'ensemble des restitutions a parfaitement montré que les différents aspects de la cybersécurité, qu'ils soient techniques, réglementaires ou assurantiels, forment un tout à considérer dans son ensemble.

Marc Loutrel a tenu à souligner que les perspectives étaient plutôt encourageantes, notamment grâce à la formulation d'idées de plan de travail pour l'année 2023, lui apparaissant de bon augure pour l'avenir. Il a ensuite rappelé l'existence, dans le Ségur du Numérique, d'exigences de sécurité des systèmes d'information, allant permettre de travailler au renforcement du niveau de cybersécurité des entreprises du numérique qui proposent des solutions aux organisations de santé (établissements, laboratoires, centres d'imagerie, médecine de ville et officines…).

« D'année en année, le CyberCamp Santé prend de l'ampleur. Il rassemble aujourd'hui une véritable communauté de personnes impliquées dans une démarche de prévention et d'action. La présence, ce matin, de plusieurs d'entre elles ayant assisté aux deux premières éditions en est la preuve », remarquait avec satisfaction Didier Ambroise, associé fondateur de Doshas Consulting, co-organisateur de l'événement.
Avant de conclure sur cette note positive, « j'ose espérer qu'à terme, le CyberCamp Santé n'aura plus de raison d'exister et que nous ne ressentirons plus le besoin d'améliorer collectivement la cybersécurité en santé. D'ici là, c'est à vous de porter la bonne parole, pour que tous les acteurs de l'écosystème soient, plus que jamais, cyber vigilants ! »

> **Je suis ravi de ma participation au Cyber Camps Santé. Je repars avec beaucoup d'idées qui vont nourrir nos plans d'action pour les mois qui viennent.**
>
> Christophe Mattler,
> de la transformation numérique
> et des SI - Institut Gustave-Roussy

Statistiques réseaux sociaux du CyberCamp

97 +30%
posts/tweets

3303 +114%
réactions et comments

156 274 +107%
vues

Données 2023 / Données 2022

CyberCamp Santé #2

Musée des Confluences - Lyon

8 février 2022

« Une cyberattaque ? Ça n'arrive pas qu'aux autres ! »

« Si je participe bien volontiers à des événements comme le CyberCamp Santé, c'est pour faire de la pédagogie et dire stop à certaines idées reçues. On entend souvent dire que les hôpitaux publics ne sont pas sécurisés, c'est complètement faux ! Ils le sont, ce qui ne les empêche pas d'être exposés à des risques comme n'importe quelle entreprise. (...)
La réalité montre cependant que la sensibilisation des équipes IT n'est pas suffisamment développée, même si différents programmes nationaux la préconisent depuis des années. Les pré-requis à atteindre présents dans HOP'EN et SUN-ES sont, à mon sens, les bases d'une bonne politique de sécurité. Elles sont néanmoins plus ou moins appliquées, en fonction des compétences, des contraintes budgétaires et techniques ainsi que des différents acteurs. D'après notre expérience à l'hôpital Nord Ouest, ce qui a accéléré la prise en compte de la sécurité pour l'ensemble des utilisateurs du SI, qu'ils soient soignants ou personnels administratifs, c'est la cyberattaque que nous avons subi, en février 2021, sur notre établissement support, le CH de Villefranche sur Saône. Et ce, malgré des campagnes de prévention portées par notre RSSI qui n'ont pas suffi à nous protéger d'une panne généralisée et totale de notre SI. Cette cyberattaque a démontré que la sensibilisation à la sécurité était l'affaire de tous, puisque la faille de sécurité première vient d'une mauvaise manipulation d'un utilisateur. J'aurai naturellement préféré que ça se passe autrement... »

Nasser Amani, Directeur des services numériques du territoire pour le GHT Rhône Nord Beaujolais Dombes

« Le risque numérique reste encore l'affaire de DSI alors que la finalité recherchée est de protéger l'activité de l'organisation pour que les professionnels de santé en milieu hospitalier puissent travailler dans de bonnes conditions. C'est pourquoi, j'étais ravie aujourd'hui de ne pas voir de RSSI sur les différentes tables rondes. »

