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 03/2024

Enseignements tirés de l'activité de surveillance des cyber-risques, précisions sur la communication FINMA sur la surveillance 05/2020 et sur les cyberexercices fondés sur des scénarios

7 juin 2024

Laupenstrasse 27, 3003 Berne, tél. +41 (0)31 327 91 00, www.finma.ch

Table des matières

1 Introduction

Depuis plusieurs années, les cyberrisques comptent parmi les principaux risques répertoriés par la FINMA dans le monitorage des risques qu'elle publie tous les ans. Le nombre de signalements reçus par la FINMA concernant des cyberattaques réussies ou partiellement réussies augmente chaque année.

La communication FINMA sur la surveillance 05/2020 « Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA » décrivait en détail l'obligation de signaler correspondante. Les signalements reçus depuis lors montrent différentes évolutions en ce qui concerne la situation en matière de menaces, les méthodes d'attaque et les objectifs des attaques. Grâce à son activité de surveillance, la FINMA peut se faire une idée détaillée de la manière dont les établissements soumis à sa surveillance gèrent les cyberrisques. Ce sont surtout les contrôles sur place spécifiques aux cyberrisques qui lui permettent d'évaluer de manière approfondie la maturité du dispositif de cyberdéfense des établissements assujettis. La FINMA a à chaque fois publié ses conclusions et constatations spécifiques sur une base agrégée dans son monitorage des risques ainsi que dans son rapport d'activité.

Dans la présente communication sur la surveillance, la FINMA fournit aux assujettis des indications spécifiques quant à la manière de gérer les cyberrisques sur la base de ces connaissances. Ces indications sont pertinentes pour tous les établissements soumis à la surveillance de la FINMA. Pour certains points, il est fait explicitement référence à la circulaire FINMA 2023/1 « Risques et résilience opérationnels – banques ». Ces indications s'adressent en premier lieu aux établissements auxquels s'applique la circulaire, mais peuvent également servir de lignes directrices aux autres établissements.

Dans ce contexte, des questions récurrentes concernant la communication FINMA sur la surveillance 05/2020 « Obligation de signaler les cyberattaques selon l'art. 29 al. 2 LFINMA » sont également traitées.

Pour terminer, le Cm 70 de la Circ.-FINMA 23/1 est abordé et précisé.

2 Enseignements tirés des activités de surveillance des cyberrisques

2.1 Externalisations

Dans le « Monitorage FINMA des risques 2020 », la FINMA faisait déjà état d'une augmentation des attaques réussies contre les chaînes d'approvisionnement des établissements surveillés, qui représentaient environ 25 % de toutes les attaques. Au cours des années suivantes, ce chiffre a déjà dépassé les 50 % et s'est maintenu de manière stable à ce niveau. La FINMA s'est donc penchée de manière plus intensive sur le thème des cyberrisques en cas d'externalisation[1] et en a fait une des priorités de sa surveillance. Son objectif était de déterminer pourquoi les attaques contre les prestataires de services réussissaient plus souvent que la moyenne. Les contrôles sur place ont montré que ce résultat s'explique notamment par le flou des exigences posées par les établissements assujettis aux prestataires de services mandatés en matière de cybersécurité ainsi que par l'irrégularité – voire l'inexistence – de la vérification du respect de ces exigences.

