CERT.be

CENTRE FOR CYBER SECURITY BELGIUM

# Charte CERT.be

## Description des Services

TLP: [WHITE]

The Federal Cyber Emergency Team

# Table des Matières

| Document information | |
|---|---|
| **Titre de la politique** | Charte de CERT.be |
| **Date d'approbation** | |
| **Autorité d'approbation** | Premier ministre |
| **Version** | 1.2 fr |
| **Remplace** | |
| **Date de prochaine révision** | 01/01/2019 |
| **Régulations apparentées** | |
| **Politiques apparentées** | |
| **Procédures apparentées** | |
| **Propriétaire de la politique** | Directeur CERT.be |

# 1 INTRODUCTION

La Charte d'un CERT est un document dont le format est codifié, et est la version publique des documents fondateurs de CERT.be. En tant que service public, l'existence de CERT.be est régie par un ensemble de documents officiels – Arrêtés Royaux, décisions du Conseil des Ministres, etc. – et internes. La présente Charte reprend les éléments nécessaires de ces documents disparates et les compile en un seul document destiné aux pairs de CERT.be et à tous ceux qui pourraient vouloir faire usage de ses services.

S'il n'est pas indiqué de changer une Charte comme celle-ci souvent, elle n'est cependant pas un document figé. La présente Charte peut être modifiée en fonction du contexte législatif, budgétaire, ou simplement régulièrement après examen interne de sa pertinence. Au minimum, elle doit être revue tous les deux ans.

# 2 MISSION

L'article 17 de l'arrêté royal du 10 octobre 2014 portant création du Centre pour la Cybersécurité Belgique (CCB)[1] précise que le CCB reprend la gestion du service Computer Emergency Response Team (CERT) crée au sein de l'ancien Service public fédéral Technologie de l'Information et de Communication (FEDICT).

Cette disposition précise que les missions de ce service sont : « […] de détecter, observer et analyser les problèmes de sécurité en ligne ainsi que d'informer en permanence les utilisateurs à ce sujet ».

Par application de cette disposition, l'ancien service CERT de FEDICT est intégré au sein du CCB et le CCB reprend dès lors toutes ses missions ci-avant décrites.

En qualité de service administratif du CCB, le CERT participe à l'exercice des autres missions légales du CCB.

La cyber sécurité réfère à toutes les mesures permettant d'assurer la confidentialité, la disponibilité et l'intégrité des Technologies d'Informations et de Communication (TICs) : mesures de sécurité techniques, mais également mesures de conscientisation des utilisateurs.

La cyber sécurité ne concerne pas l'utilisation de TICs uniquement comme outils à des fins d'activisme, de terrorisme, d'espionnage, de subversion, ou criminelles. Ces faits sont de la responsabilité d'autres services que CERT.be (police, sûreté de l'Etat, etc.). De même, l'identification d'auteurs de délits n'est pas du ressort de CERT.be. Par contre, toute atteinte à la confidentialité, l'intégrité et la disponibilité de systèmes TIC, quelle que soit la finalité de l'acte, est également un problème de cyber sécurité.

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

# 3 PUBLIC CIBLE

## AKA CONSTITUENCY

Le public cible – constituency en Anglais – est la définition de l'ensemble des parties pouvant faire appel aux services de CERT.be. Certains services ne sont accessibles que pour une partie du Public Cible.

Le fait de faire partie du public cible de CERT.be n'implique aucune obligation des sociétés ou organisations ciblées envers CERT.be, mais dénote la volonté de CERT.be de se mettre au service de ces sociétés ou organisations.

### 3.1 Operateurs de Services Essentiels et Infrastructures Critiques

La cible la plus prioritaire pour CERT.be est constituée des opérateurs d'infrastructures critiques et de services essentiels. Les opérateurs d'infrastructures critiques sont ceux visés par la Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques[2].

Les opérateurs de services essentiels sont les sociétés et services publics faisant partie des secteurs visés par la Directive NIS[3] [3] et identifiés comme tels par les autorités sectorielles compétentes :

1. Energie
    a. Electricité
    b. Pétrole
    c. Gaz
2. Transports
    a. Transport aérien
    b. Transport ferroviaire

[2] Loi du 1er juillet 2011 relative à la sécurité et la protection des infrastructures critiques,» *M.B.,15 juillet 2011*, p. 42320.
[3] 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,» *Journal Officiel de l'Union Européenne,19 juillet 2016.*

c. Transport par voie d'eau

d. Transport routier

3. Banques
4. Infrastructures de marchés financiers
5. Secteur de la santé
6. Fourniture et distribution d'eau potable
7. Infrastructures numériques

## 3.2 Opérateurs de services publics essentiels

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

## 3.3 Autorités administratives

L'infrastructure TIC des services publics belges est essentielle au bon fonctionnement du pays, et cette importance en fait une partie du public cible de CERT.be.

