Lettre des "Lundi de la cybersécurité" n° 67

La cyber-résilience dans l'Union européenne
Il est temps d'agir

Une fonction de la matière vivante m'a toujours épaté : Sa réaction efficace pour fournir une solution à un problème rencontré. Prenons un exemple : Quand vous subissez une coupure, vous continuez à vivre, mais peut être en mode dégradé, tout dépend de l'endroit et de l'importance de la plaie. Ça saigne au début, mais peu à peu, avec l'aide automatique apportée par vos leucocytes et, si nécessaire, aidé par des désinfectants avec lesquels vous stérilisez la plaie, le problème ne s'aggrave pas et l'infection par des organismes extérieurs est contenue. Puis il se forme une croute, puis, la croute se résorbe et disparait et le problème est résolu. Le fonctionnement redevient « normal ». Vous avez retrouvé votre capacité d'avant coupure. Quelle merveilleux exemple de **résilience** nous donne ici dame nature !

Mais de telles fonctionnalités sont-elles possibles pour un système d'Information qui lui aussi est plongé dans un monde de plus en plus agressif alors que l'hyperconnectivité s'installe partout ? Oui, c'est la cyber-résilience.

La **cyber-résilience** est la capacité d'une structure à détecter les incidents potentiels de cybersécurité, à y résister, à les combattre et à retrouver un fonctionnement normal (si possible). Evidemment, ça ne se fait pas tout seul, il faut pour cela avoir mis comme contre-mesures les indispensables outils, services, et sensibilisations du personnel.

La loi **CRA** Cyber *Resilience Act* de la Commission européenne améliore la coopération entre les États membres pour améliorer la cybersécurité en Europe, alors que les attaques sur les systèmes d'Information et sur l'Information se multiplient et sont de plus en plus sophistiquées.

La directive **NIS2**, La directive **RCE** (*Résilience des Entités Critiques*), La loi **DORA** *(Digital Opérationnel Resilience Act)* pour le secteur financier, autant de textes à connaître.

Pour nous parler de cette nécessaire cyber-résilience, nous avons demandé à des spécialistes, très impliqués dans ces technologies, de nous éclairer sur le sujet.

Je donne la plume aux intervenants

Plier pour ne pas rompre ! La cyber-résilience décrit la capacité de l'organisation à anticiper, protéger, détecter, répondre et récupérer rapidement d'un incident de sécurité informatique majeur. Avec l'augmentation de la digitalisation des activités professionnelles et des cyberattaques qui l'accompagnent, la cyber résilience est devenue un enjeu stratégique majeur pour toutes les entreprises. L'Union européenne avait déjà observé une augmentation de 26 % des attaques en 2022 et plus inquiétant encore, une très grande majorité des organisations déclarait avoir subie une cyberattaque. Cette tendance devrait s'être poursuivie en 2023.

Les conséquences d'une faille de sécurité peuvent être désastreuses, allant de la perte de données sensibles à la perte de confiance des clients, à la destruction de la réputation de l'organisation, voir dans les cas les plus extrême à entrainer une société en redressement judiciaire. Cela concerne tout le monde, de la plus petite à celle exerçant des activités au niveau mondial. Par conséquent, l'adoption d'une approche efficace de défense active en profondeur est devenue vitale face à l'inévitable attaque de cybersécurité.

C'est dans ce contexte que l'Union Européenne a entrepris plusieurs mesures et obligations pour renforcer la résilience cyber à l'échelle européenne, notamment la directive NIS2 (pour les Systèmes d'Information et de Communication), la directive RCE (Résilience des Entités Critiques), le règlement DORA (Digital Operational Resilience Act) pour le secteur financier, ou encore le règlement CRA (Cyber Resilience Act) pour les produits contenant des éléments numériques.

Ce cadre réglementaire devrait contribuer à renforcer une posture de cyber résilience au niveau Européen en ne limitant pas les démarches au niveau d'une organisation, mais en fixant un cap et des exigences précises pour l'ensemble de l'écosystème.

Je reprends la plume

Qui est Laurent Peliks ?

Associé EY, **Laurent Peliks** est Ingénieur de l'Ecole Nationale Supérieure des Télécommunications de Bretagne. Il est également titulaire d'un DEA Informatique de l'Université de Rennes I. Laurent dispose d'une expérience de plus de 22 ans en cybersécurité.

