Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

Communication FINMA sur la surveillance 05/2020

Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA

7 mai 2020

Laupenstrasse 27
3003 Berne
Tel. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

1 Introduction

La FINMA considère que le danger représenté par les cyberattaques[1] sur la place financière suisse est très élevé. Les établissements soumis à la surveillance de la FINMA sont la cible des cybercriminels qui sont mus par des intérêts pécuniaires directs mais cherchent aussi à entraver la disponibilité, la confidentialité et l'intégrité d'infrastructures technologiques d'importance critique et d'informations sensibles. Le danger de cyberattaques est encore accentué dans les situations de crise particulières telles que l'actuelle pandémie de COVID-19. Les cybercriminels profitent de cette phase d'incertitude, adaptent leurs stratégies d'attaques à la situation actuelle et mettent encore plus sous pression des entreprises déjà fortement mises à contribution.

La présente communication sur la surveillance vise à rappeler aux établissements soumis à la surveillance de la FINMA l'exigence légale d'annoncer immédiatement tout événement important du point de vue de la surveillance (art. 29 al. 2 LFINMA). Cela comprend les événements importants en lien avec des cyberattaques qui ont atteint leur but, entièrement ou partiellement[2]. La FINMA vérifiera ultérieurement, sur la base des expériences faites avec cette obligation d'annoncer, s'il convient d'intégrer les précisions suivantes dans une circulaire.

2 Cyberattaques importantes du point de vue de la surveillance

L'importance d'une cyberattaque se définit par le fait qu'elle entrave directement ou indirectement[3], d'une part, la protection des individus, c'est-à-dire la protection des créanciers, des investisseurs et des assurés et, d'autre part, le bon fonctionnement des marchés financiers.

Cela concerne en premier lieu les cyberattaques, qu'elles aient atteint leur but entièrement ou partiellement, sur des fonctions d'importance critique[4] d'assujettis, dont la défaillance ou le dysfonctionnement auraient des consé-

[1] Il s'agit d'attaques en provenance d'Internet et de réseaux comparables qui visent l'intégrité, la disponibilité et la confidentialité de l'infrastructure technologique, notamment en ce qui concerne les données et systèmes IT critiques et/ou sensibles.

[2] Pour les entreprises d'assurance, cette obligation découle aussi des retombées médiatiques et des atteintes à la réputation et à la solvabilité que peuvent provoquer les cyberattaques. Circulaire FINMA 08/25 « Obligation de renseigner – assureurs », Cm 1 et 5.

[3] Par exemple par des attaques sur les infrastructures d'importance critique pour les établissements soumis à la surveillance de la FINMA (par ex. fournisseur internet, fournisseur d'électricité, etc.).

[4] Produits et services d'assujettis et les processus commerciaux sur lesquels ils reposent (par ex. trafic des paiements, approvisionnement en espèces, négoce boursier, mise en place et gestion de contrats d'assurance, traitement de sinistres et de prestations, gestion de données personnelles particulièrement sensibles dans l'assurance-maladie et l'assurance-vie, gestion de titres et de placements, etc.) et leurs actifs critiques.

quences considérables sur la protection des individus et entraveraient fortement cette protection. Cela comprend notamment la protection de la disponibilité. D'autre part, ces attaques peuvent aussi compromettre la protection de l'intégrité et de la confidentialité des informations et données. Si plusieurs établissements sont touchés en même temps ou si des établissements d'importance systémique ou des établissements fournissant des services intégrés sont touchés, cela mettrait même en danger le fonctionnement des marchés financiers en Suisse.

Les cyberattaques visent en règle générale directement les ressources de ces fonctions critiques. Font en particulier partie de ces ressources considérées comme actifs critiques: le personnel, l'infrastructure technologique, les informations et les bâtiments ainsi que les fournisseurs[5] essentiels nécessaires aux processus de ces fonctions d'importance critique. Chaque établissement soumis à surveillance doit identifier ses fonctions d'importance critique, les processus correspondants et les actifs critiques supportant ces processus[6].

Si une cyberattaque visant des actifs d'importance critique 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, alors il faut immédiatement en informer la FINMA.

[5] Si un établissement externalise des fonctions essentielles à d'autres personnes physiques ou morales, il est également responsable de signaler les cyberattaques ou autres cyberincidents de ses fournisseurs, dans la mesure où ces incidents affectent les fonctions essentielles qui ont été externalisées. Cf. à ce sujet l'art. 47 al. 2 de la loi sur la surveillance des assurances (LSA; RS 961.01).

[6] Par exemple circulaire FINMA 2008/21 « Risques opérationnels – banques », Cm 135.2 ou 135.7 ss ou les standards minimaux Business Continuity Management de l'ASA, circulaire FINMA 2017/2 « Gouvernance d'entreprise — assureurs », cm 28 ss.

