CENTRE FOR
CYBER SECURITY
BELGIUM

GUIDE SUR LES NOTIFICATIONS D'INCIDENTS NIS

LES FOURNISSEURS DE SERVICE NUMÉRIQUE (FSN)

(« DIGITAL SERVICE PROVIDERS » - DSP)

CENTRE POUR LA
CYBERSECURITE BELGIQUE
Rue de la Loi, 16
1000 Bruxelles

nis@ccb.belgium.be
www.ccb.belgium.be

UNDER THE AUTHORITY
OF THE PRIME MINISTER

.be

CENTRE FOR CYBER SECURITY BELGIUM

Avertissement :

Le présent guide vise à répondre aux principales questions relatives à la notification des fournisseurs de service numérique NIS en Belgique.

Celui-ci n'est toutefois pas exhaustif et ne dispense pas les fournisseurs de service numérique de l'examen des dispositions légales générales ou sectorielles pertinentes.

Table des matières

A. Lexique 3

B. Qu'est-ce qu'un fournisseur de service numérique (FSN) ? 4

C. Notification des incidents NIS par les FSN 10

1. Quels événements doivent être notifiés obligatoirement par un FSN ? 10

2. Dans quel délai un incident doit-il être notifié ? 12

3. A qui le fournisseur de service numérique doit-il notifier l'incident ? 13

4. Comment le fournisseur de service numérique doit-il notifier l'incident ? 13

5. Quelles informations le fournisseur de service numérique doit-il transmettre ? 15

6. Quelles sont les différentes étapes de notification d'un incident ? 15

7. Quelles sont les règles relatives à la confidentialité des informations liées à un incident NIS ? 17

Que faire si un incident NIS est également une violation de données à caractère personnel 18

8. (RGPD) ? 18

D. Annexe 19

E. Sanctions 21

F. Assistance technique 22

G. Points de contact NIS 23

H. Références légales 24

A. Lexique

« Arrêté royal NIS » *: l'arrêté royal du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (M.B., 18 juillet 2019, p. 72187 et s).*

« Autorité sectorielle »*: l'autorité publique compétente pour le contrôle des FSN repris à l'annexe II de la loi du 7 avril 2019, à savoir le Ministre fédéral ayant l'Economie dans ses attributions ou, par délégation, le SPF Economie.*

« Centre pour la Cybersécurité Belgique (CCB) » : *administration fédérale sous l'autorité directe du Premier Ministre et créée par l'arrêté royal du 10 octobre 2014 (M.B., 21 novembre 2014, p. 91395 et s.).*

« Centre de crise national (NCCN) » : *Direction générale du Service public fédéral Intérieur, créé par l'arrêté royal du 18 avril 1988 (M.B., 4 mai 1988, p. 6408 et s).*

« Computer Emergency Response Team (CERT.be)» : *service opérationnel de réponse aux incidents de sécurité informatique du Centre pour la Cybersécurité Belgique.*

« CSIRT national » *: le Centre national de réponse aux incidents de sécurité informatique, à savoir le Centre pour la Cybersécurité Belgique (CCB) créé par l'arrêté royal du 10 octobre 2014.*

« Gestion d'incident » : *toutes les procédures utiles à la détection, à l'analyse et au confinement d'un incident et toutes les procédures utiles à l'intervention en cas d'incident.*

« Incident » : *tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information.*

« Loi NIS» *: la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (M.B., 3 mai 2019, p. 42857 et s).*

« Plate-forme de notification » *: la plate-forme de notification d'incidents visée à l'article 31 de la loi du 7 avril 2019.*

« Point de contact pour la sécurité des systèmes et réseaux d'information » *: le point de contact désigné par le fournisseur de service numérique et qui exerce la fonction de point de contact vis-à-vis du CCB du NCCN et de l'autorité sectorielle pour toute question liée à la sécurité des réseaux et des systèmes d'information de ses services numériques listés à l'annexe II de la loi du 7 avril 2019 ».*

« Règlement UE 2016/679 » *: le Règlement européen 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et abrogeant la Directive 95/46/CE (Règlement général sur la protection des données « RGPD »).*

« Réseau et système d'information » :

a) un réseau de communications électroniques au sens de l'article 2, 3°, de la loi du 13 juin 2005 relative aux communications électroniques ;
b) tout dispositif, tout ensemble de dispositifs interconnectés ou apparentés, de manière permanente ou temporaire, dont un ou plusieurs éléments assurent, en exécution d'un programme, un traitement automatisé de données numériques, en ce compris les composants numériques, électroniques ou mécaniques de ce dispositif permettant notamment l'automatisation du processus opérationnel, le contrôle à distance, ou l'obtention de données de fonctionnement en temps réel ;
c) ou les données numériques stockées, traitées, récupérées ou transmises par les éléments visés aux points a) et b), en vue de leur fonctionnement, utilisation, protection et maintenance.

