LES SALONS HOCHE PARIS

Compte-rendu

1ères Rencontres SSI Santé

APSSIS

Non loin de l'Arc de triomphe de l'Etoile provisoirement empaqueté et du romantique Parc Monceau, le **jeudi 23 septembre 2021** à Paris, dans les prestigieux Salons Hoche, l'APSSIS a tenu les **1ères Rencontres SSI Santé**.

Organisé par le président de l'APSSIS, Vincent Trély et son équipe, animé par le cardiologue Fabien Guez, cet évènement a réuni une centaine de participants venus de plusieurs Régions de France, avec lesquels des intervenants de très haut niveau (experts cybersécurité, directeurs d'hôpitaux, juristes, industriels…) ont apporté des connaissances précieuses lors de conférences, d'ateliers-débats et d'échanges informels.

Entre un buffet déjeunatoire, dès midi, et un excellent dîner qui s'est terminé tard dans la nuit, tout ce petit monde des professionnels de la Sécurité des SI de Santé a vécu de grands moments et connu des retrouvailles ou fait des connaissances fort utiles. Les confrontations d'expériences vécues, en cette actualité trouble où les cyberattaques contre les établissements hospitaliers se multiplient, où les infrastructures hospitalières sont rendues inopérantes par des cryptovirus, où des informations sensibles fuitent et sont commercialisées sur les marchés noirs de la cybercriminalité, ont nourri des réflexions fort intéressantes sur le secteur si menacé de la santé.

Que dire de tous les évènements vécus dans cet évènement comme, pour ne citer que celle-là, juste avant le dîner, la prestation du docteur Laurent Alexandre sur la sécurité de l'information dans le domaine de la santé à l'horizon 2030 ? Et bien justement, disons-le, entrons dans les détails de mon vécu.

Le buffet déjeunatoire et l'ouverture des Rencontres SSI Santé

Dès midi, poings contre poings ou coudes à coudes chaleureux, plutôt que serrements de mains un peu oubliés, situation sanitaire oblige, mais avec le sourire et la joie des retrouvailles, on se reconnait et on se dit ce qu'on est devenu quand on ne s'est pas vus depuis longtemps.

On récupère son badge auprès de Marie-Valentine, secrétaire de l'APSSIS. Puis on se restaure, autour d'un plantureux buffet. On prend place au premier étage des Salons Hoche pour une demi-journée riche en connaissances partagées.

Devant un amphi plein, **Vincent Trély** ouvre les **1ères Rencontres SSI Santé** en présentant l'agenda. Il introduit l'animateur de la journée, le docteur **Fabien Guez**, cardiologue et journaliste, animateur de l'émission Check Up Santé chez BFM. Le docteur Fabien Guez aura la délicate mission de synchroniser les interventions, d'être le maître du temps pour éviter les débordements, chaque intervenant ayant tant à dire, nous le constaterons.

IMPERVA : « Une réponse aux problématiques de la sécurité des SI Hospitaliers »

Imperva est une entreprise californienne de 1200 employés dans le monde, dont 9 en France. Elle est bien positionnée dans le Magic Quadrant du Gartner, pour la protection des applications Web et des API. Gerald Delplace, Area Vice-Président et Nicolas Dremond, expert cybersécurité d'Imperva positionnent leur entreprise comme un leader sur le WAP (Wireless Application Protocol).

En diminuant la complexité du numérique par la fragmentation des services, Imperva permet à ses 6200 clients de « faire plus avec moins ».

Leurs solutions protègent les applications et les API dans le cloud. Leur credo est « Sécuriser toutes les couches de la périphérie à l›application en passant par la base de données avec une plate-forme de sécurité unifiée ». Dans le jeu du chat et de la souris avec les cybercriminels, leurs clients peuvent ainsi prendre un temps d'avance.

FORTINET : Sécurité et transformation numérique dans le secteur de la santé

Christophe Auberger, Evangéliste cybersécurité et CTO de Fortinet France, pense qu'il est difficile de différencier l'extérieur de l'intérieur d'un Intranet, et qu'il n'existe plus de zones de confiance dans le numérique. L'utilisateur, premier pare-feu de l'entreprise, est soumis constamment aux attaques en ingénierie sociale. Avec le télétravail, avec les objets connectés, 9,1 milliards d'objets connectés dans le milieu industriel en 2022 nous précise le Gartner, et ceux-ci sont loin d'être « secure by design », avec les réglementations toujours plus drastiques, et face aux cyberattaques très sophistiquées, les organisations sont contraintes d'accélérer leurs offres dans l'innovation numérique mais cela augmente aussi la surface d'attaque et les cyber risques auxquels les entreprises sont soumises.

