CENTRE FOR CYBERSECURITY BELGIUM

THE CENTRE FOR CYBERSECURITY BELGIUM : MAKING BELGIUM LESS VULNERABLE

Lundi de la Cybersecurité -13.04.2026

Phédra Clouner

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

1

CENTRE FOR CYBERSECURITY BELGIUM

1 The CCB : Who are we?

2 Cybersecurity in Belgium: the National Strategy

3 Our approach: Active Cyber Protection

2

THE CENTRE FOR CYBERSECURITY BELGIUM

3

The national cybersecurity agency

A government body operating under the authority of the Prime Minister:

- Created in **2014** by Royal Decree
- Acts as Computer Security Incident Response Team (**CSIRT/CERT**)
- Coordinates the implementation of the **National Cybersecurity Strategy**
- Competent authority for coordinating the implementation of the **NIS2 Directive** on the cybersecurity of important and essential entities.

But also:

- The **National Coordination Centre** (NCC-BE) tasked with centralising EU and national funding opportunities to support investments in cybersecurity projects since 2021,
- The **National Cybersecurity Certification Authority** (NCCA) in the context of European certification schemes since 2022.

4

4

The people behind the CCB

General Management:

- **Miguel de Bruycker**, Director General
- **Phédra Clouner**, Deputy Director General

CCB staff:

- 130 staff members by end 2025
- Highly skilled technical experts (analysts, researchers, first line support staff…)
- But also experts from other fields (lawyers, project managers, international relations officers, communication specialists, etc.).

5

5

Our legal mission

High-level mission: Make Belgium one of the least vulnerable countries in the cyber domain

A coordination role at strategic level…

- Drafting the National Cybersecurity Strategy in cooperation with other government departments
- Coordinating implementation of the Strategy at national level
- Supporting national crisis management for cyber aspects
- Monitoring and updating the legal framework on cybersecurity
- Representing Belgium in international cybersecurity forums (FIC par exemple) + international collaboration

... and at operational level

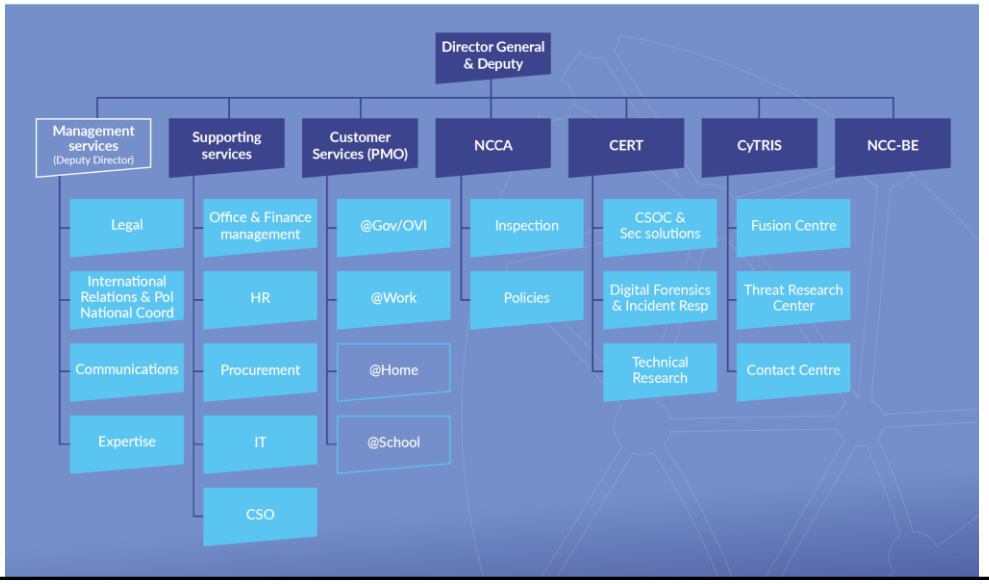
- Issuing alerts and advisories on the latest cyber threats
- Monitoring notifications and reports of cyber incidents at national and international level
- Supporting organisations in responding to cyber incidents
- Developing standards and practical guides on cyber security, etc.

6

6

CENTRE FOR CYBERSECURITY BELGIUM

ORGANIZATIONAL CHART



7

7

Our constituents

CENTRE FOR CYBERSECURITY BELGIUM

The population as a whole:
Educate & involve individuals in their own security

@Home

@Work

Organisations:
Large companies, SMEs, associations…

Organisations of vital interest:
Critical infrastructures, etc.