Béatrice Bérard, officier de sécurité pour les SI des Hospices civils de Lyon

« Le jour où le ciel vous tombe sur la tête... »

« Le matin du 2 août 2021, nous nous réveillons confrontés à une cyberattaque massive ayant mis à plat, par ransomware, tout notre système informatique. (...) Le jour où le ciel vous tombe sur la tête, il faut d'abord essayer de comprendre ce qui vous arrive. Nos premiers réflexes ont été de suivre une procédure assez classique de mise en sécurité, à savoir couper les accès internet et désactiver l'ensemble des liens avec notre cœur de réseau, l'isoler pour éviter la contagion, comme pour un virus médical. Très rapidement ensuite, nous avons rempli un processus de déclaration obligatoire permettant de qualifier, dans la journée, la nature des dégâts. Et puis surtout, nous avons activé le plan de continuité d'activité pour que les désagréments informatiques n'aient pas de conséquences néfastes pour les malades.
Dans notre malheur, nous avons eu la chance de pouvoir retirer les bénéficies du travail mené depuis deux ans sur des démarches qualités. Ces acquis nous ont évité de rajouter de nouveaux désagréments techniques à la permanence des soins. Par une cellule de crise, des points entre professionnels plusieurs fois par jour pour mesurer l'étendue des dégâts, nous avons réussi à réajuster les procédures quand elles n'étaient pas suffisantes et à prioriser les actions de contournement. Je suis convaincu que c'est par une plus grande communication autour des risques encourus par chaque établissement que nous augmenterons notre niveau de maturité collective et que nous détournerons les attaquants du secteur de la santé ! »

Rodrigue Alexander, directeur adjoint du CH d'Arles chargé des finances, de l'activité et du système d'information en 2022, actuellement DSI du CHU de Martinique.

« Les praticiens en santé n'ont aucune connaissance de la valeur de la donnée de santé qui est beaucoup plus monnayable qu'un numéro de carte bleue. On parle souvent de les sensibiliser au sein des structures hospitalières, alors que je suis convaincu qu'il faudrait plutôt raisonner en amont, dès la formation initiale, que ce soit dans le cursus des écoles d'infirmières, des écoles de kinés et des facs de médecine. »

Didier Mennecier a été précurseur dans la e-santé en tant qu'hépato-gastro-entérologue et a créé le blog https://www.medecingeek.com

Témoignages

« Les pirates viennent d'abord perturber le système puis attaquer la confidentialité de la donnée. Ils la récupèrent pour faire des usurpations d'identité, en la revendant très facilement sur le darknet. Contrairement à ce que l'on peut croire, les données de carte bancaire ne sont pas forcément les plus chères parce qu'elles sont périmées dès qu'il y a opposition. (...)
En cas d'attaque, les réflexes à avoir sont de prévenir les prestataires des établissements de santé, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), mais aussi la police ou la gendarmerie. Nous sommes en effet capable de venir en appui dans la gestion de crise, par l'intermédiaire d'enquêteurs, d'experts techniques et éventuellement de négociateurs, y compris ceux du GIGN. Et de manière totalement gratuite ! »

Colonel Barnabé Watin-Augouard, commandement cyber de la gendarmerie nationale

« Les cyberattaquants n'ont aucune limite et aucune frontière ne les arrête !
L'un des grands enjeux est celui de la souveraineté et de la maîtrise de nos donnée. On ne peut pas être dépendant en France et en Europe de technologies cyber qui ne sont ni françaises, ni européennes. L'accès aux informations est bien trop critique pour ne pas progresser collectivement sur ce sujet. Le train est lancé, il n'est pas encore arrivé... »

Olivier Morel, trésorier de l'association Hexatrust

“Contrairement à ce que l'on peut croire, les données de carte bancaire ne sont pas forcément les plus chères parce qu'elles sont périmées dès qu'il y a opposition.”

