ASSEMBLÉE NATIONALE

17ème législature

Les défaillances en cybersécurité des entreprises françaises

Question écrite n° 3971

Texte de la question

M. Aurélien Saintoul alerte Mme la ministre déléguée auprès du ministre de l'économie, des finances et de la souveraineté industrielle et numérique, chargée de l'intelligence artificielle et du numérique, sur les défaillances en cybersécurité des entreprises françaises. En 2024, une masse très alarmante de données sensibles ont été volées aux Français par le biais de cyberattaques. En février 2024, 33 millions de Français ont été concernés par des attaques visant Viamedis et Almerya, deux entreprises clés du secteur de la santé publique puisqu'elles assurent le fonctionnement du tiers-payant de la Sécurité sociale. Ce genre d'opération met en lumière la faiblesse structurelle des entreprises face à ces menaces qui ne sont désormais plus nouvelles. En mars 2024, c'est France Travail qui a été visée par une attaque touchant 43 millions de Français, permettant aux cybercriminels de revendre ces données à des acheteurs du monde entier. Ces mêmes acheteurs en profitent ensuite pour usurper l'identité des citoyens afin d'alimenter des trafics criminels allant de l'escroquerie au terrorisme. Ce phénomène d'ampleur a aussi touché en 2024 de nombreuses entreprises de la grande distribution telles que Boulanger, Cultura, Fnac, Darty, Picard, Truffaut, Auchan et Intermarché. Des entreprises de télécommunications ont, par ailleurs, été atteintes comme Free et SFR, qui à la suite de cyberattaques cumulent à elles deux, près de 23 millions de données d'utilisateurs volées. Les attaquants ont obtenu les relevés d'identité bancaire des clients de SFR et Free et en ont revendu une partie à des réseaux criminels internationaux selon *Les Échos*. Pourtant, les entreprises de télécommunications sont des « opérateurs d'importance vitale » (OIV) et sont donc tenues à des obligations de renforcement et de détection des intrusions sur leurs systèmes. Or ces obligations n'ont visiblement pas suffi à protéger les données privées des usagers. La France est désormais particulièrement visée par les cybercriminels : car ces pirates se concentrent d'abord sur les cibles faciles dont les failles et les données sont déjà connues. D'autant plus que la France accuse toujours un retard dans la transposition de la directive européenne Sécurité des réseaux et de l'information 2 (NIS2) dont la date limite de transposition était le 17 octobre 2024 ; et que cette mesure n'a pourtant toujours pas été débattue à l'Assemblée nationale, au Sénat ni même en Conseil des ministres. Ainsi, M. le député voudrait savoir ce que le Gouvernement prévoit pour lutter contre les cyberattaques dans les secteurs public et privé et s'il s'est fixé un calendrier afin de transposer la directive NIS2 dans le droit français dans les plus brefs délais. Il voudrait connaître les accompagnements prévus par le Gouvernement pour les victimes de cyberattaques et pour les entreprises ciblées et sacoir si des mesures de réparations et des campagnes de sensibilisation sont prévues. Il demande si des sanctions sont à l'agenda pour les entreprises négligentes à l'égard de leur système de sécurité.

Texte de la réponse

Face à une cybermenace devenue systémique, l'élévation du niveau général de sécurité du tissu économique et social français est une nécessité. La directive européenne NIS 2 contribue à répondre à ce besoin. La directive – dont les travaux de transposition en droit national par les assemblées parlementaires aboutiront en 2025 - impose un niveau de cybersécurité minimal de référence à des organisations dites critiques, à travers l'application de règles de sécurité informatique proportionnées au besoin et harmonisées. Dans le cadre de cette

nouvelle réglementation, les entités assujetties auront notamment l'obligation de notifier les incidents importants dont elles seront victimes. Les entités assujetties auront également l'obligation de mettre en place des mesures techniques, opérationnelles et organisationnelles adéquates, adaptées aux risques qui pèsent sur leurs réseaux et systèmes d'information. Le Gouvernement prévoit une mise en œuvre progressive de ces différentes obligations, ainsi que du régime de supervision destiné à les contrôler. L'accompagnement des entités assujetties prendra plusieurs formes, dont l'accès à l'offre de services de l'ANSSI, via le portail Internet MesServicesCyber. Un service en ligne destiné aux entités assujetties, MonEspaceNIS2, la mise en place de relais dans les territoires, ainsi qu'un appui en termes d'expertise de l'administration aux programmes d'aide en cybersécurité portés par les secteurs sont aussi prévus. Au total, l'objectif est de créer un mouvement vertueux et d'irriguer au-delà des entités assujetties par la mise en place de mécanismes incitatifs.

Données clés

Auteur : M. Aurélien Saintoul
Circonscription : Hauts-de-Seine (11e circonscription) - La France insoumise - Nouveau Front Populaire
Type de question : Question écrite
Numéro de la question : 3971
Rubrique : Numérique
Ministère interrogé : Intelligence artificielle et numérique
Ministère attributaire : Premier ministre

Date(s) clée(s)

Question publiée au JO le : 11 février 2025, page 686
Réponse publiée au JO le : 22 avril 2025, page 2898