

Cyberattaques

Vers une nouvelle obligation d'annonce

Par Célian Hirsch le 5 décembre 2022

Depuis le 1^{er} septembre 2020, les banques doivent informer la FINMA dans les 24 heures des cyberattaques réussies. Le 2 décembre 2022, le Conseil fédéral a proposé au Parlement d'introduire une nouvelle obligation d'annoncer les cyberattaques, également dans les 24 heures, mais cette fois-ci au Centre national suisse pour la cybersécurité (NCSC ; cf. art. 74a ss du projet de Loi sur la sécurité de l'information [P-LSI]).

Pourquoi cette obligation supplémentaire ? Car celle-ci s'appliquera à toutes les infrastructures critiques, dont font partie les banques, à côté des assurances, des infrastructures des marchés financiers, ou encore des hôpitaux, des hautes écoles, ainsi que des prestataires *cloud* et des fabricants de logiciels.

En raison de l'augmentation de cyberattaques, le Conseil fédéral désire octroyer au NCSC une vue d'ensemble des cybermenaces en Suisse. Avec une telle connaissance, le NCSC pourrait avertir les victimes potentielles et leur recommander les mesures qui s'imposent. Or, cette vue d'ensemble n'est possible que si toutes les infrastructures critiques lui annoncent les cyberattaques d'une certaine importance. À l'heure actuelle, le NCSC ne reçoit des informations que sur une base volontaire.

Afin que cette future obligation d'annonce soit respectée, le Conseil fédéral propose tant une incitation positive que négative. La première consiste dans le soutien que le NCSC apportera aux infrastructures critiques suite à une cyberattaque. La seconde consiste en une potentielle amende de CHF 100'000, lorsque l'assujetti persiste à ne pas respecter son devoir, après s'être vu octroyer un délai par le NCSC.

Les banques devront-elles donc tant informer la FINMA que le NCSC en cas de cyberattaque ? Conscient de ce potentiel double devoir d'annonce, le Conseil fédéral propose que le formulaire électronique du NCSC permette également de transmettre les informations pertinentes à la FINMA, avec même des informations supplémentaires auxquelles le NCSC n'aurait pas accès.

Dans sa prise de position, l'Association suisse des banquiers (ASB) appelle déjà à une modification de la Communication FINMA 05/2020 sur l'obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA. En effet, cette dernière devrait être adaptée à cette nouvelle obligation légale. L'ASB désirait également que le NCSC puisse coopérer avec les organisations de droit privé de l'économie, comme la récente association Financial Swiss

Sector Cyber Security Centre. Le Conseil fédéral n'a néanmoins pas suivi cette proposition.

En raison de l'obligation existante d'annonce à la FINMA, cette nouvelle obligation ne risque pas de créer une nouvelle charge importante pour les banques. On se demande cependant si cette révision constitue un premier pas vers une loi plus générale imposant des exigences minimales en matière de cybersécurité pour les infrastructures critiques, comme c'est déjà le cas dans l'Union européenne depuis 2018 avec la directive NIS, dont la version révisée (NIS2) vient d'ailleurs d'être adoptée.

Reproduction autorisée avec la référence suivante: Célian Hirsch, Vers une nouvelle obligation d'annonce, publié le 5 décembre 2022 par le Centre de droit bancaire et financier, <https://cdbf.ch/fr/1261/>