CENTRE FOR
CYBERSECURITY
BELGIUM

NATIONALE CSIRT-CHARTA

2026

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Datum: Januar 2026
Version: 2.0 Deutsch
Autor: Zentrum für Cybersicherheit Belgien

Das Zentrum für Cybersicherheit Belgien (ZCB) ist die nationale Cybersicherheitsbehörde und das nationale Computer Security Incident Response Team (CSIRT) in Belgien. Das ZCB überwacht, koordiniert und kontrolliert die Anwendung der belgischen Cybersicherheitsstrategie. Ein optimaler Informationsaustausch ermöglicht es Unternehmen, Behörden, NIS2-Einrichtungen und der Öffentlichkeit, sich angemessen zu schützen. Das ZCB wurde durch den Königlichen Erlass vom 10. Oktober 2014 gegründet.

Inhaltsübersicht

Einleitung

Das Zentrum für Cybersicherheit Belgien (ZCB) ist die nationale Cybersicherheitsbehörde in Belgien. Das ZCB dient als nationales Computer Security Incident Response Team (CSIRT). Der Betrieb des nationalen CSIRT als öffentlicher Dienst wird durch einen rechtlichen Rahmen definiert, der durch Beschlüsse des Ministerrats und interne Dokumente ergänzt wird. Die vorliegende Charta fasst die wesentlichen Elemente aus diesen verschiedenen Quellen in einem übersichtlichen Dokument zusammen.

Es ist zwar nicht ratsam, eine Charta häufig zu ändern, dennoch ist sie kein statisches Dokument. Die Charta kann je nach rechtlichem oder budgetärem Kontext oder einfach nach interner Überprüfung ihrer Relevanz geändert werden. Das Dokument wird grundsätzlich jedes Jahr neu bewertet.

1. Allgemeine Informationen

Das Zentrum für Cybersicherheit Belgien (ZCB) wurde durch den Königlichen Erlass vom 10. Oktober 2014 gegründet.

Das ZCB wurde im Rahmen der Umsetzung[1] des NIS2-Gesetzes[2] zur nationalen Cybersicherheitsbehörde ernannt. In dieser Funktion überwacht, koordiniert und kontrolliert das ZCB insbesondere die Anwendung der belgischen Cybersicherheitsstrategie sowie die Einhaltung des NIS2-Gesetzes durch die beteiligten Stellen. Ein optimaler Informationsaustausch ermöglicht es Unternehmen, Behörden, NIS2-Einrichtungen[3] und der Öffentlichkeit, sich angemessen zu schützen.

Die Hauptaufgaben des ZCB als nationale Cybersicherheitsbehörde[4] sind:

- Überwachung, Koordinierung und Beaufsichtigung der Umsetzung der einschlägigen belgischen Politik;
- Verwaltung der verschiedenen Cybersicherheitsprojekte nach einem integrierten und zentralisierten Ansatz;
- Sicherstellung der Koordinierung zwischen den zuständigen Abteilungen und Behörden sowie zwischen den Behörden und dem privaten oder wissenschaftlichen Sektor;
- Ausarbeitung von Vorschlägen zur Anpassung des Rechtsrahmens im Bereich der Cybersicherheit;
- Sicherstellung des Krisenmanagements bei Sicherheitsvorfällen in Zusammenarbeit mit dem Koordinations- und Krisenzentrum der Regierung;
- Ausarbeitung, Verbreitung und Überwachung der Umsetzung von Standards, Leitlinien und Sicherheitsnormen für die verschiedenen Informationssysteme von Verwaltungen und öffentlichen Einrichtungen;
- Koordinierung der belgischen Vertretung in internationalen Cybersicherheitsforen, der Weiterverfolgung der internationalen Verpflichtungen und der Vorschläge für den nationalen Standpunkt in diesem Bereich;
- Koordinierung der Bewertung und Zertifizierung der Sicherheit von Informations- und Kommunikationssystemen;
- Information und Sensibilisierung der Nutzer von Informations- und Kommunikationssystemen.

