Version 1.0
07/2024

CENTRE FOR CYBERSECURITY BELGIUM

Häufig gestellte Fragen (Frequently Asked Questions - FAQ) NIS2 in Belgien

Ziel dieses Dokument ist es Antworten auf häufig gestellte Fragen zum rechtlichen Rahmen von NIS2 in Belgien geben. Es ergänzt die Informationen, die bereits auf der ZCB-Website und auf Safeonweb@Work verfügbar sind.

Inhaltsverzeichnis

Abkürzungen & Referenzen

Die folgenden Abkürzungen und Referenzen werden in diesem Dokument verwendet:

- BELAC: *Belgische Accreditatie-instelling* (Belgische Akkreditierungsstelle)
- CAB: *Conformity Assessment Body (*Konformitätsbewertungsstelle)
- CSIRT: *Computer Security Incident Response Team* (in Belgien ist das nationale CSIRT das ZCB)
- CyFun®: *Cyberfundamentals Framework*, verfügbar auf SafonwebAtWork
- DORA: Verordnung (EU) 2022/2554 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die digitale operationale Resilienz im Finanzsektor und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 (verfügbar auf Eur-Lex)
- DSGVO: Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (verfügbar auf Eur-Lex)
- Empfehlung (2003/361/EG): Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen (verfügbar auf Eur-Lex)
- NCCN: Nationales Krisenzentrum
- NIS1-Gesetz: Gesetz vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (verfügbar auf Justel).
- 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 (verfügbar auf Eur-Lex).
- NIS2 Königlicher Erlass: Königlicher Erlass vom 9. Juni 2024 zur Ausführung des Gesetzes vom 26. April 2024 zur Schaffung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (verfügbar auf Justel).
- NIS2-Gesetz: Gesetz vom 26. April 2024 zur Schaffung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (verfügbar auf Justel).
- NIS2-Richtlinie: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (verfügbar auf Eur-Lex).
- ZCB: Zentrum für Cybersicherheit Belgien (nationale Cybersicherheitsbehörde & nationales CSIRT)

1. Allgemein - Anwendungsbereich

1.1. Was sind die Ziele des NIS2-Gesetzes?

Die Richtlinie 2022/2555 (die sogenannte "NIS2-Richtlinie") und das belgische NIS2-Gesetz, das sie umsetzt, zielen darauf ab, die Cyber-Resilienz zu stärken, indem sie sich auf die folgenden Schlüsselziele konzentrieren:

1) Cybersicherheitsschutz für wesentliche Dienste, die in der Europäischen Union erbracht werden. Im Vergleich zur NIS1-Richtlinie erweitert die NIS2-Richtlinie die Zahl der wesentlichen Dienste, die in verschiedenen hochkritischen Sektoren (Beilage I) oder anderen kritischen Sektoren (Beilage II) erfasst werden. Der Anwendungsbereich wird nun hauptsächlich durch die Verwendung europäischer Definitionen (wie "Art der Einrichtung") und eines Größenkriteriums ("size cap") bestimmt;
2) Stärkung der Maßnahmen zum Management von Cybersicherheitsrisiken, die die Einrichtungen ergreifen müssen, sowie die Meldung erheblicher Sicherheitsvorfälle (mit zwei Kategorien von wesentlichen oder wichtigen Einrichtungen);
3) Förderung des Informationsaustauschs über Sicherheitsvorfälle und -risiken im Bereich der Cybersicherheit zwischen den betroffenen Einrichtungen und den nationalen CSIRTs;
4) Verstärkte Aufsicht und Sanktionen;
5) Europäische und nationale Zusammenarbeit sicherstellen.

1.2. Was ist der Anwendungsbereich des NIS2-Gesetzes?

Das NIS2-Gesetz richtet sich an öffentliche oder private Einrichtungen, die grundsätzlich in Belgien niedergelassen sind (es gibt einige Ausnahmen zu dieser Regel) und die eine in Beilage I oder II des Gesetzes aufgeführte Dienstleistung innerhalb der Europäischen Union erbringen.

Art. 3-7 NIS2-Gesetz

Um als dem Gesetz unterliegende Einrichtung zu gelten, genügt es, unabhängig von der Rechtsform mindestens eine der in den Beilagen I oder II des Gesetzes aufgeführten Tätigkeiten innerhalb der Europäischen Union auszuüben und zumindest als mittleres Unternehmen im Sinne der Empfehlung 2003/361/EG der Europäischen Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen zu gelten.

Wesentliche Einrichtungen sind Organisationen, die eine in Beilage I aufgeführte Dienstleistung erbringen und die dem Begriff des großen Unternehmens im Sinne der Empfehlung 2003/361/EG entsprechen.

Wichtige Einrichtungen sind Organisationen, die eine Dienstleistung erbringen:

- die entweder in Beilage I aufgeführt ist und die dem Begriff "mittleres Unternehmen" im Sinne der Empfehlung 2003/361/EG entsprechen; oder
- die in Beilage II aufgeführt ist und die als mittlere oder große Unternehmen im Sinne der Empfehlung 2003/361/EG gelten;

Es ist wichtig zu betonen, dass sich **der Anwendungsbereich des NIS2-Gesetzes auf die gesamte betroffene Einrichtung bezieht** und nicht nur auf ihre in den Beilagen des Gesetzes aufgeführten Tätigkeiten.

