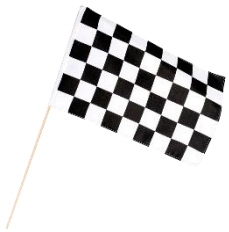
11ème Congrès National de la Sécurité des SI de santé

Par Gérard Peliks

Ceci n'est pas un compte-rendu exhaustif, ni à plus forte raison une retranscription de ce qui a été dit au CNSSIS.

C'est mon ressenti personnel des trois jours que j'ai passés dans ce grand évènement.

Deux grands évènements se sont succédés dans la cité Mancelle.



En cette première quinzaine de juin 2023, deux grands évènements se sont succédés dans la ville d'art et d'histoire du Mans. Le premier, durant le weekend du 10 et 11 juin, c'étaient **les 24 heures du Mans** qui fêtaient, cette année, leur centième anniversaire. C'est dire que la ville toute entière s'était parée d'habits de fête. A peine les vrombissements des moteurs des bolides qui tournaient sur l'asphalte, et qui ont vu la victoire de Ferrari, se sont tus et les vapeurs d'essence se sont dissipées que prenait place, dans la foulée, le deuxième évènement qui faisait à nouveau, de cette ville de la Sarthe, un pôle d'attraction national, territoires ultra marins compris.

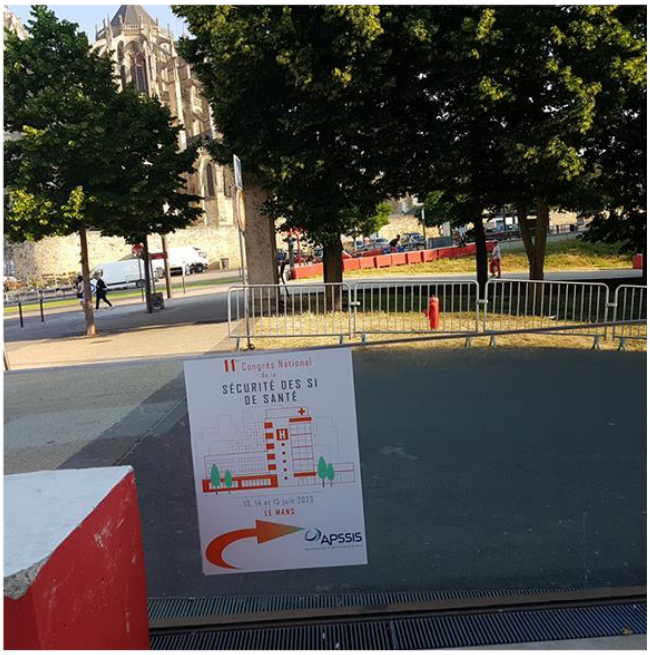
C'étaient **les 24 heures de conférences réparties sur trois jours**, du 13 au 15 juin : le **11ème Congrès National de la Sécurité des SI de Santé**, le CNSSIS, organisé par l'**APSSIS** (www.apssis.com). Vincent Trély son président, l'équipe organisatrice, les intervenants et les participants, ont fait du Mans, comme chaque année, un pôle de la sécurité du numérique, dans le domaine des groupements hospitaliers et plus généralement de la santé. Des journées de conférences, des tables rondes, des stands de présentations de solutions, des repas pris en commun, le tout dans une ambiance très conviviale, comme l'APSSIS sait en organiser, se sont succédés durant ces trois jours.

Le Congrès a été suivi par **plus de 200 professionnels**, RSSI de toutes les Régions, des représentants du ministère de la santé, des groupements hospitaliers de territoire (GHT), des offreurs de solutions, constructeurs et éditeurs de logiciels… Tout un monde autour des solutions de cybersécurité pour diminuer les risques dans le domaine hospitalier aujourd'hui si menacé par les ransomwares, le phishing, les cryptovirus, les saturations de bandes passantes et autres atteintes à la disponibilité, à l'intégrité et à la confidentialité des données médicales. Et on peut ajouter à leur traçabilité.

En route vers le centre des congrès des Quinconces

Venant de Paris par le TGV, le matin, le Congrès commençant vers 13h, je sors de la gare du Mans avec ma valise à roulettes. J'ai le choix entre prendre le tramway ou me rendre à pied **au centre des congrès des Quinconces**, situé à une trentaine de minutes de marche. J'aime bien fouler le pavé d'une ville accueillante, surtout une ville d'art et d'histoire, observer les habitants, les façades, les boutiques, aussi je choisis la marche. Je suis un habitué des CNSSIS, je connais le chemin, et d'ailleurs il n'y avait qu'à suivre les rails du tramway. Et voici qu'apparaissent au bout du chemin la place des Jacobins et l'espace culturel des Quinconces où se fera le CNSSIS. Devant moi l'imposante cathédrale Saint-Julien, avec son architecture Gothique et Romane. Voici l'entrée du centre des congrès, c'est là que l'évènement va se dérouler, c'est fléché et nous sommes attendus.

L'accueil



Ces dames de l'APSSIS, citons parmi elles Marie-Valentine Bellanger, Anne Robles et Hélène Daspe, (sans oublier Laetitia Alvez et Tristan Bellanger) ont, au long des trois jours, apporté leur disponibilité, leurs sourires et une aide aux congressistes pour que cet évènement se déroule sans problèmes et avec efficacité. Ce qu'on ne voit pas sur la photo, car ils sont derrière ces dames, ce sont sur la table, les goodies offerts par l'APSSIS. Des goodies, il y en avait aussi d'autres sur les stands des organisations partenaires de cet évènement.

Il est remis à chaque participant un petit sac, au logo de l'APSSIS, contenant outre le planning des conférences avec les heures de pauses et de repas, informations qui s'avèreront très utiles, un gros bloc pour prendre des notes. Quant aux stylos, ils étaient disponibles sur la table. Ce bloc-notes, durant ces trois jours, je l'ai entièrement rempli par des notes manuscrites qui devaient me servir à écrire ce papier. C'est dire qu'à force d'écrire et encore d'écrire, j'ai éprouvé une légère crampe à la main droite, mais c'était pour la bonne cause, pour que vous puissiez lire ce papier.

Il est aux alentours de midi. Un buffet d'accueil nous est offert. C'est copieux, nous avons le choix entre eau plate ou eau gazeuse. Chacun avec son panier repas s'assoit où il peut, c'est l'occasion des premières retrouvailles, des premières rencontres de nouveaux amis qui partagent le même intérêt pour les technologies de la cybersécurité. Un bon nombre d'entre eux est confronté aux cyber attaques, aux problèmes de budgets toujours insuffisants, à l'obligation impérative d'évangéliser, sensibiliser, voire former tous les utilisateurs pour faire de chacun d'eux, un maillon un peu moins faible de la chaine de sécurité.

Un bon nombre d'entre eux, et d'entre elles, est confronté à la nécessité de convaincre les décideurs qui détiennent les budgets qu'avant une attaque sur l'information et son système, l'investissement en solutions de sécurité peut paraître trop cher, **mais qu'après l'attaque, qui n'arrive pas qu'aux autres, il pourrait être trop tard.**

Comment décrire le premier sentiment que j'ai ressenti en arrivant sur le lieu de l'évènement ? Le voici en quelques mots : **On est bien dans ce congrès du CNSSIS**, on va connaître beaucoup de nouvelles personnalités, on sait qu'on va apprendre beaucoup de choses nouvelles, et même d'après l'agenda, qu'on va avoir une introduction à l'utilisation de la physique quantique pour le chiffrement des données, et avoir la tête plongée dans les étoiles. Attendez la suite…

Après remise du badge, dépôt des valises dans un coin du grand amphi, après les poignées de mains et les « bonjour Gérard » qui me rappellent que je ne suis pas en territoire complètement inconnu, la première table ronde étant prévue à 13h20, nous avons le temps de nous restaurer tout en discutant avec les congressistes qui partagent notre passion pour le savoir-faire et le savoir-être, aussi très important, dans la cybersécurité.

Les partenaires du congrès

C'est aussi l'occasion d'engager un premier contact avec les partenaires de l'évènement, les offreurs de solutions et les organisations, ministères et associations. Voir la liste en : https://www.apssis.com/le-congres/2023/sponsors.htm

Et je tombe sur le stand de **Stormshield**, une filiale de mon ancien employeur AIRBUS Cybersecurity. La société Stormshield je la connais bien, car dans des mastères spécialisés d'écoles d'ingénieurs et dans des MBA où j'enseigne, je soumets à mes apprenants une réponse à faire, en petits groupes, à un appel d'offre sur des architectures de cybersécurité. Il doit y avoir dans leurs réponses des firewalls, des VPN IPsec et SSL/TLS, de la sécurisation de serveurs web et de postes nomades, de la gestion centralisée, le tout traité sur les plans techniques, services et financiers… J'exige que les solutions qu'ils me proposent soient des solutions françaises, labélisées Critères Communs à un niveau au moins équivalent à EAL3+ par l'ANSSI. Avec cette demande, ils n'ont pas le choix ; il reste l'offre de Stormshield. Et voilà que j'apprends, sur ce stand, par un sympathique congressiste qui travaille en avant-vente chez Stormshield que leur gamme d'appliances, les firewalls tout en un, va évoluer !

Cet employé de Stormshield, basé au Mans, ça aussi j'ignorais que cette entreprise avait aussi des employés ailleurs qu'à Issy-les-Moulineaux, Lyon et Lille, me décrit en détail l'évolution de leur offre, la nouvelle liste de prix publics, et me promet même de m'envoyer une présentation PowerPoint que je pourrai intégrer en partie dans mes futurs cours. J'ai eu les réponses à toutes les questions que je lui ai posées, et même des réponses à des questions auxquelles je n'avais pas pensé de lui poser. Mes étudiants auront de la chance, et moi, j'ai eu une grande chance d'être au CNSSIS pour mettre au goût du jour mon projet pédagogique de réponses à cet appel d'offre.

