CENTRE FOR
CYBERSECURITY
BELGIUM

CHARTE CSIRT NATIONAL

2026

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Date : Janvier 2026
Version : 2.0 français
Auteur : Centre pour la Cybersécurité Belgique (CCB)

Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale de cybersécurité et agit en tant que CSIRT national en Belgique. Le CCB a pour mission de superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en matière de cybersécurité. C'est en optimisant les échanges d'informations que les entreprises, les autorités, les entités NIS2 et la population pourront se protéger de manière adéquate. Le Centre pour la Cybersécurité Belgique (CCB) a été créé par l'arrêté royal du 10 octobre 2014.

Table des matières

Introduction

Le Centre pour la Cybersécurité Belgique (CCB) est l'autorité nationale de cybersécurité en Belgique. Le CCB agit en qualité de Cyber Emergency Response Team (CERT) au niveau national. Le fonctionnement du CSIRT national en tant que service public est fixé dans un cadre légal, complété par des décisions du Conseil des ministres et des documents internes. La présente charte consigne les éléments essentiels issus de ces différentes sources dans un document synoptique unique.

Bien qu'il ne soit pas conseillé de modifier fréquemment une charte, il ne s'agit pas d'un document statique. La charte peut être modifiée au fil des évolutions du contexte juridique ou budgétaire, ou simplement après un examen interne de sa pertinence. En principe, le document fait l'objet d'une évaluation tous les ans.

1. Informations générales

Le Centre pour la Cybersécurité Belgique (CCB) a été créé par l'arrêté royal du 10 octobre 2014.

Dans le cadre de la mise en œuvre[1] de la loi NIS2[2], le CCB a été désigné comme l'autorité nationale de cybersécurité. Dans ce rôle, le CCB supervise, coordonne et veille notamment à la mise en œuvre de la stratégie belge de cybersécurité, ainsi qu'au respect de la loi NIS2 par les entités concernées. C'est en optimisant les échanges d'informations que les entreprises, les autorités, les entités NIS2[3] et la population pourront se protéger de manière adéquate.

Les principales missions du CCB en tant qu'autorité nationale de cybersécurité[4] sont les suivantes :

- superviser, coordonner et veiller à la mise en œuvre de la stratégie belge en la matière ;
- gérer par une approche intégrée et centralisée les différents projets relatifs à la cybersécurité ;
- assurer la coordination entre les services et autorités concernés mais aussi entre autorités publiques et le secteur privé ou le monde scientifique ;
- formuler des propositions pour l'adaptation du cadre réglementaire en matière de cybersécurité ;
- assurer la gestion de crise en cas de cyberincidents, en collaboration avec le Centre de coordination et de crise du gouvernement ;
- élaborer, diffuser et veiller à la mise en œuvre des standards, directives et normes de sécurité pour les différents types de système informatique des administrations et organismes publics ;
- coordonner la représentation belge lors des forums internationaux sur la cybersécurité, le suivi des obligations internationales et la présentation du point de vue national en la matière ;
- coordonner l'évaluation et la certification de la sécurité des systèmes d'information et de communication ;
- informer et sensibiliser les utilisateurs des systèmes d'information et de communication.

En vertu de la loi NIS2, le CCB endosse également le rôle de CSIRT national[5]. Le Cyber Emergency Response Team (CERT) et le Cyber Threat Research & Intelligence Sharing (CyTRIS) team sont les deux services opérationnels qui ensemble, au sein du CCB, constituent le CSIRT national.

Le CERT a pour mission d'analyser, de contenir, d'atténuer et d'éradiquer les cyberattaques en Belgique. Il dispense une expertise et une assistance techniques aux autres services publics. Si certains services sont fournis de manière proactive, la majeure partie du travail du CERT est cependant comparable à celui d'un « cyber-pompier ».

CyTRIS est chargé du premier contact avec les organisations signalant un incident au CCB. Ce service du CCB surveille quotidiennement diverses sources, recueille et rassemble les informations susceptibles d'être utiles pour avertir les victimes potentielles, et procède à des analyses CTI approfondies et à la rédaction de rapports stratégiques. CyTRIS envoie également des « spear warnings » (messages individuels) aux organisations dont l'infrastructure informatique présente une vulnérabilité particulière, qui ont été compromises par des logiciels malveillants ou dont les identifiants de connexion ont été volés. En outre, CyTRIS organise régulièrement des événements en ligne et en présentiel pour informer les parties prenantes quant aux cybermenaces actives et à la manière dont elles peuvent s'en prémunir.

