

Bern, 15. Februar 2021

Prüfung der Aufsicht über die Cybersicherheit bei Finanzdienstleistern

Der Stand der vier Empfehlungen sieht per 15. Februar 2021 wie folgt aus:

1. Ausdehnung der aufsichtsrechtlichen Anforderungen betreffend Cyberrisiken auf weitere Beaufsichtigte wie bspw. Versicherungen

Die FINMA hat die Empfehlung aufgenommen, die Anforderungen betreffend Cyberrisiken auf den Versicherungsbereich auszudehnen. Die entsprechende Regulierungsarbeit wird 2021 beginnen.

2. Stärkere Untermauerung der Vorgaben zur Meldepflicht

Die FINMA hat im Mai 2020 eine Aufsichtsmitteilung publiziert, in der sie klar festhält, dass sie von Beaufsichtigten bei einer wesentlichen Cyberattacke eine Meldung erwartet. In der Folge gingen bei der FINMA zahlreiche Meldungen von Beaufsichtigten über Cyberangriffe ein.

Die FINMA hat daher klare Hinweise, dass die Beaufsichtigten seit der Veröffentlichung der Aufsichtsmitteilung ihrer Meldepflicht von wesentlichen Cyberangriffen viel besser nachkommen als vorher.

Die FINMA beobachtet die Bedrohungslage im Cyberbereich weiterhin eng. Ausserdem achtet sie aufmerksam darauf, dass die Beaufsichtigten die Meldepflicht einhalten. Sollte es Hinweise geben, dass die Meldepflicht nicht angemessen eingehalten wird, wird die FINMA entsprechend reagieren.

3. Stärkere Gewichtung der Anzahl der Vor-Ort-Kontrollen zum Thema Cybersicherheit

Die FINMA hat das Thema Cybersicherheit bei ihren Vor-Ort-Kontrollen (VOK) bereits im Jahr 2020 stärker gewichtet. Sie führte zu diesem Thema zehn VOK durch, und damit doppelt so viele wie im Vorjahr. Diese Zahl wird für 2021 noch einmal erhöht. Geplant sind insgesamt 15 VOK, acht im Banken- und sechs im Versicherungsbereich sowie eine im Bereich der Finanzmarktinfrastrukturen. Die FINMA hat die Ressourcen in der relevanten Querschnittsfunktion entsprechend erhöht.

4. Detailliertere und strukturiertere Einforderung der Prüfergebnisse bei den Prüfgesellschaften

Die FINMA hat angestossen, dass die Erhebungen systematischer erfolgen, die Prüfergebnisse inhaltlich systematischer analysiert und die der Prüfgesellschaften vorgegebenen Prüfpunkte betreffend "Informatik" überprüft werden.