Face à une demande de rançon par suite d'une attaque de cryptovirus, 26% des entreprises aujourd'hui payent en espérant récupérer la clé de déchiffrement auprès des cybercriminels. Avec 5,6 milliards de comptes e-mail actifs dans le monde, et 320 milliards de mails envoyés quotidiennement, d'après le Gartner, la messagerie est l'application la plus menacée et les organisations utilisent de plus en plus une messagerie hébergée dans le Cloud. « Si vous ne voyez pas un équipement, vous ne pouvez pas le contrôler » nous dit Christophe Auberger.

La solution SD-WAN - réseau étendu défini par logiciel - proposée par Fortinet est présentée comme un rapprochement entre le réseau et la cybersécurité et va vers le modèle SASE – Secure Access Service Edge - qui place les dispositifs de contrôle du réseau à la périphérie du cloud et non dans le datacenter, ou à l'extérieur de l'entreprise. Avec le Zero-trust, le cloud ainsi sécurisé représente très certainement le futur de l'utilisation du numérique pour apporter plus de confiance sur son Information.

Pause-café

Que dis-je pause-café ? Pas seulement café, il y avait des pâtisseries à foison, des boissons et beaucoup d'occasions de revoir, de voir et connaître des personnes qui comptent dans l'écosystème de la sécurité des données de santé.

Mais… n'est-ce pas Cédric Cartau, RSSI du CHU de Nantes assis en train de discuter, saisi sur la photo de droite par l'œil de mon smartphone ? Le fameux Cédric qui écrit dans la revue DSIH des articles si intéressants sur le fond et si agréables à lire sur la forme ? Voir en : https://www.dsih.fr/tribunes/. Oui c'est bien lui ! Quelle chance de le retrouver à Paris ! De dos sur la photo, la directrice du CHU de Poitiers, Anne Costa, qui interviendra à la table ronde des directeurs d'hôpitaux et au fond, en partie cachée, se passant la main sur les cheveux, Auriane Lemesle qui sera, avec Philippe Roussel, animatrice de cette table ronde. Une occasion rêvée d'entrer dans cette conversation informelle, dans ce couloir où je les ai trouvés, près de la pause-café !

Et durant cette pause, Marie-Valentine, secrétaire de l'APSSIS m'a suggéré, en aparté, d'écrire un compte-rendu de cet évènement. En serais-je capable ?

Ô Dieu l'étrange peine ! : L'heure du choix cornélien

Deux ateliers nous sont proposés en parallèle. L'un animé par **ROHDE & SCHWARZ** sur le thème « Une réponse souveraine sur mesure aux enjeux et menaces dans la Santé » (voir encadré) , l'autre animé par **Proofpoint** où il est question du facteur humain. La duplication et l'intrication quantiques n'existant aujourd'hui que dans le domaine de l'infiniment petit, il m'a bien fallu choisir.

J'ai opté pour l'atelier de Proofpoint, qui

compte 70 collaborateurs en France, avec Loïc Guézo - au micro, sur la photo - directeur, stratégie cybersécurité, Europe du Sud et Laurent Bourgeois - responsable commercial, secteur santé de Proofpoint, sur le thème « Attaques cyber en Santé – Le facteur humain ».

Loïc Guézo est un copain de l'ARCSI (Association des Réservistes du Chiffre et de la Sécurité de l'Information). Il portait à la boutonnière la même épinglette que moi, épinglette aux deux clés entrecroisées devant une grille et un bouclier, que portait aussi Vincent Trély et plusieurs autres convives. Et puis le « PFH », expression du Québec qui se traduit par le « Putain de Facteur Humain », ce danger qui se situe entre la chaise et le clavier, c'est bien par cette menace qu'il faut commencer à trouver une solution pour diminuer le risque qui pèse sur les données numériques. Sinon quoiqu'on fasse, quelles que soient les contre-mesures mises en place, quel que soit l'investissement consenti pour sécuriser l'Information d'un établissement hospitalier, celle-ci peut se retrouver dans un état critique, voire pire, avoir disparu, ou pire encore, être compromise dans son intégrité. D'où bien sûr la nécessité impérieuse d'évangéliser tous les employés, de sensibiliser le plus grand nombre, et de former pour quelques-uns sur les aspects techniques et non techniques de la cybersécurité.

