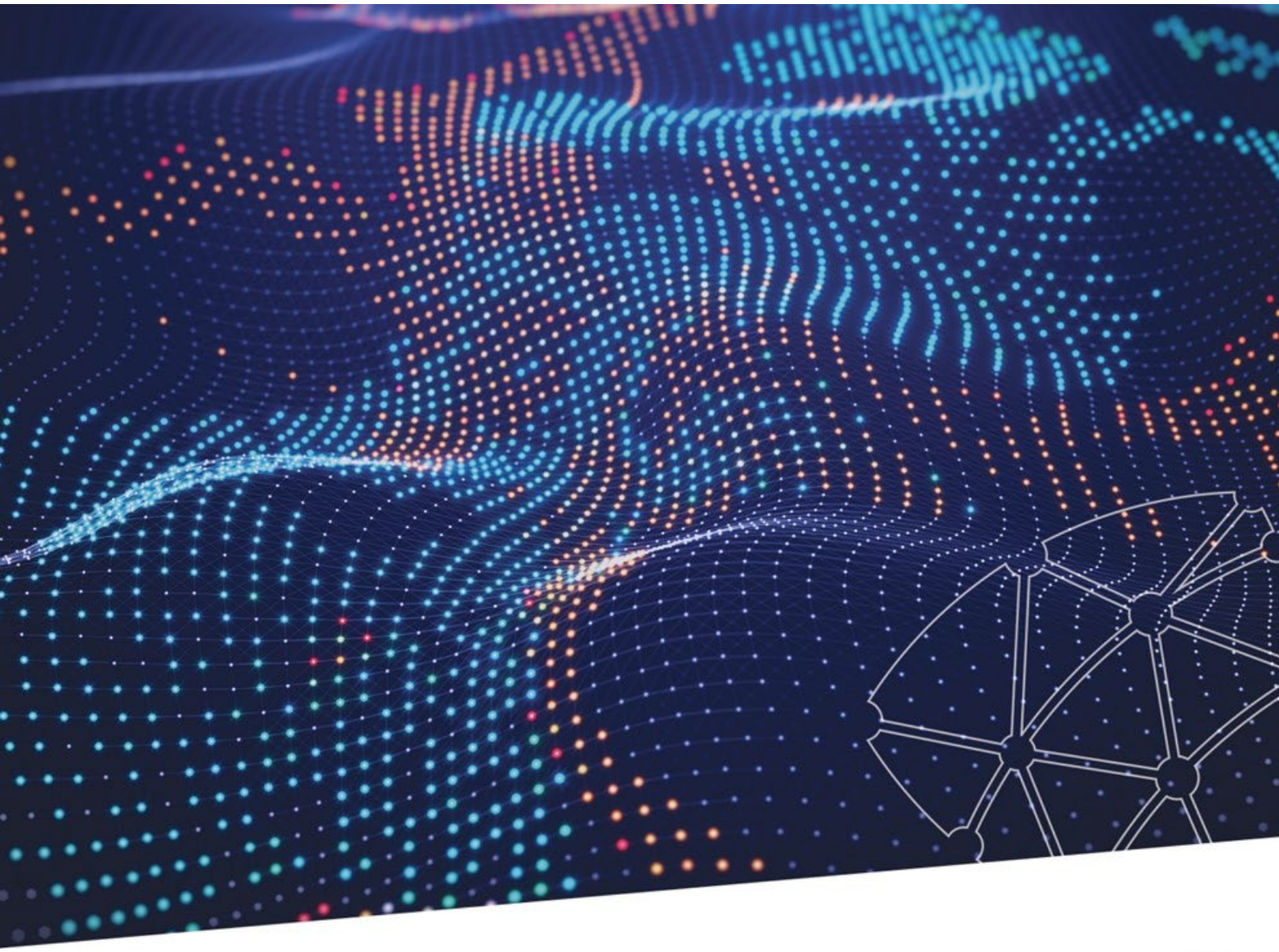
CENTRE FOR
CYBERSECURITY
BELGIUM



GUIDE SUR LES NOTIFICATIONS NIS2

Version 10.2024

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Introduction

La loi du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (la « loi NIS2 ») transpose la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 (la « directive NIS2 »).

Afin de faire face à l'expansion du paysage des cybermenaces et à l'émergence de nouveaux défis, l'Union européenne a adopté un nouveau texte législatif concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union (la directive 2022/2555 du 14 décembre 2022 - dite "directive NIS2"), qui remplace la "directive NIS1" (directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union).

L'une des obligations principales découlant de la directive et de la loi NIS2 est l'obligation d'information et de notification des incidents. Cette obligation vise à fournir de l'aide aux entités concernées, à informer adéquatement les différentes autorités compétentes, à diffuser des messages d'alerte sur certaines menaces pour d'autres entités et à collaborer au niveau national ou européen.

Le présent document a comme objectif de fournir des informations générales quant aux notifications et obligation d'information prévues dans le cadre de la loi NIS2, lesquelles entrent en vigueur le 18 octobre 2024.

Table des matières

A. Les notifications obligatoires

A.1. QUELS ÉVÉNEMENTS DOIVENT ÊTRE NOTIFIÉS OBLIGATOIREMENT PAR LES ENTITÉS SOUMISES À LA LOI NIS2 ?

Un évènement doit être obligatoirement notifiée lorsqu'il constitue un incident dit « significatif ». Cela implique deux éléments.

Premièrement, il doit s'agir d'**un incident**, tel que définit à l'art. 8, 5° de la loi NIS2 : « un événement compromettant la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles. »

Deuxièmement, l'incident doit constituer **un incident significatif** tel que définit à l'art. 8, 57° de la loi NIS2 : « tout incident ayant un impact significatif sur la fourniture de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la loi NIS2 et qui:

1° a causé ou est susceptible de causer une perturbation opérationnelle grave de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II ou des pertes financières pour l'entité concernée; ou
2° a affecté ou est susceptible d'affecter d'autres personnes physiques ou morales en causant des dommages matériels, corporels ou moraux considérables. »

A.2. COMMENT DÉTERMINER CONCRÈTEMENT SI UN INCIDENT EST OU NON SIGNIFICATIF?

