efcse.eu

Cyber 2018 - questions pour demain…

Auteur : EFCSE
5 décembre 2017

IoT : de quoi demain sera-t-il fait ?

« TO » pour Technologie Opérationnelle : permettent l'utilisation de l'énergie et autres ressources (électricité, gaz, eau…) en soutient à des services essentiels à des clients ou autres Organisations (gouvernement, industrie…). Quasi toutes les Organisations ont ajouté à cela une couche « TI », pour Technologie de l'Information (lien avec Internet, Informatique…), afin d'assurer une bonne gouvernance de cette précieuse information, d'améliorer les processus de création de valeur, de renforcer le contrôle interne, etc… (se référer aux publications liées à ce sujet).

Nous savons que la gouvernance de l'information est capitale pour toute Organisation, compte tenu des risques croissants de perte de contrôle et des impacts sur la production, quelle qu'elle soit. Il s'agit donc d'élaborer une véritable stratégie d'équilibre entre ces 2 mondes afin de faire face aux potentielles cyber attaques.

L'internet des objets (IoT) imprègne cet univers, il se répand à grande vitesse dans tous les domaines, d'aucuns affirment que la transformation numérique n'est pas envisageable sans les IoT (réf. Etude Vodafone – oct. 2017), les cyber attaques sont déjà en actions depuis plusieurs années (réf. article znet.com du 24 octobre dernier / 5 attaques cauchemardesques qui montrent les risques liés à la sécurité de l'IoT), quels sont et quels seront les moyens de prévention de risques, quel contrôle un individu peut-il et pourra-t-il avoir sur ses données dans un tel contexte ? Comment l'Europe s'organise-t-elle et s'organisera-t-elle pour faire face à cela ?

EFCSE est organisée en groupes de travail afin d'accompagner les entreprises et les personnes sur ces typologies de sujets.

Contactez-nous via le formulaire https://www.efcse.eu/fr-fr/contact.php