LES SALONS HOCHE PARIS

Compte-rendu

2èmes Rencontres SSI Santé

Jeudi 22 septembre 2022

APSSIS

Dans la lignée des 1ères Rencontres SSI SANTE organisées en 2021 par l'APSSIS, à Paris, dans les prestigieux Salons Hoche, situés entre la place de l'Etoile et le Parc Monceau (*voir le reportage écrit en 2021*), un an plus tard, le 22 septembre 2022, se sont tenues, au même endroit, les 2èmes Rencontres SSI SANTE.

Aux Salons Hoche, avec la même qualité, le même intérêt, la même convivialité et bien sûr des intervenants prestigieux, dont une qui fut Secrétaire d'Etat chargée du Numérique et de l'Innovation, aujourd'hui directrice déléguée à la Stratégie, la Transformation et l'Innovation de la Croix-Rouge française et qui est intervenue en fin de journée, ces rencontres ont réuni une centaine de participants impliqués dans le domaine de la sécurité des données de santé. Des directeurs de la sécurité des données numériques, des experts cybersécurité, des juristes, et d'autres spécialistes, qui après les présentations de la journée, se sont attablés le soir autour d'un excellent dîner.

L'accueil

Nous sommes accueillis, dès 10h, par Vincent TRÉLY, président de l'APSSIS, par Marie-Valentine BELLANGER, par Hélène DASPE et par le cardiologue Fabien GUEZ qui allait être l'animateur de cette journée. Remises des badges, sourires, goodies, et nous nous retrouvons autour d'un café-croissants avant de remplir la salle de conférence où Vincent TRÉLY présente le déroulement de la journée. Le docteur Fabien GUEZ, cardiologue, journaliste et animateur de Check-Up Santé sur BFM Business, sera le coordinateur de l'événement.

De gauche à droite: Vincent TRÉLY, Fabien GUEZ, Hélène DASPE et Marie-Valentine BELLANGER

Le Health Data Hub

La première conférence est animée par Fabien MALBRANQUE, RSSI du Health Data Hub (HDH). Le HDH est une plateforme de partage de données médicales issue d'un projet de recherche du Groupement d'Intérêt Public créé en 2019, dans la mouvance de la stratégie nationale d'Intelligence Artificielle. Les données de santé disponibles sont extrêmement nombreuses mais très éparpillées. Le HDH propose un catalogue de métadonnées, ouvert aux porteurs de projets, pour explorer et utiliser les données de santé disponibles. Bien entendu, ce projet est en accord avec les dispositions du RGPD et autorisé par la CNIL. Les éléments du HDH sont sécurisés par des fonctionnalités à l'état de l'art des technologies disponibles. Les données sont chiffrées et les accès se font au travers de VPN (tunnels virtuels chiffrant). Les données sont également cloisonnées et les opérateurs d'une part, et les porteurs de projets d'autre part, accèdent à un espace dédié. Les ambitions du HDH pour cette année sont

d'accueillir 90 projets, une centaine de collaborateurs et 130 partenaires. Ensuite, le HDH souhaite s'inscrire dans un espace européen.

Parmi les questions posées par la salle, il y a celle de l'origine des données de santé qui entrent dans cette plateforme, celle de la pseudonymisation de ces données, de la collaboration avec la CNIL, de l'analyse des risques face à l'augmentation de la menace, de la localisation de cette plateforme, en conformité avec le code des marchés publics et de la souveraineté nationale. Les Hôpitaux continueront-ils à entreposer leurs données médicales en local ou profiteront-ils de l'existence de cette plateforme, même si la profondeur des données stockées par le HDH n'est pas celle des données qu'ils possèdent ? Existe-t-il en Europe des plateformes équivalentes et comment seront assurés les transferts éventuels entre les plateformes d'autres pays européens ? Autant de questions auxquelles Fabien MALBRANQUE a répondu devant les participants fortement intéressés par cette initiative.