Tout d'abord, l'incident (voir la définition, ci-avant) doit avoir un impact sur la fourniture de l'un des services fournis dans les secteurs ou sous-secteurs repris à l'annexe I et II de la loi, c'est-à-dire qu'il doit **affecter les réseaux et systèmes d'information qui supportent la fourniture de l'un ou de plusieurs de ces services** (par exemple, la distribution d'électricité).

Les notifications obligatoires ne concernent donc que les systèmes d'information et réseaux dont l'entité concernée est tributaire pour fournir le ou les services repris dans les annexes de la loi. Un incident affectant un système d'information isolé et sans lien avec la fourniture des services précités ne doit donc pas être notifié.

Ensuite, cet impact doit être significatif, à savoir causer ou susceptible de causer au moins l'une de ces trois situations :

- une **perturbation opérationnelle grave de l'un des services fournis** (dans les secteurs ou sous-secteurs repris à l'annexe I et II de la loi NIS2) ;
- des **pertes financières pour l'entité concernée** ;
- des **dommages matériels, corporels ou moraux considérables à d'autres personnes physiques ou morales**.

Afin de guider les entités dans cette évaluation, le CCB a identifié, ci-dessous, certaines situations concrètes dans lesquelles le caractère significatif d'un incident devrait être considéré par une entité, à tout le moins, comme établi.

Les situations décrites ne sont toutefois pas exhaustives ou limitatives des différents incidents significatifs qui pourraient survenir.

1) Un événement soupçonné d'origine malveillante compromettant l'authenticité, l'intégrité ou la confidentialité des données des réseaux ou systèmes d'information de l'entité, lequel provoque ou est susceptible de provoquer une perturbation opérationnelle grave.

Un tel évènement pourrait se produite lorsque (l'une de ces circonstance suffit):

- quelqu'un a obtenu un accès plus important que prévu aux réseaux, systèmes ou informations supportant la fourniture du ou des services de l'entité ;
- un système ou un réseau supportant la fourniture du ou des services de l'entité a été ou peut être configuré par une personne qui ne devrait pas avoir les droits de configurer le système ou le réseau de l'entité ;
- un système ou un réseau supportant la fourniture du ou des services de l'entité ne peut plus être configuré

par des utilisateurs privilégiés qui devraient avoir les droits de configurer le système ou le réseau ;
- des configurations ou des informations des systèmes supportant la fourniture du ou des services de l'entité ont été illégitimement modifiées, supprimées, ajoutées ou rendues non fiables ;
- un système ou un réseau supportant la fourniture du ou des services de l'entité exécute des tâches qu'il n'est pas censé exécuter ou n'exécute pas des tâches qu'il est censé exécuter ou n'exécute pas des tâches qu'il est censé exécuter liées à l'accès ou à l'intégrité du système ou réseau.

Par exemple, lorsqu'un acteur malveillant se positionne à l'avance dans le réseau et les systèmes d'information d'une entité concernée en vue de perturber les services à l'avenir, l'incident doit être considéré comme significatif.

2) Un événement compromettant la disponibilité des données des réseaux ou systèmes d'information de l'entité, laquelle provoque ou est susceptible de provoquer une perturbation opérationnelle grave.

Un tel évènement pourrait se produire lorsque :

- au moins 20 % des utilisateurs n'ont pas accès au service pendant au moins une heure ;
- les utilisateurs perdent l'accès au service pendant au moins une heure et l'entité ne peut pas déterminer le nombre d'utilisateurs touchés (en termes relatifs ou absolus) ;
- l'évènement provoque un retard dans la livraisons de produits allant au-delà des délais de livraison garantis contractuellement ;

Dans le cas d'un arrêt planifié pour maintenance, il n'y a pas d'incident si l'impact est limité à ce qui était prévu.

Le terme « utilisateur » doit être compris comme désignant les personnes physiques et/ou morales, les clients professionnels et/ou les clients finaux qui ont conclu avec l'entité concernée un contrat leur donnant accès au service ou aux données concernés, et qui ont subi ou subiront probablement les conséquences de l'incident. Pour calculer le nombre d'utilisateurs touchés, il faut prendre en compte le nombre de personnes physiques ou morales, de clients professionnels ou de clients finaux touchés.

La durée d'un incident ayant une incidence sur la disponibilité d'un service doit être mesurée à partir de l'interruption de la fourniture correcte de ce service jusqu'au moment de son rétablissement. Lorsqu'une entité concernée n'est pas en mesure de déterminer le moment où la perturbation a commencé, la durée de l'incident doit être mesurée à partir du moment où l'incident a été détecté ou à partir du moment où l'incident a été enregistré dans les journaux du réseau ou du système ou dans d'autres sources de données, la date la plus proche étant retenue.

On considère qu'il y a disponibilité limitée notamment lorsqu'un service fourni par une entité concernée est nettement plus lent que le temps de réponse moyen ou lorsque toutes les fonctionnalités d'un service ne sont pas disponibles. Dans la mesure du possible, il convient d'utiliser des critères objectifs fondés sur les temps de réponse moyens des services fournis par les entités concernées pour évaluer les retards dans les temps de réponse. Une fonctionnalité d'un service peut être, par exemple, une fonctionnalité de chat ou une fonctionnalité de recherche d'images.