## 3.4 Personnes morales de droit privé

Les personnes morales de droit privé n'opérant pas des services essentiels peuvent faire appel à un nombre restreint de services de CERT.be.

## 3.5 Grand public

Le grand public n'a pas accès à toute l'étendue des services de CERT.be (voir section 6.5).

## 3.6 Systèmes classifiés

Les ordinateurs, réseaux ou systèmes de communication classifiés au sens de la Loi du 11 décembre 1998[4] relative à la classification et aux habilitations, attestations et avis de sécurité sont du ressort de l'Autorité Nationale de Sécurité (ANS) et par conséquent hors du champs d'action du CCB et de CERT.be.

[4] Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité,» *M.B.*, 7 mai 1999, p. 15752.

# 4 AFFILIATION

CERT.be est un service administratif du Centre pour la Cybersécurité Belgique (CCB), sous l'autorité du Premier Ministre.

# 5 COMPETENCE

La compétence est la capacité pour CERT.be d'imposer à tout ou partie de son public cible de prendre telle ou telle mesure de sécurité pour prévenir ou résoudre un incident de cyber sécurité.

CERT.be n'a de compétence que celle qui lui serait attribuée par la transposition en droit belge de la Directive NIS[5].

[5] 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,» *Journal Officiel de l'Union Européenne,19 juillet 2016.*

# 6 SERVICES

Les services fournis par un CERT peuvent être variés, et dépendent à la fois de son public cible et de son autorité sur ce dernier, et de sa position institutionnelle. On classe généralement les services d'un CERT en trois catégories[6] : 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) utilise également ces catégories dans leur liste de services qu'un CERT peut offrir[7]. Cette liste est étendue, et chaque CERT doit sélectionner les services qu'il compte rendre en fonction de sa mission et de ses ressources.

Cette section reprend cette classification, et décrit la sélection de services offerts par CERT.be.

## 6.1 Services réactifs

Les services réactifs visent à répondre à des demandes d'assistance, à des signalements, et généralement à toute menace ou attaque contre les systèmes du public cible du CERT.

### 6.1.1 Alertes et avertissements

Ce service consiste à la publication d'information décrivant une attaque, une alerte, une menace, etc., et à la fourniture de recommandations d'actions à court terme permettant de faire face au problème.

### 6.1.2 Gestion d'incident

#### 6.1.2.1 Analyse d'incident

A la demande d'un membre de son public cible, CERT.be effectuera l'analyse *a posteriori* d'un incident de sécurité. Le but de cette analyse sera l'identification de l'étendue de l'incident et des dommages causés, la cause de l'incident, et éventuellement des recommandations.

#### 6.1.2.2 Gestion d'incident sur site

A la demande de certaines catégories de son public cible, CERT.be dépêchera des spécialistes afin d'aider les équipes locales à gérer un incident de sécurité.

#### 6.1.2.3 Support à la gestion d'incident

[6] M. J. West-Brown, D. Stikvoort, K.-P. Kossakowski, G. Killcrece, R. Ruefle et M. Zajicek, «Handbook for Computer Security Incident Response Teams (CSIRTs),» Carnegie Mellon University, Pittsburgh, PA, 2003.
[7] ENISA, «CSIRT Services,» 27 04 2016, www.enisa.europa.eu/topics/csirt-cert-services [Accès le 11 07 2017].

CERT.be propose à son public cible une assistance à la gestion d'incidents de sécurité. Cette assistance prend la forme de conseils par mail ou par téléphone, d'aide à l'analyse de données, etc.

#### 6.1.2.4 Coordination de la gestion d'incidents

CERT.be coordonne, en relation avec les acteurs concernés, la réponse à des incidents. En cas d'incident grave, le Plan d'Urgence Cyber peut être activé.

### 6.1.3 Gestion de vulnérabilité – Coordination de la réponse

Lors de la découverte d'une vulnérabilité dans un logiciel, CERT.be peut, à la demande, coordonner les efforts de mitigation et de communication entre les différentes parties impliquées (chercheur, éditeur de logiciel, utilisateurs, etc.). Il est possible que CERT.be doive travailler avec des tiers afin de fournir ce service.

