Audit de la surveillance de la cybersécurité chez les prestataires de services financiers

Autorité fédérale de surveillance des marchés financiers

L'essentiel en bref

Le Contrôle fédéral des finances (CDF) a mené un audit auprès de l'Autorité fédérale de surveillance des marchés financiers (FINMA) pour examiner l'efficience et l'efficacité de la surveillance dans le domaine de la cybersécurité chez les prestataires de services financiers.

Le 8 décembre 2017, le Conseil fédéral a adopté la stratégie nationale pour la protection des infrastructures critiques pour la période 2018–2022. Deux des 27 secteurs définis sont surveillés par la FINMA : les prestations financières et les prestations d'assurance.

Le dispositif global en Suisse ne progresse que modestement

Emises par la FINMA en 2017, les directives contraignantes pour les banques et les négociants en valeurs mobilières sont appropriées. Cependant, des lacunes existent depuis des années dans le dispositif global des cyberrisques. Les mesures concrètes ne progressent que lentement en raison du peu de clarté des responsabilités et des compétences. Ainsi, une organisation de crise opérationnelle est toujours en cours de mise en place et des exercices intersectoriels réguliers sur les cyberattaques n'ont été menés qu'une seule fois.

La surveillance dépend des moyens disponibles

La surveillance des cyberrisques, l'un des six risques principaux pour la FINMA, a été développée de manière constante avec les ressources disponibles. Toutes les activités prévues dans ce domaine n'ont pas encore pu être réalisées ou mises en œuvre. La FINMA l'a reconnu et a procédé à des adaptations organisationnelles et formelles au début de l'année 2020. Toutefois, il existe toujours un risque que la surveillance ne suive pas les activités prévues, mais soit adapté aux ressources disponibles. Des gains en efficacité pourraient être réalisés dans la collecte et l'évaluation des résultats des audits.

Les banques ne respectent qu'insuffisamment l'obligation d'informer sur les cyberincidents

Les banques n'ont pas assez donné suite à l'obligation de signaler les cyberincidents. Le défaut de déclaration n'a pas eu de conséquences pour les institutions contrôlées, bien que les instruments correspondants existent. Il manque donc à la FINMA une source d'information importante sur les cyberrisques au niveau des institutions.

Cette situation est accentuée par le fait que les banques refusent à la FINMA un accès direct à MELANI (Centrale d'enregistrement et d'analyse pour la sûreté de l'information). L'intensification des contrôles sur place recommandée par le CDF pourrait remédier en partie à ces lacunes.

Texte original en allemand