Sofern die in den Beilagen enthaltene Definition der Dienstleistung nicht berücksichtigt, ob es sich bei der betreffenden Tätigkeit um eine Haupt- oder eine Nebentätigkeit handelt, fällt eine Einrichtung **auch dann in den Anwendungsbereich des Gesetzes, wenn die von ihr erbrachte wesentliche Dienstleistung nur einen untergeordneten Teil aller ihrer Tätigkeiten darstellt.**

Weitere Informationen finden Sie in den folgenden Abschnitten.

1.3. Wie berechnet man die Größe einer Einrichtung?

Art. 3, §§ 1 und 2 NIS2-Gesetz

Für die Zwecke des Anwendungsbereichs des NIS2-Gesetzes wird die Größe der Einrichtung auf Grundlage der Regeln in der Beilage der Empfehlung 2003/361/EG berechnet. Die Europäische Kommission hat dazu einen ausführlichen Leitfaden veröffentlicht und ein Berechnungstool zur Verfügung gestellt.

Eine Organisation wird als mittleres Unternehmen bezeichnet, wenn sie :

- entweder zwischen 50 und 249 Personen beschäftigt (Arbeitnehmer, Zeit- oder Leiharbeitskräfte, Betriebsinhaber, Teilhaber, usw.) - Mitarbeiterzahl berechnet in Jahresarbeitseinheiten (JAE);
- oder einen Jahresumsatz von mehr als 10 Millionen Euro bis zu 50 Millionen Euro erzielt oder eine Jahresbilanzsumme von mehr als 10 Millionen Euro bis zu 43 Millionen Euro aufweist.

Bei der Anwendung dieser Schwellenwerte für Finanzdaten hat die betreffende Organisation die Wahl, entweder ihren Jahresumsatz oder ihre Jahresbilanzsumme zu berücksichtigen. **Eine dieser beiden Daten kann den Schwellenwert für ein großes Unternehmen überschreiten**, ohne dass dies Auswirkungen auf die Einstufung einer Organisation als mittleres Unternehmen hat.

Eine Organisation wird als großes Unternehmen bezeichnet, wenn sie :

- entweder 250 oder mehr Personen beschäftigt (Arbeitnehmer, Zeit- oder Leiharbeitskräfte, Betriebsinhaber, Teilhaber, usw.) - Mitarbeiterzahl berechnet in Jahresarbeitseinheiten (JAE);
- oder einen Jahresumsatz von mehr als 50 Millionen Euro erzielt und eine Jahresbilanzsumme von mehr als 43 Millionen Euro aufweist.

Es ist zu berücksichtigen, dass in Situationen mit "Partner"- oder "verbundenen" Unternehmen eine proportionale Konsolidierung der Daten (Mitarbeiter und Finanzen) der betroffenen Einrichtung und dieser anderen Einrichtungen durchgeführt werden muss, um die Größe zu berechnen.

Abgesehen von einigen Ausnahmen gilt ein Unternehmen als "Partner", wenn es zwischen 25% und 50% des Kapitals oder der Stimmrechte (je nachdem, welcher Anteil höher ist) in der betreffenden Einrichtung hält (oder umgekehrt). Diese Art von Beziehung beschreibt die Situation von Unternehmen, die bestimmte finanzielle Partnerschaften mit anderen Unternehmen

eingehen, ohne dass das eine Unternehmen direkt oder indirekt eine tatsächliche Kontrolle über das andere ausübt.

Abgesehen von einigen Ausnahmen gilt ein Unternehmen als "verbunden", wenn es mehr als 50 % des Kapitals oder der Stimmrechte (je nachdem, welcher Anteil höher ist) in der betreffenden Einrichtung hält (oder umgekehrt).

Bei Partnerunternehmen muss das betrachtete Unternehmen zu seinen eigenen Daten einen Anteil der Mitarbeiterzahl und der Finanzdaten des anderen Unternehmens hinzufügen, um dessen Größe zu bestimmen. Dieser Anteil spiegelt den Anteil der gehaltenen Anteile oder Stimmrechte wider (je nachdem, welcher der beiden Faktoren höher ist). Im Falle von verbundenen Unternehmen muss das betreffende Unternehmen 100 % der Daten des verbundenen Unternehmens zu seinen eigenen hinzufügen.

Wenn ein Unternehmen beispielsweise zu 30 % an einem anderen Unternehmen beteiligt ist, addiert es zu seinen eigenen Zahlen 30 % der Beschäftigtenzahl, des Umsatzes und der Bilanzsumme des Partnerunternehmens. Wenn es mehrere Partnerunternehmen gibt, muss die gleiche Art von Berechnung für jedes Partnerunternehmen durchgeführt werden, das dem betreffenden Unternehmen unmittelbar vor- oder nachgelegen ist.

Im Rahmen des NIS2-Gesetzes ist jedoch ein Mechanismus vorgesehen, der es der nationalen Cybersicherheitsbehörde (ZCB) im Falle einer unverhältnismäßigen Situation ermöglicht, den Grad der Unabhängigkeit einer Einrichtung von ihren Partner- und verbundenen Unternehmen zu berücksichtigen, insbesondere in Bezug auf die Netz- und Informationssysteme, die sie zur Erbringung ihrer Dienstleistungen nutzt, und in Bezug auf die Dienstleistungen, die sie erbringt. Diese Elemente müssen dem ZCB von Fall zu Fall von der Organisation, die den Mechanismus in Anspruch nehmen möchte, nachgewiesen werden. Die Anwendung dieses Mechanismus kann dazu führen, dass eine Organisation als wichtige Einrichtung statt als wesentliche Einrichtung neu eingestuft oder ganz aus dem Geltungsbereich des Gesetzes ausgeschlossen wird.