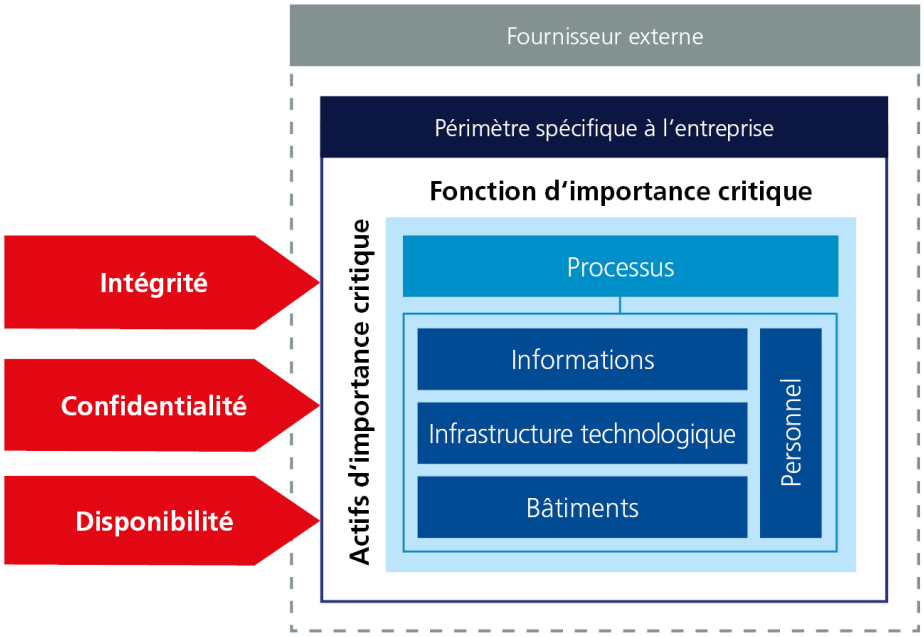

Illustration 1 : Représentation schématique d'une cyberattaque sur une fonction d'importance critique chez un assujetti.

L'annexe 2 présente des exemples non exhaustifs d'actifs d'importance critique et de cyberattaques possibles les visant.

3 Annonce immédiate à la FINMA

Une annonce immédiate à la FINMA signifie que l'établissement assujetti concerné informe la FINMA dans les 24 heures par l'intermédiaire du *(Key) Account Manager* compétent, lorsqu'une telle cyberattaque est constatée et après qu'une première évaluation de sa gravité a été faite. Cette annonce doit être faite conformément à la liste suivante, dans les 72 heures, via la plate-forme de saisie et de demande (EHP) de la FINMA[7,8].

La liste suivante décrit le contenu d'une telle annonce à la FINMA:

- Nom de l'établissement
- Personne de contact y compris données de contact (téléphone, adresse électronique)
- Date / heure de l'annonce à la FINMA

[7] https://www.finma.ch/fr/finma/extranet/plateforme-de-saisie-et-de-demande/ (disponible à partir du 1er juin 2020)

[8] Sur la plate-forme EHP: ~~"EHP" – "Déclarations" – Bouton: "Nouvelle déclaration" - Modèle pour déclarations: "Déclaration cyberattaque"~~
"EHP" – "Saisies" – Bouton: "Saisie +" – Modèle : "Déclaration cyberattaque"

- Date / heure auxquelles l'attaque a été constatée
- Date / heure de l'attaque (si déjà connues)
- Description de la cyberattaque et statut actuel
- Evaluation du degré de gravité de la cyberattaque (cf. annexe 1) *(options: Moyen, Élevé, Grave)*
- Evolution du degré de gravité *(options: décroissant, stable, croissant)*
- Entités touchées (unités organisationnelles touchées dans l'établissement ou le fournisseur)
- Objectifs de protection concernés *(options: confidentialité, intégrité, disponibilité)*
- Fonctions d'importance critique touchées, processus ou actifs (informations, infrastructure technologique, bâtiments ou personnel touchés)
- Nombre de clients touchés (état actuel)
- Vecteurs de l'attaque *(options: courriel, attaque via Internet, attaque de force brute, vol d'identité, vecteurs externes changeants, perte / vol d'appareils, exploitation de faiblesses des logiciels, exploitation de faiblesses du hardware, autres [veuillez préciser])*
- Type d'attaque (description) (par ex. DDoS, accès non autorisé, maliciel, utilisation abusive de l'infrastructure technologique, etc.)
- Mesures correctrices administratives, opérationnelles et/ou techniques avec échéances attendues
- Mesures de communication (contenu, destinataire, date)

Si, une fois que l'obligation d'annonce a été entièrement remplie, de nouveaux développements ou de nouvelles évaluations concernant la même attaque surviennent, une nouvelle annonce doit à nouveau être faite dans les 72 heures.

