Lettre des "Lundi de la cybersécurité" no 57

Au secours, je suis victime d'un hacker !

Au secours, je suis victime d'un hacker !

Il est entré dans votre Système d'Information, peut-être y est-il encore ? Votre organisation avait pourtant analysé les risques, conformément à la norme ISO 27005 et à la méthode eBios ou Mehari. Vous aviez cartographié vos informations. Vous avez identifié les gisements d'informations sensibles sur lesquelles une attaque aurait les plus graves conséquences. Ces informations étaient, pensez-vous, bien protégées.

Vos indicateurs ont reporté l'alarme, votre cockpit de sécurité centralisé affiche des écrans d'alerte. Oui, il est là le hacker et c'est sans doute loin d'être un hacker éthique. Quelle est la conduite à tenir ? Convoquer une cellule de gestion de crise ? Activer le Plan de Continuité d'Activité ? Avertir les instances comme la CNIL et l'ANSSI suivant ce qu'est votre organisation et si des données à caractère personnel ont été exfiltrées ? Porter plainte immédiatement auprès de la police ou de la gendarmerie ?

Non ! N'éteignez pas vos postes de travail, vous détruiriez vos traces, mais isolez la partie du réseau où le hacker peut se trouver ou avoir encore accès de l'extérieur. Et s'il n'y a qu'un seul de vos postes de travail qui est touché, attention à l'expansion latérale de l'attaque vers d'autres postes ou serveurs de votre réseau interne. Face à ce type d'agression, qu'aurait fait un expert en cybersécurité avec beaucoup d'expérience comme Lionel Mourer ?

Je donne la plume à l'intervenant

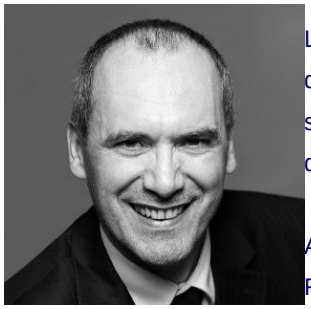
La pandémie et les cyberattaques répétées ont montré l'importance de se préparer, notamment via la gestion de crise et les tests de robustesse.

L'évolution des services numériques, le télétravail exceptionnel ou encore le recours à l'externalisation augmentent la surface d'exposition des organisations. Les réglementations de plus en plus exigeantes pèsent aussi sur les organisations qui doivent pouvoir répondre rapidement et de concert avec leurs parties-prenantes (filiales, sous-traitant, etc.).

L'actualité cyber montre également l'importance de la reconstruction et de la restauration des systèmes d'information, avec la notion de résilience qui prend une importance croissante. Celle-ci implique d'apprendre des crises et d'avoir un regard précis sur les modes de prise de décision dans l'incertitude.

Parmi les différents types de crise, la cyberattaque a ses propres particularités et doit être traitée de façon spécifique. Lors de cette présentation, Lionel MOURER s'attachera principalement aux aspects organisationnels, présentera quelques bonnes pratiques (et celles à éviter) en matière de gestion de crise lors d'une attaque par un hacker.

Qui est Lionel Mourer ?



Lionel MOURER a 35 ans d'expérience professionnelle dans les Systèmes d'Information dont plus de 25 en conseil stratégique et opérationnel en sécurité de l'information et résilience au profit de grands groupes, d'ETI et de nombreuses PME/PMI.

Associé-fondateur d'ATEXIO en 2013, cabinet de Conseil, Audit et Formation, devenu MANIKA en 2020, Lionel intervient sur des missions d'expertise et/ou de conduite de projets complexes, mais aussi en tant que formateur au sein de plusieurs écoles d'ingénieur ainsi que pour des instituts de formation.

Lionel est Ingénieur en Technologies de l'Information et de la Communication, diplômé de Télécom Lille (IMT Nord Europe).

Lionel est administrateur du Clusif - Club de la Sécurité de l'Information Français.