Siehe auch Abschnitt 1.14.2. und den Leitfaden zur Größenberechnung für weitere Einzelheiten.

1.4. Welche Sektoren und Dienstleistungen fallen unter das Gesetz?

Beilagen I und II NIS2-Gesetz, Artikel 8 NIS2-Gesetz

Die betroffene Einrichtung muss mindestens eine der in den Beilagen I oder II des Gesetzes aufgeführten Dienstleistungen erbringen (selbst wenn diese Dienstleistung nur einen untergeordneten Teil ihrer Aktivitäten ausmacht - außer wenn die Definition selbst als Kriterium den Haupt- oder Nebencharakter der erbrachten Dienstleistung verwendet), die in den folgenden Sektoren angesiedelt sind:

Sektoren mit hoher Kritikalität (Beilage I)	**Sonstige kritische Sektoren (Beilage II)**
○ Energie (Elektrizität, Fernwärme- und Fernkälte, Erdöl, Erdgas, Wasserstoff) ○ Verkehr (Luftverkehr, Schienenverkehr, Schiffsfahrt, Straßenverkehr) ○ Bankwesen ○ Finanzmarktinfrastrukturen ○ Gesundheitswesen	○ Post- und Kurierdienste ○ Abfallbewirtschaftung ○ Produktion, Herstellung und Handel mit chemischen Stoffen ○ Produktion, Verarbeitung und Vertrieb von Lebensmitteln

○ Trinkwasser ○ Abwässer ○ Digitale Infrastruktur ○ Verwaltung von IKT-Diensten ○ Öffentliche Verwaltung ○ Weltraum	○ Verarbeitendes Gewerbe/Herstellung von Waren (Medizinprodukten und In-vitro-Diagnostika; Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen; elektrischen Ausrüstungen; Maschinenbau; Kraftwagen, Kraftwagenteile; sonstiger Fahrzeugbau) ○ Anbieter digitaler Dienste ○ Forschung

Jeder Dienst, der unter das NIS2-Gesetz fällt, **ist in den Beilagen** I oder II (mit Verweis auf die Definitionen in den einschlägigen europäischen Rechtsnormen) **oder in Artikel 8 des NIS2-Gesetzes festgelegt**. Diese Definitionen müssen unbedingt konsultiert werden, um den betreffenden Dienst zu verstehen. Zu diesem Zweck sind die Beilagen auf der Website des Belgischen Staatsblatts zugänglich (unten, nach dem Gesetzestext).

Siehe auch Abschnitt 1.14.3. für weitere Einzelheiten und den NIS2-Anwendungsbreichtest (NIS2 scope tool).

1.5. Ist es möglich, die vom NIS2-Gesetz erfassten Bereiche in Zukunft auszuweiten?

Der König kann den Beilagen I und II Sektoren oder Teilsektoren durch einen im Ministerrat beratenen Erlass nach Anhörung etwaiger betroffener sektoraler Behörden und der nationalen Cybersicherheitsbehörde (ZCB) hinzufügen.

Art. 3, § 6 NIS2-Gesetz

Auf diese Weise können die Anhänge erweitert werden, wenn sich in Zukunft herausstellt, dass ein bisher nicht erfasster Sektor aufgrund seiner Bedeutung für kritische gesellschaftliche und/oder wirtschaftliche Aktivitäten in den Anwendungsbereich aufgenommen werden sollte.

1.6. Ist es möglich, dass eine Einrichtung in mehrere Sektoren fällt?

Ja, es ist möglich, dass eine Einrichtung in mehr als einen Sektor fällt. In diesem Fall sind mehrere Überlegungen zu berücksichtigen:

Art. 8, 34°; 25; 39, Abschn. 2 und 44, §1, Abs. 2 NIS2-Gesetz

- Strengere Anforderungen haben Vorrang vor weniger strengen Anforderungen. Infolgedessen und wenn das Größenkriterium erfüllt ist (großes Unternehmen), wird eine Einrichtung, die Dienstleistungen erbringt, die sowohl unter Beilage I als auch unter Beilage II fallen, insgesamt als wesentliche Einrichtung eingestuft;
- Die Einrichtung wird dann potenziell der Aufsicht der nationalen Cybersicherheitsbehörde (ZCB) und mehrerer sektoraler Behörden unterstehen. Diese werden im Rahmen der Aufsicht zusammenarbeiten;
- Eine öffentliche Einrichtung, die hauptsächlich eine Dienstleistung ausübt, die in einem anderen Sektor (als dem der öffentlichen Verwaltung) der Beilagen des Gesetzes aufgeführt ist, fällt nur in diesen Sektor (und nicht gleichzeitig in diesen Sektor und in den Sektor der öffentlichen Verwaltung).

1.7. Was ist der Unterschied zwischen "wesentlichen" und "wichtigen" Einrichtungen?

Art. 39-42; 48, §§ 1 und 2; 58 und 59 NIS2-Gesetz

Wesentliche und wichtige Einrichtungen unterscheiden sich vor allem im Rahmen der Aufsicht und der Sanktionen. Wesentliche Einrichtungen werden proaktiv "*ex ante*" und reaktiv "*ex post*" beaufsichtigt. Insbesondere werden wesentliche Einrichtungen einer regelmäßigen Konformitätsbewertung unterzogen.