3) Un événement causant ou susceptible de causer des pertes financières pour l'entité

Un tel évènement pourrait se produire lorsqu'il cause :

- une perte financière directe supérieure à 250 000€ ou à 5 % du chiffre d'affaires annuel total de l'entité concernée au cours de l'exercice complet précédent, le montant le plus faible étant retenu ;
- la perte ou la diffusion de la propriété intellectuelle d'une manière susceptible de compromettre les revenus ou le chiffre d'affaires futurs ;
- l'exfiltration de secrets commerciaux au sens de l'article 2, paragraphe 1, point 1), de la directive (UE) 2016/943 de l'entité concernée.

Pour déterminer les pertes financières directes résultant d'un incident, les entités concernées doivent prendre en compte toutes les pertes financières qu'elles ont subies du fait de l'incident, telles que :

- les coûts de remplacement ou de relocalisation des logiciels, du matériel ou des infrastructures ;
- les frais de personnel, y compris les coûts liés au remplacement ou à la relocalisation du personnel, au recrutement de personnel supplémentaire, la rémunération des heures supplémentaires et la récupération des compétences perdues ou altérées ;

- les frais liés au non-respect des obligations contractuelles ;
- les frais de réparation et d'indemnisation des clients, les pertes dues au manque à gagner ;
- les frais liés à la communication interne et externe ;
- les frais de conseil, y compris les frais liés aux conseils juridiques, aux services médico-légaux et aux services de remédiation ;
- d'autres frais liés à l'incident.

Toutefois, les amendes administratives, ainsi que les coûts nécessaires au fonctionnement quotidien de l'entreprise, ne doivent pas être considérés comme des pertes financières résultant d'un incident. Ces derniers comprennent entre autre :

- les coûts d'entretien général des infrastructures, des équipements, du matériel et des logiciels ;
- le maintien à jour des compétences du personnel ;
- les coûts internes ou externes visant à améliorer l'entreprise après l'incident, y compris les mises à niveau ;
- les améliorations et les initiatives d'évaluation des risques ;
- les primes d'assurance.

Les entités concernées doivent calculer les montants des pertes financières sur la base des données disponibles et, lorsque les montants réels des pertes financières ne peuvent être déterminés, les entités doivent les estimer.

4) Un événement causant ou susceptible de causer des dommages matériels ou immatériels affectant d'autres personnes physiques ou morales

Un tel évènement pourrait se produire lorsqu'il cause :

- la destruction partielle ou totale d'actifs physiques ou numériques ;
- des dommages à des infrastructures physiques provoquant un retard dans la livraisons de produits ou de services allant au-delà des délais de livraison garantis contractuellement ;
- des dommages tels que la mort d'une personne, l'hospitalisation, des blessures, des handicaps ;
- des conséquences financières substantielles.

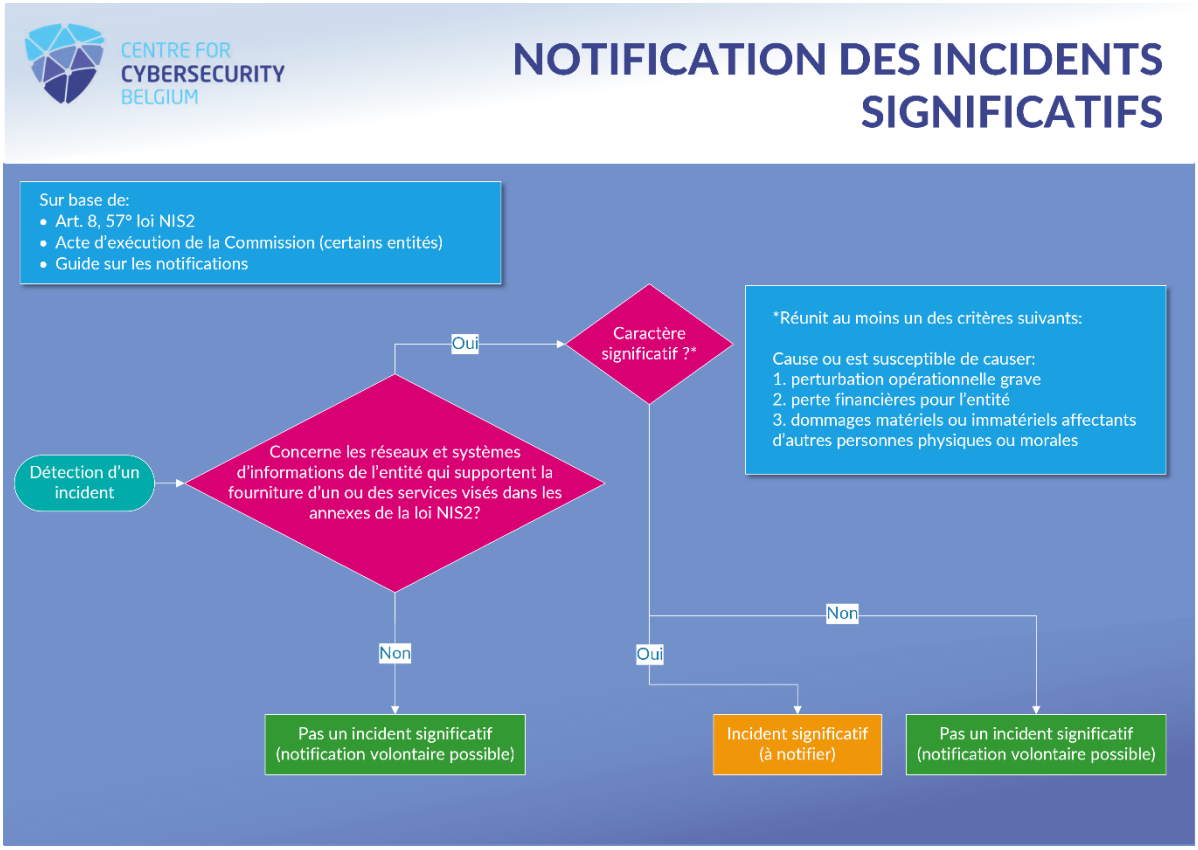
Les entités concernées devraient également être tenues de signaler les incidents qui ont causé ou sont susceptibles de causer la mort de personnes physiques ou des dommages considérables à leur santé, car ces incidents sont des cas particulièrement graves de dommages matériels ou immatériels considérables. Par exemple, un incident affectant une entité concernée pourrait entraîner l'indisponibilité de soins de santé ou de services d'urgence, ou la perte de confidentialité ou d'intégrité de données ayant un effet sur la santé de personnes physiques.

