ASSEMBLÉE NATIONALE

15ème legislature

Question N° : 44566	De **M. Pierre-Yves Bournazel** (Agir ensemble - Paris)	**Question écrite**

Ministère interrogé > Transition numérique et communications électroniques	**Ministère attributaire** > Premier ministre

Rubrique >Internet	**Tête d'analyse** >Cyberattaques et protection des collectivités publiques	**Analyse** > Cyberattaques et protection des collectivités publiques.

Question publiée au JO le : **01/03/2022**
Réponse publiée au JO le : **03/05/2022** page : **2947**
Date de changement d'attribution : **15/03/2022**

Texte de la question

M. Pierre-Yves Bournazel interroge M. le secrétaire d'État auprès des ministres de l'économie, des finances et de la relance, et de la cohésion des territoires et des relations avec les collectivités territoriales, chargé de la transition numérique et des communications électroniques, sur la protection des collectivités publiques ainsi que du tissu socio-économique de leur territoire contre les cyberattaques. En deux ans, nombre de collectivités publiques ont été victimes de cyberattaques sous la forme de rançongiciels. Pour la seule région parisienne, près d'une dizaine de communes ont été victimes de cyberattaques. Le plan de relance 2020-2022 a prévu une enveloppe de 136 millions d'euros sur la période 2021-2022 pour la cybersécurité. L'ANSSI, l'Agence nationale de la sécurité des système d'information, a pour mission de piloter la mise en place de cette cybersécurité, en venant en appui des régions candidates à la création d'un centre régional. Chaque région candidate dispose d'un soutien financier à hauteur d'un million d'euros et d'un accompagnement méthodologique sous la forme d'un programme de formation de quatre mois. Sept régions (sur treize) ont d'ores et déjà signé avec l'ANSSI pour la création d'un tel centre de réponse régional. Il souhaiterait savoir comment le Gouvernement compte encourager l'ensemble des régions à se doter de ce dispositif afin de permettre une couverture de l'ensemble du territoire.

Texte de la réponse

La menace touche l'ensemble de notre société et affecte indéniablement nos concitoyens. En conséquence, le Gouvernement a fait le choix stratégique de doter le plan France Relance d'un volet consacré au renforcement de la cybersécurité. Dans ce cadre, une première enveloppe de crédits a été fixée à 136 M€. Elle a été complétée de 40 M€ en 2022. L'objectif stratégique poursuivi est, prioritairement, de réhausser le niveau de sécurité numérique de l'Etat et des services publics. Les actions mises en place sont donc destinées aux collectivités territoriales, aux établissements de santé, aux autres établissements publics et aux institutions publiques, parmi lesquelles les ministères. Outre l'accélération de la mise en œuvre de nouveaux services de cybersécurité pour les agents et réseaux de l'Etat, plusieurs dispositifs sont accessibles aux collectivités territoriales, parmi lesquels le soutien à la création de centres territoriaux de réponse à incident de cybersécurité. Ces projets, portés par les conseils régionaux, permettront d'apporter une réponse à toutes les victimes de cyberattaques sur l'ensemble du territoire considéré. En effet, nombre d'acteurs socio-économiques primordiaux à l'échelle régionale sont aujourd'hui démunis face aux cyberattaques. Au printemps 2022, dix régions métropolitaines se sont déjà vues accorder un

soutien financier d'un million d'euro chacune pour créer un centre régional de réponse à incident. Parmi elles, sept suivent actuellement un programme d'incubation qui permettra de rendre ces structures opérationnelles d'ici la fin de l'année 2022. D'autres régions devraient incessamment se déclarer candidates à la création de centre de réponse à incident. Elles suivront un programme d'incubation similaire au second semestre. Le Gouvernement espère que l'ensemble des régions s'engagera in fine dans cette démarche. Il convient de signaler explicitement que ce dispositif a vocation à être pleinement adopté dans les outre-mer. Des discussions sont en cours pour adapter les structures aux spécificités géographiques ou économiques de ces territoires. D'ici l'été 2022, plusieurs projets seront soutenus, par zone géographique. Il s'agira de faire émerger un tissu de prestataires locaux en cybersécurité capables d'œuvrer en matière de prévention, de sécurisation et de réponse à incidents, de diffuser les bonnes pratiques en les adaptant aux contextes locaux et de faire émerger des offres de formation locales. Enfin, au-delà du soutien à la création de ces structures, en métropole ou en outre-mer, l'enjeu réside dans leur pérennisation : le modèle de fonctionnement devra prendre en compte le service rendu aux acteurs locaux et assurer auprès des victimes sa mission de réponse de premier niveau en cas d'attaque. Ces structures pourront également proposer des prestations pertinentes et à forte valeur ajoutée pour le tissu économique local et engager ainsi des collaborations étroites avec les fédérations locales, les conseils régionaux et départementaux, les chambres de commerces et les secteurs industriels locaux.