La nouvelle obligation d'annonce des cyberattaques

Claire Tistounet et Philipp Fischer, le 31 mars 2025

L'obligation d'annonce des cyberattaques, introduite par les articles 74a *et seq.* de la Loi sur la sécurité de l'information (LSI) et précisée par la nouvelle ordonnance sur la cybersécurité (OCyS), entrera en vigueur le 1 avril 2025.

I. Contexte et objectifs

L'obligation d'annonce constitue un jalon majeur dans la stratégie nationale visant à prévenir et à gérer les cyberrisques. Les cyberattaques contre les infrastructures critiques — notamment les banques, les infrastructures de marchés financiers, les prestataires *cloud* et les assurances — représentent une menace croissante pour la sécurité publique et la résilience économique de la Suisse. Dans un tel contexte, les autorités ont souhaité doter l'Office fédéral de la Cybersécurité OFCS) d'une vision d'ensemble sur les cyberattaques en Suisse, afin de permettre à l'OFCS de pouvoir informer et assister les victimes potentielles. Aussi, et pour ce faire, il est nécessaire que l'OFCS soit informé des cyberattaques visant leurs moyens informatiques.

II. Champ d'application

L'obligation d'annonce des cyberattaques s'applique à divers types d'entités, dont notamment :

- les banques, assurances et infrastructures des marchés financiers (74b let. e LSI) ;
- les assurances sociales, dont les institutions de prévoyance et de libre passage, qu'elles soient enregistrées ou non (74b let. j LSI) ; à l'inverse, la prévoyance individuelle liée ou libre (piliers 3A et 3B) n'est pas soumise à l'obligation de notification ;
- les hautes écoles (74b let. a LSI) ;
- les autorités fédérales, cantonales et communales (74b let. b LSI) ; et
- les organisations chargées de tâches de droit public dans les domaines de la sécurité et du sauvetage, de l'approvisionnement en eau potable, du traitement des eaux usées et de l'élimination des déchets (74b let. c LSI).

La liste de toutes les entités soumises à l'obligation d'annonce se trouve à l'art. 74b LSI. L'OCyS prévoit quelques exceptions à cette obligation d'annonce (art. 12ss OCyS).

III. Obligation d'annonce

A. Élément déclencheur de l'obligation d'annonce

Les exploitants d'infrastructures critiques ont ainsi l'obligation de signaler toute cyberattaque qui, *alternativement* (art. 74d LSI et art. 14 OCyS) :

- met en péril le fonctionnement de l'infrastructure critique concernée, *e.* :
  - lorsque des collaborateurs ou des tiers sont touchés par des interruptions de système ; ou
  - lorsque l'infrastructure critique touchée ne peut maintenir ses activités qu'à l'aide de plans d'urgence ;
- a entraîné une manipulation ou une fuite d'informations, ce qui signifie que les *hackers* sont en mesure d'accéder de manière non autorisée à des données de l'infrastructure critique et de les modifier, chiffrer, voler, effacer, communiquer ou rendre accessibles à des tiers non autorisés. Par exemple, il y a manipulation ou fuite d'informations lorsque :
  - des informations importantes pour les affaires sont consultées, modifiées ou publiées par des personnes non autorisées ; ou
  - la violation de la sécurité des données est signalée au Préposé fédéral à la protection des données et à la transparence conformément à l'art. 24 LPD.
- n'a pas été détectée pendant une période prolongée (*e.* 90 jours), en particulier si des indices laissent penser qu'elle a été exécutée en vue de préparer d'autres cyberattaques ; ou
- s'accompagne d'actes de chantage, de menaces ou de contrainte envers l'exploitant d'une infrastructure critique, ses responsables, ses collaborateurs (actuels ou anciens) ou contre ses représentants.

L'OFCS est en charge de recevoir, d'analyser et de coordonner les réactions aux rapports de cyberattaques.

B. Délai et forme du signalement

Si les conditions de l'obligation d'annonce sont réalisées, l'exploitant d'une infrastructure critique doit signaler la cyberattaque à l'OFCS dans les 24 heures suite à la détection de l'attaque (art. 74e al. 1 LSI). L'OFSC met à disposition sur son site internet un formulaire d'annonce.

