efcse.eu

EXTRAIT D'ACTUALITE : TESTS CYBER PRATIQUES

Auteur : Secrétariat Général EFCSE
3 mai 2019

Evénement : Locked Shields 2019

Le centre d'excellence de l'OTAN (CCD COE) organise depuis 2010 le « Locked Shields », exercice de cyberdéfense réunissant plus de 30 nations, même si c'est avant tout un exercice de coopération, la dimension compétitive entre les pays participants, est bien présente et basée sur un système de comptabilisation de points.

Cet exercice annuel de défense du réseau en temps réel est une occasion unique pour les cyber-défenseurs nationaux de protéger leurs systèmes informatiques et leurs infrastructures critiques sous la pression intense d'une cyberattaque.

Lors de cet événement il a été mis en évidence la nécessité croissante de renforcer le dialogue entre les experts techniques, les participants civils et militaires, ainsi qu'aux niveaux décisionnels.

Le CCDCOE [1]intègre jeux techniques et stratégiques, permettant aux pays participants de s'exercer à toute la chaîne de commandement en cas de cyber incident grave, intégrant des joueurs civils et militaires. Ceci reflète les cybermenaces du monde réel et les exercices ont, en premier lieu, porté sur la protection des services essentiels et des infrastructures critiques.

Cet exercice de cyberdéfense 2019 était organisé par le centre d'excellence otanien basé à Tallinn, il s'est déroulé les 25 et 26 avril derniers, avec plus de 1000 personnes appartenant à 30 nations au sein de 22 équipes. L'objectif était d'évaluer leur capacité à défendre un réseau informatique complexe face à des cyberattaques menées par un État fictif, c'est l'équipe Française qui est arrivée en tête devant les équipes Tchèque et Suédoise, respectivement 2ème et 3ème.

Cybersécurité : exercice grandeur nature pour l'UE

Début avril, le Parlement européen, les États membres de l'UE, la Commission européenne et l'Agence européenne pour la cybersécurité (ENISA) ont organisé un exercice destiné à tester la réaction de l'UE aux plans de crise relatifs aux éventuels incidents de cybersécurité affectant les élections européennes.

L'exercice devait permettre de tester l'efficacité de la réactivité des États membres de l'UE, de l'UE et des plans de crise de l'UE, ainsi que d'identifier des moyens de prévenir, détecter et atténuer les incidents de cybersécurité susceptibles d'affecter les élections au sein de l'Union européenne. Intégré aux mesures mises en œuvre par l'UE, cet exercice est fait pour garantir des élections libres et équitables en ce mois de Mai 2019.

Sur la base de scénarios variés comportant des menaces et des incidents cybernétiques, l'exercice est conçu pour que les participants puissent vérifier un certain nombre de points, tels que :

[1] NATO CCD COE: *Cooperative Cyber Defence Centre of Excellence , est l'un des centres d'excellence de l'OTAN situé à Tallinn en Estonie*

- Obtenir une vue d'ensemble du niveau de résilience (en termes de politiques adoptées, de capacités et de compétences disponibles) des systèmes électoraux à travers l'UE, y compris une évaluation du niveau de sensibilisation des autres parties prenantes ;
- Renforcer la coopération entre les autorités compétentes au niveau national ;
- Vérifier la capacité des États membres de l'UE à évaluer de manière appropriée les risques liés à la cybersécurité des élections européennes, à développer rapidement une connaissance de la situation et à coordonner la communication avec le public ;
- Tester les plans de gestion de crise existants ainsi que les procédures pertinentes pour prévenir, détecter, gérer et répondre aux attaques par cybersécurité et aux menaces hybrides, y compris les campagnes de désinformation ;
- Améliorer la coopération transfrontalière et renforcer les liens avec les groupes de coopération concernés au niveau de l'UE afin d'améliorer la capacité de réaction coordonnée en cas d'incident transfrontalier de cybersécurité ;
- Identifier toutes les autres lacunes potentielles ainsi que les mesures adéquates d'atténuation des risques, qui devraient être mises en œuvre avant les élections au Parlement européen.

Cet exercice de type test de cybersécurité va également de pair avec le plan d'action contre la désinformation que l'Union européenne a adopté en décembre 2018 pour renforcer la coopération entre les États membres et les institutions de l'UE afin de faire face de manière proactive aux menaces dues à la désinformation.