CYBERCAMP Santé

CYBERCAMP #2 SYNTHÈSE

MARDI 8 FÉVRIER 2022
MUSÉE DES CONFLUENCES, LYON

FRANCE22
PRÉSIDENCE FRANÇAISE DU CONSEIL DE L'UNION EUROPÉENNE

UN ÉVÉNEMENT ORGANISÉ DANS LE CADRE DE LA PRÉSIDENCE FRANÇAISE DU CONSEIL DE L'UNION EUROPÉENNE

AGENCE DU NUMÉRIQUE EN SANTÉ

doshas consulting

Cet événement n'est pas organisé par le Gouvernement français. Il est cependant autorisé par celui-ci à utiliser l'emblème de la présidence française du Conseil de l'Union européenne.

SOMMAIRE

INTRODUCTION

PAR MARC LOUTREL, DIRECTEUR EXPERTISE, INNOVATION ET INTERNATIONAL À L'AGENCE DU NUMÉRIQUE EN SANTÉ (ANS)

Une ouverture massive des systèmes d'information de santé, des menaces cyber qui s'intensifient et un patient décédé en Allemagne des suites d'une cyberattaque hospitalière.

La période de pandémie que nous traversons depuis 2019 a fait apparaitre la nécessité de mettre en place une continuité des soins entre l'hôpital et la ville, et avec elle, une ouverture massive des systèmes d'information hospitaliers.
Cette ouverture a entrainé l'accès aux données, notamment aux données de vaccination, nécessaires pour mettre en place les politiques de santé publiques à l'échelle régionale et nationale. Nouveauté, ces données ont aussi été communiquées massivement au grand public par Internet et des canaux plus classiques comme la télévision ou les journaux.

Cette ouverture a mis en exergue la fragilité des acteurs de santé vis-à-vis de la menace cyber. Poursuivant des objectifs financiers et politiques, les attaques dont ont été victimes de nombreux établissements (Rouen, Dax, Arles, Villefranche sur Saône, pour les plus médiatisés) n'ont cessé de se multiplier depuis deux ans. Elles ne concernent pas que la France, plusieurs pays européens ont été ciblés, l'Allemagne ayant à déplorer le premier décès d'un patient, victime d'une cyberattaque dans un hôpital de Dusseldorf, en septembre 2020.

LE CERT-SANTÉ EN 3 CHIFFRES (2021)

730 incidents déclarés (doublé en un an)

190 demandes d'accompagnement (doublé en un an)

2 000 alertes de sécurité envoyées aux différentes structures (+150% en un an)

Pour faire face à cette menace et mieux préparer les acteurs de santé en France, un **plan de renforcement** de la cybersécurité des hôpitaux a été lancé en juin 2019, accompagné en février 2021, du plan de renforcement de la sécurité informatique en santé, d'un milliard d'euros.

Ces plans comprennent, entre autres :
• la création de l'Observatoire permanent de la sécurité des systèmes d'information des établissements de santé (Opssies) qui analyse le niveau de maturité des structures de santé, en s'appuyant sur le référentiel d'évaluation de la maturité numérique des systèmes d'information des structures de santé (MaturiN-H)
• la cellule d'Accompagnement Cybersécurité des Structures de Santé (ACSS), rebaptisée en Computer Emergency Response Team Santé (CERT Santé). Le CERT Santé accompagne l'ensemble des établissements de santé et structures médico-sociales dans le cadre de la réponse aux incidents. Il mène une veille sur la menace envers la cybersécurité tout en sensibilisant la communauté. Il réalise également des audits de l'exposition sur Internet des systèmes d'information des structures de santé, afin de les aider à réduire le risque d'attaque cyber. Enfin, le CERT Santé organise des actions de prévention ciblées sur des menaces spécifiques et propose des services visant à améliorer la sécurité du SI.