Wichtige Einrichtungen werden "*ex post*" beaufsichtigt, d.h. aufgrund von Beweisen, Hinweisen oder Informationen, dass eine wichtige Einrichtung gegen die gesetzlichen Verpflichtungen verstößt.

Weitere Informationen zur Aufsicht finden Sie im Abschnitt 4.3.

Ansonsten gelten für beide Arten von Einrichtungen dieselben Pflichten, z.B. in Bezug auf die Meldung von Sicherheitsvorfällen (Abschnitt 3.3.) oder das Ergreifen von Maßnahmen zum Management von Cybersicherheitsrisiken (Abschnitt 3.2.).

1.8. Wie funktioniert ein mögliches zusätzliches Identifizierungsverfahren?

Art. 11 NIS2-Gesetz

Aus eigener Initiative oder auf Vorschlag der gegebenenfalls betroffenen sektoralen Behörde kann die nationale Cybersicherheitsbehörde (ZCB) eine Einrichtung unabhängig von ihrer Größe in folgenden Fällen als wesentlich oder wichtig identifizieren:

1. Die Einrichtung ist der einzige Anbieter in Belgien von mindestens einer Dienstleistung, die für die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Aktivitäten unerlässlich ist, insbesondere in einem der Sektoren oder Teilsektoren, die in den Beilagen I und II des Gesetzes aufgeführt sind;
2. Eine Störung der von der Einrichtung erbrachten Dienstleistung könnte sich wesentlich auf die öffentliche Sicherheit, die öffentliche Ordnung oder die öffentliche Gesundheit auswirken;
3. Eine Störung der von der Einrichtung erbrachten Dienstleistung könnte zu einem wesentlichen Systemrisiko führen, insbesondere in Sektoren, in denen eine solche Störung grenzübergreifende Auswirkungen haben könnte;
4. Die Einrichtung ist aufgrund ihrer besonderen Bedeutung auf nationaler oder regionaler Ebene für den betreffenden Sektor oder die betreffende Art von Dienstleistung oder für andere voneinander abhängige Sektoren in Belgien kritisch.

Ein Entwurf des Identifizierungsbeschlusses wird der betroffenen Einrichtung und anschließend allen betroffenen föderierten Teilgebieten sowie den sektoralen Behörden übermittelt, die innerhalb von 60 Tagen eine nicht veröffentlichte Stellungnahme abgeben.

Wenn eine sektorale Behörde eine ablehnende Stellungnahme abgibt und das ZCB an seinem Entscheidungsentwurf festhalten möchte, wird der Entscheidungsentwurf zusammen mit der Stellungnahme dem Strategischen Komitee für Aufklärung und Sicherheit (eingesetzt durch den Königlichen Erlass vom 22. Dezember 2020) vorgelegt, der eine verbindliche Stellungnahme

abgibt. Je nachdem, wie diese Stellungnahme ausfällt, wird das ZCB die Identifizierung vornehmen oder nicht.

Die ZCB bewertet und ggf. aktualisiert die Identifizierung wesentlicher und wichtiger Einrichtungen mindestens alle zwei Jahre auf die gleiche Weise.

1.9. Welchen territorialen Anwendungsbereich hat das Gesetz? Was ist mit Einrichtungen, die in mehreren Ländern tätig sind (multinationale Unternehmen, ...)?

Das belgische NIS2-Gesetz gilt grundsätzlich für Einrichtungen, die **in Belgien ansässig sind** und in der EU ihre Dienstleistungen erbringen oder ihre Geschäfte betreiben.

Art. 4 NIS2-Gesetz

Der Begriff "Einrichtung" wird in Artikel 8, 37° des NIS2-Gesetzes wie folgt definiert: *„eine natürliche Person oder nach dem an ihrem Sitz geltenden nationalen Recht geschaffene und anerkannte juristische Person, die in eigenem Namen Rechte ausüben und Pflichten unterliegen kann"*.

Der Begriff der Niederlassung beinhaltet 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.

Das NIS2-Gesetz sieht drei Ausnahmen von der Niederlassungsregel in Belgien vor:

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 Domänennamenregistrierungsdienste 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 von Belgien gegründet wurden.

Der Begriff "Hauptniederlassung" bezieht sich auf die Niederlassung, in der die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheitsrisikomanagement vorwiegend getroffen werden. Kann dieser Ort nicht bestimmt werden oder werden solche Entscheidungen nicht in der Union getroffen, so gilt als Hauptniederlassung die Niederlassung, in der die Einrichtung Cybersicherheitsmaßnahmen durchführt. Kann auch dieser Ort nicht bestimmt werden, so gilt als Hauptniederlassung der Ort, an dem die Einrichtung die höchste Beschäftigtenzahl in der Union hat.

(*) Ist eine Einrichtung im Sinne von Punkt 2) nicht in der EU niedergelassen, erbringt aber dort ihre Dienstleistungen, muss sie einen gesetzlichen Vertreter benennen, der in einem

Mitgliedstaat niedergelassen ist, in dem sie ihre Dienstleistungen erbringt. Befindet sich dieser Vertreter in Belgien, wird davon ausgegangen, dass die Einrichtung ihre Hauptniederlassung in Belgien hat.

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.

