CENTRE DE DROIT
BANCAIRE ET FINANCIER

Cyberattacken

Die neue Meldepflicht wird konkreter

Par Célian Hirsch le 27 Mai 2024

Banken, Versicherungen und Finanzmarktinfrastrukturen müssen ab dem 1. Januar 2025 Cyberangriffe innerhalb von 24 Stunden an das Bundesamt für Cybersicherheit (BfCS) melden. Der Bundesrat hat nun den Entwurf einer Verordnung zur Konkretisierung der Art. 74a ff. des Informationssicherheitsgesetzes (Meldepflicht bei Cyberangriffen) in die Vernehmlassung geschickt.

Wie wir bereits früher dargelegt haben (vgl. Hirsch, cdbf.ch/1261), müssen die Banken künftig das BKA bei Cyberangriffen informieren. Die neue Meldepflicht an das BKA betrifft alle kritischen Infrastrukturen. Zu diesen Infrastrukturen gehören insbesondere Banken, Versicherungen, Finanzmarktinfrastrukturen oder auch Cloud-Anbieter (Art. 74b ISG). Im Entwurf der Verordnung über die Cyber-Sicherheit (E-Cyber-Sicherheitsverordnung) schlägt der Bundesrat einige Erleichterungen für kleine Infrastrukturen vor (Art. 16 E-Cyber-Sicherheitsverordnung). Diese Erleichterungen betreffen jedoch nicht die Banken, Versicherungen und Finanzmarktinfrastrukturen.

So müssten Banken im Falle von Cyberangriffen möglicherweise drei verschiedene Behörden informieren, nämlich die FINMA, den EDÖB sowie das BKS. Ein neuer Art. 39 Abs. 1 FINMAG, der ebenfalls am 1. Januar 2025 in Kraft treten wird, sieht vor, dass die FINMA dem BKS bestimmte Informationen, die das BKS benötigt, mitteilen kann. Der EDÖB seinerseits wird die Zustimmung der Bank benötigen, um Informationen an das BKA weitergeben zu können.

Bevor die Bank den Cyberangriff meldet, muss sie prüfen, ob der Schwellenwert für die Informationspflicht erreicht ist. Dieser Schwellenwert ist für jede der drei Behörden unterschiedlich (siehe Tabelle unten). Mit Art. 18 E-OCyS versucht der Bundesrat, einige Klarstellungen zu den vier Situationen vorzunehmen, die eine Meldepflicht an das BKA nach sich ziehen (Art. 74d SIaG). Gemäß der letztgenannten Bestimmung ist ein Cyberangriff meldepflichtig, wenn er :

1. das Funktionieren der betroffenen kritischen Infrastruktur gefährdet ;
2. zu einer Manipulation oder einem Informationsleck geführt hat ;
3. über einen längeren Zeitraum unentdeckt geblieben ist, insbesondere wenn es Hinweise darauf gibt, dass er zur Vorbereitung weiterer Cyberangriffe durchgeführt wurde, oder
4. mit Erpressung, Drohungen oder Nötigung einhergeht.

In Bezug auf den Inhalt der Meldung bestimmt Art. 74e ISG, dass diese Informationen über die

meldepflichtige Behörde oder Organisation, über die Art und Ausführung des Cyberangriffs, über dessen Auswirkungen, über die getroffenen Maßnahmen und, soweit bekannt, über geplante Maßnahmen enthalten muss. Der Bundesrat präzisiert diesen Inhalt mit Art. 19 E-OCyS, indem er insbesondere genaue Informationen über den Cyberangriff verlangt, wie z. B. Datum und Uhrzeit der Feststellung des Angriffs, Datum und Uhrzeit des Angriffs, Art des Angriffs, Angriffsmethoden und Daten über den Angreifer. Der Bundesrat stützte sich auf die FINMA-Mitteilung 05/2020 zur Meldepflicht von Cyberangriffen gemäss Art. 29 Abs. 2 FINMAG, um die an das BAKS zu übermittelnden Informationen festzulegen.

Bezüglich dieser FINMA-Mitteilung 05/2020 hatte die Schweizerische Bankiervereinigung (SBVg) gefordert, dass diese an die neue Meldepflicht von Cyberangriffen an das BKA angepasst wird. Seither wurde der Umgang mit Cyberangriffen im Rundschreiben 2023/1 zu operationellen Risiken und Resilienz präzisiert (vgl. Hirsch, cdbf.ch/1265), doch gibt es keine Anzeichen dafür, dass die Meldepflicht gegenüber der FINMA aufgrund der neuen Meldepflicht gegenüber dem OFCS geändert wird.

Die folgende Übersichtstabelle bietet einen Überblick über die drei verschiedenen Meldepflichten im Falle eines Cyberangriffs :

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