Cybersécurité une guerre toujours gagnable ?

« Les cyberattaques sont une arme de la guerre cognitive »

À l'occasion du séminaire « Cybersécurité : une guerre toujours gagnable ? », organisé par la société savante Aristote, le 29 janvier prochain, Narisoa Ramarosy, directeur de programme pour Thales, et Yolande Lesueur, Business Development Manager pour Thales, co-organisateurs avec Alain Forestier, assistant scientifique et programmes au CEA, reviennent sur ce qui a motivé ce sujet et l'étendue de la guerre informatique dans le monde.

Lorsqu'on entend l'intitulé du séminaire, on a l'impression que la Cybersécurité est à un tournant. Pourquoi la prendre sous cet angle ?

Narisoa Ramarosy : Les actualités en 2025, ont été riches en cyberattaques, avec en point culminant, en décembre, le piratage du ministère de l'intérieur ou encore de La Poste. On pensait que ces organisations étaient des bastions imprenables, mais non, les hackers ont tout de même réussi à récupérer les Fichiers des Personnes Recherchées. La cybersécurité devient un vrai sujet central, et tout le monde commence à en avoir conscience. Mais un autre point saute aux yeux : la tournure des attaques.
Dans le contexte géopolitique, les tensions internationales, on voit que les cyberattaques deviennent un pilier de la guerre hybride. C'est devenu une arme réelle, développée et employée par des pays. Nous sommes loin du pirate dans son garage. Désormais ce sont de réelles entreprises, certains groupes ont des RH, des commerciaux, c'est beaucoup plus organisé que par le passé.

Yolande Lesueur : Pour nous ce sujet est vraiment d'actualité, et évolue constamment. C'est très important de se tenir informé, de sensibiliser et d'échanger différents points de vue. Nous accueillerons donc un nombre d'intervenants diversifiés, pour refléter des métiers et regards différents. Par exemple, Christophe Gaie, chef de division ingénierie et innovation numérique au sein des services du Premier ministre sera là, mais aussi des éditeurs, des start-ups, qui présenteront différentes solutions pour accompagner les entreprises (TPE, PME, groupe…). Nous n'avons pas souhaité organiser un séminaire essentiellement technique, mais aborder les thèmes sous des prismes différents et accessibles à tous. Par exemple, Nicolas Jeanselme, d'API Angel, nous présentera ce qu'il se passe « dans la tête d'un attaquant ».

Le but est de mieux se prémunir en amont sur un sujet qui peut paraître complexe lorsqu'on n'est pas dans le domaine de la cybersécurité.

N.R : Autre point important, Franck Rouxel de la Fédération Française de Cybersécurité sera là pour évoquer la notion d'antifragilité, ou un renversement de perspective afin de transformer les chocs des cyberattaques en leviers d'amélioration.

Y a-t-il une si grande diversité dans les manières d'attaquer une entreprise ?

Y.L : Oui. Les cyberattaques qu'on voit dans les médias ne constituent que les plus retentissantes. Mais de nombreuses entreprises sont attaquées en permanence. Vous prenez une entreprise comme Thales, c'est fréquent qu'elle soit visée sous forme diverses et variées.

N.R : Idem, les TPE-PME sont régulièrement la cible d'attaques. Dans l'écosystème de défense, la très grande majorité des attaques visent les sous-traitants. Il est beaucoup plus facile de récupérer des informations via les TPE-PME, mais les journaux n'en parlent que très peu. Aussi, les attaques atteignent également les citoyens. Des individus sont ciblés par du phishing, et se retrouvent avec le téléphone ou l'ordinateur bloqué, et les hackers demandent des rançons pour leur permettre de récupérer leurs photos de vacances. Ce sont les parties immergées de la cybersécurité. On n'en parle que très peu.

Y.L : Un intervenant abordera le sujet en ciblant les TPE-PME, pour une sensibilisation, des solutions ou pratiques permettant de se protéger.

Mais quel est le but exact de ces attaques ? Même si quelques données importantes sont volées, d'autres ne serviront jamais, n'est-ce pas ?

N.R : Pour s'attaquer à la réputation de l'organisation, du pays. Parfois, c'est juste pour la gloire mais bien souvent, la société ou l'organisation qui se fait cyberattaquer se retrouve décrédibilisée. Cela entaille son image dans le monde. C'est également une activité commerciale : il est possible de vendre les informations en aval. Mais cela fait aussi partie pour moi de la guerre cognitive, afin de démoraliser la société ou de faire en sorte qu'elle perde confiance en son État. C'est une manière de lui dire « votre État ne peut rien pour vous. Nous avons réussi à les attaquer ».

Lien vers la présentation et le programme du séminaire :
https://www.association-aristote.fr/evenements/seminaire-cybersecurite-une-guerre-toujours-gagnable/