1.10. Welche Interaktionen bestehen zwischen der DORA-Verordnung und der NIS2-Richtlinie?

Art. 6 NIS2-Gesetz
Art. 2 & 47 DORA

Die NIS2-Richtlinie und ihr Umsetzungsgesetz zielen auf bereichsübergreifende Maßnahmen zur Erhöhung der Cybersicherheit in der EU ab. Ziel ist es, die Cybersicherheit in der EU insgesamt zu verbessern und insbesondere ein hohes Maß an Cybersicherheit für bestimmte Einrichtungen zu gewährleisten, die für gesellschaftliche und wirtschaftliche Aktivitäten kritisch sind.

Die DORA-Verordnung (Digital Operational Resiliance Act) richtet sich speziell an Betreiber des Finanzsektors. Sie zielt darauf ab, die digitaler operationaler Resilienz von Informationssystemen im Finanzsektor zu verbessern und die bestehenden Vorschriften in diesem Bereich zu koordinieren.

DORA gilt für Finanzinstitute, die in Artikel 2 der Verordnung aufgelistet sind. Dabei handelt es sich um:

- Kreditinstitute,
- Zahlungsinstitute,
- Kontoinformationsdienstleister,
- E-Geld-Institute,
- Wertpapierfirmen,
- Anbieter von Krypto-Dienstleistungen,
- Zentralverwahrer,
- zentrale Gegenparteien,
- Handelsplätze,
- Transaktionsregister,
- Verwalter alternativer Investmentfonds,
- Verwaltungsgesellschaften,
- Datenbereitstellungsdienste,
- Versicherungs- und Rückversicherungsunternehmen,
- Versicherungsvermittler, Rückversicherungsvermittler und Versicherungsvermittler in Nebentätigkeit,
- Einrichtungen der betrieblichen Altersversorgung,
- Ratingagenturen,
- Administratoren kritischer Referenzwerte,
- Schwarmfinanzierungsdienstleister,
- Verbriefungsregister,

- IKT-Drittdienstleister.

Die Anwendungsbereiche von NIS2 und DORA überschneiden sich bei einigen Einrichtungen, die im Banken- und Finanzsektor tätig sind. Die NIS2-Richtlinie sieht daher eine *lex specialis*-Regel vor: Wenn auf europäischer Ebene gleichwertige sektorale Anforderungen an die Cybersicherheit und die Meldung erheblicher Sicherheitsvorfälle bestehen, gilt die spezifische Rechtsnorm (hier die DORA-Verordnung) und nicht die allgemeine Rechtsnorm (hier die NIS2-Richtlinie).

Es ist jedoch vorgesehen, dass Einrichtungen des Banken- und Finanzsektors, die sowohl in den Anwendungsbereich der DORA-Verordnung als auch der NIS2-Richtlinie fallen, sich wie andere NIS2-Einrichtungen registrieren müssen.

Schließlich werden die von den DORA-Einrichtungen gemeldeten erheblichen Sicherheitsvorfälle an die NIS2-Behörden weitergeleitet.

1.11. Fallen kritische Infrastrukturen (oder kritische Einrichtungen, die im Rahmen der CER-Richtlinie identifiziert wurden) in den Anwendungsbereich des NIS2-Gesetzes?

Art. 9, 5° und 25, §2 NIS2-Gesetz

Ja, der Betreiber einer oder mehrerer kritischer Infrastrukturen, die im Rahmen des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen (oder als kritische Einrichtungen im Sinne der Richtlinie 2022/2557 - CER-Richtlinie) identifiziert wurden, gilt als wesentliche Einrichtung im Sinne des NIS2-Gesetzes.

Die NIS2-Behörden und die nach dem Gesetz vom 1. Juli 2011 (und der CER-Richtlinie) zuständigen Behörden arbeiten bei der Aufsicht über diese Einrichtungen zusammen.

Weitere Informationen zu kritischen Infrastrukturen finden Sie auf der Website des Nationalen Krisenzentrums.

1.12. Fallen Bildungseinrichtungen in den Geltungsbereich des Gesetzes?

Beilagen I und II & Art. 8, 34° NIS2-Gesetz

Der Bildungssektor ist in den Beilagen I und II des NIS2-Gesetzes nicht explizit aufgeführt.

Hingegen könnten öffentliche Bildungseinrichtungen, wie z.B. Universitäten oder Hochschulen, unter die Definition einer "Einrichtung der öffentlichen Verwaltung" fallen. Dazu müssten diese :

- das Kriterium der Größe erfüllen (siehe Abschnitt 1.3.);
- in Belgien ansässig sein (siehe Abschnitt 1.9.);
- auf die Definition einer Einrichtung der öffentlichen Verwaltung in Artikel 8, 34° NIS2-Gesetz zutreffen;
- vom Föderalstaat oder den föderierten Teilgebieten abhängen;

Andererseits könnte eine Bildungseinrichtung auch als "Gesundheitsdienstleister" im Sinne der Beilage I zum NIS2-Gesetz eingestuft werden (z. B. ein Universitätskrankenhaus).

1.13. Können NACE-Codes verwendet werden, um festzustellen, ob eine Einrichtung unter das Gesetz fällt?

Beilagen I und II NIS2-Gesetz

Einige der in den Beilagen I und II aufgeführten Dienstleistungen beziehen sich tatsächlich auf NACE-Codes. Einrichtungen mit Sitz in Belgien, die unter diese NACE-Codes fallende Dienstleistungen erbringen, sollten daher sorgfältig prüfen, ob das NIS2-Gesetz nicht auf sie anwendbar wäre.