« Risque » : *toute circonstance ou tout événement raisonnablement identifiable ayant un impact négatif potentiel sur la sécurité des réseaux et des systèmes d'information.*

« Sécurité des réseaux et des systèmes d'information » : *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.*

B. Qu'est-ce qu'un fournisseur de service numérique (FSN) ?

Un fournisseur de service numérique (FSN)[1] est une personne morale qui fournit un service numérique visé à l'annexe II de la loi NIS, qui a son siège principal en Belgique[2] et qui n'est pas une micro ou petite entreprise.

1. *Un service numérique*

Un « service numérique » est un service au sens de l'article 1er, paragraphe 1er, point b), de la directive européenne 2015/1535[3].

Cette disposition vise tout service de la société de l'information, c'est-à-dire tout service presté normalement contre rémunération, à distance, par voie électronique et à la demande individuelle d'un destinataire de services.

i) «à distance», un service fourni sans que les parties soient simultanément présentes;
ii) «par voie électronique», un service envoyé à l'origine et reçu à destination au moyen d'équipements électroniques de traitement (y compris la compression numérique) et de stockage de données, et qui est entièrement transmis, acheminé et reçu par fils, par radio, par moyens optiques ou par d'autres moyens électromagnétiques ;
iii) « à la demande individuelle d'un destinataire de services», un service fourni par transmission de données sur demande individuelle.

2. *Visé à l'annexe II de la loi NIS*

L'annexe II de la loi NIS vise 3 types de services numériques :

i) Service d'informatique en nuage (« *cloud computing service* »)

[1] Art. 6, 20° de la loi NIS et art. 4, 18) de la directive « NIS » (directive UE n°2016/1148 du 6 juillet 2016).
[2] Art. 3, § 2 de la loi NIS (siège principal ou lieu où est établi le représentant pour l'Union européenne du FSN).
[3] Directive européenne (UE) 2015/1535 du Parlement européen et du Conseil du 9 septembre 2015 prévoyant une procédure d'information dans le domaine des réglementations techniques et des règles relatives aux services de la société de l'information.

Le service d'informatique en nuage est un service numérique qui « permet l'accès à un ensemble modulable et variable de ressources informatiques pouvant être partagées »[4].

Les « ressources informatiques » comprennent des ressources telles que les réseaux, serveurs et autres infrastructures, le stockage, les applications et les services[5].

Le terme « modulable » renvoie aux ressources informatiques qui sont attribuées d'une manière souple par le fournisseur de services en nuage, indépendamment de la localisation géographique de ces ressources, pour gérer les fluctuations de la demande[6].

Les termes « ensemble variable » sont utilisés pour décrire les ressources informatiques qui sont mobilisées et libérées en fonction de la demande pour pouvoir augmenter ou réduire rapidement les ressources disponibles en fonction de la charge de travail[7].

Les termes « pouvant être partagées » visent les ressources informatiques qui sont mises à disposition de nombreux utilisateurs qui partagent un accès commun au service, le traitement étant effectué séparément pour chaque utilisateur bien que le service soit fourni à partir du même équipement électronique[8].

Les services d'informatique en nuage couvrent donc un vaste éventail d'activités qui peuvent être fournies selon différents modèles[9].

Il existe actuellement trois principaux types de modèles de service d'informatique en nuage qu'un fournisseur peut proposer[10] :

---

[4] Art. 6, 29° de la loi NIS et art. 4, 19) de la directive NIS.
[5] Voir le considérant 17 de la directive NIS.
[6] Idem.
[7] Idem.
[8] Idem.
[9] Idem.
[10] Annexe de la Communication de la Commission européenne du 13.9.2017 (COM/2017/0476) « Exploiter tout le potentiel de la directive SRI – *Vers la mise en œuvre effective de la directive (UE) 2016/1148 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union* » (https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=celex:52017DC0476); Parlement européen, « L'informatique en nuage Une vue