Demande d'inscription pour le Lundi de la cybersécurité de mars

Lundi 13 mars à partir de 18 h 00, en ligne 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 hyperlien personnel vers la visio conférence un peu avant le jour de l'événement.

Les demandes d'inscriptions sont à adresser à : **beatricelaurent.CDE@gmail.com**

Dans votre message d'inscription, nous apprécierions que vous écriviez quelques mots sur vous et sur l'intérêt que vous accordez au sujet traité. Evitez le style télégraphique, nous sommes toujours heureux de vous lire et de connaître votre intérêt pour nos événements.

Les prénoms, noms et adresses mails des inscrits seront connus des organisateurs et communiqués aux intervenants.

Un quart d'heure avec le général Marc Watin-Augouard, créateur du FIC

Suivant la tradition de nos « Lundi de la cybersécurité », entre l'exposé des intervenants et la session questions / réponses, autour de 19h15, nous donnons pour quinze minutes la parole à une organisation, qui opère dans l'écosystème du numérique et dans la sécurité de l'information.

Le thème du FIC cette année - 5, 6 et 7 avril 2023 à Lille Grand Palais, est : "In Cloud we trust ?"

Le Cloud public revient à « utiliser l'ordinateur d'un autre » auquel les organisations confient non seulement leur patrimoine informationnel mais aussi parfois leurs processus métier les plus stratégiques. La

cybersécurité et la confiance que l'on peut -ou non- accorder à l'opérateur, sont donc essentielles. La première s'évalue, se mesure, se compare, tandis que la seconde repose sur une appréciation nettement plus subjective que les contrats suffisent rarement à conforter. Résultat : nous sommes souvent contraints de faire confiance par « défaut ».

Sur ces deux volets, les risques sont multiples.

L'Europe ne peut plus se satisfaire de cette situation d'extrême dépendance. D'autant qu'elle dispose de nombreux atouts : des acteurs performants et innovants, une industrie traditionnelle puissante, un marché potentiel important etc. Tous les leviers, qu'ils soient techniques, organisationnels, juridiques ou politiques, doivent être mobilisés pour renforcer la cybersécurité et créer la confiance.

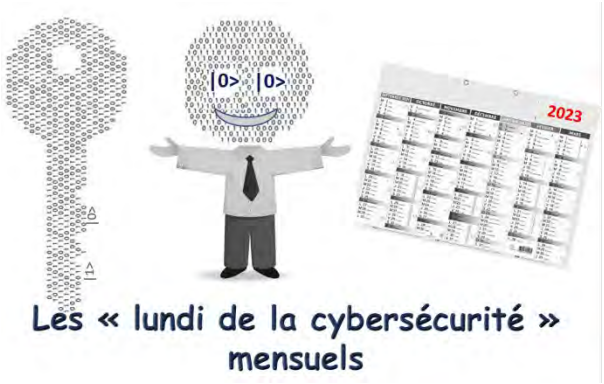
Autant de question(s) qui seront à l'honneur lors du FIC 2023 !

Retour sur les "Lundi de la cybersécurité" précédents.

Vous trouverez tous les détails, slides, enregistrés sur le web de l'ARCSI, en https://www.arcsi.fr/ pour les plus récents et en https://www.arcsi.fr/evt_passes.php pour les événements plus anciens. Les quarts d'heure accordés aux initiatives se trouvent en première page du site de l'ARCSI, là où sont les logos des organisations qui se sont déjà connectées dans nos « Lundi de la cybersécurité ».

Nous remercions Francis Bruckmann, webmestre et membre du Conseil d'Administration de l'ARCSI pour son travail qui constitue la mémoire de nos événements.

Gérard



Lundi de la cybersécurité de mars

lundi 17 avril 18h-20h

Herbert Groscot
Actuariat, Modélisation,
Risques financiers

Jean-Pierre Marbaix
Prevention IARD
Entreprises

La cyber-assurance