CENTRE FOR CYBERSECURITY BELGIUM

DIE NIS2-RICHTLINIE IN BELGIEN

Centre for Cybersecurity Belgium
Unter der Autorität des Premierministers

Einleitung

Das 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“) setzt die EU-Richtlinie 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 („NIS2-Richtlinie“) in Belgien um.

Um den zunehmenden Cyberbedrohungen und neu entstehenden Herausforderungen begegnen zu können, hat die Europäische Union einen Gesetzestext zu Maßnahmen erlassen, die ein hohes gemeinsames Cybersicherheitsniveau in der Union gewährleisten sollen (Richtlinie 2022/2555 vom 14. Dezember 2022 – die sogenannte „NIS2-Richtlinie“). Er ersetzt die „NIS1-Richtlinie“ (Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union).

Die NIS2-Richtlinie enthält erhebliche Änderungen gegenüber der NIS1-Richtlinie: Erweiterung der betroffenen Sektoren und Einrichtungen, neue Auswahlmethoden und Registrierungsverfahren, strengere Cybersicherheitsanforderungen, neue Fristen für die Meldung von Sicherheitsvorfällen und schärfere Überwachungsmechanismen.

Gleichzeitig zielt die Richtlinie auf eine Stärkung der nationalen Cybersicherheitsstrategie und -grundsätze ab. Zu diesen Grundsätzen gehören ein national strukturiertes Cyber-Krisenmanagement und dazugehörende Prozeduren, die Aufgaben der befugten Behörden sowie die nationale und internationale Zusammenarbeit.

Als nationale Cybersicherheitsbehörde spielt das Zentrum für Cybersicherheit Belgien (ZCB) eine zentrale Rolle bei der Koordination und Umsetzung dieser Richtlinie. Dem ZCB kommt dabei die Aufgabe der befugten Behörde für alle Sektoren (in Zusammenarbeit mit den dort gegebenenfalls zuständigen sektoralen Behörden) zu. Es spielt auch die Rolle des nationalen CSIRT, der zentralen nationalen Anlaufstelle und der Vertretung innerhalb der NIS-Kooperationsgruppe, des CSIRT- sowie des EU-CyCLONe-Netzwerks.

Wesentliche und wichtige Einrichtungen müssen geeignete und verhältnismäßige Maßnahmen ergreifen, um die Risiken, um ihre Cybersicherheitsrisiken zu beherrschen. Diese umfassen organisatorische, aber auch technische und operative Maßnahmen mit zwei Zielen: Sicherheitsvorfälle verhindern und deren Auswirkungen auf ihre Dienste bei erfolgreichen Vorfällen möglichst gering halten.

Um Organisationen zu unterstützen, hat das ZCB mit der Erstellung des CyberFundamentals (CyFun®) Framework übersichtliche Leitlinien entwickelt. Zu diesem Zweck profitieren Einrichtungen von einer Konformitätsvermutung, wenn sie eine CyFun®- oder ISO/IEC 27001-Zertifizierung/Label erhalten.

NIS2 Einrichtungen müssen dem nationalen CSIRT ihre erhebliche Sicherheitsvorfälle melden. Dies erlaubt eine mögliche Ausbreitung des jeweiligen Vorfalls zu begrenzen und Einrichtungen das Anfordern von Unterstützung zu ermöglichen. Mit dem Empfang dieser Informationen kann das ZCB bestmöglich mit Krisensituationen und die zugehörigen technischen Informationen mit anderen Einrichtungen zu teilen.

Nicht zuletzt spielt das ZCB mit seinem Inspektionsdienst ebenfalls eine Rolle (gegebenenfalls in Zusammenarbeit mit den sektoralen Behörden) bei der Überwachung der betroffenen Einrichtungen. Der Hauptzweck der Aufsicht besteht darin, die Widerstandsfähigkeit der Einrichtungen im Bereich der Cybersicherheit zu stärken. Sie ermöglicht aber auch die Verhängung von Sanktionen gegen Einrichtungen, die die erforderlichen Maßnahmen nicht ergreifen.

Ziel des vorliegenden Dokuments ist es, allgemeine Informationen über den Anwendungsbereich und den Inhalt der Umsetzung der NIS2-Richtlinie[1] in Belgien bereitzustellen.

---

[1] NIS2-Gesetz: https://www.ejustice.just.fgov.be/eli/loi/2024/04/26/2024202344/justel

Königlicher Erlass: https://www.ejustice.just.fgov.be/eli/arrete/2024/06/09/2024005260/justel

Inhaltsverzeichnis

Überblick: NIS2 in 7 Schritten

Es scheint, als ob Ihre Organisation von NIS2 betroffen ist, aber Sie sind sich nicht sicher, wo Sie anfangen sollen? Das ZCB hat die folgenden Empfehlungen ausgearbeitet, um Ihnen dabei zu helfen, die Anforderungen der belgischen NIS2-Gesetzgebung in nur 7 Schritten zu erfüllen.

1. **Bin ich von NIS2 betroffen?**

   a. Im Anwendungsbereich: NIS2-Einrichtungen: Mit unserem Scoping Tool[2] stellen Sie fest, ob Ihre Organisation vom belgischen NIS2-Gesetz betroffen ist;
   b. In der Lieferkette: Das ZCB empfiehlt den NIS2 Einrichtungen die Ermittlung der für Ihre Cybersicherheit entscheidenden Organisationen. Diese sollten mindestens die Sicherheitsstufe Basic des CyberFundamentals Framework umsetzen.

2. **NIS2-Einrichtung registrieren**

Alle NIS2-Einrichtungen müssen sich auf Safeonweb@Work[3] registrieren:

- Einrichtungen in den digitalen Sektoren müssen sich spätestens bis zum 18. Dezember 2024 registrieren;
- Alle anderen NIS2-Einrichtungen müssen sich spätestens bis zum 18. März 2025 registrieren.

3. **Vorbereiten der Organisation auf die Meldung und den Umgang mit erheblichen Sicherheitsvorfällen**

Ab dem 18. Oktober 2024 sind alle NIS2-Einrichtungen verpflichtet, dem ZCB alle erheblichen Sicherheitsvorfälle zu melden (siehe Leitfaden).

Diese Meldung kann über die ZCB-Plattform zur Meldung von Sicherheitsvorfällen erfolgen: **https://notif.safeonweb.be** (oder alternativ auch telefonisch an +32 (0)2 501 05 60 **für Notfälle von NIS2-Einrichtungen oder falls die Plattform nicht verfügbar ist**).

Die Meldung von Sicherheitsvorfällen ist nur ein Element eines Notfallplans. Sofern Ihre Organisation noch nicht über einen solchen Plan verfügt, wäre unsere Richtlinienvorlage als Einstieg zu empfehlen.

4. **CyberFundamentals (CyFun®)-Niveau bestimmen**

Wenn Sie sich für unser CyFun® Framework entscheiden, können Sie die für Ihre Organisation geeignete Sicherheitsstufe (Basic, Important oder Essential) mit unserem CyFun®-Auswahlwerkzeug bestimmen.

5. **Cybersicherheits-Schulungen planen**

Um auf Vorstandsebene Managemententscheidungen über Cybersicherheitsstrategien und -maßnahmen treffen zu können, sind Grundkenntnisse des Risikomanagements und der Cybersicherheit unerlässlich. Das ZCB empfiehlt, die Schulung der Führungskräfte vor April 2025 einzuplanen. Neben den Führungskräften sind immer auch die Mitarbeiter als Teil der Cybersicherheitsmaßnahmen zu schulen.

6. **Sicherheitsmaßnahmen umsetzen**

Zur Erreichung der NIS2-Konformität können NIS2-Einrichtungen die 3 Schritte des CyFun®-Frameworks nutzen:

1) Durchführung einer Lückenanalyse und Selbstbewertung mit dem CyFun® Self-Assessment Tool;
2) Umsetzung der erforderlichen Maßnahmen. Ihr Umsetzungsplan sieht die schrittweise Umsetzung von Cybersicherheitsmaßnahmen unter Berücksichtigung der im nachfolgenden Schritt 7 genannten Fristen vor;
3) Aktualisierung der Selbstbeurteilung und Einholen der erforderlichen Nachweise zur Bestätigung der Umsetzung.

[2] https://atwork.safeonweb.be/de/nis2

[3] https://atwork.safeonweb.be/de/register-my-organisation

7. Ihre Cybersicherheit überprüfen lassen

Wesentliche Einrichtungen müssen ihre Umsetzung regelmäßig durch Dritte bewerten und überprüfen lassen. Eine Möglichkeit ist eine CyFun®-Zertifizierung durch eine akkreditierte und autorisierte Konformitätsbewertungsstelle (CAB). Wesentliche Einrichtungen müssen bis zum 18 April 2026 das Sicherheitsniveau „Basic“ oder „Important“ erreichen. Das abschließende Niveau muss bis zum 18 April 2027 zertifiziert werden.
Wichtige Einrichtungen können sich im Rahmen von CyFun® der gleichen regelmäßigen Konformitätsbewertung unterziehen, die ihnen eine Konformitätsvermutung verleiht.

Das Vorliegen des entsprechenden CyFun®-Labels oder -Zertifikats kann für den Vorstand und das Management übrigens sehr wichtig werden, wenn im Falle eines Sicherheitsvorfalls die Einhaltung der Vorschriften nachgewiesen werden muss.

I. Warum NIS2? Und für wen?

Netzwerk- und Informationssysteme sind durch die digitale Transformation und die Vernetzung der Gesellschaft zu einem zentralen Bestandteil unseres alltäglichen Lebens geworden. Viele kritische gesellschaftliche und wirtschaftliche Aktivitäten hängen nun von ihrem reibungslosen Betrieb ab.

Diese Entwicklung hat zu einer sich ständig ausweitenden Vielfalt von Cyberbedrohungen und Cybervorfällen geführt. Diese stellen für die breite Öffentlichkeit, Unternehmen und Behörden eine reale Sicherheitsbedrohung dar. In kritischen Sektoren kann ein Cybersicherheitsvorfall heute mit großer Wahrscheinlichkeit schwerwiegende Betriebsunterbrechungen mit Auswirkungen auf Personen oder Unternehmen sowie erhebliche Sach-, Körper- oder immaterielle Schäden verursachen.

Alle Bürger, Unternehmen und Behörden müssen sich daher bewusst sein, wie wichtig es ist, sich präventiv gegen Cyberbedrohungen und Cybervorfälle zu schützen.

Die nachfolgende Infografik stellt das NIS2-Gesetz im Überblick vor:

II. Anwendungsbereich

Organisationen fallen (außer Ausnahmen) im Prinzip unter das belgische NIS2-Gesetz, wenn sie:

1. innerhalb der Europäischen Union eine in Anhang I oder II des NIS2-Gesetzes aufgeführte Dienstleistung erbringen;
2. die in der Empfehlung 2003/361/EG festgelegte Größe eines mittleren Unternehmens überschreiten, d. h. mindestens 50 Vollzeitbeschäftigte oder einen Jahresumsatz bzw. eine Jahresbilanzsumme von mehr als 10 Mio. Euro aufweisen; und
3. in Belgien niedergelassen sind.

A. DIE GRÖßE („SIZE-CAP“)

Die Größe einer Einrichtung wird auf Grundlage des Anhangs I der Empfehlung 2003/361/EG der Europäischen Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (die „Empfehlung“) berechnet.

Zur Größenbestimmung werden zwei Kriterien herangezogen: Mitarbeiterzahl (gemessen in Vollzeitäquivalenten (VZÄ)[4]) und Finanzsummen (Jahresumsatz und/oder Jahresbilanzsumme). Von einigen Ausnahmen abgesehen[5] findet das NIS2-Gesetz nur auf Organisationen Anwendung, die gemäß der Empfehlung mindestens als mittlere Unternehmen einzustufen sind. Mittlere Unternehmen beschäftigen mindestens 50 VZÄ oder weisen einen Jahresumsatz und/oder eine Jahresbilanzsumme von über 10 Mio. Euro auf.

