Lukas Federer
Chef de projet
Infrastructure, Energie & Environnement
Hegibachstrasse 47
8032 Zurich

Lausanne, le 9 mars 2022

Consultation relative à l'inscription d'une obligation de signaler les cyberattaques contre les infrastructures critiques

Monsieur,

Nous avons bien reçu votre courrier du 14 janvier dernier relatif au projet mentionné sous rubrique et vous adressons ainsi nos déterminations à ce propos.

Contexte général

Ces dernières années, les cyber-incidents se sont multipliés, que ce soit dans les entreprises ou au sein des autorités, avec des conséquences parfois graves (fuite de données, rançonnage, dégâts d'image, etc.). Trop souvent, les entités touchées taisent ces attaques, contribuant à masquer la gravité de la situation et encourageant ainsi les criminels de la Toile à poursuivre leurs activités criminelles. Ce problème prend une acuité particulière pour les infrastructures critiques. C'est sous cet angle qu'il faut comprendre ce projet de modification de la loi fédérale du 18 décembre 2020 sur la sécurité de l'information au sein de la Confédération (loi sur la sécurité de l'information, LSI). Celle-ci prévoit d'introduire une obligation de signaler les attaques informatiques dont sont victimes les infrastructures comme les banques, les assurances, hôpitaux ou laboratoires, mais aussi les services postaux, les transports publics ou encore d'autres entreprises spécialisées, comme les services informatiques. La liste exhaustive des entités concernées figure à l'art. 74b.

Pour la Confédération, une telle obligation permettrait de détecter précocement les cyberattaques, d'analyser le mode opératoire de leurs auteurs et d'avertir à temps les autres exploitants d'infrastructures de ce genre. Elle pourrait ainsi apporter une contribution essentielle au renforcement de la cybersécurité de la Suisse. A noter que ce projet ne prévoit pas une telle obligation pour les entreprises en général. Dans une réponse à une motion parlementaire déposée en septembre dernier, le Conseil fédéral a jugé que la protection des cantons, des communes et des PME contre les cyberattaques n'était pas de son ressort. Ladite motion a été renvoyée en commission en décembre au motif que la répartition des compétences entre Berne et les cantons, soulevée par le Conseil fédéral, devait être réexaminée.

Genèse du projet

Dans un rapport de décembre 2019 en réponse au postulat « Infrastructures critiques. Prévoir une obligation de signaler les incidents graves de sécurité », le Conseil fédéral a constaté qu'il n'existait pas d'obligation de signaler les cyber-incidents dont sont victimes ces dernières. C'est pourquoi il a chargé le Centre national pour la cybersécurité (NCSC) d'étudier la possibilité d'introduire une telle obligation. Le 11 décembre 2020, le gouvernement a demandé au Département fédéral des finances (DFF) d'élaborer un projet fournissant les bases légales nécessaires à l'introduction d'une telle obligation de signalement. Le présent projet de consultation prévoit d'inscrire cette base légale dans la loi sur la sécurité de l'information (LSI).

Outre l'obligation de signalement, la LSI doit aussi fixer les tâches du Centre national pour la cybersécurité (NCSC) et l'établir dans sa fonction de centrale de signalement.

« L'obligation de signalement ne doit s'appliquer qu'aux cyberattaques recelant un certain potentiel de dommages », explique le Conseil fédéral dans son message. Y seront soumis les exploitants d'infrastructures critiques, c'est-à-dire de processus, de systèmes et d'installations essentiels au fonctionnement de l'économie ou au bien-être de la population. Le NCSC assumera le rôle de centrale de signalement. Il réceptionnera également les signalements de cyber-incidents et de vulnérabilités des moyens informatiques transmis à titre facultatif. Le NCSC a effectué un sondage en avril 2021 auprès des exploitants de telles infrastructures et des autorités à propos de ce projet. Il en est ressorti une large acceptation, à condition qu'il soit possible de la mettre en œuvre sans trop de lourdeurs administratives.

Appréciation

La recrudescence des attaques informatiques dirigées contre la Suisse, à laquelle nous assistons ces derniers mois, fait peser un péril certain sur les infrastructures essentielles au bon fonctionnement des activités humaines. Imaginons qu'un hôpital, une grande banque ou un important producteur d'énergie soit victime de hackeurs : les conséquences pourraient en être dramatiques, en particulier si la victime du piratage cache l'incident et paie une rançon. Cela ne pourrait qu'encourager les criminels de la Toile à poursuivre leurs exactions. C'est pourquoi, comme le soutiennent la Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) et les polices cantonales, le fait d'annoncer ces attaques permet non seulement d'épauler l'institution touchée, mais aussi de détecter d'éventuelles tendances liées aux dangers sur Internet et d'agir de manière ciblée.

Conclusion

A la lumière des éléments qui précèdent, la CVCI soutient cette modification législative. La question d'étendre l'obligation de signalement aux PME, réclamée au Parlement par voie de motion, nous paraît constituer a priori une atteinte à la liberté économique. Cela dit, au vu de l'importance de la problématique, une telle obligation pourrait être envisagée dans la mesure où elle n'implique pas des démarches administratives lourdes. La CVCI est en tous les cas d'avis qu'une sensibilisation accrue des entreprises est indispensable dans ce domaine.

En vous remerciant de l'attention que vous porterez à ces lignes, nous vous prions d'agréer, Monsieur, nos salutations les meilleures.

Chambre vaudoise du commerce et de l'industrie

Romaine Nidegger
Responsable de dossiers politiques

Jean-François Krähenbühl
Chargé de communication