Le CERT Santé confirme que la menace s'est grandement amplifiée en 2021. Déjà l'an dernier, 250 établissements hospitaliers ont déclaré 360 incidents de sécurité dont 43% de ransomwares, 35% de tentatives de Phishing, et 42% de tentatives d'exploitation d'une vulnérabilité. Les informations les plus ciblées sont celles à caractère personnel des patients. Les cybercriminels ne tentent plus trop de pirater les systèmes d'Information de l'extérieur, ils se connectent directement là où les informations sensibles se trouvent. Les infrastructures numériques basculent dans le Cloud, mais les cyber attaquants aussi.

D'après une enquête menée par Verizon sur la compromission des données médicales, 85% d'entre elles sont dues au fameux facteur humain, et seulement 3% à l'exploitation de vulnérabilités techniques. Les outils anti-phishing sont pris de court par l'imagination débordante des cybercriminels. Par exemple un mail peut contenir une pièce jointe chiffrée, donc l'outil anti-phishing ne peut analyser son contenu à l'entrée du système d'Information, et dans le mail on trouve la convention secrète pour déchiffrer le fichier attaché. Le ver entre alors dans le fruit. Autre variante, le fichier attaché est piégé et la convention secrète est envoyée dans un deuxième temps, dans un autre mail. Comment faire la relation entre les deux messages ? Pas facile !

Le BEC - Business Email Compromise – ou Compromission de la messagerie en entreprise, a rapporté aux cybercriminels 4,2 milliards de dollars, selon les chiffres du FBI de 2020.

Vincent Trély intervient pour donner son avis sur les boîtes mails par qui, aujourd'hui trop souvent les compromissions commencent : Les boîtes mails sont faites pour envoyer des messages, pas pour les archiver. Il serait salutaire de se fixer un quota de mails et de ne pas garder l'excédent. A méditer…

Le niveau de stress des RSSI augmente avec la pression quotidienne dont ils font l'objet et la compréhension et le support jugés insuffisants de leur Direction Générale. Ce qui est un bon passage de relai pour la table ronde qui suit.

ROHDE&SCHWARZ

Retour sur l'atelier Rohde & Schwarz Cybersecurity :

« Une réponse souveraine sur mesure aux enjeux et menaces dans la Santé »

Rohde & Schwarz Cybersecurity a présenté sa solution de sécurité applicative en rappelant les enjeux spécifiques au secteur de la santé. En particulier, une forte actualité règlementaire s'est fait connaître ces 2 dernières années.

La conférence a été co-animée avec Fabien Malbranque, Fonctionnaire de Sécurité des Systèmes d'Information

Adjoint aux Ministères chargés des affaires sociales.

Hélène Selosse a présenté comment les solutions de Web Application Firewall de Rohde & Schwarz Cybersecurity apportent une réponse aux enjeux, tant de protection des Attaques Top10 Owasp, que 0 day, tout en garantissant une totale conformité RGPD.

La présentation d'une référence majeure de la santé liée à l'Espace numérique de Santé a permis d'aborder les enjeux fonctionnels et techniques du secteur, dans lequel Rohde & Schwarz Cybersecurity est très présent auprès des organisations publiques de santé.

La conférence a été suivie d'un témoignage de Philippe Loudenot, qui a confirmé la performance des solutions Rohde & Schwarz Cybersecurity et mis en avant l'importance du caractère souverain des solutions, au regard des enjeux du secteur.

Une intervention de Jean-François Parguet, FSSI des Ministères sociaux a ensuite confirmé la position sur l'importance d'une solution apportant la compliance RGPD dans un secteur très exposé.

Par la suite, une démonstration de la solution a été réalisé par Valentin Artaud.

Une conclusion a été présentée à Christine Amory en rappelant que Rohde & Schwarz Cybersecurity est un acteur incontournable sur la sécurité applicative dans le secteur de la santé, en citant plusieurs références majeures du secteur.

