N°6607
Entrée le 02.09.2022

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Ministère d'État

Réponse commune de M. le Premier Ministre, Ministre d'État, de M. le Ministre des Communications et des Médias, de M. le Ministre de l'Énergie, de M. le Ministre de l'Économie, de M. le Ministre des Classes moyennes et de Mme la Ministre de la Protection des consommateurs à la question parlementaire n°6607 du 4 août 2022 des honorables Députés Octavie MODERT et Marc SPAUTZ

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 ?

En 2019, le Haut-Commissariat à la Protection nationale (HCPN) a rédigé un « Guide pour l'élaboration d'un Plan de sécurité et de continuité de l'activité » à destination des opérateurs d'infrastructure critique les invitant à tenir notamment compte du risque cybernétique. Le guide détaille la structure type d'un plan de sécurité et de continuité et propose une méthodologie pour l'élaboration d'un tel.

Suite à l'invasion de l'Ukraine, le HCPN (GOVCERT) a adressé le 2 mars 2022 une note de mise en garde aux opérateurs d'infrastructure critique et entités étatiques. Cette note rappelle les recommandations de base en matière de cybersécurité et renvoie par ailleurs aux recommandations de bonnes pratiques minimales « Boosting your Organisation's Cyber Resilience » élaborées conjointement par l'ENISA et de CERT-EU dans le contexte de la crise.

Le 19 avril 2022 HCPN/GOVCERT a réitéré sa mise en garde.

De son côté, l'Institut Luxembourgeois de Régulation (ci-après, « ILR » ou l'« Institut ») a décidé d'effectuer une veille renforcée du secteur afin d'identifier le cas échéant et en temps utile une éventuelle indisponibilité majeure d'un ou de plusieurs services essentiels.

À cette fin, l'Institut a, début mars, demandé aux opérateurs de services essentiels de lui fournir des rapports sur l'état actuel de la sécurité des réseaux et systèmes d'information selon les modalités décrites dans ledit courriel. Il a aussi invité les opérateurs de services essentiels étant également propriétaires ou opérateurs d'infrastructures critiques au sens de la loi modifiée du 23 juillet 2016 portant création d'un Haut-Commissariat à la Protection nationale de l'informer quelles mesures sont en place ou ont été prises.

Par ailleurs, l'ILR transmet régulièrement aux opérateurs de services essentiels des recommandations ou informations spécifiques concernant les menaces actuelles des différents secteurs (par exemple, des recommandations ou rapports de l'ENISA).

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 ?

Oui, les notifications respectives ont été émises entre le 23 et le 26 juillet 2022 aux autorités suivantes: HCPN/GOVCERT, ILR, CNPD (Commission nationale pour la protection des données).

L'information a-t-elle également été dispatchée au niveau européen pour davantage sensibiliser les partenaires européens au risque de cyberattaques ?

Oui.

Le HCPN/GOVCERT a partagé les indicateurs de compromission (IOC) mis à disposition par Encevo avec sa propre constituante ainsi qu'avec la communauté des CERTs européens (EU CSIRTs Network).

Comme dans le cas en l'espèce il ne s'agit cependant pas d'un « data breach » transnational, la CNPD n'a pas informé ses homologues européens.

En application de l'article 8, paragraphe 6, de la loi NIS, l'ILR a informé de manière préventive les autres États membres concernés. De même, l'ILR a informé les autres opérateurs de services essentiels sur les indicateurs techniques de compromission.

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

En matière de cybersécurité le risque nul ne peut être atteint et l'éventualité d'une cyberattaque risquant de mettre en péril l'approvisionnement en énergie ne peut être complètement écartée.

Une attaque d'une telle envergure serait autrement plus complexe que celle qu'Encevo vient de subir, où « seulement » les opérations/systèmes commerciaux/bureautiques ont été touchés.
En effet, pour impacter l'approvisionnement physique en énergie, il faudrait réussir à pénétrer dans l'infrastructure de surveillance des réseaux (ce qui n'a pas été le cas dans l'attaque sur le groupe Encevo).

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

L'ILR procède à la sensibilisation des opérateurs de services essentiels (par exemple, par la conférence NISDUC, par des cyber exercices), partage avec les opérateurs les recommandations émises par les organisations européennes (Agence de l'Union européenne pour la cybersécurité ; ENISA) et élabore des mesures de sécurité à respecter par les opérateurs.

Les propriétaires ou opérateurs d'infrastructure critique sont tenus d'élaborer un plan de sécurité et de continuité de l'activité qui comporte les mesures de sécurité pour la protection de l'infrastructure critique en tenant compte du risque cyber. Ces mesures sont notamment destinées à améliorer la résilience des infrastructures critiques et leurs capacités de réaction aux incidents.

