CENTRE DE DROIT
BANCAIRE ET FINANCIER

Cyberattaques

La nouvelle obligation d'annonce se précise

Par Célian Hirsch le 27 mai 2024

Les banques, les assurances et les infrastructures des marchés financiers devront annoncer dans les 24 heures les cyberattaques à l'Office fédéral de la cybersécurité (OFCS) dès le 1er janvier 2025. Le Conseil fédéral vient de mettre en consultation le projet d'ordonnance qui concrétise les art. 74*a* ss de la Loi sur la sécurité de l'information (obligation de signaler les cyberattaques).

Comme nous l'exposions précédemment (cf. Hirsch, cdbf.ch/1261), les banques devront désormais informer l'OFCS en cas de cyberattaques. Le nouveau devoir d'annonce à l'OFCS vise toutes les infrastructures critiques. Font notamment parties de ces infrastructures les banques, les assurances, les infrastructures des marchés financiers ou encore les prestataires *cloud* (art. 74*b* LSI). Dans le projet d'Ordonnance sur la cybersécurité (P?OCyS), le Conseil fédéral propose quelques allégements pour les petites infrastructures (art. 16 P?OCyS). Ces allégements ne concernent toutefois pas les banques, assurances et infrastructures des marchés financiers.

En cas de cyberattaques, les banques pourraient ainsi devoir informer trois autorités différentes, à savoir la FINMA, le PFPDT ainsi que l'OFCS. Un nouvel art. 39 al. 1 LFINMA, qui entrera aussi en vigueur le 1er janvier 2025, prévoit que la FINMA pourra communiquer à l'OFCS certaines informations dont cette dernière aurait besoin. Pour sa part, le PFPDT aura besoin de l'accord de la banque afin de communiquer des informations à l'OFCS.

Avant d'annoncer la cyberattaque, la banque devra examiner si le seuil du devoir d'informer est atteint. Ce seuil est distinct pour chacune des trois autorités (cf. le tableau ci-dessous). Avec l'art. 18 P-OCyS, le Conseil fédéral tente d'apporter quelques clarifications aux quatre situations qui entraînent un devoir d'annonce à l'OFCS (art. 74*d* LSI). Selon cette dernière disposition, une cyberattaque doit être signalée lorsqu'elle :

1. met en péril le fonctionnement de l'infrastructure critique concernée ;
2. a entraîné une manipulation ou une fuite d'informations ;
3. n'a pas été détectée pendant une période prolongée, en particulier si des indices laissent penser qu'elle a été exécutée en vue de préparer d'autres cyberattaques, ou
4. s'accompagne d'actes de chantage, de menaces ou de contrainte.

Concernant le contenu de l'annonce, l'art. 74*e* LSI dispose que celle-ci doit inclure des informations sur l'autorité ou l'organisation assujetties à l'obligation de signaler, sur le type et

l’exécution de la cyberattaque sur ses effets, sur les mesures prises et, si elles sont connues, sur les mesures prévues. Le Conseil fédéral précise ce contenu avec l’art. 19 P-OCyS, en exigeant notamment des informations précises sur la cyberattaque, telles que la date et l’heure de la constatation de l’attaque, la date et l’heure de l’attaque, le type d’attaque, les méthodes d’attaque et les données sur l’agresseur. Le Conseil fédéral s’est fondé sur la Communication FINMA 05/2020 sur l’obligation de signaler les cyberattaques selon l’art. 29 al. 2 LFINMA afin de déterminer les informations à transmettre à l’OFCS.

Concernant cette Communication FINMA 05/2020, l’Association suisse des banquiers (ASB) avait demandé à ce qu’elle soit adaptée à cette nouvelle obligation d’annonce des cyberattaques à l’OFCS. Depuis lors, la gestion des cyberattaques a été précisée dans la Circulaire 2023/1 sur les risques et résilience opérationnels (cf. Hirsch, cdbf.ch/1265), mais rien n’indique que le devoir d’annonce à la FINMA sera modifié en raison du nouveau devoir d’annonce à l’OFCS.

Le tableau récapitulatif ci-dessous propose un aperçu des trois devoirs d’annonces distincts en cas de cyberattaque :

Devoir d'annonce des cyberattaques

	FINMA	PFPDT	OFCS
Conditions	La cyberattaque vise des actifs d'importance critique et met en danger un ou plusieurs éléments faisant l'objet d'une protection (objectifs de protection) dans les fonctions d'importance critique et leurs processus.	La cyberattaque constitue une violation de la sécurité des données et entraîne vraisemblablement un risque élevé pour les personnes concernées.	La cyberattaque: -met en péril le fonctionnement de l'infrastructure critique concernée; -a entraîné une manipulation ou une fuite d'informations; -n'a pas été détectée pendant une période prolongée, en particulier si des indices laissent penser qu'elle a été exécutée en vue de préparer d'autres cyberattaques, ou -s'accompagne d'actes de chantage, de menaces ou de contrainte.
Délai	Annonce dans les 24 heures, puis annonce détaillée dans les 72 heures	Dans les meilleurs délais	Dans les 24 heures
Contenu	L'annonce doit contenir la nature de la cyberattaque, ses conséquences et les mesures prises ou envisagées (cf. les sources ci-dessous pour les différences selon l'autorité destinataire).		
Sources juridiques	Art. 29 al. 2 LFINMA Communication FINMA sur la surveillance 05/2020 Cf. ég. Circulaire 2023/1 sur les risques et résilience opérationnels	Art. 5 let. h LPD Art. 24 LPD Art. 15 OPDo	Art. 74*d* s. LSI Art. 18 p-OCyS

Cf. ég. Hirsch Célian, Le devoir d'informer lors d'une violation de la sécurité des données, Avec un regard particulier sur les données bancaires, thèse, Genève 2023

Reproduction autorisée avec la référence suivante: Célian Hirsch, La nouvelle obligation d'annonce se précise, publié le 27 mai 2024 par le Centre de droit bancaire et financier, https://cdbf.ch/1351/