Cybersécurité : enjeu sociétal et cause nationale

Jérôme NOTIN
Directeur Général
Cybermalveillance.gouv.fr

Une menace omniprésente

L'idée d'un dispositif pour assister les victimes d'actes de cybermalveillance est issue de la stratégie nationale pour la sécurité du numérique, destinée à accompagner la transition numérique de la société française. Une stratégie qui s'appuie sur 5 objectifs : garantir la souveraineté nationale ; apporter une réponse forte contre les actes de cybermalveillance ; informer le grand public ; faire de la sécurité numérique un avantage concurrentiel pour les entreprises françaises et renforcer la voix de la France à l'international.
C'est dans ce cadre précis que le Groupement d'Intérêt Public Action contre la Cybermalveillance est né en 2017. Son statut singulier alliant puissance publique et privée lui permet en effet de rassembler un large éventail d'acteurs et de démultiplier sa force de frappe auprès de 3 publics que sont les entreprises, les collectivités et les particuliers ; pour 3 missions : l'information, l'assistance aux victimes et l'observation de la menace.

Dans un monde quasi entièrement numérisé, de nouveaux enjeux, liés à l'évolution des usages numériques sont en effet apparus.

Ainsi, en l'espace de quelques années seulement, Cybermalveillance.gouv.fr a vu sa fréquentation passer de 200 000 visites en 2017 à plus de 3,8 millions en 2002. Au total, ce sont plus de 8 millions de personnes qui sont venues chercher de l'aide sur ce guichet unique de la Cybersécurité.
Un chiffre exacerbé lors de la pandémie, qui a constitué un facteur aggravant pour les menaces, en exploitant la vulnérabilité des collaborateurs travaillant à distance sans être systématiquement dotés des bons équipements ou des bons réflexes à avoir en matière de Cybersécurité.
Un chiffre, qui, s'il témoigne sans doute quelque peu de l'augmentation de la notoriété de la plateforme, met surtout en évidence l'explosion de la menace, avec un milieu cybercriminel qui s'est professionnalisé et qui a démontré sa capacité à s'adapter à l'actualité avec une créativité infinie.

Arnaque au faux support technique, à la vignette crit'air, au bois de chauffage, aux bons d'essence, au faux conseiller bancaire, mais aussi défiguration de site web, rançongiciel, attaque contre les IPBX … Au total, le dispositif recense à ce jour plus de 51 cybermalveillances et plus de 500 contenus allant des fiches pratiques, aux guides, tutos et autres vidéos pour éveiller et responsabiliser ses publics face à la menace.

Des publics très exposés et peu conscients du risque

Si l'intensification des menaces est avérée, si plus aucun secteur d'activité ou cible n'échappe aux attaques, si les médias n'en n'ont jamais autant

parlé, si le secteur de la Cybersécurité et des acteurs publics et privés se mobilisent avec des relais d'information et des initiatives, force est de constater que trop peu de publics, qu'il s'agisse de particuliers, d'entreprises ou de collectivités ont encore pris la mesure de l'enjeu qu'il représente.
En effet, près d'1 entreprise sur 2 ne dispose toujours pas de politique Cybersécurité et la plupart d'entre elles sont persuadées de ne pouvoir faire face au risque Cyber, 1/4 considère le risque comme faible ou inexistant [1] et 21 % n'ont pris aucune mesure depuis la crise sanitaire[2]. Côté collectivités, le constat est plus édifiant encore : 65 % d'entre elles pensent que le risque est faible ou inexistant, 2/3 des publics n'ont pas été sensibilisés à la sécurité numérique et près de 6 responsables informatiques sur 10 n'ont pas été formés à la Cyber[3].
Quant aux particuliers, 9 français sur 10[4] ont déjà été confrontés à un acte de cybermalveillance et plus de la moitié d'entre eux n'ont rien fait à l'issue de l'attaque…

Enfin, nous le savons, les impacts d'une cyberattaque peuvent être considérables et quelquefois même fatals pour les organisations. Vol de données, arrêt de l'activité, perte d'exploitation, dommages juridiques… Derrière ces préjudices se cachent aussi des coûts indirects et des enjeux liés aux atouts stratégiques et à la réputation des entités concernées avec des effets à plus long terme tout aussi délétères…

Faire d'un enjeu sociétal une démarche vertueuse

La sécurisation des publics passe bien évidemment par la sécurisation des équipements réalisée par des prestataires dont l'expertise est reconnue. Nous avons développé le label ExpertCyber pour permettre justement d'identifier les prestataires à l'état de l'art dans nos territoires. Mais dans un monde en pleine transformation, les solutions et les tuyaux ne suffisent plus à garantir la sécurité des publics.
Car le facteur humain est bien souvent en cause dans un incident Cyber ; ce qui signifie que nombre d'attaques auraient pu être évitées avec des individus avertis.