CyberCamp Santé #1

Fondation Dosne-Thiers - Paris

5 février 2020

Investir dans la sécurité informatique à l'hôpital est devenue une nécessité

« Les directions hospitalières ont de plus en plus conscience de l'importance et de la fragilité d'un SI sans donner forcément à la sécurité informatique les moyens qu'elle nécessite. Ceci étant dit, avant d'en comprendre le fonctionnement, il m'a fallu avaler plus d'une boîte de paracétamol et avoir recours aux services d'un ingénieur informatique pendant des années. Et en plus j'étais volontaire !
Quoi qu'on en dise, ce domaine reste très compliqué et on ne peut pas demander à mes collègues d'acquérir cette compétence du jour au lendemain. D'autant plus que les usages évoluent. Vouloir partager la même identité au sein d'un GHT ou avec un hôpital de proximité pour « fluidifier » les parcours de soins risque d'ouvrir une faille et de fragiliser le système. Sans compter que diriger un établissement de santé suppose une gestion tellement complexe que la sécurité informatique est généralement déléguée au DSI. (...)
J'ai envie de dire à mes collègues qu'en investissant dans la sécurité informatique ils ne jettent pas l'argent public par les fenêtres. Il suffit de penser au CHU de Rouen, qui disposait d'une DSI structurée, et aux conséquences de l'attaque sur son fonctionnement pendant des semaines. Je voudrais aussi souligner la vigilance des DSI qui font des exercices de phishing ou d'hameçonnage et l'importance de les écouter en CODIR. Enfin, il est important d'accompagner les chefs d'établissements dans l'arbitrage entre sécurité et métier. Pour le personnel soignant, les outils informatiques sont avant tout une aide et ne doivent pas les empêcher de travailler. »

Alexandre Aubert, directeur du GHT Nord Ouest Vexin Val-d'Oise (NOVO)

“

C'est une belle initiative car ce CyberCamp Santé permet de faciliter le dialogue entre les différents acteurs.

Emmanuel Sohier, responsable de la cellule ACSS de l'Agence du Numérique en Santé, devenue le CERT Santé

”

« Dans le monde de la santé, nous sommes devenus, à bien des égards, assez numérico-dépendants et il faut quand même toujours penser à avoir un plan B si ça ne fonctionne pas.

Philippe Loudenot, ex-fonctionnaire de sécurité des SI pour les ministères sociaux.

« Pour une première c'était parfait puisque nous avons pu aborder de vastes sujets auxquels nous devons maintenant trouver des réponses. Il faut donc absolument refaire d'autres CyberCamp Santé ! »

Maître Amélie Beaux, avocate en droit de la santé.

“

On a eu la chance d'assister à plusieurs ateliers avec des restitutions très intéressantes.

Tristan Piron, DSI adjoint, RSSI et DPO du GHT Vendée

”

Remerciements

Les organiteurs du CyberCamp Santé remercient toutes les personnes ayant contribué au succès des trois premières éditions

Rodrigue Alexander, Nasser Amani, Pierre-Yves Antier, Alexandre Aubert, Matthieu Audibert, Maria Bäcklund-Hasel, Jean-Pierre Barré, Yves Beauchamp, Amélie Beaux, Béatrice Bérard, François Braun, Brunessen Bertrand, David Bigot, Hervé Blanc, Maëlle Cadas, Elodie Chaudron, Arthur Chedeville, Grégory Cordier, Arthur Dauphin, Antoine Débarbouillé, Enguerrand Decourtil, Quentin Desages, Charlotte Drapeau, Florence Eon-Jaguin, Thomas Fauré, Steven Garnier, Grégoire Germain, Mathieu Hernandez, Davy Hing, Thomas Jan, Karine Joannet, Christophe Jodry, Pekka Kahri, Jean-François Laigneau, Philippe Loudenot, Marc Loutrel, Christophe Mattler, Benjamin Meany, Didier Mennecier, Christophe Millet, David Noury, Bertrand Pellet, David Petauton, Fabien Pezous, Ray Pinto, Tristan Piron, Laurent Puyfoulhoux, Olivier Morel, Tristan Piron, Christophe Richard, Manon Rocroy, Patrick Ruestchmann, Romain Santini, Anthony Sbong, Richard Smadja, Emmanuel Sohier, Antoine Tesnière, Audrey Uzel, Barnabé Watin-Augouard ainsi que les équipes de l'Agence du Numérique en Santé et de Doshas Consulting.

Sponsors et partenaires

CYBERCAMP
Santé

ISBN : 978-2-494611-01-6

15 €