Le HCPN/GOVCERT propose aux opérateurs d'infrastructure critique des services de prévention (notification et détection de vulnérabilités, alertes de sécurité, détection de fuites d'information et d'identifiants) et de réponse à un incident.

En cas d'attaque cyber d'envergure contre les systèmes d'approvisionnement en énergie (électricité et gaz) et ayant un impact sur l'approvisionnement en énergie, l'action du gouvernement est définie par les plans d'intervention d'urgence en cas de rupture d'approvisionnement en énergie (« PIU Rupture d'énergie ») et Cyber (« PIU Cyber »).

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

La stratégie nationale en matière de cybersécurité IV couvre la période de 2021 à 2025. Les objectifs stratégiques définis sont génériques et cadrent les priorités du gouvernement en matière de cybersécurité pour la période de référence. Le plan d'action associée est révisé au sein du Comité coordination nationale en matière de cyberprévention et de cybersécurité (CIC-CPCS) et adapté en fonction de la situation de la menace cyber et de l'évolution du risque.

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 ?

Les opérateurs d'infrastructure critique sont invités à mettre à jour leurs plans de sécurité et de continuité de l'activité en fonction de l'état de la menace et de l'évolution du risque ainsi qu'à continuellement améliorer la pertinence, l'adéquation et l'efficacité de leur système de gestion de la sécurité et de la continuité d'activité.

Le règlement grand-ducal du 21 février 2018 fixant la structure des plans de sécurité et de continuité de l'activité des infrastructures critiques prévoit qu'*« Il est recommandé de procéder périodiquement à une évaluation du plan de sécurité et de continuité de l'activité ou en cas de faits nouveaux justifiant une évaluation en dehors de cette périodicité. »*

Le gouvernement peut-il nous indiquer si le groupe Encevo a effectué toutes les diligences (voir 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?

D'après les informations recueillies auprès d'Encevo, le système d'information du groupe Encevo est protégé par des systèmes et des processus de sécurité avancés, complétés par un centre d'opérations de sécurité fonctionnant 24 heures sur 24 et 7 jours sur 7, ainsi que par l'accès à une équipe de réponse aux urgences informatiques. Ces mesures ont permis à Encevo de détecter rapidement l'attaque et de pouvoir réagir rapidement. D'après les informations d'Encevo, le groupe investit constamment dans ses mesures de protection pour réagir à l'évolution rapide des cyber menaces et être en conformité avec les dispositions strictes du RGPD (règlement général sur la protection des données) et de la directive NIS (directive sur la sécurité des réseaux d'information).

L'attaque à laquelle le groupe a été confronté a utilisé un logiciel malveillant sophistiqué spécifiquement conçu, qui n'était pas détectable par un antivirus. La surveillance des systèmes de Encevo a été renforcée, les serveurs restorés à partir de sauvegardes sûres, la sécurité des plateformes d'accès à distance augmentés et tous les mots de passe furent changés.

Le RGPD, de par son principe de responsabilisation (« accountability »), prévoit que c'est au responsable de traitement de faire l'analyse de l'incident et de le notifier à l'autorité compétente dans des délais précis. Vu l'envergure et la complexité du cas sous revue, une telle analyse se fait en étapes et peut

nécessiter du temps. La CNPD suit les différentes étapes de cette analyse menée par le responsable de traitement. Selon les informations transmises par la CNPD, elle ne pourra avoir une appréciation complète des mesures de diligences prises par le groupe qu'une fois qu'elle aura pu prendre connaissance de l'analyse complète qui est toujours en cours.

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 ?

Il convient de noter que la CNPD peut à tout moment ouvrir une enquête sur la sécurité des traitements si elle le juge approprié et nécessaire. Pour rappel, le RGPD, de par son principe de responsabilisation, impose aux organisations, en tant que responsables du traitement de données à caractère personnel, de s'assurer de la mise en œuvre de mesures de sécurité adaptées aux risques auxquels elles sont confrontées.

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 ?

Non, ce rôle est dévolu à la CNPD et à l'ILR.

Comment s'organise cette coopération concrètement ?

Pour l'ILR il convient de mentionner l'article 9, paragraphe 3, de la loi NIS qui prévoit que *« pour traiter des incidents notifiés donnant lieu à des violations des données à caractère personnel, l'autorité compétente concernée coopère étroitement avec la Commission nationale pour la protection des données et lui transmet les informations en relation avec ces violations ».*

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) ?

