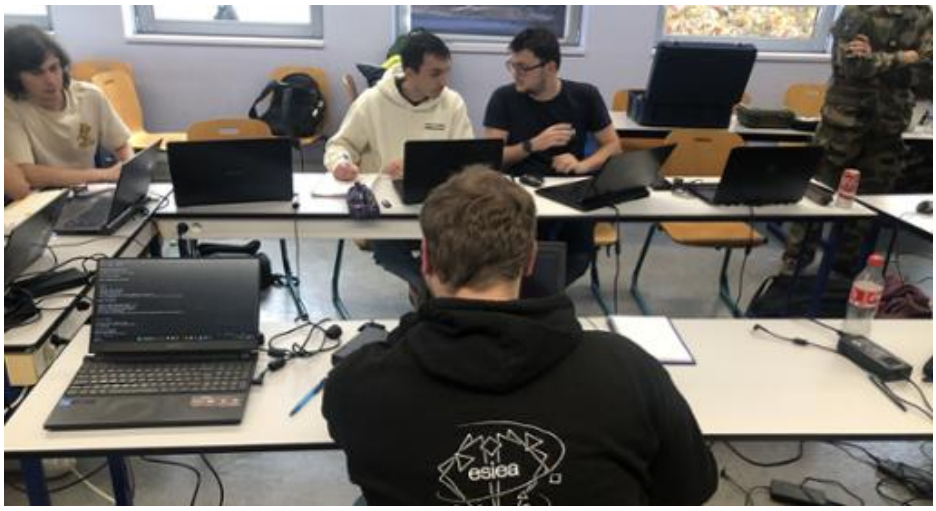
Les futurs ingénieurs face à une cyberattaque



Laval, ce jeudi 17 octobre. Vingt-cinq étudiants ont dû stopper une cyberattaque, un exercice sous pression pour ces futurs ingénieurs.

Ouest-France

Vingt-cinq étudiants de l'école d'ingénieurs ESIEA de Laval ont planché, hier, sur une cyberattaque fictive. Il s'agissait d'un exercice en lien avec le commandement de Cyberdéfense de l'armée.

Reportage

Deux salles, une même ambiance studieuse et une certaine tension. Ce jeudi, les étudiants en 5e année de l'ESIEA, l'école d'ingénieurs de Laval, ont dû se diviser en deux groupes d'intervention cyber avec un même objectif : lutter contre une cyberattaque particulièrement virulente menée par un pays ennemi, la Romania.

Les étudiants, eux, font partie du Lutécia et ont été projetés sur deux bases distinctes pour contrecarrer les plans des adversaires. Dans le scénario, les deux bases sont éloignées. Dans les faits, il n'y a quelques mètres à faire pour rencontrer les deux groupes. Ce scénario catastrophe proposé en lien avec le commandement de Cyberdéfense (ComCyber) de l'armée est bien sûr un exercice mais il s'inspire de situations réelles.

Situation de stress

Les hackers ont par exemple commencé à publier sur X (ex-Twitter) des extraits de données montrant qu'ils avaient bien eu accès à des informations, ceci pour menacer de les mettre à disposition sur le darknet. Une situation qui rappelle des attaques récentes vécues par des entreprises ou des structures publiques, parfois victimes de rançongiciels, ces logiciels qui bloquent les systèmes d'information. Les pirates demandent alors de payer une rançon pour obtenir le code qui débloquera le réseau.

Dans le cas d'une attaque sur le réseau militaire, le risque c'est aussi de compromettre des opérations et mettre en danger les personnels engagés. Ce jeudi matin, ils ont commencé leur journée par un briefing puis par une enquête dans les tréfonds du système d'information dans le but d'identifier la « porte d'entrée ». Une image pour dire qu'un serveur a été mal configuré et que les pirates ont pu s'y faufiler.

La suite vise **« à voir s'il y a eu compromission »**, détaille le sous-lieutenant Tristan, réserviste de l'armée de l'air et de l'espace et instructeur au ComCyber. Vient la phase de remédiation, en somme, comment fermer cette « porte » et remettre en route le réseau. Car tout a été fermé pour éviter une fuite plus importante de données sensibles, mails, numéros de téléphone, adresses de personnels du ministère de la Défense.

Une fois les réparations faites, les groupes se testent pour vérifier que tout est bien ficelé. Les deux groupes sont censés communiquer pour avancer plus vite. **« Mais on communique moins que ce qu'on aurait pu penser »**, souffle un des étudiants. Richard Rey, Référent enseignement défense et sécurité au sein de l'ESIEA explique : **« Dans leur cursus, ces étudiants empilent les compétences, mais à aucun moment on ne les met dans une situation où ils doivent tout utiliser. À cela on ajoute du stress avec des gens en kaki qui viennent leur mettre la pression ».** L'enseignant ajoute : **« À la fin de la journée, ils sont fatigués. Après un précédent exercice, une étudiante a dormi 22 heures d'affilée. »**

« C'est la première fois que je suis confronté à une telle situation, cela me montre une autre facette », note Baptiste Mergeay, étudiant qui a endossé le rôle de chef d'un des deux groupes.

Le ComCyber comprend 4 000 « cybercombattants » ; civils ou militaires. Ce genre d'exercice est aussi pour l'armée l'occasion de repérer des talents. **« Les étudiants pensent entreprise, mais il y a aussi l'État ou l'Europe qui peuvent être intéressés par leurs compétences »,** conclut Richard Rey.

Nicolas GOINARD.