Gemäß dem NIS2-Gesetz fungiert das ZCB auch als nationales CSIRT[5]. Das Cyber Emergency Response Team (CERT) und das Cyber Threat Research & Intelligence Sharing (CyTRIS) Team sind die beiden operativen Dienste, die zusammen innerhalb des ZCB das nationale CSIRT bilden.

Die Aufgabe des CERT ist es, Cyberangriffe in Belgien zu analysieren, einzudämmen, zu begrenzen und zu stoppen. Das CERT stellt anderen öffentlichen Diensten technisches Fachwissen und Unterstützung zur Verfügung. Einige Dienste werden proaktiv erbracht, aber der Großteil der Arbeit des CERT ähnelt der einer „Cyberfeuerwehr“.

CyTRIS ist für die erste Kontaktaufnahme mit Organisationen zuständig, die dem ZCB einen Sicherheitsvorfall melden. Dieser Dienst des ZCB überwacht täglich verschiedene Quellen, sammelt und stellt Informationen zusammen, die für die Warnung potenzieller Opfer nützlich sein könnten, und führt eingehende CTI-Analysen und strategische Berichte durch. Das CyTRIS sendet auch „Spear Warnings“ (individuelle Berichte) an Organisationen, bei denen eine bestimmte Schwachstelle in der IT-Infrastruktur, Malware oder gestohlene Anmeldedaten gefunden wurden. CyTRIS organisiert außerdem regelmäßig Online- und physische Veranstaltungen, um die Beteiligten über aktive Cyberbedrohungen zu informieren und darüber, wie man sich dagegen schützen kann.

[1] Königlicher Erlass vom 9. Juni 2024 zur Durchführung des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit, Art. 3.
[2] Gesetz vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (NIS2-Gesetz). Das NIS2-Gesetz ist die Umsetzung der Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 („NIS2-Richtlinie“) in Belgien.
[3] Wesentliche und wichtige Einrichtungen, die in den Anwendungsbereich des NIS2-Gesetzes fallen.
[4] NIS2-Gesetz, Art. 17.
[5] NIS2-Gesetz, Art. 15-16.

Die Hauptaufgaben des ZCB als nationale CSIRT[6] sind:

- Überwachung und Analyse von Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle auf nationaler Ebene;
- frühzeitige Warnungen, Benachrichtigungen und Ankündigungen sowie die Verbreitung von Informationen unter den betroffenen wesentlichen und wichtigen Einrichtungen und an die zuständigen Behörden und andere relevante Interessengruppen über Cyberbedrohungen, Schwachstellen und Sicherheitsvorfällen, möglichst in Echtzeit;
- Reaktion auf Sicherheitsvorfälle und die Unterstützung der betroffenen wesentlichen und wichtigen Einrichtungen;
- Sammlung und Analyse forensischer Daten und Gewährleistung einer dynamischen Risiko- und Vorfallsanalyse sowie eines Situationsbewusstseins im Bereich der Cybersicherheit;
- Teilnahme am CSIRT-Netzwerk;
- Funktion als Koordinator für den Prozess der koordinierten Offenlegung von Schwachstellen;
- Mitwirkung an der Einführung von sicheren Instrumenten für den Informationsaustausch;
- proaktives und nicht-intrusives Scannen von öffentlich zugänglichen Netz- und Informationssystemen;
- Erkennen, Beobachten und Analysieren von Computersicherheitsproblemen;
- Zusammenarbeit und gegebenenfalls Austausch von einschlägigen Informationen.

„Cybersicherheit“ bezieht sich auf alle Maßnahmen, die die Vertraulichkeit, Verfügbarkeit und Integrität von Informations- und Kommunikationstechnologien (IKT) gewährleisten: technische Maßnahmen, aber auch Maßnahmen zur Sensibilisierung der Nutzer.

Bei der Cybersicherheit geht es jedoch nicht darum, IKT als reines Instrument für Aktivismus, Terrorismus, Spionage, Untergrabung oder allgemein kriminelle Aktivitäten zu nutzen. Diese Handlungen fallen in die Zuständigkeit anderer Stellen als des nationalen CSIRT (Polizei, Staatssicherheit usw.). Auch die Identifizierung von Straftätern fällt nicht in die Zuständigkeit des nationalen CSIRT.

