De l'obligation de signaler les cyberattaques selon l'article 29 al. 2 LFINMA – Communication FINMA sur la surveillance 05/2020

Sébastien Fanti, le 15 décembre 2020

La Communication FINMA sur la surveillance 05/2020 est intéressante à plus d'un titre. Elle s'inscrit tout d'abord dans un contexte particulièrement périlleux et évolutif. De surcroît, elle impose aux établissements bancaires des obligations plurifactorielles protéiformes qui méritent un examen attentif et une concrétisation.

A. Contextuellement

Le 7 mai 2020, l'autorité fédérale de surveillance des marchés financiers (FINMA) a publié un document intitulé « Communication FINMA sur la surveillance 05/2020 – Obligation de signaler les cyberattaques selon l'article 29 al. 2 LFINMA ». Ainsi que le relève pertinemment Célian Hirsch[1], cette chronologie ne doit rien au hasard. Les cyberattaques ont en effet prospéré durant la pandémie[2], ce qui a assurément généré une réaction du régulateur.

Il convient à cet égard de rappeler que les cyberattaques figurent parmi les six risques identifiés par la FINMA dans son premier monitorage des risques[3]. Au moment de l'émission de ce rapport, soit en décembre 2019, la FINMA assurait avoir émis dans le cadre de sa règlementation des exigences claires, mais concises à l'égard des banques. Un monitoring avait été implémenté pour analyser en continu les menaces, dont les cyberattaques d'envergure et en tirer des enseignements utiles. Force est de constater que la séquence temporelle est très brève, ce qui permet de subodorer une concrétisation du risque au-delà ce qui était prévisible et acceptable initialement.

Le recours accru au télétravail a en effet ouvert des brèches que les cybercriminels exploitent pour soutirer de l'argent ou des données. Les cybercriminels devaient s'imaginer que leurs attaques seraient plus fructueuses, en raison du transfert d'activités quotidiennes telles que le travail et l'école vers des solutions en ligne (télétravail, enseignement à distance), avec à la clé une dépendance accrue de la connectivité et de l'accès aux ressources[4]).

En mars 2020, le rançongiciel « Ryuk » a ainsi infecté la société de technologie financière londonienne Finastra, qui fournit des logiciels et des services à plus de 8500 clients, dont 90

des 1000 plus grandes banques dans le monde. Pour stopper la propagation de l'infection, Finastra a rapidement désactivé une partie de ses serveurs, ce qui a provoqué une panne passagère pour les nombreux clients du service[5]. Le secteur bancaire est ainsi particulièrement exposé et attractif en termes de gain potentiel, ce qui explique que la recrudescence précitée ait généré une réglementation topique, à ce stade sous forme de communication[6].

B. Analyse des attentes du régulateur

I. Introduction

Dans le cadre de son activité de surveillance, la FINMA publie des communications qui s'adressent à un groupe de porteurs d'autorisation clairement défini. Ces communications contiennent des données importantes ou urgentes, des explications sur des questions cruciales pour les assujettis ou des indications sur des risques actuels[7].

La Communication 05/2020 vise à rappeler aux établissements soumis à la surveillance de la FINMA (art. 29 al. 1 LFINMA) l'exigence légale d'annoncer immédiatement tout événement important du point de vue de la surveillance (art. 29 al. 2 de la LFINMA[8]), ce qui vise les événements importants en lien avec des cyberattaques, dont le degré d'importance est exposé dans la communication[9] et dans son annexe 1[10].

L'article 29 al. 1 LFINMA est une clause générale qui régit la transmission d'informations à l'autorité de surveillance dans les cas qui ne sont pas déjà traités par une disposition spéciale. Elle suscite de nombreux débats, notamment en relation avec l'application du principe *nemo tenetur*[11].