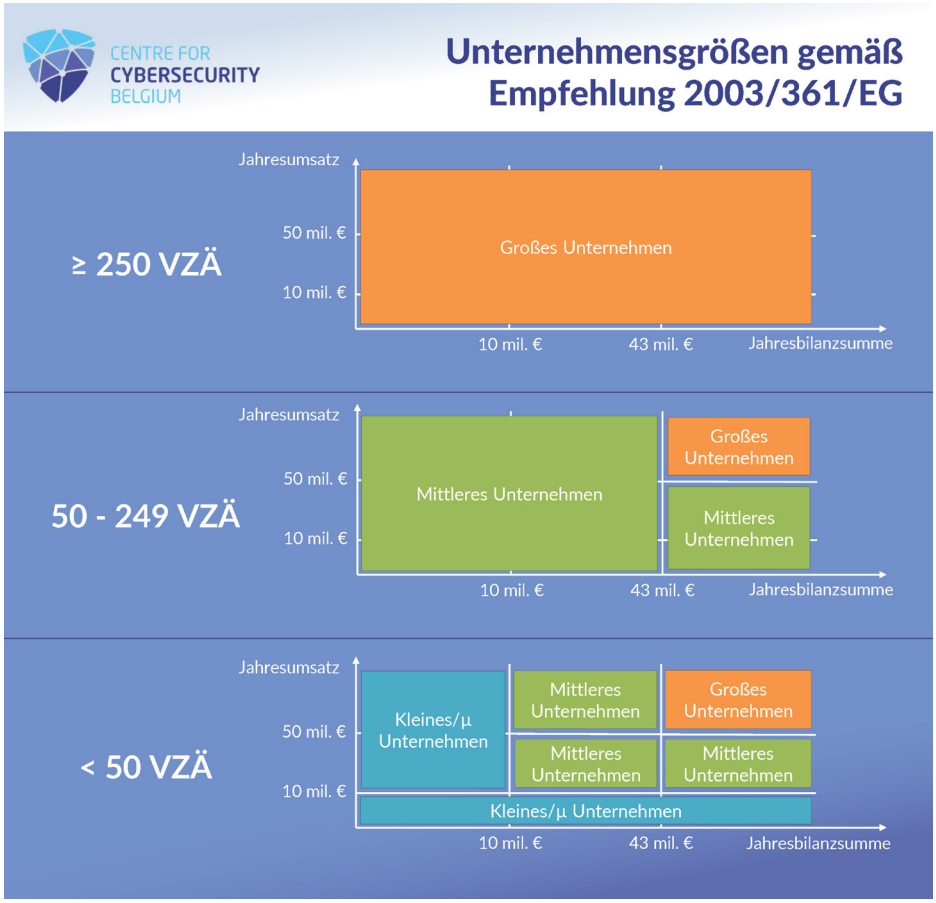
Wie genau diese beiden Kriterien ermittelt werden, ist im Anhang der Empfehlung selbst oder im „Benutzerleitfaden der Kommission zur KMU-Definition“[6] nachzulesen. Dabei ist jedoch zu beachten, dass ein Unternehmen sich entweder für die Einhaltung der Umsatz-Obergrenze oder für die Bilanzsumme entscheiden kann. Es kann eine der beiden finanziellen Obergrenzen überschreiten, ohne dass dies Auswirkungen auf seinen KMU-Status hat. Wir betrachten daher nur den niedrigsten der beiden Beträge.

Die Grafik auf der folgenden Seite stellt die verschiedenen Unternehmensgrößen visuell dar.

[4] Vollzeitäquivalente (VZÄ) (bzw. „Jahresarbeitseinheiten (JAE)” laut Empfehlung) geben die Zahl der Personen wieder, die in dem betroffenen Unternehmen oder auf Rechnung dieses Unternehmens während des gesamten Berichtsjahres einer Vollzeitbeschäftigung nachgegangen sind. Für die Arbeit von Personen, die nicht das ganze Jahr gearbeitet haben oder die im Rahmen einer Teilzeitregelung tätig waren, und für Saisonarbeit wird der jeweilige Bruchteil an JAE gezählt. Empfehlung und Benutzerleitfaden führen die zu berücksichtigenden Beschäftigten detailliert auf.

[5] Siehe Seite 7-8.

[6] https://op.europa.eu/de/publication-detail/-/publication/756d9260-ee54-11ea-991b-01aa75ed71a1



Die Empfehlung sieht insbesondere weiterhin vor, dass die Berechnung der Größe einer Organisation als Teil einer Unternehmensgruppe (sogenannte „Partnerunternehmen“ oder „verbundene Unternehmen“) eine Konsolidierung der Daten der einzelnen Konzerngesellschaften voraussetzt. Weitere Hinweise sind dem bereits erwähnten Benutzerleitfaden der Kommission sowie dem online verfügbaren „SME self-assessment questionnaire“ (Fragebogen zur Selbstbewertung von KMU)[7] zu entnehmen.

Allerdings gilt es bei der Anwendung der Empfehlung im Zusammenhang mit dem NIS2-Gesetz zwei wichtige Besonderheiten zu beachten:

1) Auf die Konsolidierung der Daten der einzelnen Konzerngesellschaften kann unter bestimmten Umständen verzichtet werden, wenn die Netzwerk- und Informationssysteme der jeweiligen Organisation unabhängig von denen der verbunden oder Partnerunternehmen sind;

2) Bei der Größenbestimmung einer Organisation bleiben die Anzahl der Beschäftigten und die Finanzbeträge einer öffentlichen Einrichtung unberücksichtigt, wenn diese die Organisation kontrolliert.

Kombiniert man die verschiedenen möglichen Größen mit dem Dienstleistungskriterium, ergibt sich der folgende Geltungsbereich (mit einigen Ausnahmen[8]):

	Mittleres Unternehmen	**Großes Unternehmen**
Dienste gemäß Anhang I	Wichtige NIS2-Einrichtung	Wesentliche NIS2-Einrichtung
Dienste gemäß Anhang II	Wichtige NIS2-Einrichtung	Wichtige NIS2-Einrichtung

Bei dem Größenkriterium gelten allerdings einige Ausnahmen. Bestimmte Einrichtungsarten unterliegen dem Geltungsbereich des NIS2-Gesetzes unabhängig von ihrer Größe:

[7] https://ec.europa.eu/growth/tools-databases/SME-Wizard/

[8] Siehe Liste unterhalb der Tabelle.

- Qualifizierte Vertrauensdiensteanbieter (wichtig);
- Nicht qualifizierte Vertrauensdiensteanbieter (wichtig, wenn es sich um ein Kleinst-, kleines oder mittlere Unternehmen handelt, und wesentlich, wenn es sich um ein großes Unternehmen handelt);
- DNS-Dienstanbieter (wesentlich);
- TLD-Namensregistrierung (wesentlich);
- Einrichtungen, die Domänennamenregistrierungsdienste erbringen (nur für die Registrierungspflicht);
- Anbieter öffentlicher elektronischer Kommunikationsnetze (wesentlich);
- Anbieter von öffentlich zugänglichen elektronischen Kommunikationsdiensten (wesentlich);
- Einrichtungen, die als Betreiber kritischer Infrastrukturen gemäß dem Gesetz vom 1 Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen identifiziert wurden (wesentlich);
- Einrichtungen der öffentlichen Verwaltung, die vom Föderalstaat abhängen (wesentlich).

Unabhängig von diesen Vorschriften ist die nationale Cybersicherheitsbehörde (das ZCB) auch in der Lage, Einrichtungen ausdrücklich als "wesentlich" oder "wichtig" zu identifizieren, z. B. wenn sie der einzige Anbieter eines Dienstes sind oder wenn die Unterbrechung des bereitgestellten Dienstes erhebliche Auswirkungen auf die öffentliche Sicherheit, die öffentliche Ordnung oder die öffentliche Gesundheit haben könnte.

B. ERBRACHTE DIENSTLEISTUNGEN

Das Dienstleistungskriterium verlangt von einer Organisation, dass sie jede ihrer für Dritte in allen Sektoren und Teilsektoren erbrachten Dienstleistungen vollständig analysiert. Selbst die kleinsten Nebendienstleistungen können nämlich dazu führen, dass die gesamte Organisation unter das NIS2-Gesetz fällt, sofern in der Definition der betreffenden Dienstleistung nicht etwas anderes angegeben ist. Anhang I und II (oder die Definitionen[9]) führen die vom NIS2-Gesetz erfassten Leistungen detailliert nach Sektoren getrennt auf:

Sektoren mit hoher Kritikalität (Anhang I)	Sonstige kritische Sektoren (Anhang II)
1. Energie a. Elektrizität b. Fernwärme und -kälte c. Erdöl d. Erdgas e. Wasserstoff 2. Transport a. Luftverkehr b. Schienenverkehr c. Schifffahrt d. Straßenverkehr 3. Bankwesen 4. Finanzmarktinfrastruktur 5. Gesundheitswesen 6. Trinkwasser 7. Abwasser 8. Digitale Infrastruktur 9. Verwaltung von IKT-Diensten (B2B) 10. Öffentliche Verwaltung 11. Raumfahrt	1. Post- und Kurierdienste 2. Abfallwirtschaft 3. Produktion, Herstellung und Handel mit chemischen Stoffen 4. Produktion, Verarbeitung und Vertrieb von Lebensmitteln 5. Verarbeitendes Gewerbe/Herstellung von Waren a. Herstellung von Medizinprodukten und In-vitro-Diagnostika b. Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen c. Herstellung von elektrischen Ausrüstungen d. Maschinenbau e. Herstellung von Kraftwagen und Kraftwagenteilen f. Sonstiger Fahrzeugbau 6. Anbieter digitaler Dienste 7. Forschung

Die Definitionen dieser Dienstleistungen sollten unbedingt herangezogen werden, um zu überprüfen, ob sie den tatsächlichen Dienstleistungen der jeweiligen Organisation entsprechen.

Die Grafiken auf Seiten 23 und 24 stellen den Geltungsbereich des Gesetzes im Überblick dar.

[9] Siehe Artikel 8 des NIS2-Gesetzes.

C. NIEDERLASSUNG

Im Wesentlichen gilt das belgische NIS2-Gesetz nur für Einrichtungen mit Sitz in Belgien, die ihre Leistungen in der EU erbringen oder dort tätig sind. Unabhängig von der gewählten Rechtsform beinhaltet der Begriff „Niederlassung" lediglich die tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung, unabhängig von der gewählten Rechtsform, ob es sich dabei um den Sitz, eine einfache Zweigniederlassung oder eine Tochtergesellschaft mit Rechtspersönlichkeit handelt.

Es gelten jedoch drei Ausnahmen von der Niederlassungsregel in Belgien:

1) Das belgische NIS2-Gesetz gilt für Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste, die ihre Dienste in Belgien anbieten;

2) Das belgische NIS2-Gesetz gilt für DNS-Dienstanbieter, TLD-Namensregister, Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter verwalteter Dienste, Anbieter verwalteter Sicherheitsdienste sowie Anbieter von Online-Marktplätzen, von Online-Suchmaschinen oder von Plattformen für Dienste sozialer Netzwerke, wenn sie ihre Hauptniederlassung in Belgien oder ihren gesetzlichen Vertreter für die EU in Belgien haben;

3) Das belgische NIS2-Gesetz gilt für Einrichtungen der öffentlichen Verwaltung, die vom Belgischen Staat gegründet wurden.

Wenn eine Einrichtung mehrere Niederlassungen in verschiedenen EU-Mitgliedstaaten hat, unterliegt sie den Umsetzungsgesetzen in jedem betroffenen Mitgliedstaat. Die verschiedenen zuständigen nationalen Behörden werden bei Inspektionen und der Meldung von erheblichen Sicherheitsvorfällen zusammenarbeiten.

D. IDENTIFIZIERUNG UND LIEFERKETTE

Im Ergebnis einer umfassenden Analyse des Geltungsbereichs des NIS2-Gesetzes kann sich herausstellen, dass bestimmte Organisationen tatsächlich nicht unter dieses Gesetz fallen. Gleichwohl können auch diese Organisationen auf zwei Arten vom NIS2-Gesetz betroffen sein.