Jedes Risiko, jede Verletzung der Vertraulichkeit, Integrität und Verfügbarkeit von IKT-Systemen, aus welchem Grund auch immer, ist jedoch ein Problem der Cybersicherheit.

[6] NIS2-Gesetz, Art. 19.

2. Zielpublikum

Das Zielpublikum ist die Gruppe derjenigen, die die Dienste des nationalen CSIRT in Anspruch nehmen können. Einige Dienste sind nur für einen Teil der Zielgruppe verfügbar.

Die Zugehörigkeit zur Zielgruppe des nationalen CSIRT verpflichtet die betreffenden Unternehmen oder Organisationen nicht gegenüber dem nationalen CSIRT – es sei denn, es liegt eine ausdrückliche gesetzliche Bestimmung vor –, sondern zeigt an, dass das nationale CSIRT seine Dienste für diese Unternehmen oder Organisationen zur Verfügung stellt.

Wer kann sich an das nationale CSIRT wenden?

- Wesentliche Einrichtungen nach dem NIS2-Gesetz.
- Verwaltungsbehörden: die IKT-Infrastruktur der belgischen öffentlichen Verwaltungen.
- Andere wichtige Einrichtungen, wie sie im NIS2-Gesetz definiert sind, können ebenfalls um Unterstützung bitten, die jedoch nach bestem Bemühen („Best Effort“) und in begrenzterem Umfang gewährt wird.
- Die breite Öffentlichkeit hat nur zu einem begrenzten Teil Zugang zu den Diensten des nationalen CSIRT.
- Private Rechtspersonen, die nicht unter NIS2 fallen, können einen begrenzten Teil der Dienste des nationalen CSIRT in Anspruch nehmen.
- Computer, Netzwerke oder Kommunikationssysteme, die als Verschlusssachen im Sinne des Gesetzes vom 11. Dezember 1998 über die Einstufung, die Sicherheitsermächtigungen, Sicherheitsgutachten und den öffentlichen regulierten Dienst eingestuft sind, fallen in den Zuständigkeitsbereich der Nationalen Sicherheitsbehörde (NSB) und somit nicht in den Anwendungsbereich des ZCB und des nationalen CSIRT.

3. Befugnisse

Das nationale CSIRT hat eine koordinierende und beratende Funktion. In Artikel 21 des NIS2-Gesetzes heißt es, dass das nationale CSIRT alle geeigneten Maßnahmen ergreift, um seinen Auftrag zu erfüllen und seinen Verpflichtungen nachzukommen. Diese Maßnahmen sollten in einem angemessenen Verhältnis zu diesen Zielen stehen und mit den Grundsätzen der Objektivität, Transparenz und Nichtdiskriminierung in Einklang stehen.

In diesem Zusammenhang kann das nationale CSIRT unbeschadet des Strafprozessgesetzbuchs[7] alle verfügbaren Daten besitzen, offenlegen, verbreiten oder nutzen, auch wenn diese Daten aus einem unbefugten Zugang zu einem IT-System durch einen Dritten stammen.

Das nationale CSIRT erfüllt seine Aufgaben stets mit der notwendigen Vorsicht, die von einer Behörde erwartet werden kann, wobei es stets vorrangig darauf achtet, dass der Betrieb des IT-Systems nicht gestört wird, und alle angemessenen Vorkehrungen trifft, um Sachschäden am IT-System zu verhindern.

[7] Art. 28quinquies § 1 und Art. 57 § 1.

4. Dienste

Die Dienste, die von einem nationalen CSIRT angeboten werden können, sind vielfältig und hängen sowohl von der Zielgruppe und der Autorität des CSIRT über diese Zielgruppe als auch von seiner institutionellen Stellung ab. Die Dienste des nationalen CSIRT werden im Allgemeinen in drei Kategorien eingeteilt: proaktive Dienste, reaktive Dienste und Dienste für das Management der Sicherheitsqualität. In diesem Kapitel wird diese Einteilung übernommen und das Angebot an Diensten des nationalen CSIRT beschrieben.