Pour déterminer si un incident a causé ou est susceptible de causer des dommages considérables à la santé d'une personne physique, les entités concernées doivent tenir compte du fait que l'incident a causé ou est susceptible de causer des blessures graves et des problèmes de santé. À cette fin, les entités concernées ne sont pas tenues de recueillir des informations supplémentaires auxquelles elles n'ont pas accès.

5) Un événement récurrent

Les incidents récurrents qui sont liés à la même cause première apparente et qui, pris individuellement, ne remplissent pas les critères d'un incident significatif, doivent être considérés collectivement comme un incident significatif, à condition qu'ils remplissent collectivement les critères de pertes financières (pour l'entité ou pour des tiers) ou de l'indisponibilité et qu'ils se soient produits au moins deux fois en l'espace de six mois.

Ces incidents récurrents peuvent révéler des lacunes et des faiblesses importantes dans les procédures de gestion du risque de cybersécurité de l'entité concernée et dans son niveau de maturité en matière de cybersécurité. En outre, ces incidents récurrents sont susceptibles d'entraîner des pertes financières importantes pour l'entité concernée.



A.3. EXISTE-T-IL DES RÈGLES PARTICULIÈRES ?

La Commission européenne va préciser dans un acte d'exécution (qui sera adopté prochainement) les critères pour évaluer si un incident est considéré comme significatif pour les types d'entités suivantes :

- les fournisseurs de services DNS ;
- les registres des noms de domaine de premier niveau ;
- les fournisseurs de services d'informatique en nuage ;
- les fournisseurs de services de centres de données ;
- les fournisseurs de réseaux de diffusion de contenu ;
- les fournisseurs de services gérés ;
- les fournisseurs de services de sécurité gérés ;
- les fournisseurs de places de marché en ligne ;
- les fournisseurs de moteurs de recherche en ligne ;
- les fournisseurs de plateformes de services de réseaux sociaux ;
- les fournisseurs de services de confiance.

Les entités relevant des secteurs bancaire et infrastructures des marchés financiers au sens de l'annexe I de la loi NIS2, et qui tombent dans le champ d'application du règlement (UE) 2022/2554 du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier (DORA), en ce compris l'activité de dépositaire central de titres exercée par la Banque Nationale de Belgique, ne sont pas soumises aux procédures de notification précitées[1].

Par ailleurs, les opérateurs de communications électroniques identifiés comme critiques utilisent la matrice d'escalade établie par l'IBPT et mettent en œuvre les moyens de redondance qui y sont prévus. De plus, il convient d'interpréter les articles 34 et 35 de la loi NIS2 comme nécessitant une notification d'alerte précoce dans les plus brefs délais, lorsque l'incident sous-jacent impacte la disponibilité des communications d'urgence visées à l'article 2, 60°, de la loi du 13 juin 2005 relative aux communications électroniques, étant donné l'importance que revêt ces communications et l'impact qu'une indisponibilité de ces communications peut avoir sur la vie ou l'intégrité physique

[1] Art. 6, § 3 de la loi NIS2.

des personnes.

A.4. DANS QUEL DÉLAI UN INCIDENT SIGNIFICATIF DOIT-IL ÊTRE NOTIFIÉ ?

Ces délais de notification courent à partir du moment où l'entité a connaissance d'un incident significatif. L'entité concernée est donc tenue de notifier les incidents qui, d'après son évaluation initiale, pourraient causer une grave perturbation opérationnelle des services ou une perte financière pour cette entité, ou affecter d'autres personnes physiques ou morales en causant des dommages matériels ou immatériels considérables.

Par conséquent, lorsqu'une entité concernée a détecté un événement suspect, ou après qu'un incident potentiel a été porté à son attention par un tiers, tel qu'une personne, un client, une entité, une autorité, un média ou une autre source, l'entité concernée doit évaluer en temps utile, en tenant compte de ses procédures internes, l'événement suspect pour déterminer s'il constitue un incident et, dans l'affirmative, en déterminer la nature et la gravité. L'entité concernée doit donc être considérée comme ayant pris « connaissance » de l'incident significatif lorsque, après cette évaluation initiale, elle a un degré raisonnable de certitude qu'un incident significatif s'est produit.

Dès le moment où une entité NIS2 est raisonnablement en situation de savoir qu'elle fait face à un incident significatif, elle doit le notifier au CSIRT national (le CCB). Cette notification se décline en plusieurs étapes[2] :

1) **sans retard injustifié et, en tout état de cause, dans les 24 heures** après avoir eu connaissance de l'incident significatif, l'entité soumet une alerte précoce (Early Warning);
2) **sans retard injustifié et, en tout état de cause, dans les 72 heures (24 heures pour les prestataires de services de confiance) après avoir eu connaissance de l'incident significatif**, l'entité soumet une notification d'incident ;
3) à la demande du CSIRT national ou, le cas échéant, de l'autorité sectorielle compétente, l'entité présente un rapport intermédiaire ;
4) **au plus tard un mois après la notification de l'incident** visée au point 2, l'entité présente un rapport final ;
5) en cas d'incident en cours au moment de la présentation du rapport final, l'entité concernée présente un rapport d'avancement puis, dans le mois qui suit le traitement de l'incident, un rapport final.