Si toutes les informations requises par la LSI et l'OCyS (voir *infra*) ne sont pas disponibles au moment du signalement, l'exploitant d'une infrastructure critique peut compléter ce dernier dans un second temps, dans un 14 jours suivant ledit signalement (art. 74e al. 3 LSI *cum* art. 16 al. 1 OCyS). À noter que si l'exploitant d'une infrastructure critique ne communique pas les informations requises dans ce délai de 14 jours, l'OFCS lui demande de compléter immédiatement le signalement ou de lui confirmer que ces informations ne sont pas disponibles (art. 16 al. 2 OCyS).

C. Contenu du signalement

Le signalement doit contenir des informations sur (art. 74e al. 2 LSI et art. 15 OCyS) :

- la nature et l'exécution de la cyberattaque :
  - la date et l'heure de la constatation de la cyberattaque ;
  - la date et l'heure de la cyberattaque (si elles ne sont pas connues, l'heure supposée de la cyberattaque peut être indiquée) ;
  - le type de cyberattaque (p. ex. DDoS, accès non autorisé, maliciel, abus ou utilisation inadéquate de l'infrastructure technologique) ;
  - le vecteur d'attaque (p. ex. phishing, exploitation de vulnérabilités, attaques par saturation des serveurs, vol d'identité) ; et
  - les données sur le *hacker* (p. ex. adresse IP, données DNS, URL de pages suspectes, valeurs de hachage de maliciels, signatures de virus, anomalies dans le trafic réseau ou comportement suspect d'un logiciel).
- l'existence ou non d'un chantage, d'une menace ou d'une contrainte en lien avec l'attaque ;
- le fait que l'attaque a fait l'objet ou non d'une plainte pénale ;
- les conséquences de la cyberattaque :
  - *la gravité du préjudice sur la disponibilité, l'intégrité et la confidentialité des informations propres et de celles de tiers* : selon l'évaluation des conséquences de la cyberattaque, un degré de gravité sera affecté au préjudice subi avec la qualification « faible, moyen, élevé ou grave », comme sur le formulaire de signalement de la FINMA (à noter que cette classification nourrit aussi la prise de décision lorsque l'aide de l'OFCS est demandée concernant la suite concrète à donner pour gérer la cyberattaque, voir *infra*) ; et
  - *les effets sur le fonctionnement de l'exploitant de l'infrastructure critique* : ces informations doivent ainsi indiquer l'ampleur des effets sur le fonctionnement de l'exploitant de l'infrastructure critique (notamment quant à l'accès aux systèmes

et aux données, la disponibilité des services pour les clients ou les citoyens et les processus internes, etc.). À cet égard, l'exploitant d'une infrastructure critique peut également s'exprimer sur l'intervalle de temps et la durée des répercussions de la cyberattaque et donner son pronostic sur la durée des conséquences de cette dernière.

- les mesures prises et, si elles sont connues, sur les mesures prévues (*cette information ressort du formulaire de l'OFCS et non des dispositions légales*) ; et
- si le signalement n'est pas transmis via les canaux de l'OFCS, la raison sociale, le nom et l'adresse de l'exploitant de l'infrastructure critique, ainsi que les coordonnées de l'auteur du signalement.

IV. Conséquences du signalement

A. Soutien de l'OFCS

L'art. 74 al. 3 LSI permet à l'OFCS d'assister les exploitants d'infrastructures critiques dans la gestion des cyberattaques et cybermenaces, sous réserve que le fonctionnement de ces infrastructures soit en péril et qu'un soutien équivalent ne soit pas disponible rapidement sur le marché. Ce soutien, basé sur des analyses techniques et des conseils organisationnels, est facultatif et inclut l'identification des causes d'incidents, l'analyse des vulnérabilités, et des recommandations pour mieux gérer ces situations.

À noter toutefois qu'en cas de demandes massives de soutien (art. 5 al. 1 OCyS) ou de cyberattaques se déclenchant simultanément (art. 5 al. 2 OCyS), l'OFCS priorise les cyberattaques selon leur impact sur la sécurité, l'ordre public, le bien-être ou l'économie, en concentrant ses ressources sur les événements les plus graves. Cette priorisation garantit une assistance rapide et adaptée aux infrastructures critiques, renforçant ainsi la résilience et la stabilité du pays face à des cybermenaces majeures.