Telles sont les opportunités inattendues qu'on rencontre au Congrès National des SI de Santé ! Et pour finir, l'employé de Stormshield me remet un assortiment de goodies ! Des employés en avant-ventes, des commerciaux de Stormshield, j'en ai vu d'autres durant ces trois jours. J'ai aussi discuté bien sûr, dans les autres stands, avec d'autres partenaires de l'évènement. J'ai beaucoup appris, j'ai beaucoup apprécié.

Voici un aperçu du couloir des partenaires sur le chemin du grand amphi, qui est au fond à gauche.

Une petite sirène retentit ; le congrès va commencer. Toutes et tous vont prendre place dans l'amphi. Un petit film d'ambiance montrant des séquences d'informations à la télé, aux journaux d'information sur la cyber attaque sur le CHU de Corbeil et sur celui de Versailles, est projeté et le sera à chaque début de séance.

Voir en : *https://www.youtube.com/watch?v=XOAcTFpUlrg*

Vincent Trély, président et fondateur de l'APSSIS (www.apssis.com), ouvre le 11ème Congrès sous les applaudissements.

Dans le grand amphi devant plus de 200 participants, Vincent donne une rétrospective de l'**A**ssociation **P**our la **S**écurité des **S**ystèmes d'**I**nformation de **S**anté qu'il a créée avec son équipe **en 2011**. Quel chemin parcouru entre les 60 adhérents du début et les plus de 200 actuellement ! Vincent Trély et l'équipe de l'APSSIS, avec en particulier Auriane Lemesle, Cédric Cartau, Charles Blanc-Rolin, seront très présents au cours des 3 jours du congrès pour animer les débats.

Vincent évoque le prochain évènement « ***les rencontres SSI Santé 2023*** » qui se tiendront à la Maison des Polytechniciens, à Paris, le 28 septembre 2023.

Première table ronde sur La Task Force Cyber

Auriane Lemesle, secrétaire générale de l'APSSIS, référente régionale Sécurité des Systèmes d'Information chez GCS e-santé Pays de la Loire et **Vincent Trély** ouvrent la première table ronde institutionnelle sur la **Task Force Cyber** créée le mercredi 21 décembre 2022, par les Ministres de l'Intérieur, Gérald Darmanin, de la Santé, François Braun, et le ministre délégué au Numérique, Jean-Noël Barrot.

Auriane présente les intervenants :

Laure Duhesme, coordinatrice sectorielle santé à l'ANSSI

Jean-Baptiste Lapeyrie, Délégation du Numérique en Santé, directeur de projets / CTO au Ministère de la Santé et de la Prévention

Marc Loutrel, Directeur expertise innovation et international, à l'Agence du Numérique en Santé

Nicolas Voss - Adjoint à la cheffe du bureau Systèmes d'Information - Ministère de la Santé et la Prévention – direction générale de l'offre de soins : DGOS

Le débat s'anime lors de cette première table ronde institutionnelle

Il est question de mutualisation de ressources, d'industrialisation en particulier dans la gestion de crises cyber, de financements annuels conditionnés par l'atteinte d'objectifs définis.

Il est question aussi de développer une offre en cybersécurité sur le plan régional et national, avec l'aide des GRADeS (Groupement Régional d'Appui au Développement de la e-Santé). Il est question de la directive européenne NIS2.
Les intervenants notent que les cyber attaques sont de plus en plus sophistiquées, mais on observe cette année une légère baisse des attaques en rançongiciel. Les efforts consentis commenceraient-ils à payer ? Les cyberattaques touchent essentiellement les collectivités locales, les établissements de santé et les TPE/PME. Les hôpitaux ne font pas l'objet de ciblage spécifique mais s'ils sont très attaqués, car ils sont très connectés.

Les actions déjà engagées par la **Task Force** portent sur cinq axes :

1. La résilience avec en particulier la gestion de crise cyber, le plan blanc numérique (premier trimestre 2023), la continuité et la reprise d'activité en cas d'attaque
2. L'implication des directions d'établissements sur la formation à la SSI
3. L'évolution des grilles RH pour retenir ou embaucher des experts en cybersécurité
4. L'ouverture d'un espace dédié à la e-santé
5. Les communications et sensibilisations régulières

Quatre domaines prioritaires ont été identifiés :

1. Audits techniques
2. Sécurité des postes de travail
3. Sécurité des accès
4. Sauvegardes

La **directive européenne NIS2,** publiée le 27 décembre 2022, pourrait s'appliquer à l'ensemble des établissements hospitaliers français. Elle concernera les prestataires de soins de santé, les laboratoires, la recherche et de développement des produits pharmaceutiques, et les entités fabriquant des dispositifs médicaux critiques. Sont concernées les entités essentielles « EE » (établissements de plus de 250 salariés) et les entités importantes « EI » (établissements entre 50 et 250 salariés). Inférieurs à 50 salariés c'est au cas par cas. Chaque centre hospitalier concerné devra réaliser une analyse d'impact. L'ANSSI voit son autorité renforcée et accompagnera les EE et les EI pour qu'ils se mettent en conformité avec cette directive.

Voici la deuxième table ronde : « Témoignage d'un établissement de santé visé par une cyberattaque. Retour d'expérience des membres de l'Asinhpa »

Prennent place **Vincent Genot**, RSSI du GHT de Dordogne, **David Henocq**, RSSI d'Okantis et **Nicole Genotelle** RSSI et DPO du Mipih.

L'**ASINHPA** est l'**A**ssociation des **S**tructures d'**I**nformatique **H**ospitalières **P**ubliques **A**utonomes. Elle regroupe les principaux acteurs publics des systèmes d'information hospitaliers et de Santé. Elle développe des solutions, conseille et accompagne dans leur mise en œuvre, les organisations au bénéfice de la qualité du parcours de soins du patient.

Un conseil est de surveiller le réseau et cartographier et maitriser l'ensemble des flux. Il faut surveiller les comptes à privilèges et pratiquer des exercices de crises cyber en y intégrant les partenaires.

L'ASINHPA a créé un CERT qui est en relation avec d'autres CERT. En cas d'agression, il est urgent de porter plainte.

Il va être question de retours d'expérience et de bonnes pratiques pour résoudre un incident qui survient dans un établissement de santé. Le CHU de Dordogne a subi une première attaque en juillet 2021, un prestataire a été corrompu, des serveurs n'étaient pas mis à jour, l'attaque s'est produite. En novembre 2022, ce CHU avait gagné en maturité mais suite à une autre cyberattaque, il a fallu isoler le réseau de l'Internet. Un expert du GIP, aidé par un expert métier ont été indispensables pour gérer le problème.

Vincent Genot nous livre un retour d'expérience relatif à une cyberattaque subie par le centre hospitalier de Bergerac, à 2h du matin, un dimanche. Trente serveurs ont subi un cryptovirus qui a chiffré leurs données. Il faut sans attendre couper les accès venant de l'Internet en

éteignant les routeurs pour isoler le réseau. On se sent très seuls face à cette cyberattaque, surtout si, en cette nuit, on n'est que deux personnes disponibles pour s'occuper du problème. Y a-t-il eu aussi exfiltration de données ? Difficile à dire. Les sauvegardes seront-elles utilisables ? Quelle angoisse, mais ce n'est pas le moment de perdre ses moyens.

David Henocq nous donne des conseils de bon sens : Couper la connexion à l'Internet, bien sûr, même si la téléphonie est sur IP. Il faut relancer les communications aussi vite que possible. Il faut savoir à qui s'adresser, sans avoir bien sûr à rechercher la liste des personnes à contacter sur Internet puisque le réseau n'est plus disponible. Les exercices de crise cyber sont indispensables pour garder les bons réflexes. Le personnel les ont-ils suivis ? Et il faut commencer par rétablir les applications nécessaires au bon fonctionnement de l'établissement hospitalier.

Nicole Genotelle insiste sur la nécessité d'avoir une idée claire des priorités pour agir efficacement, même dans la tourmente. Il est impératif de savoir quelles applications métiers sont indispensables au centre hospitalier et qui pourra les rétablir.

3ème conférence : Bonifier, partager et sécuriser la donnée : Alcatel-Lucent Enterprise et Keenturtle

Cette conférence met en scène **Laurent Bouchoucha**, VP business development chez Alcatel-Lucent Enterprise, et **François Versini**, Président-fondateur de Keenturtle.

Alcatel-Lucent Enterprise propose des solutions pour soutenir la transformation numérique des entreprises du secteur public. **Keenturtle** fournit un système d'aide à la décision, personnalisée en déterminant les données utiles. Il propose aussi une détection d'alertes, en se basant sur l'IA et sur la data.

Le problème posé avec les données de santé est : « Sont-elles pertinentes pour éclairer les professionnels de santé, les établissements et les patients ? ». Quand on connait les données utiles, on peut prendre les bonnes décisions. L'autre problème est de savoir si les données produites sont suffisamment utilisées par les GHT. Ont-ils la compétence technique et culturelle pour les exploiter, pour la prise en charge des patients, pour des travaux de recherche ? Disposer de la bonne information, au bon moment, peut s'avérer cruciale. Les algorithmes de traitements par l'IA peuvent apporter l'aide indispensable.

Alcatel-Lucent Enterprise et Keenturtle participent, avec le CEA, dans le cadre de la Filière Santé Numérique, au consortium **Pleeade** qui alimente les entrepôts de données interconnectés. Sa plateforme **Rainbow** qui héberge des données de santé sécurisées contribue à apporter la bonne information aux établissements hospitaliers et médicaux-sociaux.

Pause de 40 minutes : on va visiter les stands des partenaires. Il est 17h00 : on reprend au son de la petite sirène.

