CENTRE FOR CYBER SECURITY BELGIUM

Notification obligatoire d'un incident NIS par un OSE (résumé)			
Quoi ?	**A qui ?**	**Dans quel délai ?**	**Comment ?**
a) pour les OSE, sauf ceux supervisés par la BNB : **Tous les incidents ayant un impact** sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les service(s) essentiel(s) qu'il fournit. **b) pour les OSE supervisés par la BNB :** **Tous les incidents ayant un impact significatif** sur la disponibilité, la confidentialité, l'intégrité ou l'authenticité des réseaux et des systèmes d'information dont sont tributaires le ou les services essentiels qu'il fournit. La BNB est chargée de déterminer cet impact significatif.	**a) pour les OSE, sauf ceux supervisés par la BNB, notification simultanée de l'incident à trois autorités :** 1. le Centre pour la Cybersécurité Belgique (CCB) ; 2. le Centre de Crise national (NCCN) ; 3. l'autorité sectorielle et/ou le CSIRT sectoriel. **b) pour les OSE supervisés par la BNB :** notification directe à la BNB, selon les modalités fixées par celle-ci.	Notification de l'incident **sans retard**, c'est-à-dire le plus rapidement possible. L'OSE ne doit pas attendre de disposer de toutes les informations pertinentes sur un incident pour procéder à la notification. Lorsque les informations en sa possession lui permettent de savoir qu'il s'agit d'un incident soumis à notification, il doit le faire sans attendre.	**a) pour tous les OSE, sauf ceux supervisés par la BNB :** compléter le formulaire disponible sur la plate-forme de notification NIS : https://nis-incident.be La plate-forme assure alors l'envoi automatique des informations aux différentes autorités concernées. La plate-forme est accessible par le biais d'internet au moyen d'une connexion sécurisée et l'utilisation d'une clé d'identification unique à chaque opérateur de services essentiels. En cas d'indisponibilité de la plate-forme de notification NIS, l'OSE doit notifier l'incident via les modalités reprises sur le site du CCB (https://cert.be/fr/signaler-un-incident). **b) pour les OSE supervisés par la BNB :** notification directe à la BNB, selon les modalités fixées par celle-ci. Si la BNB impose à l'OSE d'utiliser la plate-forme de notification, la notification est simultanément aussi faite au CCB et au NCCN. Si la BNB n'impose pas l'utilisation de la plate-forme de notification, la BNB transmettra elle-même la notification, sans retard, au CCB et au NCCN.

Définitions :

Un incident est tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information.

La sécurité des réseaux et des systèmes d'information correspond à la capacité des réseaux et des systèmes d'information de résister, à un niveau de confiance donné, à des actions qui compromettent la disponibilité, l'authenticité, l'intégrité ou la confidentialité de données stockées, transmises ou faisant l'objet d'un traitement, et des services connexes que ces réseaux et systèmes d'information offrent ou rendent accessibles.

La disponibilité est l'aptitude d'un système d'information à être accessible et utilisable à la demande d'une entité autorisée. Il s'agit de garantir le fonctionnement normal d'un système d'information.

La confidentialité est l'aptitude d'un système d'information à ne pas permettre l'accès à ses données à des personnes ou entités non autorisées. Il s'agit d'éviter que les informations tombent entre des mains malveillantes ou soient rendues publiques sans le consentement du responsable du système d'information.

L'intégrité est l'aptitude d'un système d'information à ne pas être altéré par des entités non autorisées. Il s'agit de se prémunir contre une modification illégitime et nuisible du système d'information.

L'authenticité est l'aptitude d'un système d'information à confirmer qu'il est ce qu'il prétend être. Il s'agit d'être certain que les données proviennent bien d'un système d'information déterminé.

Autres obligations :

L'OSE qui est touché par un incident est obligé de **gérer l'incident et de prendre les mesures réactives afin de le résoudre**.

La gestion de l'incident demeure la responsabilité de l'opérateur de services essentiels.

L'opérateur de services essentiels doit **examiner les incidents ou évènements suspects qui lui sont notifiés par le CCB, l'autorité sectorielle ou le NCCN**.

Assistance technique:

Le CCB assure, dans la mesure du possible, un support technique de première ligne pour les utilisateurs de la plate-forme.

L'équipe technique du CCB peut être contactée :

- par e-mail : cert@cert.be
- par téléphone : +32 (0)2 501 05 60

L'IBPT assure, dans la mesure du possible, un support technique de deuxième ligne pour les utilisateurs de la plate-forme.

L'équipe technique de l'IBPT peut être contactée :

- par e-mail : netsec@bipt.be
- par téléphone : +32 (0)2 226 88 88

CSIRTs NETWORK

NIS COOPERATION GROUP

Notification des incidents NIS (sauf OSE supervisés par la BNB)

www.nis-incident.be

CENTRE FOR CYBER SECURITY BELGIUM

EUROPEAN CENTRAL BANK
EUROSYSTEM

CSIRTs NETWORK

NIS COOPERATION GROUP

Notification des incidents NIS OSE supervisés par la BNB

www.nis-incident.be

Notification volontaire			
Quoi ?	**A qui ?**	**Dans quel délai ?**	**Comment ?**
Tous les incidents ayant un impact significatif sur la continuité d'un service essentiel. Cette notification volontaire n'a pas pour effet d'imposer à l'entité qui est à l'origine de la notification des obligations auxquelles elle n'aurait pas été soumise si elle n'avait pas procédé à ladite notification.	Au CCB.	Dans les meilleurs délais	Via les modalités prévues sur le site du Centre pour la Cybersécurité Belgique (service CERT.be) : https://cert.be/fr/signaler-un-incident