Les 3èmes Rencontres SSI Santé de l'APSSIS

https://www.apssis.com/rencontres-ssis/les-rencontres-ssi-sante-2023.html

---ooo---

C'est curieux, chez les professionnels de la SI de Santé, ce besoin de multiplier les acronymes.

Aussi, pour être compris par un plus large public que les experts qui étaient présents aux 3èmes Rencontres SSI Santé, le 28 octobre 2023 à la Maison des Polytechniciens, à Paris, permettez-moi de commencer par un petit recueil d'abréviations.

Quelques abréviations qui apparaissent dans ce texte :

AD : Active Directory

APSSIS : Association Pour la Sécurité des Systèmes d'Information de Santé

ARS : Agence Régionale de Santé

BEC : Business Email Compromise

CISO : Chief Information Security Officer

EDR : Endpoint Detection & Response

GHT : Groupement Hospitalier de Territoire

IA : Intelligence Artificielle

IoT : Internet of Things

NAC : Network Access Control

SIEM : Security Information and Events Management

SOAR : Security Orchestration, Automation and Response

SOC : Security Operations Center

XDR : Extended Detection & Response

ZTNA : Zero Trust Network Access

Voici mes impressions sur les 3èmes Rencontres auxquelles j'ai été invité.

La Maison des Polytechniciens dans le 7e arrondissement de Paris, près du Musée d'Orsay, est un écrin fabuleux dans lequel allait se tenir un bijou d'évènement, et quel luxe !

Poussons la porte, nous y voici. L'APSSIS a bien fait les choses.

Nous sommes accueillis par Marie-Valentine et Hélène. Sourires, mots de bienvenues, badges goodies, et nous voici intégrés parmi les invités. On se retrouve, on se parle au sujet de cet évènement qui va traiter d'un sujet très actuel : les cyberattaques (hélas nombreuses, surtout quand elles concernent le milieu hospitalier) et la cybersécurité (indispensable) dans tous les milieux.

Tiens voilà Cédric Cartau, RSSI & DPO du CHU de NANTES, RSSI du GHT44, enseignant à l'EHESP, à l'ESIEA, au CNEH et à POLYTECH NANTES, Vice-Président de l'APSSIS, membre de l'AFCDP, de

l'ARCSI, du CESIN. Allez j'en rajoute : co-créateur du Club ISO27001 de la Région nantaise et intervenant très apprécié aux « Lundi de la Cybersécurité » qu'il anime parfois.

Lui qui écrit de si beaux textes, avec un humour particulier dont on raffole dans la revue DSIH et sur LinkedIn. Il est aussi un des vice-présidents de l'APSSIS, un autre étant Charles Blanc-Rolin, aussi présent et à côté de qui j'aurai le plaisir d'être assis à table, le soir.

Et voilà Auriane Lemesle, référente régionale Sécurité du GCS e-santé Pays de la Loire, et secrétaire générale de l'APSSIS. Auriane et Vincent Trély interrogeront le Directeur Général et le DSI du Centre Hospitalier Sud Francilien, le soir à 19h00 pour la dernière intervention de la journée. Ces intervenants nous parleront de la cyber attaque qu'ils ont subi il y a un an, des traces qu'elle a laissées et de la remédiation qui a été faite. Une intervention exceptionnelle avant le dîner.

Quel beau monde j'allais retrouver à l'occasion de cet évènement de l'APSSIS, après le 11ème Congrès National de la Sécurité des Systèmes d'Information de Santé étalé sur 3 jours au Mans, du 13 au 15 juin 2023 ! J'en avais aussi livré mes impressions sur papier. Les voici en ligne :

https://www.apssis.com/upld/2023/07-JUILLET/CR-CNSSIS2023-GPELIKS.pdf

J'avais aussi goûté au plaisir de rédiger un compte-rendu des 2èmes Rencontres de l'APSSIS, tenues le 22 septembre 2022 aux Salons Hoche – Paris 8e. Le voilà :

https://www.apssis.com/upld/2022/10-octobre/cr-gerard-peliksv1.pdf

Auriane me propose de m'assoir à la table d'honneur, pour le repas du soir. On se sent honoré parmi ces experts !

Le café d'accueil

« Miroir, mon beau et grand miroir, toi qui trônes à l'entrée du salon de la Maison des Polytechniciens, entre tes moulures et tes dorures, et que je suis en train de prendre en photo *avec mon smartphone, que vois-tu en ce moment ? »*

« Je vois Vincent Trély, président de l'APSSIS et Auriane Lemesle, secrétaire générale de cette organisation, ainsi qu'un troisième personnage qui est l'auteur de ce document. »

Après le café d'accueil et les viennoiseries, il est 10h30, Vincent Trély introduit les conférences devant les 120 participants.