Le renforcement de la stratégie du gouvernement en matière de sécurité des réseaux informatiques des établissements de santé passe également par :
• un investissement massif de plus de 350 millions d'euros afin de sécuriser les établissements de santé par la réalisation d'audits leur permettant de les accompagner dans leur démarche de cybersécurisation,
• un renforcement de la formation et de la sensibilisation des acteurs en santé,
• la création d'exercices cyber,
• le recours à un plan de continuité d'activités en cas d'attaques cyber.
Enfin, des exigences renforcées de sécurité informatique sont mises en place pour l'ensemble des établissements supports des 135 groupements hospitaliers territoriaux qui seront intégrés à la liste des « opérateurs de service essentiels » (OSE), dont l'interruption aurait un impact significatif sur le fonctionnement de l'économie ou de la société.

KEYNOTES INTRODUCTIVES

LA CYBERATTAQUE DU CH DE VILLEFRANCHE SUR SAÔNE
PAR NASSER AMANI, DSI DU GHT RHÔNE NORD BEAUJOLAIS DOMBES

« Une situation de chaos »

Il est 4h30, dans la nuit du 14 au 15 février 2021, lorsque l'équipe d'astreinte informatique du centre hospitalier de Villefranche sur Saône reçoit un appel des urgences indiquant que les données de santé des patients sont inaccessibles. Une cyberattaque est immédiatement décelée et entraîne le confinement immédiat du CH, mesure prévue dans les procédures d'urgence en cas de cyberattaque.

« En l'espace de quelques minutes, l'établissement a été plongé dans le noir, les 2800 postes de travail de l'établissement ont été chiffrés »

Du fait de l'arrêt immédiat de l'ensemble de son système informatique, l'établissement se retrouve dans le « noir complet ». Les SI étant indisponibles, toutes les données patients (antécédents, allergies, soins en cours…) sont inaccessibles, et plus grave encore, les lignes téléphoniques au sein de l'établissement sont hors service.

En pleine crise Covid-19, dans un établissement avec un service d'urgences, un service de réanimation et de néonatologie, « c'est le drame, le chaos ».

« Une remédiation qui aura pris plus de 7 semaines, 7 semaines durant lesquelles l'établissement a fonctionné en mode dégradé »

Après avoir réalisé les déclarations réglementaires à l'ANSSI, la CNIL et l'ANS, le CH est passé dans une phase de remédiation, durant 7 semaines !

Le choix fait par l'établissement, avec l'aide de l'ANSSI, a été de repenser entièrement le SI, et non de le reconstruire sur les ruines de cette cyberattaque. Une bulle de confiance a ainsi été recréée, sur laquelle se sont greffés, progressivement, l'ensemble des API nécessaires au fonctionnement de l'hôpital. Tous les serveurs ont également été recréés et le SI a été partitionné en silos, de manière à augmenter sa protection en cas de nouvelle menace.

« Ca n'arrive pas qu'aux autres »

Bien qu'aucune extraction de données ni aucune atteinte au système de sauvegarde du CH n'aient eu lieu, cette attaque aurait pu avoir de lourdes conséquences, non seulement en termes de risque de vol de données de santé des patients, mais aussi, et surtout, du point de vue des usagers, dont la vie a été mise en danger.

Par ailleurs, cette attaque est survenue dans un établissement ayant massivement investi, durant des années, dans la sécurité de ses SI. Preuve, que malgré la conscience de la menace et de la mise en place de protection, personne n'est à l'abri d'une cyber attaque et que « cela n'arrive pas qu'aux autres ».

Par la force des choses, l'ensemble du personnel de l'hôpital est aujourd'hui sensibilisé au risque informatique. D'où la nécessité de rappeler l'importance de la formation de l'ensemble des équipes et non pas uniquement des équipes SI.

LE COÛT D'UNE ATTAQUE PAR RANSOMWARE
SELON RODRIGUE ALEXANDER, DIRECTEUR ADJOINT DU CH D'ARLES

« Quoi qu'il en coûte, il faut faire en sorte que le SI redémarre »

Dans la nuit du 1er au 2 août 2021, aux alentours de 3 heures du matin, la salle informatique du centre hospitalier d'Arles est appelée pour un SGL qui ne fonctionne pas. Le technicien informatique constate alors que les fichiers sont chiffrés et que leur dénomination change très rapidement. Aucun doute possible, le CH est victime d'une cyberattaque par ransomware. L'ensemble du parc informatique est touché et, contrairement au CH de Villefranche sur Saône, les fichiers de sauvegarde ont été atteints !