Conférence du club RSSI sur les marchés de la CAIH

« Conformité numérique : Si tout commençait lors de l'achat des équipements et des services de l'hôpital ? »

Cette conférence est animée par

- **Régis Kaminski**, acheteur sur les marchés Sécurité **CAIH** (**C**entrale d'**A**chat de l'**I**nformatique **H**ospitalière)
- **Guillaume Deraedt**, RSSI du GHT Côte d'Opale et Directeur de la stratégie numérique pour la **CAIH**. Il coordonne, à la CAIH, les marchés publics, centrés sur la sécurité, à destination des établissements de santé, sociaux et médico-sociaux, et l'intégration du clausier conformité numérique.
- **Jacques Labidurie**, RSSI du Centre Hospitalier de Limoges
- **Béatrice Bérard**, Officier de sécurité des Hospices Civils de Lyon
- et **Richard Dondossola**, RSSI/DPO du CHRU de Tours

Le **Club RSSI** se compose à ce jour de 76 membres qui représentent 65 GHT en France. C'est un cercle d'échanges entre RSSI et DPO hospitaliers pour une prise en compte, par le biais d'échanges sur les normes, le marché, les éditeurs, des bonnes pratiques dès les phases d'achats. Un partenariat entre le Club RSSI, UniHA et la CAIH a été signé, à l'occasion de Santexpo 2023, pour améliorer la gestion des risques numériques dès la phase d'achat de solutions, logiciels, services ou matériels de santé.

La CEIH édite un catalogue de solutions de sécurité : portail.caih-sante.org (web réservé aux adhérents).

Un clausier de conformité pour le respect de la règle ISO 27001, du RGPD, pour la gestion des fournisseurs sera proposé pour être intégré dans les appels d'offre. La maturité des fournisseurs pourra être évaluée par une analyse EBIOS RM.

Conférence de Proofpoint, animée par Loïc Guézo

Les établissements de santé dans la tourmente

Les collectivités locales et les établissements de santé sont au cœur de la tourmente. Les rançongiciels sont omniprésents et s'appuient souvent sur des fraudes par ingénierie sociale.

Parmi ceux qui ont répondu à l'enquête de HIMSS, le phishing, ciblé ou pas, (57% des répondants), le vol d'identifiants (21% des répondants) et l'ingénierie sociale (20% des répondants) sont dans le top 3 des attaques.

85% des attaques utilisent le facteur humain pour réussir. Quand les données sont dans un Cloud des GAFAM, les attaquants s'y trouvent pratiquement chez eux.

Le BEC (Business E-mail Compromise), signale **Loïc Guézo**, se répand dans les entreprises. Des e-mails frauduleux, provenant d'organisations ayant fait les frais d'une usurpation de marque, incitent les utilisateurs à faire des virements bancaires ou à transmettre des données sensibles commerciales ou personnelles. La fraude au président peut s'opérer. Proofpoint bloque 3,4 millions d'attaques BEC par mois.

Dans les centres hospitaliers, il faut en particulier prendre ses précautions avec la Supply Chain.

Bien sûr la sensibilisation et les exercices de simulation d'attaques sont indispensables dans une organisation, mais comme le fait remarquer un participant, « *arrêtez de sensibiliser les Utilisateurs, pensez plutôt à les protéger !* »

Pour terminer les conférences de la première journée, voici venu un autre grand moment sur les applications de la physique quantique.

Présenté par Philippe Loudenot qui a été son élève et qui avoue malicieusement n'avoir pas tout compris à son cours, **le professeur Robert Erra**, enseignant chercheur à l'ESIEA monte sur scène pour nous parler d'un sujet qui dépasse le seul domaine de la Santé et des groupements hospitaliers : Qu'est-ce que la physique quantique ? Quelles sont ses applications dans le domaine du chiffrement des données ? Qu'est ce qui est utilisable aujourd'hui dans cette technologie qui semble être une technologie du futur ?

Tout de suite nous sommes conquis par l'érudition et la pédagogie de ce professeur et docteur en informatique. Elle

transpire de ses paroles. Si on connait la vitesse d'une particule qui se déplace, on ne peut connaître sa position et inversement si on connait sa position, on ne peut connaître sa vitesse. Pratique pour ne pas avoir un PV sur autoroute, mais il ne s'agit pas là du domaine macroscopique dans lequel nous sommes mais de celui de l'infiniment petit, de l'ordre du photon ou de l'électron et même encore plus petit, car ces particules sont divisibles.

Un photon rencontrant deux fentes dans une surface devant lui ne choisit pas l'une ou l'autre. Il passe simultanément par les deux fentes et interfère avec lui-même à la sortie et donne donc des franges d'interférence. Facile à démontrer, surtout si on sait produire les photons un par un.

Avec deux photons qui ont subit une **intrication quantique**, même s'ils sont séparés par plusieurs milliers de kilomètres, voire beaucoup plus, si on modifie le spin de l'un, on modifie automatiquement le spin de l'autre. C'est normal puisqu'il s'agit en fait de la même particule à deux endroits différents et la distance n'y joue aucun rôle. Bien sûr si on observe le mouvement, il y a décorrélation, perte de la **superposition quantique**, et le photon se retrouve à nouveau tout seul.

Un bit est à 0 ou à 1. Un **qubit** (quantum bit) est constitué d'une superposition quantique probabiliste d'états à 0 et à 1 en même temps. En d'autres termes un qubit est un « *vecteur de l'espace vectoriel complexe (de dimension 2) pour lequel une base particulière (orthogonale) a été choisie* ». Il évolue dans la sphère de Bloch. Les qubits sont donc pratiques pour effectuer des calculs en parallèle. Avec des algorithmes appropriés, on va beaucoup, mais beaucoup plus vite qu'avec les ordinateurs classiques. Ceci bien sûr n'existe que si les qubits perturbés ne subissent pas une **décorrélation quantique** au bout d'un moment. Ceci implique, pour ne pas causer d'erreurs de calculs, de disposer, pour chaque qubit logique utile, de nombreux qubits correcteurs d'erreur et il en faut beaucoup, pour chaque qubit utile !

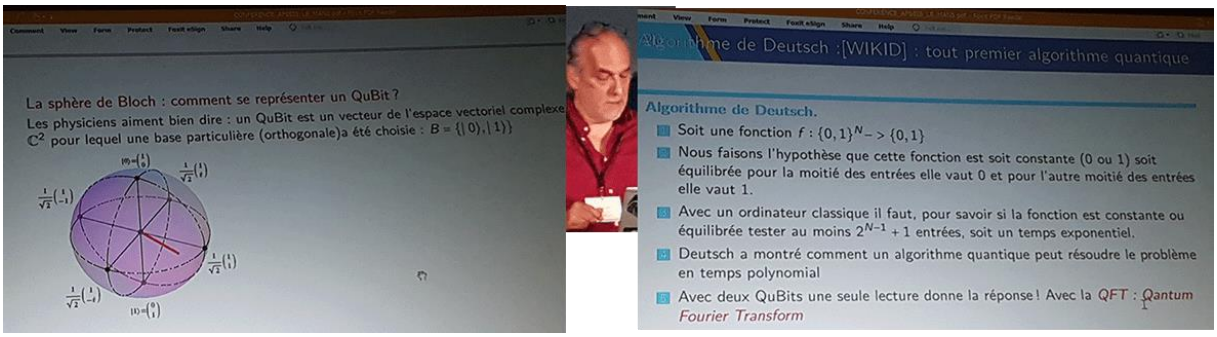
Vous avez tout compris ? Non, pas possible car notre image de pensée est basée sur la traditionnelle géométrie euclidienne, et cela suppose que vous n'avez en fait rien compris. Même Einstein était gêné de savoir que deux photons ou électrons intriqués réagissaient instantanément quelle que soit leur distance de séparation ! Peut-on vraiment aller plus vite que la vitesse de la lumière alors que la masse deviendrait plus qu'infinie. Car même si les photons n'ont pas de masse, les électrons en ont une, mais matière, énergie, tout ça est lié ?

Le calculateur quantique est assez éloigné d'une machine de Turing et n'est pas conçu par exemple pour utiliser des tableaux Excel. Alors que peut-on faire en pratique aujourd'hui avec les applications de la physique quantique appliquées au chiffrement ?

Il faut savoir qu'on différentie le **chiffrement quantique** et le **chiffrement post quantique**. Le chiffrement quantique, c'est uniquement **le transport de photons en superposition quantique** pour échanger la clé secrète symétrique de celui qui l'envoie vers celui qui la reçoit. Et si on tente d'observer cette clé au passage, pfutt, la **décorrélation** quantique s'opère et la clé doit être rejouée ou elle devient inutilisable. Génial n'est-ce pas ? Bien sûr il faut pouvoir envoyer les particules une par une, mais ça, on sait faire.

Il n'est donc plus utile de chiffrer, par le RSA, la clé secrète symétrique en utilisant la clé publique trouvée dans un certificat numérique. Le chiffrement quantique n'est plus un problème de mathématiques mais un problème de physique des particules.

D'autant plus que le chiffrement asymétrique RSA sera condamné par la vitesse de calcul, en force brute, des calculateurs quantiques. L'algorithme de **Deutsch** tuera le chiffrement asymétrique, ou alors il faudra des clés asymétriques de 4096 bits ou même bien plus, mais ça ne correspondra plus au standard du RSA jusqu'ici adopté. En 1993-94, l'algorithme de **Shor** est devenu aussi une menace pour le chiffrement asymétrique. L'algorithme de **Grover** pourrait, avec des calculateurs quantiques très puissants (Robert Erra n'aime pas le terme « ordinateur » quantique et préfère « calculateur » quantique) mettre aussi en cause, mais dans un avenir beaucoup plus lointain, le chiffrement symétrique, comme l'AES. Les fonctions de hachage et les courbes elliptiques qui interviennent par exemple dans les blockchains seront-elles condamnées par les calculateurs quantiques ? Les blockchains comme celles des bitcoins qui utilisent des courbes elliptiques, sont-elles menacées de devenir inefficaces ?