La table ronde des directeurs généraux d'hôpitaux s'installe

Il est 17 h 00. La table ronde est animée par Philippe Roussel - Directeur d'hôpital, à gauche sur la photo et par Auriane Lemesle - RSSI du GCS e-santé des Pays de la Loire à droite.

Répondent aux questions de Philippe et d'Auriane, de gauche à droite :

- Anne Costa, Directrice Générale du CHU de Poitiers
- Jacques Léglise - Directeur Général de l'hôpital Foch à Suresnes
- et Yann Bubien - Directeur Général du CHU de Bordeaux

Question d'Auriane Lemesle : « Comment voyez-vous l'évolution de la cybersécurité ? Ce sujet vous semble-t-il important ? ».

Anne Costa (Poitiers) répond qu'il y a 10 ans, le CHU de Poitiers n'avait pas de RSSI. Aujourd'hui la politique du CHU va surtout dans la sensibilisation des employés, en particulier dans l'utilisation de la messagerie.

Pour Yann Bubien (Bordeaux) la perception de la sécurité de l'Information a bien changé. Avec l'emploi de hackers éthiques, le CHU de Bordeaux passe du curatif au préventif, ce qui implique de nouvelles méthodes de travail. La prise de conscience s'est faite surtout suite à l'électrochoc causé par la cyberattaque qui avait entrainé la paralysie du CHU de Rouen. Aujourd'hui

Yann Bubien porte une attention forte aux actions du RSSI et du DSI.

Question d'Auriane Lemesle : « Comment êtes-vous informés des cyberattaques sur les centres hospitaliers et quelles sont vos réactions ? »

Jacques Léglise (hôpital Foch) répond qu'il a aussi pris conscience de la gravité de la situation quand il a appris ce qui était arrivé au CHU de Rouen. Sa réaction est de croire maintenant que la question n'est plus « si » mais « quand » le système d'Information de l'hôpital subira une attaque.

Question de Philippe Roussel : « Avez-vous tous agi pour placer la cybersécurité à son juste niveau ? Comment vous vous organisez avec votre RSSI ? »

Jacques Léglise (Foch) précise qu'ils ont un RSSI à temps plein et qu'il y a aussi une deuxième personne importante : le DPO. Le RSSI et le DPO se rencontrent au moins une fois tous les quinze jours. Ils ne doivent pas être perçus comme des empêcheurs de tourner en rond, mais comme facilitateurs du travail de tous et garants de la sécurité de l'Information et de sa conformité aux règlements.

Yann Bubien (Bordeaux) indique que, chez eux, le RSSI est indépendant de la DSI et dépend de la direction de la qualité. Il est nécessaire de mener une politique d'établissement sur la cybersécurité, claire et déterminée, en mettant le RSSI dans le comité de pilotage, sinon avec leurs 15 000 employés, ils n'y arriveront pas. Eux ont été surtout secoués par la cyberattaque sur l'hôpital de DAX.

Anne Costa (Poitiers) précise que son RSSI lui est directement rattaché et dépend aussi en partie de la direction qualité.

Question de Philippe Roussel : « La cybersécurité est un sujet assez technique. Si vous n'avez pas les ressources suffisantes en interne, avez-vous pensé à l'externalisation ? »

Pour Yann Bubien (Bordeaux), il ne faut pas externaliser la sécurité. Une politique de cybersécurité doit s'intégrer dans celle de la sécurité et de la sûreté de l'établissement. Les métiers de la cybersécurité sont très recherchés. Ce sont des métiers nouveaux qui exigent de fortes compétences techniques et non techniques, qui impliquent une recherche constante de l'innovation. Ces compétences sont rares sur le marché de l'emploi. Le Président de la République a fait une annonce très forte et très attendue sur le fait qu'il faut augmenter la compétence en cybersécurité dans le domaine de la santé, et bien sûr le budget associé.

Pour Anne Costa (Poitiers), le RSSI doit être gardé en interne car il a aussi un rôle important pour sensibiliser tous les employés. Pour bien jouer son rôle, il doit faire preuve de qualités techniques mais aussi relationnelles et humaines.

Pour Jacques Léglise (Foch), il ne faut pas externaliser la cybersécurité, mais si les grands centres hospitaliers peuvent avoir des personnes compétentes en cybersécurité en interne, il ne faut pas oublier que les centres hospitaliers de petite taille, faute de budget, ont du mal à s'attacher ces compétences rares et chères.

