CENTRE FOR
CYBER SECURITY
BELGIUM

Charte CSIRT national

CHANCELLERY OF
THE PRIME MINISTER

.be

CENTRE POUR
CYBER SÉCURITÉ BELGIQUE

01

Introduction

À propos du présent document

En tant que service public, l'existence du CSIRT national est définie par un ensemble de textes officiels – arrêtés royaux, décisions du Conseil des ministres, etc. – et de documents internes. La présente Charte reprend les éléments pertinents de ces diverses sources et les compile dans un document unique.

S'il n'est pas jugé souhaitable de modifier régulièrement une telle Charte, il ne s'agit pas non plus d'un document coulé dans le marbre. La présente Charte peut être modifiée en fonction du contexte juridique ou budgétaire, ou simplement après un examen interne de sa pertinence. Elle devrait être soumise à une révision au moins tous les deux ans.

02

Mission

Arrêté royal du 10 octobre 2014

L'arrêté royal du 10 octobre 2014 a établi la création du Centre pour la Cybersécurité Belgique (CCB). Le CCB est placé sous l'autorité du Premier ministre.

Le Centre pour la Cybersécurité Belgique est l'autorité nationale en charge de la cybersécurité en Belgique. Le CCB a repris et intégré en ses rangs la Computer Emergency Response Team (CERT) dans le but de mener des activités de détection, d'observation et d'analyse des problèmes de sécurité en ligne ainsi que de fournir aux utilisateurs des informations continues à ce sujet.
Les principales missions du CCB décrites dans l'arrêté royal sont les suivantes :

- Suivre, coordonner et superviser la mise en œuvre de la politique belge en la matière ;
- Gérer les différents projets sur le thème de la cybersécurité en utilisant une approche intégrée et centralisée ;
- Assurer la coordination entre les ministères et les gouvernements concernés, ainsi qu'entre les autorités publiques et les secteurs privés ou scientifiques ;
- Formuler des propositions visant à adapter le cadre réglementaire dans le domaine de la cybersécurité ;
- Assurer la gestion des crises en cas de cyberincidents en coopération avec le Centre de coordination et de crise du gouvernement ;
- Préparer, diffuser et superviser la mise en œuvre de normes, de lignes directrices et de standards de sécurité pour les différents systèmes d'information des gouvernements et des institutions publiques ;
- Coordonner la représentation belge dans les forums internationaux sur la cybersécurité, coordonner le suivi des engagements internationaux et des propositions nationales en la matière ;
- Coordonner l'évaluation de la sécurité et la certification des systèmes d'information et de communication ;
- Informer et sensibiliser les utilisateurs sur les systèmes d'information et de communication.

LOI NIS

L'article 3 de 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 (loi NIS) dispose que le Centre pour la Cybersécurité Belgique est désigné comme CSIRT national, au sens de la loi NIS.

L'article 60 de la loi NIS définit les tâches du CSIRT national comme étant au moins les suivantes :

1. le suivi des incidents au niveau national et international, en ce compris le traitement de données à caractère personnel lié au suivi de ces incidents ;
2. l'activation du mécanisme d'alerte précoce, la diffusion de messages d'alerte, les annonces et la diffusion d'informations sur les risques et incidents auprès des parties intéressées ;
3. l'intervention en cas d'incident ;
4. l'analyse dynamique des risques et incidents et conscience situationnelle ;
5. la détection, l'observation et l'analyse des problèmes de sécurité informatique ;
6. la promotion de l'adoption et de l'utilisation de pratiques communes ou normalisées pour les procédures de gestion des risques et incidents, ainsi que des systèmes de classification des incidents, risques et informations ;
7. l'établissement de relations de coopération avec le secteur privé, d'autres services administratifs ou autorités publiques ;
8. la participation au réseau des CSIRT visé à l'article 12 de la directive NIS.

La cybersécurité désigne l'ensemble des mesures qui assurent la confidentialité, la disponibilité et l'intégrité des technologies de l'information et de la communication (TIC, « ICT » en anglais) : non seulement les mesures techniques, mais aussi les mesures de sensibilisation des utilisateurs.

La cybersécurité ne concerne pas uniquement l'utilisation des ICT comme moyen d'activisme, de terrorisme, d'espionnage, de subversion ou, de manière générale, de criminalité. Ces actes relèvent de la responsabilité d'autres services que le CSIRT national (police, Sûreté de l'État, etc.). De plus, l'identification des auteurs de crimes n'est pas du ressort du CSIRT national.