Les chiffrements dits « **post quantiques** », sont des algorithmes de chiffrement qui s'appuient sur les calculateurs quantiques. Quand ils seront nombreux à être opérationnels, ils pourront offrir une solution utilisable alors que le chiffrement classique sera devenu obsolète.

Le **NIST**, grand organisme de standardisation US, a émis un appel à projets pour faire émerger un standard de chiffrement post quantique. Certains algorithmes sont proposés en open source, d'autres sont soumis à des brevets mais si on répond au « Call for proposal » du NIST, il faut abandonner ses droits de propriété. Et Robert Erra nous parle de Crystals-Dilithium, Falcon, Sphincs, Bike… 70 algorithmes ont été proposés au départ, 26 ont été retenus au premier round, puis 15 … La crypto à base de **réseaux euclidiens**, comme le système NTRU, semble garder ses chances d'être retenue comme un standard de chiffrement post quantique.

Robert Erra croit-il que les ordinateurs quantiques opérationnels vont devenir une réalité dans un temps pas trop lointain ? Déjà, il nous présente les 2 portes de Hadamard et une porte X, avec les équations associées et les matrices unitaires et inversibles. Elles composent un circuit quantique. Une des bases des calculateurs quantiques est donc déjà une réalité, et il y a d'autres portes qui composent des circuits quantiques opérationnels.

En conclusion, on peut penser que les calculateurs quantiques, qui rendront inefficaces, par la rapidité de leurs calculs le chiffrement classique, ne seront pas en nombre suffisant pour tout de suite, mais il faut dès aujourd'hui choisir la bonne taille de clés et migrer dans un avenir pas trop lointain vers les algorithmes post quantiques, une fois que ceux-ci auront été normalisés.

Voici venu le temps du repas convivial ! Premier dîner APSSIS et ASINHPA

La journée de conférences se termine, nous avons fait, avec la dernière intervention, notre plein d'algorithmes du futur. Nous reprenons nos valises et, chemin faisant, nous regagnons nos hôtels pour le Check-in, l'attribution et l'installation dans nos chambres. Plusieurs hôtels sont prévus pour accueillir les congressistes. Pour moi c'est le Concordia, à une dizaine de minutes de marche des Quinconces. Nous avons peu de temps à passer à l'hôtel car nous devons nous rendre à pied au restaurant la Réserve pour le repas du soir pris en commun, avec des algorithmes plein la tête.

Sur la photo de gauche, nous sortons de l'hôtel Concordia. Sur la photo du milieu nous entrons dans le restaurant « La Réserve ». Le restaurant est privatisé pour nous. Sur la photo de droite Robert Erra et Vincent Trély à la table d'honneur où j'ai été conviée.

L'APSSIS m'a en effet placé à la table d'honneur, avec le professeur Erra à côté de moi, Vincent Trély et Philippe Loudenot pas loin et l'inimitable Cedric Cartau qui écrit des rubriques remarquables, que je prends toujours plaisir à lire, dans le média DSIH et sur LinkedIn. Cédric Cartau était "en vrai", c'est-à-dire en présentiel, en face de moi, alors que j'ai plus l'habitude de ne le voir qu'en distanciel par Zoom, par exemple au « Lundi de la cybersécurité » où je l'ai fait intervenir.

Le repas ? excellent ! Le lieu ? très bien, le personnel du restaurant ? très classe, l'ambiance ? une ambiance de fête dans cette ville où, il n'y a que 3 jours, la course des 24 heures du Mans avait rempli les gradins de la piste.

Nous commençons par une coupe de champagne, que du bonheur ! Et quel condensé d'enthousiasme chez toutes ces personnalités autour de moi !

Le repas terminé, il est plus de 23h, il est temps de prendre congé, de regagner l'hôtel, et vite dormir car la deuxième journée ne va pas tarder.

Deuxième jour du CNSSIS

A l'aube du deuxième jour

Réveil pas facile, la nuit a été courte mais c'est avec enthousiasme que j'aborde le deuxième jour du CNSSIS. Je me rends de suite, à pied, à l'espace culturel des Quinconces sans passer par la case petit-déjeuner de l'hôtel. Un café, des croissants et des viennoiseries nous attendent au CNSSIS, et c'est aussi une occasion de discuter, avant la première conférence de la matinée, avec celles et ceux que j'avais quittés la veille.

L'amphi s'est rempli. **Charles Blanc-Rolin** Vice-Président de l'APSSIS et Chef de projet sécurité numérique e-santé Pays de la Loire, nous accueille pour une courte intervention sur l'**AFIB**.

L'Association Française des Ingénieurs Bio Médicaux (AFIB)

L'**AFIB** compte 380 adhérents dont 320 ingénieurs des établissements médicaux publics et privés. Elle organise des journées thématiques en Régions. La démarche de l'association est nationale et transverse. Son objectif est de permettre à un constructeur ou éditeur de logiciel de faire une réponse qui soit prise en considération par tous les établissements de santé.

L'AFIB est un organisme de formation continue qui travaille avec les Centrales d'Achats comme la CAIH et UniHA.

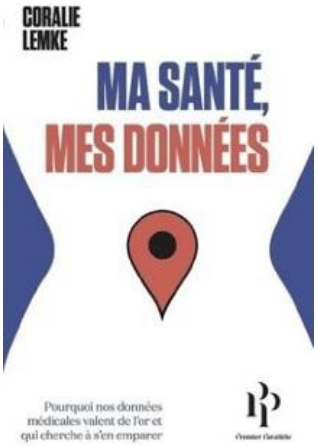
Conférence de la journaliste et écrivaine, Coralie Lemke

Coralie Lemke est journaliste scientifique pour Sciences et Avenir. Ses domaines d'intérêt sont l'intelligence artificielle en médecine, le séquençage génétique et les questions de bioéthique.

Elle est l'auteure d'un livre « **MA SANTÉ, MES DONNÉES Pourquoi nos données médicales valent de l'or et qui cherche à s'en emparer ?** » A la pause elle dédicacera son livre. Le sujet de sa conférence est : « **Données de santé : au fond, à quoi servent-elles ? ».**

Oui, à quoi peuvent-elles bien servir ? Depuis le premier essai clinique connu, attribué au capitaine Lind qui voulait comprendre, par une étude statistique, quelles étaient les causes du

Scorbut qui affectait ceux qui restaient longtemps en mer, en passant par une étude qui portait sur trois générations de personnes testées, dans la ville de Framingham, au Massachusetts, près de Harvard, pour déterminer les facteurs de risque des maladies cardio-vasculaires, Coralie nous emmène dans un voyage dans le passé, mais aussi dans le présent avec ce que deviennent nos données captées par les GAFAM et par d'autres prédateurs.



L'étude de Framingham a fait avancer la connaissance scientifique dans le domaine des maladies cardio-vasculaires. Il n'en est pas de même pour la captation de nos données médicales qui ne sont pas destinées à des recherches pour améliorer la santé de la population, mais pour faire du business souvent pas du tout légal.

Nous en venons à l'Intelligence Artificielle, sujet qui passionne Coralie. Une étude statistique montre que ce ne sont pas les conditions matérielles qui induisent le bonheur mais c'est d'être bien entouré pour être heureux.

A la pause, une queue allait se former pour acheter le livre que Coralie dédicaçait.

Conférence d'AXIANS sur la sensibilisation et la sécurisation des SI dans le domaine Biomédical

Sébastien Bonnet, DPO et RSSI chez AXIANS et **Stéphane Benoliel**, Pilote Cyber Santé, également chez AXIANS prennent la parole.

AXIANS est une marque du groupe Vinci-Energie et compte 4500 employés dans le domaine des infrastructures de télécommunications et dans celui de la transformation digitale. Les systèmes d'information IT connaissent des menaces comme les botnets, les ransomwares, les vols d'identités numériques, mais les systèmes OT (industriels) connaissent les mêmes menaces et en plus celles qui pèsent sur les objets connectés.

L'informatique biomédicale concerne les équipements de santé connectés aux systèmes d'information. Un centre hospitalier doit assurer la gestion technique des bâtiments, la qualité de l'air pour éviter les infections, la bonne marche des ascenseurs, de l'éclairage et d'une manière générale la gestion technique de l'électricité. Les ingénieurs biomédicaux et la Direction doivent pouvoir faire face à des situations sanitaires parfois exceptionnelles. Des exercices de gestion de crise et des analyses de risques doivent être menés à intervalles réguliers et concerner le plus grand nombre. Au centre du dispositif de sécurité, l'humain est un facteur clé.

Il est remarqué un manque de dialogue entre la DSI et le domaine biomédical.

C'est la pause. Je retourne sur les stands des partenaires pour papoter avec les copains dans le couloir où **Coralie Lemke dédicace son livre.**

Puis la petite sirène se fait entendre pour appeler les participants à la reprise des présentations.

Le tour est à Orange Cyberdéfense.

Orange Cyberdéfense intervient sur le thème : « Renforcement du soutien aux structures par les centres de ressources cyber régionaux – GCS eSanté des Pays de la Loire »

Le **GCS** e-santé des **Pays** de la **Loire,** c'est le **G**roupement **R**égional d'**A**ppui au **D**éveloppement de la **e-S**anté (**GRADeS**) dans cette Région.

Auriane Lemesle qui est la référente régionale Sécurité des Systèmes d'Information, et qui est aussi secrétaire générale de l'APSSIS interroge **Simon Deterre** d'Orange Cyberdéfense et **Thomas Le Clerc**, Référent santé, éducation, collectivités - Région Pays de Loire et Bretagne - Orange Cyberdefense.

