

Lettre des "Lundi de la cybersécurité" n° 69

Le facteur humain dans la cyber protection allié ou adversaire ?



Le facteur humain dans la cyber protection, allié ou adversaire ?

Organisateurs



Pr Ahmed Mehaoua
Université Paris Cité

Par webinaire Zoom

Lundi 15 avril
18h00-20h00



Alain
Ducass



Virgile
Augé



Béatrice Laurent



Gérard Peliks

Virgile Augé est un de mes anciens élèves de la promotion 2021 du MBA Management de la Cybersécurité de l'Institut Léonard de Vinci. J'ai été son « tuteur pédagogique » pour sa thèse professionnelle qui terminait son cycle d'étude. Quand il m'a proposé le titre qu'il souhaitait donner à sa thèse : « **Réduire la variable PFH dans la constante PEBKAC** », la première impression que j'ai eue a été : « Je ne connais pas ces protocoles, ce sera pour moi l'occasion de les apprendre ». Mais quand il m'a explicité ce qu'il entendait par **PFH** et **PEBKAC**, je me suis dit : « *Non, il ne va pas oser!* ». Mais oui il a osé, et je l'ai même encouragé ! Et la thèse qu'il a soutenue a été un vrai bonheur. Jamais je n'avais trouvé chez un élève un si grand enthousiasme et une thèse professionnelle si bien construite !

Mais PFH, PEBKAC, c'est quoi au juste ?

PFH : Putain de Facteur Humain.

PEBKAC : Problem Exists Between Keyboard And Chair.

Pour que ce titre passe sans problème, il l'a renommé : "*comment gérer les risques numériques d'une structure en intégrant plus efficacement l'humain dans sa protection*".

Vous saisissez le personnage : Une grande technicité et beaucoup de compétences, mêlées à de l'humour. Il sait passionner son public !

Voici un court résumé de ce qu'il a écrit au début de sa thèse :

La transformation digitale des entités publiques et privés est une nécessité qui s'impose à tous et qui se caractérise par un environnement hautement volatile, incertain, complexe et ambiguë.

Dans ce cadre, l'utilisateur du système d'information et de ces données devient une des variables d'une nuisible alternance. Il synthétise en effet le point de bascule entre, d'une part son action positive dans la création de richesse ou d'efficacité via ces transformations et, d'autre part, dans son action potentiellement négative vis-à-vis de la protection de l'infrastructure utilisée et de sa data.

Quelle est la place du décideur et de l'utilisateur dans la protection du système d'information ainsi que les méthodes à employer pour favoriser et développer son rôle de première vigie et de premier rempart plutôt que de subir ses erreurs ou mauvaises actions, bien souvent involontaires mais toujours mises à profit par les délinquants 2.0 ?

Je me suis dit : Celui-là, j'ai envie d'en faire profiter les participants à un de nos « Lundi de la Cybersécurité ». Ce sera pour le mois d'avril 2024.

Un autre expert de très haut niveau a demandé à intervenir dans un de nos « Lundi de la Cybersécurité » sur un sujet similaire. Le problème était que le premier Lundi libre était au dernier trimestre 2024. Mais, si Virgile Augé acceptait, pourquoi ne pas proposer à ce nouvel intervenant d'animer avec lui ce Lundi de la Cybersécurité ? Virgile a accepté avec plaisir. Ce deuxième intervenant est Alain Ducass, un X-Mines.

Je donne la plume aux deux intervenants

Virgile Augé

L'humain dans le cyber, finalement, allié ou adversaire ?

1/ Mise en situation : nous en sommes où sur le front des cyber-attaques ? (guerre économique, asymétrique et systémique —> Accentuation du niveau de risque avec les tensions internationales actuelles et l'amélioration des process délinquants.

2/ L'Humain dans le cyber, cela veut dire quoi finalement ? Sur ce thème, je souhaite remettre l'église au milieu du village. A la base, les systèmes d'information aident l'humain à améliorer sa productivité et à créer plus de valeur. Il est à son service.

C'est pour moi un non-sens de dire que l'humain est un maillon faible alors qu'il est le principal destinataire des capacités de cet outil de travail.