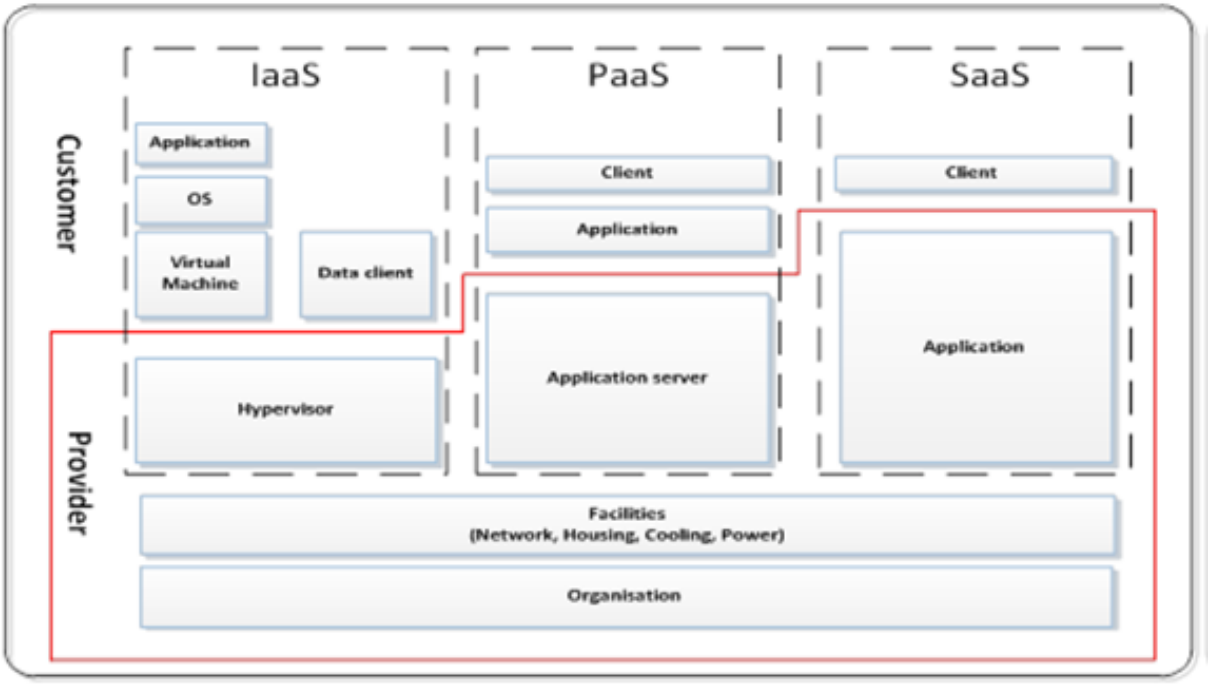
***Infrastructure à la demande (« Infrastructure as a Service – IaaS »)*:** le service fourni au client est une infrastructure. Il comprend la livraison virtuelle de ressources informatiques sous forme de matériel, de réseaux et de services de stockage. L'IaaS alimente les serveurs, le stockage, les réseaux et les systèmes d'exploitation. Il fournit une infrastructure d'entreprise dans laquelle une entreprise peut stocker ses données et exécuter les applications nécessaires à son fonctionnement quotidien.

Plateforme à la demande (« Platform as a Service – PaaS »): le service fourni au client est une plateforme. Il comprend des plateformes informatiques en ligne qui permettent aux entreprises d'exécuter des applications existantes ou de développer et tester de nouvelles applications.

Logiciel à la demande (« Software as a service – SaaS »): le service fourni au client est une application ou un logiciel déployé sur internet. Ce type de services en nuage supprime la nécessité pour l'utilisateur final d'acheter, d'installer et de gérer des logiciels et présente l'avantage de rendre le logiciel accessible depuis n'importe quel endroit avec une connexion internet.

---

d'ensemble des enjeux économiques et politiques », mai 2016 (https://www.europarl.europa.eu/RegData/etudes/IDAN/2016/583786/EPRS_IDA(2016)583786_FR.pdf).



(Modèles de services et ressources dans l'informatique en nuage) [11]

ii) Place de marché en ligne (« online marketplace »)

La place de marché en ligne est un service numérique qui permet à des consommateurs[12] et/ou à des entreprises[13] de conclure des contrats de vente ou de service en ligne avec des entreprises, soit sur le site internet de la place de marché en ligne, soit sur le site internet d'une entreprise qui utilise les services informatiques fournis par la place de marché en ligne[14].

Cette notion n'inclut pas les services en ligne qui ne servent que d'intermédiaires pour des services fournis par un tiers à travers lequel un contrat peut en définitive être conclu. Elle ne concerne donc

[11] Annexe de la Communication de la Commission européenne du 13.9.2017 (COM/2017/0476), p. 35 (Asset in cloud computing - https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes)
[12] Au sens de l'article I.1., alinéa 1er, 2°, du Code de droit économique.
[13] Au sens de l'article I.8, 39°, du Code de droit économique.
[14] Art. 6, 27° de la loi NIS et art. 4, 17) de la directive « NIS » (directive UE n°2016/1148 du 6 juillet 2016).

pas non plus les services en ligne qui comparent le prix de certains produits ou services de plusieurs professionnels, avant de réorienter l'utilisateur vers le professionnel choisi en vue de l'achat du produit[15].

Parmi les services informatiques fournis par la place de marché en ligne peuvent figurer le traitement de transactions, l'agrégation de données ou le profilage d'utilisateurs (par exemple, les magasins d'applications en ligne qui permettent la distribution numérique d'applications ou de logiciels émanant de tiers)[16].

iii) Moteur de recherche en ligne (« online search engine »)

Le moteur de recherche en ligne est un service numérique qui permet aux utilisateurs d'effectuer des recherches sur, en principe, tous les sites internet ou sur les sites internet dans une langue donnée, sur la base d'une requête lancée sur n'importe quel sujet sous la forme d'un mot clé, d'une phrase ou d'une autre entrée, et qui renvoie des liens à partir desquels il est possible de trouver des informations en rapport avec le contenu demandé[17].