Exigences en cybersécurité dans le secteur de la santé

TREND MICRO™ Securing Your Journey to the Cloud

Nicolas ARPAGIAN, directeur de la stratégie cybersécurité chez Trend Micro, expert en analyse des cybermenaces, nous parle de l'extorsion des données, du chantage, de la fraude à l'identité, du Phishing, des ransomwares et d'autres calamités auxquelles l'information de santé est de plus en plus confrontée.

Citant en exemple le cheval de Troie Emotet, utilisé par le groupe mafieux Conti, il décrit quatre étapes dans l'action d'un maliciel : l'extorsion et le chiffrement des données, l'exfiltration hors du système qui les héberge, les attaques en dénis de service faites souvent pour cacher une autre attaque, et enfin la communication directe entre agresseur / agressé, en particulier pour extorquer une rançon sous forme le plus souvent de cryptomonnaies.

En mars 2019, le CHU de Rouen avait dû afficher, sur la porte d'entrée de l'hôpital, un papier indiquant que, suite à la cyberattaque qui l'avait visé, son système d'information n'était plus utilisable, donc les patients devaient se diriger vers d'autres centres de soin. Le CH de Dax, ou plus récemment le Centre Hospitalier Sud Francilien, et bien d'autres hôpitaux ont eu à subir à leur tour des cyberattaques très pénalisantes.

Ces agressions ont de grandes chances de réussir si les systèmes d'exploitation de l'agressé sont obsolètes. Par exemple, le support de Windows XP a pris fin, celui de Windows 10, dont la mise à disposition date de 2015, ne sera plus maintenu à partir d'octobre 2025. Et que dire du système d'exploitation Windows 7 qui équipe encore beaucoup d'appareils médicaux et qui n'est plus maintenu depuis plus de 10 ans ! A cause des systèmes obsolètes, mais qui sont encore utilisés par le personnel de santé et par leurs prestataires, la prise de risque est énorme. En ont-ils conscience ? Comment assurer, face à ces menaces, la continuité des soins en cas d'attaque sur le système d'Information d'un centre hospitalier ?

S'appuyer sur des conseils d'experts, pour connaître les faiblesses des systèmes d'Information des organisations, est une sage décision et Trend Micro peut y contribuer pour qualifier les vulnérabilités de ses clients. Si on comptait 770 vulnérabilités au premier semestre 2021, on en compte 944 au premier semestre 2022, c'est dire que le danger est loin d'aller dans le sens d'une diminution ! Pour être crédible, il faut pouvoir se mettre dans la tête de l'attaquant. On peut échelonner les effets des menaces en quatre catégories : faibles, gênantes, graves et critiques. Réduire le temps d'identification d'une menace 0day par exemple, menace non connue et donc pour laquelle aucune correction n'est disponible, doit se faire dans les 30 jours pour une menace sévère voire critique, dans les 60 jours pour une menace moins sévère mais dont l'exploitation est très probable et dans les 90 jours pour les autres.

Un autre constat que souligne Nicolas ARPAGIAN est la carence en personnel pouvant opérer dans le domaine de la cybersécurité. Dès qu'un équipement est connecté, il fait courir un danger. Pour se faire une idée du danger réel, Nicolas ARPAGIAN nous précise qu'au premier semestre 2022, les équipes de

Trend Micro ont analysé et bloqué 63 milliards de menaces et ce nombre est en constante et forte augmentation.

Corrélations optimisées des signaux faibles avec Cybereason et retour d'expérience du centre hospitalier d'Annecy.

Après l'intervention de Nicolas ARPAGIAN qui laisse à réfléchir sur les dangers auxquels est confronté l'Information et sur la disponibilité menacée des systèmes d'Information de santé, prend place une expérience concrète et une solution pour diminuer les risques. Fabien GUEZ donne la parole à Samuel DESNOS, directeur de comptes secteur public entreprises chez Cybereason et pour lui donner la réplique, à Hervé PELLARIN, RSSI du Centre Hospitalier d'Annecy-Genevois.