Les principales missions du CCB en tant que CSIRT[6] national sont les suivantes :

- surveiller et analyser les cybermenaces, les vulnérabilités et les incidents au niveau national ;
- activer le mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion

[1] Arrêté royal du 9 juin 2024 exécutant 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, article 3.
[2] 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 (loi NIS2). La loi NIS2 consiste en la transposition au niveau belge de la directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 (la « directive NIS2 »).
[3] Entités essentielles et importantes relevant du champ d'application de la loi NIS2.
[4] Loi NIS2, article 17.
[5] Loi NIS2, articles 15-16.
[6] Loi NIS2, article 19.

d'informations sur les cybermenaces, les vulnérabilités et les incidents auprès des entités essentielles et importantes concernées ainsi qu'auprès des autorités compétentes et des autres parties prenantes concernées, si possible en temps quasi réel ;
- réagir aux incidents et apporter une assistance aux entités essentielles et importantes concernées ;
- rassembler et analyser des données forensiques, et réaliser une analyse dynamique des risques et incidents et une appréciation de la situation en matière de cybersécurité ;
- participer au réseau des CSIRT ;
- agir en qualité de coordinateur aux fins du processus de divulgation coordonnée des vulnérabilités ;
- contribuer au déploiement d'outils sécurisés de partage d'informations ;
- procéder à un scan proactif et non intrusif des réseaux et systèmes d'information accessibles au public ;
- détecter, observer et analyser des problèmes de sécurité informatique ;
- coopérer et, le cas échéant, échanger des informations pertinentes.

Par « cybersécurité », on entend toutes les mesures qui garantissent la confidentialité, la disponibilité et l'intégrité des technologies de l'information et de la communication (« information and communication technology », ICT) : mesures techniques, mais aussi actions de sensibilisation des utilisateurs.

Cependant, la cybersécurité ne couvre pas l'utilisation de l'ICT comme simple moyen d'activisme, de terrorisme, d'espionnage, de subversion ou, plus généralement, dans le cadre d'activités criminelles. Ces actes relèvent de la compétence d'autres services que le CSIRT national (police, sûreté de l'État, etc.). De même, l'identification des auteurs d'infractions n'est pas du ressort du CSIRT national.

Néanmoins, tout risque, toute atteinte à la confidentialité, à l'intégrité et à la disponibilité des systèmes ICT, quelle qu'en soit la raison, constitue un problème de cybersécurité.

2. Public cible

Le public cible est constitué de l'ensemble des parties qui peuvent utiliser les services du CSIRT national. Certains services sont uniquement à la disposition d'une partie du public cible.

Les entreprises ou organisations concernées qui font partie du public cible du CSIRT national n'ont, sauf disposition juridique expresse, aucune obligation envers le CSIRT national ; leur adhésion indique que ce dernier met ses services à leur disposition.

Qui peut faire appel au CSIRT national ?

- Entités essentielles concernées par la loi NIS2.
- Autorités administratives : l'infrastructure ICT des administrations publiques belges.
- Si d'autres entités importantes telles que définies dans la loi NIS2 peuvent également solliciter une assistance, celle-ci sera fournie sur la base du « meilleur effort » et dans une mesure plus limitée.
- Le grand public a uniquement accès à une partie limitée des services du CSIRT national.
- Les personnes morales privées qui ne sont pas visées par NIS2 peuvent utiliser une partie limitée des services du CSIRT national.
- Les ordinateurs, réseaux ou systèmes de communication classifiés au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé sont du ressort de l'Autorité nationale de sécurité (ANS) et, par conséquent, ne font pas partie du champs d'action du CCB et du CSIRT national.

3. Compétence

Le CSIRT national joue un rôle de coordination et de conseil. L'article 21 de la loi NIS2 prévoit que le CSIRT national prend toutes les mesures appropriées pour mener à bien sa mission et respecter ses obligations. Ces mesures devraient être proportionnées à ces objectifs et conformes aux principes d'objectivité, de transparence et de non-discrimination.

Dans ce contexte, et sans préjudice du Code d'instruction criminelle[7], le CSIRT national est autorisé à détenir, à divulguer, à diffuser ou à faire usage de toutes les informations disponibles, même si celles-ci sont issues d'un accès non autorisé à un système informatique par un tiers.

