Cyber : tous concernés !

La 41ème édition des Nocturnes Ex'pairs Formation a réuni 200 personnes le 4 juin dernier. Dirigeants d'entreprises et managers, sont venus échanger sur un paradoxe des temps modernes : le numérique qui bouleverse, transforme nos sociétés, et, apporte en même temps un lot de menaces sur nos activités.

Quatre intervenants ont répondu à l'invitation de Virginie Nogueras, dirigeante du cabinet-Conseil Ex'pairs Formation : le Vice-amiral d'escadre, Arnaud Coustillière, Directeur Général des Systèmes d'Information et de Communication du ministère des Armées, Yassir Kazar, CEO de Yogosha, Michaël BITTAN, associé responsable des activités Cyber Risk chez Deloitte et Laurent CELERIER, Responsable de transformation numérique à la direction générale du ministère des armées et ancien conseiller du directeur général de l'ANSSI (Agence nationale de la sécurité des systèmes d'information).

*D'après une étude effectuée en mars 2018 auprès de 400 ETI, 78 % des entreprises ont subi au moins une cyberattaque. La question n'est donc pas de savoir si vous allez en être victime, mais plutôt quand ? Pour **Yassir Kazar**, « penser qu'on ne peut pas être une cible est une erreur ». Pour **Arnaud Coustillière**, « l'absence de frontière sur le net rend les états et les entreprises vulnérables. Le ministère des armées a pris la mesure du danger. Le cyber est un devenu un espace de confrontation, d'espionnage, et de propagande. »*

*Les entreprises victimes de cyberattaques ont tendance à la cacher. Or, avec le nouveau RGPD, elles auront l'obligation de la déclarer dans les 72 heures. Pour **Laurent CELERIER**, « il faut impérativement en informer les autorités et se faire aider. »*

Un tiers des cyberattaques viendraient de concurrents malveillants.

L'Etat consacre aujourd'hui 3 % de son PIB à sa cyberdéfense. Idéalement, dans les entreprises, 3 % devraient être affectés à la cybersécurité.

Les attaques sont diverses et variées. Elles peuvent affecter l'image d'une entreprise, faire de l'espionnage industriel ou sur une innovation, elles peuvent tout simplement saboter un système voir détourner des fonds.

*Pour **Michaël BITTAN**, « l'hygiène informatique est le b.a.-ba. C'est comme un cambriolage. Il faut ralentir le hackeur dans sa course. Les entreprises nous contactent soit pour anticiper une cyberattaque, sujet de préoccupation du CODIR, là, on identifie les éléments à protéger et on établit une stratégie ; soit, il y a eu cyberattaque, et dans ce cas, il faut remettre l'entreprise sur pieds. »*

Quelques règles pour s'affranchir d'une cyberattaque : faire régulièrement les mises à jour des logiciels et applications ; limiter le nombre d'administrateurs au sein des entreprises ; limiter l'accès aux sites web en créant une liste blanche de sites autorisés et enfin ne pas cliquer sur les liens dans les e-mails inconnus.

Idéalement, les équipes peuvent suivre une formation, un entrainement pour mieux prévenir, se protéger et intervenir en cas de cyberattaque.

*En conclusion, **Virginie Nogueras** a rappelé que « nous étions tous concernés par la cybersécurité. Grosses, petites entreprises, dirigeants, experts, collaborateurs, citoyens, ce nouvel espace nous impose et fonde à de réelles intelligences **collectives**. L'opportunité pour nos organisations de créer une culture de la cyber résilience, et de tenter de réaliser ensemble une équation pourtant simple, celle de la confiance. »*

***Renseignements et inscriptions** : contact@expairsformation.com*

www.expairsformation.com

***I-WAY :** 4, rue Jean Marcuit 69009 Lyon*