- Après l'identification de lacunes importantes de sécurité, seuls de rares établissements avaient pris proactivement contact avec leurs principaux prestataires de services pour s'assurer qu'ils seraient en mesure d'y remédier rapidement, avant l'apparition de dommages.
- La FINMA a souvent observé que les établissements directement assujettis à sa surveillance reprenaient rapidement le contrôle en cas de graves faiblesses et étaient ainsi en mesure d'éviter des dommages directs. Quelques prestataires de services, toutefois, n'étaient souvent pas aussi efficaces et étaient insuffisamment préparés.
- Très souvent, les établissements ne disposaient pas d'un inventaire complet de leurs prestataires de services : manquaient par exemple des informations sur le fait que des données critiques étaient stockées chez tel prestataire ou que tel autre était chargé de l'exécution d'une fonction critique. C'est pourquoi ces prestataires de services ont souvent fait l'objet d'un contrôle lacunaire, voire d'aucun contrôle régulier de la part des établissements assujettis.
- L'inventaire des principaux sous-traitants en cas d'externalisation a révélé de grandes différences entre les établissements étudiés en ce qui concerne le degré de maturité de la saisie, de la documentation et des possibilités d'accès aux données critiques[2].
- Les établissements concernés n'avaient pour la plupart pas clairement défini ce qu'étaient pour eux des données critiques. Cela compliquait

[1] Voir également le nouveau risque principal « Externalisation » dans le monitorage de risques 2023 et le rapport annuel 2023 de la FINMA.

[2] Voir à ce sujet le Cm 14 de la Circ.-FINMA 18/3.

non seulement la protection interne de ces données mais aussi la classification appropriée des prestataires de services et la détermination des mesures de contrôle nécessaires en vue de réduire les risques identifiés.

Si un établissement présente une externalisation importante vers un prestataire de services (notamment en ce qui concerne des fonctions critiques ou des données critiques dans une mesure pertinente), le respect des mêmes exigences réglementaires que celles applicables à l'établissement assujetti doit y être garanti. De même, ces exigences sont également applicables aux éventuels sous-traitants impliqués. C'est pourquoi la FINMA considère qu'un inventaire actualisé des externalisations significatives, y compris des sous-traitants, est un instrument essentiel.

L'établissement reste responsable à tout moment du respect des exigences prudentielles. Il n'est pas possible d'externaliser ou de transférer cette responsabilité à un prestataire de services.

2.2 Gouvernance et identification

La gouvernance en matière de gestion des cyberrisques est un autre domaine clé. Par le passé, la FINMA a souvent constaté que les cyberrisques étaient présentés comme un problème purement technologique et qu'ils ne bénéficiaient donc pas de la priorité nécessaire au sein de la direction ou du conseil d'administration. C'est pourquoi, pour les banques par exemple, la nouvelle Circ.-FINMA 23/1 a clairement défini les responsabilités de l'organe responsable de la haute direction ainsi que de la direction (voir le Cm 61). La FINMA a en outre constaté les autres faiblesses suivantes dans le domaine de la gouvernance de nombreux établissements surveillés :

- Dans les établissements de taille moyenne, il n'existait souvent pas de délimitation claire entre la gestion opérationnelle des cyberrisques et l'instance de contrôle indépendante. Il est essentiel que l'efficacité du traitement opérationnel soit continuellement vérifiée par une instance de contrôle indépendante[3].
- L'identification des menaces liées aux cyberrisques spécifiques aux établissements était souvent lacunaire. De plus, il était souvent impossible de savoir quels collaborateurs avaient accès à ces données faute d'outil d'autorisation central. Cet état de fait compliquait la tâche de l'organisation de la sécurité propre à l'entreprise d'élaborer un dispositif de protection orienté sur les données les plus importantes.

[3] Voir les sections sur les fonctions de contrôle et les instances de contrôle indépendantes dans les circulaires FINMA 2017/1 « Gouvernance d'entreprise – banques » et 2017/2 « Gouvernance d'entreprise – assureurs ».

- De nombreux établissements assujettis n'avaient pas intégré explicitement les cyberrisques dans leur gestion globale des risques opérationnels. De ce fait, il ne leur était pas possible de garantir une gestion systématique et complète des cyberrisques.
- En outre, certains établissements assujettis n'avaient pas suffisamment défini les cyberrisques ainsi que leur appétit pour le risque et leur tolérance au risque correspondants. Ces éléments constituent pourtant des composantes centrales d'un dispositif de protection efficace contre les cyberrisques.

