cssf

Commission de Surveillance
du Secteur Financier

Questions/Réponses de la CSSF – circulaire CSSF 24/847

Cadre de notification des incidents liés aux TIC

Questions/Réponses de la CSSF – circulaire CSSF 24/847

Cadre de notification des incidents liés aux TIC

TABLE DES MATIERES

Contexte

Le présent document se réfère à une liste de questions et de réponses (Questions/Réponses) relatives à plusieurs aspects clés de la circulaire CSSF 24/847 sur le cadre de notification des incidents liés aux TIC (ci-après la « Circulaire »). L'objectif est d'apporter des clarifications supplémentaires concernant les attentes prudentielles de l'autorité compétente.

Ce document sera actualisé lorsque cela s'avère nécessaire et la CSSF se réserve le droit d'adapter, à tout moment, son approche par rapport à toute question traitée dans les Questions/Réponses. De ce fait, il est important de vérifier régulièrement sur le site Internet de la CSSF si des questions ont été ajoutées et/ou si des positions ont été reconsidérées par rapport à des sujets revêtant une importance particulière pour vous.

Définitions

Les définitions reprises de la Circulaire qui sont pertinentes au regard des Questions/Réponses sont indiquées ci-dessous :

a) « Incident lié aux TIC » : un événement unique ou une série d'événements liés entre eux que l'Entité Surveillée n'a pas prévu, qui compromet la sécurité des réseaux et des systèmes d'information, et a un impact négatif sur la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou sur les services fournis par l'Entité Surveillée ;

b) « Incident majeur lié aux TIC » : un incident lié aux TIC qui a un impact négatif élevé sur les réseaux et les systèmes d'information qui soutiennent les fonctions critiques ou importantes de l'Entité Surveillée ;

c) « Opérateur de services essentiels » (« OSE ») : conformément à l'article 2, point 3°, de la Loi NIS, une entité publique ou privée dont le type figure à l'annexe de la Loi NIS et qui répond aux critères énoncés à l'article 7, paragraphe 2, de la Loi NIS ;

d) « Fournisseur de service numérique » (« FSN ») : conformément à l'article 2, point 5°, de la Loi NIS, une entité privée qui fournit un service numérique, tel que défini à l'article 2, point 4°, de la Loi NIS ;

e) « Incident significatif » : un incident qui a un impact significatif sur la continuité des services essentiels fournis par un OSE ou sur la prestation d'un service numérique par un FSN au sein de l'Union européenne. Aux fins de la Circulaire, un incident significatif est considéré par défaut comme « incident majeur lié aux TIC ».

Informations concernant les mises à jour

05/01/2024	**Première publication**

Question 1 : Quel est le lien entre la Loi NIS (ou NIS1) / la directive NIS2 / le règlement DORA et la Circulaire ?

Le terme « Loi NIS » utilisé dans la Circulaire fait référence à la loi du 28 mai 2019 relative aux réseaux et aux systèmes d'information, qui est également appelée « Loi NIS1 ». Il s'agit de la Loi NIS qui est actuellement en vigueur et qui est également la loi visée dans la Circulaire.

La directive NIS2 sera applicable lorsqu'elle sera transposée en droit luxembourgeois d'ici le 17 octobre 2024.

Le règlement DORA (Digital Operational Resilience Act) vise à renforcer la résilience opérationnelle numérique du secteur financier. Le règlement DORA n'entrera en vigueur que le 17 janvier 2025.

Le règlement DORA agit en tant que lex specialis par rapport à la directive NIS2 pour les entités financières tombant sous la directive NIS2, mais ni le règlement DORA ni la directive NIS2 ne sont encore applicables et, de ce fait, ils ne sont pas pertinents pour le moment dans le contexte de la Circulaire.

Question 2 : À quelles entités s'applique le chapitre 3 de la Circulaire ?

