Cybersécurité en milieu sensible : immersion dans le monde de la Santé

LIVRE BLANC



STORMSHIELD

Rien n'arrête les cyber-criminels. Face à l'importance vitale du milieu médical, ils n'hésitent pas à tirer profit des fragilités creusées par la crise sanitaire ou des failles créées par la transformation numérique du secteur. En France comme à l'international, les établissements hospitaliers, les pharmacies, les laboratoires et autres structures de soin font face à des vagues incessantes de cyberattaques sur fond de grande vulnérabilité informatique.

Dans le monde de la Santé, les déclarations d'incident ont doublé en 2021 par rapport à 2020[1]. Comment expliquer cette hausse sans précédent ? Les réponses sont aussi variées que les vulnérabilités des établissements et il faut même y ajouter depuis peu le profil inédit de certaines cibles. En effet, ces incidents sont désormais rencontrés par des prestataires de services du secteur de la Santé.

Les données sensibles qui transitent dans le milieu médical sont au cœur des préoccupations. Car si leur attractivité aux yeux des cyber-criminels ne fait aucun doute, leur gestion occasionne de nombreux débats, en particulier dans le contexte actuel de structuration d'un cadre règlementaire européen.

L'objectif de ce livre blanc est donc de permettre aux responsables informatiques ainsi qu'à tout l'écosystème des sous-traitants et prestataires du secteur médical de se plonger dans un état de l'art de la question de la cybersécurité des établissements de santé.

Pour cela, nous vous proposons dans les pages qui suivent de décrypter les problématiques du secteur de la Santé, de vous offrir un inventaire opérationnel des solutions possibles et d'ouvrir quelques projections sur l'avenir de la sécurité informatique du secteur.

04 — Intervenants

01. Cybersécurité en santé : pourquoi une telle fragilité ?

08 — *Infographie : tour du monde des cyberattaques sur les établissements de santé*
10 — Des contraintes matérielles fortes : un parc informatique unique en son genre
14 — Transformation numérique en santé : une accélération tardive à pérenniser
16 — Le cas particulier des données de santé
17 — *Interview de Charles Blanc-Rolin : Quel lien entre accès à la donnée, santé et sûreté ?*

02. Anatomie d'une menace polymorphe aux points d'entrée multiples

22 — Comment les cyber-criminels s'introduisent-ils dans le SI des établissements de santé ?
26 — L'ensemble du parcours de soin dans la ligne de mire
28 — Ceci n'est pas une cyberattaque

03. Quels remèdes pour sécuriser le monde de la santé ?

32 — Quelles mesures pour protéger les infrastructures de santé ?
37 — *Focus : quelles obligations réglementaires pour les établissements de santé*
38 — Une prise de conscience et des efforts soutenus par l'action publique
40 — *Interview croisée : Le règlement européen sur les données de santé est-il à la hauteur des enjeux ?*

04. Et demain ?

46 — Un continuum de soin à l'échelle européenne
48 — Médecine préventive, pilotage de l'hôpital par la donnée : les promesses (et les défis) du Big Data médical
50 — Une collaboration à construire
52 — *Interview de Jacky Grisey : L'avenir de la cybersécurité en santé*

Intervenants

CHARLES BLANC-ROLIN

CHEF DE PROJET SÉCURITÉ NUMÉRIQUE
E-SANTÉ PAYS DE LA LOIRE

« Il m'est arrivé de mettre en place des solutions de blocage physique des ports USB en lien avec le ou la responsable biomédical. Cela évite par exemple que quelqu'un n'utilise l'échographe pour recharger son smartphone... »

PAGE 31

Quel lien entre accès à la donnée, santé et sûreté ?

PAGE 17

JACQUES LABIDURIE

RSSI CHU LIMOGES

« Les industriels doivent être formés à la cybersécurité, car beaucoup font encore de l'informatique comme il y a 30 ans. La sécurité informatique doit également entrer dans le cursus des médecins et pas uniquement la protection de données comme c'est le cas actuellement. »

PAGE 34

JACK GRISEY

SECURITY OPERATIONS MANAGER
DÉDIÉ SANTÉ ADVENS

« Les cyberattaques importantes qui se sont produites depuis quelques années ont mis en lumière la dette technique et organisationnelle des systèmes d'information des établissements de santé. Une prise de conscience a eu lieu, y compris au plus haut niveau de l'État. »

PAGE 42

L'avenir de la santé en cybersécurité

PAGE 52



CORALIE ACHARD-TORTUL

DPO CHU DE LIMOGES

« La mise en contexte est très importante dans nos actions de sensibilisation. La rencontre au préalable avec le chef de pôle permet par exemple de comprendre comment celui-ci fonctionne et de récolter des exemples réels, comme le fait de laisser sa carte en place lors de différentes manipulations radio… »

PAGE 35

JEAN-SYLVAIN CHAVANNE

RSSI CHU BREST

« Fausse facture, demande de renouvellement de mot de passe captieuse, plainte de patient imaginaire… la qualité des campagnes de phishing que nous interceptons s'accroit. Certains vont même jusqu'à usurper l'identité du CHU de Brest. »

PAGE 23

Pleins feux sur les dispositifs médicaux connectés

PAGE 13

STÉPHANE PRÉVOST

PRODUCT MARKETING MANAGER
STORMSHIELD

« Installer un correctif pour une vulnérabilité critique sur un composant exposé sur Internet n'est pas la garantie d'être protégé contre une exploitation antérieure. Il faut également analyser ses journaux pour vérifier si elle a été exploitée et en cas de doute renouveller l'ensemble de ses comptes. »

PAGE 34

RAYNA STAMBOLIYSKA

EXPERTE DIPLOMATIE NUMÉRIQUE,
SPÉCIALISTE CYBERSÉCURITÉ ET MEMBRE INDÉPENDANTE DU GROUPE DE TRAVAIL SUR LES MENACES ÉMERGEANTES ET FUTURES DE L'ENISA

« Les textes DSA et DMA, qui abordent le sujet de façon transverse et systémique, s'inscrivent dans la lignée des différents textes dont le RGPD, la directive NIS ou encore le Data Act. Ils cherchent à la fois à protéger l'innovation, protéger les résidents européens et asseoir l'autorité stratégique de l'Union européenne. »

PAGE 37

Le règlement européen sur les données de santé est-il à la hauteur des enjeux ?

PAGE 41

DAMIAN KLIMAS

ASSOCIÉ DOTLAW ET OBSERVATEUR
DU RÉSEAU EHEALTH NETWORK

« L'adoption de l'EHDS va accélérer le déploiement de MaSanté@EU. Cela signifie que d'ici 2025, les établissements de santé de tous les États membres et de la Norvège auront accès facilement et de manière sécurisée aux allergies, prescriptions et antécédents médicaux de n'importe quel patient, dans leur langue, même si celui-ci réside dans un autre pays européen. »

PAGE 47

Le règlement européen sur les données de santé est-il à la hauteur des enjeux ?

PAGE 41



01.

Cybersécurité en santé : pourquoi une telle fragilité ?

Comment expliquer que les établissements hospitaliers, les cliniques, les pharmacies et les laboratoires soient si vulnérables aux cyber-risques ? De l'architecture des systèmes d'information de santé à leurs composants, en passant par les nouveaux usages du monde médical, les raisons sont malheureusement aussi diverses que variées.

Tour du monde des cyberattaques sur les établissements de santé



Healthcare Service Executive
2021 – IRLANDE

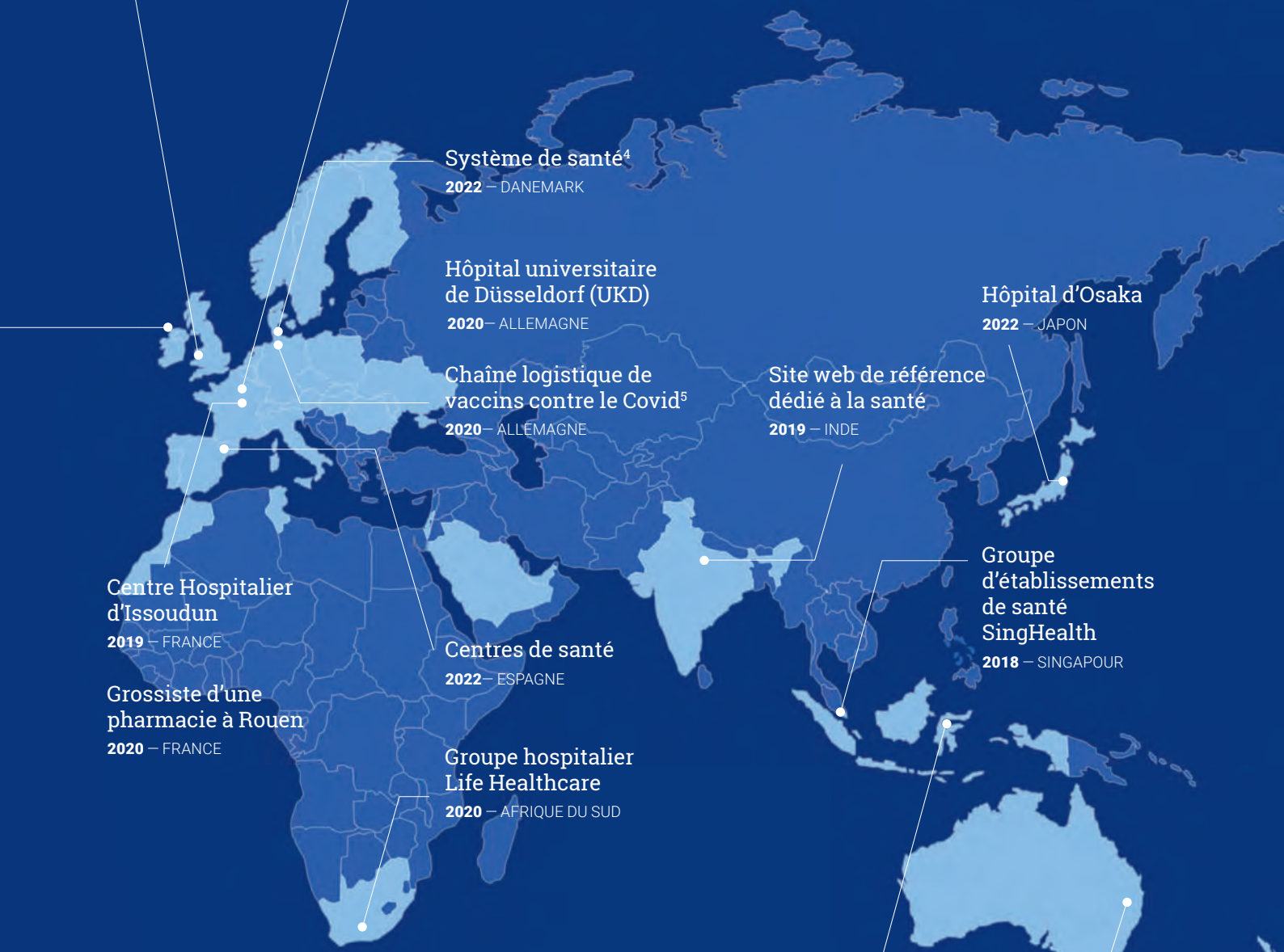
Système de santé de la province de Terre-Neuve-et-Labrador[3]
2021 – CANADA