Für alle Einrichtungen, die nicht unter die oben genannte Möglichkeit fallen, stellen die NACE-Codes keine gültige Grundlage dar um festzustellen ob eine Einrichtung in den Anwendungsbereich des NIS2-Gesetzes fällt. Einige NACE-Codes können von Einrichtungen zwar vorläufig verwendet werden, doch ist eine genauere Überprüfung ihrer genauen wirtschaftlichen Tätigkeit erforderlich, um festzustellen, ob sie unter den oftmals restriktiveren Anwendungsbereich des NIS2-Gesetzes fallen oder nicht.

1.14. Mit welcher Methode kann man feststellen ob eine Organisation in den Anwendungsbereich des NIS2-Gesetzes fällt?

Die unten beschriebene Methode stellt die einzelnen Schritte der Überlegung im Zusammenhang mit dem Anwendungsbereich des NIS2-Gesetzes dar. Diese Methode erhebt jedoch keinen Anspruch auf Vollständigkeit oder als einzig anwendbare Methode.

Dieser Abschnitt behandelt die folgenden Punkte:

1. Vor des Prüfung des NIS2-Gesetzes:
    a. Betreibt meine Organisation eine kritische Infrastruktur im Sinne des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen?
    b. Ist meine Organisation ein Betreiber wesentlicher Dienste oder ein Anbieter digitaler Dienste (NIS1-Gesetz)?
2. Wie groß ist meine Organisation?
3. Welche Dienstleistung(en) erbringt meine Organisation in der Europäischen Union?
4. Wo in Europa ist meine Organisation ansässig?
5. Könnte meine Organisation später identifiziert werden oder befindet sie sich in der Lieferkette einer NIS2-Einrichtung?

Siehe hierzu auch unseren NIS2-Anwendungsbreichtest (NIS2 scope tool).

1.14.1. Vor der Prüfung des NIS2-Gesetzes

Bevor wir mit der eigentlichen Analyse beginnen, müssen wir uns zunächst mit zwei Möglichkeiten beschäftigen, die einen großen Einfluss darauf haben, wie der Anwendungsbereich des NIS2-Gesetzes für die betroffenen Organisationen funktioniert.

A. Betreibt meine Organisation eine kritische Infrastruktur im Sinne des Gesetzes vom 1. Juli 2011 über die Sicherheit und den Schutz kritischer Infrastrukturen?

Artikel 3, §4 des NIS2-Gesetzes besagt, dass das Gesetz automatisch für Einrichtungen gilt, die, unabhängig von ihrer Größe, im Sinne des Gesetzes vom 1. Juli 2011 über die Sicherheit und den

Schutz kritischer Infrastrukturen (und in Zukunft für kritische Einrichtungen im Sinne der CER-Richtlinie) als Betreiber einer kritischen Infrastruktur identifiziert wurden.

Die Betreiber einer kritischen Infrastruktur müssen daher nicht analysieren, ob ihre Organisation in den Anwendungsbereich der NIS2-Richtlinie fällt oder nicht: Sie werden automatisch als wesentliche Einrichtungen qualifiziert.

B. Ist meine Organisation ein Betreiber wesentlicher Dienste (BWD) oder ein Anbieter digitaler Dienste (ADD)?

Einrichtungen, die im Rahmen des Gesetzes vom 7. April 2019 zur Festlegung eines Rahmens für die Sicherheit von Netz und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (NIS1-Gesetz) als Betreiber wesentlicher Dienste (BWD) identifiziert wurden oder die Anbieter digitaler Dienste (ADD) waren, unterliegen den Bestimmungen des NIS2-Gesetzes. Grund dafür ist, dass der Anwendungsbereich der NIS2-Richtlinie auf den Sektoren der NIS1-Richtlinie aufbaut.

BWD müssen, sofern keine formelle Identifizierung durch den ZCB vorliegt, das Kriterium der Größe erfüllen (siehe nächster Punkt). Die ADD hingegen mussten bereits unter der Empfehlung 2003/361/EG mindestens mittelgroße Unternehmen sein.

1.14.2. Wie groß ist meine Organisation?

Um in den Anwendungsbereich des NIS2-Gesetzes zu fallen, muss eine Einrichtung eine bestimmte Größe haben. Um diese Größe zu berechnen, bezieht sich das NIS2-Gesetz auf die Empfehlung 2003/361/EG der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen. Diese Empfehlung legt die Schwellenwerte fest, ab denen ein Unternehmen als kleines, mittleres oder großes Unternehmen eingestuft werden kann. Außer in Ausnahmefällen fallen nur mittlere und große Unternehmen in den Anwendungsbereich des NIS2-Gesetzes.

Zur Feststellung der Größe sind zwei Bedingungen zu prüfen: die Mitarbeiterzahl (gemessen in Jahresarbeitseinheiten (JAE)[1]) und die finanziellen Beträge (Jahresumsatz und/oder Jahresbilanzsumme).

Die Mitarbeiterzahl muss mit den finanziellen Beträgen kombiniert werden, um die Unternehmensgröße zu ermitteln: Ein Unternehmen kann sich dafür entscheiden, entweder die Umsatzobergrenze oder die Bilanzsummengrenze einzuhalten. Es **kann eine der finanziellen Obergrenzen überschreiten, ohne dass dies Auswirkungen auf seinen Status als KMU hat**. Grundsätzlich **berücksichtigen wir daher nur den niedrigeren der beiden** Beträge.

Beispiel 1: Ein Unternehmen mit 35 JAE (klein) hat einen Jahresumsatz von 1.000.000 € (klein) und eine Jahresbilanzsumme von 50.000.000 € (groß). Bei den finanziellen Beträgen entscheidet sie sich dafür, nur den niedrigsten zu berücksichtigen: ihren Umsatz. Es handelt sich also um ein Klein- oder Kleinstunternehmen.