Vincent TRELY – Président de l'APSSIS – ouvre l'évènement

Avec une grande convivialité mais aussi une autorité qui va faire que le planning sera strictement respecté, Vincent présente le détail de la journée : 8 conférences de 40 minutes chacune, suivies de 4 pitchs de 10 minutes, et pour terminer, une heure avec deux responsables du Centre Hospitalier Sud Francilien qui vont nous parler de la cyberattaque dont ils ont été les victimes.

Des espaces d'échanges entre participants sont prévus : le buffet déjeunatoire à 12h40 après les 3 premières interventions, la pause à 16h10 et le dîner pris à l'étage de l'hôtel de Poulpry, Maison des Polytechniciens.

Place à la première conférence, Michel Van Den Berghe monte en chaire.

La Cybersécurité en France : situation, enjeux et perspectives

Avec Michel VAN DEN BERGHE – Président du Campus Cyber

Bienvenue en Cyberie pour élever le niveau cyber de la Nation.

Initié le 15 février 2022 sur une volonté du Président de la République, le Campus Cyber occupe 26 000 m^2 dans la Tour Eria de La Défense. Il rassemble 1800 personnes, est composé à 39% d'entités publiques et à 61% d'entités privées.

Opérations, formations, innovations, animations, avec ces actions, son but affiché est d'élever le niveau cyber de la Nation.

Ce Campus Cyber anime 14 groupes de travail auxquels participent plus de 600 contributeurs actifs. Il a organisé plus de 400 évènements et formations. Michel Van Den Berghe cite un entrainement à la simulation de crise cyber avec l'exercice REMPAR22 en coopération avec l'ANSSI et le Club de la Continuité d'Activité en décembre 2022. Il cite encore l'Hackaton Cache-Cache en partenariat avec la DGSE en novembre 2022 dont le but était de simuler et déjouer un projet d'attentat terroriste. Le Campus Cyber a déjà reçu une cinquantaine de délégations ministérielles et étrangères. Il s'affirme ainsi dans l'écosystème de la sécurité du numérique.

De grands axes pour 2023 / 2024 du Campus sont, avec le Ministère de l'Education Nationale et l'ANSSI, une campagne d'affichage dans les collèges et lycées d'Île-de-France qui débutera

le 13 novembre 2023, la formation de 2000 professeurs et éducateurs aux métiers et enjeux de la filière cyber avec pour ambition de toucher 6 millions d'élèves. Il y aura bientôt, à la télé, une série « *Bienvenue en Cyberie* » sur les enjeux cyber et le renseignement.

Michel Van Den Berghe dépeint les perspectives que posent à l'économie les cyberattaques. Elles sont alarmantes : 6000 milliards de pertes financières au niveau mondial ; une PME sur deux qui, suite à une attaque par rançongiciel, paye ou ne paye pas la rançon demandée, et dépose le bilan dans les 18 mois.

La croissance du nombre d'attaques qui utilisent l'IA pour s'adapter au comportement des victimes et contourner leurs mécanismes de détection, l'automatisation pratiquée par les cybercriminels qui détectent et utilisent les vulnérabilités de leurs victimes, rendent les cyber-agressions de plus en plus redoutables.

Le Campus Cyber se veut une initiative qui vise à augmenter le niveau de défense et à diminuer les risques, hélas bien réels.

Cyber-fièvre à l'hôpital : les dernières tendances des cyber-attaques dans le monde de la santé

Avec Romain BASSET – Directeur des services clients chez VADE

L'Intelligence Artificielle pour assurer la sécurité des messageries.

Une PME sur deux a déjà subi au moins une attaque par ransomware. Les solutions de Vade protège ses clients en détectant les acteurs aux contenus malveillants avant qu'ils n'infectent leurs cibles, et bloquent, par jour, plus d'un million de ransomwares. Dans le secteur de la santé, Vade propose, en particulier, une solution pour faire face aux Menaces Persistantes Avancées (APT). Vade a observé en moyenne, dans le secteur de la santé, 141 APT par organisation et par mois.

1,4 milliards de boîtes e-mails sont ainsi protégées dans le monde, et 100 milliards d'e-mails sont analysés quotidiennement.

Le Phishing, ou hameçonnage, qui vise les messageries de Microsoft est la cybermenace la plus fréquente. Romain Basset nous parle aussi du QRishing (incitation à saisir avec son smartphone un QR code qui mène sur un web malicieux), des fausses factures jointes à des e-mails frauduleux sous format HTML, du « Spear Phishing » attaque ciblée, de type « initial contact ». Il nous décrit ce que sont la « triple attaque » puis l'attaque « Tour du monde » qui compromettent des sites légitimes.