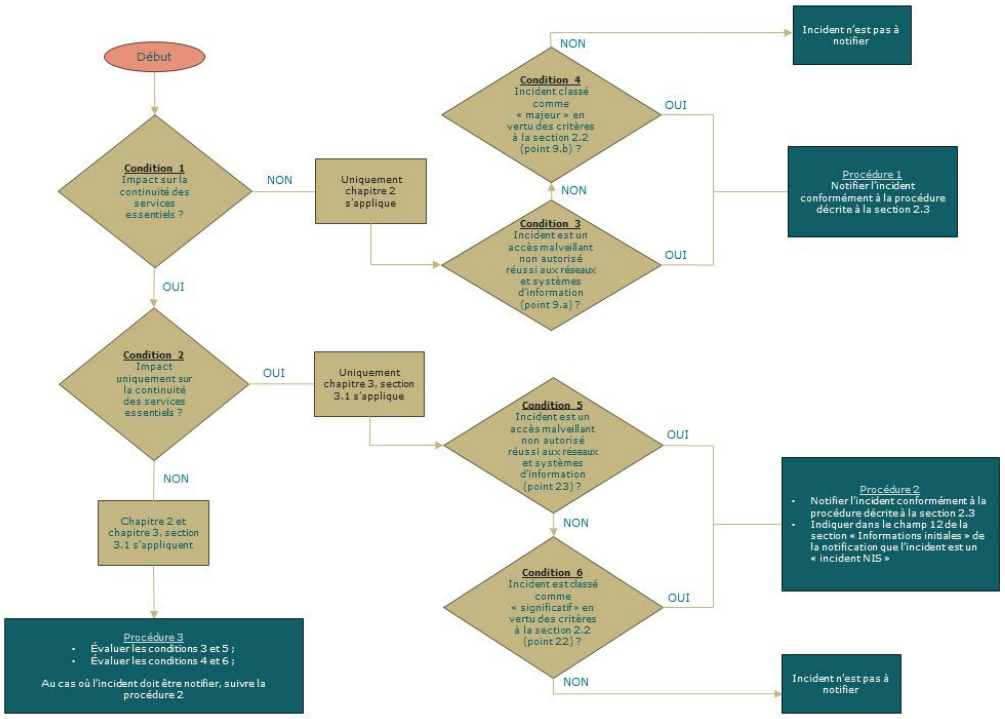
Le chapitre 3 de la Circulaire s'applique uniquement aux Entités Surveillées qui sont soit des opérateurs de services essentiels, « OES », soit des fournisseurs de service numérique, « FSN », en vertu de la Loi NIS1. Ces entités ont été notifiées de leur identification en tant qu'OSE ou ont été informées qu'elles sont considérées comme FSN lorsque la Loi NIS est entrée en vigueur. La CSSF a confirmé à nouveau le statut d'OSE respectivement de FSN aux Entités Surveillées concernées au courant du mois de février 2024. Les Entités Surveillées qui n'ont pas reçu de confirmation de la part de la CSSF ne sont donc pas désignées comme OSE ou ne sont pas considérées comme FSN sans préjudice d'une possible désignation ou information ultérieure.

Question 3 : Les dispositions du chapitre 2 sont applicables à toutes les Entités Surveillées telles que définies aux points 2.a) à n). Qu'en est-il des OSE et des FSN, tels que définis aux points 2.o) et p) ?

Les Entités Surveillées qui sont soit des OSE ou des FSN sont par défaut incluses au point 2.a). Les OSE sont soit des établissements de crédit, soit des infrastructures des marchés financiers qui sont des professionnels du secteur financier au sens de la LSF. Les FSN qui sont surveillés par la CSSF sont également des professionnels du secteur financier au sens de la LSF, plus particulièrement des PSF de support conformément à l'article 29-3 de la LSF.

Les exemples suivants clarifient la classification et le flux de notification :

1. **Un incident lié aux TIC intervient auprès d'une Entité Surveillée qui est un établissement de crédit selon le point 2.a) de la Circulaire et un OSE selon le point 2.o) de la Circulaire.**