Les grands hôpitaux doivent apprendre à employer efficacement leurs ressources disponibles compte tenu que les circuits ne seront pas rapidement changés. L'hôpital travaille aussi avec de nombreux prestataires qui observent une charte de sécurité interne, et l'accès aux services n'est distribué qu'avec parcimonie.

L'annonce du Président de la République pourra permettre d'accélérer les changements espérés en augmentant les capacités de financement dans le domaine de la Santé. Nous sommes au cœur d'une guerre économique mondiale et plus un Etat est jugé fragile, plus la probabilité d'être attaqué est forte.

Question d'Auriane Lemesle : « Comment se préparer à être confrontés à une cyberattaque ? »

Anne Costa (Poitiers) répond qu'ils ont organisé une simulation d'attaque impliquant le COMDIR.

Jacques Léglise (Foch) a également procédé à un exercice simulé de cyberattaque qui envoyait de multiples messages avertissant qu'ils entraient dans une période de crise très grave. Cette attaque visait plus l'organisationnel que la technique. Le but était de tester les réactions de chacun plus que de tester la qualité des outils. Il envisage de mener une telle simulation d'attaque sur une base annuelle.

Yann Bubien (Bordeaux) précise que chez eux, ils ont la culture des attaques d'origine bactériologique mais n'ont pas encore mené des attaques simulées sur le numérique.

Pour terminer la table ronde avant de passer aux questions, Auriane Lemesle demande aux intervenants de donner **un conseil très simple pour renforcer la communication sur la cybersécurité dans le milieu de la santé.**

Jacques Léglise (Foch) répond : sujet, verbe, complément. Restons simples et faisons des choses raisonnables en restant pragmatiques.

Yann Bubien (Bordeaux) souhaite que ceux qui ont un problème viennent le voir directement plutôt que de le contacter et lui expliquer le problème par mail.

Et viennent les questions et remarques éventuelles de la salle pour les quelques minutes restantes, afin de respecter l'horaire.

Philippe Loudenot, grand expert en cybersécurité (et membre de l'ARCSI), délégué cybersécurité du Conseil général des Pays de la Loire, dit qu'il n'a pas vraiment perçu la logistique des relations entre le RSSI et la direction d'un hôpital dans cette table ronde. Le rôle d'un RSSI est de donner des gages sur la protection des données et des systèmes d'Information, le rôle d'un directeur d'hôpital est de prendre des décisions et de les faire appliquer. Il est pour cela impératif que le directeur sache au moins parler au RSSI, comprenne son vocabulaire et son métier.

Cédric Cartau, autre grand expert cybersécurité (et aussi autre membre de l'ARCSI), RSSI du CHU de Nantes, précise que si la cyberattaque en rançongiciel au CHU de Rouen a causé un électrochoc, car c'était la première attaque très médiatisée, celle sur l'hôpital de Dax a eu des conséquences bien plus graves, qui sont encore loin d'être terminées aujourd'hui.

Je me suis permis de poser une question, puisque Vincent Trély passait près de moi avec le micro : « un expert cybersécurité, qui n'a pas travaillé dans la santé mais dans le renseignement puis dans une ESN, a dit, au cours d'un évènement très récent, que si l'attitude des établissements de santé devait être caractérisée par un seul mot, ce serait la « cyber ignorance ». Que lui auriez-vous répondu ?

Je crains avoir jeté comme un petit froid par ma question certes un peu agressive, et les intervenants se sont regardés pour savoir qui serait l'autre qui prendrait la parole. Jacques Léglise (Foch) a répondu qu'il n'était en gros plutôt pas trop en désaccord avec ce qu'avait dit l'expert.

Et trois conférences-débats en Espagnol et en Anglais, traduites et accessibles par écouteurs, suivent.

Lionel Prades, responsable des risques numériques chez Sham, du groupe Relyens, à gauche sur la photo, anime ces trois interventions. Il interroge en présentiel l'espagnol Miguel Angel BENITO TOVAR, CISO et DPO des Iles Baléares puis, en distanciel, un autre espagnol Marcos GOMEZ HIDALGO, sous-directeur de INCIBE-CERT sur le sujet « **L'organisation de la SSI à l'échelle régionale et les évolutions du cadre de SSI national en Espagne** ».