Vade utilise des technologies basées sur l'IA. En détectant les signaux faibles, l'application Vade for M365 complète l'offre de messagerie de Microsoft dans le domaine de l'anti-spam, de

l'anti-phishing et de l'anti-malware. L'application Vade Cloud, solutions en SaaS, est basée sur un moteur d'Intelligence Artificielle qui analyse les e-mails pour détecter, par des méthodes heuristiques d'analyses comportementales et de machine Learning, des attaques comme le phishing, le spear phishing, le BEC, les ransomwares et d'autres types de cyberattaques, même celles qui ne sont pas encore connues. Le but est de les arrêter avant qu'elles n'atteignent les utilisateurs.

La gestion de ces solutions est faite par console d'administration centralisée avec l'étude et l'apprentissage provenant de 1.4 milliards de boîtes e-mails. Vade propose des fonctions de remédiation, et propose également des sensibilisations.

Vade, anciennement Vade Secure, est une entreprise française, fondée en 2008. Elle est devenue aujourd'hui internationale. Son siège social se situe sur le campus d'Hem, dans la banlieue de Lille. Elle compte plus de 5000 clients à travers le monde, avec des bureaux en France, aux Etats-Unis, au Canada et au Japon.

Vade est spécialisé dans la conception et l'édition de solutions logicielles de sécurité prédictives pour la messagerie, basées sur l'intelligence artificielle, l'analyse comportementale et heuristique, et le machine learning.

Maîtriser sa cybersécurité : visibilité et contrôle de bout en bout

Avec Christophe AUBERGER – CTO et CISO mais aussi Cybersecurity sensibilisateur et vulgarisateur chez FORTINET

Une solution pour l'analyse des accès basés sur les rôles des utilisateurs.

En France, d'après le CESIN, 8 entités sur 10 subissent au moins une cyber-attaque par an, et 60 % des attaques ont une incidence sur l'activité et sur le business des entreprises. Le Phishing est l'attaque la plus fréquente, suivi de la fraude au président et l'envoi de malwares. La CNIL souligne avoir reçu 1200 à 1300 notifications d'altération ou de vol de données à caractère personnel depuis l'entrée en vigueur du RGPD.

On a observé une sophistication grandissante des attaques depuis le virus Melissa des années 1990 en passant par le ver Stuxnet en 2011 et jusqu'aux vers Wannacry et NotPetia en 2017, et ça continue ! Les dossiers volés connaissent une forte hausse et le nombre de ransomwares est passé de 3.2 millions en 2014 jusqu'à plus d'un milliard en 2020 durant la période de la Covid-19.

Aujourd'hui, en moyenne, on compte 3 mois avant de constater qu'on est attaqué, et ces attaques débutent souvent par de l'ingénierie sociale. Le cyberespace est devenu le carrefour de tous les dangers.

Les données des patients, volées dans un milieu hospitalier, se revendent à un prix supérieur à celui des autres données : un montant 10 fois plus élevé que le prix pour les numéros de cartes bancaires. Plus précisément, d'après Ponemon Institut, la revente des données volées rapporte en moyenne 408 $ pour un dossier médical, contre 140 $ pour une donnée commerciale, et 208 $ pour une donnée financière.

L'IA permet de cibler les individus qu'on veut attaquer. L'écosystème est de plus en plus complexe et les équipes pour faire face aux cyberattaques, qui sont de plus en plus personnalisées, ne sont pas suffisantes en nombre et en expertise. Les patients d'un établissement de santé sont placés au centre de la transformation numérique et sont menacés de même que l'établissement où ils sont pris en charge.

Totalisant plus de vingt ans d'expérience dans les méthodes de profilage actives et passives, l'offre FortiNAC de Fortinet permet de détecter tous les périphériques connectés au réseau d'une entreprise, de contrôler leurs accès aux ressources de ce réseau et de répondre automatiquement aux vulnérabilités de sécurité. Ceci concoure donc à implémenter le Zero Trust en permettant aux appareils connectés, y compris pour l'IoT de n'accéder aux ressources du réseau qu'avec des privilèges réduits.

La visibilité, le contrôle et les réponses faites de manière centralisée, face aux cyber-attaques renforcent la confiance des clients envers les équipements d'extrémité.
En résumé, la solution FortiNAC permet d'assurer :

- La visibilité car elle découvre et classe, en quelques secondes, les appareils connectés au réseau.
- Le contrôle avec la segmentation, l'authentification et l'autorisation de disposer d'une ressource.
- La réponse car elle détecte, répond et corrige les connexions.

Le Buffet déjeunatoire

Il est 12h40, nous avons une heure et 30 minutes pour nous restaurer. Un buffet déjeunatoire a été installé dans les jardins de la Maison des Polytechniciens. Les échanges avec les convives s'établissent. J'apprends beaucoup sur ce que sont devenus quelques amis perdus de vue. Ainsi j'apprends par Romain, directeur des services clients de Vade, que Georges Lotigier, qui fut le PDG de Netasq, avec qui j'étais en relation quand je travaillais chez EADS/AIRBUS, est le PDG de Vade.