Renverser l'avantage des attaquants au profit des attaqués en mettant les défenseurs en bonne position, sont les objectifs poursuivis par la solution Cybereason. Ceci se fait par la détection de signaux faibles, par leur corrélation et par la mise en place des préventions indispensables. Les questions auxquelles il convient de répondre sont : Sommes-nous en guerre ? Les assurances doivent-elles indemniser le paiement des rançons ou les payer directement si cela revient moins cher que d'indemniser les victimes suite à la cyberattaque ? Les moyens classiques répondent-ils aux nouvelles menaces ? Une bonne réponse serait de capitaliser sur les délais de découverte et de prise en compte d'une menace et de toutes celles déjà connues. C'est aussi de répondre à la question : « *qu'est-ce qu'un signal faible ?* » et d'assurer une protection multi couches.

Un antivirus et un firewall ne sont plus capables de faire face aux menaces sophistiquées actuelles. Les IDS (Intrusions Detection Systems) et les IPS (Intrusions Prevention Systems), les EDR (Endpoint Detection and Response) et les XDR (Extended Detection and Response) sont des contre-mesures beaucoup plus efficaces que les antivirus. Faut-il pour autant supprimer l'antivirus ? Plutôt que des solutions « On-Premise », c'est-à-dire en local, faut-il plutôt privilégier les solution SAS hébergées chez des partenaires bien sûr réputés fiables ? Telles sont les questions auxquelles le fournisseur de solutions Samuel DESNOS de Cybereason et l'utilisateur des solutions Hervé PELLARIN ont répondu. Une autre question de la salle a fait l'objet d'un débat passionné : « *Faut-il payer la rançon demandée par l'attaquant pour récupérer la clé de déchiffrement des données qu'il a réussi à chiffrer ?* ».

Important et passionnant débat qui fait d'ailleurs l'objet de résolutions très actuelles du gouvernement. Ce qui est sûr, c'est qu'il faut déclarer à l'ANSSI les attaques subies avec demandes de rançon, ne serait-ce que pour aider les défenseurs à mieux réagir à l'avenir.

Courte intervention d'ITRUST

Avant le buffet déjeunatoire qui est un des moments privilégiés pour retrouver des camarades parfois perdus de vue et pour discuter des riches enseignements du matin, David Ofer, vice-président d'Itrust et président de la Fédération Française de la Cybersécurité nous présente les solutions souveraines de cette entreprise française, société de services et d'édition de logiciels de cybersécurité, basée à Labège, près de Toulouse.

ITrust, société française, met en œuvre un SOC – Security Operations Center – souverain dont une partie, est réservée aux établissements de santé. Ce SOC est accessible aux petites structures qui ne disposent pas de gros budgets. Il fonctionne en mode SAS, avec un service 24/7 et propose la fonctionnalité d'Intelligence artificielle Reveelium, basée sur une analyse comportementale qui permet de détecter des cybermenaces connues et inconnues pour anticiper les attaques.

Découvrir les actifs connectés, les cataloguer et gérer leur sécurité

L'après-midi commence par une présentation de la solution de la société ARMIS par Jean-Michel TAVERNIER, son directeur commercial.

La solution d'ARMIS découvre les assets connectés dans un milieu hospitalier comme les serveurs, les caméras, les dispositifs d'imageries, scanners, IRM… Elle les cartographie. Elle est capable de découvrir également quel système d'exploitation, quels protocoles réseaux sont utilisés par ces assets. Après avoir référencé les assets découverts, un scanner de vulnérabilité en assure la protection et peut bloquer un asset s'il estime qu'il menace l'organisation.

Pour illustrer la portée d'une attaque contre un centre hospitalier, par des chiffres précis, recueillis un an après la paralysie du système d'Information de l'hôpital de Dax, Jean-Michel TAVERNIER donne des chiffres sur les conséquences financières de l'attaque subie : La reconstruction du réseau leur a coûté 174 000 euros ; les diverses prestations de sécurité sont montées jusqu'à 546 000 euros ; la perte de recette est estimée à 143 000 euros. Au total on parle d'un manque à gagner envoisinant les 2 344 000 euros.