Nous sommes là face au cœur du sujet : Si nous prenons pour argent comptant la phrase "l'Humain est le maillon faible de la cyber", alors il faut aller au bout du raisonnement et se poser la question ultime : **Doit-on se passer de l'Homme dans l'utilisation d'un SI afin qu'il**

soit totalement safe ? C'est pour moi le véritable point. Bien évidemment je réfute cette logique poussée à l'extrême et je propose une autre vision qui permettra, enfin, et je l'espère, à considérer l'humain plutôt comme une "*Première vigie*" et **le** un "*Dernier rempart*".

3/ Quelle philosophie (oui nous allons faire un peu de philosophie ;-), quelles possibilités, quels intérêts, quels gains, cette vision plus positive implique-t-elle ?

- Une meilleure interaction Homme - Machine —> On travaillera moins mais mieux avec un S.I ?
- Une économie sur les usages implique une économie sur les dépenses en énergie et en capacité de stockage (relire l'enfer numérique, voyage au bout d'un like de Guillaume Pitron)
- Une interrogation sur ce que l'on fait réellement comme travail avec un S.I. Par exemple, les invitations sur google agenda, Outlook et autre i.calendar.... Est-ce que cela est vraiment et finalement super utile (en plus d'être dangereux en termes de sécurité économique) ?
- ...

4/ Quelles méthodes possibles, quels instruments ou action ?

- Tout va très vite, tout s'accélère sans cesse. Il est donc temps de ralentir à défaut de ne plus rien maîtriser (et donc de perdre quoi qu'il arrive). ~~Donc~~ Il est temps de faire une pause et de redéfinir son travail et la valeur qu'apporte le SI dans ce travail. Il est temps de redonner du sens. **Donc CARTOGRAPHIE et DEFINITION de son travail et de ses outils de travail.**
- En fonction de cette cartographie et de cette définition, comment peut-on déterminer les cloisonnements à faire dans le S.I ? **Donc allons-nous vers un permis de naviguer dans le S.I de la structure ?** Si oui, quelles seraient les implications pour le DSI et le RSSI ?
- En fonction de ce cloisonnement, nous poserons quelques questions pour l'humain.

Alain Ducass

"De la cyber prévention à la conduite du changement"

Alain nous présentera les 7 couches de l'âme humaine, puis nous donnera des conseils :

1. Passer d'une posture réactive à une posture avisée
2. Avant la cyber protection il faut la cyber prévention
3. La conduite du changement au service de la cyber protection

Il expliquera comment une personne ou une entreprise adopte une posture réactive ou une posture avisée et soulignera la nécessité de la cyber prévention comme socle de la cyber protection.

Il conclura sur les principaux outils de conduite de changement, de gouvernance partagée et de médiation agile permettant aux entreprises de mobiliser les hommes et les femmes de l'entreprise et de son écosystème pour construire ensemble un climat de cyber prévention.

Je reprends la plume

Qui est Virgile Augé ?

Virgile Augé travaille dans la protection des personnes et des biens matériels et immatériels sous les aspects Techniques, Humains et Organisationnels.

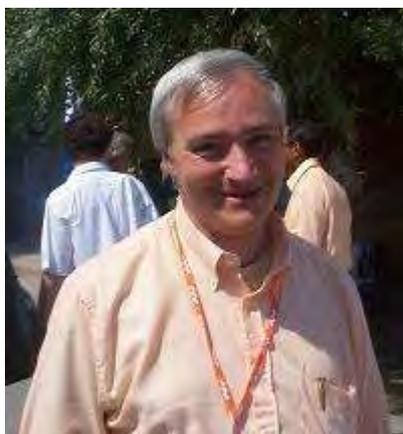
Il s'est progressivement spécialisé dans « l'acceptation » par les collaborateurs, les visiteurs et les prestataires des sites sur lesquels il est missionné des mesures de sûreté mises en place ainsi que sur le design, la fluidité et l'aspect économique de ces dernières.

Il n'est finalement « de richesses que d'Homme » dans sa méthode de travail.

Cette pratique, il la met en place tant dans ses projets sûreté que dans ceux liés à la cyber protection.



Qui est Alain Ducass ?



Alain Ducass, ingénieur polytechnicien, mineur devenu démineur, à savoir catalyseur de changement (coach, médiateur, formateur) présentera les couches de l'âme humaine face aux couches ISO de l'informatique.