Le CSIRT national accomplit toujours ses missions en usant de la prudence que l'on est en droit d'attendre d'une autorité publique, en veillant toujours en priorité à ne pas perturber le fonctionnement du système informatique, et en prenant toutes les précautions raisonnables afin qu'aucun dommage matériel ne soit causé au système informatique.

[7] Article 28*quinquies*, § 1er, et 57, § 1er.

4. Services

Les services proposés par un CSIRT national varient et dépendent à la fois du public cible et de son autorité sur celui-ci, ainsi que de sa position institutionnelle. Les services d'un CSIRT national sont généralement classés en trois catégories : services proactifs, services réactifs et services de gestion de la qualité de la sécurité. La présente section adopte cette classification et décrit l'offre de services du CSIRT national.

4.1. SERVICES PROACTIFS

Les services proactifs visent à améliorer l'infrastructure et les processus de sécurité du public cible avant qu'un incident ne se produise ou ne soit détecté.

MONITORING ET ANALYSE DES CYBERMENACES, VULNÉRABILITÉS ET INCIDENTS

La mission du CSIRT national est de détecter, de surveiller et d'analyser les cybermenaces, les vulnérabilités et les incidents en ligne au niveau national. Une équipe du CSIRT national contrôle chaque jour le paysage de la menace afin de détecter en temps utile les cybermenaces et les vulnérabilités pertinentes. En outre, le CSIRT national fournit des rapports stratégiques, opérationnels et tactiques sur les CTI afin de permettre une analyse plus approfondie des menaces spécifiques.

PARTAGE DE L'INFORMATION

Le CSIRT national envoie des alertes précoces, des notifications et des annonces concernant les vulnérabilités et les cybermenaces signalées, par l'intermédiaire de son site Internet, des médias sociaux, du Early Warning System (EWS)[8] et, si nécessaire, par contact direct (« Spear Warning »[9]), afin d'alerter les parties prenantes concernées quant aux risques liés aux nouvelles vulnérabilités ou aux nouveaux vecteurs de menaces. En outre, il organise régulièrement des événements en ligne et en présentiel pour informer les groupes cibles quant aux cybermenaces actives et à la manière dont ils peuvent s'en prémunir.

MONITORING DU CYBERDOMAINE

Le CSIRT national suit en permanence les évolutions des tendances, des développements et des solutions technologiques dans le domaine de la cybersécurité et, par extension, de la sécurité de l'information au sens le plus large. Ce suivi fournit des informations aux autres, tout en permettant de rester informé des derniers développements en la matière.

DÉTECTION, OBSERVATION ET ANALYSE DES PROBLÈMES DE SÉCURITÉ

La mission du CSIRT national est de détecter, d'observer et d'analyser les problèmes de sécurité en ligne. Il officie dès lors en tant que point de contact central pour les notifications des incidents de sécurité et les informations sur la cybermenace[10].

ÉVALUATIONS DE LA SÉCURITÉ / TESTS DE PÉNÉTRATION / ATTACK SURFACE MANAGEMENT

Sur demande, le CSIRT national peut, en fonction des ressources disponibles, effectuer une évaluation ou un test de pénétration de l'infrastructure (ou d'une partie de celle-ci) de son public cible, afin de détecter les vulnérabilités susceptibles d'avoir des conséquences significatives. En outre, il peut évaluer les risques de manière proactive du point de vue d'un assaillant, en détectant les vulnérabilités liées à Internet et en limitant ainsi le nombre de points d'accès possibles des groupes cibles au réseau. Le CSIRT national peut être amené à collaborer avec des tiers

[8] Voir https://ccb.belgium.be/fr/cytris/early-warning-system.
[9] Voir https://ccb.belgium.be/fr/cytris/faq-on-spear-warnings.
[10] Voir https://ccb.belgium.be/fr/cert/signaler-un-incident.

(externes) afin de fournir ce service.

DIFFUSION D'INFORMATIONS SUR LA CYBERSÉCURITÉ

Le CSIRT national publie, si nécessaire, des documents d'information ou des liens vers ces documents, qui peuvent présenter un intérêt pour le public cible[11].

DÉTECTION ET MISE EN GARDE CONTRE LES SYSTÈMES VULNÉRABLES OU NON SÉCURISÉS

Si cette intervention n'a aucune incidence négative sur le fonctionnement des services des entités, le CSIRT national peut effectuer une analyse proactive et non intrusive des réseaux et systèmes d'information accessibles au public, afin de détecter les réseaux et systèmes d'information vulnérables ou configurés de manière peu sûre, et d'en informer les entités concernées.