Je retrouve aussi un employé d'Egérie, Bruno, qui se reconnaitra. Bruno a été, il y a 5 ans, un de mes élèves dans le MBA Management de la Cybersécurité de l'Institut Léonard de Vinci. Je l'ai reconnu à son regard. Et nous parlons d'Egérie, cette entreprise toulonaise bien connue dans la quantification financière des risques cyber.

C'est l'occasion de lier de nouvelles connaissances et de retrouver des anciens collègues. L'APSSIS fait bien les choses !

Mais voilà que, l'heure et demi de pause se terminant, arrivent les organisateurs qui viennent nous chercher et sonner la fin de la récréation. Il est 14h10, nous regagnons la salle où se tiennent les conférences pour un après-midi qui sera fort bien rempli.

Sensibilisation, remédiation et Sécurisation de l'AD dans les hôpitaux – cas d'usage

Avec Rachida MAJERI, Territory Account Manager et Mathieu VIALETEY, responsable avant-vente chez SENTINELONE.

L'AD fortement attaqué doit être sévèrement protégé.

Voici le problème : Les défenseurs ont mille manières de subir une compromission de leur SI alors que les agresseurs peuvent passer inaperçu, choisir un seul vecteur d'attaque et une seule fois.

Alors que faire pour protéger efficacement son AD et ses datas, chacun dans son rôle et ses compétences ?

Il est indispensable que le personnel en charge du SI d'un Centre Hospitalier suive une sensibilisation à la sécurité de l'Active Directory. Ce gestionnaire d'annuaires, qui est une des applications les plus névralgiques, constitue une cible qui intéresse particulièrement les cybercriminels. Une attaque sophistiquée qui s'introduit sur un point faible du SI, terminal ou serveur, va chercher par extension latérale sur l'Intranet, à trouver et compromettre l'AD qui constitue une cible idéale. Le personnel de 90% des entreprises s'identifie et d'authentifie par l'AD, mais 50% d'entre elles ont subi des attaques sur leur AD au cours des deux dernières années.

La solution de SentinelOne met en jeu un EDR qui analyse les actions malveillantes vers l'Active Directory. Parmi les attaques, citons les vols des identifiants et des mots de passe, facilités souvent par des tentatives d'ingénierie sociale. Des études montrent que 42% des attaques sophistiquées sur l'AD réussissent.

L'exploitation de l'attaque se fait en général sur 3 étapes : la découverte des serveurs où se trouvent les datas les plus critiques donc les plus intéressantes, le déplacement vers l'AD par le plus court chemin, et la compromission qui profite surtout d'une mauvaise configuration de l'AD et permet de monter en privilèges.

Face à cette attaque, quelles sont les solutions ?

La réponse de SentinelOne est déjà d'exercer un audit continu des annuaires, avec des contrôles de sécurité en particulier pour déterminer s'il y a des extensions latérales vers l'AD et s'il y a des mauvaises configurations.

Les intervenants introduisent une nouvelle abréviation : le TDR – Threat Detection & Response. Une bonne solution est de placer des leurres pour égarer les agresseurs. Cette solution Singularity XDR avec son agent RANGER AD réduit la surface d'attaque. La solution est proposée « on premise » ou en SAS sur Azure AD.

L'ANSSI va lancer des appels d'offre pour faire émerger des projets de cybersécurité dans le cas du plan France Relance.

SentinelOne est une entreprise américaine spécialisée en cybersécurité. Son siège social est situé à Mountain View en Californie. SentinelOne propose des solutions de sensibilisation, de remédiation et de sécurisation de l'Active Directory (AD) pour les centres hospitaliers. Le Gartner a placé SentinelOne parmi les leaders dans son Magic Quadrant 2022 consacré aux plateformes de protection des endpoints.

Cyberattaque : à qui la faute ?

De Christophe MILLET, Cyber Risk Manager chez RELYENS

Maîtriser les risques, mutualiser la confiance

Christophe MILLET décrit, du point de vue juridique, la notion de faute suite à une cyberattaque. Est-elle imputable à un Centre Hospitalier ?

- Elle peut impliquer une personne morale comme le paiement d'une rançon dans le cas d'une attaque par ransomware quand un cryptovirus a chiffré les données.
- Elle peut être à l'initiative des patients en cas de fuite de données médicales imputable à l'établissement
- Elle peut aussi être à l'initiative du personnel et avoir des impacts individuels.

Quelle peut être la réponse d'un Centre Hospitalier ? Il doit constituer un dossier de défense, qui sera soumis à un juge, et dans lequel sont précisées les mesures prises pour protéger les données avant l'attaque. Ces mesures étaient-elles suffisantes ? Le Centre Hospitalier a-t-il détecté rapidement l'attaque et limité sa propagation et ses impacts ? La demande entre les soins et la nécessaire cybersécurité, malgré les contraintes budgétaires et la pénurie générale de compétences, est-elle ajustée à l'offre du marché ?