Hôpital pour enfants de Boston
2014 – ÉTATS-UNIS

Centre médical presbytérien de Hollywood
2016 – ÉTATS-UNIS

Hôpitaux de Baton Rouge General, Jack Huston Memorial et Southwest Health[2]
2022 – ÉTATS-UNIS

Ministère de la Santé
2021 – BRÉSIL



Centre Hospitalier Universitaire d'Ile-de-France AP-HP
2020 — FRANCE

Organisations de santé
2020 — ROYAUME-UNI

Centre Hospitalier Sud Francilien de Corbeil Essonne
2022 — FRANCE

National Health Service
2017 — ROYAUME-UNI

Système français d'Assurance
2022 — FRANCE

Système de santé[4]
2022 — DANEMARK

Hôpital universitaire de Düsseldorf (UKD)
2020— ALLEMAGNE

Hôpital d'Osaka
2022 — JAPON

Chaîne logistique de vaccins contre le Covid[5]
2020— ALLEMAGNE

Site web de référence dédié à la santé
2019 — INDE

Centre Hospitalier d'Issoudun
2019 — FRANCE

Groupe d'établissements de santé SingHealth
2018 — SINGAPOUR

Centres de santé
2022— ESPAGNE

Grossiste d'une pharmacie à Rouen
2020 — FRANCE

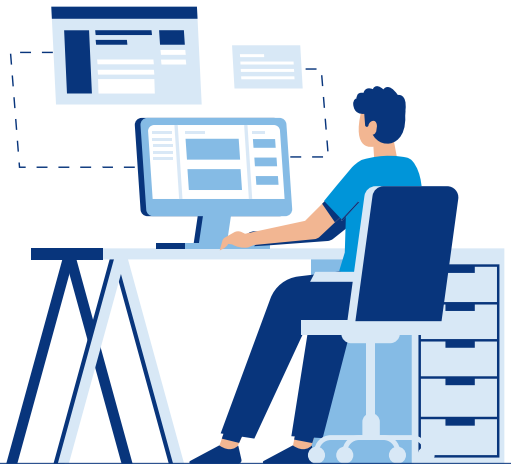
Groupe hospitalier Life Healthcare
2020 — AFRIQUE DU SUD

Hôpitaux de Dharmais et Harapan Kita
2017 — INDONÉSIE

Entreprise australienne d'assurance
2022 — AUSTRALIE

1.1 Des contraintes matérielles fortes : un parc informatique unique en son genre

Le réseau informatique constitue une partie critique du fonctionnement de l'hôpital. Il agit comme une véritable courroie de transmission avec le réseau opérationnel et l'extérieur mais doit faire avec un parc informatique particulier et des maux inhérents au secteur de la Santé.



OBSOLESCENCE, CONVERGENCE DES SI, PERMÉABILITÉ DES RÉSEAUX : DES MAUX PARTAGÉS

À l'instar d'autres secteurs, notamment industriels, le secteur de la santé est sujet à l'obsolescence logicielle. Ainsi, il n'est pas rare d'être confronté à des parcs en établissements de santé dont le socle logiciel n'a pas évolué depuis 20 ans. Cette durée de vie conséquente, due à un amortissement du matériel médical, a pour effet que ces versions de systèmes ne sont pas maintenues et deviennent obsolètes, à l'image de Windows XP. Elles fragilisent alors la sécurité de ces environnements.

Une vulnérabilité renforcée par la perméabilité des réseaux, à l'image de la convergence des SI dans les groupements hospitaliers de territoire en France (GHT). Interconnectés de façon non sécurisée, ils augmentent en effet le risque de propagation des cyberattaques.

Enfin, la télémaintenance, répandue depuis longtemps dans les hôpitaux du fait des interventions à distance de constructeurs de dispositifs médicaux, d'éditeurs ou d'intégrateurs de solutions applicatives, présente également un risque puisque les accès sont plus ou moins sécurisés.

LA GESTION SENSIBLE DES BÂTIMENTS HOSPITALIERS

Parler de cybersécurité évoque immédiatement l'univers des systèmes d'information. Cependant, il est aujourd'hui nécessaire d'aborder la question de façon plus large du fait de l'interconnexion croissante entre réseaux informatiques et réseaux opérationnels.

Ainsi, le périmètre comprend également les infrastructures techniques (Gestion Technique Centralisée [GTC], Gestion Technique du Bâtiment [GTB]). Ces dernières permettent de gérer la sécurité incendie, les accès, la vidéosurveillance, la gestion énergétique ou encore la qualité de l'air intérieur d'un bâtiment hospitalier.

« Même en s'appuyant sur le référentiel général de sécurité (RGS)[6], il est encore difficile de faire appliquer aux géants de l'industrie biomédicale les exigences minimales de sécurité sur leurs protocoles de télémaintenance par exemple. Bien souvent, augmenter la sécurité à ce niveau ressemble encore à un bras de fer. »

CHARLES BLANC-ROLIN — CHEF DE PROJET SÉCURITÉ NUMÉRIQUE E-SANTÉ PAYS DE LA LOIRE

Ces différents systèmes opérationnels, composés d'automates de marques et de générations hétérogènes, sont encore trop souvent connectés avec le réseau informatique de façon non sécurisée et passent parfois sous le radar des responsables de la sécurité des systèmes d'information. De même, l'infrastructure téléphonique de l'établissement de santé est souvent négligée. Or la mise hors service des téléphones IP d'un hôpital par une attaque DDoS aurait des conséquences désastreuses.

Cette problématique en devient d'autant plus complexe qu'une même structure gère parfois différents bâtiments disséminés sur le territoire.

FLASHER

UN SCÉNARIO DE CYBERATTAQUE

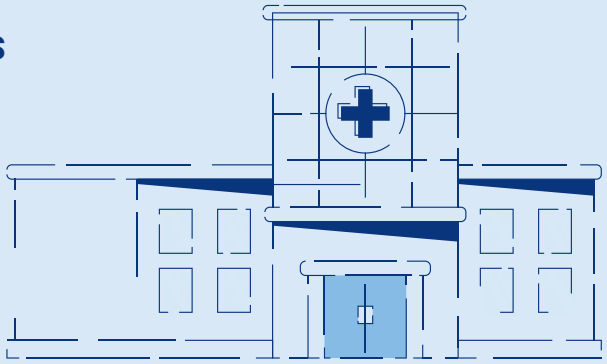
a Découvrez un scénario concret de cyberattaque sur la sécurité incendie d'un établissement hospitalier. —

À NOTER

LA QUALITÉ DE L'AIR

relève du confort dans les chambres des patients mais elle revêt un caractère vital au bloc opératoire.

LA GESTION SENSIBLE DES BÂTIMENTS HOSPITALIERS



- Liens avec d'autres services d'urgence
- Intégration du système
- Validation du système
- Systèmes commerciaux et administratifs
- Services aux patients
- Gestion de l'énergie
- Chauffage, ventilation et climatisation
- Protection du périmètre
- Structuration et gestion des câbles
- Communications voix et données
- Convergence IP
- Services et maintenance
- Télévision par antenne
- Vidéo d'information publique/ panneaux d'affichage
- Services de très basse tension
- Sonorisation et annonces vocales
- Éclairage
- Détection et alarme incendie
- Contrôle des accès
- Gestion des ascenseurs et des escaliers mécaniques
- Gestion de la localisation des patients/des biens/ du flux de travail clinique
- Sécurité/télévision en circuit fermé et vidéosurveillance numérique

LA PROTECTION DES ÉQUIPEMENTS BIOMÉDICAUX SOUS LE FEU DES PROJECTEURS

Utilisés en imagerie médicale ou encore en biologie, une grande partie des équipements biomédicaux est connectée au système d'information (SI).

C'est ce qui permet par exemple à certains chirurgiens d'être assistés en direct par un ou une collègue à l'autre bout du monde via une caméra connectée.

En plus d'améliorer le confort des soins pour les patients, cet Internet des objets médicaux (IoMT) aide au diagnostic et améliore la collaboration entre professionnels de santé. Il apporte même une réponse partielle à la problématique des déserts médicaux dans le cas de la télémédecine. Mais il représente un risque pour la sécurité de l'hôpital.

Ces dispositifs, rarement visés de façon ciblée, font souvent partie des dommages collatéraux des cyberattaques. Leur faiblesse : être connecté au réseau sans embarquer la sécurité nécessaire… Et ce, alors qu'ils sont en contact direct avec les patients.

Conçus par des fabricants industriels à la culture cyber limitée, ils constituent souvent de potentiels nids à microbes.

ACTU

UN MOT DE PASSE EN DUR

a Une vulnérabilité a été révélée en octobre 2022 sur un équipement de laboratoire médical utilisé pour les dépistages du cancer du col de l'utérus. La faute à des informations d'identification codées en dur dans l'équipement.

20 000

CHIFFRE CLÉ

ÉQUIPEMENTS BIOMÉDICAUX

Il s'agit du nombre d'équipements biomédicaux répartis sur l'ensemble du Centre Hospitalier Universitaire (CHU) de Brest.

ACTU

L'ATTAQUE DE TROP

À la suite de l'attaque visant le Centre hospitalier Sud-Francilien[7] basé à Corbeil-Essonnes fin août 2022, le gouvernement a injecté 20 millions d'euros dans l'ANSSI pour renforcer son accompagnement des hôpitaux.

« Les établissements de santé ne connaissent pas toujours le système d'exploitation sur lequel reposent ces dispositifs, souvent vulnérable et obsolète, ni les logiciels et bibliothèques embarqués. Dans ces conditions, difficile de réagir lors de la publication de vulnérabilités »

CHARLES BLANC-ROLIN — CHEF DE PROJET SÉCURITÉ NUMÉRIQUE E-SANTÉ PAYS DE LA LOIRE

UN SECTEUR SOUS TENSION

La cybersécurité en santé fait aussi les frais du manque de moyens général du secteur. Des financements ont été débloqués par le gouvernement ces dernières années mais ceux-ci concernent seulement les investissements et non la maintenance. La sécurité informatique dans le monde du soin souffre également d'un manque de ressources et d'experts dédiés. —

« Aujourd'hui, nous concentrons nos ressources humaines en sécurité informatique sur la partie projet : nous n'avons aucune ressource opérationnelle malgré un poste ouvert en février. »

JACQUES LABIDURIE — RSSI CHU LIMOGES

PLEINS FEUX SUR LES DISPOSITIFS MÉDICAUX CONNECTÉS

AVEC **JEAN-SYLVAIN CHAVANNE** — RSSI CHU BREST

a **Le marquage CE médical. Ce signe de conformité, apposé sur les dispositifs médicaux, représente un défi de sécurité majeur. En effet, toute modification structurelle remettrait en cause le marquage, ce qui empêche d'effectuer les mises à jour et patchs de sécurité nécessaires sur ces objets ou machines de santé.**

Cette situation expose particulièrement les dispositifs médicaux aux vulnérabilités type Log4Shell et oblige à recourir à des solutions de sécurisation périmétrique (cloisonnement réseau, éléments de supervision, etc.).