L'ensemble du personnel de l'hôpital doit continuer son activité malgré le risque quant à la qualité et la sécurité des soins (accès à l'imagerie compliquée, interprétation plus longue des résultats, CR de biologie disponibles dans des délais plus longs, pas d'accès aux données patients donc aux antécédents…). « Quoi qu'il en coûte, il faut faire en sorte que le SI redémarre », c'est l'ordre reçu par Rodrigue Alexander. Immédiatement après l'attaque, 360 000€ vont être nécessaires pour répondre à cette injonction.

« Des coûts, à chaud »

Si la remise en fonctionnement du système informatique a coûté 60 000€ (switch et serveurs), la facture aurait pu être beaucoup plus conséquente sans la possibilité pour le CH de réutiliser son matériel. L'établissement a dû également investir 300 000€ en prestations diverses, des heures supplémentaires de l'équipe IT aux prestataires extérieurs pour l'installation de nouveaux serveurs. S'ajoutent à ces 360 000€ initiaux, 300 000€ investis (dont 275 000€ pris en charge par l'ARS) dans le projet de sécurisation du parc informatique du CH d'Arles.

« Des délais de paiement rallongés »

Les coûts d'une cyberattaque ne s'arrêtent malheureusement pas là… Il faut également évoquer la tension sur la trésorerie qui, plus de 6 mois plus tard, se fait encore sentir. En effet, la facturation a été complètement suspendue, entrainant ainsi un allongement des délais de paiement, voire leur suspension. De plus, il a fallu recruter du personnel administratif afin de ressaisir informatiquement, un à un, l'ensemble des actes (plus de 40 000 actes) réalisés durant le temps d'indisponibilité du SI du centre hospitalier. A ces salaires s'ajoutent les heures supplémentaires ainsi que les éventuelles pertes de revenus suite à la mauvaise saisi d'acte ou à la perte de facturation papier.

« Des coûts indirects insoupçonnés »

Il y a également des coûts indirects, qu'on ne perçoit pas immédiatement lors de l'attaque, mais qui sont pourtant bien réels comme des indemnisations liées à la qualité des soins. Le temps de l'indisponibilité du SI, l'ensemble des informations médicales ont été retranscrites sur papier, engendrant des risques d'oubli et d'erreur, contraignant les soignants à ne pas disposer des antécédents du patient lors d'une future prise en charge.

« Les PME qui mettent la clef sous la porte, une possibilité pour l'hôpital également »

Enfin, il existe un risque réel de perte d'activité à long terme, dû en partie à l'altération de la réputation de l'établissement, suite à un événement aussi dramatique. Au total, 30% du budget annuel a été consacré à la remédiation de cette attaque, dont la reconstruction complète n'est toujours pas terminée.

LE RISQUE CYBER EN SANTÉ ANALYSÉ
PAR DIDIER MENNECIER, MÉDECIN GEEK

Depuis deux ans, on remarque une recrudescence d'attaques dans deux grands secteurs : les établissements de santé et les collectivités territoriales.

Alors que chacun d'entre nous veille sur sa carte bleue et ne souhaite généralement pas l'enregistrer sur son ordinateur par crainte de se faire dérober des informations si précieuses, nous avons tous, à tort, beaucoup plus de facilité à enregistrer notre numéro de sécurité sociale ou nos données de santé… A tort, parce qu'aujourd'hui, il est plus intéressant, pour des hackers, de voler des données de santé qu'un numéro de carte bancaire qui pourra être bloquée très rapidement.

Ayant le vent en poupe sur le darknet, elles se revendent à des prix particulièrement élevés. A titre d'exemple, un dossier médical se monnaye 350€ sur le marché noir numérique, contre 35€ pour une carte de crédit et 150€ pour un compte gmail. Les données de santé sont devenues de véritables mines d'or pour les cybercriminels. Elles contiennent des informations à caractère personnel extrêmement sensibles telles que les dates de naissance, les adresses postales, les données biométriques, les numéros de sécurité sociale et de mutuelles qui vont permettre aux criminels d'usurper l'identité des victimes.

