Les Echos

LE **POINT DE VUE**

de **Nicolas Arpagian**

Les entreprises doivent se mettre au « hacking »

Il est révolu le temps où l'identification par un chasseur de têtes d'un profil compétent en informatique se résumait à la présence du candidat envisagé dans l'annuaire des anciens de Télécom ParisTech. Un des chantiers qui conditionne aujourd'hui la pérennité des entreprises est certainement celui de la cybersécurité. Pas une semaine ne passe sans que soit révélée la pénétration du système d'information d'un groupe industriel ou la publication de fichiers sensibles d'une administration gouvernementale.

La cybersécurité est plus que jamais le point de faiblesse des organisations économiques, politiques, administratives ou militaires les plus puissantes de la planète. Malgré cela, on constate toujours un réel conservatisme dans les méthodes de recrutement et de formation pour ces tâches pourtant éminemment stratégiques – alors même que le caractère innovant de cette notion de cybersécurité exige une remise à plat du mode d'appréhension des compétences dans ce domaine.

Ici, le diplôme ne constitue pas nécessairement l'indication d'une véritable aptitude à appréhender les problématiques de l'attaque informatique. Seul le hacker détient cette faculté de décortiquer un système au point d'en repérer les failles et les faiblesses. Une disposition de l'esprit qui mêle débrouillardise, inventivité et créativité à un bagage technique souvent acquis de manière très empirique. Le suivi d'un enseignement académique figé n'est souvent pas le cadre d'épanouissement idéal pour ces talents aux capacités créatives bien spécifiques.

De telles dispositions ne sont pas distinguées par un diplôme et pourtant elles sont indispensables pour anticiper les formes multiples d'attaques informatiques. Et donc préparer au mieux les organisations à limiter les effets d'une intrusion malintentionnée. Ce savoir-faire ne peut être identifié par les voies traditionnelles du recrutement. Il suppose en effet de faire appel à d'autres moyens d'évaluation de ces compétences hors norme.

> Seuls les hackeurs ont la faculté de décortiquer un système au point d'en repérer les failles.

> Il convient d'organiser sans tarder des filières de formation qui intègrent ces profils atypiques.

Idem quand il s'agit de procéder à l'analyse d'une attaque dont on pense avoir été la cible : pour identifier le mode opératoire, les cibles concernées et le type de dommage qui a pu être causé (vol ou détérioration de données, altération de systèmes…), il faut un(e) collaborateur(trice) qui soit doté(e) de cette tournure d'esprit. Ce qui suppose qu'on lui a laissé l'occasion de poursuivre un cursus scolaire approprié et que les filtres de recrutement aient su apprécier et jauger ses aptitudes si particulières.

Il convient donc d'organiser sans tarder des filières de formation qui intègrent ces profils atypiques, afin de doter les entreprises et les administrations françaises de ressources adaptées à la menace cybernétique. Le « hacking » ne doit pas être considéré comme une forme de piratage mais bien comme une capacité d'autonomie de la connaissance pour ne pas être cantonné au seul rôle de consommateur d'un outil technique.

Toutes les organisations (firmes commerciales, état-major ou administrations…) ont besoin de compter en leur sein ces tempéraments qui décortiquent l'appareillage technique qui irrigue désormais les systèmes d'information omniprésents dans nos infrastructures. C'est également de leur savoir-faire que naîtront les innovations technologiques de rupture. Précisément car ils (ou elles) ne se contentent pas d'être des utilisateurs, mais sont bien à leur manière des créateurs.

De tels esprits sont souvent plus difficiles à identifier, stimuler et canaliser que des « bêtes à concours » formatés pour des épreuves universitaires conventionnelles. Néanmoins, nous ne pouvons nous permettre de ne pas exploiter leur forme d'intelligence, qui correspond parfaitement à la logique des systèmes d'information de la société numérique construite autour de la valorisation des données. Et donc de leur sécurité.

Nicolas Arpagian est directeur scientifique du cycle sécurité numérique de l'Institut national des hautes études de la sécurité et de la justice (INHESJ).