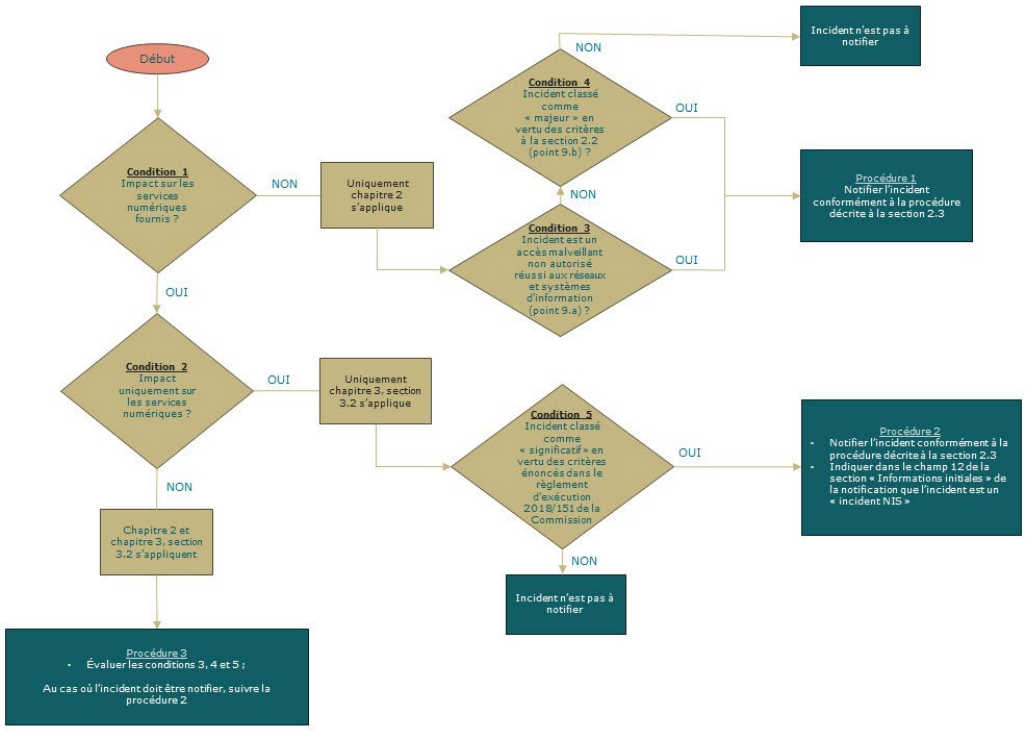
L'Entité Surveillée doit évaluer si l'incident lié aux TIC a un impact sur la continuité des services essentiels :

a) Non (par exemple, impact sur d'autres fonctions critiques ou importantes) : uniquement le chapitre 2 de la Circulaire s'applique ;

b) Oui, et uniquement sur les services essentiels : uniquement le chapitre 3, section 3.1. de la Circulaire s'applique. Ce chapitre décrit les étapes nécessaires afin de se conformer à la Loi NIS. Il se réfère aux éléments du chapitre 2 pour les critères de classification (2.2) et les exigences de notification (2.3) car la Loi NIS ne contient aucune disposition sur ce point. Les Entités Surveillées doivent indiquer dans le formulaire de notification que l'incident lié aux TIC est notifié en vertu du cadre NIS.

c) Oui, avec un impact sur les services essentiels ainsi que sur d'autres fonctions critiques ou importantes : le chapitre 2 (dans son entièreté) de même que le chapitre 3, section 3.1. de la Circulaire se référant aux mêmes exigences de classification et de notification s'appliquent. L'entité doit indiquer dans le formulaire de notification que l'incident lié aux TIC est également notifié en vertu du cadre NIS.

2. Un incident lié aux TIC intervient auprès d'une Entité Surveillée qui est un PSF de support selon le point 2.a) de la Circulaire et un FSN selon le point 2.p) de la Circulaire.



L'Entité Surveillée doit évaluer si l'incident lié aux TIC a un impact sur la fourniture de services numériques par l'entité :

a) Non (par exemple, impact sur d'autres services) : uniquement le chapitre 2 de la Circulaire s'applique ;

b) Oui, et uniquement sur les services numériques : uniquement le chapitre 3, section 3.2. de la Circulaire s'applique. Ce chapitre décrit les étapes nécessaires afin de se conformer à la Loi NIS. L'entité doit évaluer si l'incident est à classer en tant qu'incident significatif en vertu de la Loi NIS conformément aux seuils indiqués dans le règlement d'exécution (UE) 2018/151 de la Commission (point 26.a)). La section 3.2. fait également référence au chapitre 2 uniquement pour certains points de la section 2.2. (non liés à la classification) et pour la section 2.3. (pour les exigences de notification) alors que la Loi NIS et le règlement d'exécution de la Commission ne contiennent aucune disposition sur ce point. Les Entités Surveillées doivent indiquer dans le formulaire de notification que l'incident lié aux TIC est notifié en vertu du cadre NIS.