Or, 8 fois sur 10, la faille est humaine. Ni le pare-feu, ni l'antivirus, ni même la mise à jour des logiciels ne permettent d'y faire face. C'est pourquoi, il ne suffit plus seulement de sensibiliser les personnels dès leur arrivée dans les établissements ou les structures, il faut mettre en place de véritables actions de sensibilisation, à l'instar des serious game, qui seront suivies de formations et d'exercices en conditions réelles, comme c'est le cas, depuis des décennies, dans le domaine des incendies. Pour information, l'Association nationale pour la formation permanente du personnel hospitalier (ANFH) est en train de travailler sur un « parcours cyber » à destination des établissements de santé, qui sera gratuit et disponible courant 2022.

FAIRE APPEL À LA GENDARMERIE APRÈS UNE CYBERATTAQUE
CONSEIL DU COLONEL BARNABÉ WATIN-AUGOUARD, COMMANDEMENT CYBER DE LA GENDARMERIE NATIONALE

La gendarmerie, et plus généralement, les forces de l'ordre, jouent un rôle dans le domaine de la cybersécurité et non pas uniquement dans le domaine de la cybercriminalité.
La gendarmerie intervient, par exemple, dans la sensibilisation des dirigeants et travaille également sur l'ensemble des réflexions menées au niveau national (comment conserver l'intégrité des données, comment mettre en place des exercices annuels sur la cybersécurité…).
Les forces de sécurité intérieure peuvent également venir appuyer les équipes des établissements hospitaliers victimes d'une attaque. C'est pourquoi il est important de faire appel à ces unités dès lors que l'attaque est détectée.
En effet, disposant d'unités spécialisées, la gendarmerie peut entamer une enquête grâce à ses capacités de rétro-ingénierie. Par ailleurs, dans le cas de ransomware, bien que la règle en France consiste à ne pas payer la rançon demandée, la gendarmerie pourra apporter sa capacité de négociation qui permettra surtout de gagner du temps, pendant lequel les équipes de rétro-ingénierie pourront enquêter.
Enfin, il est nécessaire de rappeler que la plainte et l'enquête sont les seuls moyens de mettre en œuvre la justice, et d'obtenir ainsi une indemnisation.

TABLES RONDES

TABLE RONDE

LES RÈGLEMENTS EUROPÉENS (CYBERSÉCURITÉ/NUMÉRIQUE) ET LEURS IMPACTS SUR LA SANTÉ NUMÉRIQUE

ANIMATEUR

. Maître Florence Eon-Jaguin, avocate experte en droit de la santé

PARTICIPANTS

. Romain Santini, en charge des affaires juridique à l'ANSSI

. Ray Pinto, directeur de la transformation numérique pour Digital Europe

GRAND TÉMOIN

. Pekka Kahri, DSI du CHU d'Helsinki

LES FINALITÉS ET L'APPORT OPÉRATIONNEL DE LA CRÉATION DE L'ESPACE EUROPÉEN DES DONNÉES DE SANTÉ

La création d'un espace européen des données de santé est l'une des priorités de la Commission européenne. Cet espace contribuera à améliorer les échanges et l'accès à différents types de données sur la santé, dans l'objectif d'assurer la continuité des soins d'un patient voyageant au sein de l'UE, mais également de soutenir la recherche.

L'identité numérique, au cœur des transactions

Dans ce cadre, l'identité numérique est un catalyseur essentiel des transactions numériques. La crise du Covid-19 a montré l'urgence de fournir rapidement à tous les citoyens et aux entreprises européennes, une identité nationale pour permettre les échanges au sein de l'UE mais également l'accès au service public du système de santé.

Le règlement eIDAS (Electronic IDentification And Trust Services) est le règlement sur l'identification électronique et les services de confiance pour les transactions électroniques au sein des 28 états membres de la communauté européenne. Adopté le 23 juillet 2014, il instaure un cadre européen en matière d'identification électronique et de services de confiance, afin de faciliter l'émergence du marché unique du numérique.