[1] Die Jahresarbeitseinheiten (JAE) entsprechen der Anzahl der Personen, die in dem betreffenden Unternehmen oder für dieses Unternehmen während des gesamten Jahres vollzeitlich gearbeitet haben. Die Arbeit von Personen, die nicht das ganze Jahr über gearbeitet haben, oder die Teilzeitarbeit, unabhängig von der Dauer der Teilzeitarbeit, oder Saisonarbeit wird als Bruchteil einer JAE gezählt.

Beispiel 2: Ein Unternehmen mit 80 JAE (mittelgroß) hat einen Jahresumsatz von 1.000.000 € (klein) und eine Jahresbilanzsumme von 70.000.000 € (groß). Bei den finanziellen Beträgen entscheidet sie sich dafür, nur den kleinsten zu berücksichtigen: ihren Umsatz. Da der Umsatz klein, die Mitarbeiterzahl aber mittelgroß ist, handelt es sich um ein mittelgroßes Unternehmen.

Eine visuelle Zusammenfassung der möglichen Unternehmensgrößen finden Sie auf unserer Website.

Wenn wir die verschiedenen möglichen Größen mit dem Dienstleistungskriterium kombinieren, ergibt sich folgender Anwendungsbereich :

- Ein mittleres Unternehmen beschäftigt zwischen 50 und 249 JAE oder hat einen Jahresumsatz/eine Jahresbilanzsumme von mehr als 10 Millionen EUR:
  - ➔ Fällt als "wichtige Einrichtung" in den Anwendungsbereich, wenn sie eine in Beilage II des Gesetzes aufgeführte Dienstleistung erbringt.
  - ➔ Fällt **grundsätzlich** als "wichtige Einrichtung" in den Anwendungsbereich, wenn sie eine in Beilage I des Gesetzes aufgeführte Dienstleistung erbring.
- Ein großes Unternehmen beschäftigt mindestens 250 JAE oder hat einen Jahresumsatz von mehr als 50 Mio. EUR und eine Jahresbilanzsumme von mehr als 43 Mio. EUR:
  - ➔ Fällt als "wesentliche Einrichtung" in den Anwendungsbereich, wenn sie eine in Beilage II des Gesetzes aufgeführte Dienstleistung erbring.
  - ➔ Fällt **grundsätzlich** als "wesentliche Einrichtung" in den Anwendungsbereich, wenn sie eine in Beilage I des Gesetzes aufgeführte Dienstleistung erbring.

Die Empfehlung sieht insbesondere vor, dass bei Einrichtungen, die als "verbundene Unternehmen" oder "Partnerunternehmen" gruppiert sind, je nach den festgelegten Kriterien die Daten (Mitarbeiterzahl & Finanzbeträge) der anderen Einrichtungen, die Teil der Gruppe von Einrichtungen sind, bei der Berechnung der Größe berücksichtigt werden (siehe auch Abschnitt 1.3.).

Für weitere Informationen zur Anwendung der Empfehlung empfehlen wir dringend, den Benutzerleitfaden für die Definition von KMU der Kommission zu konsultieren. Er enthält alle Kriterien und visuelle Beispiele, die Ihnen bei der Anwendung der Empfehlung helfen sollen. Die Kommission hat außerdem ein Tool entwickelt, mit dem Sie die Größe Ihrer Organisation testen können.

Es gibt jedoch einige **Ausnahmen**. Die folgenden Arten der Einrichtungen fallen unabhängig von ihrer Größe in den Anwendungsbereich des NIS2-Gesetzes:

- 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 (wesentlich) identifiziert wurden;
- Einrichtungen der öffentlichen Verwaltung, die vom Föderalstaat abhängen (wesentlich);

Im folgenden Abschnitt wird erläutert, wie man die Definitionen der von diesen Arten von Einrichtungen erbrachten Dienstleistungen finden kann.

1.14.3. Welche Dienstleistung(en) erbringt meine Organisation in der Europäischen Union?

Sobald die Größe einer Einrichtung bekannt ist, muss als nächstes eine detaillierte Analyse aller Dienstleistungen, die die Einrichtung für Dritte erbringt, nach Sektoren oder Teilsektoren durchgeführt werden. Es ist wichtig, eine Topographie jeder Dienstleistung zu erstellen, selbst wenn diese nur eine Nebentätigkeit der Einrichtung darstellt (es sei denn, die Definition der Dienstleistung berücksichtigt ob die betreffende Dienstleistung eine Haupt- oder Nebentätigkeit ist).

In den Beilagen I und II (oder den Definitionen) des NIS2-Gesetzes werden die betreffenden Dienste ("Art der Einrichtung") im Einzelnen aufgeführt, häufig mit einem Verweis auf die entsprechenden europäischen Rechtsvorschriften oder die in Artikel 8 des Gesetzes vorgesehenen Definitionen.

