CENTRE FOR
CYBER SECURITY
BELGIUM

National CSIRT Charter

CHANCELLERY OF
THE PRIME MINISTER

.be

01
Introduction

About this document

As public service, The National CSIRT's existence is defined by a set of official – Royal decrees, Council of Ministers decisions, etc. – and internal documents. The present Charter takes the necessary elements from these diverse sources and compiles them in a single document.

While it's not considered advisable to change such a Charter often, it isn't a dead document. The present Charter can be modified depending on the legal or budgetary context, or simply after internal examination of its relevance. At the very least, it should be revised every other year.

02

Mission

Royal Decree of 10 October 2014

Royal Decree of 10 October 2014 established the creation of the Centre for Cyber Security Belgium (CCB). The CCB is under the authority of the Prime Minister.

The Centre for Cyber Security Belgium is the national authority for cyber security in Belgium. The CCB took over and integrated the Computer Emergency Response Team (CERT) for the purpose of carrying out activities relating to the detection, observation and analysis of online security problems as well for providing continuous information related thereto to users.
The main missions of the CCB described from the Royal decree are:

- Monitoring, coordinating and supervising the implementation of Belgian policy on the subject;
- Managing the various projects on the topic of cyber security using an integrated and centralized approach;
- Ensuring coordination between the relevant government departments and governments, as well as the public authorities and the private or scientific sectors;
- Formulating proposals aimed at adapting the regulatory framework in the field of cyber security;
- Ensuring crisis management in case of cyber incidents in cooperation with the government's Coordination and Crisis Centre;
- Preparing, disseminating and supervising the implementation of standards, guidelines and security standards for the various information systems of the governments and public institutions;
- Coordinating the Belgian representation in international cyber security forums, coordinating the monitoring of international commitments and national proposals on this subject;
- Coordinating the security evaluation and certification information and communication systems;
- Informing and raising awareness among users on information and communication systems.

NIS LAW

Article 3 of the Royal Decree of 12 July 2019 about implementation of the Law of 7 April 2019 regarding Network and Information Security (NIS Law) states that the Cybersecurity Centre for Belgium is designated as National CSIRT in the sense of the NIS Law.

Article 60 of the NIS Law defines the missions of the National CSIRT as :

1. Follow up incidents at the National and International Level, including the processing of personal data related to the follow up of incidents.
2. Activating the Early Warning System, publish alert messages, announcements and publication of information related to risks and incidents for stakeholders.
3. Incident handling.
4. Dynamic analysis of risks and incidents related to Network and Information Systems.
5. Detect, observe and analysis of Network and Information Security problems.
6. Promote adoption and use of common or normalised procedures for handling risks and incidents, including classification of incidents, risks and information.

7. Establish relations with the private sector, other administrative departments or public authorities.
8. Take part in the CSIRTs Network created by the EU NIS Directive.

Cybersecurity refers to all measures that ensure the confidentiality, the availability and the integrity of Information and Communication Technologies (ICT): technical measures, but also user awareness measures.

Cybersecurity is not about the use of ICT only as a means of activism, terrorism, espionage, subversion, or generally criminal. These deeds are the responsibility of other services than The National CSIRT (police, State security, etc.). Moreover, the identification of the authors of crimes is not within the National CSIRT's purview.

However, any risk against the confidentiality, the integrity and the availability of ICT systems, for whatever reason, is a cybersecurity problem.

03

Constituency

The constituency is the set of parties that may make use of The National CSIRT's services. Some services are only available to some of the constituency.

Being part of The National CSIRT's constituency does not engage in any obligation of the targeted companies or organisations towards The National CSIRT but indicates The National CSIRT's willingness to be of service to these companies or organisations.

Operators of Essential Services and Critical Infrastructures

An Important part of the National CSIRT's constituency consists of operators of critical infrastructures and essential services. The operators of critical infrastructure are those identified by the Law of 1 January 2011 pertaining the security and protection of critical infrastructures.
Operators of essential services are the companies and public services that are part of the sectors concerned by the NIS Directive and identified as such by the relevant sectorial authorities:

1. Energy
    a. Electricity
    b. Petrol
    c. Gas
2. Transports
    a. Air transport
    b. Railway transport
    c. Water transport
    d. Road transport
3. Banks
4. Financial markets infrastructures
5. Health sector
6. Drinkable water provision and distribution
7. Digital infrastructures

Public Services

Public services essential to the Belgian population but not covered by the NIS Directive are not defined by regulations, but by internal criteria within the CCB.

Administrative Authorities

The ICT infrastructure of Belgian public services is essential to the good working of the country, and that importance makes it a part of The National CSIRT's constituency.

Private moral persons

Private moral persons that don't offer essential services can make use of a limited subset of the the National CSIRT's services.