Orange Cyberdéfense a déployé avec le GCS des Pays de la Loire, et dans six autres centres régionaux, l'escape game **Sant'escape** qui apporte une touche ludique dans la formation à la cybersécurité des équipes IT. L'entreprise accompagne également les TPE/ PME dans la conduite des analyses de risque cyber.

Le constat est que ces organisations similaires aux structures médico-sociales n'ont pas souvent dressé l'inventaire de leurs actifs numériques. leurs applications sont rarement à jour et ont gardé, par défaut, leur paramétrage initial. Les règles de la politique de sécurité sont paramétrées par les prestataires, pas par les organisations clientes. Pour pallier ces insuffisances, des fiches reflexes ont été mises à leur disposition et un accompagnement auprès des ESMS permet d'élever leur niveau de maturité. Une formation à la destination des équipes IT pour la détection et réaction face à un rançongiciel coconstruite par Orange Cyberdéfense, le GCS e-santé et un GHT a été présentée. Le programme de la formation permet également de faire le lien avec l'accompagnement proposé par le GCS sur le déploiement du_logiciel open source **SELKS**, système de protection contre les intrusions

IDS/IPS, et de détection des menaces. Orange Cyberdéfense propose le logiciel open source **SELKS**, système de protection contre les intrusions IDS/IPS, et de détection des menaces.

La principale difficulté réside dans le temps d'accompagnement nécessaire, qui est dédié à chaque établissement.

RELYENS : Quels arbitrages en cybersécurité ? Quelles stratégies d'investissements ?

Fort de ses 1100 collaborateurs et de ses plus de 34 000 clients, **RELYENS** est un groupe mutualiste lyonnais, mais implanté dans plusieurs pays, spécialisé dans l'assurance et la gestion des risques aux services des acteurs de la santé et des territoires.

Christophe Millet, Cyber Risk Manager pour le groupe **RELYENS,** utilise les Shadocks pour illustrer certains de ses transparents.

« *Il vaut mieux sécuriser ses données en pensant que ça ne servira à rien, plutôt que ne pas les sécuriser en attendant qu'il se passe quelque chose* »

Cette devise que je propose, issue de la philosophie Shadock, je suis sûr que la ferez vôtre 😊.

Les cyberattaques qui détruisent ou pire corrompent les données des patients, ou les révèlent au grand public, entraînent une perte de confiance vis-à-vis des centres hospitaliers. Et il est dit qu'il est difficile pour eux de maintenir un niveau de sécurité suffisant car il faut investir. Pour cela il faut commencer par quantifier le risque cyber.

Les équipes de RELYENS accompagnent les acteurs du soin et des territoires dans la sécurisation de leurs activités, dans la protection de leurs employés, et propose une offre de gestion des risques cyber.

Christophe Millet nous décrit les biais de décisions qui pèsent sur les investissements dans la cybersécurité :

1. L'aspect légal : Les référentiels sont trop nombreux et parfois contradictoires
2. L'aspect budgétaire : On fait surtout la chasse à la subvention
3. L'aspect culturel : Ce n'est pas mon problème, c'est celui du RSSI, pense-t-on.

Il faut prendre conscience qu'il ne faut surtout pas se calquer sur les USA car leur cadre réglementaire est très différent du nôtre. Par exemple, si moins de 500 patients sont concernés par un problème, il n'y a pas de déclaration à faire aux autorités américaines.

Pour mener des choix éclairés, il faut confronter les attaques et les défenses. Il faut convaincre sa Direction, avec ROI à l'appui, que l'investissement dans la cybersécurité est un choix qui rapporte. Il faut optimiser le budget en cybersécurité, mais quid de la cyber assurance pour

répondre aux risques résiduels ? Bien sûr, dans un centre hospitalier, ce n'est pas pour l'assureur qu'on travaille mais pour aider les patients et une assurance ne doit pas entrainer une déresponsabilisation.

Il est l'heure d'aller déjeuner.

Nous nous rendons à la Brasserie Madeleine, située de l'autre côté de la place des Jacobins,

Je m'arrange pour être assis en face d'un congressiste avec qui je souhaite discuter : **Jacques Labidurie**. Si vous assistez à nos « Lundi de la cybersécurité » mensuels, vous avez forcément remarqué, dans la séquence questions/réponses qui suit ces évènements, les interventions de Jacques, ses questions aux intervenants, et même parfois le récit de ses expériences, et il en a !!!

Un bonbon pour l'esprit et pour augmenter notre connaissance sur les sujets autour de la cybersécurité et la cyberdéfense.

Jacques est le Responsable de la Sécurité des Systèmes d'Information du Groupement Hospitalier Territorial du Limousin et un fidèle de nos « Lundi de la cybersécurité ». Alors le voir en vrai et pas seulement à travers un écran par webinaire Zoom, je tenais à être à la même table.

Jacques est intervenu le premier jour du CNSSIS, à la conférence de la CAIH. Et bien sûr, il a posé et posera de forts intéressantes questions lors des trois journées du CNSSIS. J'ai confié mon smartphone au DPO du CHU de Limoge, Lilian SOKOLOWSKI, assis également à notre table pour qu'il me prenne une photo à caractère personnel avec Jacques. Celui-ci est à ma droite, avec la barbe😉

Et puisqu'on parle des « Lundi de la cybersécurité », voyez l'intervention de l'incroyable Cédric Cartau que nous avons fait intervenir en février 2023 sur le thème « La cyber en santé et ses spécificités"

Pour le replay, c'est en : https://www.dailymotion.com/video/x8i71a9

Et pour la lettre d'information en : https://www.arcsi.fr/doc/Lettre-Lundi-Cyber-No56.pdf

Viennent deux séries de conférences en état de superposition

Au retour du restaurant, nous avons un choix difficile à faire. Deux conférences se tiendront dans le grand amphi et deux autres, en parallèle, dans le petit. Le professeur Robert Erra pourrait-il m'aider à trouver une solution pour assister à ces quatre présentations ? L'état de superposition quantique qui me permettrait d'être dans les deux amphis à la fois, tout en étant un unique moi-même, est-ce faisable, professeur ? J'y ai pensé, mais il y a deux problèmes :

1. La physique quantique ne s'applique qu'aux particules élémentaires, électrons, photons, quarks ; pas à moi qui suis comme vous un macro organisme.
2. Les intervenants nous observeraient et causeraient donc une décorrélation quantique, avec écroulement de la fonction d'onde, et je me retrouverais immédiatement dans un seul amphi.

Voilà, j'ai tout compris dans ce que nous a dit le professeur Robert Erra la veille et Il m'a fallu choisir. Les quatre conférences m'intéressaient mais la physique quantique n'apportant pas de solution, j'ai choisi de rester dans le grand amphi.

Dans le grand amphi, c'est **All4Tec** sur le thème l'analyse de risques Ebios RM, puis **Wallix**. Dans le petit amphi, c'est **Claranet** sur la sécurisation des applications web, puis **Advens**. L'APSSIS a prévu un replay. Je n'aurai donc pas perdu les deux présentations où je n'étais pas présent.

All4Tec, « Gagnez en efficacité pour vos analyses de risques EBIOS RM : la preuve par l'exemple ! »

Auriane Lemesle anime le débat, avec **Tony Hedoux** d'All4Tec et **Kevin Delmotte** de WELIOM.

All4Tech et **WELIOM** proposent aux GHT et aux structures médicaux-sociales, la solution **Agile Risk Manager**. Les équipes WELIOM et ALL4TEC particularisent, pour leurs clients, cet outil d'analyse de risques conformément à la méthode Ebios RM, en conformité avec la norme ISO 27005. Des scénarii de risques préétablis avec des bases de connaissances pré-intégrées, sont adaptés aux différents contextes. Cela permet des gains de temps importants et la construction d'un système de pilotage centralisé des risques.

Wallix et le RSSI du CHT Côte d'Opale

François Lancereau de Wallix, Responsable de comptes Secteur Public France et **Guillaume Deraedt**, RSSI du CHT de la Côte d'Opale nous expliquent comment fédérer des équipes techniques hétérogènes. L'association d'un fournisseur de solutions : Wallix, et d'un client qui les utilise : le

GHT de la Côte d'Opale, pour nous présenter un bastion d'administration, est une excellente idée.

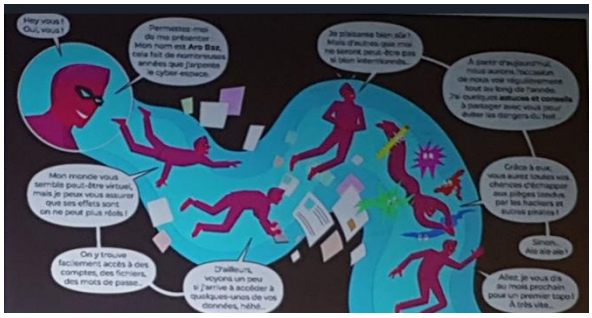
C'est la pause

Me revoici à visiter les stands des partenaires, mais on respecte l'horaire. Après 25 minutes, la petite sirène retentit et nous reprenons le cours des conférences des partenaires dans le grand amphi.

Cédric Cartau, RSSI et DPO du CHU de Nantes et du GHT44, vice-président de l'APSSIS et membre de l'ARCSI, introduit l'entreprise SIGMA.

SIGMA sur le thème « Faites de vos collaborateurs le maillon fort de votre cyberdéfense »

Avec **François Machacek**, responsable de l'offre infogérance du groupe SIGMA, **Arnaud Meunier**, RSSI du GHT de Cornouaille, à Quimper, et **Léo Fermaux**, designer Innovation de Sensipode.



Sigma, une entreprise nantaise, opère et héberge en France, des services de sécurité avec l'offre Qomity, sensibilise les entreprises par des formations et des exercices de phishing avec l'ambition de faire des agents et des collaborateurs du monde hospitalier, des maillons forts de la cyberdéfense.

