NANCY

Cyberguerre entre étudiants et militaires

Ce n’est qu’un exercice, mais le wargame technologique organisé par la base de défense de Nancy et Lorraine INP (réunion des écoles d’ingénieurs) avec des moyens du Grand Nancy est une première. Il permet aux civils et aux militaires de travailler et d’apprendre ensemble à combattre les virus.

Depuis lundi, la base de défense de Nancy organise une cyberguerre avec Lorraine INP (réunion des écoles d’ingénieurs de l’Université de Lorraine) et la Métropole du Grand Nancy. Un peu à l’exemple des attaques informatiques subies par les hôpitaux de Villefranche-sur-Saône (Rhône) ce lundi et de Dax (Landes) le 9 février. En décodé, les militaires – des officiers de réserve spécialisés dans ce domaine technologique du commandement de la cyberdéfense – ont élaboré tout un système informatique, de l’ordinateur au site web, de la caméra de vidéosurveillance à l’imprimante, bases de données clients, adresses mail et autres d’une société de vente de prêt-à-porter bio baptisée Blacksheep. Une entreprise fictive mais qu’ils ont fait exister sur les réseaux sociaux, le web et dans le serveur (le Cyber Range) de ce laboratoire.

En face, deux équipes d’étudiants de Polytech Nancy et de l’École des Mines de Nancy s’affrontent. Les bleus, « Blacksheep », défendent l’entreprise à l’infrastructure « vieillissante » ou composée de pièces rapportées au fil du temps. Les rouges, « BarbHack », doivent pirater la société pour voler des documents, compromettre son fonctionnement, missionné par une autre entreprise probablement concurrente. La construction de cet exercice est un travail cumulé de 200 jours de l’équipe de militaires et d’universitaires au sein du laboratoire.

Une dimension technique, mais aussi humaine

Les 25 étudiants, tous des volontaires qui seront ingénieurs à la fin de l’année scolaire, se sont très vite pris au jeu. Depuis mardi, de 8 h 30 à 17 h 30, ils s’affrontent par écrans interposés pour atteindre leurs objectifs. Et ce n’est pas qu’un défi de lignes de code. « C’est fatigant mais je ne suis pas déçu , constate Nicolas Gondstein, chef de projet chez les bleus et étudiant de Polytech Nancy, pas tellement au niveau technique, mais d’arriver à s’organiser, à tout gérer, surtout quand cela se passe mal. » Le capitaine Jean-Philippe, qui surveille l’exercice, loue pourtant leurs qualités et leur autonomie : « Et nous, on apprend aussi à mieux former à la gestion de crise. Ce n’est pas seulement de la technique. »

Développer la créativité

Les étudiants doivent gérer des éléments qui dépassent l’univers des lignes de codes. Par exemple, dans toutes ces données, se trouvent des fichiers compromettants comme des comptes cachés en Suisse, des documents attachés à une organisation terroriste… Comment vont-ils gérer les aspects légaux et moraux ? Les bleus doivent-ils dénoncer leur employeur ? Les rouges qui sont certes dans l’illégalité par leur action, mais qui travaillent légalement dans une entreprise française, doivent-ils en référer aux autorités ? Bien sûr, encore faut-il que les équipes arrivent à tomber sur ces fichiers sur des milliers d’autres.

Le Cyber Range a truffé la société de surprises pour provoquer la créativité des deux teams, mais aussi les confronter à la vie réelle où il n’y a jamais que du 1 ou du 0, mais des combinaisons presque infinies. Ce jeudi après-midi, tous se retrouveront pour faire les comptes. Chaque opération se solde par des points gagnés en défense ou en attaque. Une des deux équipes va remporter la partie, mais tous auront gagné en connaissance et en expérience, même les arbitres.

Cédric CITRAIN

Les étudiants de Polytech-Nancy et de l’École des Mines s’affrontent en défense et en attaque d’une société fictive sous le regard des militaires de la cyberdéfense qui ont organisé l’exercice. Photo ER/Patrice SAUCOURT

Un lien armée-nation du virtuel au réel

Si les étudiants vont apprendre, les militaires également. Le colonel Lipski, correspondant réserve cyber pour le Grand Est, y voit « un défi technique et une aventure humaine ».

« Le virtuel rejoint le réel. Dans le premier, il est formé de militaires comme de civils, on utilise les compétences des uns et des autres au profit de l'innovation. Il y a des difficultés techniques, mais le vrai défi, c' est les êtres humains. Il faut transmettre et apprendre. Un vrai lien armée-nation. »

Faisant l'analogie avec le virus du Covid-19, il veut aussi que chacun développe sa connaissance des gestes barrières contre celui de l'informatique. Et il sait de quoi il parle. Ses soldats réservistes spécialisés en cyber sont tous des personnes qui exercent comme ingénieurs, docteurs ou universitaires dans la vie civile.

La société fictive a même reçu des candidatures spontanées

L'exercice permet aussi de tester des logiciels, pour la défense comme l'attaque des systèmes d'information numérique, qui ont été développés au sien de ce laboratoire.

Guillaume Bonfante, universitaire du laboratoire Loria, qui enseigne la création des « malwares » (logiciels malveillants) à l'École des Mines, développe aussi un antivirus de nouvelle génération qui permettrait aussi de bloquer les « variants » de virus déjà connus ou recomposés. Il fait partie des arbitres dans l'exercice. Et la nécessité d'infuser une sécurité dans la vie civile est évidente.

En quelques jours, la société fictive Blacksheep de l'exercice a reçu des offres de collaboration d'autres entreprises, des CV et est référencée par Google… Catherine Bower, sa dirigeante toute aussi inventée, a de nouvelles relations professionnelles sur LinkedIn et des followers sur Twitter!

C. C.

7 photos : https://c.estrepublicain.fr/defense-guerre-conflit/2021/02/18/un-exercice-de-cyberguerre-prend-place-a-la-caserne-verneau-blandan-a-nancy