16 décembre 2019

L'AMF publie la synthèse de ses contrôles thématiques sur les dispositifs de cybersécurité en place dans les sociétés de gestion de portefeuille

Conformément à ses priorités de supervision pour l'année, l'Autorité des marchés financiers a passé en revue les dispositifs de cybersécurité de cinq sociétés de gestion de portefeuille. Forte de ses observations, elle met en avant les bonnes pratiques constatées.

A l'occasion de ces contrôles courts et thématiques dits « SPOT » (Supervision des Pratiques Opérationnelle et Pratique), le régulateur a examiné :

- l'organisation des dispositifs de cybersécurité en matière de moyens humains et techniques ;
- la gouvernance de ces dispositifs ;
- les dispositifs d'administration et de surveillance du système d'Information ; le processus de gestion des incidents cyber ;
- la gestion des données sensibles ;
- le plan de continuité d'activité ;
- le contrôle interne en place sur le système d'information et sur le dispositif de cybersécurité .

Pour la réalisation de ses travaux, l'AMF a considéré le risque cyber comme découlant de toute atteinte malveillante potentielle, interne ou externe, à l'une des caractéristiques clés du système d'information d'une société de gestion que sont sa disponibilité, son intégrité, la confidentialité des données qu'il traite et la traçabilité des actions qui y sont menées.

Dans ce cadre, l'AMF a constaté que les établissements contrôlés commencent à prendre la mesure du risque cyber en l'intégrant dans leur cartographie des risques, en collectant les incidents de cybersécurité qu'elles subissent et en faisant appel à des prestataires spécialisés pour vérifier ponctuellement la robustesse de leur système d'information. En revanche, les dispositifs analysés ne prennent pas en compte les impacts potentiels de la matérialisation des risques de cybersécurité sur la conformité réglementaire des établissements en matière (i) de respect du niveau de fonds propres réglementaires, (ii) de conservation des données sensibles, (iii) de maintien d'un plan de continuité d'activité efficace et (iv) de maintien de moyens (informatiques) adaptés.

Par ailleurs, l'AMF a constaté l'absence quasi-générale de cartographie (i) des données sensibles et (ii) des systèmes critiques, ainsi que d'une politique de classification des données, d'où un risque de couverture partielle des risques majeurs par le dispositif de contrôle. De surcroît, l'identification formelle des incidents cyber, pour l'évaluation continue du niveau de risque associé, s'avère malaisée dans les bases de collecte existantes. Enfin, les vulnérabilités identifiées ou confirmées par le contrôle interne ne font pas l'objet d'une remédiation suffisamment rapide et suivie.

Pour les sociétés de gestion appartenant à un groupe (majorité de l'échantillon testé), il a été identifié un pilotage interne insuffisant des prestations (relatives à l'informatique, la cybersécurité et la continuité d'activité) réalisées par la maison-mère. Or, la réalisation technique de ces prestations par le groupe ne saurait exonérer les sociétés de gestion de leurs responsabilités quant à la définition (prioritaire) des principales zones de risque et au pilotage des contrôles associés.

Parmi les bonnes pratiques observées, l'AMF relève par exemple le fait :

- d'assurer l'indépendance de la fonction RSSI (Responsable de la Sécurité des Systèmes d'Information) par rapport à la DSI (Direction des systèmes d'information) soit par un rattachement (hiérarchique ou fonctionnel) du RSSI au comité exécutif, soit par l'instauration d'une fonction de contrôle indépendante des activités du RSSI ;
- de sensibiliser les collaborateurs de la SGP aux risques de cybersécurité en intégrant ces derniers au plan de formation annuel et réaliser, au moins annuellement, un test de réaction des collaborateurs à une tentative d'hameçonnage par courriel (« phishing ») ;

- d'intégrer, dans la stratégie de continuité d'activité de la SGP, la vérification régulière : (i) des capacités de travail collaboratif des équipes clés en situation de crise, (ii) de la capacité à restaurer les données sauvegardées, (iii) du niveau de sécurité physique et informatique des installations de secours ;

À l'inverse, l'AMF a relevé les mauvaises pratiques suivantes :

- déployer un dispositif de cybersécurité en l'absence (i) d'identification préalable, (ii) de classification par niveau de criticité (en fonction des critères DICT) et (iii) de revue régulière des données et des systèmes informatiques sensibles ;
- cantonner, dans la cartographie des risques des SGP, l'analyse des risques de cybersécurité aux seuls impacts de risque opérationnel sur les fonds et/ou mandats gérés ;
- ne pas assurer le blocage des ports USB des postes utilisateurs ;
- déployer le processus de contrôle permanent/périodique des prestataires informatiques externes sensibles sur la base d'une liste non exhaustive de ces derniers.

Au-delà de la synthèse publiée ce jour, cette série de contrôles SPOT a donné lieu à l'envoi de lettres de suites aux SGP concernées. Les risques de cybersécurité feront l'objet d'autres contrôles de l'AMF dans les mois à venir. À l'aune des constats effectués à l'issue de ces contrôles, l'AMF envisage d'élaborer une doctrine spécifique à la cybersécurité et proportionnée en fonction de la taille des acteurs.

À propos de l'AMF
Autorité publique indépendante, l'AMF est chargée de veiller à la protection de l'épargne investie en produits financiers, à l'information des investisseurs et au bon fonctionnement des marchés. Visitez notre site https://www.amf-france.org

En savoir plus

↘ Synthèse des contrôles SPOT sur le dispositif de cybersécurité des sociétés de gestion de portefeuille

SUR LE MÊME THÈME

S'abonner à nos alertes et flux RSS

COMMUNIQUÉ AMF

SUPERVISION

23 mai 2022

L'AMF publie la synthèse de ses constats sur les coûts et frais des OPCVM commercialisés auprès des particuliers

ACCORD MULTILATÉRAL

SUPERVISION

27 avril 2022

Accord-cadre du Crisis Management Group (CMG) de la chambre de compensation américaine Options Clearing Corporation (OCC)

COMMUNIQUÉ AMF

SUPERVISION

13 avril 2022

L'AMF publie la synthèse de ses contrôles SPOT sur la transparence post-négociation sur le marché obligataire

Mentions légales :
Responsable de la publication : Le Directeur de la Direction de la communication de l'AMF. Contact : Direction de la communication, Autorité des marchés financiers - 17, place de la Bourse - 75082 Paris Cedex 02