La définition d'un moteur de recherche en ligne ne s'applique pas aux fonctions de recherche qui se limitent au contenu d'un site internet spécifique, indépendamment de la question de savoir si la fonction de recherche est assurée par un moteur de recherche externe[18]. Elle ne concerne pas non plus les services en ligne qui comparent le prix de certains produits ou services de différents professionnels et qui réorientent ensuite l'utilisateur vers le professionnel choisi en vue de l'achat du produit[19].

---

[15] Idem.
[16] Idem. Par exemple, un fournisseur tel qu'eBay peut être considéré comme une place de marché en ligne car il permet à d'autres fournisseurs de créer des boutiques sur sa plate-forme afin de mettre leurs produits et services en ligne à la disposition des consommateurs ou des entreprises (voir Annexe de la Communication de la Commission européenne du 13.9.2017 (COM/2017/0476), p. 33).
[17] Art. 6, 28° de la loi NIS et art. 4, 17) de la directive NIS.
[18] Considérant 16 de la directive NIS et Annexe de la Communication de la Commission européenne du 13.9.2017 (COM/2017/0476), p. 33.
[19] Idem.

3. *Qui n'est pas une micro ou petite entreprise*

Les micro ou petites entreprises, au sens de la recommandation de la Commission européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises 2003/361/CE, ne sont pas soumises aux obligations découlant de la loi NIS :

Petite entreprise[20]	entreprise qui occupe **moins de 50 personnes <u>et</u>** dont le chiffre d'affaires annuel (ou le total du bilan annuel) **n'excède pas 10 millions d'euros**. - **les deux conditions sont cumulatives**
Microentreprise[21]	entreprise qui occupe **moins de 10 personnes <u>et</u>** dont le chiffre d'affaires annuel (ou le total du bilan annuel) **n'excède pas 2 millions d'euros.** - **les deux conditions sont cumulatives**

En d'autres termes, la personne morale doit, d'une part, occuper plus de 50 personnes et, d'autre part, disposer d'un chiffre d'affaires annuel (ou total du bilan annuel) supérieur à 10 millions d'euros pour être considérée comme un fournisseur de service numérique visé par la loi NIS.

C. Notification des incidents NIS par les FSN

1. Quels événements doivent être notifiés obligatoirement par un FSN ?

Le fournisseur de service numérique NIS belge (voir point B), doit notifier **tout incident ayant un impact significatif sur la fourniture du ou des service(s) numérique(s) qu'il offre dans l'Union européenne** [22].

[20] Art. 2 (2.) Recommandation de la Commission européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises 2003/361/CE.
[21] Art. 2 (3.) Recommandation de la Commission européenne du 6 mai 2003 concernant la définition des micro, petites et moyennes entreprises 2003/361/CE.
[22] Art. 35, § 1er et 3, de la loi NIS.

Un incident est tout événement ayant un impact négatif réel sur la sécurité des réseaux et des systèmes d'information.[23]

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[24].

La Commission européenne a précisé les hypothèses où l'existence d'un impact significatif sur la fourniture d'un service numérique dans l'Union serait manifeste (Règlement d'exécution n° 2018/151 du 30 janvier 2018) :

Durée de l'incident : ***indisponibilité pendant plus de 5.000.000 hrs-utilisateur***	- ***la durée*** est calculée entre la perturbation de la bonne prestation du service en termes de disponibilité, d'authenticité, d'intégrité ou de confidentialité jusqu'au moment de son rétablissement *;* - ***une heure-utilisateur*** correspond au nombre d'utilisateurs affectés dans l'Union européenne pendant une durée de soixante minutes.
Nombre d'utilisateurs : ***plus de 100.000 utilisateurs affectés***	- ***les utilisateurs*** de service(s) numérique(s) englobent toutes les personnes physiques ou morales qui sont des clients ou abonnés d'un marché en ligne ou d'un service informatique en nuage, ou qui sont les visiteurs d'un moteur de recherche en ligne souhaitant effectuer des recherches par mots clés.

[23] Art. 6, 13°, de la loi NIS.
[24] Art. 6, 8° et 9°, de la loi NIS.

Nature de l'impact : ***risque pour la sécurité*** ***<u>ou</u> la sûreté publiques*** ***<u>ou</u> risque d'entraîner un décès***	- la nature de l'impact peut être connue par le FSN sur la base d'indications telles que la nature de ses relations contractuelles avec le client ou, le cas échéant, le nombre potentiel d'utilisateurs touchés.
Préjudice matériel : ***préjudice causé > 1.000.000 €***	- l'incident cause à <u>au moins un utilisateur dans l'Union</u> européenne un préjudice **> 1.000.000 €**

<u>Attention</u> :

Les seuils repris dans le règlement d'exécution de la Commission européenne du 30 janvier 2018 (n° 2018/151) ne doivent pas être considérés comme une liste exhaustive de tous les incidents ayant un impact significatif sur la fourniture d'un service numérique : il s'agit simplement d'une liste des cas manifestes où un incident doit être considéré comme ayant un impact significatif sur la fourniture d'un service numérique.