Le Plan blanc

Le 15 juin, la DGOS - Direction générale de l'offre de soins – a publié un guide pour préparer les RSSI des établissements de santé au volet numérique du Plan blanc. Ce guide est applicable immédiatement en France.

La question pour un chef d'établissement est d'établir si son organisation est bien préparée pour prévenir les risques du numérique. Sa responsabilité peut-elle être engagée s'il n'a pas suivi les recommandations du Plan blanc ? Un plan de mise en conformité aux exigences de cybersécurité, telle que la directive NIS (depuis peu NIS2) est-il bien adapté ?

Le Plan Blanc numérique qui doit être inclus dans le dossier de défense et comporte 3 parties :

1. Les mesures préventives de sécurité numérique à mettre en œuvre pour prévenir, diminuer l'exposition et maîtriser le risque numérique
2. Les travaux de préparation à anticiper pour faire face à un incident numérique
3. L'organisation des soins en mode dégradé.

Composé de 140 items dont 50 sont obligatoires, comme la tenue d'un journal qui servira de valeur probante en cas de problèmes, ou encore la possibilité d'utiliser une solution dégradée sur un réseau de secours. D'autres sont recommandées, comme le signalement en interne

d’une anomalie quand elle est décelée ou son impact sur l’organisation des soins ou la sauvegarde des données.

Le Plan Blanc établit ainsi une nouvelle doctrine de la cybersécurité en Centre Hospitalier.

Le Plan Bleu

Le Plan Bleu, qui est sous la responsabilité du directeur d’un établissement médico-social, est en cours d’élaboration pour les ESMS (établissements et services sociaux et médico-sociaux) qui ne sont pas concernés par le Plan blanc.

RELYENS est un groupe mutualiste européen de 1 100 collaborateurs spécialisé dans l'assurance et le management des risques auxquels sont confrontés les établissements de santé.

RSSI en santé : Vous n’êtes pas seuls ! Comment faire face à des milliards d’évènements de sécurité par jour ?

Avec René FUHRMANN – Responsable Commercial du Pôle d'expertise Santé chez ADISTA, et trois autres intervenants de Cyberprotect.

Passer d’une logique d’investissement à une logique de charges.

Comment peut-on arriver à traiter tous les risques et répondre aux incidents ? :

Utiliser son expertise pour identifier les failles des logiciels et détecter les menaces potentielles pour réduire les risques.

Recruter les profils adaptés pour constituer des équipes d’experts

Des milliards d’évènements sont traités hebdomadairement par des applications de SIEM et de SOAR. Corrélés, les résultats donnent 100 000 alertes qui, après analyse sont envoyées à des SOC qui affichent des informations compréhensibles à l’aide d’histogrammes et de camemberts. On observe une évolution dans ce type d’attaques. Les fuites de données sont toujours particulièrement présentes mais si, en 2023, le nombre d’attaques par ransomware est en diminution, le chiffrement malveillant des données est en forte hausse.

Dans le secteur de la santé, 80% des attaques ont un but financier et 10% sont faites dans un but idéologique.

ADISTA est un opérateur de données de santé hébergées dans 14 Datacenters certifiés ISO 27001, répartis sur toute la France. L'entreprise compte un millier de collaborateurs et 50 000 clients. Elle propose Oppidum, une solution de Clouds d'entreprises et des services d'infrastructure.

ADISTA propose des audits et des services de migration vers le Cloud, en s'appuyant sur le SOC opéré par Cyberprotect, société lyonnaise rachetée par ADISTA, pour protéger les clients qu'il héberge.

Cyberprotect est un pure player du SOC avec 19 ans d'expérience en cybersécurité. Quatre milliards d'évènements sont traités chaque semaine avec un temps de réponse inférieur à 30 minutes.

C'est l'heure de la pause !

Encore de nouveaux amis, encore des échanges de cartes de visite. On me demande ce qu'est cette épinglette, avec un sphinx devant une grille et derrière deux clés entrecroisées, que je porte à ma boutonnière. C'est l'insigne de l'ARCSI, Association des Réservistes du Chiffre et de la Sécurité de l'Information, et plusieurs ARCSIstes, comme Vincent Trély et Cédric Cartau, sont présents.

Etablissements de santé : protégez les données de vos patients tout en innovant grâce au cloud

Avec Mathieu JEANDRON, responsable des équipes techniques pour le secteur public, et Marko MAKSIMOVIC, responsable souveraineté numérique – tous deux d'AWS France (Amazon Web Services). Leur nom de domaine se termine d'ailleurs par « .fr » : amazon.fr

Les données confiées en France à AWS restent en France et AMAZON n'a pas accès aux clés de chiffrement.

