Swiss Banking

FS-CSC Swiss Financial Sector Cyber Security Centre

Aux banques membres Circulaire n° 8130

Bâle, le 28 mars 2025

Obligation de signaler les cyberattaques – entrée en vigueur de la nouvelle réglementation (révision de la loi sur la sécurité de l'information et ordonnance sur la cybersécurité)

Mesdames, Messieurs,

Le 7 mars 2025, le Conseil fédéral a décidé de mettre en vigueur au 1er avril 2025 la nouvelle ordonnance sur la cybersécurité (OCyS) – en même temps que la révision de la loi sur la sécurité de l'information (LSI) adoptée par le Parlement le 29 septembre 2023.

L'objet principal de cette nouvelle réglementation est d'instaurer à l'échelon intersectoriel une obligation de signaler les cyberattaques telle qu'elle existait déjà dans le secteur financier depuis le 1er septembre 2020 (cf. la Communication FINMA sur la surveillance 05/2020 concernant l'obligation de signaler les cyberattaques).

Dans le cadre de la procédure de consultation, l'Association suisse des banquiers (ASB) et le Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC) ont pris conjointement position sur l'OCyS. Contrairement à ce que nous avions proposé, le Conseil fédéral n'a pas prévu de délai transitoire; la nouvelle réglementation s'applique à compter du 1er avril 2025.

Nous vous communiquons ci-après quelques informations détaillées à ce sujet.

1. Les cyberattaques doivent désormais être signalées à l'**Office fédéral de la cybersécurité (OFCS)** qui, pour ce faire, met un système électronique à disposition (voir point 6 *infra*).

2. L'obligation de signaler s'applique à **tous les établissements financiers** (art. 74*b,* al. 1, let. e LSI). Dans le secteur financier, à la différence d'autres secteurs, l'art. 12 OCyS ne prévoit aucune exception pour les petits établissements et pour les cyberattaques n'ayant que des effets mineurs sur l'activité.

3. Les **critères de l'obligation de signaler** sont définis à l'art. 74*d* LSI, aux termes duquel doit être signalée toute cyberattaque qui:

   «*a. met en péril le fonctionnement de l'infrastructure critique concernée;*

   b. a entraîné une manipulation ou une fuite d'informations;

Schweizerische Bankiervereinigung
Association suisse des banquiers
Associazione Svizzera dei Banchieri
Swiss Bankers Association

Aeschenplatz 7
Case postale 4182
CH-4002 Bâle

office@sba.ch
www.swissbanking.ch

c. 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

d. s'accompagne d'actes de chantage, de menaces ou de contrainte.»

L'art. 14 OCyS précise à cet égard:

«*[1] Le fonctionnement d'une infrastructure critique est mis en péril lorsque:*

a. des collaborateurs ou des tiers sont touchés par des interruptions de système, ou

b. l'organisation ou l'autorité touchée ne peut maintenir ses activités qu'à l'aide de plans d'urgence.

[2] Une manipulation ou une fuite d'informations est avérée:

a. lorsque des personnes non autorisées consultent, modifient ou publient des informations importantes pour les affaires;

b. lorsqu'une violation de la sécurité de données est annoncée conformément à l'art. 24 de la loi fédérale du 25 septembre 2020 sur la protection des données.

[3] Une cyberattaque est considérée comme indétectée pendant une période prolongée si elle s'est produite plus de 90 jours auparavant.»

4. Le **délai du signalement** est de 24 heures à compter de la détection de la cyberattaque (art. 74*e*, al. 1 LSI). Le signalement doit contenir des informations sur l'établissement assujetti 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 (art. 74*e*, al. 2 LSI). Si l'établissement assujetti dispose de nouvelles informations *a posteriori*, il lui appartient de compléter le signalement (art. 74*e*, al. 3 LSI).
L'art. 16 OCyS précise à cet égard:

«*[1] Si toutes les informations nécessaires ne sont pas connues dans les 24 heures suivant la détection de la cyberattaque, l'OFCS accorde à l'autorité ou à l'organisation concernée un délai de 14 jours pour compléter le signalement.*

[2] Si les informations nécessaires n'ont pas toutes été fournies dans le délai accordé, l'OFCS demande à l'autorité ou à l'organisation concernée de les compléter immédiatement ou de confirmer que les informations ne sont pas disponibles.»

5. L'art. 15 OCyS ainsi que le formulaire de signalement fournissent des précisions quant au **contenu du signalement**. Outre les informations prévues à l'art. 74*e*, al. 1 LSI (voir point 4 *supra*), l'art. 15 OCyS exige que soient indiqués la date et l'heure de l'attaque et de sa constatation, les données de l'attaquant, les éventuels actes criminels liés à l'attaque (chantage, menaces ou contrainte), ainsi que des informations estimatives sur la gravité et les effets de l'attaque (al. 1–3).

6. L'OFCS met à disposition un **système de communication électronique** des signalements de cyberattaques (art. 74*f* LSI). Celui-ci permet aux établissements assujettis «*de communiquer [le signalement de*

la cyberattaque ou de ses effets] à d'autres autorités», comme le Préposé fédéral à la protection des données et à la transparence (PFPDT) et la FINMA (art. 74*f*, al. 2–3 LSI).

Pour communiquer leurs signalements, les établissements peuvent utiliser le formulaire disponible sur le Cyber Security Hub (CSH), la plateforme d'échange d'informations avec les opératrices et opérateurs d'infrastructures critiques créée par l'OFCS en 2022 (art. 8–11 OCyS). Il n'y a pas d'obligation de s'enregistrer; les établissements qui n'ont pas accès au CSH peuvent communiquer leurs signalements par d'autres canaux, en particulier via le site Internet de l'OFCS qui propose un formulaire électronique à renvoyer par courriel.

7. Après deux notifications restées sans effet, les **violations de l'obligation de signaler** sont punissables d'une amende de CHF 100 000 au plus (art. 74*g*–74*h* LSI). Ces dispositions entreront en vigueur le 1er octobre 2025.

A titre complémentaire, nous vous invitons à visionner les deux vidéos suivantes mises en ligne par l'OFCS (en allemand uniquement):

- Meldepflicht für Cyberangriffe auf kritische Infrastrukturen
- Wie melde ich einen Cyberangriff auf kritische Infrastrukturen

Nous vous remercions de votre intérêt et restons à votre disposition pour tout renseignement complémentaire.

Avec nos salutations les meilleures
Association suisse des banquiers et Swiss FS-CSC

August Benz
Responsable International & Transformation et vice-CEO, Association suisse des banquiers

Alexandra Arni
Directrice,
Swiss FS-CSC

Contact: info@fscsc.ch