Pour les cyberattaques dont le degré de gravité est Élevé ou Grave (cf. annexe 1), la FINMA attend de l'établissement, une fois que celui-ci a terminé de traiter le cas, un rapport conclusif sur les causes (analyse *root cause*) comprenant notamment une analyse, les raisons pour lesquelles l'attaque a réussi, les effets de celle-ci sur le respect des prescriptions réglementaires, sur l'entreprise et sur les clients, ainsi que les mesures visant à réduire les conséquences de l'attaque. Pour les cyberattaques dont le degré de gravité estGrave (cf. annexe 1), il faut également transmettre les preuves et analyses du bon fonctionnement de l'organisation de crise.

Pour les cyberattaques dont le degré de gravité est Moyen (cf. annexe 1), un rapport conclusif sur les causes est suffisant.

La FINMA attend des assujettis que la communication sur la surveillance dédiée aux annonces de cyberattaques soit concrétisée au plus tard d'ici le 1er septembre 2020 ou même plus tôt sur une base *best effort*.

Annexe 1 : détermination du degré de gravité d'une cyber-attaque

Les critères suivants peuvent être utilisés pour procéder à une première évaluation du degré de gravité d'une cyberattaque:

Degré de gravité	Définition	Critères
Grave	Dommages (présents ou attendus) durables et de grande ampleur aux objectifs de protection que sont la disponibilité, l'intégrité et la confidentialité d'actifs d'importance critique	– Disponibilité: Les actifs d'importance critique ne sont pas disponibles à moyen ou long terme (défaillance > 200% du RTO[9]) – Confidentialité/intégrité: Informations sensibles touchées dans (presque) leur intégralité – Effets financiers menaçant l'existence de l'entreprise ou atteinte à la réputation – La maîtrise de la cyberattaque requiert d'activer l'organisation de crise (BCM)
Élevé	Les objectifs de protection (disponibilité, intégrité, confidentialité) d'actifs d'importance critique sont considérablement atteints ou menacés	– Disponibilité: Les actifs d'importance critique ne sont pas disponibles à moyen terme (défaillance >= RTO) – Confidentialité/intégrité: Informations sensibles touchées en grande partie et/ou informations d'importance critique pour les processus touchées – Effets financiers importants ou atteintes à la réputation – La maîtrise de la cyberattaque requiert de recourir à des ressources externes
Moyen	Atteinte ou menace immédiate des objectifs de protection (disponibilité, intégrité, confidentialité) d'actifs d'importance critique	– Disponibilité: Les actifs d'importance critique ne sont pas disponibles à court terme (défaillance > 50% du RTO) – Confidentialité/intégrité: Informations sensibles touchées de manière significative[10] – Effets financiers ou atteintes à la réputation sensibles – La cyberattaque peut être maîtrisée avec les ressources internes disponibles

[9] *Recovery Time Objective* – Temps prévu pour la remise en service d'actifs d'importance critique

[10] En dehors de la marche normale des affaires (*business as usual*)

Annexe 2 : exemples d'actifs d'importance critique et de cyberattaques sur leurs objectifs de protection

	Exemples d'actifs d'importance critique	Exemples de cyberattaques
Informations	Informations sensibles / confidentielles telles que les données d'identification de clients, les contrats d'assurance, les données liées au règlement des sinistres ou le traitement des prestations, procès-verbaux du CA ou de la direction, informations sur la stratégie, données RH, etc.	Attaques sur les objectifs de protection au moyen d'un accès non autorisé aux données au sein de l'entreprise ou depuis l'extérieur, fuites de données, vol de données, modification des données, etc.
Infrastructure technologique	Infrastructure technologique nécessaire à une fonction d'importance critique (par ex. *hardware*, logiciel, infrastructure réseau, etc.).	Attaques sur des objectifs de protection au moyen de (D)DoS, perte/vol de support de données contenant des informations confidentielles, *ransomware*, etc.
Bâtiments	Bâtiments essentiels aux fonctions d'importance critique (par ex. centres de calcul, filiales, bureaux de *back office*, etc.).	Attaques sur des objectifs de protection au moyen de dysfonctionnements ou de désactivations des mesures de protection réglant l'accès aux domaines sensibles.
Personnel	Collaborateurs assumant des fonctions d'importance critique ou y contribuant de manière essentielle, tels que la direction, les négociants, les conseillers clients, etc. ainsi que les collaborateurs clés (par ex. ceux ayant des droits accrus, les administrateurs systèmes, le personnel de sécurité, comptabilité, etc.).	Attaques sur des objectifs de sécurité au moyen de procédés d'ingénierie sociale (par ex. *spear phishing*), menaces d'*insiders*, vol d'identité, chantage, etc.