@OIV

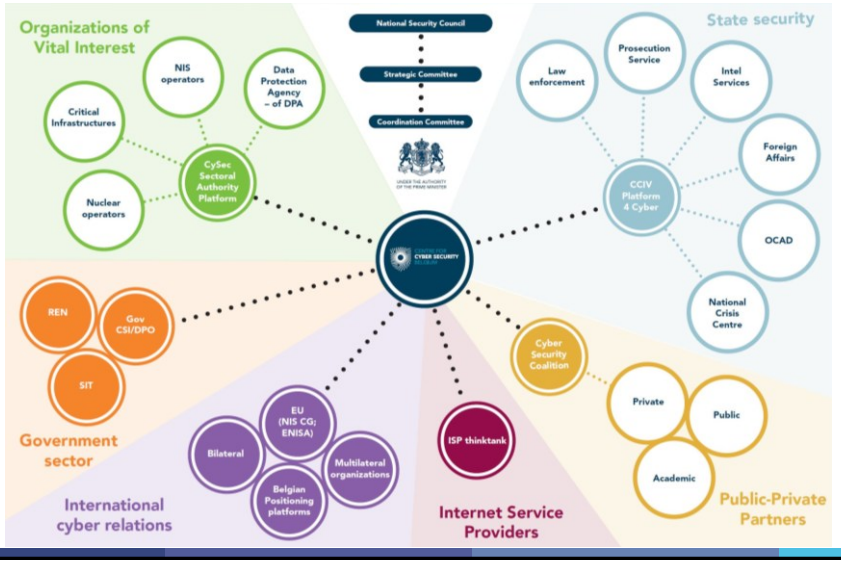
@Gov

Public authorities:
Federal, but also regional and local

8

8

Belgian Cybersecurity Governance



9

9

ACTIVE CYBER PROTECTION

10

What is Active Cyber Protection (ACP)?

CENTRE FOR CYBERSECURITY BELGIUM

A proactive, tailored, automated ad participative approach to cybersecurity:

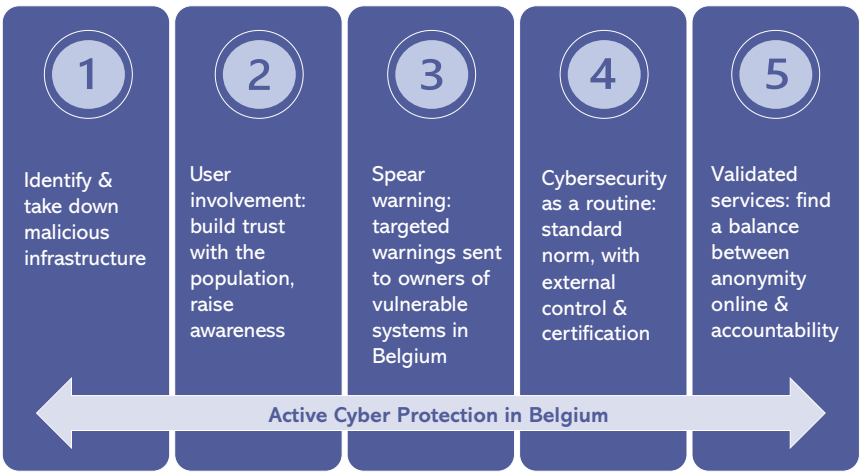
proactive	rather than just reacting to attacks, a **proactive search** for potential threats and vulnerabilities to support preparedness and prevent cybersecurity breaches
tailored	Because there is no "one size fits all" solution, customised solutions needed to take into account the **different needs** of stakeholders
automated	In a rapidly changing cybersecurity landscape, speed is essential & **automated solutions** are needed to protect systems from increasingly automated attacks
participative	**Active involvement** of all actors, from individuals to small and large organisations, in identifying and fixing vulnerabilities

11

11

Active Cyber Protection in Belgium

CENTRE FOR CYBERSECURITY BELGIUM



12

12

User involvement: Safeonweb

In 2023:

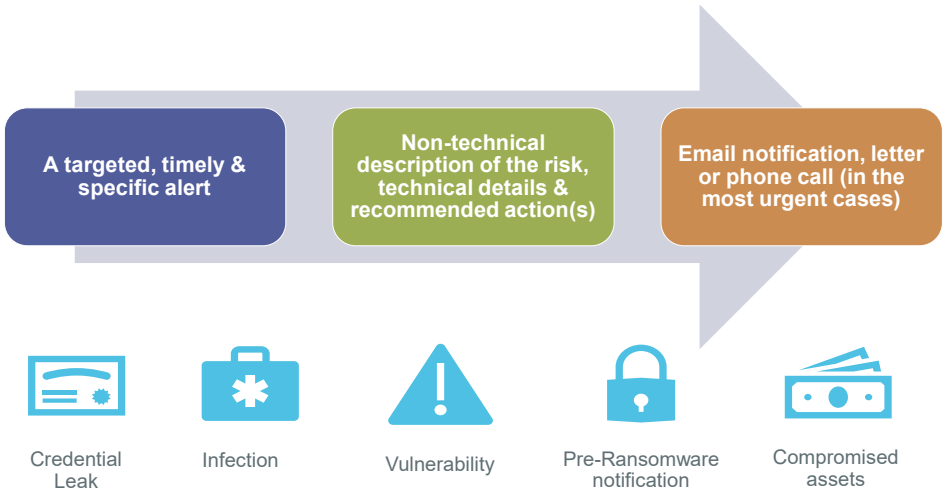
- Close to **10 million messages** were sent to suspect@safeonweb.be
- **1.2 million suspicious hyperlinks** detected thanks to these notifications.
- Fraudulent sites were neutralised thanks to a **warning page** displayed via the Belgian Anti-Phishing Shield (BAPS).

