Lettre des "Lundi de la cybersécurité" no 56

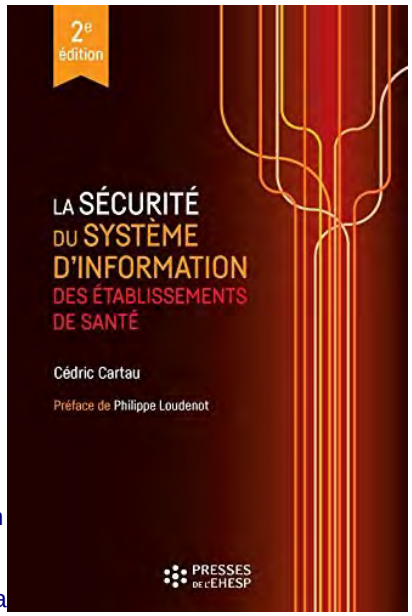
La cyber en santé et ses spécificités

La cyber en santé et ses spécificités

On sait bien que ça n'arrive qu'aux autres, c'est ce qui rassure quand il est question de cyberattaques. Mais quand ça arrive dans son propre Centre Hospitalier, en général un samedi et durant la nuit…, c'est la douche froide, c'est l'effet de sidération garanti, plus rien ne fonctionne ! Ecrans noirs. Plus de téléphones et plus d'accès aux données numériques, les dispositifs d'imagerie sont à l'arrêt ou on ne peut plus sauvegarder les résultats sur supports magnétiques !!! Alors… papier, stylos, système D ?

En plus, les données médicales des patients ont été exfiltrées, celles qui résident encore dans le système d'information du CHU sont chiffrées, une rançon est réclamée avec menace de divulguer les données sensibles exfiltrées si le paiement n'est pas fait dans les prochaines 48 heures. Les sauvegardes ? Chiffrées aussi !
Quand les blés sont sous la grêle…

On pense à déclencher une cellule de crise, mais c'est la nuit, peu importe, on réveille qui on pense pouvoir être utile. Mais avant de penser à convoquer la cellule de crise, on avertit de l'attaque l'ARS (Agence régionale de santé), la CNIL, l'ANSSI si on y a droit, ou cybermalveillance.gouv.fr si on n'est ni un Opérateur d'Importance Vitale, ni un Opérateur de Service Essentiel. Il faut porter plainte. Doit-on, de suite, en faire part à son assureur cyber ? Et à qui encore ? Restons calmes, facile à dire…



Le CHU de Rouen en novembre 2019, le CHU de Dax en février 2021, le CHU Sud Francilien de Corbeil-Essonnes en août 2022 et l'hôpital de Versailles André Mignot en décembre 2022, et bien d'autres ont subi des cyberattaques, hélas réussies. Après avoir affronté le tsunami de l'attaque, les CHU restent des mois dans la houle des procédures et des fonctionnements dégradés, avant de retrouver une mer calme. Cette catastrophe se chiffrera en millions d'euros, en recomposition du système d'Information et en perte de revenus, sans compter l'image qui en a pris un coup. Résilience, où es-tu ?

Il est révoltant, inadmissible, odieux de s'en prendre à nos structures de santé, mais les données que ces enfoirés dérobent semblent être le nouvel eldorado des pirates qui achètent des données médicales sur les marchés noirs de la cybersécurité où la demande est grande, et il faut bien que d'autres enfoirés s'approvisionnent et y trouvent leur compte. Quand ce n'est pas devenu aussi le terrain de jeu d'organismes gouvernementaux qui veulent jeter le désarroi, la panique sur toute la population d'un pays au cours d'une « opération spéciale ».

Comment réagir ? Commentaire repartir ? Actionner le Plan de Reprise d'Activité (PRA) ? Sans doute, … s'il existe. En tout cas, à Partir d'aujourd'hui, ce sera le **« *Zero Trust*** ». Confiance Zéro, que ne t'avions-nous pas acceptée plus tôt ! ☹

Je donne la plume à Cédric Cartau

Ces dernières années, les SI de santé ont régulièrement fait l'actualité : attaques en série par rançongiciels, pannes à répétition, mais aussi financement dédiés, prise en compte des pouvoirs publics de leurs spécificités, intégration dans la directive NIS, etc.

Quelles sont les spécificités des SI de santé ? Peut-on les comparer, en totalité ou en partie, à des SI "classiques" d'entreprise de même taille ? Pourquoi les DSI hospitalières

semblent avoir autant de mal à protéger leurs actifs ? Pourquoi un tel fractionnement dans les équipes, l'offre logicielle, les métiers utilisant l'outil informatique ?

Nous tenterons d'apporter pour partie la réponse à ces questionnements légitimes, sachant que pas mal de ces questions restent au stade du débat.

Je reprends la plume

Quand je reçois, dans ma messagerie, la lettre de DSIH Magazine, je cherche, pour commencer, si Cédric Cartau y a écrit un article, j'aime son humour, son franc parler et bien sûr sa compétence et son vécu dans le milieu hospitalier.

Qui est Cédric Cartau ?

Cédric Cartau est le responsable de la sécurité des systèmes d'information et le délégué à la protection des données du CHU de Nantes et du GHT44. Cédric Cartau assure également des formations aux systèmes d'Information à l'EHESP (Ecole des hautes études en santé publique). Il est chroniqueur dans DSIH Magazine (où ses écrits sont un bonbon pour l'esprit). Lisez sa "lettre au Père Noël" : https://www.dsih.fr/article/4953/ma-lettre-au-pere-noel-2022.html .

