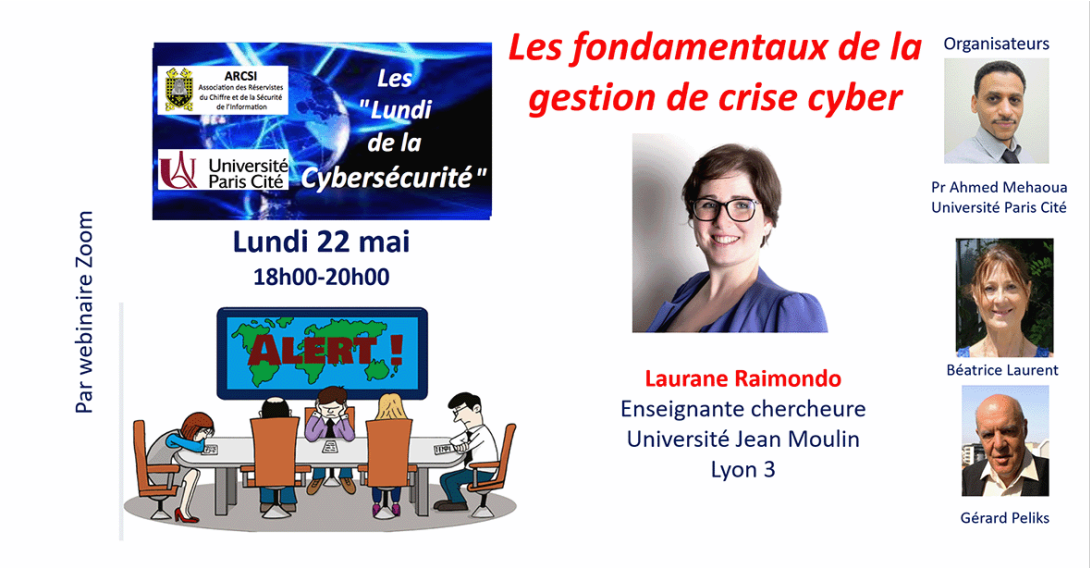
Lettre des "Lundi de la cybersécurité n° 59

Les fondamentaux de la gestion de crise cyber



Les fondamentaux de la gestion de crise cyber

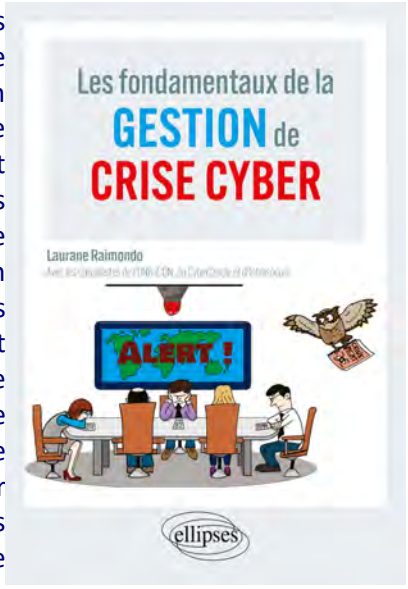
Les crises cyber sont devenues inévitables. Comment les anticiper ? Sont-elles imprévisibles ou peut-on les repérer avant qu'elles ne surviennent ? Quels sont les réflexes qu'il faut maitriser lorsqu'une attaque se produit dans votre datasphère ?

Non, la bonne question à débattre n'est pas : « *Qui est coupable ?* » alors que le monde s'écroule autour de votre organisation. Les bonnes questions concernent la technique, la gouvernance, le juridique, la communication. Et pour cela la cellule de gestion de crise doit inclure, au moins un décideur pour la suite des actions à décider, un technicien, un membre des relations humaines ; un membre de la communication et des chefs de projets pour déterminer ce qu'on dit et ne dit pas aux clients, aux partenaires, au personnel de l'organisation, à la presse.

Si votre organisation n'est pas préparée à gérer la crise, arrive un phénomène de sidération puis la panique s'installe. L'existence de votre organisation est menacée. Si votre organisation est préparée par des exercices de gestion de crise, vous saurez comment réagir et sortir de la crise par le haut.