Selon le monitorage des risques de la FINMA, les cyberrisques font partie des principaux risques depuis des années, raison pour laquelle il est essentiel que les établissements assujettis intègrent ce risque comme un risque à part entière dans la gestion des risques opérationnels qualitatifs et définissent un appétit pour le risque correspondant ainsi que des tolérances en matière de risque.

De même, en ce qui concerne les cyberrisques, il est indispensable que des contrôles clés soient intégrés dans le système de contrôle interne (SCI) selon des normes ou des pratiques internationalement reconnues et que leur efficacité soit régulièrement vérifiée, évaluée et documentée par une instance de contrôle indépendante. La séparation des tâches, des responsabilités et des compétences pour garantir l'indépendance et prévenir les conflits d'intérêts doit aussi faire l'objet d'évaluations régulières.

2.3 Dispositif de protection

En ce qui concerne le dispositif de protection, une tendance positive a pu être observée dans le cadre de la surveillance courante ces dernières années. Par exemple, dans le domaine de la défense contre les attaques par déni de service distribué[4], les établissements assujettis ont pris des mesures de protection toujours plus performantes et efficaces. Toutefois, dans ce domaine également, des conclusions importantes ont été tirées des points faibles existants :

- Les mesures de protection pour la prévention des pertes de données (*Data Loss Prevention* ou DLP) se limitaient souvent aux seuls éléments d'identification des clients ou aux numéros de carte de crédit. D'autres données critiques (telles que les données personnelles sensibles, les secrets commerciaux, la propriété intellectuelle) n'étaient pas couvertes par les mesures de protection DLP.
- Presque tous les établissements contrôlés avaient défini une politique et des processus en matière de sauvegarde des données *(back-up)* ainsi

[4] Attaque DDoS : un nombre élevé de requêtes, émanant de sources distribuées, provoque une surcharge des systèmes (par ex. d'un site Internet).

que des plans de restauration. Toutefois, dans certains établissements, il manquait un test de ces processus en cas de cyberattaque grave, par exemple par un logiciel malveillant de cryptage (logiciel rançonneur ou *ransomware*).

- Pour un grand nombre d'établissements assujettis, il existe également un potentiel d'amélioration dans les domaines de la formation et de la sensibilisation aux cyberrisques. Pour assurer un dispositif de protection efficace, les collaborateurs à tous les échelons hiérarchiques doivent obligatoirement être informés et formés régulièrement sur les cyberrisques, connaître les méthodes d'attaque les plus courantes, comme l'hameçonnage *(phishing)*, et savoir à quels services s'adresser au sein de l'entreprise s'ils découvrent des indices de cyberattaque. Il est possible de remplir cet objectif en organisant des tests réguliers pour les collaborateurs.

Pour les établissements auxquels s'applique la Circ.-FINMA 23/1, les exigences relatives à la formation et à la sensibilisation aux cyberrisques figurent explicitement dans la circulaire (voir le Cm 26).

En outre, il est indispensable que tous les établissements envisagent un scénario dans lequel leurs mesures de protection pourraient être déjouées et où une attaque parviendrait à causer le plus de dégâts possibles dans l'entreprise. Il est important que les stratégies de sauvegarde et de restauration existantes soient examinées afin de déterminer si, par exemple dans le cadre d'un cryptage complet des données (critiques), celles-ci peuvent être restaurées dans les délais impartis et en respectant les critères d'actualité, d'intégrité, de qualité et d'exhaustivité. Pour les banques, il est notamment fait référence aux nouvelles exigences prudentielles en matière de respect de la résilience opérationnelle selon la Circ.-FINMA 23/1.

2.4 Détection, réaction et récupération

La capacité d'enregistrer, de détecter et de réagir en temps réel aux cyberattaques est une priorité dans la plupart des contrôles sur place de la FINMA liés aux cyberrisques et fait souvent l'objet d'examens approfondis.