Cependant, tout risque planant sur la confidentialité, l'intégrité et la disponibilité des systèmes ICT, pour quelque raison que ce soit, constitue un problème de cybersécurité.

03

Public cible

Le public cible est l'ensemble des parties qui peuvent faire appel aux services du CSIRT national. Certains services ne sont disponibles que pour une partie du public cible.

L'appartenance au public cible du CSIRT national n'engage en rien les entreprises ou organisations ciblées envers le CSIRT national ; elle indique au contraire la volonté du CSIRT national d'être au service de ces entreprises ou organisations.

Opérateurs de services essentiels et d'infrastructures critiques

Une partie importante du public cible du CSIRT national est constituée d'opérateurs d'infrastructures critiques et de services essentiels. Les opérateurs d'infrastructures critiques sont ceux identifiés par la loi du 1er janvier 2011 relative à la sécurité et à la protection des infrastructures critiques.
Les opérateurs de services essentiels sont les entreprises et les services publics qui font partie des secteurs concernés par la directive NIS et qui sont identifiés comme tels par les autorités sectorielles compétentes :

1. Énergie
    a. Électricité
    b. Pétrole
    c. Gaz
2. Transports
    a. Transport aérien
    b. Transport ferroviaire
    c. Navigation intérieure
    d. Transport par route
3. Banques
4. Infrastructures des marchés financiers
5. Secteur de la santé
6. Approvisionnement et distribution d'eau potable
7. Infrastructures numériques

Services publics

Les services publics essentiels à la population belge mais non couverts par la directive NIS ne sont pas définis par des règlements, mais par des critères internes au CCB.

Autorités administratives

L'infrastructure ICT des services publics belges est essentielle au bon fonctionnement du pays, ce qui en fait une partie intégrante du public cible du CSIRT national.

Personnes morales de droit privé

Les personnes morales de droit privé qui ne proposent pas de services essentiels peuvent faire appel à un sous-ensemble limité des services du CSIRT national.

Grand public

Le grand public en tant que tel n'a accès qu'à un sous-ensemble limité des services du CSIRT national (voir plus bas).

Systèmes d'information classifiés

Les ordinateurs, réseaux ou systèmes de communication qui sont classifiés au sens de la loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité sont placés sous la tutelle de l'Autorité nationale de Sécurité (ANS) et ne font dès lors pas partie du champ d'action du CCB ou du CSIRT national.

04

Affiliation

Le Centre pour la Cybersécurité Belgique (CCB) est un service administratif placé sous l'autorité du Premier ministre.

05

Autorité

L'autorité est la capacité pour le CSIRT national de contraindre tout ou partie de son public cible à appliquer telle ou telle mesure de sécurité afin de prévenir une menace à la cybersécurité ou de résoudre un incident de cybersécurité.
L'article 62 de la loi NIS dispose que le CSIRT national prend toutes les mesures adéquates afin de réaliser sa mission et ses objectifs. Dans ce cadre, le CSIRT national est autorisé à détenir, à divulguer à une autre personne, 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.

06

Services

Les services proposés par un CSIRT 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 sont généralement classés en trois catégories : services réactifs, services proactifs et services de gestion de la qualité de la sécurité. L'Agence européenne pour la sécurité des réseaux et de l'information (ENISA, « European Union Agency for Cybersecurity ») utilise également ces catégories dans sa liste des services potentiellement

proposés par les CSIRT. Cette liste est longue et chaque CSIRT doit faire sa propre sélection en fonction de sa mission et de ses ressources.
La présente section adopte cette classification et décrit l'offre de services du CSIRT national.

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.

Alertes et avertissements

Ce service consiste à publier des informations décrivant une attaque, une alerte, une menace, etc. et à fournir des recommandations d'actions à court terme qui permettent de faire face au problème.

Traitement des incidents

Analyse des incidents

À la demande d'un membre de son public cible, le CSIRT national effectuera une analyse *post-mortem d'*un incident de cybersécurité. L'objectif de cette analyse sera d'identifier l'étendue de l'incident et les dommages causés, sa cause première et éventuellement de formuler des recommandations.

Traitement des incidents sur site

À la demande de certains membres de son public cible, le CSIRT national enverra des spécialistes afin d'aider les équipes locales à traiter 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 e-mail ou par téléphone, d'aide à l'analyse des données, etc.

