

Cyber attacks

Towards a new reporting obligation

Par Célian Hirsch le 5 December 2022

Since September 1, 2020, banks have had to notify FINMA within 24 hours of successful cyber attacks. On December 2, 2022, the Federal Council proposed to Parliament the introduction of a new obligation to report cyberattacks, also within 24 hours, but this time to the Swiss National Center for Cybersecurity (NCSC ; cf. art. 74a ff of the draft Information Security Act [P-LSI]).

Why this additional obligation ? Because it will apply to all critical infrastructures, including banks, insurance companies, financial market infrastructures, hospitals, universities, cloud providers and software manufacturers.

In view of the increase in cyber attacks, the Federal Council wishes to provide the NCSC with an overview of cyber threats in Switzerland. With such knowledge, the NCSC could warn potential victims and recommend appropriate measures. However, this overview is only possible if all critical infrastructures notify the NCSC of cyber attacks of some significance. At present, the NCSC only receives information on a voluntary basis.

To ensure compliance with this future reporting obligation, the Federal Council is proposing both positive and negative incentives. The former consists in the support that the NCSC will provide to critical infrastructures following a cyber attack. The second consists of a potential fine of CHF 100,000, should the subject persist in failing to comply with its duty, after having been granted a delay by the NCSC.

Will banks therefore have to inform both FINMA and the NCSC in the event of a cyber attack ? Aware of this potential double reporting obligation, the Federal Council is proposing that the NCSC's electronic form should also be used to transmit the relevant information to FINMA, including additional information to which the NCSC would not have access.

In its position paper, the Swiss Bankers Association (SBA) has already called for an amendment to FINMA Communication 05/2020 on the obligation to report cyber attacks in accordance with art. 29 para. 2 FINMASA. Indeed, the latter should be adapted to this new legal obligation. The SBA also wanted the NCSC to be able to cooperate with private-sector organizations, such as the recently formed Financial Swiss Sector Cyber Security Centre. However, the Federal Council did not follow this proposal.

Given the existing obligation to report to FINMA, this new obligation is unlikely to create a major new burden for banks. However, we wonder whether this revision is a first step towards a more

general law imposing minimum cybersecurity requirements for critical infrastructures, as has already been the case in the European Union since 2018 with the NIS Directive, the revised version of which (NIS2) has just been adopted.

Reproduction autorisée avec la référence suivante: Célian Hirsch, Towards a new reporting obligation, publié le 5 December 2022 par le Centre de droit bancaire et financier, <https://cdbf.ch/en/1261/>