Lors de ces contrôles sur place, la FINMA a notamment observé les schémas récurrents suivants auprès des établissements surveillés :

- Certains établissements n'avaient aucun plan de réaction, ou des plans de réaction incomplets, en cas de cyberincidents ou ne vérifiaient pas l'efficacité de ces plans.
- En ce qui concerne la manière de reconnaître et de recenser les cyberattaques, il est en outre apparu que certains établissements ne surveil-

laient pas systématiquement et en permanence leur technologie d'information et de communication. Il manquait parfois une évaluation des fichiers journaux critiques ou celle-ci n'avait lieu que durant les heures de bureau.

- La plupart des établissements ont pris des mesures pour assurer un rétablissement rapide du fonctionnement normal consécutivement à des événements extraordinaires. Toutefois, il manquait souvent des mesures de récupération spécifiques à la suite de cyberattaques.

Il est essentiel pour les établissements assujettis de se préparer aux incidents et aux crises liés aux cyberattaques en fonction des risques et sur la base de scénarios. L'élaboration de plans de réaction réalistes et testés constitue un facteur de réussite essentiel pour gérer efficacement les situations de crise liées aux cyberattaques. En particulier, après une cyberattaque réussie, il est extrêmement important de tirer les enseignements correspondants et de mettre en œuvre immédiatement des améliorations.

3 Précisions sur la communication FINMA sur la surveillance 05/2020

Depuis que l'obligation de signaler les cyberattaques pour tous les établissements assujettis a été précisée dans la communication FINMA sur la surveillance 05/2020, la FINMA a reçu diverses demandes concernant son interprétation.

Certains points sont donc précisés ci-dessous :

- À partir du moment où une cyberattaque est détectée, l'établissement dispose de 24 heures pour faire une première annonce à la FINMA.
- Durant ces 24 heures, les établissements assujettis sont censés procéder à une première évaluation de la gravité de l'attaque afin de déterminer si elle remplit les conditions de matérialité pour être signalée à la FINMA[5].
- Pour le premier signalement dans les 24 heures, la FINMA attend une annonce informelle par courriel, téléphone, etc. au *key account manager* chargé de la surveillance de l'établissement concerné. Cette notification initiale doit contenir une première évaluation de la gravité de l'attaque et décrire de manière concise ce qui est connu à ce moment. Il n'est pas nécessaire à ce stade de remplir intégralement un formulaire via la plate-forme de saisie et de demande (EHP).

[5] Voir la communication FINMA sur la surveillance 05/2020, annexe 1.