Sigma met en œuvre une bande dessinée avec un personnage « **Aro Baz** », conçu par Léo Fremaux, qui rend ludique ses formations en cybersécurité.

Sigma est **certifié HDS** (Hébergeur de Données de Santé). L'entreprise propose des services dans les domaines Plan de Reprise d'Activité (PRA) et Plan de Continuité d'Activité (PCA).

Il faut poursuivre le passage de la sensibilisation à l'action dans un contexte très verticalisé où chacun a un rôle à jouer.

Cédric Cartau donne maintenant la parole à **iTrust**.

iTrust « Pourquoi le renseignement stratégique cyber est essentiel à la protection de l'écosystème français de la santé ? »

Avec **Thomas Bourthoumieux**, directeur de l'offre Cyber Threat Intelligence de iTrust et **Stéphane Robin**, responsable commercial Santé de iTrust.

iTrust, société implantée à Toulouse et à Issy-Les-Moulineaux commercialise un SOC souverain et une technologie SIEM : **Reveelium,** qui détecte et analyse les cybermenaces connues et inconnues. Autre offre, un scanner de vulnérabilité **IKare.**

La Cyber Threat Intelligence (CTI) ou service de renseignement sur les cyber menaces, a pour but de collecter et d'analyser les évènements venant du cyberespace, en s'aidant de l'Intelligence artificielle. Ceci est essentiel dans le domaine des centres hospitaliers, et comme l'a dit le général chinois du il y a 2600 ans, Sun Tzu : « *Si tu ignores ton ennemi, tu es sûr de perdre* ».

Le groupe Iliad par sa filiale Free Pro, en avril 2023 est devenu actionnaire majoritaire de iTrust.

Les intervenants nous parlent des ransomwares ravageurs comme LockBit 3.0 qui ont ciblé 11% des établissements de santé en 2019 et de BlackCat en 2021.

Pour la dernière conférence de cette deuxième journée, l'amphi retient son souffle, car voici un spationaute, Jean-François Clervoy, qui va nous passionner sur le thème **« Se préparer au pire en espérant le meilleur »**

La dernière intervention évènement de la journée précédente portait, avec le professeur Robert Erra, sur le chiffrement post quantique qui donnait un aperçu d'une nouvelle manière de chiffrer les données. Nous allons avoir maintenant un aperçu d'une nouvelle manière de gérer les risques : la **méthode de gestion des risques dans l'espace**. Cette dernière intervention de la deuxième journée accueille un spationaute, **Jean-François Clervoy** qui va nous parler de la manière d'appréhender les risques, au décollage, en orbite, autour de notre planète et à l'atterrissage : ***Se préparer au pire, en espérant le meilleur***.

Que la terre est belle vue en orbite, avec 16 couchers de soleil par jour ! Mais pour l'admirer à partir d'une station orbitale, il faut avoir subi un entrainement très dur car, dans un voyage spatial, les risques sont immenses. Mais s'ils sont bien maîtrisés par de très nombreuses simulations, le meilleur semble possible.

Polytechnicien puis élève de Sup Aero, chef du programme des vols paraboliques, Ingénieur Général de l'Armement, **Jean-François Clervoy** a mené de 1985 à 2018 une carrière de **spationaute** avec 3 missions dans l'espace, de 1994 à 1997. La sélection pour participer aux vols spatiaux est très sévère, les casse-cous ne sont pas acceptés. Les élus aux programmes spatiaux doivent savoir gérer les risques !

Quand un programme spatial est lancé pour 10 ans, la moitié des problèmes n'a pas encore trouvé de solutions. Mais ce n'est pas en orbite qu'arrivent les pires catastrophes, bien que les spationautes filent à 28 000 km/heure, alors que le vaisseau chute, attiré par la terre mais sans jamais la rencontrer. C'est au lancement et au retour sur terre que se situent les phases qui présentent le plus de risques.

Un spationaute, au moins le pilote, est avant tout un opérateur de machine. Les tableaux de bord ont grandement évolué. Les écrans ont remplacé beaucoup de boutons poussoirs et beaucoup de manettes. Nous voici donc venu au tout numérique et donc à la gestion de crise cyber.

Je livre ici quelques paroles que j'ai retenues de ce spationaute, concernant la gestion de crise dans l'espace :

- *Le futur est incertain mais il arrive avec des opportunités*
- *Il faut faire preuve d'audace pour progresser,*
- *Il faut innover, mais pas n'importe comment.*
- *Il faut avoir un plan et constamment l'adapter.*
- *Il faut savoir apprendre des erreurs passées pour évoluer*.

Et surtout, il faut atteindre **un niveau de perfection** car les marges d'erreurs acceptables sont très faibles. Avec les entrainements, les spationautes sont conditionnés à attendre la panne qui va forcément arriver, et ils restent zens car ils ont développé une forte capacité à résoudre les problèmes.

Et il est indispensable de travailler en équipes vers un but commun.

Le tableau de bord d'une station orbitale présente de multiples écrans pour un tout numérique.

A la question : L'implantation de l'humanité sur la planète Mars est-elle pour bientôt ? Jean-François Clervoy s'adresse aux jeunes dans l'amphi et leur prédit que dans quelques décennies, quand ils auront atteint l'âge d'être dans un EHPAD, cette conquête pourrait être en effet envisageable.

Un Social Event à l'Abbaye Royale de l'Epau

Il est déjà 18h30 ! Nous n'avons pas vu le temps passer, mais il est l'heure de retourner à nos hôtels. Nous devons être présents à 19h25 pour prendre les bus qui vont nous conduire vers l'**Abbaye Royale de l'Epau** où se tiendra un « Social Event » dont l'APSSIS a le secret. Ne perdons pas de temps, les bus n'attendront pas !

Le bus affecté à l'hôtel Concordia nous fait parcourir les 5 km qui nous séparent de l'Abbaye. Nous y retrouvons les deux monstres sacrés du 11e Congrès du CNSSIS : **Le professeur Robert Erra** et **le spationaute Jean-François Clervoy** sont sur la photo autour de **Vincent Trély** et de **Céline Lagrais**, Directrice Générale de l'EPSM de la Sarthe. Dans une ambiance détendue, les conversations et les questions vont bon train.

Je demande à Robert Erra au sujet de l'écroulement de la fonction d'onde qui s'opère et cause la décorrélation quantique, comment une particule peut savoir que l'expérience est observée, tout en pensant que ma question est un peu idiote ?...

Je demande à Jean-François Clervoy s'il pense qu'un spationaute accepterait de partir au loin, dans l'espace sans espoir de retour sur terre. Jean-François me répond qu'à son avis, c'est « non » pour un spationaute mais qu'on pourrait toujours trouver des humains qui accepteraient.

Bon, on est tellement à l'aise avec ces intervenants que pour un peu, je les tutoierais et les appellerais par leurs prénoms, l'ai-je fait ?

En tout cas, pour répondre à Jean-François qui me demandait quel est cette épinglette que je porte à ma boutonnière et qui est aussi portée par plusieurs des convives, je lui ai expliqué ce qu'est l'**ARCSI** - **A**ssociation des **R**éservistes du **C**hiffre et de la Sécurité de l'Information (www.arcsi.fr).

Le repas est excellent, arrosé et copieux, la nuit sera courte car le Social Event a duré jusqu'à minuit, avec une chanteuse et des musiciens.

Le CNSSIS au troisième jour

La vengeance du panda

Auriane Lemesle ouvre le troisième jour de ce magnifique évènement. Elle accueille sur scène **Philippe Loudenot** de Forecomm.

Philippe Loudenot est cyber stratégist chez **Forecomm** qui commercialise la solution **BlueFiles** de chiffrement de e-mails**.** Il est membre d'honneur de l'APSSIS et membre de l'ARCSI.

Philippe nous révèle un fait peu connu et fort triste : « ***chaque fois que vous envoyez une information sensible, un panda meurt*** ». Comme c'est triste pour cette espèce si sympathique et protégée. Son intervention aura pour titre « **La vengeance du Panda** ».

Depuis des temps immémoriaux, des secrets de fabrication sont dérobés. Déjà, il y a fort longtemps, le secret de la fabrication de la soie avait fuité. Avec les étapes par lesquelles est passée l'humanité : la chasse, puis l'agriculture puis l'industrie et enfin l'établissement du savoir pour tous, quand au début de cette dernière époque, on voulait sauvegarder un secret, on le mettait à la Poste. Aujourd'hui, avec les réseaux, l'Information est devenue un bien à protéger et le vol des secrets a atteint un degré alarmant.

Dans les établissements de santé, personne ne partage la même vision sur les données à protéger que gère un système d'information. Les données s'échangent essentiellement par messagerie, et c'est plutôt le contenant que l'on protège, pas le contenu. **Big Brother** is watching you, et Big Mother aussi : *Donnez, donnez, dooô..ônez, GAFAM vous les prendra*.

Mais en fait, rassurez-vous, en fait le Panda n'est pas mort. Il est bien vivant mais il est furieux de ne pas avoir été protégé durant si longtemps. Philippe Loudenot nous passe une animation qui montre le panda en colère, balayer d'un violent coup de patte la table sur laquelle un utilisateur inconscient échange des informations sensibles. Il fait valser le clavier, la souris, l'écran. Et PAN dans la gueule de l'utilisateur. C'est comme ça que le panda peut survivre. Et pour un système d'Information c'est pareil, il faut le protéger !