Cette approche nécessite des compétences précises que les équipes informatiques ne maitrisent pas forcément. Il y a donc un vrai enjeu de formation à la cybersécurité et de collaboration entre les services IT, RSSI et biomédical.

Sans quoi des situations critiques perdureront, à l'image d'équipements de radiothérapie encore infectés par le ver Conficker en 2022, à cause d'une version obsolète de Windows. —

1.2 Transformation numérique en santé : une accélération tardive à pérenniser

Ces dernières années, la bascule du monde médical dans l'e-santé est indéniable. Le secteur est en pleine refondation. Il adopte de nouveaux usages qui ont été mis à l'épreuve dans le contexte tendu de la pandémie de Covid-19.



ESSOR DE LA TÉLÉMÉDECINE ET TÉLÉSURVEILLANCE

Le recours de plus en plus courant à la télémédecine et à la télésurveillance, notamment dans le cadre des hospitalisations à domicile, étend la surface d'attaque potentielle des établissements de santé. En effet, lorsqu'un patient bénéficie d'une assistance respiratoire chez lui, son respirateur peut devenir un nouveau point d'entrée vers le système d'information de l'hôpital.

EXTERNALISATION DE SERVICES

Le service le plus emblématique de ces usages est sans doute l'externalisation de la prise de rendez-vous via des plateformes en ligne, comme Doctolib, qui ne va pas sans soulever son lot de questions et de polémiques, notamment sur la sécurité des données échangées.

« Le recours massif à des services numériques externalisés, souvent moins sécurisés, y est une pratique largement répandue que les attaquants ne manquent pas d'exploiter. »

ANSSI — 2020[8]

DES FAILLES HUMAINES : UNE MÉCONNAISSANCE DES RISQUES CYBER

Et il y a le facteur humain. Car la transformation numérique dans l'univers de la Santé impacte les collaborateurs des établissements de Santé. Des collaborateurs qui ne partagent pas tous les mêmes réflexes d'hygiène numérique... Comme le détaille l'ANSSI dans son guide d'hygiène numérique : *« Chaque utilisateur est un maillon à part entière de la chaîne des systèmes d'information. À ce titre et dès son arrivée dans l'entité, il doit être informé des enjeux de sécurité, des règles à respecter et des bons comportements à adopter en matière de sécurité des systèmes d'information à travers des actions de sensibilisation et de formation. »*

26 janvier 2022

Une fragilité renforcée par la pratique du Bring Your Own Device (BYOD) : certains médecins, qui partagent leur temps entre cabinet privé et hôpital, utilisent du matériel non fourni par ce dernier et parfois non conforme à ses règles de sécurité informatique. —

DATE CLÉ

LE 26 JANVIER 2022 EN FRANCE

Date à laquelle la Haute Autorité de Santé a publié les quatre premiers référentiels de télésurveillance médicale pour les pathologies suivantes : diabète, insuffisance cardiaque chronique, insuffisance rénale chronique, et insuffisance respiratoire chronique.

D'autres travaux sont à venir pour enrichir ce socle, destiné à déployer la télésurveillance de façon pérenne et sécurisée. —

1.3 Le cas particulier des données de santé

Le monde de la santé est particulièrement visé par les cyber-criminels du fait du nombre de données de santé, sensibles et vitales par nature, qu'il traite. Quelles sont-elles et quels sont les enjeux qui les entourent ?



QUEL LIEN ENTRE ACCÈS À LA DONNÉE, SANTÉ ET SÛRETÉ ?

INTERVIEW

CHARLES BLANC-ROLIN
— CHEF DE PROJET SÉCURITÉ NUMÉRIQUE
E-SANTÉ PAYS DE LA LOIRE

« Les chirurgiens préfèreront revenir à une médecine de guerre : cela implique de faire sans donnée plutôt que de se fier à des données potentiellement erronées ou partielles. »



Comment définissez-vous une donnée de santé ?

C.BR — Le terme désigne toute donnée qui a trait à la santé du patient, qu'il s'agisse d'un compte rendu opératoire, de la cotation d'un acte médical ou encore d'un rendez-vous avec un professionnel de santé.

En quoi l'accès à cette donnée de santé est-il lié à la sureté des patients ?

C.BR — La question des données sensibles est souvent abordée sous l'angle de la **confidentialité**. Le grand public redoute la divulgation de ses numéros de cartes bancaires mais se représente mal les conséquences d'un vol de numéro de sécurité sociale. Or dans les cas des données médicales plus qu'ailleurs, les conséquences sont graves. L'**intégrité** des données est une question de sûreté : en cas d'altération d'une posologie ou de suppression d'une mention d'allergie, c'est parfois la vie du patient qui est en jeu. La **disponibilité** est également très importante, les chirurgiens ont par exemple besoin d'images pour opérer.

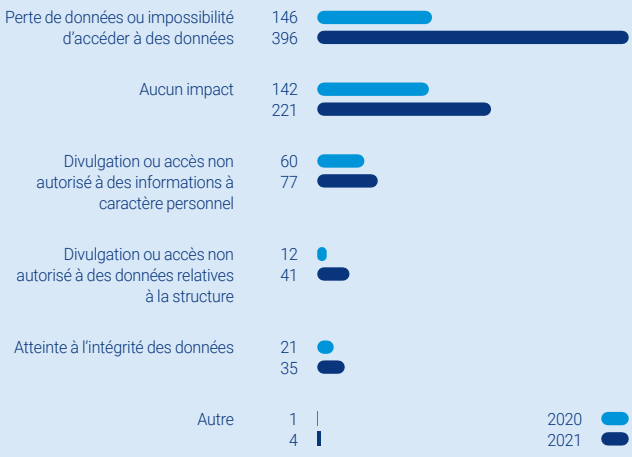
Pourquoi la confiance dans la donnée est-elle critique dans la santé ?

C.BR — Pour reprendre l'exemple des chirurgiens, ils préfèreront revenir à une **médecine de guerre** : cela implique de faire sans donnée plutôt que de se fier à des données potentiellement erronées ou partielles.

L'inaccessibilité des données est-elle fréquente dans le secteur de la santé ?

C.BR — D'après le CERT-Santé, c'était le cas pour « tout ou partie des données des applications de la structure » dans la moitié des incidents signalés en 2021. —

RÉPARTITION DES INCIDENTS DE SÉCURITÉ PAR TYPE D'IMPACT SUR LES DONNÉES



Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé (2021)

DE PLUS EN PLUS DE DONNÉES À PROTÉGER

Autre paramètre à prendre en compte, le volume de données générées par les établissements de santé n'a cessé de croitre ces dernières années.

La dématérialisation est clairement à l'œuvre dans le quotidien des praticiens avec le déploiement de services numériques socles à l'instar de « Mon espace santé ». Disponible depuis le début de l'année 2022, cet espace permet à chaque Française et à chaque Français de retrouver tous ses documents de santé (ordonnances, résultats de biologie, etc.), de renseigner des informations personnelles sur ses antécédents familiaux et d'échanger de façon sécurisée avec les professionnels de santé.

Le numérique fait également désormais partie intégrante des processus métier des soignants comme l'illustre la multiplication des outils d'aide au diagnostic comme Psychaclic[9] ou l'obligation en France depuis le 1er mars 2022 d'établir les certificats de décès par voie électronique.

Des bases de données toujours plus fournies dont la gestion et le maintien en conformité s'annoncent de plus en plus complexes, entre obligations de conservation et droit à l'effacement[10] prévu par le RGPD…

UNE MINE (D'OR) D'INFORMATIONS

Si les données de santé peuvent être au cœur d'actes de malveillance ayant vocation à déstabiliser les opérations d'un hôpital ou à nuire à une personne en particulier, les cybercriminels en raffolent surtout parce que leur revente est très lucrative. Exemple en juin 2022 : 1 milliard de données personnelles chinoises dont des informations médicales avaient été mises en vente pour la somme de 10 Bitcoins (200 000 dollars)[11].

CHIFFRE CLÉ

x30

LE VOLUME TOTAL DES DONNÉES DE E-SANTÉ

En 2016, l'Anap indiquait que le volume total des données de e-santé doublait tous les 73 jours… Il aurait donc été multiplié par 30 depuis.

CHIFFRE CLÉ

Entre 50 et 250 €

DOSSIER MÉDICAL
C'est le prix de revente d'un seul dossier médical[12]

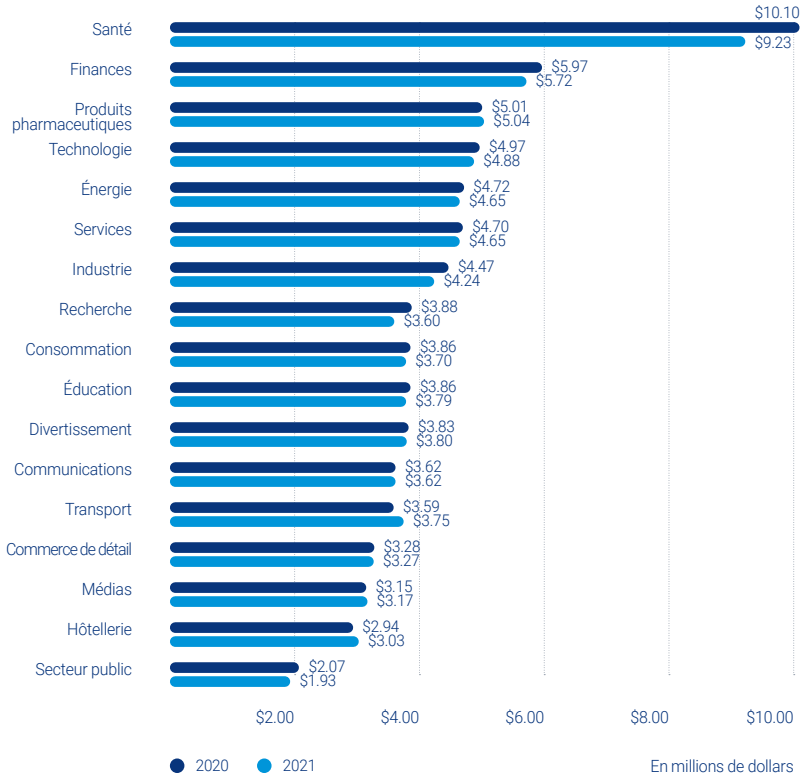
Les données de santé constituent donc une ressource précieuse qui intéresse également d'autres acteurs comme les GAFAM. Le site d'investigation The Markup[13] a ainsi révélé en juin 2022 que des établissements de santé américains transmettaient des informations sensibles (nom du médecin, mots-clés recherchés ou encore pathologie) sur leurs patients à Facebook via leur utilisation du « Meta Pixel ».

DES FUITES QUI COÛTENT CHER

De plus en plus médiatisé, ce type d'affaires sensibilise petit à petit l'opinion publique. La réputation des entreprises victimes est également mise à l'épreuve à l'instar de Shields, un groupe américain d'imagerie et de chirurgie ambulatoire qui a subi un vol de données affectant près de 2 millions de personnes.