c) Oui, avec un impact sur les services numériques ainsi que sur d'autres services : le chapitre 2 (dans son entièreté) de même que le chapitre 3, section 3.2. de la Circulaire s'appliquent. L'entité doit indiquer dans le formulaire de notification que l'incident lié aux TIC est également notifié en vertu du cadre NIS.

Question 4 : Quelle est la signification du terme « réussi » dans le contexte de la section 2.1. point 9.a) « *Tout accès malveillant non autorisé réussi aux réseaux et systèmes d'information* » ?

L'utilisation par la CSSF du terme « réussi » dans le cadre d'accès malveillants non autorisés vise à différencier ces accès des simples « tentatives » sans intrusion.

Quelques exemples sont fournis ci-dessous :

Cas d'utilisation 1 : Ingénierie sociale, telle que l'hameçonnage (phishing), au cours duquel un employé de l'Entité Surveillée a cliqué sur un lien reçu par courriel :

- Si l'Entité Surveillée a des mécanismes de protection en place et bloque l'intrusion, ces tentatives d'ingénierie sociale ne sont pas considérées comme réussies et elles ne doivent pas être notifiées à la CSSF.
- Si l'Entité Surveillée n'a pas de mécanismes de protection en place, ou ces mécanismes sont en place mais ne suffisent pas pour bloquer l'intrusion, la CSSF considère que l'intrusion a eu lieu et l'incident est à notifier comme accès malveillant non autorisé réussi.

Cas d'utilisation 2 : Une Entité Surveillée est piratée, et les pirates informatiques ont pu chiffrer 2% des fichiers. Cependant, l'Entité Surveillée a été en mesure de détecter et d'isoler le problème :

- L'exemple montre qu'une vulnérabilité a existé et a été exploitée par un acteur malveillant. Même si l'impact est considéré comme limité par l'Entité Surveillée et aucun impact sur l'entreprise n'a été identifié au moment de l'incident, la CSSF estime que de telles intrusions non autorisées, même si les impacts ne sont pas connus immédiatement ou sont considérés comme mineurs, peuvent avoir des conséquences graves, notamment des violations de données et des fuites de données.
- La CSSF considère que cet incident doit être notifié comme accès malveillant non autorisé réussi.

Les attaques par hameçonnage visant des clients d'Entités Surveillées ne tombent pas dans le champ d'application de la Circulaire.

Question 5 : Quelle est la différence entre les notions d'« authenticité » et d'« intégrité » ?

La CSSF considère les définitions de base d'ISO/IEC 27000:2018, telles que documentées dans le « Cyber Lexicon » du Financial Stability Board (FSB).

- Authenticité : propriété selon laquelle une entité est ce qu'elle prétend être ;
- Intégrité : propriété d'exactitude et de complétude.

Dans le cadre de la circulaire CSSF 24/847, la CSSF estime qu'un incident lié aux TIC a un impact sur l'authenticité respectivement l'intégrité lorsque :

- L'incident a compromis la fiabilité de la source des données (authenticité)
- L'incident a occasionné une modification non autorisée des données qui les a rendues erronées ou incomplètes (intégrité).

Question 6 : Les incidents de sécurité physique sont-ils inclus dans le champ d'application de la Circulaire ?

Un incident de sécurité physique est considéré comme un incident lié aux TIC et ainsi inclus dans le champ d'application de la Circulaire si, à la suite d'un tel incident, la sécurité des réseaux et des systèmes d'information est compromise et si cela a un impact négatif sur la disponibilité, l'authenticité ou la confidentialité des données ou sur les services fournis par les Entités Surveillées.

Par exemple, les coupures du câble de réseau de fibre sont à considérer comme des incidents liés aux TIC.