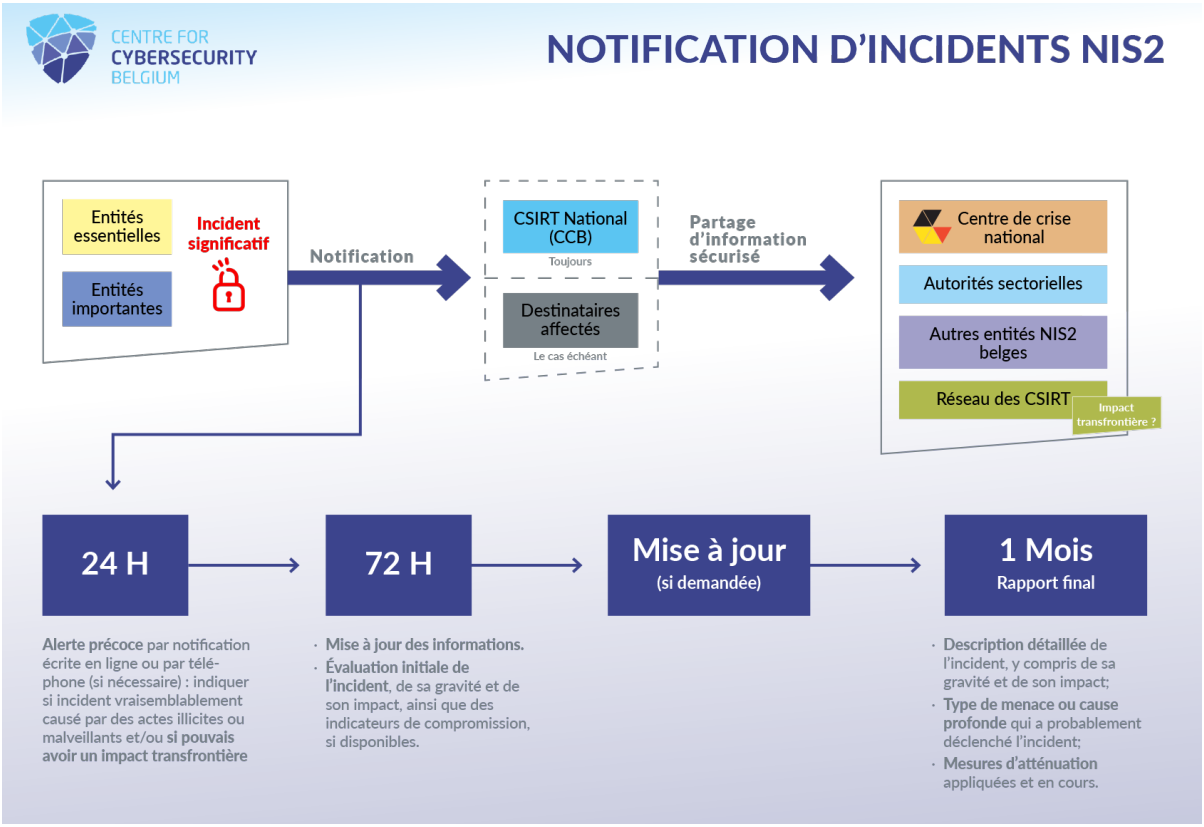
Le terme "sans retard injustifié" signifie que l'entité qui est en mesure de le faire doit notifier l'incident le plus vite possible, sans attendre les échéances maximales de 24 heures et 72 heures. Seules des circonstances particulières dûment justifiées peuvent conduire à attendre l'extrême limite de ces échéances. Le respect des procédures internes de l'organisation ne peut conduire à un retard déraisonnable dans la notification de l'incident.

Lorsque l'incident significatif est susceptible de nuire à la fourniture des services repris dans les annexes de la loi, l'entité doit également informer, sans retard injustifié, les destinataires de ses services (pour autant que ceux-ci soient identifiables). Cette obligation d'information peut être réalisée par tous moyens disponibles (informations sur le site internet, mailing list, message dans une application, communications papier, etc).

L'entité NIS2 doit également communiquer, sans retard injustifié, aux destinataires de ses services potentiellement affectés par une cybermenace importante (voir la définition reprise ci-après dans la section notification volontaire) toutes les mesures ou corrections que ces destinataires peuvent appliquer en réponse à cette menace.

Le CCB peut partager les informations reçues par l'entité avec d'autres autorités dans la limite de ce qui est nécessaire.

[2] Art. 35 de la loi NIS2 et le visuel ci-dessous.



A.5. COMMENT L'ENTITÉ DOIT-ELLE NOTIFIER UN INCIDENT ?

Pour chacune des étapes mentionnées au point précédent, la notification est effectuée par l'entité concernée au travers d'un formulaire en ligne: https://notif.safeonweb.be (sauf indisponibilité ou impossibilité technique). Les différents champs du formulaire de notification en ligne sont expliqués à l'annexe 2 de ce guide.

Afin d'éviter d'éventuels obstacles à la notification et étant donné la situation d'urgence présumée dans lequel se trouve toute entité, l'usage de l'outil de notification ne requiert pas d'authentification préalable.

Un numéro d'appel téléphonique d'urgence **(+32 (0)2 501 05 60**) est également disponible. Ce canal a pour objectif de permettre aux entités qui le souhaitent de contacter le CSIRT national en cas d'urgence, lorsqu'une intervention immédiate du CSIRT national est nécessaire dans le cadre d'un incident. En cas d'indisponibilité du formulaire ou d'impossibilité technique pour l'entité, un tel appel téléphonique d'urgence peut être considéré équivalent aux notifications visées à l'article 35 de la loi NIS2.