La solution d'ARMIS repose sur trois piliers : La visibilité des assets, les rapports constitués et l'élimination des menaces. Cette solution, basée sur des algorithmes d'apprentissage profond, et qui s'appuie sur la connaissance de 2 milliards d'assets et de 16 millions de profils, apporte, avec un déploiement rapide, une solution au chaos, à l'incertitude, à la complexité et à l'ambiguïté que présente aujourd'hui tout système d'Information. Et la base de connaissances s'enrichit avec le temps.

La protection des données personnelles des patients, la protection contre la fuite de données médicales trouvent une solution dans la compréhension des flux de données et la collecte des métadonnées issues de différentes sources (messagerie SMTP, Active Directories, EDR, XDR…). La solution d'ARMIS corrèle les données et les classe automatiquement. Les couches physiques, réseaux, mais aussi la couche comportementale, sont explorées. Par exemple, si un appareil connecté envoie beaucoup d'images numériques vers un certain serveur, il peut être déduit que cet appareil est un scanner.

Contrôler les attaques DDoS en moins de 3 secondes et bloquer les attaques 0days

Lionel GORAM manager et expert en cybersécurité chez IMPERVA nous parle de protection de la donnée médicale et de ses accès, en insistant en particulier sur les attaques en déni de service distribué.

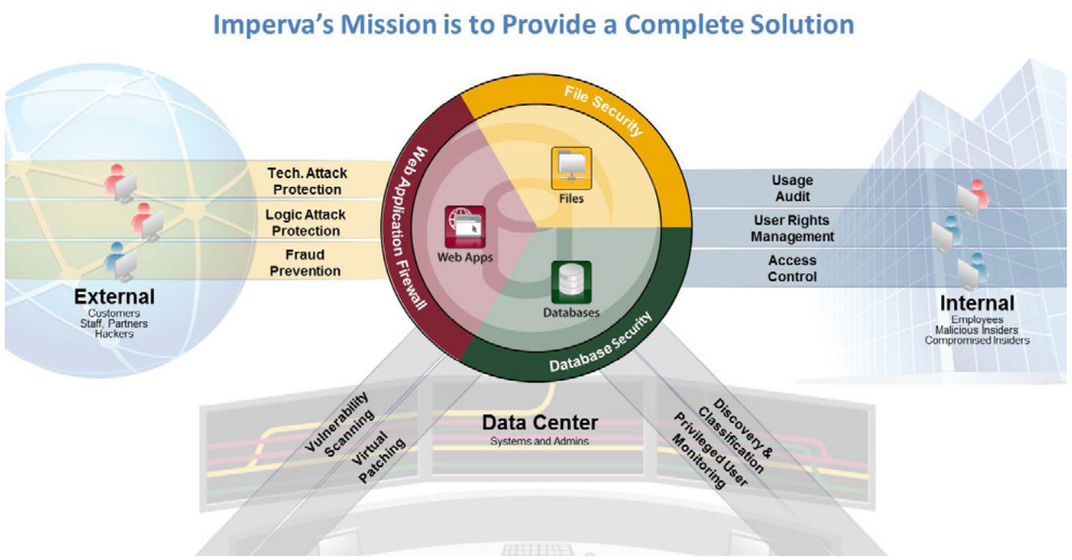
Il commence par donner un exemple : le jeu de société « Simon » contrôlé par ordinateur. Plus on y joue, plus on découvre des séquences possibles et plus le jeu devient complexe. Il en est de même pour les menaces sur l'Information et les systèmes qui la gère qui deviennent de plus en plus complexes. Ajouté à cela que les agresseurs mutualisent leurs plateformes d'attaques. De plus les patients gèrent maintenant leur santé en utilisant le numérique et les organismes d'assurance produisent de plus en plus de données. Il convient, pour faire face efficacement aux attaques, de gagner en efficacité en mutualisant les plateformes de défense. Malheureusement les ressources ne sont pas disponibles, aujourd'hui, en nombre et en qualité suffisants.