B. Transmission d'informations entre autorités

Le formulaire d'annonce de l'OFCS permet aux exploitants d'infrastructures critiques de demander que les informations y incluses soient immédiatement transmises à d'autres autorités compétentes.

Aussi, concrètement, lors du signalement initial d'une cyberattaque, le formulaire de l'OFCS contient une option permettant de transmettre les informations à d'autres autorités concernées, notamment la FINMA et le PFPDT. Cette option prend la forme de cases à cocher dans

le formulaire.

Il sied toutefois de noter que l'harmonisation permise par le formulaire de l'OFCS est partielle, dans la mesure où ce dernier permet, si nécessaire, une annonce simultanée en faveur de plusieurs autorités, telles que la FINMA, le PFPDT, l'Office fédéral des assurances sociales (OFAS) pour les organes d'exécution de l'AVS, et le Secrétariat d'État à la politique de sécurité (SEPOS) pour les unités administratives de l'administration fédérale.

Pour ce faire, l'exploitant d'une infrastructure critique doit concrètement cocher, dans le formulaire de l'OFCS, la case « Transmettre à [la FINMA/au PFPDT/…] » afin que l'annonce soit transmise à l'autorité correspondante. L'exploitant d'une infrastructure critique doit également vérifier si les informations requises pour toutes les annonces nécessaires (*e.g.*, FINMA, PFPDT, OFCS) sont prévues dans le formulaire de l'OFCS. Si tel n'est pas le cas, l'exploitant devra transmettre les informations additionnelles directement aux autres autorités.

Après cette annonce initiale, le traitement ultérieur du dossier est effectué séparément par chaque autorité compétente. Les éventuelles demandes complémentaires ou précisions ne peuvent donc plus être soumises via le formulaire de l'OFCS. Aussi, quand bien même cette approche répond à l'objectif principal d'éviter une double saisie des informations initiales, un échange direct avec les différentes autorités peut rester nécessaire, car les obligations d'annonce poursuivent des objectifs distincts et peuvent nécessiter des informations spécifiques.

C. Conséquences en cas de violation de l'obligation de signaler

Si des indices laissent présumer une violation de l'obligation de signaler, l'OFSC en informe l'exploitant d'une infrastructure critique et lui fixe un délai approprié pour s'acquitter de son obligation (art. 74g al. 1 LSI). Si ce dernier ne s'acquitte pas de son obligation dans ce délai, l'OFCS rend une décision dans laquelle il lui fixe un nouveau délai et l'informe qu'elle est menacée d'une amende (art. 74g al. 2 LSI).

En l'absence de rectification après ces avertissements, une amende de CHF 100'000.- au maximum pourra être infligée à la personne physique en charge de l'obligation de signalement (art. 74h al. 1 et 2 LSI). A noter toutefois que les bases légales relatives aux amendes n'entreront en vigueur qu'au 1 octobre 2025, afin de laisser le temps aux autorités et aux organisations concernées de s'adapter au nouveau système. L'obligation de signalement s'applique pendant les 6 premiers mois, mais sans sanction en l'absence de déclaration pendant cette période.

V. Conclusion

L'entrée en vigueur de l'obligation d'annonce des cyberattaques représente une avancée majeure pour la cybersécurité en Suisse. En centralisant les signalements, l'OFCS acquiert une vue d'ensemble précieuse pour informer et soutenir les acteurs concernés, tout en offrant des analyses et des conseils adaptés en cas de crise. De plus, la mise en place de sanctions dissuasives souligne l'importance de la conformité et de la responsabilité dans la gestion des cyberrisques.

En conclusion, cette obligation d'annonce témoigne de l'engagement de la Suisse à renforcer sa sécurité numérique, tout en assurant une coordination efficace entre les exploitants d'infrastructures critiques et l'État, contribuant ainsi à la protection de l'économie et de la société face aux défis du cyberespace.

Proposition de citation : Claire TISTOUNET / Philipp FISCHER, La nouvelle obligation d'annonce des cyberattaques, 31 mars 2025 *in* www.swissprivacy.law/345