4.1. PROAKTIVE DIENSTE

Proaktive Dienste konzentrieren sich auf die Verbesserung der Sicherheitsinfrastruktur und -prozesse der Zielgruppe, bevor ein Sicherheitsvorfall eintritt oder entdeckt wird.

ÜBERWACHUNG UND ANALYSE VON CYBERBEDROHUNGEN, SCHWACHSTELLEN UND SICHERHEITSVORFÄLLEN

Der Auftrag des nationalen CSIRT besteht darin, Cyberbedrohungen, Schwachstellen und Sicherheitsvorfälle auf nationaler Ebene zu erkennen, zu überwachen und zu analysieren. Ein Team innerhalb des nationalen CSIRT überwacht täglich die Bedrohungslandschaft, um relevante Cyberbedrohungen und Schwachstellen zeitnah zu erkennen. Darüber hinaus stellt das nationale CSIRT strategische, operative und taktische CTI-Berichte zur weiteren Analyse spezifischer Bedrohungen bereit.

INFORMATIONSAUSTAUSCH

Das nationale CSIRT gibt über seine Website, die sozialen Medien, das Early Warning System (EWS)[8] und erforderlichenfalls durch direkten Kontakt („Spear Warning“[9]) Frühwarnungen, Meldungen und Hinweise auf festgestellte Schwachstellen und Cyberbedrohungen ab, um die betroffenen Akteure auf die Risiken neuer Schwachstellen oder Bedrohungsvektoren hinzuweisen. Es organisiert außerdem regelmäßig Online- und Präsenzveranstaltungen, um die Zielgruppen über aktive Cyberbedrohungen zu informieren und darüber, wie man sich dagegen schützen kann.

ÜBERWACHUNG DER CYBERDOMÄNE

Das nationale CSIRT überwacht kontinuierlich technologische Trends, Entwicklungen und Lösungen im Bereich der Cybersicherheit und damit auch der Informationssicherheit im weitesten Sinne. Diese Überwachung liefert anderen einen Input und ermöglicht es uns, mit den neuesten Entwicklungen in diesem Bereich Schritt zu halten.

ERKENNUNG, BEOBACHTUNG UND ANALYSE VON SICHERHEITSPROBLEMEN

Die Aufgabe des nationalen CSIRT besteht darin, Online-Sicherheitsprobleme zu erkennen, zu beobachten und zu analysieren. Es ist daher die zentrale Anlaufstelle für die Meldung von Sicherheitsvorfällen und Informationen über Cyberbedrohungen.[10]

SICHERHEITSBEWERTUNGEN/PENETRATIONSTESTS/ATTACK-SURFACE-MANAGEMENT

Auf Anfrage und je nach Verfügbarkeit von Ressourcen kann das nationale CSIRT eine Bewertung oder einen Penetrationstest der Infrastruktur (oder eines Teils davon) seiner Zielgruppe durchführen, um Schwachstellen mit potenziell erheblichen Auswirkungen zu ermitteln. Darüber hinaus kann es proaktiv das Risiko aus der Sicht eines Angreifers bewerten, indem es Schwachstellen im Internet aufspürt, um die Anzahl der möglichen Zugangspunkte von Zielgruppen zum Netzwerk zu reduzieren. Das nationale CSIRT muss möglicherweise mit (externen) Dritten

[8] Siehe https://ccb.belgium.be/de/cytris/early-warning-system.
[9] Siehe https://ccb.belgium.be/de/cytris/faq-on-spear-warnings.
[10] Siehe https://ccb.belgium.be/de/cert/einen-vorfall-melden.

zusammenarbeiten, um diesen Dienst zu erbringen.