La révision du règlement eIDAS est en cours et une proposition en date du 3 juin 2021 vient en préciser les principales pistes d'amélioration. En effet, ce règlement est amené à évoluer afin d'offrir aux citoyens européens une véritable boite à outils pour interagir avec des services publics et privés.

> ***Promouvoir la dématérialisation, promouvoir l'échange et le partage des données entre les acteurs de nature différente, promouvoir la sécurité des systèmes d'information et la vie privée de chacun.***

Depuis sa mise en application en 2014, on constate que le développement de l'identification électronique dans les différents états membres de l'union européenne est assez disparate.

Avec cette nouvelle proposition législative, la volonté de la commission européenne est que les états s'assurent de l'obligation de mettre à disposition des citoyens le portefeuille européen d'identité numérique, incluant un moyen d'identification électronique de niveau élevé et une signature électronique qualifiée. Ce portefeuille comporte enfin une nouvelle fonctionnalité qui n'existait pas dans la version précédente du règlement IDAS, à savoir la divulgation d'attributs sans envoyer la totalité des informations (localité, âge …). Le réseau de prestataires de services de confiance vérifie les attributs, l'authenticité et les émet au possesseur du portefeuille.

Et ailleurs en Europe ? Le témoignage de Pekka Kahri, DSI du CHU d'Helsinki

A Helsinki, la réglementation européenne a impliqué un investissement massif des instances gouvernementales, destiné à assurer le respect de la réglementation européenne et l'espace européen des données de santé.

Le risque cyber rend la collaboration transfrontalière difficile dans les pays nordiques dont les contrôleurs de données se montrent particulièrement hésitants à prendre de tels risques. En effet, dans ces pays, les échanges de données de santé à l'échelle internationale ne sont pas bien perçus, malgré les différentes analyses démontrant la sécurisation de ces données. C'est pourquoi cet espace est perçu comme une aubaine et, notamment, comme LA solution à la problématique de l'utilisation secondaire des données médicales.

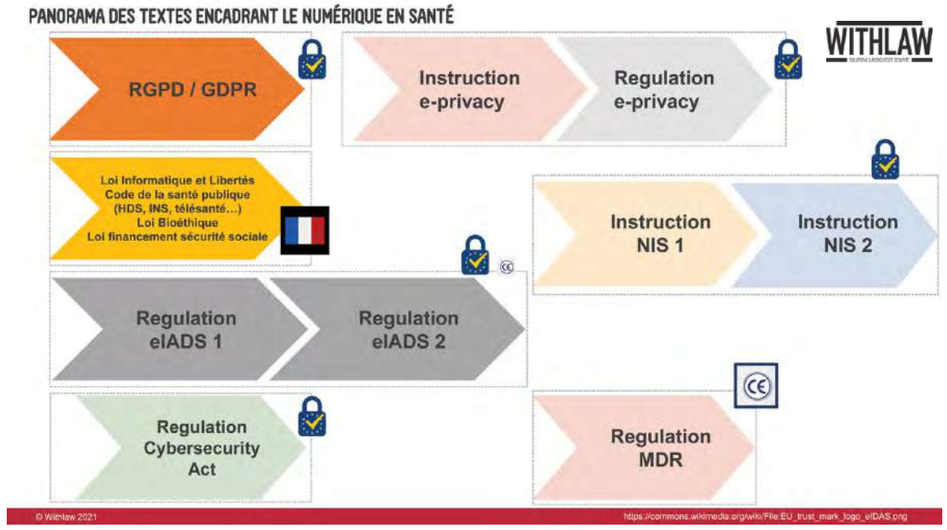


TABLE RONDE

LES LOGICIELS DISPOSITIFS MÉDICAUX : COMMENT PRENDRE EN COMPTE LES ENJEUX DE PROTECTION DES DONNÉES DE SANTÉ ?