Lisez aussi sa toute récente intervention sur DSIH :
https://www.dsih.fr/article/4982/chatgpt-a-l-epreuve-d-un-test-rigoureux.html

Il est l'auteur de 6 ouvrages sur les systèmes d'Information, aux éditions Presses de l'EHESP.

Cédric est vice-président de l'**APSSIS** (Association Pour la Sécurité des Systèmes d'Information de Santé) dont le 11e Congrès National de la SSI Santé se tiendra au Mans du 13 au 15 juin 2023. Le site de l'APSSIS **https://www.apssis.com/** est riche en enseignements sur la sécurité dans le domaine de la santé. Le président de l'APSSIS, Vincent Trély est intervenu dans le quart d'heure des associations au Lundi de la cybersécurité du mois de novembre 2021. Voir l'enregistrement en :
https://www.arcsi.fr/media/Lundi-Cyber-nov2021-APSSIS.mp4

Demande d'inscription pour le Lundi de la cybersécurité de février

Lundi 6 février à partir de 18 h 00, en ligne par visio-conférence Zoom.

Nos « Lundi de la cybersécurité » **sont gratuits** et veulent vous offrir une fête technologique. **Demandez votre inscription, par courriel,** nous vous enverrons un hyperlien personnel vers la visioconférence un peu avant le jour de l'événement.

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Dans votre message d'inscription, nous apprécierions que vous écriviez quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité. Evitez le style télégraphique, nous sommes toujours heureux de vous lire et de connaître votre intérêt pour nos événements.

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants.

Un quart d'heure avec Paul-Olivier Gibert, président de l'AFCDP

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses, autour de 19h15, nous donnons pour quinze minutes la parole à une organisation, qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

L'Association française des correspondants à la protection des données à caractère personnel (**AFCDP**) est une association loi de 1901, créée en 2004, dans le contexte de la modification de la Loi informatique et libertés qui a officialisé une nouvelle fonction, celle de « Correspondant à la protection des données à caractère personnel ». L'association se focalise sur le métier, devenu celui de Délégué à la protection des données, ou **DPO** (pour *Data Protection Officer* ou *Data Privacy Officer*), dans le cadre du Règlement général sur la protection des données (RGPD).

Retour sur les "Lundi de la cybersécurité" précédents.

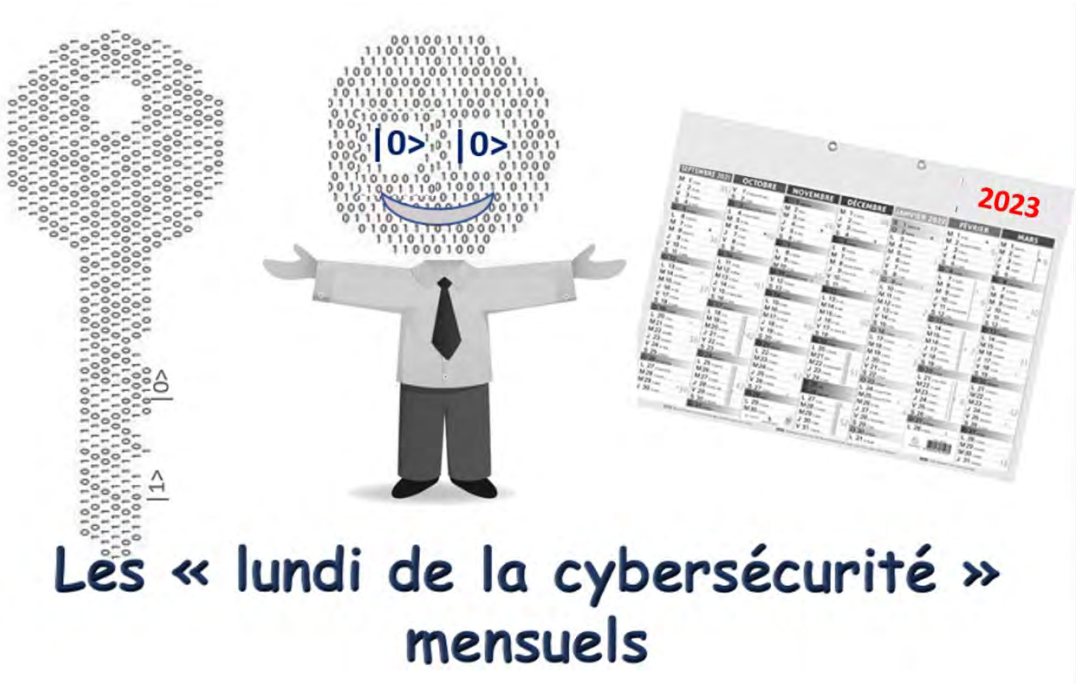
Vous trouverez tous les détails, slides, enregistrements sur le web de l'ARCSI, en https://www.arcsi.fr/ pour les plus récents et en https://www.arcsi.fr/evt_passes.php

pour les événements plus anciens. Les quarts d'heures accordés aux initiatives se trouvent en première page du site de l'ARCSI, là où sont les logos des organisations qui se sont déjà manifestées dans nos « Lundi de la cybersécurité » précédents.

Nous remercions Francis Bruckmann, webmestre et membre du Conseil d'Administration de l'ARCSI pour son travail qui constitue la mémoire de nos événements.

EXCELLENTE ANNEE 2023, avec nos « Lundi de la cybersécurité » mensuels !

Gérard



Lundi de la cybersécurité de mars

lundi 13 mars 18h-20h

Avec Lionel Mourer
Directeur Général, Consultant principal de Manika

Au secours, je suis victime d'un hacker !!!