Les attaques causent une atmosphère de peur et les attaquants dérobent les données médicales car elles se vendent bien. Multiplier les points de défense, avoir un Plan de Continuité et de

Reprise d'Activité (PCA / PRA) à l'état de l'art sont devenus des impératifs. Il convient d'avoir en particulier une protection contre les attaques en déni de service distribué (DDoS -Distributed Denny of Services). Ces attaques DDoS peuvent également être employées pour dissimuler d'autres attaques. Statistiquement, beaucoup d'attaques en DDoS ne sont découvertes qu'après 7 minutes. Ce délai, durant lequel on ne perçoit pas qu'une attaque est en cours, est beaucoup trop long.

Les contre-mesures qui atténuent l'effet des attaques sont, pour un centre hospitalier, une garantie qui doit être établie par contrat auprès d'un prestataire de service. Le SLA, Service Level Agreement, pour ce type d'attaque, exige un temps de mitigation de moins de 3 secondes, voire de moins d'une seconde. Les attaques dont la découverte est moins urgente peuvent attendre d'être identifiées après plusieurs minutes. Le temps de latence et la capacité de gérer un débit de paquets pouvant atteindre plusieurs Teraoctets sont aussi des paramètres à prendre en compte dans le contrat de services.

La solution d'IMPERVA, entreprise californienne forte de plus de 1200 employés, réside dans un Cloud et s'utilise en mode SAS pour bloquer les flux de données identifiés comme dangereux.



Pause-café : Une heure accordée pour discuter entre nous

Les organisateurs des 2èmes Rencontres SSI SANTE ont prévu une pause d'une heure, avec café, thé et viennoiseries pour permettre aux participants de dialoguer entre eux et avec les intervenants. Echanges de cartes de visite, discussions sur les solutions proposées pour sécuriser les information, visites sur les tables des sponsors où des goodies nous attendent.

Et il est près de 17h00, il est temps de regagner les salles où deux présentations vont avoir lieu en parallèle : L'une porte sur la manière d'augmenter la méfiance des utilisateurs par des campagnes de Phishing. Elle est animée par Michel GERARD, président de Conscio Technologies et Fabien GUEZ. L'autre présentation porte sur les cyberattaques via les e-mails et comment s'en défendre. Elle est animée par Romain FAVRAUD - Channel Sales Engineer chez Vade et Vincent TRÉLY dans une salle attenante. Ces deux sujets m'intéressaient, et j'avoue que pendant la pause, je suis allé dans une salle puis dans l'autre sans pouvoir me décider. Finalement j'ai choisi la sensibilisation par attaque en Phishing (hameçonnage) en regrettant de ne pas pouvoir être aussi en parallèle dans la salle où il était question d'attaques par messagerie. Mais il a fallu faire un choix.

Romain FAVRAUD a donc animé la session « *L'email premier vecteur de cyberattaques : actualités, stratégies d'attaque et moyens de protection pour les établissements de santé* », que son entreprise Vade permet avec une solution basée sur un Cloud (voir encadré «VADE»). J'étais dans l'autre salle. A l'issue de cette présentation, les participants nous ont rejoint et ils avaient l'air très satisfait. Moi j'étais donc dans la salle où était expliqué comment le personnel d'un centre hospitalier se fait avoir par une tentative de Phishing fictive.

Campagnes de sensibilisation des employés au Phishing pour éviter des catastrophes

Michel GERARD, président de Conscio Technologies anime cette session si nécessaire surtout pour ceux qui cliquent sans réfléchir aux conséquences possibles, et reçoivent une grosse claque. Les conséquences peuvent être, par exemple, le blocage du système d'Information d'un centre hospitalier ou le chiffrement des Informations avec demande de rançon.

Basée sur la remontée du terrain suite à des attaques en Phishing, Michel GERARD donne le pour et le contre de la mise en œuvre des sensibilisations pour diminuer le risque de ces attaques.