Erstens kann die nationale Cybersicherheitsbehörde (das ZCB) bestimmte Organisationen aufgrund ihrer Kritikalität anhand von vier Kriterien auch unabhängig von ihrer Größe als wesentliche oder wichtige Einrichtungen im Sinne des NIS2-Gesetzes identifizieren. Dies erfolgt immer in Abstimmung mit der betroffenen Einrichtung und anderen Behörden gemäß Artikel 11 des NIS2-Gesetzes.

Zweitens kann eine Organisation als Teil der direkten Lieferkette einer NIS2-Einrichtung zum Beispiel aufgrund einer vertraglichen Verpflichtung gegenüber dieser Einrichtung von Maßnahmen zum Management von Cybersicherheitsrisiken veranlasst werden. In diesem Zusammenhang rät das ZCB allen betroffenen Organisationen, zumindest die im CyberFundamentals (CyFun®) Framework Level „Basic" festgelegten Maßnahmen einzuhalten[10].

E. ZUSAMMENHANG ZWISCHEN NIS2 UND DORA

Das NIS2-Gesetz sieht vor, dass die Titel 3 bis 5 des Gesetzes (Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit, Aufsicht und Sanktionen, spezifische Bestimmungen für die Bereiche der öffentlichen Verwaltung) nicht für Einrichtungen in den Sektoren Bankwesen und Finanzmarkt gelten, die in den Anwendungsbereich von DORA fallen. Letzteres ist die Abkürzung für die EU-Verordnung 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operative Widerstandsfähigkeit des Finanzsektors, die Anforderungen an die Sicherheit der Netzwerk- und Informationssysteme der in ihren Anwendungsbereich fallenden Finanzinstitute festlegt.

Dies ergibt sich aus der NIS2-Richtlinie, nämlich aus dem Ausschluss sektorspezifischer Rechtsakte der Union (sogenannte *lex specialis*), in denen solche Rechtsakte NIS2-Einrichtungen dazu verpflichten, Maßnahmen zum

[10] https://cyfun.be

Risikomanagement im Bereich der Cybersicherheit zu ergreifen oder erhebliche Sicherheitsvorfälle zu melden, und in denen diese Anforderungen in ihrer Wirkung mindestens den in NIS2 festgelegten Verpflichtungen entsprechen.

In der Praxis können sich alle NIS2-Einrichtungen, die unter DORA fallen, auf die Einhaltung von DORA in Bezug auf die in den Titeln 3 bis 5 des NIS2-Gesetzes festgelegten Verpflichtungen beschränken. Dazu gehören die Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit, die obligatorische und freiwillige Meldung von Sicherheitsvorfällen, die Aufsicht, und die administrativen Maßnahmen und Geldbußen. Alle anderen Bestimmungen des NIS2-Gesetzes, wie die Bestimmungen zur Registrierung und zur Zuständigkeit des ZCB, gelten jedoch weiterhin für diese Einrichtungen.

III. Verpflichtungen

A. REGISTRIERUNG

NIS2-Einrichtungen müssen sich beim ZCB registrieren, wenn sie in den Geltungsbereich des belgischen NIS2-Gesetzes fallen. In der Praxis erfolgt diese Die Registrierung über ein Onlineformular auf Safeonweb@Work[11].

Die Frist für die Registrierung hängt von der Art der Einrichtung ab. Grundsätzlich haben wesentliche und wichtige Einrichtungen sowie Einrichtungen zur Registrierung von Internet-Domain-Namen ab Inkrafttreten des Gesetzes **5 Monate Zeit** für die Registrierung, das heißt bis spätestens dem **18. März 2025**[12].

Für die nachfolgend aufgeführten Einrichtungen der digitalen Sektoren gelten leicht angepasste Fristen:

- DNS-Diensteanbieter;
- TLD-Namenregister;
- Einrichtungen, die Domänennamen-Registrierungsdienste erbringen;
- Anbieter von Cloud-Computing-Diensten;
- Anbieter von Rechenzentrumsdiensten;
- Betreiber von Inhaltszustellnetzen;
- Anbieter von verwalteten Diensten;
- Anbieter von verwalteten Sicherheitsdiensten;
- Anbieter von Online-Marktplätzen;
- Anbieter von Online-Suchmaschinen;
- Anbieter von Plattformen für Dienste sozialer Netzwerke.

Diese Einrichtungen müssen sich mit anderen Informationen innerhalb von **2 Monaten** nach Inkrafttreten des Gesetzes, d. h. spätestens bis zum **18. Dezember 2024**, registrieren[13].

Jede Einrichtung muss das ZCB umgehend (nach spätestens 2 Wochen) von geänderten Angaben in Kenntnis setzen.

B. RISIKOMANAGEMENTMASSNAHMEN IM BEREICH DER CYBERSICHERHEIT

Die Risikomanagementmaßnahmen im Bereich der Cybersicherheit sind technische, operative und organisatorische Maßnahmen, die der betroffenen Einrichtungen erlauben ihre Netz- und Informationssysteme gegen Sicherheitsrisiken abzusichern und Auswirkungen von Sicherheitsvorfällen zu verhindern oder zu minimieren. Diese Maßnahmen sind möglichst an den Stand der Technik, die geltenden Normen und ihre Kosten anzupassen.

Für die einzelnen Einrichtungen müssen die Maßnahmen zweckmäßig, angemessen und auf die ermittelten Risiken, die konkrete Risikoexposition der Einrichtung, ihre Große sowie die Wahrscheinlichkeit und Schwere von Sicherheitsvorfällen abgestimmt sein.

Das Gesetz führt 11 Mindestmaßnahmen auf, die von jeder NIS2-Einrichtung umzusetzen sind[14]. Eine Übersicht finden Sie in der Grafik auf der nächsten Seite.

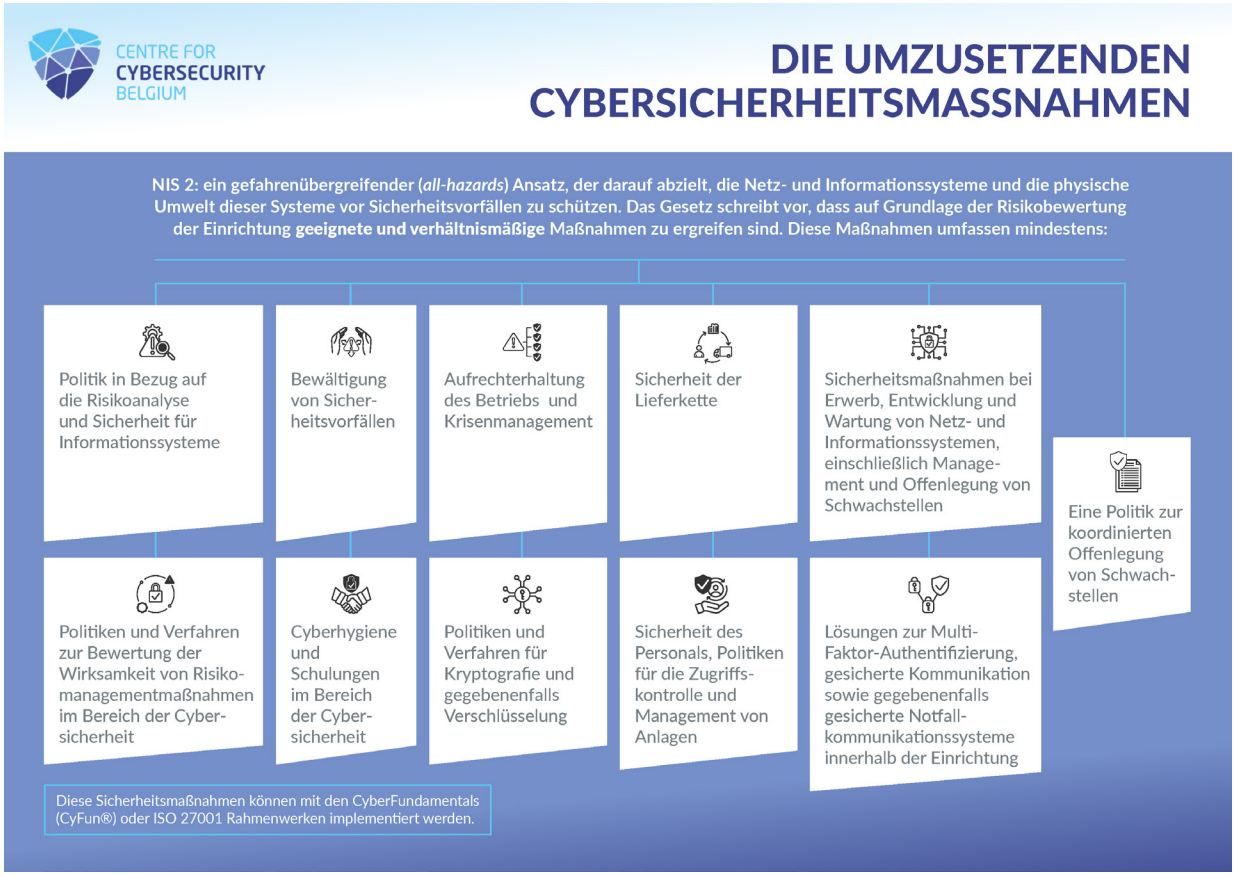
---

[11] https://atwork.safeonweb.be/de/register-my-organisation

[12] Die Informationen, die innerhalb der normalen Registrierungsfrist bereitgestellt werden müssen, finden Sie in Artikel 13, §1 des NIS2-Gesetzes.

[13] Die Informationen, die im Rahmen der angepassten Regelung bereitgestellt werden müssen, finden Sie in Artikel 14, §1 des NIS2-Gesetzes.

[14] Siehe auch den Durchführungsrechtsakt der Kommission: https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks



Das ZCB hat mit dem „CyberFundamentals Framework“ (CyFun®) ein kostenloses und öffentlich zugängliches Rahmenwerk erstellt, das all diese Punkte abdeckt. Damit können NIS2-Einrichtungen die Umsetzung der verpflichtend zu ergreifenden, zweckmäßigen und angemessenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit gewährleisten[15].

C. SICHERHEIT DER LIEFERKETTE

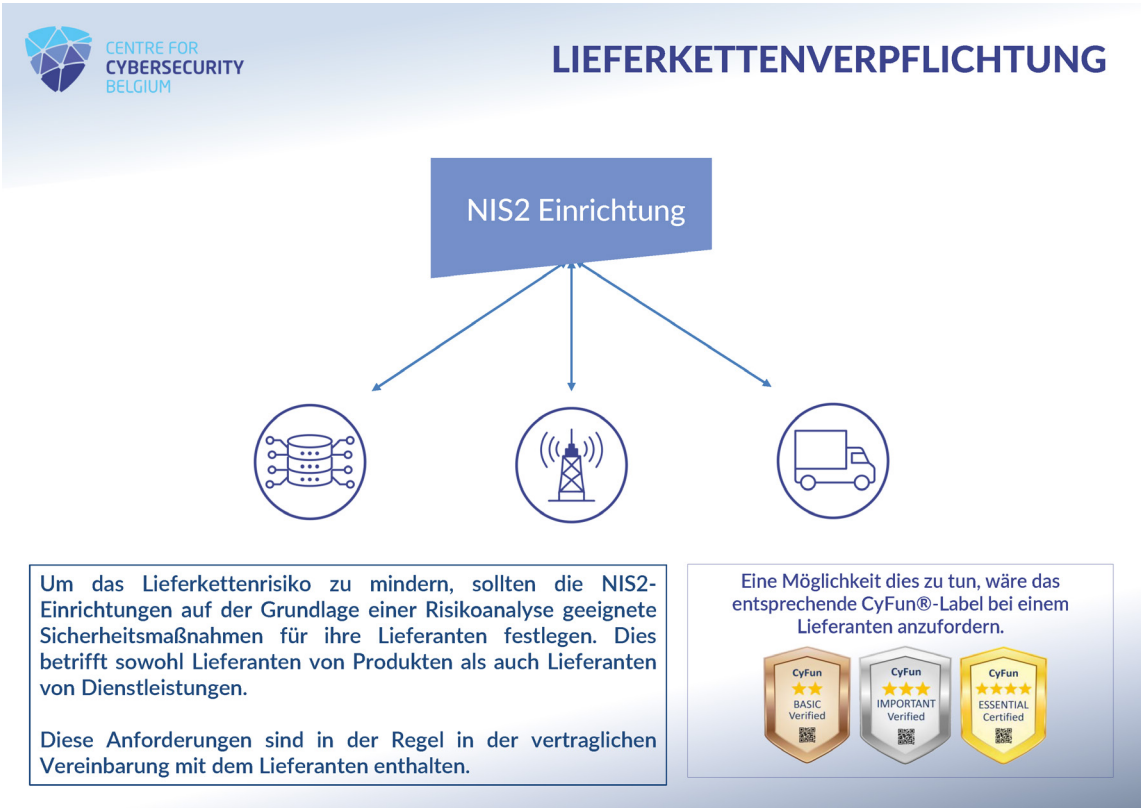
Das NIS2-Gesetz verlangt von allen betroffenen Einrichtungen das Ergreifen zweckmäßiger und angemessener Maßnahmen zur Beherrschung von Cybersicherheitsrisiken. Eine der spezifischen Maßnahmen betrifft die *„**Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern“*.