A.6. INFORMATIONS À TRANSMETTRE LORS DE LA NOTIFICATION D'UN INCIDENT SIGNIFICATIF

Les différentes étapes de notification comportent différentes informations à transmettre (voir le formulaire en ligne) :

- **L'alerte précoce** (Early warning) indique si l'on suspecte que l'incident significatif pourrait avoir été causé par des actes illicites ou malveillants ou s'il pourrait avoir un impact transfrontière (c'est-à-dire un impact dans un autre pays de l'Union européenne). Cette alerte précoce inclut uniquement les informations nécessaires pour porter l'incident à la connaissance du CSIRT, et permet à l'entité concernée de demander une assistance, si nécessaire.
  Cette alerte ne doit pas détourner les ressources de l'entité effectuant la notification des activités liées à la gestion des incidents qui devraient avoir la priorité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents importants ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard.
- **La notification d'incident** dans les 72h a pour objectif de mettre à jour les informations communiquées dans le cadre de l'alerte précoce. Elle fournit également une évaluation initiale de l'incident, y compris de sa gravité et de son impact, ainsi que des indicateurs de compromission (IOC), lorsqu'ils sont disponibles.

Comme pour l'alerte précoce, la notification d'incident ne doit pas détourner les ressources de l'entité, afin d'éviter que les obligations de notification des incidents ne détournent les ressources de la gestion des incidents significatifs ou ne compromettent d'une autre manière les efforts déployés par l'entité à cet égard.

- **Le rapport intermédiaire** contient les mises à jour pertinentes de la situation.
- **Le rapport final** doit comprendre une description détaillée de l'incident, y compris de sa gravité et de son impact; le type de menace ou la cause profonde qui a probablement déclenché l'incident; les mesures d'atténuation appliquées et en cours; et le cas échéant, l'impact transfrontière de l'incident.
- **Le rapport d'avancement** contient autant que possible les informations qui devraient se trouver dans le rapport final et qui sont en la possession de l'entité au moment de la communication du rapport d'avancement.

B. Les notifications volontaires

Les entités essentielles et importantes peuvent notifier les incidents (non significatifs), les cybermenaces et les incidents évités.

Une cybermenace est « toute circonstance, tout événement ou toute action potentiels susceptibles de nuire ou de porter autrement atteinte aux réseaux et systèmes d'information, aux utilisateurs de tels systèmes et à d'autres personnes, ou encore de provoquer des interruptions de ces réseaux et systèmes »[3].

Un incident évité est « un événement qui aurait pu compromettre la disponibilité, l'authenticité, l'intégrité ou la confidentialité des données stockées, transmises ou faisant l'objet d'un traitement, ou des services que les réseaux et systèmes d'information offrent ou rendent accessibles, mais dont la réalisation a pu être empêchée ou ne s'est pas produite »[4].

Les entités qui ne sont ni essentielles, ni importantes peuvent notifier des incidents significatifs, des cybermenaces et des incidents évités.

Ces notifications volontaires sont traitées de la même manière que les notifications obligatoires, mais les notifications obligatoires peuvent néanmoins être traitées en priorité.

Un signalement volontaire n'a pas pour effet direct de mener à une inspection de l'entité ayant effectuée le signalement ou de lui imposer des obligations supplémentaires auxquelles elle n'aurait pas été soumise si elle n'avait pas transmis la notification[5].

C. Règles de confidentialité qui s'appliquent aux informations transmises lors d'une notification

L'entité NIS2 et ses sous-traitants limitent l'accès aux informations relatives aux incidents, au sens de la loi NIS2, 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 cette loi. Cette règle vaut également pour le CCB (en tant que CSIRT national), le Centre de crise national (NCCN) et l'éventuelle autorité sectorielle compétente.

Les notifications sont partagées immédiatement par le CSIRT national aux éventuelles autorités sectorielles compétentes, et au NCCN lorsque la notification émane d'une entité essentielle[6].

Les informations fournies au CCB, au NCCN et à l'autorité sectorielle par une entité NIS2 peuvent être échangées de manière anonymisées avec des autorités d'autres États membres de l'Union européenne et avec d'autres

[3] Art. 8, 10° de la loi NIS2 et art. 2, point 8), du règlement (UE) 2019/881 – « CSA ».
[4] Art. 8, 6° de la loi NIS2.
[5] Art. 38, § 2, al. 3 de la loi NIS2 – sans préjudice de la prévention et de la détection d'infractions pénales et des enquêtes et poursuites en la matière.
[6] Art. 34 de la loi NIS2.

autorités belges 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 (RGPD), de la confidentialité des informations concernées, de la sécurité et des intérêts commerciaux des entités NIS2.

D. Que se passe-t-il si un incident se produit et qu'il implique aussi des données à caractère personnel ?

Comme cela est déjà le cas actuellement, les notifications d'incident dans le cadre de la loi NIS2 ne remplacent les éventuelles notifications dans le cas d'une violation de données à caractère personnel, par exemple à l'Autorité de protection des données (APD). Deux notifications distinctes seront toujours nécessaires.

Toutefois, la loi prévoit une collaboration renforcée entre l'autorité nationale de cybersécurité et les autorités de protection des données. Cette collaboration pourrait conduire au développement d'outils communs.

Une notification à l'APD peut se faire sur leur site internet[7].

[7] https://www.autoriteprotectiondonnees.be/professionnel/actions/fuites-de-donnees-personnelles.

