EFCSE, présente à l'édition 2018 du FIC

Auteur : Corinne FRANCE – General Secretary EFCSE
25 Janvier 2018

Favoriser une réelle coopération internationale

EFCSE était présente au 10ème Forum International de la Cybersécurité à Lille (France) en ce mois de Janvier 2018 et a constaté une volonté affichée de favoriser une réelle coopération internationale pour faire face aux attaques cyber.

Avec beaucoup d'exposants de toutes tailles et de toutes notoriétés, de nombreux participants, de nombreuses solutions exposées pour lutter et prévenir le risque d'attaque cyber, une intonation à dominante technique et politique, le FIC a bien grossi, il est un bel espace dédié à la réflexion et aux échanges, où la promotion d'une vision européenne de la cybersécurité représente l'un des éléments clefs à suivre et à alimenter.

Il reflète l'augmentation de l'importance de la cybersécurité et de son organisation coordonnée au sein de toutes les nations sur la scène mondiale, en réponse à la complexification des attaques, ainsi qu'à la rapidité d'évolution et d'adaptation de celles-ci.

Une richesse de thèmes en adéquation avec la complexité du monde cyber

Le FIC, c'est une multitude d'ateliers, de conférences, de présentations et de démonstrations techniques, des espaces de recherches, carrières, solutions, etc… de quoi, pour le visiteur, repartir avec à minima une liste de questions et pistes de réflexion, à maxima une vision plus éclairée sur les grands thèmes du monde cyber, ses acteurs et ses enjeux majeurs.

Parmi tous les thèmes présentés, abordés, argumentés, renseignés, représentés, dont beaucoup très techniques, chaque visiteur devait pouvoir trouver intérêts et arguments pour enrichir sa propre activité et disposer de pistes concrètes pour aborder la cybersécurité.

Que ce soit au format conférence, atelier ou démonstration pour ne citer qu'eux, la richesse des sujets était au rendez-vous, voici un échantillon du programme :

- La conformité au RGDP en 3 clics - 2020 : Intelligence connectée – Comment sécuriser le cloud public ? Réponse en 10 recommandations. - Ransomware : quelle coopération internationale pour faire face ? - Cyber Threat Intelligence : quelle est sa réelle valeur ajoutée ? - La sécurité by design, nouvel impératif business et industriel. - SOC : Construire un plan de surveillance efficace pour faire face aux nouvelles menaces. - La sécurité des accès en six étapes : méthodologie et retours d'expérience - Garantir la sécurité de votre SI en gardant le contrôle permanent de son état de santé - DIGITAL Security : Label de sécurité de l'IoT, etc…

ZOOM EFSCE

IoT, une « explosion » de propositions mais encore beaucoup de défaillances et de points de vulnérabilité. La sécurité ne semble pas être tout à fait au rendez-vous de la fourniture de services, entrainant des risques élevés et des conséquences pouvant être dramatiques. Citons par exemple dans le domaine de la santé une pompe à insuline qui se dérègle ou un pèse personne qui ne transmet pas une mesure du poids alarmante dans le cadre du suivi d'un patient insuffisant cardiaque sévère…

Tant en termes de gouvernance des données (définition claire des parties prenantes, des accès aux informations, de leur traitement…), que de référencement de celles-ci, l'IoT est à suivre attentivement quant à sa montée en puissance. Sachant que les problématiques d'interopérabilité, de normes et de standards d'échange de données sont également des éléments essentiels pour une efficacité de services digne de ce nom.

S'ajoute à cela la problématique de responsabilité en cas de sinistre provoqué par un objet connecté, les assureurs ont à étudier attentivement les garanties d'assurances spécifiques à mettre en place.

Notons enfin qu'à l'heure du RGPD, le sujet de l'accès à des données pour contrer des attaques, tout en respectant les droits fondamentaux de chacun, reste une équation compliquée où le chiffrement est un point sensible.