ASSEMBLÉE NATIONALE

17ème législature

Piratage de l'ANTS

Question écrite n° 15644

Texte de la question

M. Jocelyn Dessigny attire l'attention de M. le ministre de l'intérieur sur les défaillances structurelles de l'État en matière de cybersécurité, illustrées de façon particulièrement grave par le piratage de l'Agence nationale des titres sécurisés (ANTS). Le 15 avril 2026, le portail moncompte.ants.gouv.fr, plateforme régalienne centralisant les demandes de passeports, cartes d'identité, permis de conduire et titres de séjour, a été victime d'une cyberattaque. Entre 12 et 18 millions de lignes de données auraient été exfiltrées puis proposées à la vente sur des forums cybercriminels. La faille exploitée (une vulnérabilité IDOR basique sur une API) a été qualifiée par le *hacker* (âgé de seulement 15 ans) lui-même de « vraiment stupide » : il suffisait de modifier un chiffre dans une requête pour accéder aux données d'un autre citoyen. Ce n'est pas une attaque sophistiquée d'un État ennemi. C'est une faille élémentaire, qui n'aurait jamais dû exister sur un système gouvernemental gérant les documents d'identité de dizaines de millions de Français. Depuis le début de l'année 2026, les cyberattaques contre les administrations françaises se multiplient à un rythme alarmant : en janvier, le fichier FICOBA du ministère de l'économie a été piraté avec 1,2 million de comptes bancaires compromis ; en février, la CAF a été frappée avec environ 70 000 dossiers RSA exfiltrés ; en mars, les bulletins de 3,5 millions d'élèves ont été mis en vente sur le *dark web* après le piratage d'EduConnect. L'espace numérique de l'État français est devenu une passoire. La stratégie nationale de cybersécurité 2026-2030, présentée en janvier 2026, ne mentionne aucun chiffre budgétaire, un point qui cristallise les critiques des experts du secteur. Le rapport ANSSI publié le 11 mars 2026 révèle que près de 29 % des vulnérabilités exploitées en 2025 l'ont été le jour même de leur publication ou avant et que plus de 6 200 actifs en France restaient encore vulnérables fin 2025 à des failles connues depuis 2023 ou 2024. La lenteur dans l'application des correctifs est systémique. Elle n'est pas une fatalité : c'est un choix de gestion. Face au scandale, M. le Premier ministre a qualifié la situation de « casse du siècle » qui aurait lieu « pratiquement tous les mois » et annoncé une enveloppe de 200 millions d'euros. Pour autant, des annonces budgétaires réactives, formulées après chaque scandal, ne constituent pas une politique de sécurité. Les Français sont en droit d'exiger mieux que des rustines post-incident sur des systèmes qui gèrent leurs données les plus sensibles. Il lui demande quelles mesures structurelles, et non conjoncturelles, il entend mettre en œuvre pour garantir la sécurité des systèmes d'information régaliens ; quel calendrier d'audit obligatoire est prévu pour l'ensemble des plateformes gouvernementales traitant des données personnelles et comment l'État entend rendre compte aux citoyens dont les données ont été compromises des suites données à ces incidents répétés.

Données clés

Auteur : M. Jocelyn Dessigny
Circonscription : Aisne (5e circonscription) - Rassemblement National
Type de question : Question écrite
Numéro de la question : 15644
Rubrique : Numérique
Ministère interrogé : Intérieur
Ministère attributaire : Premier ministre

Date(s) clée(s)

Version web : https://www.assemblee-nationale.fr/dyn/17/questions/QANR5L17QE15644

Question publiée au JO le : 2 juin 2026, page 4748