### 6.1.4 Analyse d'artefact

Un artefact est le résidu d'une intrusion ou tentative d'intrusion sur un système TIC. Des fichiers, des logs, des informations systèmes sont des exemples (non limitatifs) d'artefacts.

CERT.be a la possibilité d'analyser des artefacts soumis par certaines catégories de son public cible. CERT.be se réserve le droit de faire appel à des tiers pour offrir ce service.

## 6.2 Services proactifs

Les services proactifs ont pour objectif d'améliorer l'infrastructure et les processus de sécurité du public cible avant qu'un incident se produise ou soit détecté.

### 6.2.1 Annonces

CERT.be fournit des annonces via son site web et si nécessaire des canaux privés afin de prévenir son public cible de risques suites à des vulnérabilités ou l'existence de nouveaux vecteurs d'attaques.

### 6.2.2 Veille technologique

CERT.be effectue une veille technologique constante dans les domaines de la sécurité informatique et de l'information au sens large. Cette veille nourrit les différents autres services et permet à CERT.be de rester au courant des dernières évolutions en la matière.

### 6.2.3 Détection, observation et analyse de problèmes de sécurité

CERT.be a pour mission de détecter, observer et analyser les problèmes de sécurité en ligne [1]. Il est donc le point de contact central pour la notification d'incidents de sécurité et d'informations concernant la menace cyber.

### 6.2.4 Audits de sécurité / Tests de pénétration

A la demande, CERT.be peut, selon la disponibilité de ses ressources, effectuer un audit ou un test de pénétration de l'infrastructure (ou d'une partie de celle-ci) de son public cible. Il est possible que CERT.be fasse appel à des tiers afin de fournir ce service.

#### 6.2.5 Publication d'information en matière de cyber sécurité

CERT.be publie à l'occasion des documents de guidance, ou de liens vers de tels documents, qui pourraient avoir de l'intérêt pour son public cible.

## 6.3 Gestion de la qualité de la sécurité

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

#### 6.3.1 Conscientisation

CERT.be participe aux efforts de conscientisation du CCB.

#### 6.3.2 Formation

CERT.be a la possibilité de développer des formations dans les domaines relevant de ses compétences, et d'organiser des sessions de formation.

## 6.4 Services non fournis par CERT.be

Les services ci-dessous font partie de la liste de services repris par l'ENISA[8], mais ne sont pas fournis par CERT.be :

- Services réactifs :
    - Analyse de vulnérabilité
    - Gestion de vulnérabilité – correction de vulnérabilité
- Services Proactifs :
    - Configuration et maintenance d'outils de sécurité
    - Développement d'outils de sécurité
- Gestion de la qualité de la sécurité
    - Analyse de risques
    - Continuité des activités (BCP/DRP)
    - Consultance en sécurité
    - Evaluation ou certification de produits

[8] ENISA, «CSIRT Services,» 27 04 2016, www.enisa.europa.eu/topics/csirt-cert-services [Accès le 11 07 2017].

## 6.5 Offre de services en fonction du public cible

### 6.5.1 Services réactifs

| | Opérateurs de services essentiels et infrastructures critiques | Opérateurs de services publics essentiels | Autorités administratives | Personnes morales de droit privé | Grand Public |
|---|---|---|---|---|---|
| Alertes et avertissements | Oui[i] | Oui[i] | Oui[i] | Oui[i] | Oui |
| Analyse d'incidents | Oui[ii] | Oui[ii] | Oui[i] | - | - |
| Gestions d'incidents sur site | Oui[ii] | Oui[ii] | - | - | - |
| Support à la gestion d'incidents | Oui[ii] | Oui[ii] | Oui[i] | Oui[i] | - |
| Coordination de la gestion d'incidents | Oui[ii] | Oui[ii] | Oui[i] | Oui[i] | - |

| | Opérateurs de services essentiels et infrastructures critiques | Opérateurs de services publics essentiels | Autorités administratives | Personnes morales de droit privé | Grand Public |
|---|---|---|---|---|---|
| Coordination de gestion de vulnérabilité[iii] | Oui[i] | Oui[i] | Oui[i] | Oui[i] | - |
| Analyse d'artefacts[iii] | Oui[ii] | Ou[iii] | - | - | - |