Annexe 1 -Tableau récapitulatif – incident significatif

Type d'évènement	Exemples
Evénement soupçonné d'origine malveillante compromettant l'authenticité, l'intégrité ou la confidentialité des données des réseaux ou systèmes d'information de l'entité, lequel provoque ou est susceptible de provoquer une perturbation opérationnelle grave	• quelqu'un a obtenu un accès plus important que prévu aux réseaux, systèmes ou informations supportant la fourniture du ou des services de l'entité ; • un système ou un réseau supportant la fourniture du ou des services de l'entité a été ou peut être configuré par une personne qui ne devrait pas avoir les droits de configurer le système ou le réseau de l'entité ; • un système ou un réseau supportant la fourniture du ou des services de l'entité ne peut plus être configuré par des utilisateurs privilégiés qui devraient avoir les droits de configurer le système ou le réseau ; • des configurations ou des informations des systèmes supportant la fourniture du ou des services de l'entité ont été illégitimement modifiées, supprimées, ajoutées ou rendues non fiables ; • un système ou un réseau supportant la fourniture du ou des services de l'entité exécute des tâches qu'il n'est pas censé exécuter ou n'exécute pas des tâches qu'il est censé exécuter liées à l'accès ou à l'intégrité du système ou réseau.
Evénement compromettant la disponibilité des données des réseaux ou systèmes d'information de l'entité, laquelle provoque ou est susceptible de provoquer une perturbation opérationnelle grave	• au moins 20 % des utilisateurs n'ont pas accès au service pendant au moins une heure ; • les utilisateurs perdent l'accès au service pendant au moins une heure et l'entité ne peut pas déterminer le nombre d'utilisateurs touchés (en termes relatifs ou absolus) ; • l'évènement provoque un retard dans la livraisons de produits allant au-delà des délais de livraison garantis contractuellement ; • les opérations de maintenance planifiées ne doivent pas être prises en considération (par exemple, l'arrêt planifié pour maintenance).
Pertes financières pour l'entité concernée	• une perte financière directe supérieure à 250 000 € ou à 5 % du chiffre d'affaires annuel total de l'entité concernée au cours de l'exercice complet précédent, le montant le plus faible étant retenu ; • la perte ou la diffusion de la propriété intellectuelle d'une manière susceptible de compromettre les revenus ou le chiffre d'affaires futurs ; • l'exfiltration de secrets commerciaux au sens de l'article 2, paragraphe 1, point 1), de la directive (UE) 2016/943 de l'entité concernée.
Dommages matériels, corporels ou moraux considérables à d'autres personnes physiques ou morales	• Destruction partielle ou totale d'actifs physiques ou numériques ; • Dommages à des infrastructures physiques provoquant un retard dans la livraisons de produits allant au-delà des délais de livraison garantis contractuellement ; • Dommages tels que la mort d'une personne, l'hospitalisation, des blessures, des handicaps ; • Conséquences financières substantielles.

Annexe 2 - Explications du formulaire de notification

Les différents champs du formulaire de notification sont décrit ci-dessous. Dans la colonne de gauche se trouvent l'intitulé technique du champ (entre crochets) ainsi que l'intitulé visible par les utilisateurs (en gras). Dans la colonne de droite se trouve la description du champ. Les champs sont divisés en section qui reprennent chacune leur intitulé technique (entre crochets et en majuscules).

[ENTITE NOTIFIANT L'INCIDENT]	
[A. Field Name: 1-Submission_Type] **S'agit-il d'un signalement d'incident soumis à la loi NIS2?**	Ce champ vous permet d'indiquer si votre notification relève du champ d'application de la loi NIS2 (champ obligatoire)
[B. Field Name : 2-Submitter] **Je suis…**	Ce champ vous permet d'indiquer si vous êtes une entités NIS2 (champ obligatoire)
[CARACTERISTIQUES SPECIFIQUES NIS]	
[C. Field Name: 3-NIS_Type] **Comment l'organisation est-elle définie dans le cadre de la loi NIS2 ?**	Ce champ vous permet d'indiquer si vous êtes une entité importante ou essentiel au sens de la loi NIS2 (champ obligatoire)
[D. Field Name: 4-Sector] **Dans quel(s) secteur(s) votre organisation opère-t-elle ?**	Ce champ vous permet d'indiquer le ou les secteurs dans lesquels vous êtes actifs, il est possible de cocher plusieurs cases (champ obligatoire)
[E. Field Name: 5-NIS_Notification] **Quel type de notification d'incident NIS2 soumettez-vous ?**	Ce champ vous permet d'indiquer à quelle étape de la notification vous vous trouver. Pour rappel, les étapes sont décrites au point A. « Dans quel délai un incident significatif doit-il être notifié ? » (champ obligatoire)
[DETAILS SUR L'INCIDENT]	
[F. Field Name: 6-Malicious_Intent] **Pensez-vous que cet incident soit le résultat d'une intention malveillante**	Ce champ vous permet d'indiquer si l'incident revêt, selon vous, une intention malveillante. Si vous ne le savez pas ou vous n'en êtes pas convaincu, cocher « Incertain » (champ obligatoire)
[G. Field Name: 7-Incident_Type] **Type d'incident**	Ce champ vous permet de choisir parmi une liste de types d'incidents celui ou ceux à qui correspond l'incident que vous souhaitez notifier, il est possible de cocher plusieurs cases (champ obligatoire)
[H. Field Name: 8-Incident_Date] **Quand l'incident a-t-il eu lieu ?**	Ce champ vous permet d'indiquer la date au format Mois/Jour/Année. En cas d'incertitude, le champ suivant (I.) peut être utilisé pour fournir les informations en votre possession relatives au moment où l'incident a eu lieu (champ facultatif)