Je donne la plume à Laurane Raimondo

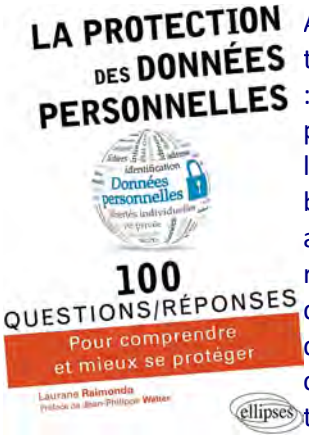
La survenue d'une crise, cyber ou non, est par essence déstabilisante. Nul ne l'attend, beaucoup la craignent et certains ne s'en remettent pas. Pourtant, les crises sont porteuses d'opportunités. Dans une société où tous les rouages doivent être parfaitement huilés pour faire tourner la grande machine, un grain de sable suffit à bloquer des pans entiers de nos activités. La « machine numérique » ne fait pas exception, au contraire. Plus les activités humaines dépendent d'elle, plus elle se complexifie, plus sa vulnérabilité croît. Par tradition, lorsque survient la cybercrise, c'est au domaine technique que la responsabilité est imputée. Pourtant, nous utilisons tous ces outils. Mais peu cherchent à les comprendre et préfèrent confier les rênes aux « spécialistes » tout en pestant lorsque la machine se bloque suite à une mauvaise manipulation et râlant contre la technologie et leur propre incapacité à comprendre l'origine du problème, parfois pourtant d'une simplicité déconcertante.



Les cyber-incidents. Souvent mineurs, de plus en plus régulièrement majeurs, ils surprennent encore tout le monde et ont une particularité : il ne suffit pas qu'un organisme soit attaqué pour déclencher une volonté de montée en compétence en interne. Beaucoup se sentent « sécurisés » une fois la crise surmontée, se disant « nous avons été touchés une fois, peu de chance de l'être une seconde fois ». L'aspect « invisible » de la menace pèse : un attentat terroriste est spectaculaire, le sang coule, les médias se déchaînent ; une attaque cyber est souvent silencieuse, les dégâts provoqués par certaines d'entre elles peuvent commencer longtemps avant d'être découverts, durer et coûter extrêmement cher. Cette croissance exponentielle des cyberattaques et leur sophistication permanente doivent nous alerter : nous devons réapprendre à vivre avec la menace, extérieure mais aussi intérieure.

Souvent on entend que « le principal danger est placé entre la chaise et le clavier ». La sécurité aussi ! Peu importe la hauteur et l'épaisseur des murs d'une forteresse, un pan de bois aurait une efficacité équivalente si quelqu'un ouvre la porte de l'intérieur. Idem si une taupe est abritée dans ladite forteresse, des informations précises suffisent à la faire tomber. Tout système a ses failles, donc partir du principe qu'il tombera à un moment donné est l'attitude la plus responsable et sécurisante à adopter, si elle n'est évidente. Nous sommes intrinsèquement tous en charge de cette responsabilité car c'est bien nous, humains, qui devront sortir de cette crise, sinon indemne, plus résilients. Pour cela, un tableau des risques et menaces doit être brossé pour tracer un chemin de réflexion. Le rapprochement comme

la différenciation de la cybercrise avec la crise « classique » devrait être abordé pour essayer d'en extraire une méthodologie d'approche spécifique avec une certitude : la réponse ne peut être uniquement technique.



Anticiper deviendra la clef, savoir que tôt ou tard l'incident nous touchera. Cette anticipation doit tout d'abord être d'ordre juridique : l'Union européenne et la France en particulier se veulent pionnières en la matière en essayant de donner un cadre à l'« environnement cyber », chose délicate. Le pan technique n'est bien sûr pas à négliger, il est sur la ligne de front lors d'une attaque mais pas le seul. La transversalité de la cybercrise doit se retrouver dans la cellule de crise, technique et gouvernance deviennent alors indissociables. Si nous tâtonnons encore, la question des formations issues de nos expériences donneront des clefs aux acteurs de demain, d'où une nécessité d'entraînement à travers des simulations de gestion de crise cyber. Simulation = intégration de l'humain dans la réponse qui doit, pour fédérer et permettre de sortir de la crise, être organisée et efficace.

Autre composante de celle-ci, la communication de crise. Extrêmement différente d'une communication de crise classique, elle doit impérativement s'adapter au contexte spécifique de la cybercrise. Tout ceci favorisera, une fois le retour à l'équilibre, le dessin d'un schéma de sortie de crise serein et permettra à l'organisme touché de recouvrer une pleine santé et d'organiser sa résilience à travers les retours d'expérience, indispensables même si une règle reste de rigueur : aucune crise ne se ressemble.

