ASSEMBLÉE NATIONALE

9 novembre 2022

D’ORIENTATION ET DE PROGRAMMATION DU MINISTÈRE DE L’INTÉRIEUR - (N° 436)

Commission	
Gouvernement	

Rejeté

AMENDEMENT

N º 470

présenté par
Mme Ménard

ARTICLE ADDITIONNEL

APRÈS L'ARTICLE 16, insérer l'article suivant:

Dans les trois mois qui suivent la promulgation de la présente loi, le Gouvernement remet au Parlement un rapport en vue de proposer des solutions concrètes et efficaces pour lutter efficacement contre les cyberattaques et plus particulièrement contre les tentatives croissantes de compromission de cibles de haute valeur.

EXPOSÉ SOMMAIRE

Depuis le début de la crise sanitaire en France, les cybermenaces ont augmenté de 400 % et 50 % des entreprises déclarent avoir constaté une augmentation significative des attaques suite à la généralisation du télétravail. Le développement du télétravail lié à la crise sanitaire oblige les entreprises à investir dans des dispositifs de sécurité.

Par ailleurs, lors de son rapport annuel d’activité, le GIP ACYMA (Groupement d’Intérêt Public Action contre la Cybermalveillance) révèle une hausse importante des demandes d’assistance en ligne.

Au travers de la plateforme cybermalveillance.gouv.fr, 173 000 demandes en 2021 soit 65 % de plus que l’année 2020 de demandes d’aide de victimes de cyber attaques ont été collectées. Concernant les particuliers, 31 % des demandes portaient sur l’hameçonnage, 19% concernant le piratage de compte et 13 % sur les faux supports techniques. Pour les professionnels, la première cause reste les rançongiciels également appelés ransomwares (environ 22%).

Enfin, ainsi que l’a souligné notre collègue Aurélien Lopez-Liguori dans son avis versé au PLF 2023 sur les communications électroniques et l’économie numérique, "les cybercriminels tendent à attaquer, de façon récurrente, les prestataires de services d’hébergement, de maintenance logicielle

ou les professions juridiques, ce qui leur permet d’exercer une pression plus importante pour obtenir des paiements ou d’accéder à des données d’intérêt faisant l’objet de divulgation ou de revente. Le ciblage de personnalités publiques par des outils de surveillance fait également partie des menaces visant des cibles de haute valeur. L’utilisation d’outils sophistiqués complique la détection de ce type de compromission et l’attribution des attaques à leurs commanditaires."

Face à cette menace aussi massive qu'exponentielle, si l'on peut saluer la création de 1 500 "cyber-patrouilleurs", d'une école de formation cyber et du "17 cyber" pour signaler une cyberattaque, on peut également se demander si ces efforts seront suffisants.