II. Risques identifiés et actions attendues

La FINMA évoque plusieurs types de risques : des risques pécuniaires directs[12], mais également d'entrave à la disponibilité, la confidentialité et l'intégrité d'infrastructures technologiques d'importance critique et d'informations sensibles. Elle qualifie l'importance d'une cyberattaque à l'aune a) d'une entrave directe ou indirecte de la protection des individus (créanciers, investisseurs, assurés), b) respectivement du bon fonctionnement des marchés, avant de c) définir et détailler l'annonce à opérer.

a) Entrave directe ou indirecte de la protection des individus

L'obligation d'annonce concerne donc les cyberattaques qui ont atteint partiellement ou tota-

lement leur but, sur des fonctions d'importance critique[13], dont la défaillance ou le dysfonctionnement auraient des conséquences considérables sur la protection des individus et entraveraient fortement cette protection. La protection de la disponibilité est nommément évoquée. Il s'agit donc d'assurer que les données sont accessibles et exploitables sur demande par une entité autorisée[14]).

La mise en œuvre de cette exigence a lieu, notamment, par la sauvegarde des informations, la gestion de la continuité de l'activité et la protection des enregistrements. Le régulateur évoque également la protection de l'intégrité et de la confidentialité. L'intégrité des données comprend l'assurance de l'intégralité des données, de leur validité et de leur actualité. Elle est mise en œuvre notamment par l'implémentation d'une protection contre les logiciels malveillants, ainsi que le développement et la maintenance des systèmes d'information. Quant à la confidentialité, elle consiste à assurer que des données ne sont pas communiquées ou révélées à des individus, entités ou processus non autorisés. Sa préservation nécessite de multiples actions citées ici à titre exemplatif[15] :

- Sécurisation des appareils mobiles et des processus de télétravail ;
- Gestion des actifs ;
- Contrôle d'accès ;
- Utilisation de la cryptographie ;
- Sécurité physique et environnementale ;
- Journalisation et surveillance ;
- Sécurité de l'information dès la gestion de projet (Privacy by Design)
- …[16]

Somme toute, la FINMA ne fait ainsi que rappeler les principes fondamentaux figurant dans différentes normes (notamment l'art. 7 LPD) de sécurité des systèmes d'information, en les concrétisant de manière superficielle dans sa critérisation du degré de gravité d'une cyberattaque, ainsi que dans la définition du degré de gravité[17]. Il est à cet égard expressément indiqué que les critères présentés le sont pour procéder à une première évaluation du degré de gravité de la cyberattaque. Ils n'exonèrent dès lors pas les assujettis d'un examen qui s'apparente, en réalité, à un audit complet du système d'information.

À ces fonctions d'importance critique, le régulateur lie des ressources intitulées « actifs critiques ». Il s'agit entre autres du personnel, de l'infrastructure technologique, des informations, des bâtiments, et des fournisseurs essentiels aux processus de ces fonctions d'importance critique[18].

La FINMA, qui offre un panorama dans l'Annexe 2 des actifs d'importance critique et de cyberattaques sur leurs objectifs de protection, attend donc de chaque assujetti qu'il identifie ses fonctions d'importance critique, les processus corrélés et les actifs critiques qui les supportent. Cette véritable cartographie devra, en sus d'atteindre une granularité importante, être mis à jour en permanence. Il s'agit en réalité d'une obligation de résultat. La FINMA indique en effet que la concrétisation doit intervenir d'ici le 1er septembre 2020, voire auparavant sur une base *best effort.*

b) Bon fonctionnement des marchés financiers en Suisse

La deuxième hypothèse évoquée de manière plus générale (le bon fonctionnement des marchés financiers en Suisse) constitue en réalité le *worst case scenario*, dès lors qu'il s'agirait d'une cyberattaque concernant simultanément plusieurs établissements, ou des établissements d'importance systémique ou des établissements fournissant des services intégrés. Le fonctionnement intégral du marché financier pourrait alors être affecté.

c) Définir et détailler l'annonce à opérer

Lorsqu'une cyberattaque répondant à la critérisation, ainsi qu'aux degrés de gravité précités est identifiée, l'établissement concerné informe (par le biais du Key Account Manager) la FINMA dans les 24 heures, après qu'une première analyse de gravité a été opérée. Dans les faits ce délai est très court et il nécessite une parfaite organisation interne et des ressources en suffisance. Dans les 72 heures, il conviendra ensuite de détailler via la plate-forme de saisie et de demande de la FINMA la nature, la gravité, les conséquences, ainsi que les mesures correctrices et de communication. Tout nouveau développement génère une obligation d'annonce supplémentaire dans les 72 heures.