Diese Verpflichtung wirkt in zwei Richtungen: Einerseits müssen NIS2-Einrichtungen von den Organisationen in ihrer Lieferkette (wie direkte Anbieter oder Diensteanbieter) entsprechende Risikomanagementmaßnahmen im Bereich der Cybersicherheit verlangen und diese überwachen, andererseits müssen nicht von NIS2 betroffene Einrichtungen derlei Maßnahmen in zweckmäßigem und angemessenem Umfang ergreifen.

Dabei legt das NIS2-Gesetz nicht fest, wie dieser Verpflichtung durch die NIS2-Einrichtungen nachzukommen ist. So liegt insbesondere die Überprüfung der pflichtgemäßen Umsetzung der genannten Maßnahmen entlang der direkten Lieferkette bei den Einrichtungen selbst. Um den Nachweis der Pflichterfüllung entlang der zu vereinfachen, empfiehlt das ZCB allen NIS2-Einrichtungen, von den Organisationen in der Lieferkette vertraglich ein Label oder Zertifikat zum Beispiel gemäß dem CyberFundamentals (CyFun®) Framework zu verlangen.

Das ZCB empfiehlt ebenfalls allen nicht dem NIS2-Gesetz unterliegenden Einrichtungen die Einführung entsprechender zweckmäßiger und angemessener Risikomanagementmaßnahmen für den Fall, dass sie in die Lieferkette einer NIS2-Einrichtung geraten. Hier hilft wiederum das CyFun® Framework bei der Ermittlung und Umsetzung konkreter Maßnahmen, wie sie gegebenenfalls verlangt werden können.

[15] Für weitere Hinweise siehe Kapitel IV, Abschnitt B.



D. MELDUNG VON SICHERHEITSVORFÄLLEN (SIEHE LEITFADEN)

Das NIS2-Gesetz verpflichtet NIS2-Einrichtungen ebenfalls dazu dem ZCB all „erheblichen“ Sicherheitsvorfälle zu melden. Laut Definition im Gesetz ist ein solcher Sicherheitsvorfall:

„Jeder Sicherheitsvorfall, der erhebliche Auswirkungen auf die Erbringung einer der in den Anhängen I und II des Gesetzes aufgeführten Dienstleistungen hat und der:

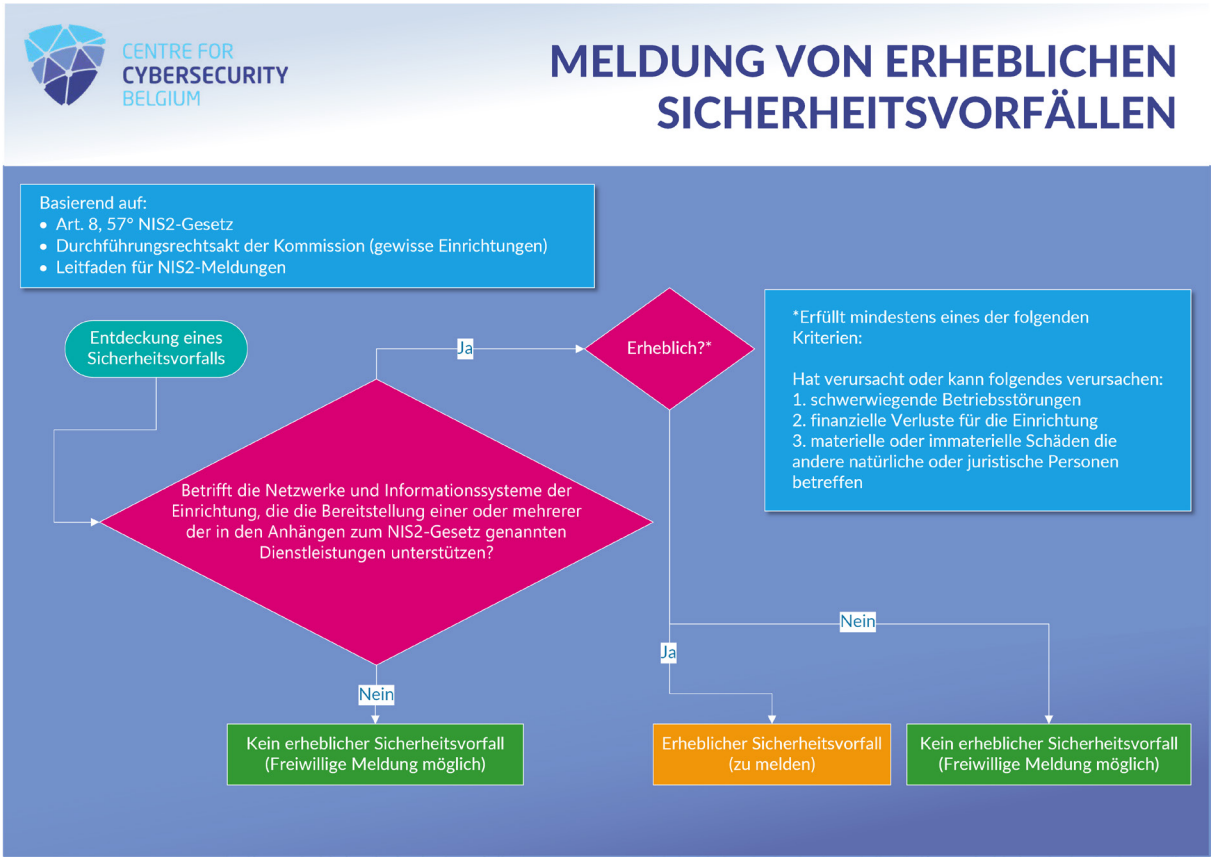
1° schwerwiegende Betriebsstörungen eines der in den in Anhang I und II aufgeführten Sektoren oder Teilsektoren erbrachten Dienstes oder einen finanziellen Verlust für die betreffende Einrichtung verursacht hat oder verursachen kann, oder
2° andere natürliche oder juristische Personen durch erhebliche materielle, persönliche oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.“

Der Sicherheitsvorfall muss sich auf die Erbringung einer der Dienste auswirken, die in den in Beilage I und II des Gesetzes aufgeführten Sektoren oder Teilsektoren erbracht werden, d.h. er **muss sich auf die Netzwerk- und Informationssysteme auswirken, die die Erbringung einer oder mehrerer dieser Dienste unterstützen** (z.B. Stromverteilung).

Die Meldepflicht bezieht sich daher nur auf Netzwerk- und Informationssysteme, auf die die betroffene Einrichtung angewiesen ist, um die in den Beilagen des Gesetzes aufgeführten Dienste zu erbringen. Ein Sicherheitsvorfall, der ein isoliertes Informationssystem betrifft, das nicht mit der Bereitstellung der genannten Dienste in Verbindung steht, muss daher nicht gemeldet werden.

Zweitens muss die Auswirkung erheblich sein, d.h. sie muss mindestens eine der folgenden drei Situationen verursachen oder verursachen können:

- eine **schwerwiegende Betriebsstörung** bei einer der erbrachten Dienstleistungen (in den Sektoren oder Teilsektoren, die in Beilage I und II des NIS2-Gesetzes aufgeführt sind);
- **finanzielle Verluste für die betroffene Einrichtung**;
- **erhebliche materielle, körperliche oder moralische Schäden für andere natürliche oder juristische Personen**.



Jeder bei einer NIS2-Einrichtung auftretende Sicherheitsvorfall, der dieser Definition entspricht, ist dem ZCB zu melden. Der Meldevorgang umfasst mehrere Stufen (siehe die nachfolgende Abbildung):

1) die Einrichtung übermittelt **unverzüglich, in jedem Fall aber innerhalb von 24 Stunden** nach Kenntnisnahme des erheblichen Sicherheitsvorfalls eine Frühwarnung;
2) die Einrichtung übermittelt **unverzüglich, in jedem Fall aber innerhalb von 72 Stunden (24 Stunden für Vertrauensdiensteanbieter) nach Kenntnisnahme des erheblichen Sicherheitsvorfalls** eine Vorfallmeldung;
3) auf Ersuchen des nationalen CSIRT oder gegebenenfalls der zuständigen sektoralen Behörde übermittelt die Einrichtung einen Zwischenbericht;
4) **spätestens einen Monat nach Meldung des Sicherheitsvorfalls gemäß Punkt 2** übermittelt die Einrichtung einen Abschlussbericht;
5) dauert der Sicherheitsvorfall zum Zeitpunkt der Vorlage des Abschlussberichts noch an, übermittelt die betroffene Einrichtung einen Fortschrittsbericht und anschließend innerhalb eines Monats nach Ende des Sicherheitsvorfalls einen Abschlussbericht.

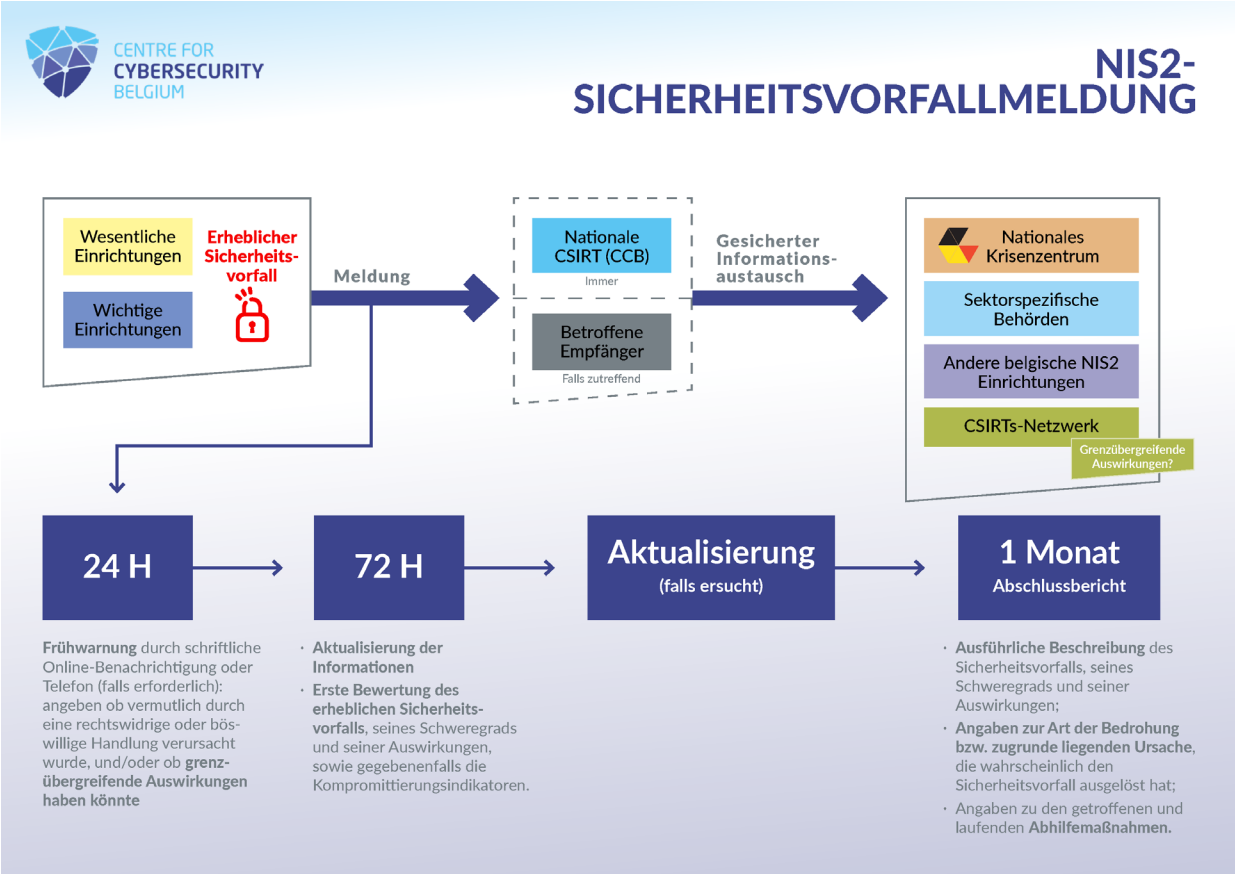
Je nach Schwere des Sicherheitsvorfalls muss die Einrichtung auch die Empfänger ihrer Dienstleistungen über den Sicherheitsvorfall sowie über alle Maßnahmen oder Abhilfemaßnahmen die diese Empfänger als Reaktion ergreifen können informieren. Das ZCB kann die Informationen der Einrichtung je nach Bedarf an andere Behörden weitergeben.

