ASSEMBLÉE NATIONALE

16ème législature

Protection cyber des PME de la BITD française

Question écrite n° 4174

Texte de la question

Mme Isabelle Santiago attire l'attention de M. le ministre des armées sur le soutien apporté aux PME de la BITD en matière de cyberdéfense. La question de la cyberdéfense est aujourd'hui plus que jamais essentielle, alors qu'on voit régulièrement à l'œuvre des attaques en ligne, notamment russes. Le ministère des armées et les grandes entreprises qui assurent la prospérité du complexe militaro-industriel français sont habitués à devoir se défendre face à de telles attaques. Elles en ont les moyens. Mais derrière cette dizaine de fleurons français, de mastodontes économiques, il y a des milliers de PME qui constituent l'essentiel de la BITD française. Or en France, 60 % des PME ferment après avoir été victimes de cyberattaques. Autant dire qu'en cas d'attaques massives, les PME de la BITD française ne tiendraient pas le choc. Il existe certes des financements, notamment de Bpifrance à hauteur de 80 % pour les PME qui le demandent. Or, pour en bénéficier, il faut que le SGA atteste du caractère « critique » de l'entreprise. Mais seule le SGA a la liste de ces PME critiques. C'est donc à la PME d'investir pour se mettre en conformité avec les nouvelles conditions que la DGA compte mettre en place pour les futurs marchés. Mais les PME n'ont généralement pas les moyens d'avoir un RSSI. Les maîtres d'œuvre industrielle travaillent sur un référentiel national à quatre niveaux et les PME qui se verraient attribuer un niveau 3 ou 4 seraient contraintes d'acquérir des systèmes cybers hors de prix pour une PME. On se retrouve donc dans une situation paradoxale. Les cyberattaquants visent de moins en moins les grosses entités et ciblent davantage les plus petites, mais ces petites entités n'ont pas les moyens suffisants pour se protéger. Des mesures semblent devoir être prises. Il faut soit des financements nouveaux fléchés vers les PME pour leur protection cyber, soit mettre en place un service de RSSI tournant qui assurerait la défense de plusieurs PME. Dès lors, elle lui demande commet il compte, en concertation avec d'autres acteurs, améliorer la cyberdéfense des PME de la BITD.

Texte de la réponse

Le niveau de maturité cyber des PME et ETI sous-traitantes au sein de la base industrielle et technologique de défense (BITD) est un point d'attention du ministère des armées depuis plusieurs années. En atteste la signature en 2018 avec les principaux industriels de l'armement de la convention cyber dont un volet porte sur la sécurisation des sous-traitants les plus critiques. Dans le même ordre d'idée, le lancement mi-2020 du dispositif « Diag Cyber Défense », financé par la direction générale de l'armement et distribué par Bpifrance, permet à une PME ou ETI de la BITD de solliciter une aide pour faire établir son état de vulnérabilités par un expert reconnu par l'agence nationale de la sécurité des systèmes d'information (ANSSI) et bénéficier d'un plan de mesures correctives à mettre en œuvre. Cette aide financière est effectivement réservée aux entreprises les plus critiques de la BITD. L'année 2022 a vu une amplification de l'état de la menace et, parallèlement, le ministère, dans le cadre du passage à une économie de guerre, a pris différentes initiatives qui devraient se concrétiser au cours de l'année afin d'accélérer la cybersécurisation de tous les opérateurs économiques de la BITD : l'élaboration, avec l'appui de l'ANSSI, d'un cadre de maturité cyber national à destination des entreprises en contrat direct ou indirect (sous-traitant) avec le ministère ; la mise en œuvre d'un processus de certification des entreprises afin de garantir la conformité de ces dernières au nouveau cadre de maturité et l'intégration

progressive dans les contrats de clauses imposant la conformité au nouveau cadre de maturité. L'objectif est, dans un premier temps, d'amener les sous-traitants de la BITD au premier niveau « socle » du cadre de maturité, afin d'augmenter leur résilience dans le cas des attaques les plus courantes. Les services compétents du ministère et de l'ANSSI estiment que le coût de cette mise en conformité dans une petite structure est négligeable car elle met principalement en jeu des mesures organisationnelles et appelle à déployer des configurations de sécurité au sein d'équipements informatiques usuels, dont sont déjà équipées les entreprises. Néanmoins, le ministère des armées est conscient de la nécessité d'accompagner les PME de la BITD, dont la gouvernance en matière cyber s'avère souvent perfectible, en particulier dans l'optique du rehaussement, dans un second temps, pour certaines d'entre elles, du niveau de certification requis afin de tenir compte de la sensibilité des prestations confiées dans le cadre des nouveaux programmes. En lien avec les régions, des programmes locaux de montée en maturité cyber pour certaines PME duales doivent être progressivement lancés. Ils incluent, dans certains cas, une prestation d'un responsable de la sécurité des systèmes d'information (RSSI) externalisé intervenant au profit de plusieurs PME, afin de leur permettre notamment de se maintenir au niveau requis dans la durée. Un premier programme de ce type est opérationnel en région Auvergne Rhône-Alpes, par l'intermédiaire du pôle de compétitivité MINALOGIC. De même, une coopération a été établie avec le groupement professionnel GIFAS qui dispose depuis plusieurs années, via son programme AirCyber, d'une démarche analogue à destination des sous-traitants aéronautiques dont certains relèvent également de la BITD.

Données clés

Auteur : Mme Isabelle Santiago
Circonscription : Val-de-Marne (9e circonscription) - Socialistes et apparentés (membre de l'intergroupe NUPES)
Type de question : Question écrite
Numéro de la question : 4174
Rubrique : Défense
Ministère interrogé : Armées
Ministère attributaire : Armées

Date(s) clée(s)

Question publiée au JO le : 20 décembre 2022, page 6327
Réponse publiée au JO le : 7 mars 2023, page 2171