Le contre :

• Les utilisateurs vivent mal l'impression de s'être fait piéger
• Une sensibilisation sur le Phishing peut sembler être inutile puisque la messagerie est censée être sécurisée, donc le Phishing ne peut être une vraie menace.
• Le scénario utilisé n'a rien à voir avec son métier ou ses préoccupations.

Attention aussi dans des campagnes de Phishings fictifs à l'utilisation de vraies marques ou noms de domaines. Ça peut entrainer des problèmes d'ordre juridique. Dans des campagnes de Phishing fictif vers le milieu médical, ne pas utiliser par exemple un nom de domaine ARS ou celui d'un hôpital.

Le pour :

• Le nombre d'attaques en Phishing explose, et peut concerner tout le monde. Personne ne doit l'ignorer, donc les campagnes de sensibilisation contre le Phishing sont indispensables. Mauro ISRAEL, assis à côté de moi apporte une précision : Introduire des fautes d'orthographe pour faire penser qu'un mail peut être une tentative de Phishing n'est pas très utile vu le niveau en orthographe de la plupart des utilisateurs. 😊
• Une campagne unique n'est pas très intéressante, par contre des campagnes répétées apportent des informations qui peuvent renseigner sur la psychologie des utilisateurs et la sociologie de l'entreprise.
• Une campagne de Phishing peut créer une réaction salutaire et le piégé peut se méfier et s'assurer qu'on ne le reprendra plus. Il peut aussi faire part aux autres de sa conduite irresponsable pour qu'eux non plus ne tombent pas dans un tel piège.

Il faut se rendre compte qu'une montée brusque du stress entraine une diminution des capacités cognitives, donc apprendre à gérer le stress est aussi un facteur intéressant induit par les campagnes de Phishing fictif.

Concernant la sensibilisation elle-même ; il y a peu de contre, et le pour est dans la réduction de la surface d'attaque et la diminution des réactions inappropriées. Le pour est aussi dans la balance entre le coût des sensibilisations et le nombre d'incidents évités.

Et Michel GERARD de citer une pensée d'Abraham Lincoln : « *Si vous trouvez que l'éducation coûte cher, essayez l'ignorance* ». Puis il donne quelques chiffres issus des retours de terrain d'IMPERVA, pratiqués sur 9000 personnes de janvier 2021 à juillet 2022 : 2 collaborateurs sur 10 se font piéger par une campagne fictive de Phishing et 19% plus précisément dans le domaine de la santé. 84% des campagnes de Phishing se font avec des outils Microsoft. Demander le login et le mot de passe avant de pouvoir télécharger un fichier est ce qui marche le mieux (44% de piégés), proposer de rentrer son login et son mot de passe pour entrer dans une visioconférence Teams est aussi très efficace (39% de piégés).

IMPERVA propose des outils de sensibilisation et une solution de protection contre le Phishing « Imperva DDoS Protection for Networks ».

L'email : un véritable missile

C'est avec VADE que la deuxième salle entame cette seconde partie d'après-midi, autour d'une conférence de Romain FAVRAUD, Channel Sales Engineer, intitulée : « L'email, premier vecteur de cyber attaque ». Romain nous décrit par le menu les différents types d'emails dangereux, que ce soit par leurs titres, leurs contenus (y compris le code HTML), leurs signatures, leurs imitations d'images et leurs renvois automatisés vers des pages web corrompues.

C'est incroyable ce qu'un simple email peut fournir comme informations, et c'est également sidérant de constater toutes les techniques utilisées par les pirates pour faire de l'email un véritable missile. La spécialité de VADE, c'est justement d'analyser en profondeur les emails pour détecter leur potentiel offensif, à l'aide de leur base de connaissance régulièrement mise à jour, et pour en bloquer un maximum, réduisant ainsi la surface potentielle de nuisance. Remarquable intervention, toute en fluidité et en pédagogie, qui ravit la salle tout en la laissant perplexe sur l'usage quotidien de la boite mail !