L'évaluation du caractère significatif ou non de l'impact d'un incident demeure <u>la responsabilité du fournisseur de service numérique</u>, sous le contrôle *a posteriori* du service d'inspection du SPF Economie.

Indépendamment des seuils et paramètres précités, les fournisseurs de service numérique sont encouragés à signaler volontairement tout incident dont ils ignoraient précédemment les caractéristiques, tels de nouveaux vecteurs d'attaque, menaces, risques ou vulnérabilités.

2. Dans quel délai un incident doit-il être notifié ?

Le FSN doit notifier l'incident sans retard, c'est-à-dire le plus rapidement possible[25].

L'obligation de notifier un incident ne s'applique qu'à partir du moment où le fournisseur de service numérique a accès aux informations nécessaires pour évaluer, complètement ou partiellement, l'impact de l'incident[26].

3. A qui le fournisseur de service numérique doit-il notifier l'incident ?

a) Le fournisseur de service numérique doit notifier simultanément l'incident à trois autorités[27] :

- le Centre pour la cybersécurité Belgique (CCB - service CERT.be) ;
- le Centre de Crise du Service public fédéral Intérieur (NCCN) ;
- Le SPF Economie (l'autorité sectorielle).

En pratique, cette notification est réalisée en une seule démarche en complétant le formulaire disponible sur la plate-forme de notification NIS. La plate-forme assure alors l'envoi automatique des informations aux trois autorités concernées.

b) Le FSN qui fournit un service numérique à un OSE doit également notifier, sans retard, à l'OSE concerné (son client) tous les incidents liés au(x) service(s) numérique(s) fourni(s) à cet OSE et qui ont un impact significatif sur la continuité des services essentiels de l'OSE concerné.

L'OSE doit notifier ensuite l'incident, selon les procédures de notification prévues pour les OSE.

4. Comment le fournisseur de service numérique doit-il notifier l'incident ?

---

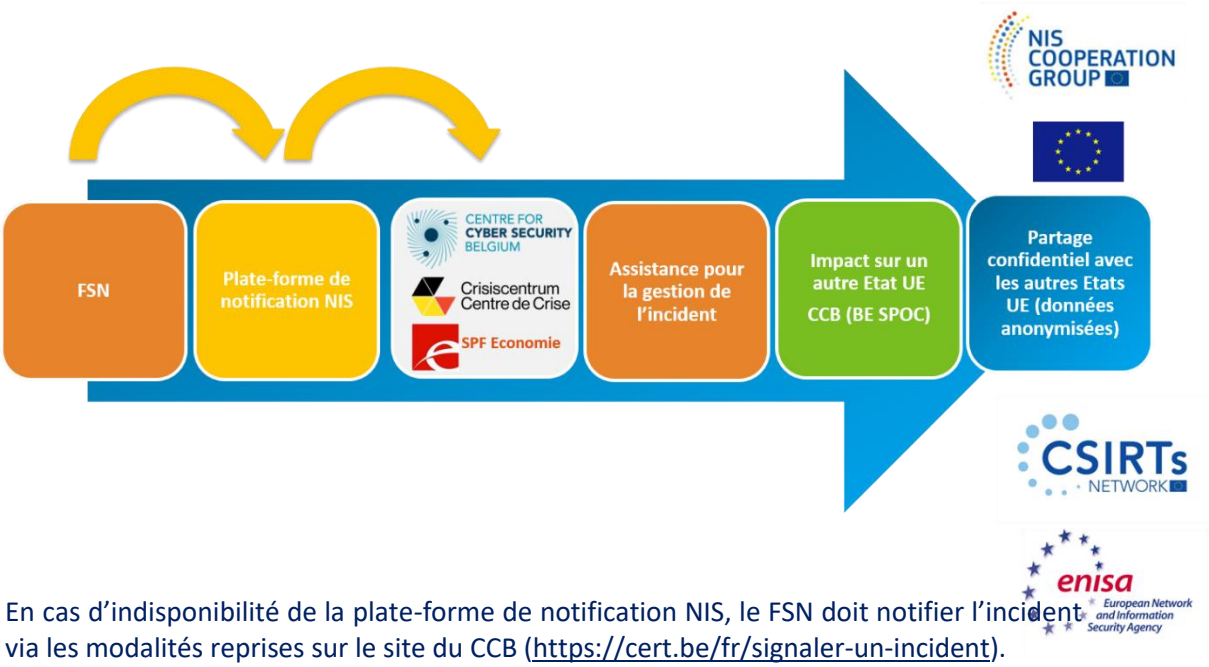
[25] Art. 35, § 1er, de la loi NIS.
[26] Art. 35, § 3, de la loi NIS.
[27] Art. 35, § 1er, de la loi NIS.

