Lettre des "Lundi de la cybersécurité" no 40

Le Cyber Risk Index et les Cyber notations

Le Cyber Risk Index et les Cyber notations ?

Le Lundi de la cybersécurité de **décembre 2018**, qui s'appelait encore à l'époque un Lundi de l'IE, s'est déroulé en présentiel à Télécom Paris. L'intervenant **Pierre-Luc Réfalo** nous avait très intéressés et même enchantés par son intervention sur le thème « *Cyber Sécurité versus Sécurité Numérique - Le poids des mots - Le choc des nombres ».* Ce fut un très grand évènement. Certaines phrases de Pierre-Luc, comme celle avec laquelle il a caractérisé le numérique face aux cyberattaques aujourd'hui de plus en plus nombreuses, de plus en plus sophistiquées, dont le cyberespace fait l'objet depuis le milieu du siècle dernier, m'avaient marqué. Citons entre autres : « *Les trente glorieuses, suivies des trente piteuses* ».

Nous avons invité Pierre-Luc Réfalo à revenir sur scène pour notre « Lundi de la cybersécurité » d'**octobre 2021** sur un nouveau thème : « **Le Cyber Risk Index et les Cyber notations** ».

Pierre-Luc a posté sur LinkedIn une série de quatre articles sur le sujet « *Toute chose est nombre* ». Le premier des articles se trouve en : https://www.linkedin.com/pulse/la-cybers%C3%A9curit%C3%A9-par-les-nombres-episode-0-pierre-luc-refalo/

A notre Lundi de la cybersécurité d'octobre, Pierre-Luc Réfalo répondra à la question suivante *: « Sur la base de quelles métriques et avec quels processus, une entreprise doit-elle disposer de sa propre analyse et définir un Cyber Risk Index spécifique et pertinent dans son contexte ? ».*

Je donne la plume à l'intervenant :

L'univers est régi par les nombres. Le monde de la cybersécurité n'échappe pas à la règle !

Chaque jour, chaque individu est assailli de données chiffrées sur la pandémie, sur la situation économique, sur les performances de son entreprise, le nombre de « post », de « retweet » et de « Like », etc.

A quoi servent-elles ? Simplement informer ? Ou faire peur ? Aider à comprendre ? Et faire réagir ? Orienter les décisions ? Voire se faire plaisir ?

Depuis que la sécurité informatique est née (en gros depuis Turing et Enigma, puis avec le PC et Internet), les professionnels de la cybersécurité ont progressivement été assaillis de chiffres et de statistiques démontrant la croissance exponentielle des codes malveillants et des vulnérabilités connues pour n'en citer que deux.

Parallèlement, le marché de la cybersécurité s'est développé pour dépasser les 100 milliards de dollars en 2017. Avec une répartition 50/50 entre produits et services (selon les données du Gartner Group) et surtout une croissance soutenue à 2 chiffres.

Les deux nouveaux facteurs de la cybersécurité

Désormais, l'accent est mis sur 2 nouveaux facteurs : d'une part, les impacts économiques des cyber-attaques qui se sont aussi envolés au-delà de dizaines voire de centaines de millions d'euros (mettant en danger la vie même d'entreprises, de leurs salariés et de citoyens) et d'autre part, la pénurie de professionnels aguerris et engagés pour lutter contre des groupes cybercriminels mafieux comme étatiques.

Enfin, ces derniers mois ont mis l'accent sur la vulnérabilité d'un écosystème numérique interconnectant entreprises et individus d'un côté, fournisseurs de services numériques et de technologies d'autre part (cf. attaque des outils de SolarWinds). L'attaque, dûment préparée, ne vise pas directement sa cible mais compromet d'abord les intermédiaires…

Dans ce contexte, la cybersécurité n'est plus un sujet de discussion pour les dirigeants ! Mais que faire, au-delà des fondamentaux, de la prise de conscience, à la nomination d'un (e) RSSI et de la mise en œuvre des « bonnes pratiques » ? Comment maintenir une situation « sous contrôle » tout en transformant et s'adaptant à un environnement évolutif et de plus en plus risqué ? Comment prendre des décisions fiables et sereines sans succomber à la mode du moment et au marketing de la peur ?