En fonction du degré de gravité de la cyberattaque, le devoir de documenter les faits s'avère plus ou moins étendu. En cas de cyberattaque de gravité élevée ou grave, il faut produire un rapport conclusif sur les causes (ténorisant les motifs de la réussite, les effets en termes réglementaires et de clientèle, ainsi que les mesures prises). Les preuves et analyses du bon fonctionnement de la cellule de crise doivent également être apportées en cas de cyberattaque grave. La FINMA exige également un rapport conclusif sur les causes pour les cyberattaques de gravité moyenne. La Communication manque de clarté et de précision à cet égard, car les obligations seraient les mêmes qu'en cas de cyberattaque de gravité élevée, ce qui semble peu plausible.

C. Conclusions prospectives

La Communication 05/2020 constitue un premier pas intéressant. Elle a le mérite d'orienter les actions des assujettis et de définir un chemin en cas de cyberattaque. Satisfaire aux attentes du régulateur demeure toutefois relativement complexe. Les indications sont très générales pour ne pas dire génériques et les établissements devront investir massivement à l'aveugle sans avoir la certitude de satisfaire aux attentes émises par nature évolutives. Dans ces circonstances, l'émission d'une Circulaire s'avère nécessaire pour qu'une sécurité juridique puisse prospérer.

1. https://cdbf.ch/reperages/obligation-dinformer-la-finma-des-cyberattaques/.
2. Timothée Talbi, Les cyberattaques contre les banques ont triplé pendant le confinement, Les Échos 15 juillet 2020.
3. FINMA, Monitorage des risques 2019, p. 7 et 10.
4. Rapport semestriel 2020/I, Centrale d'enregistrement et d'analyse pour la sûreté de l'information Melani , p. 24.
5. https://www.bloomberg.com/news/articles/2020–04-08/how-finastra-survived-a-Ransomware-attack-without-paying-ransom.
6. la FINMA se réserve la possibilité d'émettre une circulaire.
7. Lignes directrices applicables à la communication du 25 septembre 2014.
8. pour un examen de la nature et l'ampleur du devoir de collaboration, cf. arrêt non-publié 2C_790/2019 du 14 septembre 2020, consid. 7.2.
9. Jacques de Werra / Yaniv Benhamou, Cyberassurance : instrument utile pour la cybersécurité des entreprises ? in : Jusletter 24 août 2020, p. 6.
10. Qui comprend une critérisation, associée à une définition du degré de gravité permettant de conclure à l'existence d'un risque moyen élevé ou grave.
11. Le droit de ne pas s'auto-incriminer ; BSK FINMAG-TRUFFER, Art. 29 FINMAG, N 20 ff.
12. À l'instar des rançongiciels
13. À titre exemplatif : trafic des paiements, négoce boursier, gestion de données personnelles particulièrement sensibles dans l'assurance-vie ou l'assurance maladie, etc.
14. Notamment Préposé fédéral à la protection des données et à la transparence, Annexe des directives sur les exigences minimales qu'un SGPD doit remplir, version du 15 avril 2014.
15. Cf. Annexe de la norme ISO 27001.
16. pour de plus amples informations, cf. Sébastien Fanti, Protection des données informatiques, in : Jean-Philippe Dunand / Pascal Mahon (éds), La protection des données dans les relations de travail, Genève / Zurich 2017, 230 ss.
17. Cf. Annexe 1.
18. Par exemple des fournisseurs de services essentiels ; en cas de cyberattaque ou de

cyberincident chez le fournisseur, l'établissement est responsable de le signaler ; mieux vaudrait dès lors intégrer aux contrats conclus avec ces fournisseurs la totalité des obligations figurant dans la Communication.

Proposition de citation : Sébastien FANTI, De l'obligation de signaler les cyberattaques selon l'article 29 al. 2 LFINMA – Communication FINMA sur la surveillance 05/2020, 15 décembre 2020 *in* www.swissprivacy.law/43

Les articles de swissprivacy.law sont publiés sous licence creative commons CC BY 4.0.