Le fournisseur de service numérique doit notifier l'incident via la plate-forme de notification NIS [28]: ***https://nis-incident.be***

Le FSN doit s'adresser au SPF Economie (nis-dsp@economie.fgov.be) pour obtenir la création d'un compte (nom d'utilisateur/mot de passe) pour accéder à la plate-forme de notification NIS.

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 fournisseur de service numérique[29].

Notification des incidents FSN NIS



En cas d'indisponibilité de la plate-forme de notification NIS, le FSN doit notifier l'incident via les modalités reprises sur le site du CCB (https://cert.be/fr/signaler-un-incident).

---

[28] Art. 36 de la loi NIS et art. 8 de l'AR NIS.
[29] Art. 7 de l'AR NIS.

5. Quelles informations le fournisseur de service numérique doit-il transmettre ?

Le fournisseur de service numérique utilisera le formulaire de notification d'incident, repris sur la plate-forme de notification NIS : ***https://nis-incident.be***

La notification contient toutes les informations disponibles permettant de déterminer la nature, les causes, les effets et les conséquences de l'incident [30]:

a) le nom et les coordonnées du fournisseur de service numérique et le service numérique qu'il fournit ;
b) la date et le moment où l'incident s'est produit ;
c) la durée de l'incident ;
d) l'étendue géographique de l'incident et son caractère éventuellement transfrontalier;
e) le nombre d'utilisateurs concernés ;
f) les informations sur la nature de l'incident ;
g) la portée de l'impact de l'incident, notamment sur les activités sociales et économiques ;
h) l'importance des systèmes ou de l'information concernée ;
i) l'impact de l'incident sur des organisations internationales installées en Belgique ;
j) les actions entreprises ;
k) la description de la situation actuelle.

6. Quelles sont les différentes étapes de notification d'un incident ?

Le fournisseur de service numérique doit tenir informé le CCB, le NCCN et le SPF Economie de l'évolution de l'incident ainsi que des actions de remédiation entreprises.

[30] Art. 8, § 1er, de l'AR NIS.

Lorsque le fournisseur de service numérique n'est pas en mesure de fournir toutes les informations reprises dans le formulaire à l'aide des éléments en sa possession, il complète la notification initiale via la plate-forme de notification dès que les informations manquantes sont disponibles. [31]

Il fait de même lorsque de nouvelles informations sont connues ou lorsque des développements importants surviennent. [32]

A la demande du CCB, du NCCN , du SPF Economie, le fournisseur de service numérique notifie via la plate-forme de notification une mise à jour du formulaire de notification retraçant la gestion de l'incident de sa découverte à sa clôture et reprenant toutes les informations reprises dans le formulaire de notification.[33]

La procédure de notification peut s'accomplir en plusieurs étapes :

a) ***Une notification initiale*** doit être effectuée, sans retard, même si le FSN ne dispose pas encore de toutes les informations pertinentes. Le but de cette notification initiale est d'attirer l'attention du CCB, du SPF Economie et du NCCN sur l'incident et de ses possibles conséquences.

b) ***Des notifications complémentaires***[34] doivent être envoyées périodiquement ou dès que le FSN dispose de nouvelles informations. Le but de ces notifications complémentaires est de mettre à jour le CCB, du SPF Economie, et du NCCN sur le statut de l'incident. Le FSN crée alors une nouvelle notification sur la plate-forme, en y ajoutant seulement les données nouvelles ainsi que le numéro de référence de la notification initiale.

c) ***Un éventuel rapport final*** (à la demande de l'une des autorités précitées) reprenant toutes les informations envoyées au CCB, au SPF Economie, et au NCCN. Le but de ce rapport final est de donner une vue d'ensemble de l'incident et de pouvoir en tirer des conclusions.

---

[31] Art. 8, § 2, de l'AR NIS.
[32] Art. 8, § 3, de l'AR NIS.
[33] Art. 8, § 4, de l'AR NIS.
[34] Art. 8, § 3, de l'AR NIS.

Le FSN doit tenir informé le CCB, le NCCN et le SPF Economie, de l'évolution de l'incident ainsi que des actions de remédiation entreprises.

Le CCB, le SPF Economie et le NCCN peuvent demander au fournisseur de service numérique des informations complémentaires sur les notifications qu'il a effectuées.

Lorsque les circonstances le permettent, le CCB fournit au fournisseur de service numérique qui est à l'origine de la notification toutes les informations utiles au suivi de sa notification, et le cas échéant toutes les informations qui pourraient contribuer à une gestion efficace de l'incident.[35]

7. Quelles sont les règles relatives à la confidentialité des informations liées à un incident NIS ?

Le FSN et ses sous-traitants limitent l'accès aux informations relatives aux incidents aux seules personnes ayant besoin d'en connaître et d'y avoir accès pour l'exercice de leurs fonctions ou de leur mission en lien avec la loi NIS.[36]

Cette règle vaut également pour le CCB (CSIRT national), le NCCN, le SPF Economie.

Les membres du personnel du fournisseur de service numérique et ses sous-traitants sont tenus au secret professionnel en ce qui concerne les informations en rapport avec un incident NIS [37].