Dans un tel contexte, naviguer avec les bonnes cartes en main permettrait aux individus et aux organisations d'échapper à bien des déboires.

Car la Cybersécurité est l'affaire de Tous.
Bien-sûr, des dispositifs tels que Cybermalveillance.gouv.fr ont été conçus et imaginés pour comprendre et analyser les phénomènes de risques Cyber, pour sensibiliser et assister au mieux les victimes de ces menaces. Mais je reste convaincu que nous avons tous, nous, individus, entreprises et organisations, une responsabilité à porter en matière de cybersécurité.

Certains secteurs, comme l'environnement, par exemple, en ont d'ores et déjà fait la preuve. Ils sont nés d'une prise de conscience qui a conduit les individus, les organisations puis les Etats à prendre la mesure des enjeux et des risques encourus.
Et de ces politiques environnementales, souvent vécues comme des contraintes au début, sont nées des habitudes ou des règles de vie, des bonnes pratiques puis de vrais réflexes qui se sont imposés à tous, et que chacun d'entre nous s'est approprié au quotidien (tri sélectif, usage de produits non dangereux…).

Mieux encore, ces ***démarches vertueuses ont donné vie*** à de vraies innovations, comme le recyclage, par exemple… Que nul n'irait remettre en cause aujourd'hui.

[1] Source IPSOS pour CISCO
[2] Source MEDEF
[3] Etude Cybermalveillance.gouv.fr pour les collectivités de moins de 3500 habitants
[4] Source : Etude INC pour Cybermalveillance.gouv.fr

Autrement dit : *il revient à nous tous de définir l'objectif et le niveau d'exigence que nous voulons assigner à la Cybersécurité. Quelle importance souhaitons-nous lui donner ?*

Pour répondre à cette question, il suffit d'observer les dommages causés par des attaques au quotidien. Ou de revenir un instant au nombre de visiteurs uniques de Cybermalveillance.gouv.fr. En cette seule année 2022, il y a eu sur la plateforme autant d'internautes que les 4 années précédentes.

Le constat est sans appel : **il ne peut y avoir de transformation numérique sans Cybersécurité.** Et comme dans toute mutation, l'accompagnement des publics est indispensable.

L'État en a d'ailleurs fait une priorité en développant une stratégie nationale cyber qui s'inscrit dans le plan national d'investissement France 2030.
En rejoignant Cybermalveillance.gouv.fr, nos membres se sont, eux aussi, engagés à participer au rayonnement du dispositif et à partager les valeurs fondamentales de la sécurité numérique en relayant les réflexes clés à adopter.

Mais l'enjeu Cyber dépasse de loin notre dispositif et celui notre écosystème et chacun à son niveau, a un rôle à jouer pour **accompagner ce changement et vivre dans un monde numérique de confiance, *avec une Cybersécurité plus responsable.***

La Cybersécurité : un défi majeur, une cause nationale

Pour relever ce défi, il reste beaucoup à accomplir. Plusieurs entreprises et de nombreux particuliers nous ont déjà informé de leur volonté de prendre part à cette démarche qui s'inscrit pleinement dans la mission d'intérêt public du GIP.
Mais il nous faut aller plus loin.
C'est pourquoi Cybermalveillance.gouv.fr invite *toutes les organisations et tous les citoyens à* ***devenir des ambassadeurs de la Cyber.***

L'objectif ?
S'emparer de cet enjeu sociétal en proposant à chaque citoyen de devenir acteur de la Cyber ; permettre à chacun à son niveau, particulier, entreprise, collectivité ou association, de s'engager à faire de la Cyber *non seulement un levier d'innovation technologique* - en élevant le niveau de sécurité de ses équipements - mais *aussi un facteur de progrès social* en éveillant les consciences face à la menace.

La tâche est vaste et la réponse doit être collective pour atteindre la confiance numérique indispensable au développement économique et à la protection des citoyens.
Il existe de nombreuses façons d'apporter sa pierre à l'édifice « Cyber » : communiquer sur les bonnes pratiques et les réflexes à adopter ; former les collaborateurs et en faire des relais ; sensibiliser son écosystème et ses parties prenantes à cet enjeu et contribuer à accroître le niveau de connaissances et de compétences Cyber, pour une meilleure inclusion numérique.

Désormais, le mouvement est en route et chacun y a une place.

Alors qu'attendez-vous pour devenir, vous aussi, ambassadeur de la Cyber ?