Mais le prix à payer est également sonnant et tranchant. Un rapport IBM[14] estime que le coût moyen d'une violation de données dans le cas d'une structure de santé dépasse les 10 millions de dollars. —

LE COÛT MOYEN D'UNE FUITE DE DONNÉES PAR MARCHÉ VERTICAL, DOMINÉ PAR LA SANTÉ



1,5 M€

CHIFFRE CLÉ

AMENDE

1,5 million d'euros. C'est le montant de l'amende dont la société Dedalus Biologie a écopé pour défaut de sécurité « ayant conduit à la fuite de données médicales de près 500 000 personnes » (CNIL).

POUR ALLER PLUS LOIN

CINQ WEBINAIRES DÉDIÉS

a Retrouvez notre série de 5 webinaires[15] pour aller plus loin sur la question de l'hypersensibilité des milieux hospitaliers face aux cyberattaques.



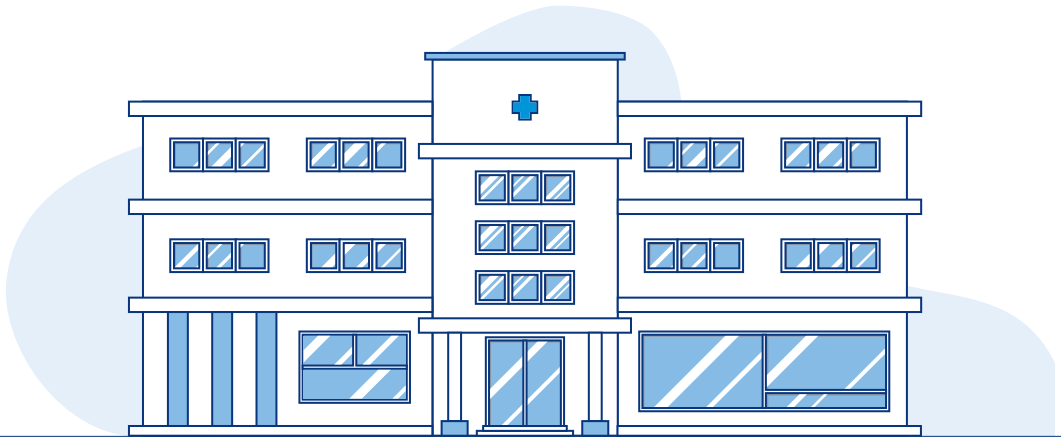
02.

Anatomie d'une menace polymorphe aux points d'entrée multiples

Par quels vecteurs la menace cyber pénètre-t-elle dans les établissements de soin ? Quels sont les différents types d'attaques qu'ils subissent ? S'agit-il toujours d'incidents ciblés ? Les cyber-criminels ne manquent pas d'ingéniosité pour s'en prendre au monde médical, mais parfois l'incident de sécurité est dû à une défaillance et non à une cyberattaque. Ses conséquences sont pourtant tout aussi désastreuses.

2.1 Comment les cyber-criminels s'introduisent-ils dans le SI des établissements de santé?

Les points d'entrée des cyber-menaces dans les structures de soin sont malheureusement nombreux. Il est possible de les regrouper en quatre vecteurs.



1. HUMAIN

Les cyberattaques utilisent ou ciblent un ou plusieurs individus (médecins, infirmiers, agents, administrateurs jusqu'aux patients eux-mêmes).
En 2020, un grossiste rouennais, fournisseur des pharmacies de la région, a passé une commande de 6,6 millions d'euros pour des gels et masques à une société qui s'est finalement avérée être fantôme. Un exemple dramatique d'arnaque au président[16] dans le contexte tendu de la pandémie de Covid-19.

2. LOGICIEL

Les cyberattaques logicielles regroupent toutes les attaques qui exploitent une faiblesse, une faille ou l'obsolescence d'un logiciel installé sur un équipement informatique ou un instrument médical informatisé.
En 2020, une polémique a mis au jour un certain nombre de failles de sécurité dans une solution du groupe Dedalus, spécialisé dans les logiciels de santé. L'une d'elles permettait d'accéder aux tickets ouverts par les hôpitaux et laboratoires clients de la société, dans lesquels pouvaient se trouver des identifiants et mots de passe de télé-administration.

3. RÉSEAU

Comme son nom l'indique, une cyberattaque réseau correspond à toutes les cyberattaques transitant par le réseau de l'hôpital.
Les services de l'Assistance Publique – Hôpitaux de Paris (AP-HP) ont été visés en 2020 par une attaque réseau par déni de service (DDoS) sur deux de ses adresses internet. Résultat : un accès perturbé à la messagerie et aux applications pour les collaborateurs.

4. PHYSIQUE

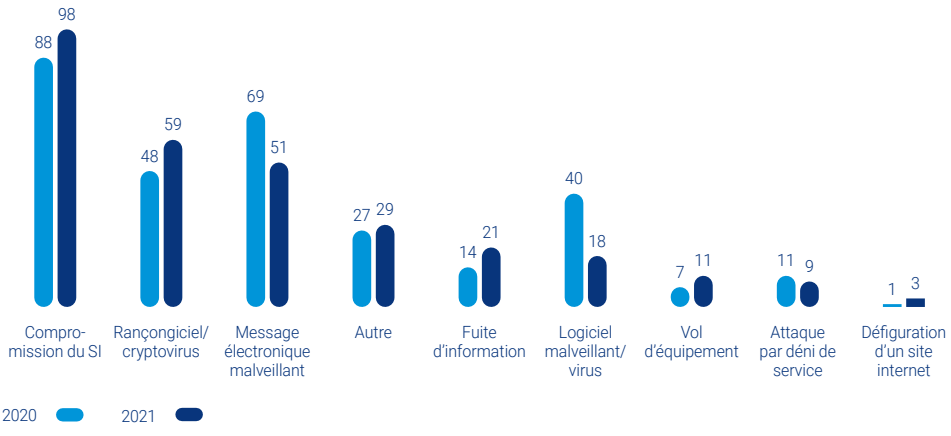
Les cyberattaques physiques regroupent les attaques qui visent spécifiquement la dimension matérielle d'un équipement médical, informatique ou opérationnel.
Dès 2019, des chercheurs israéliens ont simulé une attaque *man-in-the-middle* en introduisant un Raspberry Pi au sein même d'un hôpital. Ils ont ainsi pu intercepter des données d'imagerie médicale transmises via le protocole DICOM et démontrer que celles-ci pouvaient être altérées.

Quel que soit le vecteur d'attaque choisi par le cyber-criminel, la « charge virale » la plus commune dans le secteur de la santé aujourd'hui est le ransomware. Mais les structures de soin sont également fortement exposées aux attaques de déni de service distribué et au vol de données. —

« Fausse facture, demande de renouvellement de mot de passe captieuse, plainte de patient imaginaire, la qualité des campagnes de phishing que nous interceptons s'accroît, certaines vont même jusqu'à usurper l'identité du CHU de Brest. Mais l'augmentation la plus flagrante concerne les initial access brokers (IAB). Ces courtiers en accès initiaux se spécialisent dans la recherche d'identifiants utilisateurs pour les revendre. »

JEAN-SYLVAIN CHAVANNE
— RSSI CHU BREST

NOMBRE D'INCIDENTS PAR TYPE D'ORIGINE



Source : rapport IBM Security, Cost of Data Breach (2022)



2.2 L'ensemble du parcours de soin dans la ligne de mire

Hôpitaux et cliniques représentent la première cible des cyberattaques dans le monde de la Santé. Mais ils ne sont pas les seuls. Laboratoires, fournisseurs et même patients sont aussi dans le viseur des cyber-criminels.



Plusieurs établissements hospitaliers américains en ont déjà fait les frais en 2022 (Baton Rouge General en Louisiane, Jack Huston Memorial à Phoenix et le Southwest Health Center dans le Wisconsin), ainsi qu'en France (Vitry-le-François, Saint-Dizier, Charleville-Mézières, Corbeil-Essonnes) et en Espagne (Barcelone).

Mais les laboratoires sont également visés, notamment pour les données médico-administratives qu'ils saisissent dans des logiciels de biologie médicale du type Mega Bus[18].

Plus récemment, les cyber-criminels ont encore élargi leur panel de cibles. D'une part, ils s'attaquent désormais aux différents fournisseurs, qui peuvent leur ouvrir les portes virtuelles des systèmes d'information des établissements hospitaliers. Et d'autre part, ils n'hésitent plus désormais à s'en prendre aux patients eux-mêmes, victimes de chantage suite à des vols de leurs données de santé et/ou personnelles. —

QUAND LES CYBER-CRIMINELS VISENT LES PATIENTS

a **En 2020, les patients d'une vingtaine de centres de psychothérapie finlandais, gérés par la société Vastaamo, ont eu la mauvaise surprise de recevoir une demande de rançon de 500 euros à régler en Bitcoin, sous peine de divulgation des données récoltées lors de leurs séances. Un cas de double extorsion[19] qui a généré des milliers de plaintes auprès des autorités. —**

QUAND LES CYBER-CRIMINELS VISENT LA CHAÎNE LOGISTIQUE

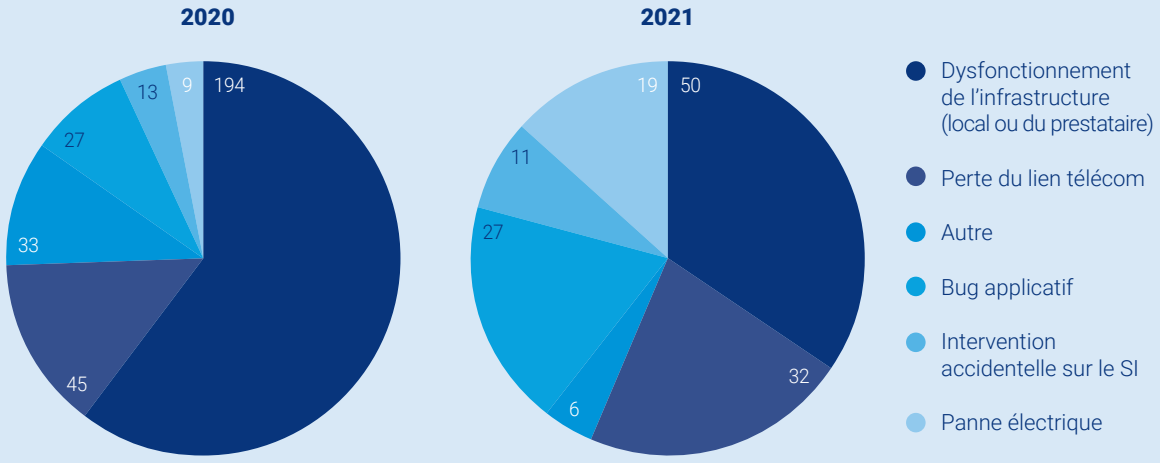
a **En 2020, des prestataires spécialisés dans la chaîne du froid des vaccins contre le Covid-19 ont été la cible de campagnes de phishing. L'objectif : récupérer des informations sensibles sur leur transport et leur distribution. Une campagne qui a les caractéristiques d'une attaque d'un niveau étatique, d'après les chercheurs en cybersécurité d'IBM. —**

2.3 Ceci n'est pas une cyberattaque

S'il faut bien sûr prendre toutes les mesures nécessaires pour se protéger des cyberattaques, il ne faut pas oublier que même les incidents d'origine non malveillante peuvent avoir de graves conséquences sur le système de santé.