Weitere Informationen zur Meldung von Sicherheitsvorfällen finden Sie in unserem **Leitfaden zur Meldung von NIS2-Sicherheitsvorfällen**[16].

NIS2-Sicherheitsvorfälle können über unser Webformular zur Meldung von Sicherheitsvorfällen gemeldet werden: **https://notif.safeonweb.be/de**.

[16] https://ccb.belgium.be/de/cert/einen-vorfall-melden

Siehe auch den Durchführungsrechtsakt der Kommission: https://digital-strategy.ec.europa.eu/en/library/nis2-commission-implementing-regulation-critical-entities-and-networks



E. VERPFLICHTUNGEN FÜR DIE UNTERNEHMENSLEITUNG

Das NIS2-Gesetz sieht verschiedene Elemente für die Unternehmensleitung von NIS2-Einrichtungen vor:

1) Die Leitungsorgane müssen Risikomanagementmaßnahmen im Bereich der Cybersicherheit genehmigen und deren Umsetzung überwachen.
2) Die Mitglieder von Leitungsorganen müssen eine Schulung absolvieren, um sicherzustellen, dass ihre Kenntnisse und Fähigkeiten ausreichen, um Risiken zu erkennen und Verfahren zum Management von Cybersicherheitsrisiken und deren Auswirkungen auf die von der Einrichtung erbrachten Dienstleistungen zu bewerten;
3) Die Leitungsorgane haften für die Entscheidungen über das Management von Cybersicherheitsrisiken, einschließlich des Managements von Sicherheitsvorfällen;

Diese Maßnahmen zielen darauf ab, Cybersicherheit zu einem zentralen Thema für die Leitungsebene zu machen.

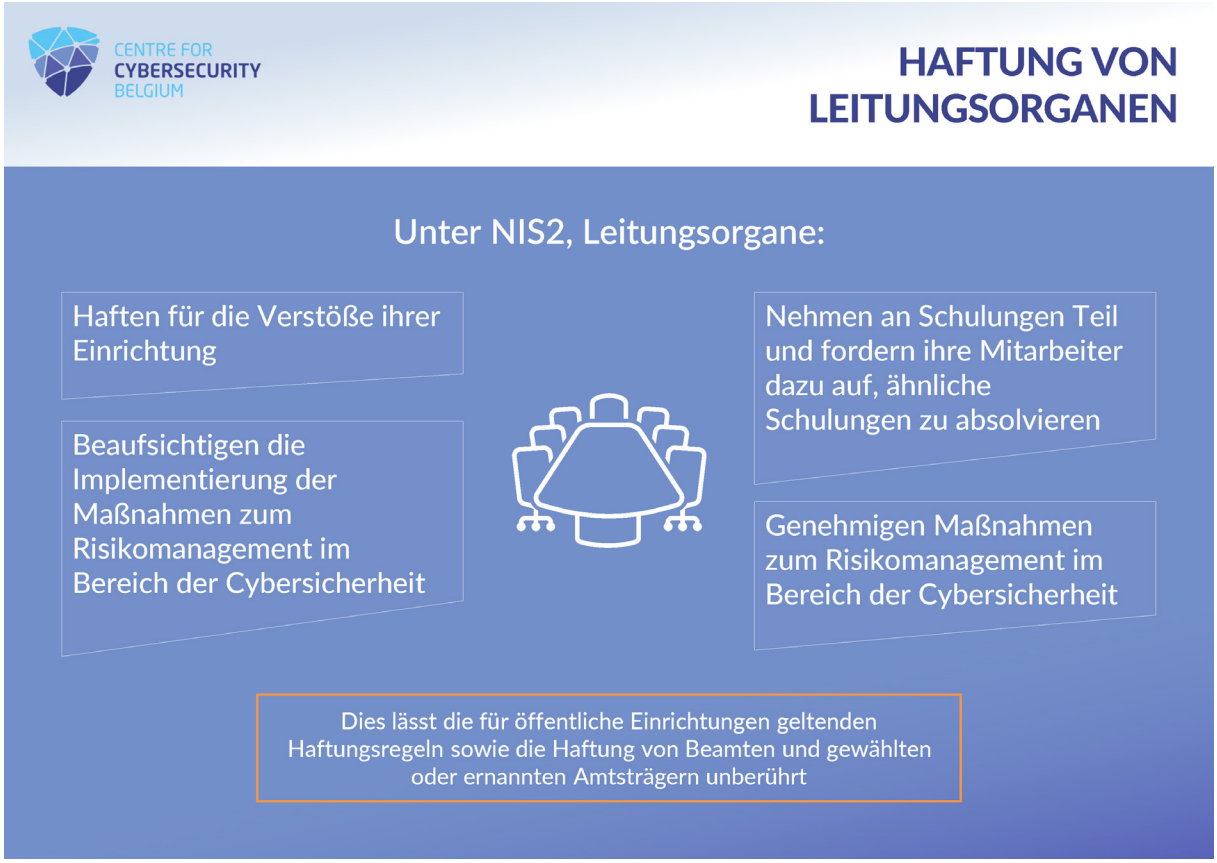
In der Begründung zum NIS2-Gesetz wird „Mitglied eines Leitungsorgans“ wie folgt definiert:

> *Jede natürliche oder juristische Person, die:*
>
> *(i) eine Funktion bei oder in Verbindung mit einer Einrichtung ausübt, die sie dazu berechtigt, (a) die betreffende Einrichtung zu verwalten und zu vertreten oder (b) im Namen und für Rechnung der Einrichtung Entscheidungen zu treffen, die für diese rechtlich bindend sind, oder in einem Organ der Einrichtung an solchen Entscheidungen mitzuwirken, oder*
>
> *(ii) die Kontrolle über die Einrichtung ausübt, d.h. die rechtliche oder tatsächliche Befugnis, einen entscheidenden Einfluss auf die Bestellung der Mehrheit der Verwaltungsratsmitglieder oder Geschäftsführer der Einrichtung oder auf die Ausrichtung ihrer Geschäftsführung auszuüben.*
>
> *Wenn es sich bei der Einrichtung um eine Gesellschaft nach belgischem Recht handelt, wird eine solche Kontrolle gemäß den Artikeln 1:14 bis 1:18 des Gesetzbuches der Gesellschaften und Vereinigungen bestimmt.*

Wenn die Person, deren Rolle untersucht wird, eine juristische Person ist, wird der Begriff "Mitglied eines Leitungsorgans" rekursiv untersucht und umfasst sowohl die betreffende juristische Person als auch jedes Mitglied eines Leitungsorgans der genannten juristischen Person.

Die für öffentliche Einrichtungen sowie die für die Haftung von Beamten und von gewählten oder ernannten Vertretern geltenden Haftungsvorschriften bleiben von diesen Haftungsregeln unberührt.

Es ist zu beachten, dass natürliche Personen, die in einer NIS2-Einrichtung auf der Ebene des Geschäftsführers oder des gesetzlichen Vertreters Führungsaufgaben wahrnehmen, vorübergehend von der Ausübung von Führungsaufgaben in dieser Einrichtung ausgeschlossen werden können, wenn sie gegen die Anforderungen des NIS2-Gesetzes verstoßen.



IV. Aufsicht

A. ALLGEMEINE BESTIMMUNGEN

Bei der Aufsicht unterscheidet das Gesetz zwischen wichtigen und wesentlichen Einrichtungen:

- Wichtige Einrichtungen werden „*ex-post*“ überwacht, d. h. eine Kontrolle findet erst statt, nachdem ein Sicherheitsvorfall eingetreten ist, oder wenn die Aufsichtsbehörde genügend Anhaltspunkte hat um den Verdacht zu hegen, dass eine wichtige Einrichtung gegen das Gesetz verstoßen hat;
- Wesentliche Einrichtungen können sowohl „*ex-pos*t“ als auch „*ex-ante*“ überwacht werden, d. h. sie müssen jederzeit nachweisen können, dass sie die Gesetze einhalten. Zu diesem Zweck verpflichtet das Gesetz wesentliche Einrichtungen zu einer regelmäßigen Konformitätsbewertung.

Eine solche obligatorische regelmäßige Konformitätsbewertung kann auf drei verschiedene Arten erfolgen:

1) Eine Zertifizierung (Stufe Essential) oder Verifizierung (Stufe Important oder Basic) der Einrichtung nach dem **CyberFundamentals (CyFun®) Framework** durch eine akkreditierte und vom ZCB zugelassene Konformitätsbewertungsstelle (CAB) mit dem entsprechenden Anwendungsbereich. Für CyFun muss das CAB von BELAC akkreditiert sein;