VERBREITUNG VON INFORMATIONEN ZUR CYBERSICHERHEIT

Gegebenenfalls veröffentlicht das nationale CSIRT Leitlinien oder Links zu solchen Dokumenten, die für die Zielgruppe von Interesse sein könnten.[11]

IDENTIFIZIERUNG UND MELDUNG VON ANFÄLLIGEN ODER UNSICHEREN SYSTEMEN

Das nationale CSIRT kann proaktiv und nicht-intrusiv öffentlich zugängliche Netz- und Informationssysteme scannen, um anfällige oder unsicher konfigurierte Netz- und Informationssysteme aufzuspüren und die betroffenen Einrichtungen zu informieren, sofern der Betrieb der Dienste der Einrichtungen dadurch nicht beeinträchtigt wird.

4.2. REAKTIVE DIENSTE

Reaktive Dienste sind darauf ausgerichtet, auf Hilfeersuchen, Warnungen und generell auf alle Bedrohungen oder Angriffe zu reagieren, die sich gegen die Systeme der Zielgruppe des nationalen CSIRT richten.

BEHANDLUNG VON SICHERHEITSVORFÄLLEN

- Erste Kontaktaufnahme und Registrierung bei (NIS2-)Sicherheitsvorfällen

Bearbeitung von (Vorfall-)Meldungen per Telefon und E-Mail und ggf. erste Kontaktaufnahme.

- Analyse der Sicherheitsvorfälle

Auf Anfrage der Zielgruppe führt das nationale CSIRT eine Post-Mortem-Analyse eines Sicherheitsvorfalls durch. Ziel dieser Analyse ist es, das Ausmaß des Vorfalls und des entstandenen Schadens zu ermitteln, die Ursache zu identifizieren und gegebenenfalls Empfehlungen auszusprechen.

- On-Site-Vorfallmanagement

Auf Anfrage bestimmter Mitglieder ihrer Zielgruppe entsendet es nationale CSIRT-Spezialisten, um lokale Teams bei der Bewältigung eines bestimmten Sicherheitsvorfalls zu unterstützen.

- Unterstützung beim Vorfallmanagement

Das nationale CSIRT bietet seiner Zielgruppe Unterstützung bei der Bewältigung von Sicherheitsvorfällen. Diese Unterstützung kann Beratung per E-Mail oder Telefon, Hilfe bei der forensischen Datenanalyse usw. umfassen.

- Koordinierung von Sicherheitsvorfällen

Das nationale CSIRT koordiniert in Zusammenarbeit mit den beteiligten Akteuren die Reaktion auf Sicherheitsvorfälle. Bei schweren Vorfällen kann der nationale Cybernotfallplan aktiviert werden.

SCHWACHSTELLENMANAGEMENT – REAKTIONSKOORDINATION

Wenn eine Schwachstelle in einem bestimmten Softwareprodukt festgestellt wird, kann das nationale CSIRT auf Anfrage die Bemühungen um Schadensbegrenzung und Kommunikation zwischen den verschiedenen beteiligten Parteien (Forscher, Softwarehersteller, Benutzer usw.) koordinieren.[12] Das nationale CSIRT muss möglicherweise mit Dritten zusammenarbeiten, um diesen Dienst zu erbringen.

[11] Siehe https://ccb.belgium.be/advisories.
[12] Siehe https://ccb.belgium.be/de/regulation/cvdp.

ARTEFAKTEANALYSE

Ein Artefakt ist das, was nach einem (versuchten) Eindringen in ein IKT-System übrig bleibt. Dateien, Protokolle, oder Informationssysteme sind (nur einige) Beispiele für Artefakte. Das nationale CSIRT kann die gemeldeten Artefakte analysieren. Das nationale CSIRT muss möglicherweise mit Dritten zusammenarbeiten, um diesen Dienst zu erbringen.

4.3. DIENSTE DES SICHERHEITSQUALITÄTSMANAGEMENTS

Diese Dienste nutzen die Erkenntnisse und Lehren, die aus der Praxis der verschiedenen reaktiven Dienste gewonnen wurden.