ANIMATEUR

. Fabien Pezous, PDG de Baquento

PARTICIPANTS

. Grégory Cordier, responsable conformité technique chez RESMED
. Maria Bäcklund Hasel, Agence suédoise de la e-santé
. Jean-Pierre Barré, directeur commercial chez Wallix
. Benjamin Meany, digital health manager chez MedTech Europe

LES ENJEUX LIÉS AUX DONNÉES DE SANTÉ AUTOUR DES DISPOSITIFS MÉDICAUX

« Si on arrive à créer un environnement de confiance, alors les patients donneront leur consentement éclairé à la collecte de leurs données personnelles »

L'un des premiers enjeux liés aux données de santé des dispositifs médicaux est de pouvoir collecter les données des patients. Cette première étape à l'exploitation de ces données est la plus critique car elle nécessite d'obtenir le « consentement éclairé » des patients.

« Communication, transparence et confiance »

Selon un sondage réalisé en Suède, 90% des patients sont prêts à donner leur consentement une fois qu'il leur a été expliqué que la sécurité de leurs données sera respectée et qu'ils y auront accès.
Gagner la confiance pour collecter ces informations passe par la pédagogie. En ce sens, la catégorisation des données est un point clef dans la sécurisation de l'accès aux données et il est impératif d'expliquer au patient que toutes ses données ne seront pas accessibles à tous. Il a également besoin d'être informé sur l'utilisation qui en sera faite : utilisation primaire ou secondaire, en matière de recherche médicale, d'innovation pour les traitements et les solutions de demain.
Par ailleurs, le professionnel de santé a également un rôle à jouer dans ce processus. Il est donc primordial de le sensibiliser sur sa responsabilité dans la protection des données personnelles de ses patients.

« La cybersécurité est une responsabilité conjointe »

Le travail collaboratif est également un outil permettant de créer une relation de confiance entre l'ensemble des acteurs concernés par les données de santé. En effet, la confiance ne doit pas uniquement être établie entre l'industriel et le patient, ou entre le professionnel de santé et son patient, mais également entre les autorités de santé et le patient, ou encore entre les autorités de santé et les industriels, en gardant toujours en ligne de mire, l'intérêt du patient.

Outils, méthodes, et solutions mises en œuvre pour garantir la sécurité des données

La confiance nécessaire au consentement éclairé du patient passe également par le cadre réglementaire français et européen. Le corpus réglementaire relatif à la protection des données personnelles est vaste :
. le RGPD,
. la directive NIS 2, qui harmonise les exigences de cybersécurité entre les états membres et définit des mécanismes de coopération pour mieux gérer les risques cyber,
. le Medical Device Regulation (MDR2017/745/UE) qui remplace la précédente directive relative aux dispositifs médicaux (MDD) en Europe. Entré en vigueur le 26 mai 2021, il renforce l'accent sur la sécurité, la performance, la transparence et la qualité. Il concerne l'ensemble du cycle de vie du produit du dispositif médical : de la conception et la fabrication au suivi après commercialisation jusqu'à l'élimination.

« La sécurité n'est pas un simple composant, c'est une qualité intrinsèque au système »

Différents principes viennent également garantir la protection des données personnelles :
. le Privacy by design qui implique d'intégrer les principes du RGPD dès la conception d'un projet,
. le Security by design qui consiste, pour le constructeur de l'objet connecté, à inclure la notion de risque dans son projet dès la phase de conception. C'est un travail d'identification des vulnérabilités de l'objet lui-même,
. la Post market surveillance qui est un suivi clinique après marquage CE, qui consiste à recueillir des données cliniques en vie réelle, pour confirmer les revendications de performance et de sécurité d'un dispositif médical. Ce dispositif s'inscrit dans les obligations associées au marquage CE d'un dispositif médical et a pour objectif de s'assurer que les DM soient toujours à jour dans la sécurisation des données personnelles.

