Éducation Journée de sensibilisation à la sécurité sur le web ce jeudi au département Réseau et télécommunication de l'IUT de Belfort-Montbéliard. Où l'on voit que les hackers sont surtout des « gentils ».

La double face du dieu internet

ORGANISER UNE JOURNÉE sécurité au sein d'une antenne spécialisée informatique de l'IUT n'est-ce pas un peu redondant, voire inutile ? De l'avis de tous, professeurs comme élèves, bien au contraire.

D'abord la technologie évolue vite. Ensuite et surtout le nombre d'utilisateurs du web en général est en telle expansion que mathématiquement il se trouve, parmi eux, un certain nombre de malhonnêtes et/ou d'espions. Enfin, de l'avis de Geoffrey Glangine, président de l'association belfortaine HackGyver, les cordonniers sont souvent les plus mal chaussés : même pour des futurs informaticiens ou techniciens, le cursus scolaire ne fait pas toujours la part belle aux questions de sécurité.

■ **Le jeune président de HackGyver, titre qui fait référence, pour les moins de trente ans, à la débrouillardise légendaire du certain Mac Gyver…** Photo Lionel VADAM

Eviter l'espionnage industriel

À Montbéliard, l'IUT s'est, lui, saisi de la question : cela fait quatre ans que le département réseau et télécommunication organise le Sécu'RT, journée ouverte à tous les étudiants du campus des Portes du Jura mais aussi aux chefs d'entreprise. Car c'est d'abord chez eux que se pose de manière cruciale la sécurité des réseaux informatiques. Son absence ouvre bien sûr la porte à l'espionnage industriel ou intellectuel. Mais la perte de confidentialité ou tout simplement le non-recrutement de personnes dédiées au sujet et compétentes ouvrent la porte à d'autres abus. « Une faille dans un réseau commercial ou autre permet de récupérer toutes les données clients. Des choses personnelles mais aussi des codes bancaires par exemple », explique Geoffrey Glangine. Embêtant…

Son association, fondée en 2007 et qui rassemble deux fois par semaine à l'Usine de Belfort des passionnés de divers horizons, ne gère pas directement ces problèmes. Mais, composée majoritairement par des hackers, elle dispose d'une expertise sur le sujet. D'où sa triple intervention, parmi une dizaine d'autres participants au podium, business développer, consultante en stratégie de communication, lieutenant des armées ou encore spécialiste du droit numérique, lors de cette journée.

Mais les hackers, ce ne sont pas des « méchants », ça ?

Des cas à la limite de la légalité

L'expression fait sourire le jeune (et gentil) étudiant. Car, comme tout outil -car ce ne sont que ça- l'informatique comme le web, peuvent être utilisés par les forces du mal (les terroristes en l'occurrence) comme celles du bien. « En Corée du Nord, en Syrie, pendant les printemps arabes, les hackers ont permis de contourner la censure et la répression d'état et d'informer le monde », souligne un membre de l'association, qui évoque également le rôle social et politique d'Edward Snowden.

Sans parler des cas à la limite de la légalité, les hackers, les « white hat » par opposition aux méchants « black hat » aujourd'hui sont recherchés par les entreprises : alors que les seconds piratent leur site web pour de l'argent, les premiers testent le système de sécurité afin d'éviter qu'il ne ressemble à un gruyère !

Même en termes de sécurité de la société, les cyber vigilants ont toute leur place : ils savent comment accéder au deep web où se trament des échanges tout sauf clairs (d'armes par exemple) et des complots. Le principe est simple et ancien : on ne lutte bien que contre ce qu'on connaît. La confidentialité et la sécurité sont ici les deux faces d'une même médaille.

Une chose est certaine : le domaine de la cyber sécurité a le vent en poupe. Question emploi, c'est et ce sera une belle piste d'avenir pour les étudiants. Rien qu'hier, des stages étaient proposés pour la sécurité informatique des armées.

Sophie DOUGNAC