AUTORITÉ
DES MARCHÉS FINANCIERS

Impression à partir d'une page du site internet de l'AMF

10 octobre 2019

Cybercriminalité boursière : l'AMF publie une étude

L'Autorité des marchés financiers (AMF) publie une étude consacrée à la cybercriminalité boursière. Objectif : comprendre les enjeux, les modes opératoires et les problématiques de potentiels manquements boursiers auxquels le régulateur pourrait être confronté. Zoom sur les principaux enseignements de cette étude.

La cybercriminalité : une menace majeure

Depuis plusieurs années, et la presse s'en est souvent fait l'écho, la cybercriminalité est devenue une menace majeure. Elle représente une des formes de criminalité les plus coûteuses avec un ordre de grandeur de 0,5 % du PIB mondial. Les différentes études estiment que cet impact varie entre -1 % et -5 %. Le secteur financier et, plus particulièrement, la sphère boursière n'échappent pas à cette menace, mais il semble plus difficile de leur associer un coût spécifique.

Trois principaux manquements boursiers observés

En excluant la cybercriminalité liée aux cryptomonnaies, l'étude montre que la cybercriminalité boursière s'articule autour des trois manquements suivants : cybermanquement d'initié (ex : piratage informatique visant l'obtention d'informations privilégiées), cyberdiffusion de fausses informations financières (ex : création de « faux » sites internet ou fausses rumeurs diffusées à travers les réseaux sociaux afin d'influer sur le

cours d'une société cotée) et cybermanipulation de cours (ex : piratage de comptes de trading visant la mise en place de schémas de type « pump&dump »).

Tous les acteurs de la chaîne potentiellement touchés

L'analyse des cas de cyber-manquements d'initié ou de cyberdiffusion de fausses informations montre que toute la chaîne des acteurs du monde financier peut être touchée : émetteur, banque, diffuseur d'information, régulateur boursier, bourse, etc. De leur côté, les cas de cybermanipulation de cours analysés découlent principalement de l'intrusion de comptes de trading de particuliers.

La nécessité d'une coopération internationale renforcée

L'étude montre l'étendue de la cybercriminalité boursière et ses conséquences importantes, dans un contexte où, malgré la prise de conscience généralisée du risque cyber et des nouvelles lois relatives à la cybersécurité, à la protection des données personnelles ou aux « fake news », la coopération internationale des régulateurs reste difficile et le cadre juridique international encore peu adapté. La poursuite de la mobilisation des régulateurs, à l'instar de la SEC qui dès juillet 2017 créait sa « cyberunit » ou de l'AMF, la participation active aux différents groupes de travail internationaux dédiés à la cybersécurité financière et l'implication des institutions européennes apparaissent donc primordiales afin d'enrayer cette cybercriminalité boursière.

En savoir plus

↘ Etude sur la cybercriminalité boursière : définition, cas et perspectives

Mots clés MARCHÉS RISQUES ET TENDANCES

SUR LE MÊME THÈME

S'abonner à nos alertes et flux RSS

ACTUALITÉ ABUS DE MARCHÉ

10 juin 2022

Différé de publication d'information privilégiée pour les établissements de crédit : l'AMF applique les orientations de l'ESMA

RÈGLES PROFESSIONNELLES MARCHÉS

18 mai 2022

Décision du 26 avril 2022 relative à la modification des règles de fonctionnement du système multilatéral de négociation (SMN) opéré par TP ICAP (Europe) S.A.

RÈGLES PROFESSIONNELLES MARCHÉS

19 avril 2022

Décision du 29 mars 2022 relative à la modification des règles de fonctionnement du système multilatéral de négociation (SMN) Aquis Exchange Europe visant le carnet d'ordre à…

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