### 6.5.2 Services proactifs

| | Opérateurs de services essentiels et infrastructures critiques | Opérateurs de services publics essentiels | Autorités administratives | Personnes morales de droit privé | Grand Public |
|---|---|---|---|---|---|
| Annonces | Oui[i] | Oui[i] | Oui[i] | Oui[i] | Oui |
| Veille technologique | Oui[i] | Oui[i] | Oui[i] | Oui[i] | Oui |
| Détection, observation et | Oui[i] | Oui[i] | Oui[i] | Oui[i] | Oui |

| | | | | | |
|---|---|---|---|---|---|
| **analyse de problèmes de sécurité** | | | | | |
| **Audits de sécurité / Tests de pénétration[iii]** | Oui[i] | Oui[i] | Oui[i] | - | - |
| **Publication d'informations** | Oui[i] | Oui[i] | Oui[i] | Oui[i] | Oui |

### 6.5.3
### Gestion de la qualité de la sécurité

| | Opérateurs de services essentiels et infrastructures critiques | Opérateurs de services publics essentiels | Autorités administratives | Personnes morales de droit privé | Grand Public |
|---|---|---|---|---|---|
| Conscientisation | Oui[i] | Oui[i] | Oui[i] | Oui[i] | Oui |
| Formations | Oui[i] | Oui[i] | Oui[i] | Non | Non |

[i] Durant les heures de bureau
[ii] 24x7 en coopération avec le Centre de Crise
[iii] Eventuellement avec la participation de tiers

# 7 NIVEAU DE SERVICE

CERT.be est joignable les jours ouvrables de 09h00 à 17h00 par email (cert@cert.be). La réception des mails envoyés à cert@cert.be est confirmée en quelques minutes par un système automatique. Ce système attribue un numéro de dossier à chaque signalement. Le retour de mail par un opérateur n'est pas garanti, et dépend de la gravité de l'incident et la qualité du correspondant.

En collaboration avec le Centre de Crise du SPF Intérieur, CERT.be est joignable par téléphone 24/7 pour le traitement d'incidents de sécurité chez les opérateurs de services essentiels et d'infrastructures critiques.

# 8 RESUME DES POLITIQUES

## 8.1 Types d'incidents et niveau de support

CERT.be traite tout incident lié à un système d'information ou réseau situé sur le territoire belge, ou tout domaine internet finissant par « .be ». Le niveau de support dépend de la gravité de l'incident et de la qualité du correspondant.

Priorité sera donnée au public cible comme suit :

1. Opérateurs de services essentiels et infrastructures critiques ;
   Services publics opérateurs de services essentiels ;
2. Autorités administratives ;
3. Personnes morales de droit privé ;
4. Grand public.

## 8.2 Coopération, interaction et divulgation d'information

CERT.be traite l'information qui lui est confiée selon la législation belge en vigueur. CERT.be est donc attentif à protéger les données à caractères personnels et les informations sensibles qui lui sont communiquées.

Comme spécifié dans le Plan d'Urgence Cyber, CERT.be coordonne les activités des différents intervenants en cas d'incident national de cyber sécurité. Dans le cas de crise nationale de cyber sécurité, CERT.be collabore avec la Direction Générale du Centre de Crise pour coordonner les activités des différents intervenants.

Lorsque la résolution d'un incident nécessite la divulgation de telles données, CERT.be veillera à ne transmettre que le minimum requis.

Des informations transmises par email sous forme chiffrée avec la clef PGP de CERT.be ne seront stockées que sous cette forme et ne seront déchiffrées que lorsque nécessaire à la résolution d'un incident. Si un transfert de ces informations est nécessaire, ce transfert sera également chiffré avec PGP.

CERT.be utilise et respecte le Traffic Light Protocol tel que décrit par FIRST (version 1.0)[9].

Autant que possible, CERT.be partagera son expérience avec ses pairs et avec son public cible, pour autant que cela ne contrevienne pas aux provisions ci-dessus. Une attention particulière sera portée aux groupes suivants : EGC[10], TF-CSIRT[11], FIRST[12], et le EU CSIRTs Network.

N'auront des contacts avec la presse que les personnes autorisées à le faire par le CCB.

## 8.3 Communication et authentification

CERT.be est joignable par mail à cert@cert.be. Une clef PGP est associée à cette adresse :

```
pub   4096R/52982D62 2016-12-31 [expires: 2019-12-31]
    Key fingerprint = 59FC 9F8A 4EE8 8BCF 6558  597E 2AFB E221 5298 2D62
uid      [  full  ] CERT.be <cert@cert.be>
```

CERT.be dispose de personnel habilité à traiter de l'information classifiée au sens de la Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité[13].

[9] 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/.
[10] European Governmental CERTs
[11] Task Force – Cooperation of Computer Security Incident Response Teams
[12] Forum of Incident Response Teams
[13] Loi du 11 décembre 1998 relative à la classification et aux habilitations, attestations et avis de sécurité,» *M.B.*, 7 mai 1999, p. 15752.