Greater Public

The public-at-large only has access to a limited subset of The National CSIRT's services (see

Classified Information Systems

Computers, networks or communication systems that are classified in the sense of the Law of 11 Decembre 1998 pertaining the security classification, clearance and advice are under the authority of the National Security Authority (ANS) and thus out of the scope of the CCB and The National CSIRT.

04

Affiliation

The Centre for Cybersecurity for Belgium (CCB) is an administrative service under the authority of the Prime Minister.

05

Authority

Authority is the ability for The National CSIRT to compel all or parts of its constituency to apply such or such security measure in order to prevent a cybersecurity threat or resolve a cybersecurity incident.
Article 62 of the NIS Law states that the National CSIRT takes all measures commensurate in order to realise its mission and fulfil its obligations. In this setting, the National CSIRT has the right to hold, process, transfer all needed information, even if this information results from unauthorised access to a Network or Information System.

06

Services

The services that can be offered by a CSIRT are varied and depend both of its constituency and its authority on the latter, and of its institutional position. CSIRT services are generally classified in three categories: reactive services, proactive services, and security quality management services. The EU Agency for information and networks security (ENISA) also uses these categories in their list of possible CSIRT services. This list is extensive, and each CSIRT must make its own selection in function of its mission and resources.
This section adopts this classification and describes The National CSIRT's services offering.

Reactive services

Reactive services aim at answering calls for assistance, notifications, and generally at any and all threat or attack against the CSIRT's constituency's systems.

Alerts and warnings

This service consists in the publication of information describing an attack, an alert, a threat, etc. and in the providing of short-term actions recommendations that allow to face the problem.

Incident handling

Incident analysis

At the request of a member of its constituency, The National CSIRT will make a *postmortem* analysis of a cybersecurity incident. The goal of this analysis will be to identify the extent of the incident and the damage done, its root cause, and possibly recommendations.

On-site incident handling

At the request of certain members of its constituency, The National CSIRT will dispatch specialists in order to assist local teams in handling a specific incident.

Incident handling support

The National CSIRT provides its constituency with its support in handling security incidents. This support takes the form of advice by email or phone, help in data analysis, etc.

Incident coordination

The National CSIRT coordinates, in relationship with the concerned partners, the handling of incidents. In case of serious incident, the Cyber Emergency Plan can be activated.

Vulnerability handling – response coordination

When a vulnerability is found in some software product, The National CSIRT can, on request, coordinate mitigation and communication efforts between the different parties involved (researcher, software vendor, users, etc.). It may be that The National CSIRT must collaborate with external third parties in order to provide this service.

Artefact analysis

An artefact is a trace of an intrusion or attempt at intrusion on an ICT system. Log files and systems information are examples of artefacts.

The National CSIRT may analyse artefacts submitted by some categories of its constituency. The National CSIRT may have to work with external third parties in order to provide this service.

Proactive services

Proactive services aim at improving the constituency's security infrastructure and processes before an incident occur or is detected.

Announcements

The National CSIRT provides announcements via its web site and if necessary private channels in order to warn its constituency of risks caused by newly found vulnerabilities or the existence of new threat vectors.

Technology watch

The National CSIRT performs a continuous technology watch in the field of cyber security and information security in the broadest sense. This watch feeds The National CSIRT's other services and allows it to keep on top of the latest evolutions in the field.

Detection, observation and analysis of security problems

The National CSIRT's mission is to detect, observe and analyse online security problems[1]. It is thus therefore the central contact point for the notification of security incidents and information about cyber threat.

Security assessments / Penetration tests

On request, The National CSIRT may, depending on resources availability, perform an assessment or a penetration test of the infrastructure (or part thereof) of its constituency. The National CSIRT may have to work with external third parties in order to provide this service.

Cybersecurity information dissemination

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

The National CSIRT publishes when necessary guidance documents or links to such documents, that may be of interest for its constituency.

Security quality management services

These services aim at using the findings and lessons learned from the practice of the various reactive services.

Awareness raising

The National CSIRT takes part in the CCB's awareness raising campaigns.

Training

The National CSIRT has the possibility to develop training about its competencies, and to organise training sessions.