4.2. SERVICES RÉACTIFS

Les services réactifs visent à répondre aux appels à l'aide, aux notifications et, d'une manière générale, à toute menace ou attaque contre les systèmes du public cible du CSIRT national.

TRAITEMENT DES INCIDENTS

- Premier contact et enregistrement en cas d'incidents (NIS2)

Traitement des notifications (d'incident) par téléphone et par mail, et éventuellement première prise de contact.

- Analyse des incidents

À la demande du public cible, le CSIRT national effectue l'analyse post mortem d'un incident de cybersécurité. Cette analyse a pour but de déterminer l'ampleur de l'incident et des dommages causés, sa cause principale et, le cas échéant, de formuler des recommandations.

- Gestion des incidents sur site

À la demande de certains membres de son public cible, le CSIRT national enverra des spécialistes pour aider les équipes locales à gérer un incident spécifique.

- Soutien à la gestion des incidents

Le CSIRT national apporte aux membres de son public cible son soutien dans le traitement des incidents de sécurité. Ce soutien prend la forme de conseils par mail ou par téléphone, d'aide à l'analyse de données forensiques, etc.

- Coordination des incidents

Le CSIRT national coordonne, en collaboration avec les acteurs concernés, la réponse aux incidents. En cas d'incidents graves, le plan d'urgence national cyber peut être activé.

GESTION DES VULNÉRABILITÉS - COORDINATION DES RÉPONSES

Lorsqu'une vulnérabilité est détectée sur un logiciel, le CSIRT national peut, sur demande, coordonner les efforts d'atténuation et de communication entre les différentes parties concernées (chercheur, revendeur de logiciels,

[11] Voir https://ccb.belgium.be/fr/advisories.

utilisateurs, etc.)[12]. Le CSIRT national peut être amené à coopérer avec des tiers pour fournir ce service.

ANALYSE D'ARTEFACT

Un artefact consiste en une trace d'intrusion ou tentative d'intrusion sur un système ICT. À titre d'exemples (non exhaustifs) d'artefacts, l'on peut citer les fichiers, les logs, les systèmes d'information. Le CSIRT national peut analyser les artefacts signalés. Le CSIRT peut être amené à coopérer avec des tiers pour fournir ce service.

4.3. SERVICES DE GESTION DE LA QUALITÉ EN MATIÈRE DE SÉCURITÉ

Ces services s'appuient sur les résultats et les enseignements tirés de la pratique des différents services réactifs.

SENSIBILISATION

Le CSIRT national participe aux campagnes de sensibilisation du CCB. En outre, il organise régulièrement des événements en ligne et en présentiel pour informer les groupes cibles quant aux cybermenaces actives et à la manière dont ils peuvent s'en prémunir.

FORMATION

Le CSIRT national a la possibilité de développer des formations dans les domaines relevant de ses compétences, et d'organiser des séances de formation. Le CSIRT national peut être amené à coopérer avec des tiers pour fournir ce service.

[12] Voir https://ccb.belgium.be/fr/reglementation/cvdp.

4.4. SERVICES NON FOURNIS PAR LE CSIRT NATIONAL

Services proactifs :

- Analyses générales des risques et modélisation
- Planification de la continuité des activités (BCP/DRP) et conseils en sécurité
- Évaluation ou certification de produits de sécurité

Services réactifs :

- Gestion des vulnérabilités - correction des vulnérabilités (« patchs »)
- Sécurité opérationnelle
- Reconstruction en cas de cyberattaque

5. Disponibilité du service

Le CSIRT national est disponible par mail ou par téléphone[13] pendant les heures de bureau (de 9h30 à 16h30), du lundi au vendredi, en dehors des jours de fermeture officiels.

Les mails envoyés au CSIRT national font l'objet d'un accusé de réception automatique en quelques minutes. Ce système automatique attribue un numéro unique à chaque notification. Il n'est pas garanti que le CSIRT puisse répondre systématiquement au mail ; cela dépendra de la gravité de l'incident et de la fonction du correspondant.

En collaboration avec le Centre de crise national (NCCN) du ministère de l'Intérieur, le CSIRT national est joignable par téléphone 24h/24 pour traiter les incidents graves qui touchent les entités essentielles NIS2.

[13] Pour les coordonnées, voir le paragraphe 6.