Des données fiables

Les dirigeants ont besoin de données fiables et simples. Pour comprendre et décider. C'est ainsi que 2 méthodes de notation de la cybersécurité se sont développées ces dernières années. Pour faire simple :

1. *Quelle notation de la Gouvernance d'une entreprise dans une logique ESR (Environmental & Societal Responsibility) ? Ecovadis, Cybervadis et les Dow Jones Sustainability Indexes par exemple, mais les Assureurs ont aussi leur propre démarche.*
2. *Quelle notation des entreprises et de leurs fournisseurs, basée sur les vulnérabilités de leur exposition sur Internet ? Security ScoreCard, Bitsight, RiskRecon et d'autres solutions répondent à la question, mais des cabinets de conseil créent aussi leurs propres solution (Almond pour n'en citer qu'un).*

Elles ont le mérite d'exister mais posent de grandes questions conceptuelles et pratiques.

Une entreprise ne doit-elle pas disposer de sa propre analyse et définir un Cyber Risk Index spécifique et pertinent dans son contexte ? Associant vues « interne » et « externe », aspects techniques et humains, intégrant les incidents et des éléments « temporels », des tendances. Si oui, sur la base de quelles métriques et avec quels processus ?

Cette conférence des « Lundi de la Cybersécurité » proposera une vision des problématiques de notation « cyber » et des approches possibles facilitant les prises de décision pour une meilleure gouvernance des cyber-risques.

Je reprends la plume

Qui est Pierre-Luc REFALO, notre intervenant ?
Vice-Président – Capgemini Group Cybersecurity

Pierre-Luc REFALO reporte au Chief Cybersecurity Officer de Capgemini et dirige une équipe et des programmes de gestion des cyber risques. Il contribue à impliquer les dirigeants, les équipes informatiques et les métiers afin de faire de la sécurité un avantage compétitif. Ses activités couvrent : la gestion des Cyber Risks, les politiques et standards, la communication & sensibilisation, les projets globaux et la conformité (NIS, GDPR, ISO, etc.).

Il a dirigé les offres et activités de Conseil « cybersécurité et protection des données » de Capgemini-Sogeti (2013-2018) pour accompagner les

Directions générales et les professionnels de la sécurité dans le renforcement de leur gestion des risques numériques, en particulier pour la protection des données sensibles / personnelles et la résilience des infrastructures critiques. Il a également défini et lancé les services RGPD de Capgemini.

Impliqué dans la sécurité numérique depuis 1990, il a travaillé pour différents cabinets de conseil et a été Directeur du Programme Sécurité de l'information de SFR (1997-2002). Il a ensuite créé et développé des sociétés de conseil dédiées à la gouvernance des risques numériques et à la sensibilisation / formation des dirigeants, métiers, utilisateurs et informaticiens.

Il est aussi conférencier international et formateur dans plusieurs Mastères Cybersécurité. Il a publié 2 ouvrages de référence « Sécuriser l'entreprise connectée » (2002) et « La Sécurité Numérique de l'entreprise » (2012), primé au Forum International de la Cybersécurité en 2013.

Demande d'inscription au Lundi de la cybersécurité d'octobre

Nos « Lundi de la cybersécurité » **sont gratuits. Le prochain** se fera encore par **visioconférence Zoom,** webinaire organisé par Ahmed Mehaoua, professeur à l'université de Paris. Nous verrons, suivant la situation sanitaire quand cet évènement pourra se faire aussi, en parallèle, en présentiel à l'université de Paris, rue des Saints-Pères Paris 6^{e} (quartier de Saint-Germain des Prés).

Demandez votre inscription, par courriel, et vous recevrez un hyperlien personnel vers la visioconférence Zoom un peu avant le jour de l'évènement. Les demandes d'inscription sont à adresser à : **beatricelaurent.CDE@gmail.com** avec « ***Inscription 18/10*** » dans l'objet **ET** dans le corps du mail, si vous n'êtes pas encore un habitué de nos « Lundi de la cybersécurité », quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité.