Découvrir sa surface d'attaque et comment se protéger des cyberattaques

Mauro ISRAEL, expert très reconnu en cybersécurité, monte sur scène pour nous parler de SECURITYSCORECARD. Le connaissant bien et depuis de nombreuses années, je pressens qu'il va créer un grand moment conversationnel avec la salle et je n'ai pas été déçu ! Son sujet : « *Découvrez votre surface d'attaque et comment vous protéger concrètement des cyberattaques* » était une occasion rêvée pour cela.

Puis-je ajouter que, au cours de cet évènement, Mauro m'a offert et dédicacé son dernier livre en français «Cyber Security Instinct Reloade !» Ce livre insiste sur 3 piliers : Eclairer le risque cyber, renforcer nos défenses, permettre aux métiers de travailler dans un environnement numérique stable, rapide et sécurisé. Je m'y plongerai dès que j'aurai fini d'écrire ce compte-rendu, et bien sûr, je vous conseille de vous le procurer.

Mauro évite autant que possible les acronymes qui foisonnent en cybersécurité mais que le commun des mortels ne connait pas. Il souligne le manque de compétences tant sur le plan qualitatif que sur le plan quantitatif, en particulier chez les décideurs et chez les politiques. Il note la distorsion qui existe entre le soin apporté par les structures de santé et le fait qu'elles se font pirater.

Il cite une phrase de Darwin : « *Ce n'est pas la plus forte des espèces qui survit, ni la plus intelligente, mais celle qui s'adapte le mieux au changement* ».

Dans ce monde sans frontières où chacun peut joindre un dispositif connecté et l'attaquer en moins d'une seconde, s'adapter au changement, voilà ce qui est vital de faire. Il faut s'adapter en effet, et en mode résilient. Là où le commun des mortels levant les yeux au ciel par une belle nuit sans nuages voit des étoiles, les pirates eux voient des patterns qui lient ces étoiles et ils savent les exploiter.

Mauro prend pour image la constellation de la Grande Ourse avec pour chaque étoile une fonctionnalité qui intervient dans une « cyber kill chain ». Ces étoiles ont pour nom la reconnaissance du réseau cible, la préparation de l'attaque, l'envoi d'un mail de Phishing, la compromission d'un serveur, l'établissement du C2 (attaque en Commande et Contrôle), la post exploration, l'élévation de privilège, le mouvement latéral et le pivoting. Voilà ce que les pirates voient dans la constellation de la Grande Ourse alors que le pecus vulgaris ne voit que des étoiles.

Expliquez ça à un centre hospitalier et on vous prendra pour un pessimiste, un parano et peut-être même un adepte du catastrophisme. Et pourtant la question n'est plus « *va-t-on être attaqué ?* » mais quand va-t-on l'être ? L'important est de connaître la surface d'attaque à laquelle on est exposé. Un attaquant averti la voit et attaque à l'endroit où c'est le plus facile et le plus rapide car il n'a pas de temps à perdre. Si la surface d'attaque indique une maîtrise suffisante de la sécurité du système

d'information, il ira attaquer ailleurs.

Etablir un scoring, c'est-à-dire une note en fonction de différents critères, permet d'évaluer le profil d'une organisation ou d'une personne. La notation de sécurité de l'exemple choisi par Mauro va de « A » (la mieux protégée) à « F ». Le risque de piratage augmente avec la hauteur de la lettre de la notation attribuée, dans l'alphabet. Avec un score B, l'entité a 2.6 fois plus de chance de se faire pirater qu'avec un score A. Avec un score F, une entité a 7.7 fois plus de chance de subir une cyberattaque qui va réussir.

Mauro nous fait une démonstration de recherche de vulnérabilités et de surfaces d'attaques sur des domaines liés à la santé. La confidentialité réclamée ne nous permet pas d'en dire plus dans ce compte-rendu.

L'entretien avec une personnalité politique : Axelle LEMAIRE

Dernière intervenante de la journée, Axelle LEMAIRE monte sur scène, pour un entretien mené par Fabien GUEZ.