RÉPARTITION DES INCIDENTS D'ORIGINE NON MALVEILLANTE



Source : Observatoire des signalements d'incidents de sécurité des systèmes d'information pour le secteur santé (2021)

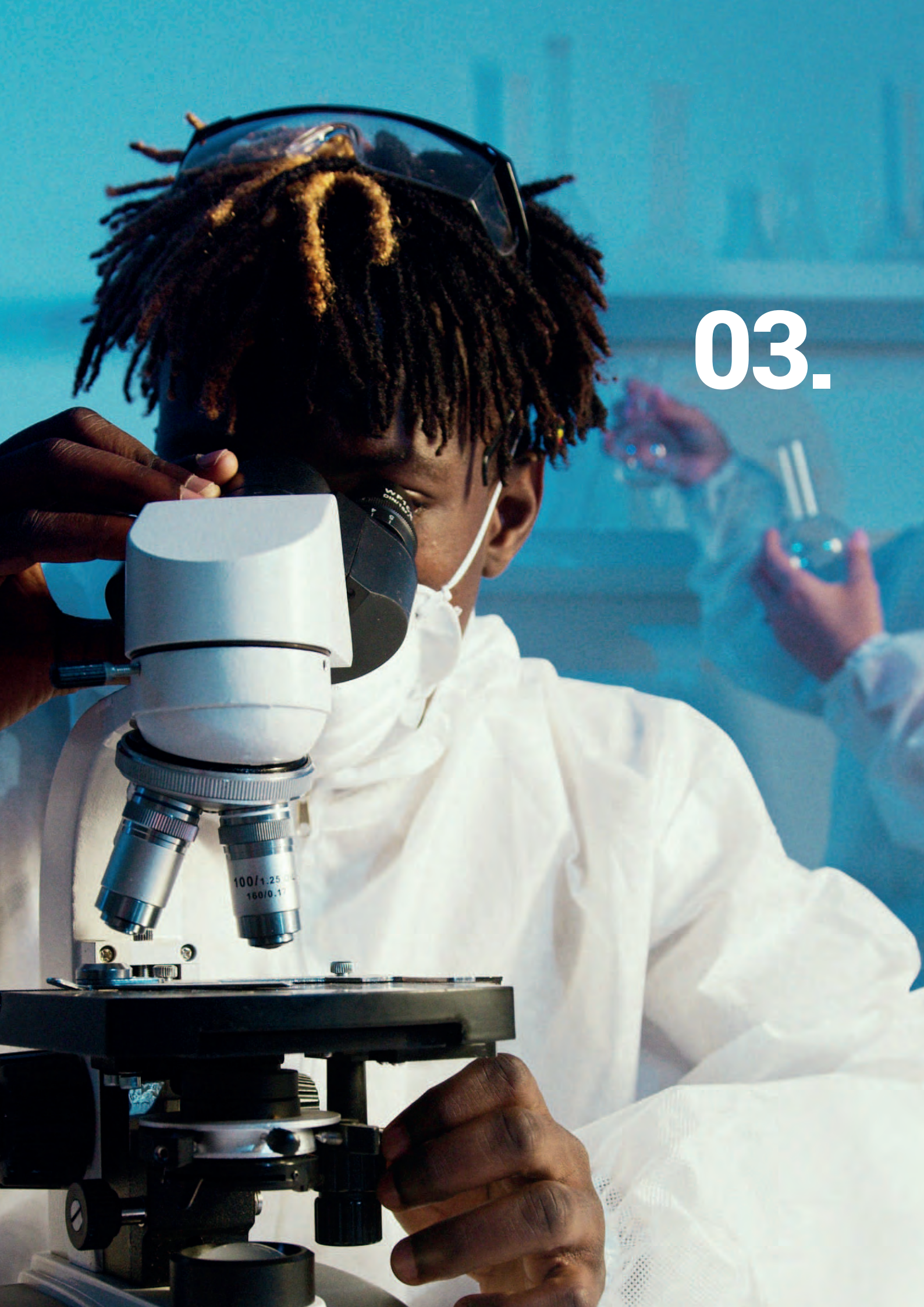
Dans un univers hospitalier vulnérable et fragile, un incident informatique peut en effet déboucher sur un incident de sécurité. Comme en juin 2022 du côté du CHU de Nantes, où une panne majeure, causée par l'antivirus installé, a affecté tous les postes de travail sous Windows 7, y compris des équipements biomédicaux rendus inutilisables. —

48%

CHIFFRE CLÉ

NON MALVEILLANT

48 % des signalements à l'Observatoire CERT-Santé[20] ne sont pas d'origine malveillante



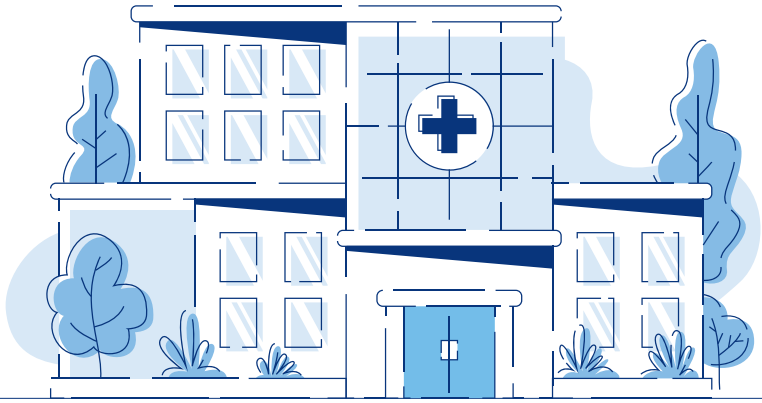
03.

Quels remèdes pour sécuriser le monde de la santé?

Comment se prémunir des cyberattaques ? Que dit la législation actuelle à ce sujet ? Quelle aide peuvent fournir les autorités publiques à ce niveau ? La démarche peut s'avérer complexe, mais vitale pour se protéger convenablement.

3.1 Quelles mesures pour protéger les infrastructures de santé ?

Les infrastructures des établissements de santé sont vitales par nature. La performance et la disponibilité des réseaux informatiques de nos systèmes de santé sont d'autant plus importantes que la vie de patients dépend souvent des informations qu'ils permettent d'échanger.



ÉTAPE 1 : AUDIT ET ANALYSE DE RISQUES

La première mesure de toute démarche de protection cyber doit concerner la connaissance des systèmes. À ce stade, le but est d'identifier les actifs les plus sensibles afin de réduire la surface d'attaque en définissant une politique de sécurité.

« Cette cartographie permet de repérer et de classifier les composants des systèmes d'information et opérationnels des structures de santé selon différents critères tels que l'obsolescence ou la criticité. »

STÉPHANE PREVOST — PRODUCT MARKETING MANAGER, STORMSHIELD

ÉTAPE 2 : DÉPLOIEMENT DE SOLUTIONS DE SÉCURITÉ ADAPTÉES

Ces moyens, fournis par des équipements comme ceux proposés par Stormshield, couvrent différents périmètres.

Protection des réseaux

Parmi les fonctionnalités à réunir pour sécuriser les réseaux informatiques hospitaliers figurent :

- La segmentation réseau,
- Le contrôle des accès, la gestion de la télémaintenance et autres accès à distance,
- La sécurisation des communications,
- L'authentification à double facteur,
- Le filtrage par utilisateur,
- La sécurisation des protocoles de communication des équipements biomédicaux (prévention d'intrusion - IPS OT).

Protection des postes de travail

Pour bénéficier d'une protection renforcée de leurs terminaux, les établissements de santé doivent veiller à mettre en place :

- L'authentification à double facteur,
- La prévention d'intrusion sur les postes (HIPS) par analyse comportementale,
- La gestion des périphériques externes (jusqu'à la mise en place de stations blanches).

« Il m'est arrivé de mettre en place des solutions de blocage physique des ports USB en lien avec le ou la responsable biomédical. Cela évite par exemple que quelqu'un n'utilise l'échographe pour recharger son smartphone en risquant de compromettre le dispositif. »

CHARLES BLANC-ROLIN — CHEF DE PROJET SÉCURITÉ NUMÉRIQUE E-SANTÉ PAYS DE LA LOIRE

LA PSEUDONYMISATION OU LA RÉVERSIBILITÉ DE L'ANONYMAT

AVEC **JEAN-SYLVAIN CHAVANNE** — RSSI CHU BREST

a « *L'une des particularités de la santé est que certaines données sensibles ne peuvent être rendues complètement anonymes : un établissement de santé peut en effet avoir besoin de remonter a posteriori à un patient ayant suivi un traitement spécifique par exemple. C'est pourquoi les données du patient sont divisées en deux bases de données pour permettre la réidentification en cas de besoin.* » —

L'application d'une politique de mots de passe suffisamment robustes[21] est également nécessaire afin d'éviter d'être la cible d'actions malveillantes depuis Internet.

Enfin, l'amélioration du suivi des correctifs est indispensable pour augmenter le niveau de sécurité des postes de travail au sein des structures de santé. Pour cela, il faut assurer une veille des composants exposés et les mettre à jour quand un correctif est mis à disposition, en traitant en priorité les vulnérabilités critiques. Le drame aurait ainsi pu être évité lors de la cyberattaque de l'hôpital de Düsseldorf : un patch de la vulnérabilité exploitée avait en effet été mis à disposition sept mois auparavant.

Protection des données

Si la première mesure à ce niveau est de proscrire l'envoi de tout dossier patient par email en clair, d'autres mesures sont nécessaires. Il faut garantir :

- Un dossier médical chiffré avec différentes clés d'accès,
- Le chiffrement de bout en bout des informations, particulièrement quand elles sont extraites du SI pour être transmises à un autre hôpital (dans le cadre d'un parcours de soin coordonné par exemple),
- Un processus d'anonymisation et de pseudonymisation pour un traitement efficace de la donnée.



ÉTAPE 3 : VÉRIFICATION ET AMÉLIORATION CONTINUE

L'étape suivante consiste à contrôler la conformité et à vérifier les écarts par rapport à la politique de sécurité. Pour cela, il convient notamment de :

- analyser régulièrement les journaux de ses équipements périmétriques,
- pratiquer des audits de sécurité ou des tests de pénétration,
- relancer une phase de planification en vue d'appliquer des actions correctives.

