La cybersécurité. Dès. Maintenant.

Préparer l'avenir de la cybersécurité mondiale

Lettre ouverte : Ottawa doit prendre au sérieux la cybersécurité. Dès. Maintenant.

Les dirigeants politiques du Canada doivent s'engager plus sérieusement en faveur de la cybersécurité au pays, et ce dès maintenant.

Selon le Baromètre de confiance Edelman 2021, les Canadiens sont plus inquiets d'être victimes d'une cyberattaque que de tout autre sujet, y compris la COVID et le changement climatique. Et qui peut les en blâmer ? Les cybercriminels ont réussi, à plusieurs reprises, à cibler nos infrastructures essentielles, notamment nos hôpitaux, nos écoles, nos réseaux de transport en commun et les gouvernements locaux et fédéral, provoquant des perturbations importantes des services essentiels.

Non seulement les services essentiels ont été perturbés dans des proportions exponentielles, mais ces attaques ont entraîné la perte, parfois irréversible, de données sensibles comme des renseignements médicaux, de la propriété intellectuelle vitale et des données très personnelles sur nos finances, voire sur nos enfants. La chef du Centre de la sécurité des télécommunications (CST) du gouvernement fédéral, Shelly Bruce a déclaré publiquement que la cybercriminalité était « la menace la plus répandue et la plus omniprésente pour les Canadiens et les entreprises canadiennes ». Que faut-il de plus pour inciter le gouvernement à prendre au sérieux la cybersécurité ?

Les attaques de ce type se sont multipliées au cours des dernières années et la grande majorité des Canadiens réclament des mesures urgentes pour sécuriser les systèmes informatiques publics et privés du Canada. Selon un récent sondage de l'Institut Angus

Reid, 92 pour cent des Canadiens estiment que le gouvernement fédéral doit accorder la priorité aux investissements dans la cybersécurité.

En tant que membres de la campagne *La Cybersécurité. Dès. Maintenant.*, nous pressons le gouvernement du Canada d'inclure les trois mesures suivantes en matière de cybersécurité dans le budget fédéral de 2022 pour que notre infrastructure soit résistante aux cyberattaques et que notre économie puisse continuer à se développer en tant que l'un des endroits les plus innovants, dynamiques et sûrs au monde pour faire des affaires.

- **Protéger les infrastructures essentielles, les chaînes d'approvisionnement et les entreprises de toutes tailles** du Canada contre les cybermenaces en investissant dans la cybersécurité à des niveaux comparables à ceux des autres pays du G7;
- **Faire croître l'économie** en accélérant la commercialisation des innovations en matière de cybersécurité au Canada et avec nos partenaires commerciaux;
- **Renforcer la main-d'œuvre canadienne dans le domaine de la cybersécurité** en investissant dans l'éducation, le développement des talents, la rétention et les programmes de diversification et d'expansion de la main-d'œuvre en cybersécurité.

Le but de la campagne *La cybersécurité. Dès. Maintenant.*, soutenue par plus d'une vingtaine d'entreprises technologiques et d'organisations spécialisées dans la cybersécurité de partout au Canada, est de faire du Canada un chef de file mondial en matière de cybersécurité. Nous pensons que chaque personne et chaque organisation au Canada mérite une protection efficace contre les cybermenaces, dont la complexité et l'ampleur ne font qu'augmenter. Les sociétés canadiennes, les entreprises de toutes tailles et les leaders technologiques de tous les horizons sont désireux de mettre leur expertise au service de la lutte contre cette menace persistante et croissante.

Pour rendre à César ce qui appartient à César, le gouvernement fédéral a fourni jusqu'à présent un financement total d'environ 1,5 milliard de dollars à l'Agence du revenu du Canada, à Développement économique et social Canada, au Centre de la sécurité des télécommunications et à Services partagés Canada dans le budget 2021 pour renforcer certaines parties des cyberdéfenses du gouvernement. Ce financement était important. Mais le champ d'application du financement était très étroit et la somme en dollars ne suffira pas à remédier à l'ampleur des faiblesses du Canada. Même si le gouvernement fédéral ne devait se préoccuper que de sa propre sécurité (ce qui serait imprudent), l'approche est encore beaucoup trop étroite. Il faut considérer que les organisations

faisant affaire avec le gouvernement fédéral sont des cibles de choix des attaques contre la chaîne d'approvisionnement et ont connu une augmentation significative des attaques de 42 % au premier trimestre de 2021. Par exemple, les maillons faibles de la chaîne d'approvisionnement aux États-Unis ont permis aux pirates d'exploiter et de prendre le contrôle de l'infrastructure de Solar Winds et de Colonial Pipelines, ce qui a considérablement perturbé les infrastructures essentielles pendant des mois.

Protéger les Canadiens ne se limite pas à protéger le gouvernement fédéral.

Le rythme de la numérisation s'accélérant à l'échelle mondiale, surtout depuis mars 2020, le Canada ne peut tout simplement pas se permettre de laisser ses entreprises, ses infrastructures et ses collectivités exposées aux cybermenaces. La cybersécurité n'a jamais été aussi déterminante pour la sécurité nationale et le potentiel économique de notre pays.

Si le budget fédéral de 2022 réserve une place importante à la cybersécurité, le Canada pourra se positionner comme un chef de file mondial dans ce domaine. Il est temps pour Ottawa de démontrer que le gouvernement comprend toute l'ampleur du défi qui se présente à nous et qu'il s'engage sérieusement à le relever à l'échelle nationale.

Le moment est venu d'agir en matière de cybersécurité.

--

Cette lettre ouverte a été rédigée par la campagne La Cybersécurité. Dès. Maintenant de la Chambre de commerce du Canada. Cette campagne est soutenue par : BlackBerry, Microsoft Canada, Cisco, Amazon Web Services (AWS), Calian, eSentire, General Dynamics Mission Systems-Canada, Innovapost, Terranova Security, Beauceron Security, Échange canadien de menaces cybernétiques, Communitech, CyberNB, Rogers Cybersecure Catalyst, Cycura, CYDEF, Difenda, F12.net, Field Effect, FWDSEC, Hitachi ID, Idealogical Systems Inc., Nirico Systems Inc., l'Institute for Cybersecurity & Resilient Systems de l'Ontario Tech, OPTIV, RHEA Group, RiskAware, rSolutions, Turbo IT, et la Women CyberSecurity Society.