Miguel Angel est aussi membre de la Société Espagnole d'Informatique de la Santé (Sociedad Española de Informática de la Salud, aka SEIS), et coordinateur de son Comité Sécurité. Les objectifs de la SEIS pour la cybersécurité, en tant que Société Scientifique, sont similaires à ceux de l'APSSIS en France. La SEIS coordonne les CISO du secteur Santé en Espagne et collabore avec les Administrations Publiques pour les développements de projets numériques de Santé.

Miguel Angel suit en particulier de près les travaux des Opérateurs de Services Essentiels et les évolutions de la deuxième version de la directive NIS.

Marcos présentait la situation cyber du secteur santé privé en Espagne et le travail de support de l'INCIBE pour la promotion et la coordination de la cybersécurité en particulier grâce aux services et formations fournis par son CERT.

La cybersécurité dans le domaine de la santé est gérée en Espagne suivant un modèle décentralisé auprès de 17 communautés autonomes, dont celle des Îles Baléares.

Plusieurs organismes coopèrent entre eux au niveau national et avec d'autres pays avec pour but principal d'améliorer la sécurité et la résilience des systèmes de santé du pays. Ils participent ensemble à la Stratégie Nationale de Cybersécurité sous la coordination du Conseil de la Santé Numérique (CSDE , sous la Tutelle du Ministère) :

L'INCIBE (Instituto Nacional de

Ciberseguridad) soutient les organisations privées en matière de sécurité de l'Information, le CCN-CERT (Centre Cryptographique National) gère les organisations publiques, l'AEPD (Agence Espagnole de Protection des Données) a une action équivalente à la CNIL.
En Espagne aussi, la situation de crise causée par la COVID a entraîné la mise en œuvre d'un grand plan de renforcement des capacités de cybersécurité.

Lionel Prades donne ensuite la parole, en distanciel et en anglais, à Amir Magner, diplômé du Technion, qui a fait carrière au bureau du Premier ministre Israélien, avant de créer et présider la société CyberMDX, appartenant maintenant au groupe Relyens. CyberMDX se positionne en pionnier de la cyber intelligence et de la sécurité des objets connectés dans le domaine de la santé. La devise de CyberMDX est : *« Nous protégeons les objets qui protègent les vies humaines ».*

CyberMDX travaille avec le groupe Sham d'assurance cyber pour créer une solution de gestion des risques complète, pour les soins dans le domaine de la Santé. Amir Magner intervient sur le sujet « Prospective de l'exposition à la menace sur les hôpitaux ». Les défis relevés sont principalement la sécurité des patients, la sécurité des dispositifs médicaux et la prévoyance des cyber menaces. Il identifie le maillon faible au niveau des objets connectés pour lesquels les vulnérabilités connues ne sont pas souvent corrigées, et les contrôles restent très basiques, ce qui pose un grave problème, en particulier dans le domaine de la Santé.

Amir Magner nous donne sept recommandations : Cartographier les informations pour savoir où se trouvent les gisements de données sensibles à protéger, suivre des règles d'hygiène informatique pour diminuer les risques de pénétration dans les systèmes d'Information, protéger les ressources critiques, limiter les mouvements latéraux des maliciels dans les réseaux des entreprises, sauvegarder les données, détecter les attaques le plus en amont possible et sensibiliser et former les utilisateurs.

Et voici la dernière et lumineuse intervention de la journée avant le cocktail et le dîner. Laurent Alexandre nous parle de cybersécurité à l'horizon 2030 : vision et prospective.

Le docteur Laurent Alexandre, chirurgien-urologue et neurobiologiste, fondateur de Doctissimo.fr monte sur scène, sous les applaudissements.

« Nous sommes en guerre », commence-t-il. Nous sommes au cœur d'une cyberguerre géopolitique et des officiers de cette cyberguerre, sont dans cette salle. Avec les GAFAM dont la présence est plus forte que celle des opérateurs hospitaliers, il faut reconnaitre que c'est devenu un joyeux bordel. L'hôpital est une des industries les moins qualifiée dans le domaine de la sécurité de l'Information et l'écart entre ceux qui sont très qualifiés et ceux qui ne le sont pas est énorme. Dans les centres hospitaliers, les enjeux seront multiples. Nous faisons face à des géants puissants et sommes confrontés à une menace mondialisée et multiple. Ces menaces prévisibles, nous ne pouvions même pas les imaginer il y a dix ans. Le cyber piratage va se développer dans des proportions inimaginables et nous restons en plein dans le brouillard.