Car que penser, dans un Centre Hospitalier d'un dossier de patient qui traine sur un charriot ? De quoi avons-nous besoin pour une réelle protection de l'Information ? :

- de la **D**isponibilité,
- de l'**I**ntégrité,
- de la **C**onfidentialité
- et de la **T**raçabilité

Acronyme : **DICT**

Certifié CSPN par l'ANSSI, le logiciel **BlueFiles**, commercialisé par Forecomm est une solution, très facile à implémenter. Elle permet de réaliser des transferts de messages et de fichiers de manière sécurisée, en appliquant un chiffrement de bout en bout. Et BlueFiles permet aussi de transférer des fichiers beaucoup plus volumineux que ceux permis par les messageries classiques

Cette solution repose sur les quatre « **S** » qui sont les quatre piliers de la cybersécurité,

- **S**écurité
- **S**implicité
- **S**obriété numérique
- **S**ouveraineté

La présentation de Philippe devient très technique, il y est question de règles de contournement.

Pour cette 17ème conférence, la parole est à Palo Alto Networks : « Nécessité d'intégrer l'IA dans la sécurité pour faire face aux menaces cybercriminelles avancées »

Avec **Olivier Kassian**, avant-vente sur le marché de la santé chez Palo Alto Networks.

Tout le monde utilise aujourd'hui l'Intelligence Artificielle, souvent même sans en avoir conscience. L'IA évolutive, comme celle utilisée par l'application ChatGPT ou Bard, devient un phénomène de société. Le premier usage de l'IA évolutive réside dans les moteurs de recherche, mais les cybercriminels en font aussi usage. Avec l'aide d'une application d'IA évolutive, ils créent des maliciels, ce qui n'est pas normalement ce pourquoi l'IA a été développée dès ses origines. Dans le domaine de la santé, le **Machine Learning** (capacité d'apprendre) et le **Deep Learning** (capacité de raisonner) sont indispensables pour renforcer la sécurité et prévenir les attaques.

Le **Deep Learning** qui utilise des réseaux neuronaux pour créer des tables de décisions peut détecter, très rapidement, des attaques avancées et éliminer les faux positifs. Ils sont bien plus efficaces que les anti-virus à base de signatures. Palo Alto injecte chaque jour un volume de 2 Tera-Octets de données dans son Cloud. Ces données alimentent ses programmes de détection de cyberattaques.

Olivier Kassian donne l'exemple de la Kill Chain qui est une méthode de modélisation des intrusions qui menacent les données sur un réseau.

Olfeo présente « la technologie Trust-Centric qui permet de mettre en place un environnement sécurisé de navigation internet »

Avec **Frédéric Napoleone**, directeur commercial d'Olfeo

Olfeo, éditeur français en cybersécurité, présente une solution « **Trust-Centric** » pour écarter les menaces qui pèsent sur la navigation web en bloquant les pages réputées dangereuses. Il crée ainsi un environnement de confiance. Leurs proxies web analysent chaque jour des centaines de milliers de page web. La solution d'Olfeo est proposée en mode « On-premise » ou sur des serveurs en mode SAS, hébergés sur des serveurs en France, dans le cloud souverain d'Orange. Cette solution est accompagnée de formations par l'offre « **Olfeo Awereness** », de e-learning. Il y a, entre autres trainings, une sensibilisation pour savoir ce qu'est le phishing, et s'en méfier.

Parmi ses plus de mille clients qui utilisent sa base de filtrage, Olfeo compte par exemple IBM. Dans le milieu hospitalier, citons parmi ses clients le CHU de Savoie qui utilise actuellement la solution Olfeo en mode « On Premise » et migrera en modèle SAS après avoir structuré ses annuaires.

Les chiffres annoncés par Philippe, donnent le tournis : En 2022, 43 000 attaques ont visé 50% des entreprises françaises. 13 millions de pages web malicieuses sont trouvées chaque mois, soit 400 000 pour une seule journée. Olfeo référence en continu des centaines de millions de pages web soit 99,5 % des requêtes web en entreprise. Les pages trouvées sont réparties en 100 catégories et 9 thèmes.

La stratégie d'Olfeo ne repose pas sur des black lists, méthode qui serait perdue d'avance, mais sur des **white lists** qui sont intégrées dans sa base globale, après un filtrage très fin, et ce toutes les 15 minutes. Les utilisateurs ne peuvent accéder qu'aux URL contenus dans les white lists.

Dans la solution Olfeo utilisée dans les hôpitaux, 20 millions de domaines sont classifiés au moyen de l'IA ou manuellement. L'administration de cette solution pour décider de la base de filtrage est très simple. Le mode SAS est intéressant en particulier si le centre hospitalier n'a pas le personnel nécessaire pour s'en occuper.

Stormshield ou « La Santé à l'heure de la cybersécurité … et l'OT dans tout ça ? »

Avec **Vincent Nicaise**, Industrial Partnership and Ecosystem Manager chez Stormshield

Stormshield est une entreprise française, filiale à 100% d'Airbus Cybersecurity. Elle compte plus de 450 employés.

Ce constructeur et éditeur de logiciel propose une offre de solutions en IT pour sécuriser les systèmes d'information : sécurisation des réseaux avec des appliances, sécurisation des postes de travail avec du chiffrement et analyse des menaces par des sondes de détection d'intrusion). Elle propose également des solutions pour sécuriser les dispositifs OT.

L'OT (Technologie Opérationnelle) est dédiée aux centres hospitaliers car ces centres s'appuient sur de nombreux process industriels (imagerie médicale, dispositifs biomédicaux, gestion du froid…). Tout disfonctionnement des dispositifs OT comme une défaillance de la ventilation, de la distribution d'énergie, des ascenseurs, de la sécurité incendie, et d'autres systèmes critiques, entraine des conséquences catastrophiques.

Il est donc essentiel pour un centre hospitalier d'organiser une gestion des risques métiers dans le domaine industriel et de s'outiller pour les éviter.

Pour sécuriser une infrastructure OT des agressions venant de l'extérieur, Stormshield propose une gamme d'appliances (sécurité tout en un), qui contient un firewall industriel, un proxy VPN IPsec et SSL/TLS, des sondes IDS et IPS entre autres fonctionnalités : la gamme Sni20 (sur l'image) et Sni30 est spécialement dédiée à la sécurisation de l'OT. Ces firewalls peuvent être mis en haute disponibilité avec deux appareils, l'un surveillant l'autre. Les Sni20 et Sni30 sont conçus pour ne pas être affectés par des chocs, des interférences électromagnétiques ou des températures extrêmes.

Un partenariat avec Siemens permet d'augmenter la surface de solutions dédiées à la sécurité dans le domaine hospitalier.

Fortinet et le « chemin de modernisation des infrastructures de cybersécurité dans un établissement support de GHT : retour d'expérience avec le CH de Dunkerque »

Avec **Thomas Briend** ingénieur avant-vente chez Fortinet et **Laurent Basset** – RSSI du Centre Hospitalier de Dunkerque.

C'est une très bonne idée d'associer, dans une conférence du CNSSIS, un fournisseur de solutions et un utilisateur.

Une vulnérabilité a été trouvée, au niveau de l'interface d'administration des produits de Fortinet, et fort honnêtement Thomas Briend s'en excuse.

Je trouve que paradoxalement cette remarque empreinte d'honnêteté renforce au contraire la confiance qu'on peut accorder aux produits et à celui qui les présente. Car quelle application peut se targuer de n'être entachée d'aucune vulnérabilité ? Qui peut prouver que l'ensemble d'un logiciel a été testé par des preuves formelles ? Donc, les premières contre-mesures de Fortinet ont été de restreindre, à des adresses IP de confiance, les accès vers l'interface d'administration. Bien sûr la vulnérabilité a été depuis corrigée. Je préfère entendre cette approche honnête plutôt que d'entendre dire : « *ma solution vous sécurisera à 100%, car avec nous vous n'aurez jamais de problèmes parce que nous sommes les meilleurs* ».

Mais revenons au retour d'expérience du Centre Hospitalier de Dunkerque.

Laurent Basset nous livre un retour d'expérience sur la modernisation des infrastructures de cybersécurité du Groupement Hospitalier des Territoires de cette Région.

En novembre 2020, le Centre Hospitalier de Dunkerque a subi une cyberattaque par un **crypto virus**. Les postes de travail ont été déconnectés. Le personnel de l'hôpital a pris conscience, à cette occasion, du déficit en culture de la sécurité des SI et des pratiques non conformes, en particulier concernant les mots de passe. Ils ont découvert que les règles qui paramétrisent leur politique de sécurité, avec leur firewall de Checkpoint, n'étaient pas à jour. De graves lacunes techniques ont été mises en évidence dans l'administration de leur cybersécurité.

En janvier 2021, ils ont entrepris un audit de sécurité et se sont fixés sur l'offre d'un seul fournisseur : **Fortinet**. Le contrôle des accès à privilèges, les authentifications à doubles facteurs, la sensibilisation du personnel, l'implémentation de cette solution de sécurité ont pris 4 jours.

La journalisation et l'analyse centralisée des logs est faite par **Fort Analyser**. Les règles de filtrage n'ont pas encore été implémentées en totalité.

Les menaces par e-mail comme le phishing, les ransomwares de type Zero-Day et la compromission des e-mails professionnels (BEC) sont sécurisés par la solution **FortiMail**. La messagerie de l'hôpital est sous Lotus et va migrer vers Outlook.

Le FortiClient VPN permet de chiffrer les transactions.

En 2023, ils pensent déployer la solution **Fortinet Secure SD-WAN** qui sécurisera le réseau étendu. Ils ont pris la décision de trouver un prestataire pour installer un **SOC** opéré 24/7 ainsi que des solutions **EDR**. Ils proposeront des exercices de gestion de crises cyber, et se focaliseront sur les couches basses des applications.

En conclusion ont déclaré les intervenants, « *Pour agir il faut savoir ; pour savoir il faut comprendre* ».

Nous sommes bien d'accord !