TABLE RONDE

LA CARTOGRAPHIE DES ACTEURS ET DES RESSOURCES DISPONIBLES SUR LA CYBERSÉCURITÉ EN SANTÉ

ANIMATEUR

. Olivier Morel, trésorier d'Hexatrust

PARTICIPANTS

. Charlotte Drapeau, cheffe du bureau santé et société à l'ANSSI
. Yves Beauchamp, référent numérique en santé à l'ANAP
. Emmanuel Sohier, responsable du CERT Santé à l'ANS

ACTIONS MENÉES PAR L'AGENCE DU NUMÉRIQUE EN SANTÉ (ANS) SUR LE VOLET CYBER DES SI DANS LES STRUCTURES DE SANTÉ

Accompagnement des industriels

L'ANS accompagne les acteurs de santé et les industriels en vue de la prise en compte de la sécurité dans la conception ou les évolutions des systèmes d'information, notamment à travers des référentiels et des guides de sécurité publiés sur son portail.

Dans le cadre du Ségur du Numérique en Santé, l'ANS intervient également auprès des industriels, notamment dans le cadre de leur référencement.

Un questionnaire avec une dizaine de thématiques portant sur différents aspects de la sécurité (gouvernance, audit) a été mis à disposition des industriels afin d'estimer leur niveau de sécurité et la maturité de leurs solutions. Suite à ce questionnaire, des exigences prioritaires ont été définies (identification, authentification) pour les éditeurs souhaitant être référencés Ségur et bénéficier ainsi du financement associé.

Sensibilisation des acteurs de la santé

L'ANS mène également une activité de sensibilisation à travers l'animation de webinaires consacrés à la cybersécurité.

Il est également à noter la disponibilité du portail cyberveille-sante.gouv.fr qui réunit :

. toute la documentation relative à la menace de cybersécurité en santé ainsi que des guides de bonnes pratiques,

. des bulletins d'information sur les vulnérabilités des solutions les plus utilisées par les établissements de santé,

. des alertes de sécurité relatives aux solutions déployées dans les SI auxquelles il est possible de s'abonner à travers le flux RSS,

. des audits de cybersurveillance pour évaluer le niveau d'exposition aux vulnérabilités critiques et pour vérifier l'absence de systèmes sensibles tels que les mots de passe sensibles. Un rapport est rédigé à la suite de chaque audit et communiqué aux structures concernées. Un service en ligne permettant de commander un audit est en cours de déploiement

Veille et réponse opérationnelle

Avec l'appui de l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'ANS a produit une cartographie des SI Santé exposés. Les structures de santé sont alertées sur les compromissions potentielles ou avérées de boites de messagerie, de comptes VPN, ou de données sensibles ayant fuité sur Internet. Ces structures peuvent aussi solliciter l'ANS pour les appuyer dans la réponse à apporter en cas d'incident.

En raison du manque de visibilité des directeurs/managers d'établissements de santé et services médico-sociaux d'ES et ESMS, l'Agence Nationale d'Appui à la Performance des établissements de santé et médico-sociaux (ANAP) mène actuellement une cartographie des acteurs et des ressources constituant l'écosystème de la cybersécurité en santé qui sera disponible au cours du deuxième trimestre 2022. L'objectif de cette cartographie est double :

. identifier l'ensemble des fournitures et des services proposés par les différents acteurs,

. permettre à l'établissement de santé de consolider les outils et les ressources auxquels il peut s'appuyer compte tenu de ses priorités.

CONCLUSION

CONCLUSION

PAR DIDIER AMBROISE, ASSOCIÉ FONDATEUR DE DOSHAS CONSULTING

Depuis 2013, nous développons chez *Doshas Consulting* une approche « humaine » du risque cyber, en mettant l'accent sur les comportements et la collaboration entre acteurs du système de santé. Face à une menace aussi organisée, nous sommes convaincus que la réponse ne peut être, en effet, que collective.

Belle illustration, cette deuxième édition du *CyberCamp Santé* a été une journée riche en échanges et retours d'expérience. Elle a permis de constater, une fois encore, que sans le prérequis de la sécurité des données de santé et des systèmes d'information de santé au sens large, il n'existera ni confiance ni éthique dans la santé numérique.