Quel est l'intérêt pour les services SAS d'utiliser les clouds d'Amazon ?

1. Rester au niveau « état de l'art » avec une infrastructure de calcul mondiale évolutive, fiable et sécurisée
2. Bénéficier d'une sécurité pour un coût marginal
3. Utiliser des services managés d'où allègement des charges
4. Compter sur une standardisation et une automatisation
5. Pouvoir observer et auditer en continu

AWS explique n'avoir jamais communiqué les données qui lui sont confiées, situées hors des USA, malgré les requêtes qui ont pu lui avoir été ordonnées par les autorités. Et ceci est un engagement contractuel.

AWS propose une sécurité « by design » avec de la traçabilité : Chaque évènement est automatiquement journalisé. La conformité à la politique de sécurité est automatisée**.**

Le Plan de Reprise d'Activités (AWS Elastic Disaster Recovery) réduit les temps d'arrêt et les pertes de données par une restauration rapide et fiable des applications sur site et dans le cloud. La gestion de la sécurité des infrastructures des clouds d'AWS est vérifiée par des auditeurs tiers indépendants et les rapports d'audit sont consultables.

52 services AWS sont certifiés selon le code de conduite CISPE (Cloud Infrastructure Service Providers Europe) approuvé par la CNIL, en conformité avec les exigences de l'article 28 du RGPD (Règlement Général Pour la Protection des données à caractère personnel).

Et par engagement contractuel, AWS ne déplace jamais les données qu'on lui confie hors d'une Région. Ceci est vérifié par des auditeurs indépendants. Il y a 32 Régions AWS dans le monde, dont 8 en Europe et la France est une de ces Régions.

L'hyperviseur AWS Nitro protège et vérifie en permanence les matériels et les logiciels, déchargeant ainsi les ressources de virtualisation vers du matériel et des logiciels dédiés. Il

garantit que même les employés d'AWS ne peuvent pas accéder aux données clients dans les machines virtuelles.

AWS Key Management Service permet de créer et de contrôler, de façon centralisée, les clés de chiffrement / déchiffrement qui protègent la confidentialité des données. Ce chiffrement présente peu d'impact sur les performances. Le paiement se fait à la consommation et ne coûte que quelques dollards par mois. Les employés d'AWS n'ont pas accès aux clés de chiffrement et de déchiffrement des données confiées. De plus l'offre AWS KMS External Key Store permet de protéger les données des clients à l'aide de clés de chiffrement stockées dans un système de gestion de clés externe qui est donc sous leur contrôle.

Anticipez les risques d'attaques sur les applications critiques en les externalisant dans un cloud souverain certifié HDS : retour d'expérience !

Avec Julien BIANCHI, directeur technique et Alain FAIVRE, directeur commercial d'OSPI (anciennement Groupe PSIH)

La technique n'est pas le seul critère à prendre en compte.

Julien BIANCHI souligne que les applications utilisées dans le domaine hospitalier sont très critiques et une altération de leurs services présente un fort impact sur la continuité des soins. En cas d'incidents, le redémarrage est long et l'impact économique est loin d'être négligeable.

Avec la Fondation Cognacq-Jay, OSPI propose de sécuriser les process informatiques, de protéger les applications les plus critiques en adaptant les ressources aux besoins clients tout en leur permettant de maîtriser les coûts.

Pour maîtriser les enjeux suite à des cyberattaques, en tenant compte des contraintes métiers, OSPI propose un mode dégradé et un plan de reprise d'activité.

En se projetant dans le futur, OSPI fait un premier pas vers l'unification des systèmes hospitaliers de santé en fusionnant les diverses applications, en jetant des ponts vers les autres services hébergés du catalogue et en proposant des sauvegardes.

L'aspect humain est également pris en compte car la technique n'est pas le seul critère à considérer.

OSPI, né du rapprochement entre le groupe PSIH, hébergeur de données de santé et Collective Thinking, spécialisé dans l'intelligence artificielle et dans l'analyse des données, est dédié 100% à la cybersécurité des établissements de santé. C'est une entreprise 100% française.

André Zaphiratos, DSI de la fondation Cognacq Jay nous explique pourquoi sa fondation a choisi de faire gérer l'hébergement de ses données chez OSPI.

OSPI ambitionne d'améliorer le pilotage et le codage des différentes activités des établissements hospitaliers, la recherche clinique et le suivi de la qualité des soins. Son projet est de devenir un acteur majeur des données hospitalières et de l'intelligence artificielle dans le domaine de la santé. La société emploie une centaine de salariés à Paris et à Lyon.

Spécialisé dans la santé et le médico-social, OSPI se veut être un partenaire de confiance dans des services dédiés à un cloud souverain avec de la transparence et une chaîne de sous-traitants contrôlée, en respectant le cadre légal.