Il est 13 heures

C'est l'heure du repas. Comme au premier jour lors de l'accueil, des paniers repas nous attendent. Je monte sur les marches de l'entrée du Centre Culturel des Quinconces, et avec d'autres convives, nous discutons et nous nous restaurons.

EGERIE : « SI de santé : Comment superviser leur cybersécurité, assurer la conformité règlementaire et anticiper l'arrivée de NIS2 »

Avec **Arno Lasso**, ingénieur cybersécurité et **Bruno Guilloux** directeur des ventes, tous deux chez Egerie.

Egerie est une entreprise européenne, basée à Toulon, Paris et Londres, qui propose une approche de la cybersécurité par la gestion des risques, et par la conformité règlementaire (RGPD NIS2…). Cette conformité est nécessaire dans l'Union européenne qui est d'ailleurs l'institution qui génère le plus grand nombre de normes dont les autres pays s'inspirent.

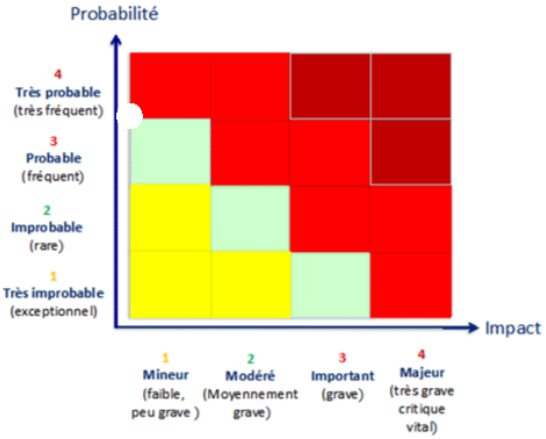
NIS1 ne disparait pas mais **NIS2** le remplace en apportant plus d'éléments. Par exemple, les Opérateurs d'Importance Vitale (OIV) sont remplacés par les entités essentielles (**EE**) et par et les entités importantes (**EI**). La différence est dans la criticité des secteurs associés.

La conformité à la norme rend nécessaire de considérer la conformité aux métiers et faire une analyse de risques.

La plateforme logicielle **EGERIE Risk Manager,** par son moteur d'analyse, **et ses bibliothèques métiers et normatives**, permet de réaliser une cartographie des risques et de les comprendre. Elle alimente l'outil et programme les mesures. Ceci permet de bâtir une vision à long terme pour fournir des éléments à sa Direction. L'outil apporte de nombreuses bases de connaissances sur les menaces, les vulnérabilités et les attaques.

EGERIE Privacy Manager apporte aux DPO une gestion de la conformité de leurs données à caractère personnel avec le RGPD.

Quels sont les principaux risques ? quels sont les cas d'usage couverts en suivant une approche statistique et probabiliste, dans le domaine de la santé ? La matrice avec en abscisse l'impact d'une cyberattaque, en ordonnée la probabilité qu'elle se produise, particularisée à un Centre Hospitalier apporte une aide précieuse pour placer en priorité les bonnes contre-mesures au bon endroit. Et bien sûr ce placement se fera dans une optique métier.



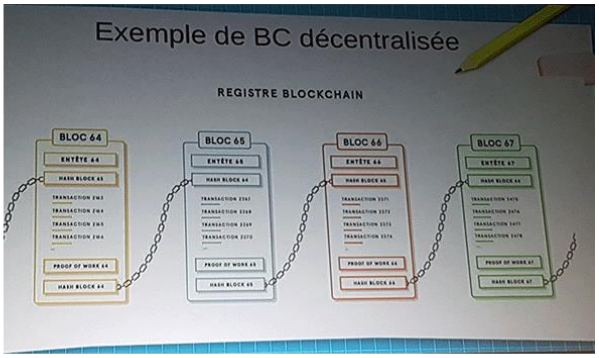
La plateforme logicielle **EGERIE Risk Manager** est labellisée EBIOS Risk Manager par l'ANSSI. EGERIE la propose en mode « On-premise » ou dans un Cloud. Elle fournit une vision globale

et centralisée des risques cyber au moyen d'une cartographie. Elle permet de mettre en pratique une stratégie de cybersécurité dans un centre hospitalier et d'assurer la résilience du Système d'Information. EGERIE Risk Manager permet aussi d'assurer la conformité avec les normes comme l'ISO 27001, l'ISO 27002 et l'ISO27005 RM (Risk Manager).

Conférence 22 : « Blockchain en santé : regards croisés juridiques et techniques »

Avec **Maître Marguerite Brac de la Perrière**, avocate, pour le côté juridique

… et l'incontournable **Cédric Cartau** pour le côté technique.



Encore un grand moment qui s'annonce, et sur un sujet d'avenir : Les blockchains !

Pour nous placer dans l'ambiance, Cédric annonce que le volet technique des blockchains est encore en friche et Marguerite annonce que le volet juridique n'est ni stabilisé, ni débroussaillé. La technique doit s'adapter aux besoins, mais côté juridique cela pose un problème car, techniquement, la durée de conservation du contenu des éléments dans une blockchain, ne peut être limitée. Une blockchain conserve en effet toutes les transactions qui ont été rentrées depuis son début. Mais côté juridique, il peut être exigé de ne pas dépasser une limite maximale de conservation des documents.

Cédric définit une blockchain : C'est un ensemble de blocs chainés. Chaque bloc est signé et contient le condensat (on dit communément le hash ou l'empreinte) du bloc précédant. Pas possible de corrompre une blockchain car le chaînage imposerait de le faire pour tous les blocs à partir de celui qui a été corrompu.

De plus, les blockchains sont réparties sur plusieurs nœuds qui peuvent résider dans de multiples endroits. Pas possible de corrompre une blockchain car il faudrait corrompre toutes

ses occurrences. Il y a donc, par ces propriétés, l'assurance de l'intégrité de chaque bloc et l'intangibilité de l'ensemble de la blockchain.

Mais les blockchains ont des variantes qui modulent ce qui a été dit. Il existe des blockchains sans permissions, décentralisées comme celle du bitcoin et d'ethereum qui obéissent au modèle de base où tout le monde peut proposer une transaction, et les blockchains avec permissions qui, elles, sont privées.

Qui peut rentrer un nouveau bloc dans une blockchain ? Deux technologies sont possibles : La PoW ou preuve de travail : Des mineurs doivent résoudre un problème mathématique très coûteux en ressources de calcul et aussi donc en consommation d'électricité. C'est sur ce type de blockchain qu'est construit le bitcoin. Il y a la PoS ou preuve d'enjeu où il faut prouver qu'on possède une certaine somme en jetons, et qu'on a gardé cette somme un certain temps. C'est sur ce type de blockchain que Ethereum, qui permet de conserver des contrats intelligents, a migré récemment.

La technologie des blockchains est complexe, et il est préférable de la comprendre. Pour conduire une voiture, point n'est besoin de savoir comment fonctionne le moteur. Pour utiliser les bitcoins, il est préférable de savoir comment fonctionne sa blockchain.

Faut-il investir dans des cryptomonnaies ? Tel est le dilemme : Préfèrerait-on confier sa fortune à la banque du Far West ou placer ses lingots d'or dans son grenier ?

Parmi les problèmes posés par le bitcoin, il y a, nous l'avons écrit, la consommation d'électricité mais aussi la vulnérabilité dite de « l'attaque des 51 % ». Si au moins 51% du nombre des mineurs s'associent, ils peuvent créer une dérivation (un fork) de la blockchain et on se retrouve avec deux blockchains parallèles. Ajouté à cela, il y a la menace que fait peser le quantique sur la solidité du chiffrement basé sur les courbes elliptiques car les calculateurs quantiques du futur, par leur rapidité, permettront de résoudre, dans un temps acceptable, le difficile problème du décryptement.

Côté juridique, 8 sociétés détiendraient 80% de la capacité de minage. Il y a là un risque légal pour lequel on ne trouve que peu de jurisprudence. Et qui est responsable des traitements ? Est-ce le mineur qui exécute les demandes de ses clients ou est-ce les clients qui ont confié aux mineurs le soin de rentrer leur transaction dans une blockchain ?

Pourquoi ne pas se contenter d'un EDR ?

Avec **Charles Blanc-Rolin,** Chef de projet sécurité numérique en santé - GCS e-santé Pays de la Loire et VP de l'APSSIS.

Une technique d'attaque consiste à utiliser un driver vulnérable pour obtenir des privilèges administrateur et arrêter, par exemple avec le rançongiciel BlackCat, des processus pourtant protégés tels que les antivirus, l'EDR et le XDR. Aussi, dans les nouvelles versions professionnelles de **OneNote**, programme informatique de prise de notes intégré à la suite Office, Microsoft bloque par défaut les macros VBA qui faisaient le bonheur des attaquants.

Charles Blanc-Rolin, VP, fait remarquer que quand Microsoft ferme la fenêtre, les attaquants passent par la porte Il nous fait une démo de contournement d'un EDR.

Mais j'ai une contrainte d'horaire. Je dois être à Paris avant le soir, aussi je m'éclipse de l'amphi. J'ai aussi donc raté aussi la dernière intervention où il était question du métier de RSSI dans le domaine de la santé, mais avec le replay qui sera disponible, je n'aurai pas tout manqué.

Le rideau tombe sur ce 11ème CNSSIS

Nos charmantes hôtesses et organisatrices nous disent au revoir !

Il est remis à tous les congressistes un « panier Sarthois » avec un pot de rillettes du Mans, une boîte de biscuits et une bouteille de vin.

Sur la route du retour à la gare du Mans, je rencontre, assis sur le trottoir, un chapeau posé devant lui, un vieux monsieur qui semble être dans la nécessité. Je prends dans mon panier Sarthois mon pot de rillettes et le lui donne. Il me remercie chaleureusement et me dit qu'il adore les rillettes.

Encore une bonne action qu'on peut attribuer au CNSSIS !