Au sein de notre cabinet de conseil, nous n'avons pas attendu la multiplication des cyberattaques et des actes de malveillance envers les établissements hospitaliers, pour faire de la sécurisation des données de santé à caractère personnel une préoccupation cruciale au cœur de notre expertise. Alors qu'une étude récente montre que les dispositifs médicaux deviennent également des cibles potentielles pour les hackers, la grande majorité des professionnels de santé n'a toujours pas conscience de l'étendue des dangers.

De l'Europe aux régions, la cybervigilance est toujours et plus que jamais l'affaire de chacun, l'affaire de tous. Etre sur ses gardes dans sa pratique quotidienne et veiller continuellement à ne pas se laisser dépasser par l'inventivité des pirates, à l'affût de nouvelles portes dérobées pour atteindre le cœur des établissements de santé, la sensibilisation à la cybersécurité est plus que jamais indispensable. Elle passe notamment par la solution *MediRisk*©, un serious game dédié, très bien accueilli par les différents utilisateurs du numérique en santé.

L'engouement et la satisfaction des participants à ce *CyberCamp Santé #2*, ayant pour cadre le magnifique *Musée des Confluences* de Lyon, nous confortent dans notre volonté d'organiser rapidement une prochaine édition et de lancer un tour de France, voire d'Europe, de la cybersécurité, pour rester au plus près des différents acteurs des territoires.

SOUTIENS INSTITUTIONNELS

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté Égalité Fraternité

AGENCE DU NUMÉRIQUE EN SANTÉ

l'anap agence nationale de la performance sanitaire et médico-sociale

ars Agence Régionale de Santé Auvergne-Rhône-Alpes

LE DISPOSITIF MÉDICAL snitem Pour faire avancer la santé

CLUSIF

Com CyberGend

MedTech Europe from diagnosis to cure

CESIN

GSN FRANCE

RoAM

HEXATRUST CLOUD CONFIDENCE & CYBERSECURITY

eHälsomyndigheten

C.A.I.H. Centrale d'Achat de l'Informatique Hospitalière

eum

SOUTIENS ACTEURS PRIVÉS

Phealing

ResMed

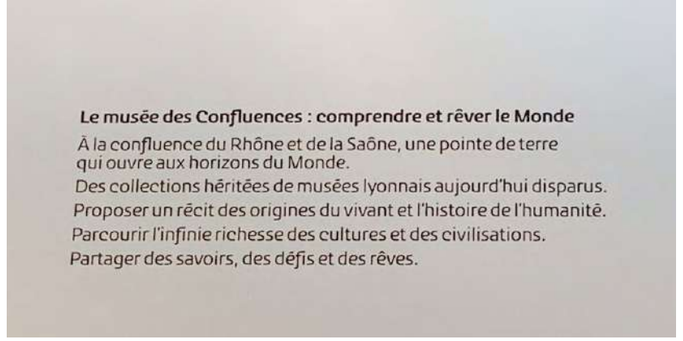
BAQUENTO Life sciences Contract Service Organisation

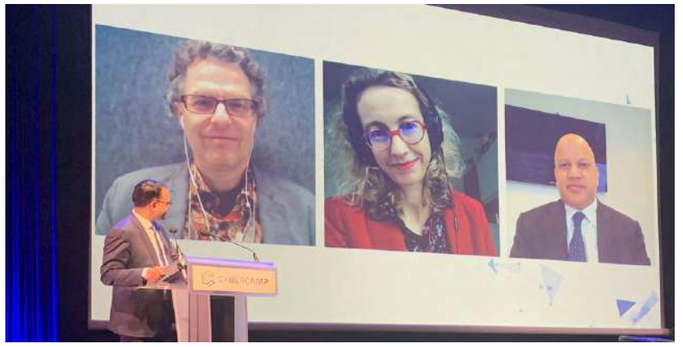
WITHLAW SOLUTIONS JURIDIQUES DE SECURITE

Pytharec

CYBER-DETECT ANALYSE MORPHOLOGIQUE

ADEQUACY





CYBERCAMP
Santé

POUR SUIVRE TOUTES NOS INFORMATIONS :

www.cybercampsante.org/

www.linkedin.com/company/cybercamp