« Nous sommes en guerre »

Une veille technologique est indispensable pour appréhender l'évolution de ces menaces.

Dans les dix années qui viennent, nous connaîtrons un changement radical dans le métier de la cybersécurité où on prendra de plus en plus de pouvoir. Quand pourrons-nous compter sur une IA forte à laquelle nous ne sommes pas préparés aujourd'hui ? Entre 2029 et 2200 annoncent les prévisionnistes. L'IA faible, ce sont de gros transferts de données par les process afin de les corréler et les analyser. Les réseaux de neurones, bases du Deep Learning, même s'ils atteignent 10 000 couches, ne sont pas explicables. Nous faisons

ainsi face à une Black Box et les médecins ne sont pas capables de rattraper les conneries engendrées par l'IA. Dans les années qui viennent, les infrastructures informatiques sauront faire ce que les médecins ne sauront pas faire.

Le darknet est un endroit privilégié pour s'équiper et attaquer les infrastructures numériques. Le Phishing se fera sur mesure en comprenant la psychologie des victimes, pour activer le chantage. Faire chanter le patron ? il suffit de récupérer les éléments compromettants à partir du cyberespace. Laurent Alexandre cite les Chinois qui ont récupéré, directement sur l'iPhone du patron d'AWS, des photos compromettantes sur ses relations avec sa maîtresse pour le faire chanter en le menaçant de tout révéler à son épouse.

Nos libertés régressent de même que régresse notre souveraineté technologique. L'Europe devient une colonie numérique des GAFAM. Aujourd'hui 68% des jeunes français ont plus confiance en Google qu'en les informations officielles de la France. Comment garder les meilleures compétences attirées par les sirènes des monopoles étrangers ? Le budget de recherche d'Amazon est de 40 milliards de dollars, ce qui représente 5 fois le budget du CNRS et deux fois celui de la Recherche en France. En 2035 il y aura une pénurie de 85 millions d'employés ultra qualifiés dans l'industrie du numérique, et nos données seront toutes hébergées dans des entreprises telles que Google et Amazon. Evidemment une solution serait de démanteler les GAFAM, mais les Etats Unis ne le permettraient pas.

Les vrais acteurs du futur dans le domaine de la santé ne seront plus les médecins mais ceux qui gèrent l'IT. En 2040, une dizaine de cyber groupes géants comme les GAFAMI et les BATX aujourd'hui, se partageront le marché, et cela implique, pour les hôpitaux, pour y faire face, de mutualiser leurs efforts. Les malades seront assimilés à des data, et les docteurs à des logiciels. La volumétrie générée par la médecine ne pourra être exploitée que par l'IT. Le médecin sera alors pour un tiers un infirmier, pour un tiers un technicien et pour le tiers restant une assistante sociale. La cybercriminalité, en faussant les images médicales et les diagnostiques permettra de tuer autant de patients qu'elle voudra.

Le cerveau humain est bon quand il a peu de données à analyser, mais il est inopérant quand les données sont nombreuses. Il faut fuir le big data et s'intéresser à la Neurologie. La neuro sécurité sera de mise.
Laurent Alexandre nous donne trois conseils pour un avenir meilleur dans le milieu médical :

1. Restons groupés
2. Partageons nos expertises
3. Fuyons le big data

Cette décennie verra une augmentation drastique des écarts sur les revenus dans le domaine de la santé. Laurent Alexandre prédit qu'en 2030, les experts cybersécurité dans le domaine de la santé seront au top des compétences recherchées, et au centre des établissements hospitaliers, avec un salaire annuel entre 500k€ et 1 m€ par an, pour les meilleurs d'entre eux.

Sur ces paroles qui remuent, Fabien Guez, animateur de cette demi-journée conclut l'évènement.

Cette mystérieuse glace bleu clair au goût si particulier

Et tout a fini autour d'un banquet, par un excellent repas servi dans le salon Vendôme. Vincent Trély remercie les sponsors de cet évènement : IMPERVA, FORTINET, PROOFPOINT, ROHDE & SCHWARZ et RELYENS.