Encevo a défini un concept de communication en 3 phases qui est en ligne avec l'article 34 du RGPD. Cette disposition prévoit que, lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, le « data controller », donc ici « Encevo Group », pour son propre compte ou celui de ses filiales, communique la violation de données à caractère personnel à la personne concernée dans les meilleurs délais.

Dans un *premier* temps, des communiqués de presse ont été publiés pour une information à grande échelle et un site, dédié à l'information sur l'évolution du traitement du vol de données, a été mis en place. Le site est actualisé régulièrement avec les informations dont le groupe Encevo dispose.

Dans un *deuxième* temps, tous les fournisseurs ainsi que tous les employés ont été informés par e-mail de l'attaque.

Dans un *troisième* temps, un fichier d'analyse reprend l'ensemble des cas identifiés avec une analyse détaillée du risque pour les personnes concernées. Aussitôt que les risques sont identifiés, des courriers individuels sont préparés et envoyés en indiquant les données personnelles en question. Ce courrier

contient également les mesures entreprises pour limiter les risques ainsi que des consignes et bonnes pratiques pour limiter les risques. Afin de pouvoir accélérer le processus d'analyse des fichiers, Encevo travaille avec des sociétés externes spécialisées en méthodes et outillage, et reconnues comme expertes dans ce domaine.

Le RGPD prévoit que le responsable de traitement est tenu de faire une analyse de l'incident et des impacts potentiels sur les personnes concernées. Si le risque est jugé élevé, le responsable de traitement a l'obligation de prévenir les personnes concernées de façon individuelle et de façon à ce qu'elles puissent prendre elles-mêmes des dispositions utiles pour se protéger des conséquences potentielles de la violation de données. Si une communication individuelle n'est pas possible (par exemple, impossibilité technique d'effectuer la communication individuelle, impossibilité d'identifier les individus concernés dans un délai court), une communication publique doit être effectuée dans un premier temps.

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 n'entend pas se livrer à des appréciations sur la composition de l'actionnariat d'un groupe.

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

Dans le contexte de la notification et des différents échanges d'information, Encevo a informé les autorités que l'auteur présumé à l'origine de la cyberattaque sur le groupe Encevo serait le groupe de cybercriminels connu sous le nom de « BlackCat ». Le groupe a fait son apparition en novembre 2021 et est supposé être à l'origine de plusieurs cyberattaques de grande envergure en Europe et aux États-Unis au cours des derniers mois.

BlackCat s'attaque à ses victimes en volant et chiffrant leurs données pour ensuite menacer de les publier en cas de non versement de rançon. Il n'existe pas de profil type des victimes. Le modèle d'affaires criminel du groupe *BlackCat* est basé sur le principe du « ransomware-as-a-service ». Il s'agit en l'occurrence d'un modèle d'affiliation où les développeurs d'un code malveillant proposent ce dernier, ainsi qu'un ensemble de services associés, sur les marchés cybercriminels à d'autres attaquants.
Depuis son apparition fin 2021, *BlackCat* est activement à la recherche d'affiliés sur des plateformes fréquentées par des cybercriminels qui seraient disposés à déployer leur rançongiciel connu sous l'acronyme « ALPHV ». Si une coopération entre *BlackCat* et un groupe affilié est établi, il est prévu que le groupe affilié touche 80-90% de la rançon et le reste revient à *BlackCat*. En ce qui concerne l'attribution officielle de l'attaque, elle est toujours destinée à *BlackCat*.

S'agit-t-il d'un groupe qui agit pour le compte d'un ou de plusieurs Etat(s) étranger(s) ?

L'état actuel des informations disponibles ne permet pas de conclure que le groupe agit pour le compte d'un ou plusieurs État(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?

Oui, mais le Gouvernement ne souhaite pas révéler le montant exact demandé dans le cadre d'une réponse à une question parlementaire en raison de la confidentialité de ce type d'éléments au regard de l'enquête en cours.

Des rançons de ce genre ont-elles également été demandées dans le contexte de cyberattaques similaires (au Luxembourg ou à l'étranger) ?

De telles demandes de rançon sont usuelles lors d'attaques du type ransomware et ont été faites à d'autres victimes, dont notamment récemment aussi deux autres groupes énergétiques (Entega AG, Mainzer Stadtwerke).

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

Tel qu'indiqué sur la page web spécialement mise en ligne sur l'attaque par le groupe Encevo, Encevo n'a pas donné suite à cette demande. C'est d'ailleurs l'avis général des autorités compétentes dans ce genre de situation.

Luxembourg, le 2 septembre 2022

Le Premier Ministre, Ministre d'État

(s.) Xavier BETTEL