Les informations fournies au CCB, au NCCN et au SPF Economie par un fournisseur de service numérique peuvent être échangées avec des autorités de l'Union européenne, avec d'autres autorités belges ou étrangères, lorsque cet échange est nécessaire à l'application de dispositions légales.

Cette transmission d'informations se limite toutefois à ce qui est pertinent et proportionné à l'objectif de cet échange, dans le respect du Règlement UE 2016/679, de la confidentialité des informations concernées, de la sécurité et des intérêts commerciaux du fournisseur de service numérique[38].

---

[35] Art. 10 de l'AR NIS.
[36] Art. 9, § 1er, de la loi NIS.
[37] Art. 9, § 2, de la loi NIS.
[38] Art. 9, § 3, de la loi NIS.

8. Que faire si un incident NIS est également une violation de données à caractère personnel (RGPD) ?

En fonction des informations introduites, le FSN recevra un message standard l'informant de son obligation de notifier les éventuelles violations de données à caractère personnel[39] à l'une des « autorités de contrôle » via les outils de notification appropriés (par exemple : www.autoriteprotectiondonnees.be/formulaire-notification-de-fuites-de-donnees).

Règles particulières relatives aux données à caractère personnel

Les traitements de données à caractère personnel effectués par un FSN dans le cadre de la loi NIS peuvent éventuellement déroger aux articles 12 à 22 du Règlement général sur la protection des données « RGPD » (*Règlement (UE) 2016/679 Chapitre III - Droits de la personne concernée*). L'exemption vaut, sous réserve du principe de proportionnalité et le cas échéant de minimisation des données, pour toutes les catégories de données à caractère personnel, dans la mesure où le traitement de ces données n'est pas étranger à la finalité du traitement (par exemple, la notification d'un incident) et est nécessaire pour cette finalité[40].

Les données (en ce compris les données à caractère personnel) ne doivent pas être conservées par le FSN plus longtemps que nécessaire pour la poursuite des objectifs de la loi avec une durée maximale de conservation ne pouvant excéder la durée du délai de prescription des infractions éventuelles visées aux articles 51, § 1 et 52, § 2 de la loi NIS[41].

---

[39] Art. 33, 1er alinéa, du règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
[40] Art. 71, § 2 et § 4 de la loi NIS.
[41] Art. 71, § 5, de la loi NIS.

D. Annexe

Extrait du Règlement d'exécution de la Commission européenne du 30 janvier 2018 (n° 2018/151) :

Article 3

Paramètres à prendre en compte pour déterminer si l'impact d'un incident est significatif

« 1. En ce qui concerne le nombre d'utilisateurs touchés par un incident, en particulier ceux qui recourent au service pour la fourniture de leurs propres services, visé à l'article 16, paragraphe 4, point a), de la directive (UE) 2016/1148, le fournisseur de service numérique est en mesure de procéder à une estimation de l'une des deux manières suivantes:

a) le nombre de personnes physiques et morales affectées avec lesquelles un contrat de prestation de service a été conclu; ou

b) le nombre d'utilisateurs affectés ayant utilisé le service sur la base, notamment, de précédentes données relatives au trafic.

2. La durée de l'incident visée à l'article 16, paragraphe 4, point b), est la période qui s'écoule entre la perturbation de la bonne prestation du service en termes de disponibilité, d'authenticité, d'intégrité ou de confidentialité jusqu'au moment de son rétablissement.

3. En ce qui concerne la portée géographique eu égard à la zone touchée par l'incident visée à l'article 16, paragraphe 4, point c), de la directive (UE) 2016/1148, le fournisseur de service numérique est en mesure de déterminer si l'incident affecte la fourniture de ses services dans des États membres donnés.

4. La gravité de la perturbation du fonctionnement du service visée à l'article 16, paragraphe 4, point d), de la directive (UE) 2016/1148 est mesurée en fonction d'une ou plusieurs des caractéristiques suivantes affectées par un incident: la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données ou des services connexes.

5. En ce qui concerne l'ampleur de l'impact sur les fonctions économiques et sociétales visée à l'article 16, paragraphe 4, point e), de la directive (UE) 2016/1148, le fournisseur de service numérique est en mesure de déterminer, sur la base d'indications telles que la nature de ses relations contractuelles avec le client ou, le cas échéant, le nombre potentiel d'utilisateurs touchés, si l'incident a causé d'importants préjudices matériels ou moraux aux utilisateurs, notamment en ce qui concerne la santé, la sécurité ou les dommages causés aux biens (…)».