La technique n'est pas le seul critère à prendre en compte !

Les 4 pitchs

Quatre sociétés vont se succéder, avec un temps de parole de 8 à 10 mn chacune.

1) Les capacités de détection de la plateforme Cybereason

Avec Benjamin LEGRAY – Ingénieur Système chez CYBEREASON

Des agents au niveau des Endpoint.

CYBEREASON revendique le déploiement et la sécurisation de plus de 500 000 agents logiciels au niveau des endpoints, dont 200 000 agents en France sur les SI des centres hospitaliers publics. Ils communiquent avec un moteur de recherche de menaces hébergé dans le cloud. L'entreprise gère les EPP (plateformes de protection des terminaux) et les EDR Nouvelle Génération avec un agent unique. Cet EDR est compatible avec tous les EPP du marché et propose une remédiation intelligente et multi machines avec un faible taux de faux positifs.

Forte de plus de 1000 employés, CYBEREASON est passée d'entreprise visionnaire à ses débuts, à un des leaders dans le cadran du Gartner.

La base de connaissance MITRE ATT&CK accorde à CYBEREASON un statut de top performer pour sa couverture des solutions sous Linux.

2) La protection, la surveillance et la réaction aux cyberattaques : au-delà de la bataille des acronymes (EDR, NDR, XDR, ZTNA…)

Avec Hasina BESSE-RAMASINIRINA, directrice du pôle achat réseaux télécoms, et Vincent BRANGER – Consultant au RESAH

Protéger c'est bien, surveiller c'est mieux.

Au-delà de la bataille des acronymes, EDR, NDR, XDR, CDR, FDR, ADR, avec DR qui signifie Détection and Response, il s'agit avant tout de protection et de surveillance pour réagir aux cyberattaques.

Le RESAH est un centre de ressources et d'expertises qui propose des achats responsables autour du Endpoint Detection & Response, pour les établissements de santé. Le RESAH fournit aussi un catalogue de formations et possède un centre d'expertise.

Resah est un groupement d'intérêt public national (GIP) dont l'objectif est d'appuyer la mutualisation et la professionnalisation des achats. La centrale d'achat du Resah est accessible aux entreprises du secteur sanitaire, médico-social ou social. Leur catalogue qui comprend 11 familles d'achats et 1000 fournisseurs est accessible à plus de 2600 bénéficiaires.

3) Pourquoi changer d'EDR ne sert à rien ?

Avec Frédéric JUBERT - Directeur Commercial Secteur Public chez HARFANGLAB

HarfangLab est un logiciel de cybersécurité qui analyse et détecte les menaces et activités suspectes sur les terminaux en bout de réseau (endpoints) en Intégrant des systèmes d'apprentissage automatique.

Avec cette solution, les RSSI n'ont plus à choisir entre la protection de leur SI et la maitrise de leurs données, ni entre la souveraineté et la cybersécurité

Pourquoi s'équiper d'une telle solution ? Pour faire des économies ? Pour obtenir de meilleures performances ? Pour rationaliser les coûts ?

Oui, mais il faut aussi prendre en compte la gestion projet et les coûts cachés.

4) Détection, identification et sécurisation des équipements connectés dans un environnement médical

Avec Jérôme BOURGUET – Ingénieur avant-vente chez ARMIS

C'est la plateforme qui doit s'adapter à nous, pas l'inverse.

ARMIS est une plateforme de sécurité pour les équipements connectés. Elle découvre les actifs de l'entreprise et fournit des renseignements sur les appareils managés, et non managés, IoT, industriels et médicaux. Elle identifie les risques et les lacunes du SI et réagit aux évènements, sans agents et en temps réel.

Avec une base de connaissances alimentée par l'IA, la plateforme apprend les comportements normaux et anormaux de 3 milliards d'équipements, ce qui lui permet d'atténuer les menaces de manière proactive. C'est une solution sans agents qui s'intègre à un SOC.

La plateforme Armis Asset Intelligence fournit une réponse orchestrée aux cybermenaces en temps quasi réel tout en surveillant l'utilisation des équipements cliniques. Elle améliore la productivité et la résilience de l'organisation.

Et la dernière intervention : « Il y a 1 an : la cyber attaque ! »

Avec Gilles CALMES - Directeur Général et Patrice GARCIA - DSI - CH Sud Francilien
Interviewés par Auriane LEMESLE et Vincent TRELY

« Une cyberattaque, on a beau s'y préparer, tant qu'on ne l'a pas vécue, on ne sait pas ce que c'est. »

Il y a un an, le ciel leur tomba sur la tête…

Dans la nuit du samedi 20 au dimanche 21 août 2022, le Centre Hospitalier Sud Francilien de Corbeil-Essonnes subissait une cyberattaque et perdait ses data et son réseau. Il s'ajoutait à la longue liste des Centres Hospitaliers touchés par un rançongiciel. Ses applications, ses informations d'imagerie médicale et d'autres fichiers stockés étaient devenus inaccessibles.