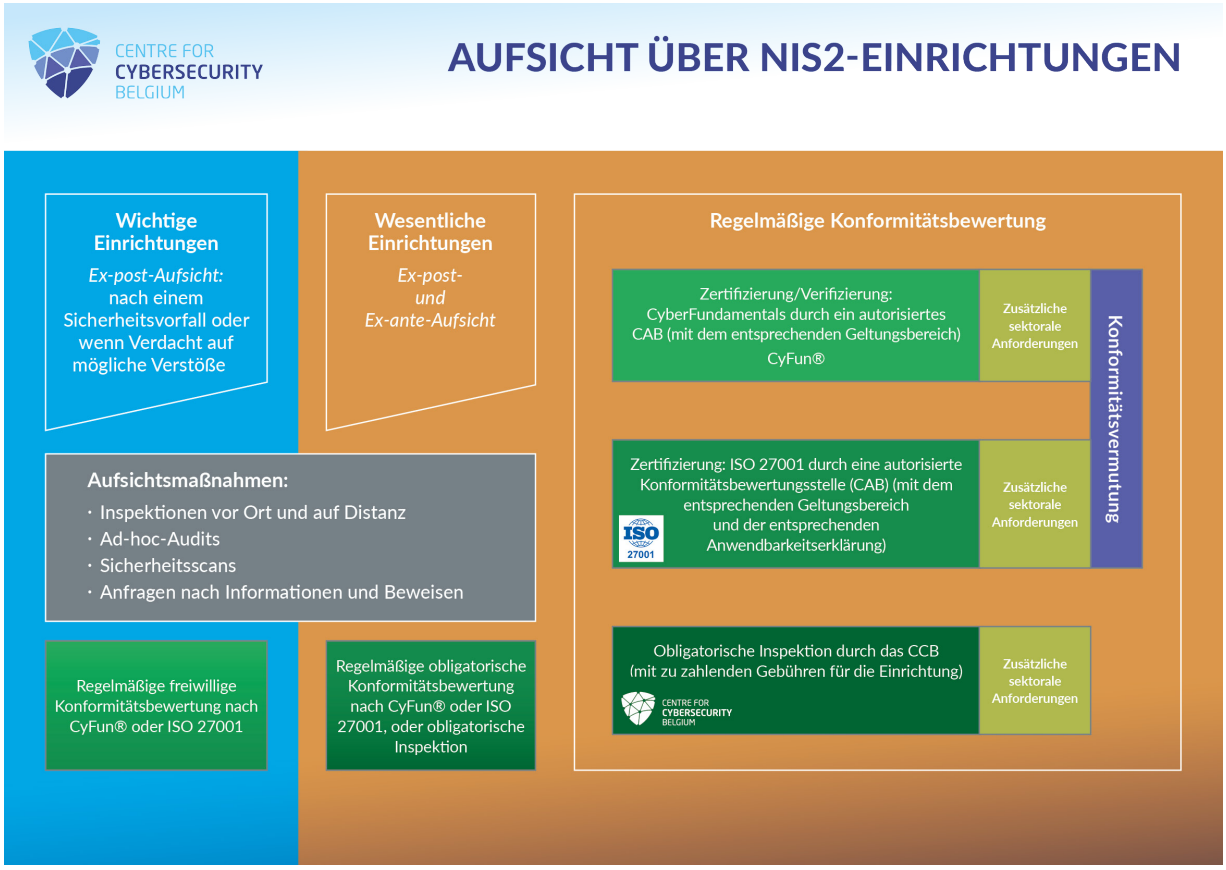
2) Eine Zertifizierung der Einrichtung gemäß der Norm **ISO/IEC 27001**, die von einem akkreditierten CAB mit dem entsprechenden Anwendungsbereich und *Statement of Applicability* ausgestellt wird. Für ISO/IEC 27001 muss das CAB von einer Akkreditierungsstelle akkreditiert werden, die das Multi-Lateral Agreement (MLA) unterzeichnet hat, unter das ISO/IEC 27001 im Rahmen der European co-operation for Accreditation (EA) oder des International Accreditation Forum (IAF) fällt, und ebenfalls vom ZCB zugelassen sein;

3) Eine **Inspektion** durch den Inspektionsdienst des ZCB (diese Dienstleistung ist entgeltpflichtig).

Für alle drei Möglichkeiten kann eine sektorale Behörde zusätzliche Anforderungen festlegen, die von den Einrichtungen in ihrem Sektor zu erfüllen sind. Einrichtungen die sich für die Durchführung der regelmäßigen Konformitätsbewertung gemäß CyFun® oder der ISO/IEC 27001 entscheiden, können gegebenenfalls von einer Konformitätsvermutung profitieren.

Bei seiner Tätigkeit kann der Inspektionsdienst auf Untersuchungen vor Ort oder außerhalb des Unternehmens, Ad-hoc-Audits, aber auch auf Sicherheitsüberprüfungen und allgemeine Informations- und Beweisanfragen zurückgreifen. Alle NIS2-Einrichtungen müssen den Aufforderungen des Inspektionsdienstes jederzeit nachkommen. Andernfalls riskieren sie administrative Maßnahmen und Geldbußen.

Wichtige Einrichtungen können sich auch freiwillig einer regelmäßigen Konformitätsbewertung unterziehen. In diesem Fall können sie nur zwischen CyFun® und ISO/IEC 27001 wählen.



B. DIE CYBERFUNDAMENTALS (CYFUN®)

Das CyberFundamentals (CyFun®) Framework[17] ist ein Rahmenwerk mit konkreten Maßnahmen um:

- Daten zu schützen;
- das Risiko der häufigsten Cyberangriffe erheblich zu reduzieren;
- die Cyber-Resilienz einer Organisation zu erhöhen.

Um der Schwere der Bedrohung, der eine Organisation ausgesetzt ist, gerecht zu werden, gibt es neben der Ausgangsstufe Small drei weitere Sicherheitsstufen: Basic, Important und Essential. Das Rahmenwerk wurde mit Hilfe von Angriffsprofilen des CERT (aus erfolgreichen Angriffen gewonnen) validiert. Die Schlussfolgerung lautet:

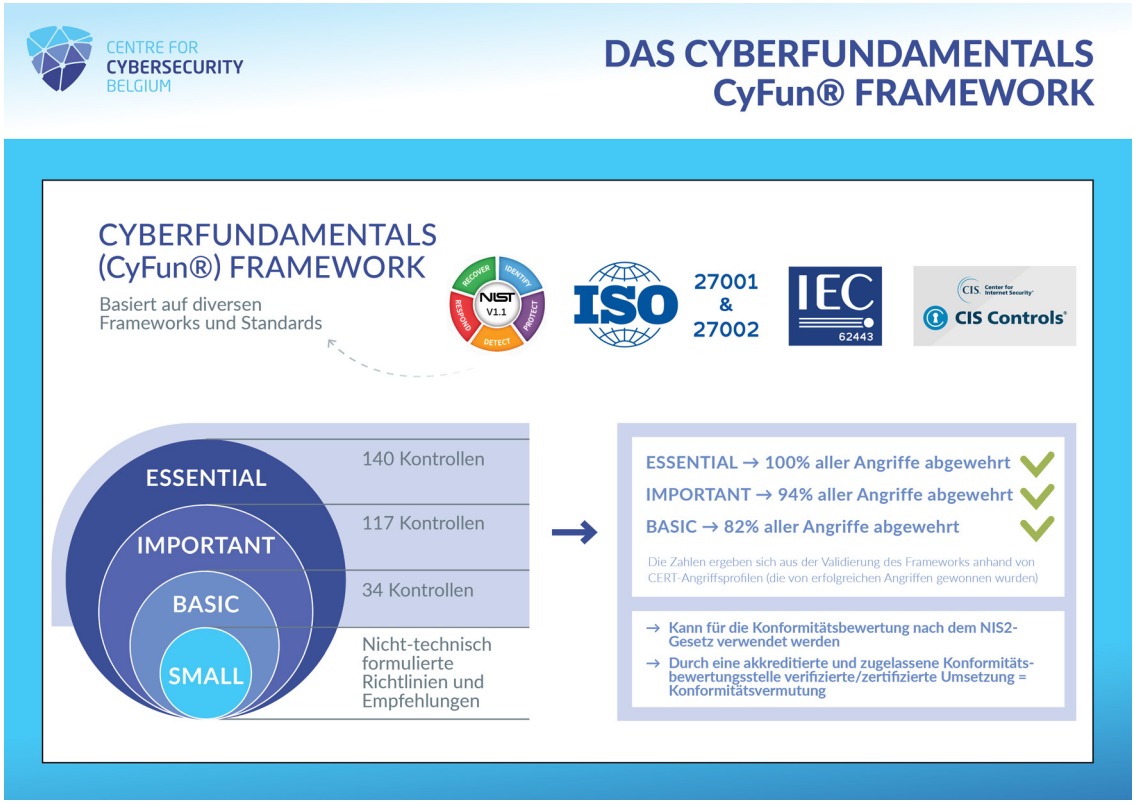
- Maßnahmen der Sicherheitsstufe „Basic" können 82 % der Angriffe abdecken;
- Maßnahmen der Sicherheitsstufe „Important" können 94 % der Angriffe abdecken;
- Maßnahmen der Sicherheitsstufe „Essential" können 100 % der Angriffe abdecken.

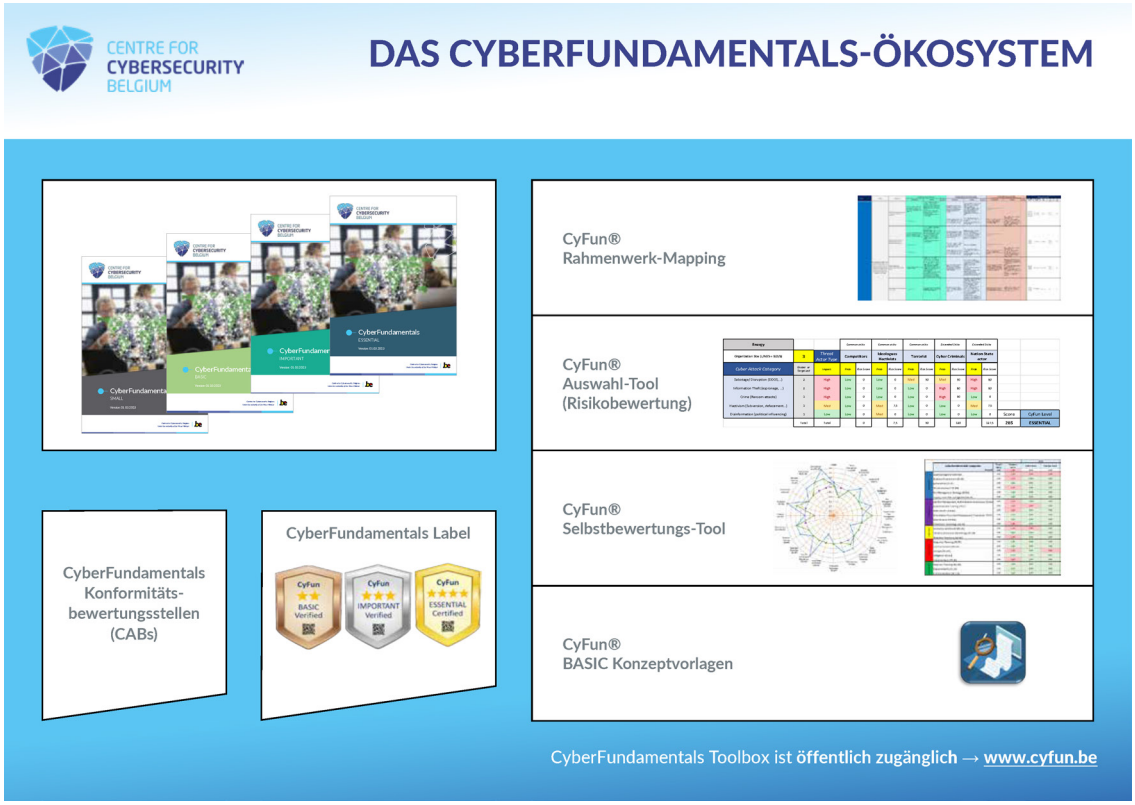
Darüber hinaus ist das CyFun® Framework:

- **Auf anerkannten Normen basiert**: CyFun® wählt relevante Kontrollen auf der Grundlage gemeinsamer Standards wie NIST CSF, ISO/IEC 27001, CIS-Controls und IEC 62443 aus;
- **entspricht den Maßnahmen, die notwendig sind**, um die wichtigsten vom ZCB identifizierten Angriffe zu verhindern;
- **Von jedem selbst verwendbar**: Zu jeder Kontrolle gibt es eine Anleitung, die bei der Implementierung hilft. Das Selbstbewertungstool von CyFun hilft den Überblick über eine Implementierung zu behalten;
- **Zur Validierung einer Implementierung**: Man kann seine Implementierung validieren, indem man eine Bewertung durch eine zugelassene Konformitätsbewertungsstelle anfordert. Diese Bescheinigung dient als Nachweis für die Implementierung gegenüber Kunden und Behörden (z. B. zur Einhaltung von NIS2).

[17] https://cyfun.be

Das CyFun® Framework ist bezüglich NIS2 für die regelmäßige Konformitätsbewertung wesentlicher Einrichtungen, aber auch für wichtige Einrichtungen besonders nützlich. Es ist kostenlos verfügbar und bietet unkomplizierte Lösungen für Risikobewertung, Selbstbewertung und die konkrete Umsetzung der vom NIS2-Gesetz geforderten Mindestmaßnahmen für das Risikomanagement im Bereich der Cybersicherheit. Darüber hinaus wird bei einer validierten oder zertifizierten Implementierung des CyFun®-Frameworks davon ausgegangen, dass die betreffenden Einrichtungen im Rahmen der Aufsicht gemäß NIS2 konform sind. Das ZCB empfiehlt allen NIS2-Einrichtungen nachdrücklich, das CyFun®-Framework zu verwenden.