« L'intérêt des structures de santé pour le SOC managé vient confirmer l'attrait de la mutualisation des ressources au vu des difficultés de recrutement sur ces postes (pénurie de profils, financements, etc.). »

JACKY GRISEY — SECURITY OPERATIONS MANAGER DÉDIÉ SANTÉ, ADVENS

« Installer un correctif pour une vulnérabilité critique sur un composant exposé sur Internet n'est pas la garantie d'être protégé contre une exploitation antérieure. Il faut également analyser ses journaux pour vérifier si elle n'a pas été exploitée sur un autre composant et en cas de doute renouveler l'ensemble de ses comptes. »

STÉPHANE PRÉVOST — PRODUCT MARKETING MANAGER STORMSHIELD

S'ENGAGER DANS UNE DÉMARCHE DE SENSIBILISATION ET DE FORMATION

La sensibilisation est impérative pour espérer augmenter le niveau de protection des établissements de santé. Ces campagnes doivent s'adresser dans un premier temps aux professionnels du secteur comme ici en Centre-Val de Loire[22] avec le développement de **plateformes de sensibilisation et de formation** pour les établissements sanitaires et médico-sociaux. Mais ces actions de communication et sensibilisation doivent également s'adresser aux patients ainsi qu'aux fabricants de dispositifs médicaux. Avec un ton adapté à chaque population.

« Les industriels doivent être formés à la cybersécurité, car beaucoup font encore de l'informatique comme il y a 30 ans. La sécurité informatique doit également rentrer dans le cursus des médecins et pas uniquement la protection de données comme c'est le cas actuellement. »

JACQUES LABIDURIE — RSSI CHU LIMOGES

Certains acteurs n'hésitent pas à aller plus loin dans la responsabilisation des utilisateurs. Le centre hospitalier de Calais procède désormais à l'enregistrement des sessions sur ses serveurs[23], considérés comme critiques. Cette nouvelle politique s'applique même à ses prestataires dont 40 % procèdent de la sorte.

Toutefois, dans ce secteur déjà en grande tension, il faut impérativement **que la cybersécurité soit cohérente avec les pratiques métiers :** par exemple, les demandes répétées de saisie de mot de passe à 12 caractères en situation d'urgence ne sont pas adaptées. —

COMMENT SÉCURISER LES DISPOSITIFS MÉDICAUX SANS REMETTRE EN CAUSE LEUR MARQUAGE CE ?

a **La principale solution de sécurité réseau consiste à cloisonner les réseaux et à les isoler du reste du SI via une micro-segmentation. Ainsi, lorsqu'un besoin d'échange de flux se présente, il faut tâcher d'avoir un filtrage très fin, et prévoir si possible la détection d'anomalies sur ces mêmes flux via une sonde IDS par exemple. —**

« La mise en contexte est très importante dans nos actions de sensibilisation. La rencontre préalable avec le chef de pôle permet par exemple de comprendre comment celui-ci fonctionne et de récolter des exemples réels comme le fait de laisser sa carte en place lors de différentes manipulations radio. Les services administratifs, achats, recherche clinique, tous ont un vocabulaire spécifique qu'il faut maîtriser pour être efficace. »

CORALIE ACHARD-TORTUL —
DPO DU CHU DE LIMOGES

CYBER-SÉCURISER LES STRUCTURES DE SANTÉ AVEC STORMSHIELD

CYBERSÉCURITÉ & SANTÉ

a **Stormshield participe à la construction d'une cybersécurité européenne de confiance. Toutes les lignes de produits s'inscrivent dans une démarche continue de qualification et certification de sécurité auprès des autorités européennes compétentes.**

STORMSHIELD NETWORK SECURITY POUR LA PROTECTION RÉSEAU

Parce que la disponibilité des services est clé dans cet univers, la gamme de firewalls Stormshield Network Security (SNS) garantit la continuité et la disponibilité des services grâce à leur segmentation réseau, leur fonctionnalité bypass ou encore leur système de prévention des intrusions. Et pour protéger les données patients lors des échanges, ces firewalls sécurisent les accès à distance de télémaintenance, via des réseaux privés virtuels (VPN).

STORMSHIELD DATA SECURITY POUR LA PROTECTION DES DONNÉES

Protéger les données de santé devient un axe central et vital pour les établissements de soin. Avec un chiffrement de bout en bout, la Stormshield Data Security (SDS) préserve l'intégrité et la confidentialité des informations sensibles. Particulièrement quand la donnée est extraite du système d'information.

STORMSHIELD ENDPOINT SECURITY POUR LA PROTECTION DES SERVEURS ET DES POSTES DE TRAVAIL

Pour accompagner les transformations du secteur médical et les nouveaux usages professionnels, la solution Stormshield Endpoint Security (SES) offre une protection autonome aux terminaux, capables de modifier de manière dynamique les niveaux de protection en fonction de leur environnement.

STORMSHIELD LOG SUPERVISOR POUR LA VISIBILITÉ DES ÉVÉNEMENTS RÉSEAU

Grâce à l'outil Stormshield Log Supervisor (SLS), il est possible de visualiser en clin d'oeil l'état de votre réseau informatique et d'accéder aux journaux d'événements. Une solution idoine pour optimiser les tâches de recherche ainsi que la réponse aux incidents.

QUELLES OBLIGATIONS RÉGLEMENTAIRES POUR LES ÉTABLISSEMENTS DE SANTÉ ?



AUX ÉTATS-UNIS

a Le standard américain HIPAA (Health Insurance Portability and Accountability Act) s'applique, ainsi que son volet sur les données personnelles de santé baptisé ePHI (electronic Protected Health Information).

AU NIVEAU EUROPÉEN

a La directive NIS 2 liste un certain nombre d'obligations pour les opérateurs de services essentiels (OSE) dont font partie la plupart des établissements de santé disposant d'un service d'urgences médicales. Parmi elles, l'obligation de déclaration des incidents de sécurité. Comme toutes les organisations opérant dans l'Union européenne, elles doivent également se conformer au RGPD.

EN FRANCE

a Ces établissements sensibles, parfois classés opérateurs d'importance vitale (OIV), sont également soumis au Code de la santé publique, à l'instruction interministérielle n° 901, à la PGSSI-S. Depuis le mois d'avril, le premier document opposable de cette dernière, le référentiel d'identification électronique[24] est disponible. Il impose aux établissements et aux éditeurs des contraintes au niveau de l'identification des patients et des professionnels pour renforcer la sécurité des accès. En complément, les structures de santé peuvent se référer au guide des bonnes pratiques édité par l'ANSSI.

3.2 Une prise de conscience et des efforts soutenus par l'action publique

Pour autant, la vulnérabilité des établissements de santé n'est pas une nouveauté et préoccupe les professionnels depuis plus d'une décennie. Des initiatives existent déjà, tant au niveau européen qu'à une échelle nationale.



AU NIVEAU EUROPÉEN

Face à l'émergence d'une véritable économie de la donnée, l'Union européenne est en pleine structuration avec tout un éventail de textes à l'étude ou déjà entrés en application :

- Règlement général sur la protection des données (RGPD) à caractère personnel.
- Règlement sur le cadre global utilisation des données à l'échelle de l'Union européenne (Data Gouvernance Act [DGA]).
- Règlement sur les services numériques (Digital Services Act [DSA]).
- Règlement sur les marchés numériques (Digital Markets Act [DMA]).

Le projet de règlement sur l'Espace européen des données de santé (EHDS)[25] est le premier texte vertical du corpus, c'est-à-dire le premier texte à proposer un cadre de partage des données pour un secteur en particulier. Publié début mai 2022, il a été qualifié de « *nouveau départ pour la politique de santé numérique de l'Union* »[26] par Margarítis Schinás, vice-président de la Commission européenne. —

DATE CLÉ

Juillet 2016

Dès juillet 2016, l'Europe se saisissait du sujet cyber à travers la directive NIS et l'identification d'Opérateurs de Services Essentiels (OSE) dans le secteur de la Santé (aux côtés d'autres secteurs comme l'énergie, le transport, l'eau, la banque ou encore l'infrastructure numérique). L'objectif : protéger leurs systèmes d'information essentiels.

« Ces travaux (DSA et DMA), qui abordent le sujet de façon transverse et systémique, s'inscrivent dans la lignée des différents textes dont le RGPD, la directive NIS ou encore le Data Act. Ils cherchent à la fois à favoriser l'innovation, protéger les résidents européens et asseoir l'autorité stratégique de l'Union européenne. »

RAYNA STAMBOLIYSKA — EXPERTE DIPLOMATIE NUMÉRIQUE, SPÉCIALISTE CYBERSÉCURITÉ ET MEMBRE INDÉPENDANTE DU GROUPE DE TRAVAIL SUR LES MENACES ÉMERGEANTES ET FUTURES DE L'ENISA

INTERVIEW CROISÉE

CE RÈGLEMENT EUROPÉEN SUR LES DONNÉES DE SANTÉ EST-IL À LA HAUTEUR DES ENJEUX?

Ce texte répond aux enjeux auxquels nous sommes confrontés aujourd'hui. Il faudra l'actualiser d'ici 5 à 10 ans pour prendre en compte les nouvelles menaces qui auront émergé avec les technologies de décentralisation, Web 3.0, etc. mais à ce stade, **il s'agit d'un complément bienvenu au RGPD et à la directive NIS.**

C'est donc bien un jalon important de notre histoire commune mais il me semble que c'est la pandémie de COVID-19 qui a initié ce renouveau. C'est dans ce contexte que le réseau eHealth Network, qui réunit des représentants des États membres du numérique en santé et auquel je participe en tant qu'observateur, a fourni un premier exemple de coopération européenne : une boite à outils commune pour le développement d'applications mobiles de suivi de contact.

La pandémie a mis en évidence qu'il fallait continuer à réglementer le secteur pour réellement garantir la protection des données de santé. Les décideurs européens l'ont compris et ce règlement en est la preuve. **Il propose un schéma de sécurisation du partage de l'information, renforce les obligations de signalement d'incidents et d'interopérabilité.** Différents standards de certification (pour les dossiers patients informatisés, les applications de soin, etc.) devraient également en découler.

Ce texte, à la croisée d'autres régulations, figure parmi les plus avancés : nous pouvons même parler de texte unique en ce qui concerne les chapitres sur l'utilisation primaire et secondaire des données. Cette dernière ouvre la voie à un usage dans le cadre de recherches pour orienter les politiques de santé publique et améliorer le suivi patient. —



DAMIAN KLIMAS — ASSOCIÉ DOTLAW ET OBSERVATEUR DU RÉSEAU EHEALTH NETWORK

Oui plutôt

En tant que cadre sectoriel, le texte s'adosse au cadre horizontal posé par la directive NIS2 en ce qui concerne les enjeux de sécurité. L'article 50 fournit toutefois des éléments spécifiques concernant la sécurité des accès.

La vocation de ce texte est de proposer un cadre de partage des données qui aura un impact majeur sur la façon dont on utilise les données en Europe. Ses ambitions sont significatives : harmoniser la notion d'utilisation secondaire de données de santé entre différents États et implémenter une infrastructure technologique robuste pour permettre la valorisation de ces données.



RAYNA STAMBOLIYSKA — EXPERTE DIPLOMATIE NUMÉRIQUE, SPÉCIALISTE CYBERSÉCURITÉ ET MEMBRE INDÉPENDANTE DU GROUPE DE TRAVAIL SUR LES MENACES ÉMERGEANTES ET FUTURES DE L'ENISA

À ce stade, il soulève des questions liées à la maîtrise des données dans le contexte de ce partage. **Nous pouvons regretter la création d'un droit d'accès incohérent avec celui déjà défini par le RGPD**, qui pourrait aboutir à des situations d'incertitude juridique. Le sujet du contrôle par l'individu y est également traité de façon insuffisante : l'organe de gouvernance de l'EHDS ne prévoit par exemple pas de représentant de patients.