Coordination du traitement des incidents

Le CSIRT national coordonne, en relation avec les partenaires concernés, le traitement des incidents. En cas d'incident grave, le plan d'urgence cyber peut être activé.

Traitement des vulnérabilités – coordination des réponses

Lorsqu'une vulnérabilité est découverte dans 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, utilisateurs, etc.). Le CSIRT national peut être amené à collaborer avec des tiers externes afin de fournir ce service.

Analyse d'artefacts

Un artefact est une trace d'intrusion ou de tentative d'intrusion sur un système ICT. Les fichiers journaux et les informations sur les systèmes sont des exemples d'artefacts.
Le CSIRT national peut analyser les artefacts soumis par certaines catégories de son public cible. Le CSIRT national peut être amené à collaborer avec des tiers externes afin de fournir ce service.

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.

Annonces

Le CSIRT national diffuse des annonces au moyen de son site Internet et, si nécessaire, il utilise des canaux privés, afin de prévenir son public cible des risques liés aux nouvelles vulnérabilités découvertes ou à l'existence de nouveaux vecteurs de menace.

Veille technologique

Le CSIRT national effectue une veille technologique continue dans le domaine de la cybersécurité et de la sécurité de l'information au sens large. Cette veille alimente les autres services du CSIRT national et lui permet de se tenir informé des dernières évolutions dans le domaine.

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[1]. Il officie dès lors en quant que point de contact central pour les notifications des incidents de sécurité et les informations sur la cybermenace.

Évaluations de sécurité / Tests de pénétration

Sur demande, le CSIRT national peut, en fonction de les ressources disponibles, effectuer une évaluation ou un test de pénétration de l'infrastructure (ou d'une partie de celle-ci) de son public cible. Le CSIRT national peut être amené à collaborer avec des tiers 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 être intéressants pour son public cible.

Services de gestion de la qualité de la sécurité

Ces services visent à utiliser les résultats et les enseignements tirés de la pratique des différents services réactifs.

Sensibilisation

Le CSIRT national participe aux campagnes de sensibilisation du CCB.

Formation

Le CSIRT national a la possibilité de développer des formations sur ses compétences, et d'organiser des sessions de formation.

[1] Arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique, *M.B.,* 21 novembre 2014, p. 91395.

Services non fournis par le CSIRT national

Services réactifs :

- Traitement des vulnérabilités – correction des vulnérabilités
- Sécurité opérationnelle

Services proactifs :

- Configuration et maintenance des outils de sécurité
- Développement d'outils de sécurité
- Gestion de la qualité de la sécurité :
  - Analyse générale des risques et modélisation
  - Planification de la continuité des activités (BCP/DRP) et
  - Conseils en sécurité
  - Évaluation ou certification de produits de sécurité

Offre de services en fonction du public cible

Services réactifs

	Opérateurs de services essentiels et d'infrastructures critiques	Opérateurs de services publics essentiels	Autorités administratives	Personnes morales de droit privé	Grand public
Alertes et avertissements	Oui[2]	Oui[2]	Oui[2]	Oui[2]	Oui
Analyse des incidents	Oui[3]	Oui[3]	Oui[2]	-	-
Traitement des incidents sur site	Oui[3]	Oui[2]	-	-	-
Soutien à la gestion des incidents	Oui[3]	Oui[3]	Oui[2]	Oui[2]	-
Coordination du traitement des incidents	Oui[3]	Oui[2]	Oui[2]	Oui[2]	-
Coordination du traitement des vulnérabilités[4]	Oui[2]	Oui[2]	Oui[2]	Oui[2]	-

[2] Pendant les heures de bureau
[3] 24/7, en coopération avec le Centre de crise
[4] Potentiellement avec le soutien de tiers

	Opérateurs de services essentiels et d'infrastructures critiques	Opérateurs de services publics essentiels	Autorités administratives	Personnes morales de droit privé	Grand public
Analyse des artefacts[4]	Oui[3]	Oui[3]	-	-	-