6. La politique du CSIRT national en résumé

6.1. TYPES D'INCIDENTS ET NIVEAU D'ASSISTANCE

Le CSIRT national traite tout incident lié à un réseau ou système d'information survenant sur le territoire belge, ou à tout domaine Internet qui finit par « .be ». Le niveau d'assistance dépend de la gravité de l'incident et de la fonction du correspondant.

L'ordre de priorité du public cible est le suivant :

1. entités essentielles concernées par la loi NIS2 ;
2. autorités administratives : l'infrastructure ICT des administrations publiques belges ;
3. les autres entités importantes telles que définies dans la loi NIS2 peuvent également solliciter une assistance, celle-ci sera fournie sur la base du « meilleur effort » et dans une mesure plus limitée ;
4. le grand public a uniquement accès à une partie limitée des services du CSIRT national. Les personnes morales privées qui ne sont pas visées par NIS2 peuvent utiliser une partie limitée des services du CSIRT national.

Les ordinateurs, réseaux ou systèmes de communication classifiés au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé sont du ressort de l'Autorité nationale de sécurité (ANS) et, par conséquent, ne font pas partie du champ d'action du CCB et du CSIRT national.

6.2. COOPÉRATION, INTERACTION ET DIFFUSION DES INFORMATIONS

Le CSIRT national traite les informations qui lui sont transmises, conformément à la législation belge en vigueur. Le CSIRT national veille donc de près à la protection des données à caractère personnel et des informations sensibles qu'il reçoit.

Comme spécifié dans le plan d'urgence national cyber[14], le CSIRT national coordonne les activités des différentes parties prenantes en cas d'incident national de cybersécurité. En cas de crise nationale de cybersécurité, le CSIRT national travaille en collaboration avec le Centre de crise national (NCCN) pour coordonner les activités des différentes parties prenantes[15].

S'il s'avère nécessaire de communiquer des données à caractère personnel pour traiter un incident, le CSIRT national veillera à seulement transmettre le minimum d'informations requis.

Les informations transmises par mail sous forme chiffrée seront uniquement stockées sous cette forme et ne seront déchiffrées que lorsque cela s'avère nécessaire à la résolution d'un incident. Si un transfert de ces données est requis, il sera également effectué sous forme chiffrée.

Le CSIRT national utilise et respecte le Traffic Light Protocol 2.0 tel que décrit par FIRST[16].

Dans la mesure du possible, le CSIRT national partagera son expérience avec ses pairs et son public cible, à condition que cela ne soit pas contraire aux dispositions reprises ci-dessus. Une attention particulière sera portée aux points suivants : EGC6, TF-CSIRT7, FIRST8 et le EU CSIRTs Network.

Seules les personnes spécifiquement désignées par le CCB pourront contacter la presse.

---

[14] Le plan national d'incidents de cybersécurité et de réaction à une cybercrise (ou plan d'urgence national cyber) ; plan national au sens de l'article 9, § 2, de la loi du 15 mai 2007 relative à la sécurité civile. Ce plan a été élaboré par le CCB, en collaboration avec le NCCN. Le plan d'urgence national cyber n'est pas un document public. Voir aussi l'article 29 de la loi INS2.
[15] Article 18 de la loi NIS2.
[16] https://www.first.org/tlp/.

6.3 COMMUNICATION ET AUTHENTIFICATION

Le CSIRT national est disponible par mail via info@ccb.belgium.be. Le CSIRT national est également joignable par téléphone au +32 (0)2 501 05 60, uniquement en cas d'urgence liée à un incident. Le CSIRT national est joignable pendant les heures de bureau (de 9h30 à 16h30) du lundi au vendredi, hors jours de fermeture officiels.

Pour le traitement des incidents graves concernant les entités essentielles NIS2, le CSIRT national est joignable 24h/24 par téléphone, en collaboration avec le Centre de crise national (NCCN) du ministère de l'Intérieur.

Pour une communication sécurisée et discrète, il est possible d'utiliser le chiffrement PGP. Des informations à jour sur les adresses mail à disposition et leurs clés PGP associées sont disponibles à l'adresse suivante : https://ccb.belgium.be/fr/cert/envoyer-un-message-crypte.

Le personnel du CSIRT national est habilité à traiter des informations classifiées au sens de la loi du 11 décembre 1998 relative à la classification, aux habilitations de sécurité, aux avis de sécurité et au service public réglementé.