N°6607
Entrée le 04.08.2022
Déclarée recevable
Président de la Chambre des Députés
(s.) Fernand Etgen
Luxembourg, le 04.08.2022

Monsieur Fernand Etgen
Président de la Chambre
des Députés

Luxembourg, le 4 août 2022

Monsieur le Président,

Par la présente, nous avons l'honneur de vous informer que, conformément à l'article 80 du Règlement de la Chambre des Députés, nous aimerions poser une question parlementaire à Monsieur le Premier Ministre, Ministre d'Etat, à Monsieur le Ministre des Communications et des Médias, à Monsieur le Ministre de l'Energie, à Monsieur le Ministre de l'Economie, à Monsieur le Ministre des Classes Moyennes et à Madame le Ministre de la Protection des consommateurs au sujet d'une cyberattaque sur le groupe Encevo.

Dans un communiqué de presse daté du 25 juillet 2022, le groupe Encevo informe que :

« ses entités luxembourgeoises Creos (gestionnaire de réseau) et Enovos (fournisseur d'énergie) ont été victimes d'une cyberattaque dans la nuit du 22 au 23 juillet 2022. La cellule de crise du Groupe Encevo a été déclenchée immédiatement et la situation est actuellement sous contrôle. Nous sommes en train de réunir tous les éléments nécessaires à la compréhension et à la résolution complète de l'incident. Néanmoins, cette attaque a un impact négatif sur le fonctionnement des portails clients de Creos et d'Enovos. Nous nous excusons auprès de nos clients pour les désagréments et nous faisons au mieux afin de rétablir le service le plus rapidement possible. Creos et Enovos soulignent que la fourniture d'électricité et de gaz ne sont pas touchées et que le service de dépannage est garanti. »

Le 28 juillet 2022, le groupe publie un deuxième communiqué indiquant qu'un certain nombre de données ont été exfiltrées des systèmes informatiques ou rendues inaccessibles par les pirates. Encevo y souligne également que les personnes concernées par une violation de données seraient activement contactées.

D'après un article paru avant-hier sur lessentiel.lu, le groupe de pirates informatiques, BlackCat, aussi appelé ALPHV aurait revendiqué cette attaque et environ 150 gigabytes de données (180.000 fichiers, i.e. factures, e-mails, contrats etc.) auraient été dérobées.

Il est utile de rappeler dans ce contexte que le groupe Encevo domine largement le marché de l'électricité « retail » luxembourgeois avec une part de marché de quelque 90%. Au niveau du gaz pour ménages privés, la part de marché du groupe Encevo est plus réduite avec « seulement » 49,5% de la part de marché.

Notons également que l'Etat luxembourgeois est actionnaire du groupe Encevo à hauteur de 28%. Via la BCEE, Post Luxembourg, la SNCI et la Ville de Luxembourg, l'Etat contrôle de manière indirecte quelque 75% des actions du groupe.

Au vu de tout ce qui précède, nous souhaiterions poser les questions suivantes au gouvernement :

- Alors que le risque de cyberattaques a augmenté depuis l'invasion russe en Ukraine, le gouvernement peut-il nous détailler les recommandations adressées par les autorités compétentes (dont l'ANSSI) aux entreprises en général et aux entreprises gérant / exploitant des infrastructures critiques en particulier ?

- Le gouvernement peut-il nous confirmer que toutes les autorités compétentes (CNPD, ILR etc.) ont été dûment informées de la cyberattaque dont a été victime le groupe Encevo ? L'information a-t-elle également été dispatchée au niveau européen pour davantage sensibiliser les partenaires européens au risque de cyberattaques ?

- Le gouvernement considère-t-il que des cyberattaques puissent mettre à l'arrêt, du moins temporairement, l'approvisionnement en énergie du Luxembourg ?

    - Dans l'affirmative, quelles sont les diligences entreprises par les autorités gouvernementales pour parer à cette éventualité ?

- La stratégie nationale en matière de sécurité des réseaux et des systèmes d'information est-elle régulièrement mise à jour ?

- Les plans de sécurité et de continuité de l'activité des infrastructures critiques en général et des secteurs de l'énergie et des technologies de l'information et de la communication en particulier sont-ils toujours à jour et à la hauteur des défis actuels ? Une actualisation de ceux-ci est-elle actuellement en cours ?

- Le gouvernement peut-il nous indiquer si le groupe Encevo a effectué toutes les diligences (voir à cet égard e.a. l'article 32 du règlement (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données sur la sécurité des traitements) pour éviter faire l'objet d'une telle cyberattaque voire pour en minimiser l'impact

sur le réseau de gaz et d'électricité, voire sur ses clients, sachant que d'autres groupes européens du secteur énergétique ont au cours du mois de juillet 2022 déjà fait l'objet d'attaques similaires ?

- Le gouvernement peut-il nous confirmer que la CNPD organise, pour une attaque d'une ampleur telle celle dont a fait l'objet le groupe Encevo, une descente sur les lieux pour s'assurer que les mesures prises pour anticiper et contrer d'éventuelles attaques futures soient appropriées ? Le Haut-Commissariat à la Protection nationale, l'ANSSI, le CIRCL et le CERT Gouvernemental sont-ils associés à l'élaboration et l'implémentation de telles mesures ? Comment s'organise cette coopération concrètement ?

- Comment le groupe Encevo entend-il faire en sorte que toute personne concernée d'une violation de données à caractère personnel en est informée en temps utile (sachant que le site mis en place par le groupe Encevo dans le contexte de la cyberattaque ne contient actuellement que des généralités dont une foire aux questions) ?

- Quelle appréciation le gouvernement porte-t-il sur la composition de l'actionnariat actuel du groupe Encevo sur fond des tensions sino-américaines ?

- Le gouvernement dispose-t-il d'informations sur le groupe de pirates informatiques à l'origine de la cyberattaque sur le groupe Encevo ?

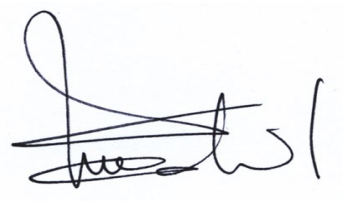
    - S'agit-il d'un groupe qui agit pour compte d'un ou de plusieurs Etat(s) étranger(s) ?

    - Dans l'affirmative, de quel(s) Etat(s) s'agit-il concrètement ?

- Le gouvernement dispose-t-il d'informations sur la hauteur de la rançon exigée par le groupe BlackCat ? Des rançons de ce genre ont-elles également été demandées dans le contexte de cyberattaques similaires (au Luxembourg ou à l'étranger) ?

- Le gouvernement juge-t-il probable que le groupe Encevo paie une telle rançon ?

Nous vous prions d'agréer, Monsieur le Président, l'expression de notre très haute considération.



Octavie Modert
Députée

Marc Spautz
Député