Enfin, **la question de l'implémentation d'un tel espace n'est pas très claire en l'état :** nous pouvons croire qu'il s'agit de constituer une énorme base de données unique, là où en réalité, le texte prévoit d'interconnecter différentes bases décentralisées.

Cette architecture renvoie à tout un tas de questions (gouvernance, parcours utilisateurs, formats de données, démarches de recours, etc.) dont les réponses ne peuvent et ne doivent pas être d'abord technologiques. —

À RETENIR

a Ce règlement prévoit tout de même quelques exigences techniques de sécurité sur des questions pratiques d'accès et de traçabilité (CF article 50).

Non pas tout à fait

132

CHIFFRE CLÉ

132 établissements sont engagés dans le Parcours de cybersécurité du plan France Relance

CHARLOTTE DRAPEAU — CHEFFE DU BUREAU SANTÉ ET SOCIÉTÉ, ANSSI, 2022[29]

AU NIVEAU NATIONAL

Le gouvernement français a présenté en avril 2019 une feuille de route pour « *accélérer le virage numérique en santé* »[27] dans le cadre d'un plan plus large, baptisé *Ma Santé 2022*. Cette publication a été suivie de celle d'une doctrine technique[28]. Révisée annuellement, cette dernière pose un cadre de référence et propose une trajectoire à l'ensemble des acteurs de l'e-santé en France.

Le volet numérique du Ségur de la santé s'inscrit dans ce cadre de référence et entend accélérer le processus de transformation. À travers lui, ce sont 2 milliards d'euros d'investissements que le ministère des Solidarités et de la Santé a débloqués. Les objectifs : accompagner la transition numérique des établissements de santé et médico-sociaux, moderniser les systèmes d'information existants et renforcer l'interopérabilité, la convergence et la sécurité. Ce budget inclut 350 millions d'euros spécifiquement dédiés à la cybersécurité de ces structures.

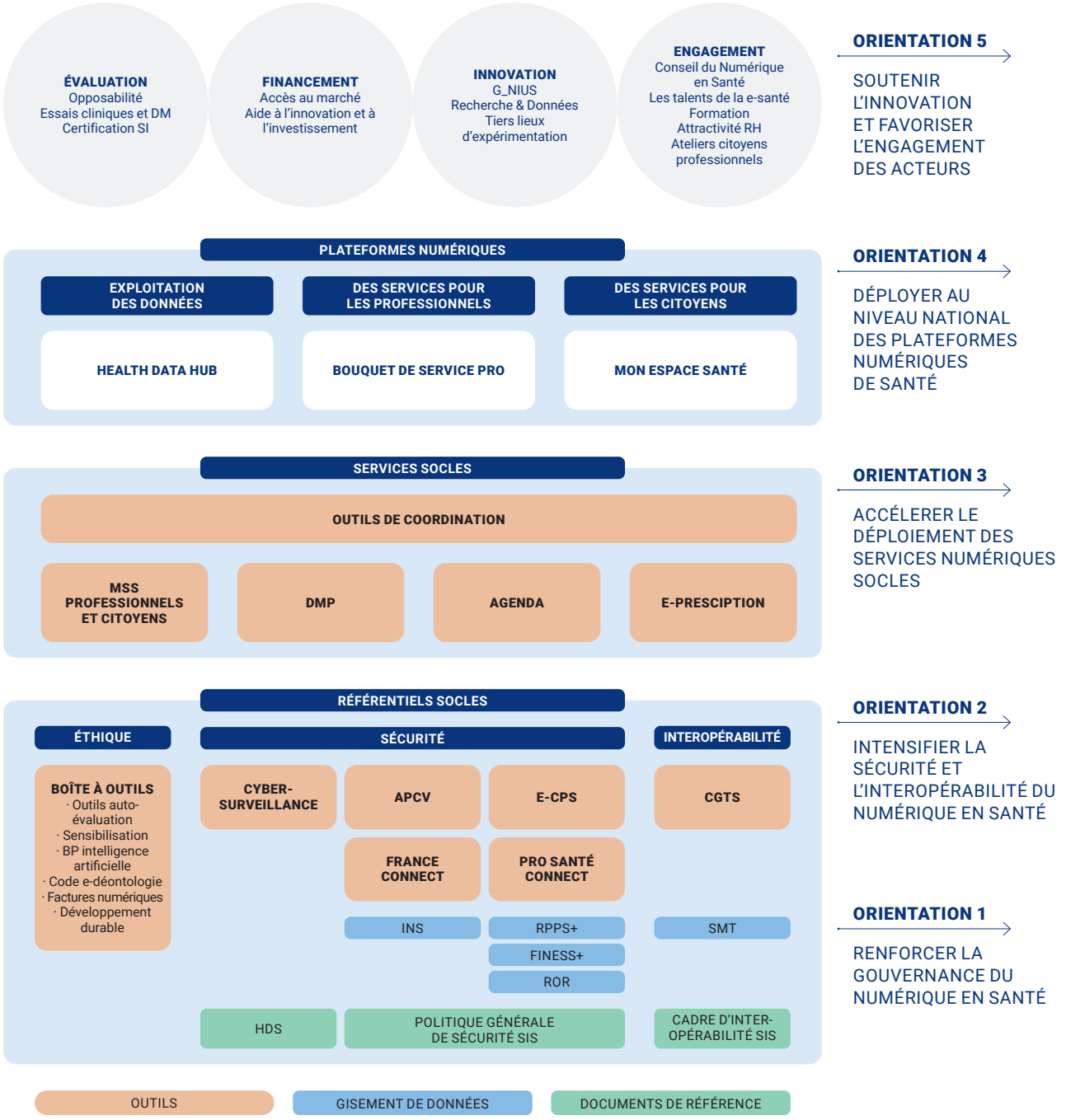
De son côté, l'ANSSI a reçu une enveloppe de 136 millions d'euros dans le cadre du plan France Relance pour renforcer la cybersécurité de l'État. Sur cette somme, 25 millions seront consacrés à la cybersécurisation des établissements de santé via la réalisation d'audits dans le cadre de parcours de cybersécurité. —

« Les cyberattaques importantes qui se sont produites depuis quelques années ont mis en lumière la dette technique et organisationnelle des systèmes d'information des établissements de santé. Une prise de conscience a eu lieu, y compris au plus haut niveau de l'État. »

JACKY GRISEY — SECURITY OPERATIONS MANAGER DÉDIÉ SANTÉ, ADVENS

LES COMPOSANTS DU CADRE DE RÉFÉRENCE MIS À DISPOSITION PAR L'ÉTAT FRANÇAIS

Ce schéma synthétise les composants du cadre de référence de la e-santé en France, à lire du bas vers le haut : d'abord les référentiels socles, puis les services socles et enfin les plateformes numériques.



Source : Doctrine du numérique en santé, Ministère des Solidarités et de la Santé (2021)



04.

Et demain?

À quoi ressemblera le monde de la santé ces prochaines années ? Quel(s) impact(s) sur sa sécurité informatique ? Un exercice de prospective qui souligne l'ampleur de la tâche.

4.1 Un continuum de soin à l'échelle européenne

Le partage des données de santé entre professionnels de santé, chercheurs et industriels doit permettre aux citoyens de bénéficier de meilleurs soins. Telle est la promesse du European Health Data Space (EHDS), que la Commission européenne a présenté comme le futur espace européen des données de santé. À condition qu'interropérabilité rime avec sécurité.





Si le règlement sur l'EHDS est adopté sans grand changement, le programme MaSanté@UE (MyHealth@EU) deviendra obligatoire au sein de l'Union européenne et permettra à chaque résident de bénéficier d'une continuité de soin dans chaque état membre. Le service a déjà été déployé en France à travers le portail Sesali.fr depuis juillet 2021[30].

L'interopérabilité et la sécurité des données devraient donc continuer d'être au cœur des politiques européennes de santé ces prochaines années. —

« L'adoption de l'EHDS va accélérer le déploiement de MaSanté@EU. Cela signifie que d'ici 2025, les établissements de santé de tous les États membres et de la Norvège auront accès facilement et de manière sécurisée aux allergies, prescriptions et antécédents médicaux de n'importe quel patient, dans leur langue, même si celui-ci réside dans un autre état européen. »

DAMIAN KLIMAS — ASSOCIÉ DOTLAW ET OBSERVATEUR DU RÉSEAU EHEALTH NETWORK

4.2 Médecine préventive, pilotage de l'hôpital par la donnée : les promesses (et les défis) du Big Data médical

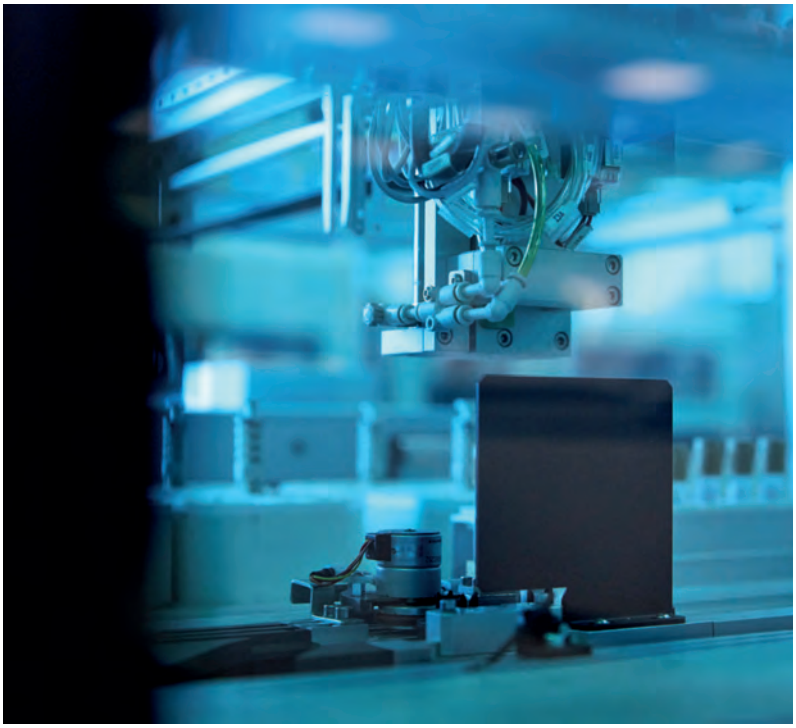
Si la collecte des données médicales s'apparente à une tâche relativement facile, leur traitement et analyse sont des actions plus complexes. Derrière la notion de Big Data médical, les promesses d'une médecine personnalisée et prédictive sont pour autant soumises à des exigences de cybersécurité.



Ces dimensions seront d'autant plus stratégiques que les perspectives liées à l'exploitation d'importantes quantités de données sont prometteuses. De nombreuses entreprises s'appuient sur le machine learning pour mettre à disposition des soignants des outils de diagnostic. Parmi elles, la start-up lituanienne Ligence[31] fournit un logiciel d'analyse d'échocardiogramme à destination des cardiologues. Autant de solutions qui doivent intégrer la question de la cybersécurité dès leur conception.