Au sein de la zone EMEIA (Europe, Moyen-Orient, Inde et Afrique), Laurent est responsable des offres de cyber résilience qui couvrent l'accompagnement à la gestion de crise cyber, la résilience opérationnelle, la gestion de la continuité et reprise d'activité ainsi que le renforcement de la résilience des infrastructures IT.

Il intervient depuis plus de 20 ans en France auprès des acteurs publics et groupes privés pour les accompagner dans l'évaluation de leur maturité cybersécurité et l'homologation de leurs systèmes d'information.

Qui est Stéphane Brebion ?

Doté de 9 ans d'expérience, **Stéphane Brebion** possède de nombreuses expériences relatives aux problématiques de Cyber Résilience. Il réalise depuis plusieurs années du conseil auprès des RSSI et a notamment défini un framework de Cyber Résilience ou encore accompagné sur le diagnostic et la mise en œuvre opérationnelle de capacités de résilience.
Stéphane Brebion est le leader EY des offres de Cyber résilience pour la région Europe de l'Ouest.

Qui est Maître Olivier Iteanu ?

Avocat à la Cour, Olivier Iteanu est un expert juridique .autour des sujets du numérique, de la cybersécurité, et des Data.

Olivier Iteanu est aussi chargé d'enseignement en Master 2 Droit des données à l'Université Paris I Sorbonne et en Master 2 Droit des activités spatiales et des télécoms à Université Paris Saclay

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

Lundi 26 février, 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 personnel vers la visioconférence.

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.

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

Et bien entendu, si vous vous inscrivez pour assister à notre évènement, soyez connectés, avec votre prénom et votre nom, le lundi 26 février, dès 18 h 00**. Prévenez-nous, dès que possible si vous êtes inscrits mais avez un empêchement pour assister à ce webinaire.**

Quelques minutes avec une organisation : l'ARCSI

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'organisation sera l'**ARCSI** et l'intervenant sera **le général (2S) Jean-Louis Desvignes** président de cette organisation.

Le coin des « 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. Les événements plus anciens sont en **https://www.arcsi.fr/evt_passes.php.**

Les enregistrements des organisations qui sont intervenues durant les « quelques minutes » se trouvent en première page du site de l'ARCSI, là où sont les logos de ces organisations. Cliquez sur un logo, vous obtenez l'enregistrement s'il a été fait.

Le coin coin de l'IA générative

Question posée à BARD (l'IA générative de Google) :

« ***C'est quoi la cyber-résilience à l'échelle européenne ?*** »

Voici une partie de la réponse reçue :

« La cyber-résilience à l'échelle européenne est la capacité de l'Union européenne et de ses États membres à résister, à absorber, à atténuer et à se remettre d'une cyberattaque. Elle vise à protéger les infrastructures essentielles, les systèmes et les données, ainsi que les citoyens et les entreprises européens.

La cyber-résilience est un défi croissant pour l'Europe, car les cyberattaques sont de plus en plus sophistiquées et ciblées. Elles peuvent avoir des conséquences graves, telles que des perturbations des services publics, des pertes financières ou des dommages à la réputation.

Pour renforcer la cyber-résilience à l'échelle européenne, l'Union européenne a adopté une série de mesures, notamment :

- Le règlement sur la cyber-résilience, qui impose des exigences en matière de cybersécurité aux produits matériels et logiciels.
- La directive sur la sécurité des réseaux et des systèmes d'information, qui oblige les organisations des secteurs critiques à mettre en place des mesures de sécurité pour protéger leurs systèmes d'information.
- Le Centre européen de cybersécurité, qui coordonne les efforts de l'Union européenne en matière de cybersécurité.

Ces mesures visent à renforcer la cyber-résilience de l'Europe en :

- Améliorant la protection des produits et services numériques.
- Réduisant la vulnérabilité des organisations des secteurs critiques.
- Améliorant la coordination des efforts de cybersécurité au niveau européen.

La cyber-résilience est un processus continu, qui nécessite une coopération étroite entre l'Union européenne, les États membres et le secteur privé. »

Gérard

Lundi de la Cybersécurité de mars

lundi 18 mars 18h-20h

en présentiel au siège de l'université Paris Cité, rue de l'Ecole de médecine

Table ronde sur la cybersécurité et la e-Santé