J'étais assis à une table avec Cédric Cartau, RSSI du CHU de Nantes à ma gauche et Michel Dubois, directeur scientifique et technique du Groupe La Poste, et ancien colonel du service de santé des armées à ma droite (deux ARCSIstes). A cette table étaient également assis Vincent Trély, Auriane Lemesle, RSSI du GCS e-santé des Pays de la Loire, Philippe Loudenot, délégué cybersécurité du Conseil général des Pays de la Loire, maître Omar Yahia, avocat au barreau de Paris, spécialisé dans le domaine de la santé. Je ne vais pas les citer tous, mais, avec tous, nous avons poursuivi des échanges très intéressants autour d'un excellent repas.

Voici Vincent Trély assis, à gauche, qui cause avec Philippe Loudenot debout, et Michel Dubois au premier plan. Tout étant intéressant dans cette soirée, je me suis permis de prêter l'oreille et même de participer à la conversation. Quel merveilleux endroit pour les échanges informels !

Après les entrées et le plat, excellent et arrosés d'un très bon Bordeaux, vint le dessert : Une pâtisserie servie avec une mystérieuse glace bleu clair au goût particulier mais très agréable. Ce n'était pas un parfum connu, en tout cas par ceux autour de moi. Michel Dubois a suggéré que ce devait être une glace à la fleur. Cédric Cartau s'est rangé à cette idée, moi j'ai pensé que si fleur il y avait, ce ne devait pas être une glace à la violette. Vincent Trély nous a abandonné quelques minutes et nous est revenu triomphant. Comme d'habitude, il avait demandé la bonne information au bon endroit :

C'était une glace à la lavande.

Voici encore Vincent Trély et derrière lui, debout, Marie-Valentine. Assise à gauche Smahane Belhadais avocate dans le cabinet Yahia Avocats. Maître Yahia, bien connu pour ses rubriques sur le droit de la sécurité du numérique, et ses interventions lors des Congrès SSI santé du Mans, annuellement organisés par l'APSSIS, est à sa droite mais pas visible sur la photo.

Une vive volonté de nous revoir

Merci Vincent pour cette précision sur le parfum de la *mystérieuse glace bleue*, merci surtout pour cette excellente 1ère rencontre SSI Santé, évènement qui restera dans nos mémoires et pour l'équipe qui l'a organisé, et je sais toutes les difficultés qu'il y a à organiser un évènement de cette ampleur. Merci à Marie-Valentine qui m'a suggéré d'écrire ce compte-rendu, et j'ai été très flatté de sa confiance. Merci aux intervenants et aux participants ; vous avez toutes et tous été formidables !

Le 10ème Congrès national de la Sécurité des SI de Santé se tiendra au Mans les 5, 6 et 7 avril 2022.

Un Compte-rendu amicalement rédigé par Gérard Peliks

Gérard Peliks travaille depuis plus de 20 ans dans le domaine de la sécurité de l'Information. Ingénieur diplômé, il a travaillé pour Airbus Defence & Space Cybersecurity.

Lieutenant-colonel de gendarmerie dans la Réserve Citoyenne de Cyberdéfense (DGGN) et membre du Conseil d'Administration de l'Association des Réservistes du Chiffre et de la Sécurité de l'Information (ARCSI), il co-organise, sur une base mensuelle, les Lundi de la cybersécurité. Chargé de cours sur la cybercriminalité / cybersécurité dans des mastères d'écoles d'ingénieurs, en particulier à l'Institut Mines-Télécom, il est directeur adjoint du MBA Management de la cybersécurité de l'Institut Léonard de Vinci.

Son activité principale aujourd'hui est de porter l'esprit de cybersécurité / cyberdéfense auprès du citoyen en organisant des présentations pédagogiques de tous niveaux et en écrivant des articles de vulgarisation sur les dangers du cyberespace et sur les contre-mesures pour en diminuer les risques.

Gérard Peliks
Membre de l'ARCSI
gerard.peliks@noos.fr

www.arcsi.fr

APSSIS
Association Pour la Sécurité des SI de Santé

APSSIS
www.apssis.com
84 rue du Luart
72160 DUNEAU
secretaire@apssis.fr