CENTRE FOR CYBER SECURITY BELGIUM

CCB SERVICES TO INTERNATIONAL ORGANIZATIONS

International Organizations (IOs) are important and of special interest to Belgium. As a host nation, Belgium has the duty to take all necessary measures to ensure the independence and the smooth functioning of the International Organizations located on its territory. Guaranteeing their security is therefore a priority for us as a host country.

In terms of cybersecurity, the Centre for Cybersecurity of Belgium (CCB) is the national authority for cybersecurity and the national CSIRT (Computer Security Incident Response Team). The CCB is strongly committed to actively protecting the organizations of Vital interest in our country. These organizations offer critical services also to IOs, therefore ensuring their protection fundamentally adds to the security and functioning of IOs. The national Cyber Emergency Plan also ensures a coordinated response by all Belgian security services in case of severe cyber incidents in our country.

However, the CCB englobes important international organizations themselves also as part of a special category of stakeholders, to which it offers privileged security services: **Organizations of Special Interest (OSI)**. This OSI category includes: International Public Institutions located on Belgian soil ; Belgian government services; and the national Scientific and Economic Potential. Because of their importance, OSIs can rely on the CCB's Early Warning System as well as to other Spear Warning-, and incident mitigation services.

Within the CCB, different technical services collaborate in order to increase effectiveness in incident response and intel sharing. For instance, CERT.be (Computer Emergency Response Team) assists constituents in incident response, provides forensics services, digital artefact analysis and advices the CCB when activation of the national cyber emergency plan is required. The CCB also has a unique Cyber Threat Intel unit, CyTRIS (Cyber Threat Research & Intelligence Sharing), which monitors cyber threats, publishes regular reports and advisories, sends out warnings, and manages the Early Warning System.

The **Early Warning System (EWS)** was created by the CCB in order to alert Organizations of Vital or Special Interest in Belgium in a fast and standardised way about relevant vulnerabilities, intrusions and other cyber threats or attacks. The warnings are based on intel that the CCB received and filtered, often in collaboration with commercial partners. Information is shared both in a broadcasted and individually targeted manner. Such alerts allow constituents to quickly obtain relevant information from a reliable source and take action as quickly as possible to protect themselves against active threats and thereby prevent attacks. The EWS-project is a central part of the CCB's key service objective of 'spear warning', i.e. direct and instant, targeted warning. It thereby helps to elevate the level of security in our country.
Specific CCB services to OSIs are:

- **Incident Response:** The CCB offers support during incidents to OSI constituents. When an OSI witnesses a cyber incident, they may contact the CCB at cert@cert.be or if more urgently at +32 (0)2 501 05 60. CCB will assist OSIs via advisories and Cyber Threat Intelligence (CTI-packages), and it can also assist OSIs, where appropriate, in liaising with other national partners, such as law enforcement. This support and advise to OSIs is offered remotely, on voluntary basis, free of charge and is available 24/7. For more details, such as options for encrypted contact, please visit https://www.cert.be/en/report-incident

- **The EWS-Portal** is an online broadcast platform, where OSIs can freely consult a repository containing strategic and operational reports and notifications relevant for their sector. A general threat landscape report is also published daily on the Portal, and notifications of newly available information are sent to onboarded constituents via email. This can be in real time or in a digest-form. Constituents who have been fully onboarded can log in to the portal, via 2-Factor Authentication, and they need to respect the information sharing rules. The Competence Centre, being part of the OSI constituents, would have access to this online platform. Reports relevant for them will be made available to them in the Portal via a special OSI-tag.

- **Malware Information Sharing Platform (MISP):** after onboaxrding on the EWS-portal OSIs will be invited to connect to a MISP hosted by the CCB, which will automatically push relevant technical Indicators of Compromise (IoC's) to the systems of connected constituents. A special OSI sharing group is available in MISP.

- **Spear Warning:** Based on the technical information that organizations provide to the CCB during their onboarding to the EWS Portal (specifically IP ranges), the CCB can also perform tailored screening of the web for particular vulnerabilities and infections, according to its legal missions and powers. With the help of several private partners the CCB has a wide-range of other web-monitoring services, for instance concerning leaked credential, domain squatting, or discussions on the dark web about our constituents. When relevant, the CCB can then send out tailored email-warnings to OSI's, either through an automated system or via direct contact with a CCB-analyst for urgent communications. CCB-experts can always offer individual advise to the OSI.

- **Anti-Phishing:** All constituents may forward suspicious emails to suspect@safeonweb.be. The CCB parses all incoming mails and extracts (only) URLs and attachments. The URLs are enriched and scored for suspiciousness, and the more suspicious ones are sent to the phishing initiative system for analysis. All the potentially malicious attachments are extracted and pushed to our sandbox(es). After analyses, the malicious links are forwarded to the EU Phishing Initiative so that, in collaboration with 4 major internet browsers, access to these links is blocked in Belgium. This project, developed within the CCB, is named BeFish. The CCB analyses about 7-8000 emails per day. In 2019 the CCB received in total 1,7million such emails resulting in 4000 blocked malicious sites. For more information see, https://safeonweb.be/.

- **Bad Domains** identified through the BeFish project are also shared with stakeholders via their MISP connection.

- **Quarterly Cyber Threat Report:** Once every three months, the CCB invites its EWS-constituents to attend the presentation and discussion of its Cyber Threat Report. The report addresses the main threats to Belgium and to entities located here, noticed during the preceding quarter. During the event, these threats are discussed, experiences shared, and experts debate what can be expected in the upcoming months. The event also features specialist guest speakers, feedback on the workings of the EWS and networking opportunities.

The CCB offers all of these services voluntary and free of charge to OSIs. Interested organizations or their Computer Emergency Response Team (CERTs), Computer Security Incident Response Teams (CSIRTs), or Security Operation Centre (SOCs) may contact us at relations@ccb.belgium.be and ews@cert.be. We will be glad to answer any further questions and offer give explanations on the different services that we offer.

If the Competence centre would be located in Belgium, it would, like any other European Institution located on Belgian territory, fall in the Organizations of Special Interest (OSI) category and, therefore could enjoy the EWS and incident response services.