Services not delivered by the National CSIRT

Reactive services:

- Vulnerability handling – vulnerability patching
- Operational security

Proactive services:

- Configuration and maintenance of security tools
- Security tools development
- Security quality management:
  - General risk analysis and modelling
  - Business continuity (BCP/DRP) planning and
  - Security consultancy

    Evaluation or certification of security products

Services offering in function of the constituency

Reactive services

	Operators of essential services and critical infrastructures	Operators of essential public services	Administrative authorities	Personnes morales de droit privé	Public-at-large
Alerts and warnings	Yes[i]	Yes[i]	Yes[i]	Yes[i]	Yes
Incident analysis	Yes[ii]	Yes[ii]	Yes[i]	-	-
Incident handling on-site	Yes[ii]	Yes[ii]	-	-	-
Incident handling support	Yes[ii]	Yes[ii]	Yes[i]	Yes[i]	-
Incident handling coordination	Yes[ii]	Yes[ii]	Yes[i]	Yes[i]	-
Vulnerability handling coordination[iii]	Yes[i]	Yes[i]	Yes[i]	Yes[i]	-
Artefact analysis[iii]	Yes[ii]	Yes[ii]	-	-	-

Proactive services

	Operators of essential services and critical infrastructures	Operators of essential public services	Administrative authorities	Personnes morales de droit privé	Public-at-large
Announcements	Yes[i]	Yes[i]	Yes[i]	Yes[i]	Yes
Technology watch	Yes[i]	Yes[i]	Yes[i]	Yes[i]	Yes
Detection, observation and analysis of security problems	Yes[i]	Yes[i]	Yes[i]	Yes[i]	Yes
Security audits / Penetration tests[iii]	Yes[i]	Yes[i]	Yes[i]	-	-
Information dissemination	Yes[i]	Yes[i]	Yes[i]	Yes[i]	Yes

Security Quality Management Services

	Operators of essential services and critical infrastructures	Operators of essential public services	Administrative authorities	Personnes morales de droit privé	Public-at-large
Awareness Raising	Yes[i]	Yes[i]	Yes[i]	Yes[i]	Yes
Trainings	Yes[i]	Yes[i]	Yes[i]	-	-

07

Service Level

The National CSIRT can be contacted during working hours (09:00 to 17:00) by email (cert@cert.be). Reception of mails sent to the National CSIRT is automatically acknowledged within a few minutes. This automatic system gives a unique number to each report. Return email by an operator is not guaranteed and depends on the gravity of the incident and the correspondent's quality.

In collaboration with the Ministry of Interior Affairs' Crisis Centre, The National CSIRT can be contacted 24/7 by phone for the purposes of incident handling for operators of essential services and critical infrastructures.

08

Summary of the Policies

Types of incidents and support level

The National CSIRT handles any incident linked to an information or network system located on the Belgian territory, or any internet domain in ".be". The level of support depends on the gravity of the incident and the quality of the correspondent.
Priority within the constituency is as follows:

1. Operators of essential services and critical infrastructures;
   Operators of essential public services;
2. Administrative authorities;
3. Companies;
4. Public-at-large.

Cooperation, interaction and information dissemination

The National CSIRT treats information it is handed according to the current Belgian legislation. The National CSIRT is therefore careful to protect personal data and sensitive information it receives.
As specified in the Cyber Emergency Plan, The National CSIRT coordinates the activities of the different stakeholders in the case of a national cybersecurity incident. In the case of a national cyber security crisis, The National CSIRT works together with the Crisis Centre in order to coordinate the activities of the different stakeholders.
When it is necessary to communicate personal data in order to handle an incident, The National CSIRT will be careful to only send the required minimum of information.

Information sent by email and encrypted with The National CSIRT's PGP key will only be stored encrypted and will only be deciphered when required. If a transfer of these information is necessary, that transfer will also be PGP encrypted.

The National CSIRT uses and respects the Traffic Light Protocol as described by FIRST (version 1.0)[2].

As much as possible, The National CSIRT will share its experience with its peers and its constituency, provided this doesn't contravene the above provisions. Special attention will be given to the following groups: EGC[3], TF-CSIRT[4], FIRST[5], et le EU CSIRTs Network.

Only specifically CCB-designated persons will have contact with the press.

Communication and authentication

The National CSIRT can be joined by email at cert@cert.be. A PGP key is associated with this address:

```
pub   rsa4096 2020-12-01 [SC] [expires: 2022-01-31]
      9EB0 13DE 9396 CEAB AC2D  336A BE9D 11AE 598B 4690
uid           [  full  ] CERT.be 2021 <cert@cert.be>
sub   rsa4096 2020-12-01 [E] [expires: 2022-01-31]
```

The National CSIRT has personnel cleared to handle classified information in the sense of the Law of 11 December 1998 pertaining to information classification, security clearances and security advice[6].

[2] 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/.

[3] European Governmental CERTs

[4] Task Force – Cooperation of Computer Security Incident Response Teams

[5] Forum of Incident Response Teams

[6] 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

[i] During office hours
[ii] 24x7 in cooperation with the Crisis Centre
[iii] Possibly with third-parties support

CENTRE FOR
CYBER SECURITY BELGIUM
Rue de la Loi, 16 – Brussels

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

CHANCELLERY OF
THE PRIME MINISTER

.be