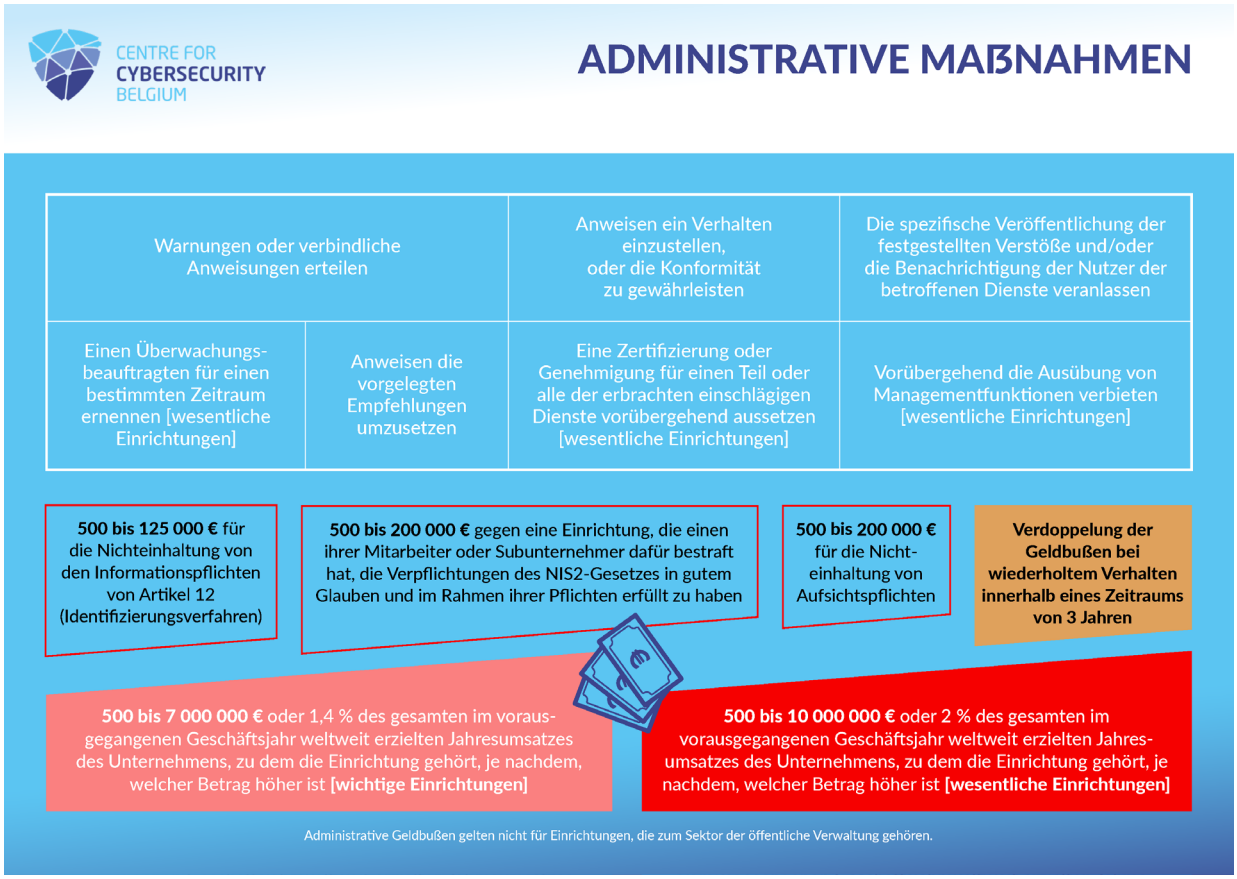
V. Sanktionen

NIS2-Einrichtungen, die ihren Verpflichtungen nicht nachkommen, können mit einer Reihe von administrativen Maßnahmen und Geldbußen belegt werden.

Das Ziel des ZCB ist, in enger Zusammenarbeit mit allen betroffenen Einrichtungen, ein hohes Cybersicherheitsniveau im ganzen Land zu erreichen. Dennoch gibt es Situationen, in denen Sanktionen erforderlich sein können. Zu diesem Zweck sieht das Gesetz (Titel 4, Kapitel 2) ein spezielles Verfahren vor, das die Interaktion zwischen dem ZCB und der betroffenen Einrichtung regelt. Dieses Verfahren beinhaltet insbesondere die Verpflichtung des ZCB (oder einer sektoralen Behörde), die Einrichtung über seine Absicht, eine Sanktion zu verhängen, zu informieren. Es versteht sich von selbst, dass dieser Entwurf einer Sanktionsentscheidung mit einer ausreichenden Begründung einhergehen muss. Die Einrichtung hat dann die Möglichkeit, sich zu verteidigen.

Sollte eine Sanktion dennoch für notwendig erachtet werden, muss das ZCB eine bestimmte Mindestanzahl von Elementen berücksichtigen, um eine angemessene und verhältnismäßige Sanktion zu bestimmen, z. B. die Kategorie der Einrichtung, die Schwere des Verstoßes, seine Dauer, frühere Verstöße, Schäden, Fahrlässigkeit usw.

Die nachfolgende Grafik fasst die möglichen administrativen Maßnahmen und Geldbußen zusammen.



VI. Zeitleiste

Die meisten im NIS2-Gesetzeskader festgelegten Verpflichtungen gelten ab dem 18. Oktober 2024. Das Gesetz bzw. der königliche Erlass räumt den Einrichtungen bei einigen Verpflichtungen jedoch längere Fristen für die Umsetzung ein.

Ab dem 18. Oktober 2024 gelten insbesondere die folgenden Verpflichtungen:

- Implementierung von Mindestrisikomanagementmaßnahmen im Bereich der Cybersicherheit;
- Meldung aller erheblichen Sicherheitsvorfälle;
- Wahrnehmen der Aufsichtsplichten und Zusammenarbeit mit den zuständigen Behörden;
- Für Leitungsorgane: Genehmigung von Risikomanagementmaßnahmen im Bereich der Cybersicherheit, Überwachung der Umsetzung entsprechender Maßnahmen, Haftung für Rechtsverletzungen durch die Einrichtung und Teilnahme an Cybersicherheitsschulungen.

Zur Registrierung der Einrichtungen beim ZCB über Safeonweb@Work legt das Gesetz folgende Fristen fest:

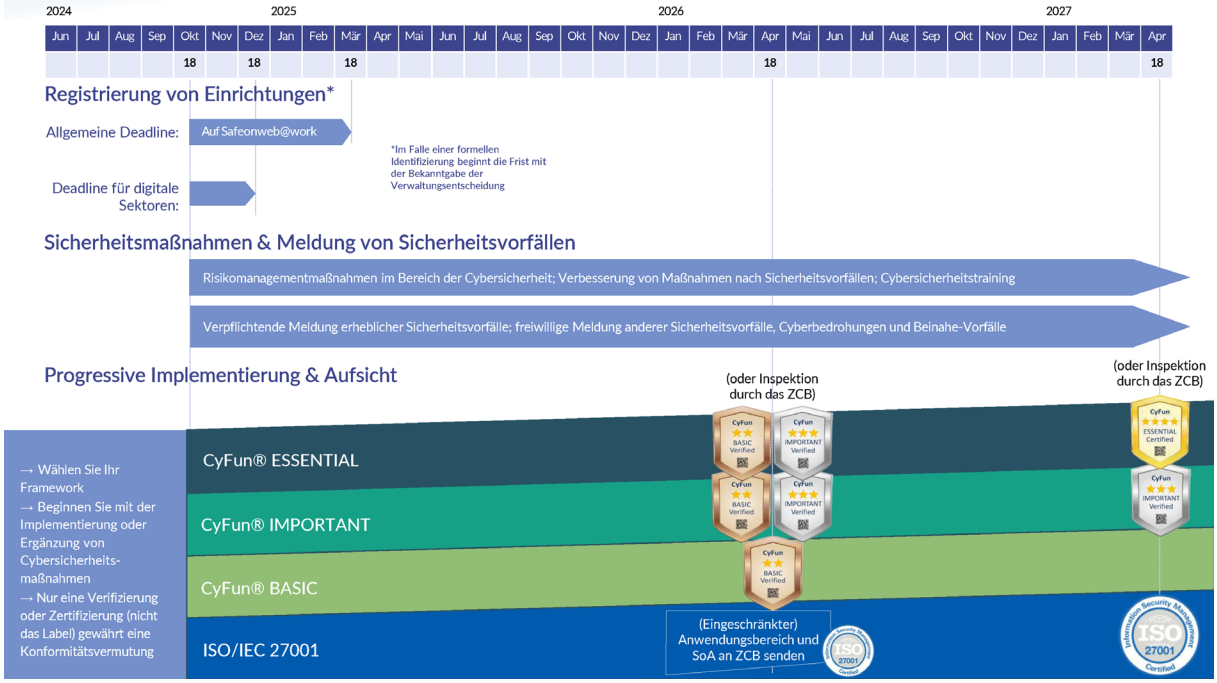
- Gehören die Dienstleistungen einer Einrichtung gemäß dem jeweiligen Anhang zu den digitalen Sektoren (siehe Liste in Art. 14, §1 des Gesetzes), hat die Einrichtung ab dem 18. Oktober 2024 2 Monate Zeit für die Registrierung (**spätestens bis zum 18. Dezember 2024**).
- Alle übrigen Einrichtungen haben 5 Monate nach dem 18. Oktober 2024, um sich zu registrieren (**spätestens bis zum 18. März 2024**).

Auch bei der Aufsicht/regelmäßigen Konformitätsbewertung wesentlicher Einrichtungen wird unterschieden:

- Bei Nutzung des CyberFundamentals (CyFun®) Frameworks:
    - Einrichtungen, die auf der Grundlage ihrer Risikobewertung feststellen, dass sie die **Sicherheitsstufe Basic** einhalten müssen, haben eine Frist von 18 Monaten (**spätestens bis zum 18. April 2026**), innerhalb derer sie eine Verifizierung durch eine akkreditierte und autorisierte Konformitätsbewertungsstelle (hiernach ein „CAB“) durchführen lassen müssen;
    - Einrichtungen, die auf der Grundlage ihrer Risikobewertung feststellen, dass sie **Sicherheitsstufe Important** einhalten müssen, haben eine Frist von 18 Monaten (**spätestens bis zum 18. April 2026**), innerhalb derer sie entweder eine Basic- oder eine Important-Verifizierung durch eine akkreditierte und autorisierte CAB erhalten müssen.
      Falls erforderlich, können sie eine erste Verifizierung auf Stufe Basic und eine Verifizierung auf Stufe Important nach einer zusätzlichen Frist von 12 Monaten durchführen (**spätestens bis zum 18. April 2027**);
    - Einrichtungen, die auf der Grundlage ihrer Risikobewertung feststellen, dass sie **Sicherheitsstufe Essential** einhalten müssen, haben eine Frist von 18 Monaten (**spätestens bis zum 18. April 2026**), innerhalb derer sie entweder eine Basic- oder eine Important-Verifizierung durch ein akkreditiertes und autorisiertes CAB erhalten müssen.
      Sie haben eine zusätzliche Frist von 12 Monaten (**spätestens bis zum 18. April 2027**), innerhalb derer sie eine Sicherheitsstufe Essential-Zertifizierung durch ein akkreditiertes und autorisiertes CAB erhalten müssen.
- Entscheidet sich eine Einrichtung für ein Zertifikat gemäß ISO/IEC 27001, muss sie ihren Anwendungsbereich und ihr *Statement of Applicability* bis zum 18. April 2026 an das ZCB übermitteln und bis zum 18. April 2027 eine Zertifizierung durch eine CAB erhalten.
- Entscheidet sich eine Einrichtung für die direkte Überprüfung durch das ZCB:
    - **Bis spätestens dem 18. April 2026**: Entweder Einreichung der Selbstbewertung von CyFun® Sicherheitsstufe Basic oder Important, oder der ISO/IEC 27001-Informationssicherheitsrichtlinie, den Anwendungsbereich und das *Statement of Applicability* an das ZCB übermitteln;
    - **Bis spätestens dem 18. April 2027**: Bericht über den Konformitätsfortschritt.