For more details: **safeonweb.be**

13

13

Spear warning



14

14

Cybersecurity as a routine

CENTRE FOR CYBERSECURITY BELGIUM

A reference **framework with 4 levels**, freely available:

- **ESSENTIAL :** 144 key measures to address the risk of advanced cyber-attacks by actors with extensive skills and resources
- **IMPORTANT :** 107 key measures to minimise the risks of targeted cyber-attacks by actors with common skills and resources
- **BASIC:** 34 key measures based on readily available tools
- **SMALL:** basic recommendations in non-technical language for micro-organisations

The Cyberfundamentals framework integrates **NIS2 requirements**, thereby helping important and essential entities in their compliance efforts..

15

15

Cybersecurity as a routine

CENTRE FOR CYBERSECURITY BELGIUM

The Cyberfundamentals **mapping** facilitates compliance with international cybersecurity standards:

IEC 62443
OT standards

Mor details at: **cyfun.be**

A **self-assessment tool:**

CCB Cyberfundamentals Framework	Target Score	2023 Policy Score	2023 Practice Score
Overall >>	3,00	3,02	2,70
Asset Management (ID.AM)	3,00	3,42	2,00
Business Environment (ID.BE)	3,00	3,00	1,00
Governance (ID.GV)	3,00	5,00	3,00
Risk Assessment (ID.RA)	3,00	2,00	4,00
Risk Management Strategy (ID.RM)	3,00	4,00	2,00
Supply Chain Risk Management (ID.SC)	3,00	1,00	3,00
Identity Management, Authentication and Access Control (PR.AC)	3,00	3,00	1,00
Awareness and Training (PR.AT)	3,00	5,00	3,00
Data Security (PR.DS)	3,00	1,00	3,00
Information Protection Processes and Procedures (PR.IP)	3,00	3,00	1,00
Maintenance (PR.MA)	3,00	5,00	4,00
Protective Technology (PR.PT)	3,00	1,00	2,00
Anomalies and Events (DE.AE)	3,00	3,00	5,00
Security Continuous Monitoring (DE.CM)	3,00	5,00	2,00
Detection Processes (DE.DP)	3,00	2,00	3,00
Response Planning (RS.RP)	3,00	4,00	1,00
Communications (RS.CO)	3,00	1,00	4,00
Analysis (RS.AN)	3,00	2,00	5,00
Mitigation (RS.MI)	3,00	3,00	2,00
Improvements (RS.IM)	3,00	4,00	2,00
Recovery Planning (RC.RP)	3,00	5,00	3,00
Improvements (RC.IM)	3,00	1,00	3,00
Communications (RC.CO)	3,00	3,00	3,00

16

16

Cybersecurity as a routine

CENTRE FOR CYBERSECURITY BELGIUM

Safeonweb@work: A dedicated portal with a full set of free **tools & services** available to all organisations registered in Belgium :

Self-Assessment
Questionnaire to assess your level of cyber maturity & obtain recommendations

Policy templates
Customisable documents e.g. Identity and Access Management Policy, Incident Management, etc.

Cyberfundamentals
4-level guide, mapping, self-assessment tool…

Coordinated Vulnerability Disclosure Policy
How to design a reward program for ethical hackers

Videos & Webinars
Latest information on the threat landscape, best practices…

Information on cybersecurity subsidies
e.g. EU & Belgian calls for proposals

… and much more !

For more details: **atwork.safeonweb.be**

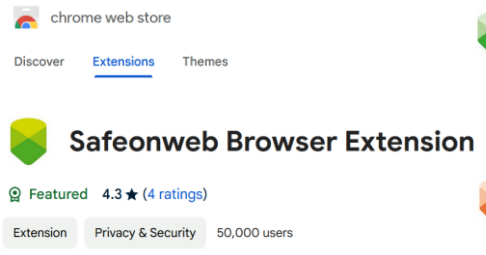
17

17

Validated services

CENTRE FOR CYBERSECURITY BELGIUM

An example: the Safeonweb browser extension



Green (OK) – 4/4: website owner has an Extended Validation Certificate issued by a Certificate Authority or the site owner is registered on Safeonweb@work (BE organisations only)

Amber (!) – 1 to 3/4: he website owner has an Organisation Validation Certificate, or a Domain Validation Certificate
→ risk if sharing personal data

Red (X) – 0/4: website lacks basic security features or is known as malicious.
→ high risk when browsing & sharing data

18

18

Going the last mile

CENTRE FOR CYBERSECURITY BELGIUM

We think big, but start small:

- Several iterations often needed: explore & learn
- Stay realistic & focus on concrete results

Change is easier in small steps!

19

CENTRE FOR CYBERSECURITY BELGIUM

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister
Rue de la Loi / Wetstraat 18 - 1000 Brussels
www.ccb.belgium.be

.be

20