- Les établissements qui sont également soumis à l'obligation de signaler selon la loi sur la sécurité de l'information (LSI; RS *128*) peuvent soumettre leur annonce dans les 24 heures via le formulaire de déclaration de l'Office fédéral de la cybersécurité (OFCS) et sélectionner l'option de transmettre le signalement à la FINMA, à condition que le respect du délai puisse être garanti. L'annonce complète dans les 72 heures doit toujours être transmise via EHP.
- Si un établissement doit choisir entre achever la détermination du degré de gravité pour une évaluation initiale ou respecter le délai de 24 heures, la priorité doit être donnée au respect du délai.
- Un premier signalement effectué dans les 24 heures à la FINMA peut être retiré à tout moment si l'établissement conclut, dans le cadre de la poursuite de l'enquête sur le degré de gravité et de son évaluation, que la cyberattaque n'a pas atteint le seuil de matérialité.
- Si le prestataire de services d'un établissement (par ex. hôpital, gestionnaire de fortune, cabinet d'avocats) n'est pas un partenaire d'externalisation important au sens de la Circ.-FINMA 18/3 « *Outsourcing* », l'établissement doit s'assurer – conformément notamment à l'art. 22 LSA, au Cm 68 Circ.-FINMA 23/1, à la communication FINMA sur la surveillance 05/2020 – qu'il est informé par le prestataire de services des cyberincidents survenant chez ce dernier. Si, dans un tel cas, l'établissement considère un cyberincident qui lui a été annoncé comme pertinent au sens de la communication FINMA sur la surveillance 05/2020, il doit également procéder aux signalements nécessaires auprès de la FINMA.
- Les délais d'annonce de 24 ou 72 heures ne comptent que les jours ouvrables bancaires officiels. Les cyberattaques dont le degré de gravité est « grave » constituent une exception. Celles-ci doivent être signalées à la FINMA dans les 24 heures, même en dehors des jours ouvrables bancaires.
- L'obligation de signaler en cas d'externalisation se présente comme suit : selon le Cm 23 Circ.-FINMA 18/3, l'assujetti continue d'assumer la même responsabilité vis-à-vis de la FINMA que s'il assurait lui-même la fonction externalisée. Cela signifie a contrario que le délai de signalement commence à courir dès que l'établissement, ou le prestataire tiers dans le cas de fonctions externalisées, a découvert un cyberincident. Cela garantit également l'égalité de traitement prudentielle pour les établissements qui n'ont pas externalisé de fonctions.
- Selon la communication FINMA sur la surveillance 05/2020, un rapport conclusif sur les causes (comprenant au moins le rapport d'enquête ou forensique, interne ou externe) est exigé pour les annonces de cyberattaques d'un degré de gravité « moyen ». Pour les annonces de cyberattaques de niveau « élevé » ou « grave », ce rapport sur les causes doit comprendre les éléments suivants :
    - Raison du succès de la cyberattaque

- Effets de l'attaque sur le respect des prescriptions prudentielles, sur le fonctionnement de l'établissement et sur les clients
- Mesures d'atténuation mises en place pour faire face aux conséquences de l'attaque

Pour les cyberattaques évaluées comme « graves », il faut également transmettre les preuves et analyses du bon fonctionnement de l'organisation de crise.

4 Cyberexercices fondés sur des scénarios

Pour les établissements auxquels s'applique la Circ.-FINMA 23/1, des cyberexercices fondés sur des scénarios doivent être réalisés en fonction des risques conformément au Cm 70 de la Circ.-FINMA 23/1. L'étendue et le contenu de ces exercices sont régis par le principe de proportionnalité. Pour les établissements d'importance systémique, la FINMA considère les exercices de *red teaming*[6] comme une composante nécessaire des cyberexercices. Les établissements qui ne sont pas d'importance systémique devraient réaliser au moins un exercice annuel de type *table-top*[7].

Les établissements des catégories de surveillance 4 et 5 peuvent s'acquitter de cette obligation en participant aux exercices du Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC)[8]. Chaque établissement participant doit s'assurer que le potentiel de menace de ces exercices est documenté de manière compréhensible et que les enseignements spécifiques à l'établissement tirés de ces exercices font l'objet d'un rapport. Si le potentiel de menace spécifique à un établissement ne peut pas être déduit du cyberexercice du Swiss FS-CSC (par ex. parce que le scénario d'exercice n'a pas de pertinence marquée pour le profil de cyberrisque d'un établissement), l'établissement doit tout de même effectuer un cyberexercice individuel fondé sur un scénario pour répondre au Cm 70.

La FINMA se réserve le droit de faire réaliser de tels cyberexercices fondés sur des scénarios en fonction du risque de manière sélective dans le cadre de l'audit prudentiel ou d'un audit supplémentaire, et de les accompagner étroitement. Il convient d'utiliser comme base des dispositifs établis[9].

[6] *Red teaming* : les experts en sécurité jouent le rôle d'un cybercriminel et tentent d'attaquer et de contourner les mesures de cybersécurité d'une entreprise en copiant le mode d'attaque d'un pirate.

[7] Exercice *table-top* : simulation et mise en œuvre d'un scénario sur papier (exercice à sec)

[8] Voir https://fscsc.ch/

[9] Comme TIBER-EU, CBEST Threat Intelligence-Led Assessments