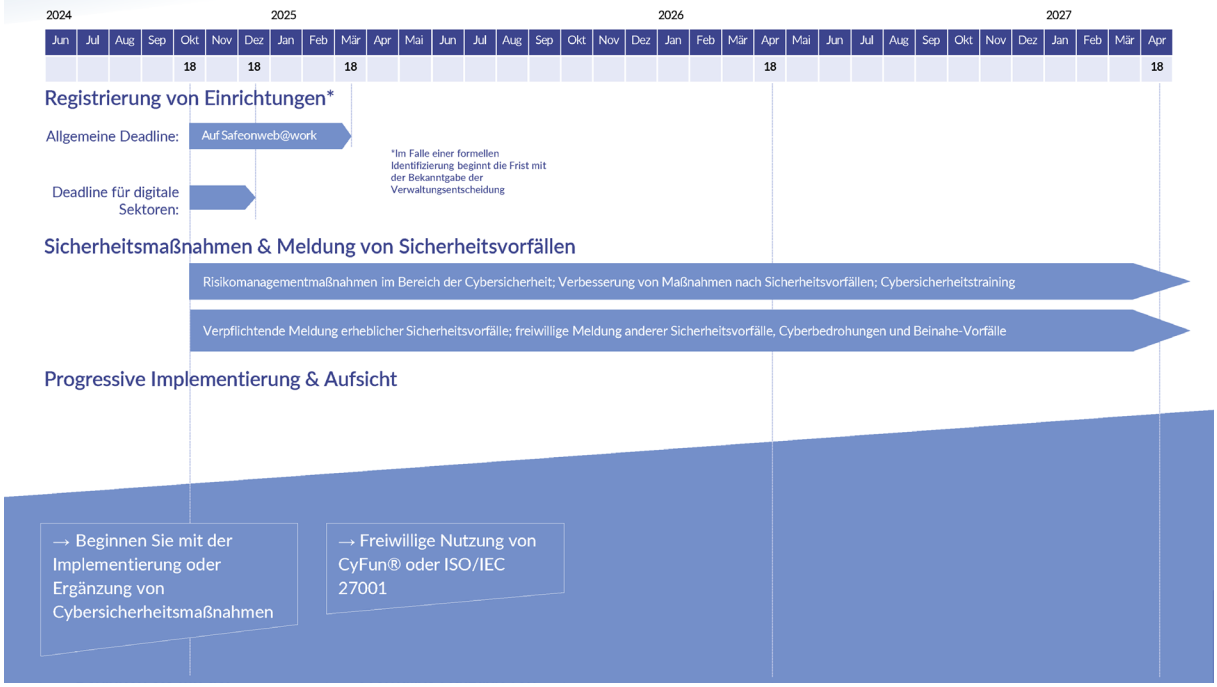
CENTRE FOR CYBERSECURITY BELGIUM

ZEITLEISTE IMPLEMENTIERUNG WESENTLICHE EINRICHTUNGEN



CENTRE FOR CYBERSECURITY BELGIUM

ZEITLEISTE IMPLEMENTIERUNG WICHTIGE EINRICHTUNGEN



CENTRE FOR CYBERSECURITY BELGIUM

ANHANG I: HOCHKRITISCHE SEKTOREN

SEKTOR	TEILSEKTOR und/oder ART DER EINRICHTUNG		GROßE UNTERNEHMEN *Mitarbeiteranzahl von mindestens 250 VZÄ, oder > € 50 Mio. Jahres-umsatz und € 43 Mio. Jahresbilanzsumme*	MITTELGROßE UNTERNEHMEN *Mitarbeiteranzahl von mindestens 50 VZÄ, oder > € 10 Mio. Jahresumsatz / Jahresbilanzsumme*	KLEINE & KLEINST-UNTERNEHMEN
1. Energie	Elektrizität	Elektrizitätsunternehmen; Verteilernetzbetreiber; Übertragungsnetzbetreiber; Erzeuger; Nominierte Strommarktbetreiber; Marktteilnehmer; Betreiber von Ladepunkten	Wesentlich	Wichtig*	Nur wenn identifiziert*
	Fernwärme und -kälte	Betreiber von Fernwärme oder Fernkälte			
	Erdöl	Betreiber von Erdöl-Fernleitungen; Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen; Zentrale Bevorratungsstellen			
	Erdgas	Versorgungsunternehmen; Verteilernetzbetreiber; Fernleitungsnetzbetreiber; Betreiber einer Speicheranlage; Betreiber einer LNG-Anlage; Erdgasunternehmen; Betreiber von Anlagen zur Raffination und Aufbereitung von Erdgas			
	Wasserstoff	Betreiber im Bereich Wasserstofferzeugung, -speicherung und -fernleitung			
2. Verkehr	Luftverkehr	Luftfahrtunternehmen die für gewerbliche Zwecke genutzt werden; Flughafenleitungsorgane, Flughäfen und Einrichtungen, die innerhalb von Flughäfen befindliche zugehörige Einrichtungen betreiben; Betreiber von Verkehrsmanagement- und Verkehrssteuerungssystemen, die Flugverkehrskontrolldienste bereitstellen			
	Schienenverkehr	Infrastrukturbetreiber; Eisenbahnunternehmen			
	Schifffahrt	Passagier- und Frachtbeförderungsunternehmen der Binnen-, See- und Küstenschifffahrt; Leitungsorgane von Häfen und Einrichtungen, die innerhalb von Häfen befindliche Anlagen und Ausrüstung betreiben; Betreiber von Schiffsverkehrsdiensten			
	Straßenverkehr	Straßenverkehrsbehörden die für Verkehrsmanagement und Verkehrssteuerung verantwortlich sind, ausgenommen öffentliche Einrichtungen, für die das Verkehrsmanagement oder der Betrieb intelligenter Verkehrssysteme ein nicht wesentlicher Teil ihrer allgemeinen Tätigkeit ist; Betreiber intelligenter Verkehrssysteme			
3. Bankwesen	Kreditinstitute *[DORA Lex specialis]*				
4. Finanzmarkt infrastrukturen	Betreiber von Handelsplätzen; Zentrale Gegenparteien *[DORA Lex specialis]*				
5. Gesundheitswesen	Gesundheitsdienstleister; EU-Referenzlaboratorien; Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel; Herstellung pharmazeutischer Erzeugnisse; Herstellung von Medizinprodukten, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden				
6. Trinkwasser	Lieferanten von und Unternehmen der Versorgung mit Wasser für den menschlichen Gebrauch, **nur wenn** wesentlicher Teil ihrer allgemeinen Tätigkeit				
7. Abwasser	Unternehmen die Kommunales Abwasser, häusliches Abwasser oder industrielles Abwasser sammeln, entsorgen oder behandeln, **nur wenn** wesentlicher Teil ihrer allgemeinen Tätigkeit				
8. Digitale Infrastruktur	Qualifizierte Vertrauensdiensteanbieter		Wesentlich		
	DNS-Diensteanbieter [ausgenommen Betreiber von Root-Namenservern]				
	TLD-Namenregister				
	Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste		Wesentlich		Wichtig*
	Nicht-qualifizierte Vertrauensdiensteanbieter		Wesentlich	Wichtig*	Nur wenn identifiziert*
	Betreiber von Internet-Knoten				
	Anbieter von Cloud-Computing-Diensten				
	Anbieter von Rechenzentrumsdiensten				
	Betreiber von Inhaltszustellnetzen				
9. Verwaltung von IKT-Diensten	Anbieter verwalteter (Sicherheits-) Dienste				
10. Öffentliche Verwaltung (ausgenommen Justiz, Parlamente, Zentralbanken; nationale Sicherheit, öffentliche Sicherheit, Verteidigung oder Strafverfolgung	Einrichtungen der öffentlichen Verwaltung die vom Föderalstaat abhängen		Wesentlich		
	Einrichtungen der öffentlichen Verwaltung die von den föderalen Teilgebieten abhängen (nach Identifizierung im Anschluss an eine risikobasierte Bewertung der Kritikalität der erbrachten Dienstleistungen)		Wichtig*		
	Hilfeleistungszonen (einschließlich der Feuerwehr und dem medizinische Notdienst der Region Brüssel-Hauptstadt)				
11. Weltraum	Betreiber von Bodeninfrastrukturen, die die Erbringung von weltraumgestützten Diensten unterstützen, ausgenommen Anbieter öffentlicher elektronischer Kommunikationsnetze		Wesentlich	Wichtig*	Nur wenn identifiziert*

Die Definitionen dieser Arten von Einrichtungen können in den Anhängen I und II oder in Artikel 8 des NIS2-Gesetzes gefunden werden.

(*) Das ZCB kann gegebenenfalls, je nach Kritikalität der erbrachten Dienstleistungen und der eingegangenen Risiken, bestimmte wichtige Einrichtungen als wesentliche Einrichtungen identifizieren oder innerhalb eines Sektors andere Kategorien von Einrichtungsarten als wichtig oder wesentlich identifizieren.

CENTRE FOR CYBERSECURITY BELGIUM

ANHANG II: ANDERE KRITISCHE SEKTOREN

SEKTOR	TEILSEKTOR und/oder ART DER EINRICHTUNG	GROßE UNTERNEHMEN *Mitarbeiteranzahl von mindestens 250 VZÄ, oder > € 50 Mio. Jahresumsatz und € 43 Mio. Jahresbilanzsumme*	MITTELGROßE UNTERNEHMEN *Mitarbeiteranzahl von mindestens 50 VZÄ, oder > € 10 Mio. Jahresumsatz / Jahresbilanzsumme*	KLEINE & KLEINSTUNTERNEHMEN
1. Post- und Kurierdienste	Anbieter von Postdiensten, einschließlich Anbieter von Kurierdiensten	Wichtig*		Nur wenn identifiziert*
2. Abfall-bewirtschaftung	Nur wenn Hauptwirtschaftstätigkeit			
3. Chemische Stoffe	Herstellung von Stoffen und Handel mit Stoffen oder Gemischen; Produktion von Erzeugnissen aus Stoffen oder Gemischen			
4. Lebensmittel	Großhandel sowie industriellen Produktion und Verarbeitung			
5. Herstellung	Medizinprodukte und In-vitro-Diagnostika; Datenverarbeitungsgeräte, elektronische und optischen Erzeugnisse; elektrische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile; sonstiger Fahrzeugbau (NACE C 26-30)			
6. Anbieter digitaler Dienste	Anbieter von Online-Marktplätzen			
	Online-Suchmaschinen			
	Plattformen für Dienste sozialer Netzwerke			
7. Forschung	Forschungseinrichtungen, mit Ausnahme von Bildungseinrichtungen			

(*) Das ZCB kann gegebenenfalls, je nach Kritikalität der erbrachten Dienstleistungen und der eingegangenen Risiken, bestimmte wichtige Einrichtungen als wesentliche Einrichtungen identifizieren oder innerhalb eines Sektors andere Kategorien von Einrichtungsarten als wichtig oder wesentlich identifizieren.

Hinweis: Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, fallen ebenfalls unter NIS2, müssen sich jedoch nur bei Safeonweb@Work registrieren und eine genaue und vollständige Datenbank mit Domainnamen-Registrierungsdaten erstellen und pflegen.

DIE NIS2-RICHTLINIE IN BELGIEN

Dieses Dokument wurde vom Zentrum für Cybersicherheit Belgien (ZCB) verfasst. Diese Föderalverwaltung wurde durch den Königlichen Erlass vom 10. Oktober 2014 geschaffen und untersteht dem Premierminister.

Die bereitgestellten Informationen:
- sind rein allgemeiner Natur und zielen nicht darauf ab, alle spezifischen Situationen abzudecken;
- sind nicht unbedingt in jeder Hinsicht vollständig, genau oder aktuell.

Verantwortlicher Herausgeber:
Zentrum für Cybersicherheit Belgien
M. De Bruycker, Generaldirektor
Wetstraat 18
1000 Brüssel

Pflichtexemplar:
D/2024/14828/008