Cet ingénieur en chef des instruments de mesure, était précédemment délégué régional adjoint de l'ANVAR, chef du service de l'action économique du Conseil Régional d'Ile de France et directeur de l'action régionale et internationale de l'ADEME.

Il a été rédacteur en chef du courriel du club-telecom pour le développement de la société de l'information sur les territoires et dans les entreprises et premier président du réseau R@CINES des réseaux d'animation de la compétitivité numérique des entreprises.

Demande d'inscription pour le Lundi de la cybersécurité du mois d'avril 2024

Lundi 15 avril, à partir de 18 h 00, par visio-conférence Zoom.



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

Les demandes d'inscriptions sont à adresser à :

beatricelaurent.CDE@gmail.com

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants. Si vous voulez être ajoutés à ma liste de distribution de mes lettres des « *Lundi de la cybersécurité* » mensuels, demandez-le nous.

Et bien entendu, si vous vous inscrivez pour assister à notre évènement, soyez connectés le lundi 15 avril, dès 18 h 00. La salle d'attente Zoom sera ouverte aux alentours de 17 h 00. Prévenez-nous, dès que possible si vous êtes inscrits mais avez un empêchement qui ne vous permet pas d'assister à ce webinaire.

Quelques minutes avec une organisation : Hexatrust



Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé de l'intervenant et la session questions / réponses, autour de 19 h 15, nous donnons pour une dizaine de minutes la parole à une organisation qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

L'intervenant du Lundi d'avril sera **Jean-Noël de Galzain** et l'organisation dont il sera question sera **Hexatrust**.

Hexatrust, est une association loi 1901 qui regroupe et fédère des start-up, des PME et des ETI, éditeurs de logiciels, fournisseurs de solutions, sociétés de services champions français & européens de la cybersécurité, du cloud de confiance. Cette alliance répond aux besoins des Entreprises, des Administrations et des organisations de toutes tailles, publiques et privées, soucieuses de bénéficier d'offres innovantes d'origine française, couvrant l'ensemble de leurs besoins en matière de sécurité informatique.

H E X A T R U S T
CLOUD CONFIDENCE & CYBERSECURITY

Jean-Noël de Galzain est le président de cette association.

Le coin des « Lundi de la cybersécurité » précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements et des comptes-rendus, écrits par Clarisse Véron, élève du master1 « Cybersécurité et e-Santé de l'université Paris Cité sur le web de l'ARCSI en https://www.arcsi.fr/evt_passes.php.

Mais attention, il n'est pas garanti qu'il y aura ces documents pour chacun de nos « Lundi ». Donc il est conseillé de les suivre par Zoom.

Le coin coin du facteur humain dans la cybercriminalité

Question posée à Gemini IA Générative de Google : *Comment intervient le facteur humain dans le problème de cybercriminalité qui existe entre la chaise et le clavier ?*

Voici la réponse reçue :

Le facteur humain dans la cybercriminalité : Entre la chaise et le clavier

Le facteur humain joue un rôle crucial dans la cybercriminalité, souvent considéré comme le "maillon faible" de la sécurité informatique. Entre la chaise et le clavier, l'utilisateur représente une cible de choix pour les cybercriminels qui exploitent ses faiblesses psychologiques et ses erreurs involontaires.

Voici quelques exemples de l'intervention du facteur humain dans la cybercriminalité :

1. Ingénierie sociale :

- **Phishing et hameçonnage :** Les cybercriminels manipulent l'utilisateur en lui envoyant des emails, SMS ou messages sur les réseaux sociaux imitant des institutions légitimes pour l'inciter à divulguer des informations sensibles ou à télécharger des logiciels malveillants.
- **Attaques par appât du gain :** Des offres alléchantes ou des messages d'urgence incitent l'utilisateur à agir impulsivement sans réfléchir aux risques potentiels.

2. Erreurs humaines :

- **Mauvaise gestion des mots de passe :** Utilisation de mots de passe faibles ou identiques sur plusieurs plateformes, partage de mots de passe avec des tiers, ou clic sur des liens suspects

OK, mais quelle différence entre Phishing et hameçonnage ?

Gérard

Lundi de la Cybersécurité du mois de mai

lundi 13 mai 18h-20h

en distanciel par Zoom

Bug Bounty et tests de pénétration

Intervenant Yassir Kazar, CEO de Yogosha