[I. Field Name: 9-Incident_Description] **Décrire l'incident (cause initiale, impact sur l'organisation, nom du virus ou du logiciel malveillant, données et systèmes affectés, mesures prises, systèmes d'exploitation/logiciels concernés, etc.)**	Ce champ vous permet de fournir les informations en votre possession relatives à l'incident, en ce compris les indicateurs de compromissions. Pour savoir quelles informations indiquer en priorité, veuillez vous référer au point A. « Informations à transmettre lors de la notification d'un incident siginificatif » qui décrit les informations à fournir pour chaque étape de la notification. Veuillez noter que le formulaire comporte des champs spécifiques pour ce qui relève des causes, des conséquences et de la gravité de l'incident. Vous disposez de 500 caractères maximum (champ obligatoire)
[J. Field Name: 9-Assessment_Severity] **Veuillez fournir une évaluation de la gravité de l'incident**	Ce champ vous permet de décrire la gravité de l'incident. Dans le cadre de l'alerte précoce, une telle évaluation peut être très succincte et/ou partielle. Dans le cadre de la notification dans les 72 heures suivant l'incident, vous devez fournir une évaluation initiale de la gravité de l'incident. Dans le cadre du rapport final, cette évaluation doit être détaillée. Vous disposez de 500 caractères maximum (champ obligatoire)
[K. Field Name: 11-Assessment_Consequence] **Quelles sont les conséquences de l'incident ?**	Ce champ vous permet de décrire l'impact de l'incident. Dans le cadre de l'alerte précoce, une telle évaluation peut être très succincte et/ou partielle. Dans le cadre de la notification dans les 72 heures suivant l'incident, vous devez fournir une évaluation initiale de l'impact de l'incident. Dans le cadre du rapport final, cette évaluation doit être détaillée. Veuillez noter que le formulaire comporte des champs spécifiques sur le potentiel impact transfrontière de l'incident. Vous disposez de 500 caractères maximum (champ obligatoire)
[L. Field Name: 12-Threat_Type_Root_Cause] **Quelle est la cause de l'incident ?**	Ce champ vous permet d'indiquer si la cause de l'incident est connue et, le cas échéant, de fournir des informations sur celle-ci. Veuillez noter qu'au stade du rapport final, vous devez indiquer le type de menace ou la cause profonde qui a probablement déclenché l'incident. Vous disposez de 500 caractères maximum (champ obligatoire)
[M. Field Name: 13-Cross_Border_Impact] **Pensez-vous que cet incident pourrait déboucher sur des problèmes transfrontaliers ?**	Ce champ vous permet d'indiquer si l'incident revêt, selon vous, un impact transfrontière. Si vous ne le savez pas ou vous n'en êtes pas convaincu, cocher « Incertain ». Veuillez noter qu'au stade du rapport final, vous devez indiquer, le cas échéant, l'impact transfrontière de l'incident (champ obligatoire)
[N. Field Name: 14-Cross_Border_Impact_Description] **Donner des détails sur les problèmes frontaliers que cet incident pourrait engendrer:**	Ce champ vous permet de fournir des détails sur l'impact transfrontière de l'incident. Veuillez noter que ce champ n'apparaît que si vous avez cocher « Oui » au champ précédent (M.) (champ facultatif)

[O. Field Name: 15-Police_Involved] **Avez-vous signalé l'incident à la police ? (Si vous avez été victime d'une cyberattaque réussie, nous vous conseillons de la signaler à la police)**	Ce champ vous permet d'indiquer si vous avez déjà signaler l'incident à la Police. Il est conseillé de le faire lorsque l'incident revêt un caractère malveillant ou intentionnel (champ facultatif)
[P. Field Name: 16-Help_Needed] **Avez-vous besoin d'un support, d'une investigation ou d'un conseil de la part du CCB?**	Ce champ vous permet, le cas échéant, de demander expressément un soutien de la part du CCB en cochant la case oui. Ce soutien consiste en des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation, voire en un soutien technique supplémentaire (champ obligatoire)
[Q. Field Name: 17-Help_Type_Needed] **Spécifiez le plus précisément possible le soutien dont vous avez besoin de la part du CCB:**	Ce champ vous permet de décrire le type d'aide dont vous auriez besoin dans le cadre de la gestion de l'incident à l'origine de la notification. Ce soutien consiste en des orientations ou des conseils opérationnels sur la mise en œuvre d'éventuelles mesures d'atténuation, voire en un soutien technique supplémentaire. Vous disposez de 500 caractères maximum (champ obligatoire)
[R. Field Name: 18-Actions_Taken] **Quelles mesures avez-vous prises ?**	Ce champ vous permet de décrire les mesures prises pour atténuer et/ou remédier à l'incident. Veuillez noter que ce champ est facultatif mais que, dans le cadre du rapport final, vous devez décrire les mesures d'atténuation appliquées et en cours. Vous disposez de 500 caractères (champ facultatif)
[S. Field Name: 19-Resolved] **L'incident est-il à présent résolu ?**	Ce champ vous permet d'indiquer si l'incident est résolu au moment de la notification concernée (champ obligatoire)
[DONNEES DE CONTACT DE L'ENTITE]	
[T. Field Name: 20-Anonymous]	Ce champ n'est pas visible et indique si la notification est faite de manière anonyme
[U. Field Name: 21-Contact_Person] **Personne de contact**	Ce champ vous permet d'indiquer le nom de la personne de contact dans le cadre de la gestion de l'incident (champ facultatif)
[V. Field Name: 22-Organization] **Nom de l'organisation -BCE**	Ce champ vous permet d'indiquer le nom de l'organisation au nom de laquelle la notification est effectuée (champ obligatoire)
[W. Field Name: 23-Email] **Email**	Ce champ vous permet d'indiquer l'adresse email qui peut être utilisée par le CCB pour prendre contact avec l'organisation victime de l'incident (champ obligatoire)

[X. Field Name: 24-Telephone] **Téléphone**	Ce champ vous permet d'indiquer le numéro de télephone qui peut être utilisé par le CCB pour prendre contact avec l'organisation victime de l'incident (champ obligatoire)
[Y. Field Name: 25-Location] **Où l'incident a-t-il eu lieu ?**	Ce champ vous permet d'indiquer l'endroit où l'incident a eu lieu (champ facultatif)

GUIDE SUR LES NOTIFICATIONS NIS2

Ce document a été élaboré par le Centre pour la Cybersécurité Belgique (CCB). Cette administration fédérale a été créé par l'arrêté royal du 10 octobre 2014 et est sous l'autorité du Premier Ministre.

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.

Éditeur responsable :
Centre pour la Cybersécurité Belgique
M. De Bruycker, Directeur général
Rue de la loi, 18
1000 Bruxelles

Dépot légal:
D/2024/14828/011