L'organisation qui sera mise en valeur dans notre Lundi d'octobre

Depuis le Lundi de juin, entre la fin du discours de l'intervenant et le début des questions des participants, nous mettons en avant, pour quelques minutes, une organisation qui va dans le même sens que nos « Lundi de la cybersécurité ». En juin ce fut l'association **ARCSI**, en septembre le **CyberCercle**, en octobre ce sera le **CEFCYS**. La présidente du CEFCYS, Nacira Salvan, nous présentera les actions de son organisation qui promeut la place des femmes dans les métiers de la sécurité du numérique.

Retour sur le Lundi de la cybersécurité du mois de septembre

Quel évènement ce fut ! Un intervenant en or, à qui nous avons décerné le trophée des **PI d'Or** des "Lundi de la cybersécurité" au passage du 314e inscrit. Cet intervenant incroyable, **Bernard Barbier**, nous a décoiffé sur un sujet redoutable : **la cyber coercition**. Vous pouvez télécharger **ses slides** et visualiser **le replay** de son intervention à partir du web de l'**ARCSI** - **A**ssociation des **R**éservistes du **C**hiffre et de la

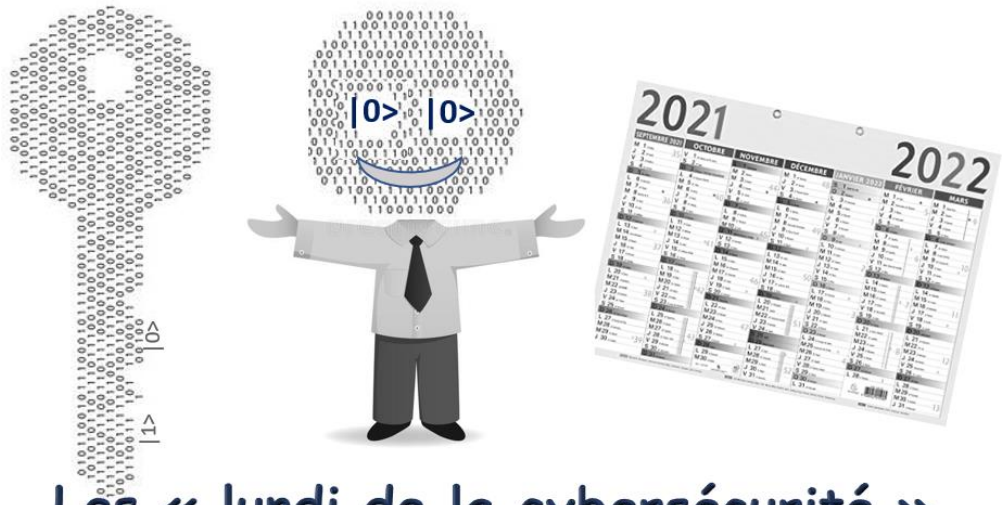
Sécurité de l'**I**nformation en : https://www.arcsi.fr/evt_passes.php**.** Ce replay sur la chaîne DailyMotion de l'ARCSI est limité à une heure sur les deux heures de cet évènement.

Le replay complet du Lundi de la cybersécurité de septembre

le replay complet des deux heures de l'évènement est accessible en :
https://u-paris.zoom.us/rec/share/ufmyNe79dlF2fG1YZT8Vhrc0OY3W0Ky7Yw9ZVvKdO_8BB1TGlfU9Cd7TEw4WX4Lo.uqlmPbtQ15mxgcT6
avec le code **@#yu=a2stC**
Passez la première vidéo de 9 secondes, le vrai replay de deux heures est la deuxième vidéo.

Ce Lundi de la cybersécurité de septembre restera dans les mémoires des "Lundi de la cybersécurité", comme le restera certainement celui d'octobre, objet de cette lettre.

A bientôt
Take care, Stay safe & tuned
Gérard Peliks



Les « lundi de la cybersécurité » mensuels

Lundi de la cybersécurité de novembre
15 novembre

« Crise systémique et Etat stratège »

avec Bernard Besson