SENSIBILISIERUNG

Das nationale CSIRT beteiligt sich an den Sensibilisierungskampagnen des ZCB. Es organisiert außerdem regelmäßig Online- und Präsenzveranstaltungen, um die Zielgruppen über aktive Cyberbedrohungen zu informieren und darüber, wie man sich dagegen schützen kann.

AUSBILDUNG

Das nationale CSIRT ist in der Lage, Ausbildungen in seinen Zuständigkeitsbereichen zu entwickeln und Schulungen zu organisieren. Das nationale CSIRT wird möglicherweise mit Dritten zusammenarbeiten, um diesen Dienst zu erbringen.

4.4. DIENSTE, DIE NICHT VOM NATIONALEN CSIRT ERBRACHT WERDEN

Proaktive Dienste:

- allgemeine Risikoanalyse und Modellierung
- Betriebskontinuitätsplanung (BCP/DRP) und Sicherheitsempfehlungen
- Bewertung oder Zertifizierung von Sicherheitsprodukten

Reaktive Dienste:

- Schwachstellenmanagement – Schließen von Schwachstellen (Korrekturen)
- Operative Sicherheit
- Wiederaufbau im Falle eines Cyberangriffs

5. Serviceniveau

Das nationale CSIRT ist per E-Mail oder telefonisch[13] während der Bürozeiten (9:30 bis 16:30 Uhr) von Montag bis Freitag – außer an offiziellen Feiertagen – zu erreichen.

Der Empfang von E-Mails, die an das nationale CSIRT gesendet werden, wird innerhalb weniger Minuten automatisch bestätigt. Durch dieses automatische System wird jeder Meldung eine eindeutige Nummer zugewiesen. Es ist nicht gesagt, dass das CSIRT in der Lage sein wird, die Post systematisch zu beantworten; dies hängt von der Schwere des Sicherheitsvorfalls und der Funktion des Ansprechpartners ab.

In Zusammenarbeit mit dem Nationalen Krisenzentrum (NCCN) des Innenministeriums steht das nationale CSIRT rund um die Uhr telefonisch zur Verfügung, um schwerwiegende Sicherheitsvorfälle für wesentliche NIS2-Einrichtungen zu bearbeiten.

[13] Kontaktinformationen finden Sie in Abschnitt 6.

6. Zusammenfassung der nationalen CSIRT-Politik

6.1. ARTEN VON SICHERHEITSVORFÄLLEN UND UMFANG DER UNTERSTÜTZUNG

Das nationale CSIRT befasst sich mit allen Sicherheitsvorfällen, die ein Netz- oder Informationssystem auf belgischem Hoheitsgebiet oder eine Internetdomäne mit der Endung „.be“ betreffen. Der Umfang der Unterstützung hängt von der Schwere des Vorfalls und der Funktion des Ansprechpartners ab.

Die Priorität für die Zielgruppe wird wie folgt festgelegt:

1. Wesentliche Einrichtungen nach dem NIS2-Gesetz.

2. Verwaltungsbehörden: die IKT-Infrastruktur der belgischen öffentlichen Verwaltungen.

3. Wichtige Einrichtungen, wie sie im NIS2-Gesetz definiert sind, können ebenfalls um Unterstützung bitten, die jedoch nach bestem Bemühen („Best Effort“) und in begrenzterem Umfang gewährt wird.

4. Die breite Öffentlichkeit hat nur zu einem begrenzten Teil Zugang zu den Diensten des nationalen CSIRT. Private Rechtspersonen, die keine wesentlichen Dienste erbringen, können einen begrenzten Teil der Dienste des nationalen CSIRT in Anspruch nehmen.

Computer, Netzwerke oder Kommunikationssysteme, die als Verschlusssachen im Sinne des Gesetzes vom 11. Dezember 1998 über die Einstufung, die Sicherheitsermächtigungen, Sicherheitsgutachten und den öffentlichen regulierten Dienst eingestuft sind, fallen in den Zuständigkeitsbereich der Nationalen Sicherheitsbehörde (NSB) und somit nicht in den Anwendungsbereich des ZCB und des nationalen CSIRT.