Article 4

Impact significatif d'un incident

« 1. Un incident est considéré comme ayant un impact significatif si au moins l'une des situations suivantes s'est présentée:

a) le service fourni par un fournisseur de service numérique a été indisponible pendant plus de 5.000.000 heures-utilisateur, une heure-utilisateur correspondant au nombre d'utilisateurs affectés dans l'Union pendant une durée de soixante minutes;

b) l'incident a entraîné une perte de l'intégrité, de l'authenticité ou de la confidentialité des données stockées, transmises ou transformées ou des services connexes offerts ou accessibles par l'intermédiaire d'un réseau et d'un système informatique du fournisseur de service numérique, qui a touché plus de 100.000 utilisateurs dans l'Union;

c) l'incident a engendré un risque pour la sécurité <u>ou</u> la sûreté publiques <u>ou</u> a entraîné un décès [sic];

d) l'incident a causé un préjudice matériel à au moins un utilisateur dans l'Union dès lors que le préjudice causé à cet utilisateur dépasse 1.000.000 EUR (…) »

E. Sanctions

Manquement	Sanction pénale (par manquement)	Sanction administrative (par manquement)
Défaut de notification d'un incident.	Emprisonnement de 8 jours à 1 an et amende pénale de 208 € (26 € x 8 (*)) à 160.000 € (20.000 € x 8 (*)) ou une de ces deux peines.	Amende administrative de 500 à 75.000 €
Non-respect de la confidentialité /du secret professionnel.	Emprisonnement d'un an à trois ans et amende pénale de 800 € (100 € x 8 (*)) à 8.000 € (1.000 € x 8 (*)) ou une de ces deux peines (voir art. 458 du Code pénal).	
Faire subir des conséquences négatives aux personnes ayant procédés de bonne foi à la notification d'un incident.		Amende administrative de 500 à 200.000 €
Récidive	En cas de récidive pour les mêmes faits dans un délai de trois ans, l'amende pénale est doublée et le contrevenant puni d'une peine d'emprisonnement de 15 jours à 3 ans.	En cas de récidive pour les mêmes faits dans un délai de trois ans, l'amende administrative est doublée.

(*) décimes additionnels applicables au mois d'avril 2020 – voir le site du SPF Justice pour une actualisation du coefficient multiplicateur des décimes additionnels.

F. 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 : info@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

G. Points de contact NIS

CENTRE POUR LA CYBERSECURITE BELGIQUE (CCB)
Rue de la Loi, 16
1000 Bruxelles

NIS Team	nis@ccb.belgium.be	+32 (0)2 501 02 11	www.ccb.belgium.be
CERT.be Team	cert@cert.be	+32 (0)2 501 05 60	www.cert.be

SERVICE PUBLIC FÉDÉRAL INTÉRIEUR (SPF)
CENTRE DE CRISE NATIONAL (NCCN)
Rue Ducale, 53
1000 Bruxelles
www.centredecrise.be/fr/contact

SERVICE PUBLIC FEDERAL (SPF) ECONOMIE, P.M.E., CLASSES MOYENNES ET ENERGIE
Direction générale Qualité et sécurité
Métrologie – Service Réglementation Métrologie, cellule Digital Trust
Bd du Roi Albert II, 16
1000 Bruxelles

nis-dsp@economie.fgov.be

+32 0800 120 33 (contact center)

H. Références légales

- Loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (*M.B.*, 3 mai 2019, p. 42857 et s) – « loi NIS ».

- Arrêté royal du 12 juillet 2019 portant exécution de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique, ainsi que de la loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques (*M.B.*, 18 juillet 2019, p. 72187 et s) – « AR NIS ».

- Règlement d'exécution de la Commission du 30 janvier 2018 (n°2018/151) portant modalités d'application de la directive (UE) 2016/1148 du Parlement européen et du Conseil précisant les éléments à prendre en considération par les fournisseurs de service numérique pour gérer les risques qui menacent la sécurité des réseaux et des systèmes d'information ainsi que les paramètres permettant de déterminer si un incident a un impact significatif.

- Règlement UE 2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (Règlement générale sur la protection des données « RGPD »).

- Loi du 30 juillet 2018 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel (*M.B.*, 5 septembre 2018, p. 68616 et s.).

CENTRE FOR
CYBER SECURITY
BELGIUM

GUIDE SUR LES NOTIFICATIONS D'INCIDENTS - FOURNISSEURS DE SERVICE NUMÉRIQUE (FSN) NIS

Ce document et ses annexes ont été élaborés par le Centre pour la Cybersécurité Belgique (CCB), administration fédérale créé par l'arrêté royal du 10 octobre 2014 et sous l'autorité du Premier Ministre.

Tous les textes, mises en page, conceptions et autres éléments de toute nature dans ce document sont soumis à la législation sur les droits d'auteurs. La reproduction d'extraits de ce document est autorisé à des fins non commerciales exclusivement et moyennant mention de la source.

Le CCB décline toute responsabilité éventuelle en lien avec le contenu de ce document.

Les informations fournies :
• sont exclusivement à caractère général et n'entendent pas prendre en considération toutes les situations particulières ;
• ne sont pas nécessairement exhaustives, précises ou actualisées sur tous les points.

Éd. Responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur
Rue de la Loi, 16
1000 Bruxelles

Dépôt légal :
D/2020/14828/009

2020