Le temps n'est plus où la question cyber était pensée en vase clos, elle doit s'ouvrir : à tous de s'en saisir.

Je reprends la plume

Qui est Laurane Raimondo ?

Auteure des ouvrages *Les Fondamentaux de la gestion de crise cyber*, rédigé avec un panel d'experts (2022, Ellipses) et de *La protection des données personnelles en 100 questions-réponses* (2020, Ellipses), **Laurane Raimondo** a commencé sa carrière au Conseil de l'Europe, dans l'unité de protection des données, avant d'enseigner dans le master Relations Internationales de l'Université Jean Moulin Lyon 3.

Recevant le Prix du Gouverneur militaire de Lyon pour ses travaux en 2019, puis de la Femme chercheure cyber du CEFCYS en 2021 et enfin du Livre FIC en 2022 pour son premier ouvrage, elle continue aujourd'hui l'enseignement et prend en sus la direction du MSc Relations Internationales et Cyberespace à l'Ileri Paris tout en restant *advisor* du CyberCercle, stratégiste en confiance numérique

pour l'ONG iCON et dirigeant une entreprise de conseil spécialisée dans la protection des données et la cybersécurité.

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

Lundi 22 mai 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.

Que peuvent vous apporter nos « Lundi de la cybersécurité » ? C'est la question que j'ai posée à un programme d'Intelligence Artificielle générative. Voir la réponse à la fin de cette lettre.

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

Si vous souhaitez ne plus recevoir les lettres des « Lundi de la cybersécurité » mensuelles, une simple demande par mail suffit. Si vous voulez être ajouté à la liste de distribution, demandez-le nous.

Le quart d'heure des organisations

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 une dizaine de minutes la parole à une organisation, qui opère dans l'écosystème du numérique et dans la sécurité de l'Information.

Quelques minutes avec l'ONG iCoN

Ce Lundi de la cybersécurité du mois de mai, la séquence "La parole à une organisation" sera animée par **Pierre-Marie Lore**, un des trois fondateurs de cette association et par ailleurs Directeur cybersécurité de Framatome, après avoir été directeur cybersécurité du groupe RATP. Pierre-Marie est membre de l'ARCSI et diplômé du MBA Management de la Sécurité des Données Numériques de l'Institut Léonard de Vinci.

Basée à Genève**, l'ONG ICON** fédère une communauté européenne et internationale d'experts et de spécialistes travaillant sur la confiance dans le cyberespace, en mettant l'accent sur la cybersécurité et l'intelligence artificielle. **https://icon.ngo/fr**

Par des actions concrètes, des outils innovants et le partage des meilleures pratiques, l'ONG ICON cherche à déclencher la prise de conscience pour partager, démystifier et décoder la société de l'information afin d'apporter la confiance dans le monde digital.

Retour sur les "Lundi de la cybersécurité" précédents.

Vous trouverez tous les détails, slides, parfois aussi les enregistrements 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 sont déjà intervenues 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.

Le coin de l'Intelligence Artificielle générative

Question posée au moteur de recherche Bing qui intègre aujourd'hui un module d'IA générative :

Quels sont les avantages de participer aux Lundi de la cybersécurité

Réponse reçue

La réponse est tirée des résultats de la recherche web.
Les avantages de participer aux Lundi de la cybersécurité sont :

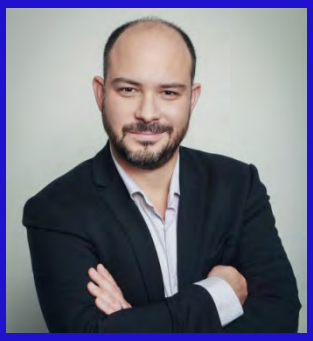
- *Se former et se tenir informé sur des sujets d'actualité et de pointe dans le domaine de la sécurité du numérique.*
- *Échanger et débattre avec des experts et des professionnels du secteur.*
- *Renforcer son réseau et ses opportunités professionnelles.*
- *Protéger son entreprise et ses données contre les cyberattaques.*

Finalement, pas si bête 😊

Gérard

Lundi de la cybersécurité de juin

lundi 12 juin 18h-20h



Ivan Fontarensky,

directeur technique cyberdéfense chez Thales

La Cyber Threat Intelligence