ASSEMBLÉE NATIONALE

16ème législature

Fuite des données personnes de participants au SNU

Question écrite n° 13900

Texte de la question

M. Bastien Lachaud interroge Mme la secrétaire d'État auprès du ministre des armées et du ministre de l'éducation nationale et de la jeunesse, chargée de la jeunesse et du service national universel, sur la récente fuite de données personnelles de participants au service national universel (SNU). Depuis le 22 novembre 2023, une base de données du SNU contenant les données personnelles de plus de 60 000 mineurs est en vente sur un forum de cybercriminels pour la somme de 50 dollars. La situation a été signalée au ministère de l'éducation nationale dès le 24 novembre 2023. Ce n'est qu'à partir du mercredi 6 décembre 2023 que des milliers de volontaires du SNU ont été informés du vol de leurs données. Les informations dérobées sont : le nom, le prénom, la date de naissance, l'adresse postale et l'adresse *mail*. Cette fuite de données concernerait 62 500 jeunes (nouveaux et anciens volontaires) et 87 000 parents, soit environ 150 000 personnes. Dans le *mail* envoyé aux victimes de cette fuite, l'administration du SNU explique avoir porté plainte et mettre « tout en œuvre pour limiter la diffusion de ces données, avec l'aide des autorités ». Aucune information n'a cependant été fournie aux victimes pour prévenir les risques d'hameçonnage (*phishing*) découlant du vol de données. Enfin, l'administration ne précise pas d'où provient la fuite. On ne sait donc pas comment un cybercriminel a accédé aux données personnelles de 150 000 personnes inscrites sur le site du SNU rattaché à l'éducation nationale. De plus, le SNU permettant d'obtenir automatiquement le certificat individuel de participation (CIP) à la Journée défense et citoyenneté (JDC). Ces données revêtent ainsi un caractère particulièrement sensible. Cette situation interroge sur la politique de sécurité des données mise en place par le SNU. Il est crucial d'établir l'origine de cette cyberattaque afin de renforcer les défenses et de prévenir de futures violations de données. C'est pourquoi M. le député souhaite savoir si les services du ministère connaissent l'origine de la cyberattaque (erreur interne ou contournement des systèmes de sécurité mis en place) et, au surplus, les mesures envisagées par M. le ministre pour prévenir ce genre d'attaque. Il souhaite également savoir où sont stockées les données utilisées par le site du SNU (en France, en Europe ou à l'étranger). Enfin, il souhaite savoir si les victimes de la cyberattaque recevront une information concernant les risques d'hameçonnage dont ils pourraient être la future cible.

Texte de la réponse

Le site Internet du SNU a été la cible d'une cyberattaque, directement signalée à la délégation générale au service national universel (DGSNU), laquelle a immédiatement lancé une procédure de vérification. L'origine de cette cyberattaque a ainsi été identifiée : l'exploitation par un individu malveillant d'une faille applicative, qui a été corrigée immédiatement après la découverte du vol de données. La situation a ainsi été rapidement maitrisée et les inscriptions pour les séjours de 2024 ont pu se poursuivre. Le procureur de la République a été également été saisi par la DG SNU et l'enquête est en cours. Un signalement a par ailleurs été fait à la CNIL, conformément au cadre applicable en matière de protection des données à caractère personnel. Les données volées ne comprennent pas d'identifiants ou de mots de passe permettant d'accéder aux plateformes, ce qui a permis de limiter les conséquences. Tous les jeunes ayant fait l'objet d'un piratage de données ont été prévenus, ainsi que leurs représentants légaux. Pour faire face à de tels risques, les plateformes du SNU sont

homologuées dans le cadre du Référentiel général de sécurité (RGS), ainsi que de la politique de sécurité des systèmes d'information de l'État (PSSIE). Elles bénéficient à ce titre d'une homologation dédiée auprès de l'ANSSI. Les dispositions de sécurisation des plateformes sont conformes aux normes légales et règlementaires, tandis qu'un audit de sécurité est réalisé chaque année par un prestataire agréé. Il comprend un examen approfondi des éléments logiciels ainsi que des tests d'intrusion et une évaluation des protections (pare-feu) mis en place. Les données sont hébergées en France, conformément aux règles qui s'appliquent aux plateformes numériques de l'État. En complément et afin de prévenir la réitération de tels faits, un plan d'action a été engagé par la DGSNU. Ainsi, les plateformes du SNU vont faire l'objet d'un nouvel audit de sécurité en 2024, qui s'inspirera des faits récents pour s'assurer du meilleur niveau de sécurité pour le futur système d'information du SNU en construction, avec pour priorité première de renforcer la protection des données.

Données clés

Auteur : M. Bastien Lachaud
Circonscription : Seine-Saint-Denis (6e circonscription) - La France insoumise - Nouvelle Union Populaire écologique et sociale
Type de question : Question écrite
Numéro de la question : 13900
Rubrique : Numérique
Ministère interrogé : Jeunesse et service national universel
Ministère attributaire : Éducation et jeunesse

Date(s) clée(s)

Question publiée au JO le : 19 décembre 2023, page 11399
Réponse publiée au JO le : 19 mars 2024, page 2192