Axelle LEMAIRE est aujourd'hui directrice déléguée à la stratégie, la transformation et l'innovation à la Croix Rouge Française. Elle a été députée des Français établis à l'étranger en 2012, puis Secrétaire d'Etat chargée du Numérique et de l'Innovation dans le gouvernement de Manuel VALLS de 2014 à 2017.

La loi pour une République numérique, dont elle est la principale architecte, introduit l'ouverture par défaut des données publiques, la neutralité du net, une obligation de loyauté des plateformes en ligne, ainsi qu'une protection accrue pour les données personnelles des usagers du net. Et tout cela a été voté en 2016.

En réponse à une question de Fabien GUEZ, Axelle LEMAIRE explique que la prise de conscience par les politiques du danger réel du cyberespace a été grandement amenée, suite à la cyberattaque en avril 2015 qui a ciblé TV5 monde, chaîne internationale francophone, qui émet en français dans 200 pays et territoires dans le monde avec 290 millions de foyers connectés. TV5 monde est un vecteur important de la diplomatie de la France. Cette attaque a causé un électrochoc qui a atteint le gouvernement. Le signal d'émission des programmes diffusés par TV5 monde a été rendu inopérant. Les téléspectateurs qui regardaient cette chaine avaient un écran noir et cela a duré toute une nuit jusqu'à ce que le signal ait pu être rétabli. Le web et le compte Twitter de TV5 Monde étaient compromis et diffusaient de la propagande de l'état islamique. En fait cette attaque provenait en réalité des Russes.

Une autre question a porté sur l'ouverture des données dans l'espace public. Cela a été rendu nécessaire en particulier pour lutter contre la pandémie du Coronavirus car l'accès à ces données était devenu indispensable. Bien sûr il fallait rester en conformité avec le RGPD, sinon la CNIL aurait pu infliger des sanctions.

Fabien GUEZ pose aussi la question de l'interopérabilité des données et du pouvoir des GAFA sur le contrôle possible des données à caractère personnel de tous pays, Europe comprise. Axelle LEMAIRE nous a parlé des actions faites par les pouvoirs publics sur cette question.

La souveraineté de la France a été aussi une question importante. Il est par exemple inadmissible que le nom de domaine « vin.com » ait été acheté aux enchères par les Américains.

Pour conclure, Axelle LEMAIRE pense qu'il y a beaucoup de chemins d'amélioration à parcourir et qu'il faut s'en donner les moyens.

Vincent TRÉLY conclut la journée, remercie les sponsors de ces rencontres et nous allons dans le salon Vendôme où nous attend un excellent dîner.

Voici les sponsors de ces 2èmes rencontres SSI Santé :

ARMIS

Security Scorecard

TREND MICRO

conscio technologies

vade

cybereason

imperva

ITrust IT Security Services

Le dîner

Encore une occasion d'échanges avec l'excellent dîner convivial où les conversations ont continué autour de tables rondes accueillant chacune une dizaine de convives.

Autour de moi deux avocats dont Maître Omar YAHIA, avocat au Barreau de Paris et un des vice-présidents de l'APSSIS ; l'inoxydable Cédric CARTAU, autre vice-président de l'APSSIS et RSSI et DPO du CHU de Nantes dont je lis avec passion les chroniques pleine d'humour dans le magazine DSIH ; Michel DUBOIS, chef du pôle expertise cybersécurité au sein de la direction de la cybersécurité du Groupe La Poste ; deux charmantes dames et deux charmants messieurs. C'est dire l'intérêt des conversations que nous avons eues lors de cet excellent repas à base de poissons. Vous ne me voyez pas sur la photo ? Normal, c'est moi qui la prends avec mon smartphone.

L'évènement se termine vers 22h30. Il est temps de rentrer avec la promesse faite aux organisateurs de ces merveilleuses deuxièmes rencontres de l'APSSIS que j'essaierai d'écrire un compte-rendu sur mon ressenti au cours de cette inoubliable journée !

Gérard Peliks

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