6.2. ZUSAMMENARBEIT, INTERAKTION UND INFORMATIONSVERBREITUNG

Das nationale CSIRT behandelt die erhaltenen Informationen gemäß den geltenden belgischen Rechtsvorschriften. Das nationale CSIRT legt daher auch großen Wert auf den Schutz der personenbezogenen Daten und sensiblen Informationen, die es erhält.

Wie im nationalen Cybernotfallplan[14] angegeben, koordiniert das nationale CSIRT die Aktivitäten der verschiedenen Beteiligten im Falle eines nationalen Sicherheitsvorfalls. Im Falle einer nationalen Cybersicherheitskrise arbeitet das nationale CSIRT mit dem Nationalen Krisenzentrum (NCCN) zusammen, um die Aktivitäten der verschiedenen Beteiligten zu koordinieren.[15]

Wenn die Übermittlung personenbezogener Daten zur Bearbeitung eines Sicherheitsvorfalls erforderlich ist, achtet das nationale CSIRT darauf, nur das erforderliche Minimum an Informationen zu übermitteln.

Daten, die per E-Mail in verschlüsselter Form übermittelt werden, werden nur in dieser Form gespeichert und nur dann entschlüsselt, wenn dies zur Lösung eines Sicherheitsvorfalls erforderlich ist. Falls eine Übermittlung dieser Daten erforderlich ist, werden sie ebenfalls verschlüsselt.

Das nationale CSIRT verwendet und beachtet das von FIRST beschriebene Traffic Light Protocol 2.0.[16]

Das nationale CSIRT wird seine Erfahrungen so weit wie möglich mit Peers und seinen Zielgruppen teilen, sofern dies nicht gegen die oben genannten Bestimmungen verstößt. Besondere Aufmerksamkeit wird den folgenden Gruppen gewidmet: EGC6, TF-CSIRT7, FIRST8 und dem EU CSIRTs Network.

Nur die vom ZCB speziell benannten Personen haben Kontakt zur Presse.

---

[14] Der nationale Plan für Sicherheitsvorfälle und die Reaktion auf Cyberkrisen (kurz: nationaler Cybernotfallplan). Dieser Plan ist ein nationaler Plan im Sinne von Artikel 9 § 2 des Gesetzes vom 15. Mai 2007 über die zivile Sicherheit. Dieser Plan wurde vom ZCB zusammen mit dem NCCN ausgearbeitet. Der nationale Cybernotfallplan ist kein öffentliches Dokument. Siehe auch Art. 29 des NIS2-Gesetzes.

[15] NIS2-Gesetz, Art. 18.

[16] https://www.first.org/tlp/

6.3 KOMMUNIKATION UND AUTHENTIFIZIERUNG

Das nationale CSIRT kann per E-Mail kontaktiert werden unter: info@ccb.belgium.be. Nur für dringende Hilfe bei Sicherheitsvorfällen ist das nationale CSIRT auch telefonisch unter +32 (0)2 501 05 60 erreichbar. Das nationale CSIRT ist während der Bürozeiten (9:30 bis 16:30 Uhr) von Montag bis Freitag – außer an offiziellen Feiertagen – zu erreichen.

Um schwerwiegende Sicherheitsvorfälle für wesentliche NIS2-Einrichtungen zu bearbeiten, steht das nationale CSIRT in Zusammenarbeit mit dem Nationalen Krisenzentrum (NCCN) des Innenministeriums rund um die Uhr telefonisch zur Verfügung.

Für eine sichere und diskrete Kommunikation kann die PGP-Verschlüsselung verwendet werden. Aktuelle Informationen über verfügbare E-Mail-Adressen mit ihren PGP-Schlüsseln sind aufgeführt unter: https://ccb.belgium.be/de/cert/eine-verschluesselte-mitteilung-senden.

Das nationale CSIRT verfügt über Mitarbeiter, die zum Umgang mit Verschlusssachen im Sinne des Gesetzes vom 11. Dezember 1998 über die Einstufung, die Sicherheitsermächtigungen, Sicherheitsgutachten und den öffentlichen regulierten Dienst ermächtigt sind.