Le maliciel avait chiffré ces données, les rendant illisibles. Plus possible, par exemple, de gérer les admissions par voie numérique.

Mais il fallait continuer à donner les soins aux patients, à évacuer vers d'autres hôpitaux les cas les plus urgents, à accueillir, à facturer, mais comment ? avec quoi sans bureautique, sans imprimantes ?

Déclencher le plan blanc, cela s'imposait et rappeler le personnel de maintenance indispensable et les soignants, mais comment faire sans possibilité d'utiliser les dispositifs informatiques prévus à cet effet ? Et c'était dans la nuit de samedi au dimanche… A la hâte, des petits papiers ont été glissés sous les portes du personnel soignant, administratif et technique pour que le lundi matin, ces employés du CHSF les trouvent et soient informés du désastre.

Effectivement, la sauvegarde sur papier a du bon, quand elle est faite, car il n'y a plus d'accès aux annuaires électroniques…

Déclencher le PCA – Plan de Continuité d'Activité – est l'une des premières mesures à laquelle on pense, car il faut continuer à travailler en mode dégradé et même fortement dégradé. Pour le PRA, Plan de Reprise d'Activité, ce sera pour plus tard, mais hélas bien plus tard, il faudra compter 3 mois.

Pour l'instant, le personnel hospitalier prend son stylo et on écrit, feuilles après feuilles, et il en utilisera beaucoup. Nostalgie des écrans et des claviers, avec lesquels tout semblait facile ? Bien sûr mais ils sont devenus inopérants.

Une plainte a été déposée et une enquête a été ouverte. L'ARS, la CNIL et l'ANSSI ont été informées.

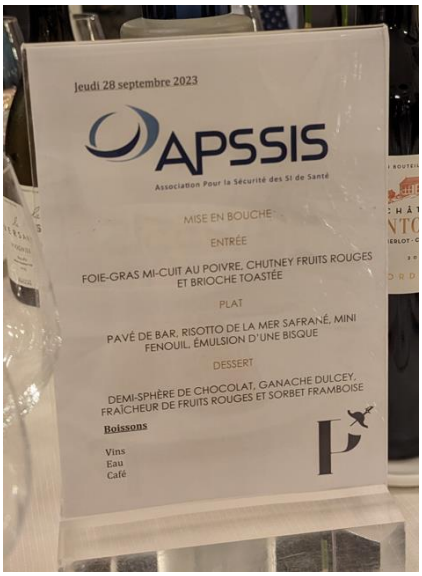
Aujourd'hui, le CHSF fonctionne mais les effets se font encore sentir. Evidemment tous se sentent maintenant concernés par la sécurité du numérique et par la résilience des systèmes hospitaliers. Avant, le bon fonctionnement de l'informatique allait de soi, maintenant la conscience a été prise par le personnel qu'il fallait veiller à la sécurité des datas et des applications, que des guides de bonnes pratiques pour utiliser les outils logiciels sont indispensables et doivent être lus, que des exercices de gestion de crise doivent être pratiqués avant la prochaine cyberattaque.

Une rançon de 10 millions de dollars, demandée par les attaquants pour restituer les données chiffrées a-t-elle été payée ? La réponse est non.

En conclusion, les bonnes pratiques, car ce genre d'attaque va se reproduire, et le CHSF en a subi et bloqué d'autres depuis, sont de cartographier son SI pour savoir où se trouvent les ressources les plus critiques et donc à protéger en priorité, pratiquer des audits réguliers, souscrire une assurance qui couvre les risques cyber. Les solutions métiers les plus prioritaires sont la biologie, la pharmacie et l'imagerie.

Les 3 800 professionnels de santé du CHSF seront devenus encore plus riches et plus performants après la gestion de cette crise majeure

Le dîner pris au 1er étage de la Maison des Polytechniciens



Voilà la table où j'ai eu le plaisir de dîner (ma place est vide sur la photo puisque je suis en train de la prendre avec mon smartphone), entre Charles Blanc-Rolin, vice-président de l'APSSIS et Béatrice Bérard, Officier de Sécurité des Systèmes d'Information des HCL (Hospices Civils de Lyon) et également vice-présidente de l'APSSIS.

A cette table vous remarquerez Auriane Lemesle, secrétaire générale de l'APSSIS, entre le président Vincent Trély à sa droite et Patrice Garcia, le DSI du Centre Hospitalier Sud Francilien. Gilles Calmes - Directeur Général de ce Centre Hospitalier est assis à droite de la table, à côté de la représentante des HCL.

Et la carte du menu est à gauche de ce texte 😊

Les partenaires des 3èmes Rencontres SSI Santé de l'APSSIS