« Si nous voulons détecter les pathologies à l'avenir plutôt que les soigner, nous devons absolument nous saisir des questions de gouvernance de la donnée de santé et donc des mesures de sécurité associées. C'est pourquoi la mission du RSSI en établissement de santé est de créer les conditions de cette confiance dans les SI hospitaliers chez les professionnels comme chez les patients. »

JEAN-SYLVAIN CHAVANNE — RSSI CHU BREST



Sur les questions du pilotage des structures de santé par la donnée, certains acteurs comme le Fonds FHF[32] estiment que le PMSI (Programme de Médicalisation des Systèmes d'Information), en tant que première base de données médicalisée nationale, fournit des informations suffisamment structurées pour alimenter un algorithme de process mining. Une opération permettrait en définitive de comparer les données terrain, issues du PMSI, à un parcours patient idéal et d'optimiser la prise en charge petit à petit. —

« La marge de progression est encore très importante avant le pilotage par la donnée, beaucoup d'établissements de santé en sont encore à l'état des lieux et à la construction d'une feuille de route. »

CHARLES BLANC-ROLIN — CHEF DE PROJET SÉCURITÉ NUMÉRIQUE E-SANTÉ PAYS DE LA LOIRE

POUR ALLER PLUS LOIN

DATA MANAGER

a Avoir des données, c'est bien ; les partager, c'est mieux. Si le data sharing permet aux chercheurs du monde entier de mettre leurs ressources en commun, il doit cependant respecter une réglementation extrêmement stricte, visant à la protection et à la sécurisation des données relatives aux patients. De quoi créer un métier à part entière de Data manager en santé.

4.3 Une collaboration à construire

Avec l'intégration du biomédical et des systèmes opérationnels de gestion technique des bâtiments, la couverture SSI des établissements s'annonce toujours plus large et il devient impératif de réunir tous les acteurs autour de la table : IT, SSI et biomédical.



Car développer cette coopération implique de réconcilier les priorités et le rythme des uns et des autres : la DSI qui veut avancer vite, les équipes informatiques qui se sentent plus ou moins concernées par l'aspect sécurité (alors qu'elles ont des privilèges plus élevés) ou encore le biomédical qui ne veut faire prendre aucun risque aux patients.

La collaboration est également amenée à se développer au niveau bureautique avec des technologies cloud de plus en plus présentes. Cette évolution des usages doit être accompagnée, car elle présente un véritable enjeu de prise en main.

Le monde de la santé va devoir relever de nouveaux défis liés à la gouvernance, à la coopération et à la technique pour garantir la sécurité des patients dans un environnement toujours plus numérique.

« Plus on s'engage dans la voie de la technologie, plus on doit prendre en compte la SSI. Si historiquement les relations ont souvent été compliquées avec les équipes métiers, les RSSI en santé doivent s'accrocher pour faire comprendre aux autres fonctions que notre défi commun, c'est la confiance. »

JACQUES LABIDURIE — RSSI CHU LIMOGES

« Comprendre les implications techniques et technologiques devient une obligation, notamment quand nous observons outre-Atlantique l'impossibilité de maîtriser le devenir des données de santé des femmes dans un contexte de pénalisation de l'avortement. […] Plus que jamais, il nous revient à toutes et à tous de contribuer à la construction d'un système intelligent et résilient qui respecte les droits et libertés fondamentaux. »

RAYNA STAMBOLIYSKA — EXPERTE DIPLOMATIE NUMÉRIQUE, SPÉCIALISTE CYBERSÉCURITÉ ET MEMBRE INDÉPENDANTE DU GROUPE DE TRAVAIL SUR LES MENACES ÉMERGEANTES ET FUTURES DE L'ENISA

Des défis qui ne devront pas éclipser la mission de service public et d'accueil traditionnellement portée par le secteur : il faudra réussir à « *remettre de l'humain dans la machine* » comme le demandait la Défenseure des droits Claire Hédon[33] au micro de France Inter en juillet 2022. —

« Seul l'avenir nous dira si le secteur de la santé réussira à circonscrire le risque cyber. Mais il y a fort à parier que la numérisation à grande vitesse et la montée en compétences des groupes de ransomwares ne faciliteront pas le rattrapage de sa dette technique ».

JACKY GRISEY — SECURITY OPERATIONS MANAGER DÉDIÉ SANTÉ ADVENS

L'AVENIR DE LA CYBERSÉCURITÉ EN SANTÉ

INTERVIEW

JACKY GRISEY — SECURITY OPERATIONS MANAGER DÉDIÉ SANTÉ ADVENS

« La mutualisation dans le cadre d'un SOC managé concourt à une forme d'intelligence collective, bénéfique et caractéristique du secteur de la santé. »



Des attentes du secteur en matière de cybersécurité opérationnelle concernent l'automatisation. Nous utilisons déjà l'automatisation dans le cadre du travail de nos analyses sécurité, ce qui nous permet d'optimiser les temps de détection. Il y a un fort enjeu concernant la remédiation, le but étant de réduire autant que possible le temps de réponse. Du point de vue de l'établissement, la première étape de l'automatisation est la délégation de la réponse au partenaire dans un cadre opérationnel précis. Ensuite nous pouvons envisager l'exécution automatique de réponses « simples » : blocage d'adresses IP, blacklistages de noms de domaine de messagerie, de comptes utilisateurs, etc. ce qui peut aussi nécessiter une évolution des mentalités des équipes IT.

Une autre évolution à venir concerne le domaine biomédical, en particulier la gestion de vulnérabilités et la détection d'incidents par le SOC. Nous avons quelques clients qui ont démarré le déploiement de sondes dédiées, cela permet d'étendre la surface de détection. Les acteurs des systèmes d'information s'accordent sur un point : le domaine est une zone d'ombre !

En définitive, seul l'avenir nous dira si le secteur de la santé réussira à circonscrire le risque cyber. Pour le moment il faut jongler entre la dette technique, la numérisation des métiers qui s'opère toujours à grande vitesse et l'industrialisation des groupes de cyberattaquants. Mais la mutualisation dans le cadre d'un SOC managé, c'est-à-dire le fait que les uns profitent de ce qui est fait pour les autres (des vulnérabilités détectées, des indices de compromission, des règles de détection ou même des spécificités d'intégration) concourt à une forme d'intelligence collective, bénéfique pour tous. —

SOURCES ET ANNEXES

[1]CERT Santé
[2]https://www.techtarget.com/searchsecurity/news/252521771/Healthcare-breaches-on-the-rise
[3]https://health-trends.co.uk/wi-ga-la-hospitals-confirm-recent-healthcare-cyberattacks/
[4]https://health-trends.co.uk/wi-ga-la-hospitals-confirm-recent-healthcare-cyberattacks/
[5]https://www.cbc.ca/news/canada/newfoundland-labrador/nl-cyberattack-update-march-29-22-1.6401700
[6]lefigaro.fr/secteur/high-tech/covid-19-des-cyberattaques-contre-la-chaine-logistique-des-vaccins-20201203
[7]https://www.ssi.gouv.fr/entreprise/reglementation/confiance-numerique/le-referentiel-general-de-securite-rgs/
[8]https://www.usine-digitale.fr/article/le-gouvernement-injecte-20-millions-d-euros-dans-l-anssi-pour-renforcer-son-accompagnement-des-hopitaux.N2036952
[9]https://www.ssi.gouv.fr/actualite/lanssi-et-le-bsi-alertent-sur-le-niveau-de-la-menace-cyber-en-france-et-en-allemagne-dans-le-contexte-de-la-crise-sanitaire/
[10]https://www.psychiaclic.fr/
[11]https://www.dsih.fr/article/4790/effacer-une-donnee-medicale-d-un-patient-vraiment.html
[12]https://www.france24.com/fr/%C3%A9co-tech/20220705-fuite-de-donn%C3%A9es-il-affirme-mettre-en-vente-la-vie-priv%C3%A9e-des-deux-tiers-des-chinois
[13]https://themarkup.org/pixel-hunt/2022/06/16/facebook-is-receiving-sensitive-medical-information-from-hospital-websites
[14]https://www.ibm.com/security/data-breach
[15]https://www.stormshield.com/fr/webinar-sante-face-aux-cybermenaces/
https://www.dsih.fr/article/4790/effacer-une-donnee-medicale-d-un-patient-vraiment.html
[16]https://www.leparisien.fr/faits-divers/coronavirus-le-milieu-medical-nouvelle-cible-des-arnaques-au-president-01-04-2020-8292336.php
https://www.lemondeinformatique.fr/actualites/
[17]lire-dedalus-biologie-ecope-d-une-amende-d-1-5-meteuro-par-la-cnil-86527.html
[18]https://www.lemonde.fr/pixels/article/2020/10/27/la-finlande-secouee-par-le-piratage-de-milliers-de-dossiers-de-patients-en-psychotherapie_6057561_4408996.html
[19]https://esante.gouv.fr/sites/default/files/media_entity/documents/mss_ans_rapport_public_observatoire_signalements_issis_2021_vf.pdf
[20]https://www.cyberveille-sante.gouv.fr/sites/default/files/documents/documents-secteur-sante/ACSS_Sensibilisation_s%C3%A9curit%C3%A9_mot_passe.pdf
[21]https://www.esante-centre.fr/portail_pro/services-d-accompagnement/ssi-securite-des-systemes-d-information-131-111.html
[22]https://www.lemagit.fr/etude/Cybersecurite-du-systeme-de-sante-beaucoup-reste-a-faire
[23]https:/esante.gouv.fr/sites/default/ les/media_entity/documents/webinaires_ie-usagers_2022-05-09_v2.pdf
[24]https://health.ec.europa.eu/publications/proposal-regulation-european-health-data-space_en
[25]https://esante.gouv.fr/actualites/lespace-europeen-des-donnees-de-sante-cest-parti
[26]https://solidarites-sante.gouv.fr/IMG/pdf/190425_dossier_presse_masante2022_ok.pdf
[27]https://esante.gouv.fr/sites/default/ les/media_entity/documents/Doctrine_du_numerique_en santé_Version%202021_Février%2022_VF.pdf
[28]https://sante-achat.info/performance/charlotte-drapeau-anssi-le-secteur-de-la-sante-est-une-cible-particulierement-vulnerable/
[29]https://sesali.fr/ncpehfr-gui/index.html
[30]https://www.ligence.io
[31]https://www.fondsfhf.org
[32]https://www.francetvinfo.fr/societe/services-publics-il-n-est-pas-possible-d-imposer-a-tout-le-monde-d-avoir-un-smartphone-alerte-la-defenseure-des-droits_5238622.html

LE CHOIX EUROPÉEN DE LA CYBERSÉCURITÉ

WWW.STORMSHIELD.COM

Toute diffusion, reproduction ou représentation, même partielle de ce livre blanc, à d'autres fins qu'une utilisation privative sur un quelconque support, est interdite et pourrait engager la responsabilité civile et pénale de la personne qui ne respecterait pas cette interdiction.
Copyright © 2022 Stormshield

STORMSHIELD