Services proactifs

	Opérateurs de services essentiels et d'infrastructures critiques	Opérateurs de services publics essentiels	Autorités administratives	Personnes morales de droit privé	Grand public
Annonces	Oui[2]	Oui[2]	Oui[2]	Oui[2]	Oui
Veille technologique	Oui[2]	Oui[2]	Oui[2]	Oui[2]	Oui
Détection, observation et analyse des problèmes de sécurité	Oui[2]	Oui[2]	Oui[2]	Oui[2]	Oui
Évaluations de sécurité / Tests de pénétration4	Oui[2]	Oui[4]	-	-	-
Diffusion d'informations	Oui[2]	Oui[2]	Oui[2]	Oui[2]	Oui

Services de gestion de la qualité de la sécurité

	Opérateurs de services essentiels et d'infrastructures critiques	Opérateurs de services publics essentiels	Autorités administratives	Personnes morales de droit privé	Grand public
Sensibilisation	Oui[2]	Oui[2]	Oui[2]	Oui[2]	Oui
Formations	Oui[2]	Oui[2]	Oui[2]	-	-

07

Niveau de service

Le CSIRT national peut être contacté pendant les heures de travail (de 9h00 à 17h00) par e-mail (cert@cert.be). Les e-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 signalement. La réponse par e-mail d'un opérateur n'est pas garantie et dépend de la gravité de l'incident et du statut du correspondant.

En collaboration avec le Centre de crise du SPF Intérieur, le CSIRT national peut être contacté par téléphone 24 heures sur 24 et 7 jours sur 7 pour gérer des incidents pour les opérateurs de services essentiels et d'infrastructures critiques.

08

Résumé des *policies*

Types d'incidents et niveau de soutien

Le CSIRT national traite tout incident lié à un système d'information ou de réseau situé sur le territoire belge, ou à tout domaine internet en « .be ». Le niveau de soutien dépend de la gravité de l'incident et du statut du correspondant.
L'ordre de priorité au sein du public cible est le suivant :

1. Opérateurs de services essentiels et d'infrastructures critiques ;
   Opérateurs de services publics essentiels ;
2. Autorités administratives ;
3. Entreprises ;
4. Grand public.

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 à la protection des données personnelles et des informations sensibles qu'il reçoit.
Comme spécifié dans le plan d'urgence cyber, 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 afin de coordonner les activités des différentes parties prenantes.
Lorsqu'il est nécessaire de communiquer des données personnelles pour traiter un incident, le CSIRT national veillera à n'envoyer que le minimum d'informations requis.
Les informations envoyées par e-mail et cryptées avec la clé PGP du CSIRT national ne seront stockées que de manière cryptée et ne seront déchiffrées que lorsque cela s'avèrera indispensable. Si un transfert de ces informations est indiqué, ce transfert sera également crypté avec la clé PGP.
Le CSIRT national utilise et respecte le Traffic Light Protocol tel que décrit par FIRST (version 1.0)[5].
Dans la mesure du possible, le CSIRT national partagera son expérience avec ses pairs et son public cible, à condition que cela ne contrevienne pas aux dispositions précitées. Une attention particulière sera accordée aux groupes suivants : EGC[6] , TF-CSIRT[7] , FIRST[8] et le EU CSIRTs Network.
Seules les personnes spécifiquement désignées par le CCB pourront avoir des contacts avec la presse.

Communication et authentification

Le CSIRT national est disponible par e-mail à l'adresse cert@cert.be. Une clé PGP est associée à cette adresse :

```
pub   rsa4096 2021-11-03 [SC] [expires: 2023-01-31]
      100049EF4B8A2266475F867C7E2A6E16BCDAA13E
uid           [  full  ] CERT.be 2022 <cert@cert.be>
sub   rsa4096 2021-11-03 [E] [expires: 2023-01-31]
```

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 et aux habilitations, attestations et avis de sécurité[9].

[5] Forum of Incident Response and Security Teams (FIRST), «Traffic Light Protocol (TLP) - FIRST Standards Definitions and Usage Guidance — Version 1.0,» 16 08 2016, www.first.org/tlp/.
[6] « European Governmental CERTs »
[7] « Task Force – Cooperation of Computer Security Incident Response Teams »
[8] « Forum of Incident Response Teams »
[9] Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité, *M.B.,* 7 mai 1999*,* p. 15752.

Charte CSIRT National

CENTRE POUR
CYBER SÉCURITÉ BELGIQUE
Rue de la Loi, 16 - Bruxelles

T. : +32 2 501 05 63
info@ccb.belgium.be
www.ccb.belgium.be

CHANCELLERY OF
THE PRIME MINISTER

.be