Hydro Québec

Le 10 janvier 2021

PAR COURRIEL

Pierre Gagnon, Ad. E.
Vice-président exécutif – Affaires corporatives, juridiques, et chef de la gouvernance
Édifice Jean-Lesage
20e étage
75, boulevard René-Lévesque Ouest
Montréal (Québec) H2Z 1A4

Objet : Demande d'accès à l'information DAI-2021-0375

Bonjour.

Nous donnons suite à votre demande d'accès reçue à nos bureaux le 9 décembre 2021 et dans laquelle vous nous demandez :

1. *« Résultats et/ou rapports d'enquête sur les exercices de simulation faites dans le cadre du programme de formation à la cybersécurité d'Hydro-Québec. Ses résultats et rapports doivent couvrir l'année 2021 incluant les simulations du 27 octobre 2021 et du 25 novembre 2021.*
2. *Les modèles de courriels qui ont été transmis en 2021 dans le cadre des exercices de simulation du programme de formation à la cybersécurité d'Hydro-Québec.*
3. *Nombre de plaintes et commentaires logés par les employés à la suite de la transmission des courriels de tentatives d'hameçonnage en 2021.*
4. *Rapports et statistiques provenant de la firme de sondage externe Terra Nova concernant les simulations faites dans le cadre du programme de formation à la cybersécurité d'Hydro-Québec en 2021.*
5. *La liste des formations données aux employés en 2021 dans le cadre de la sensibilisation sur la cybersécurité d'Hydro-Québec.*
6. *Organigramme en vigueur du Centre de Surveillance de Sécurité des TIC d'entreprise (CSSE).*
7. *Politiques, code d'éthique, règles de gestion ou tout autre document en vigueur qui balisent et encadrent la liberté d'action relatifs aux exercices de simulations faites dans le cadre du programme de formation à la cybersécurité d'Hydro-Québec. »*

En réponse aux points 1 et 4 de votre demande, nous vous informons qu'entre le 4 février et le 9 décembre 2021, la Direction Cybersécurité d'Entreprise (DCE) a effectué 45 simulations auprès de 12 470 employés tous groupes confondus dans le cadre de son programme Culture de cybersécurité d'entreprise. Toutefois, nous ne pouvons communiquer le détail des résultats et les statistiques, ainsi que les rapports effectués suite à ces simulations, puisqu'ils contiennent notamment des renseignements dont la communication comporte des enjeux de sécurité et des renseignements personnels confidentiels sur les employés. Nous invoquons en conséquence les articles 22, 28, 29, 53, 54 et 56 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* («Loi sur l'accès») en annexe.

En réponse au point 2 de votre demande, nous vous informons que nous ne pouvons vous communiquer les modèles de courriel qui ont été transmis dans le cadre des exercices de simulation effectués par la DCE en 2021. Cette divulgation aurait notamment pour effet de réduire l'efficacité du programme de sécurité. Nous invoquons à cet égard les articles 22, 28 et 29 de la Loi sur l'accès.

...2

En réponse au point 3 de votre demande, nous vous informons que nous n'avons reçu aucune plainte formelle de la part des employés suite de la transmission des courriels de tentatives d'hameçonnage en 2021. Par ailleurs, quelques appels ont été logés par les employés au Centre de surveillance de cybersécurité d'entreprise (CSCE). Toutefois, nous ne détenons pas le nombre exact de commentaires reçus des employés. Nous invoquons en conséquence l'article 1 de la Loi sur l'accès en annexe.

En réponse au point 5 de votre demande, nous vous informons qu'il existe plusieurs formations en cybersécurité offertes aux employés d'Hydro-Québec. Vous trouverez ci-après la liste des principales formations :

- Hameçonnage web
- Sécurité wi-fi
- Chasse à la baleine
- Usurpation d'identité d'un haut dirigeant par courriel
- Escroquerie par courriel d'affaires
- Être conscient de la sécurité
- Rançongiciel
- Détection de cyberattaque
- Traiter avec des personnes non identitées
- Protection de l'information sensible – Traitement de l'information
- Clé USB à risque
- Quiz NERC (formation obligatoire couvrant certains thèmes liés à la cybersécurité)
- Sensibilisation à la sécurité informatique (comprend 5 thèmes différents)

En réponse au point 6 de votre demande, vous trouverez en annexe l'organigramme des Opérations de cybersécurité, dont le Centre de surveillance fait partie.

Concernant le point 7 de votre demande, nous vous référons aux politiques «Nos actifs» et «Notre sécurité» accessibles sur le site Web de l'entreprise à l'adresse suivante : https://www.hydroquebec.com/a-propos/gouvernance/politiques-codes-conduite.html. Ces politiques constituent l'engagement de l'entreprise en matière de sécurité. Hydro-Québec reconnaît que ses biens constituent des actifs stratégiques essentiels à la société québécoise et au bien-être des citoyens. Ainsi, l'entreprise planifie, met en œuvre et maintien des stratégies et des mesures de sécurité adaptées afin de protéger les actifs TIC contre les risques auxquels ils font face en fonction de leur criticité, des cadres réglementaires ou autres exigences auxquels ils sont assujettis. C'est dans ce contexte que s'inscrit le programme de sensibilisation à la cybersécurité et les exercices de simulation en découlant.

Pour toute informations additionnelles, nous vous invitons à communiquer avec Martine Roux, Conseillère principale Conditions et relations de travail au 514 289-2211 poste 5360.

La révision de cette décision peut être demandée auprès de la Commission d'accès à l'information. Vous trouverez ci-joint une note explicative à ce sujet.

Veuillez accepter nos meilleures salutations.

Le responsable de l'accès aux documents
et de la protection des renseignements personnels,

Pierre Gagnon

p. j.