Die verschiedenen Sektoren und Teilsektoren sind wie folgt:

Sektoren mit hoher Kritikalität (Beilage I)	Sonstige kritische Sektoren (Beilage II)
1. Energie a. Elektrizität b. Fernwärme und Fernkälte c. Erdöl d. Erdgas e. Wasserstoff 2. Verkehr a. Luftverkehr b. Schienenverkehr c. Schiffsfahrt d. Straßenverkehr 3. Bankwesen 4. Finanzmarktinfrastrukturen 5. Gesundheitswesen 6. Trinkwasser 7. Abwasser 8. Digitale Infrastruktur 9. Verwaltung von IKT-Diensten (B2B) 10. Öffentliche Verwaltung 11. Weltraum	1. Post- und Kurierdienste 2. Abfallbewirtschaftung 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

Es geht also darum, die von der Organisation erbrachten Dienstleistungen mit den oben genannten Definitionen aus den Beilagen in Verbindung zu bringen. Die Bedingung der erbrachten

Dienstleistung ist dann erfüllt, wenn die beiden übereinstimmen. Es ist durchaus möglich, dass eine Organisation mehrere Dienstleistungen erbringt, die in verschiedenen Sektoren aufgelistet sind (siehe hierzu Abschnitt 1.6.).

Zusammenfassend sind die "wichtigen" und "wesentlichen" Einrichtungen die folgenden (mit Ausnahme der am Ende des Abschnitts 1.14.2. aufgelisteten Arten von Einrichtungen):

	Mittleres Unternehmen	**Großes Unternehmen**
Dienstleistungen in Beilage I	Wichtig	Wesentlich
Dienstleistungen in Beilage II	Wichtig	Wichtig

1.14.4. Die Niederlassung

Grundsätzlich gilt das belgische NIS2-Gesetz für Einrichtungen, die **in Belgien niedergelassen sind und in der EU ihre Dienstleistungen erbringen oder ihre Geschäfte betreiben**.

Der Begriff der Niederlassung setzt lediglich die tatsächliche Ausübung einer Tätigkeit mittels einer festen Einrichtung voraus, unabhängig davon, welche Rechtsform gewählt wird, ob es sich dabei um den Hauptsitz, eine einfache Zweigniederlassung oder eine Tochtergesellschaft mit Rechtspersönlichkeit handelt.

Je nach Art der Einrichtung gibt es jedoch einige Ausnahmen von der Regel, dass Einrichtungen in Belgien ansässig sein müssen. Die Regeln für den territorialen Anwendungsbereich des belgischen NIS2-Gesetzes werden in Abschnitt 1.9 erläutert.

1.14.5. Zusätzliche Identifizierung und Lieferkette

Ungeachtet der oben genannten Regeln hat das ZCB die Möglichkeit, bei Bedarf bestimmte Einrichtungen, die in Belgien ansässig und in den in den Beilagen zum NIS2-Gesetz aufgeführten Sektoren tätig sind, zu identifizieren. Diese zusätzliche Identifizierung erfolgt in Absprache mit der betroffenen Organisation - siehe Abschnitt 1.8 "Identifizierung".

Unabhängig vom Anwendungsbereich des NIS2-Gesetzes ist zu berücksichtigen, dass eine große Anzahl von Organisationen indirekt von den neuen gesetzlichen Anforderungen betroffen sein wird, wenn sie sich in der Lieferkette einer oder mehrerer NIS2-Einrichtungen befinden. Letztere sind verpflichtet, die Sicherheit ihrer eigenen Lieferkette zu gewährleisten, und können daher ihren unmittelbaren Anbietern oder Dienstanbietern vertraglich Verpflichtungen auferlegen. Weitere Erläuterungen dazu finden Sie in Abschnitt 3.8.

2. Öffentlicher Sektor

2.1. Welchen Anwendungsbereich hat das Gesetz für den öffentlichen Sektor?

Art. 8, 34° und Beilage I, Sektor 10 (Öffentliche Verwaltung) NIS2-Gesetz

Art. 8, 34° des Gesetzes definiert eine "Einrichtung der öffentlichen Verwaltung" als eine Verwaltungsbehörde im Sinne von Art. 14, § 1, Abs. 1 der koordinierten Gesetze über den Staatsrat, die folgende Kriterien erfüllt:

a) sie hat keinen industriellen oder kommerziellen Charakter;
b) sie übt nicht hauptberuflich eine Tätigkeit aus, die in der Spalte Art der Einrichtung eines anderen Sektors oder Teilsektors in einer der Beilagen des Gesetzes aufgeführt ist;
c) sie ist keine juristische Person des Privatrechts.

Für die Definition einer Einrichtung der öffentlichen Verwaltung legt Artikel 6, 35) der Richtlinie fest, dass der Begriff gemäß dem nationalen Recht als solcher anerkannt werden muss, mit Ausnahme der Justiz, der Parlamente und der Zentralbanken. Daher wurde beschlossen, auf bestehende Begriffe im belgischen Recht zu verweisen, die die betreffenden Einrichtungen abdecken, um die Anwendung unterschiedlicher Begriffe nicht zu vervielfachen.

Im vorliegenden Fall übernimmt die Definition den Begriff der Verwaltungsbehörde gemäß Artikel 14, §1 , Absatz 1 der koordinierten Gesetze vom 12. Januar 1973 über den Staatsrat, der die Kriterien hinzugefügt werden, dass sie keinen industriellen oder kommerziellen Charakter hat, nicht hauptberuflich eine Tätigkeit ausübt, die unter einen der anderen Sektoren oder Teilsektoren fällt, die in den Anlagen des Gesetzes aufgeführt sind, und keine juristische Person des Privatrechts ist.

Diese Definition muss mit den Arten von Einrichtungen in Beilage I, Sektor 10 (Öffentliche Verwaltung) kombiniert werden:

- Einrichtungen der öffentlichen Verwaltung, die vom Föderalstaat abhängen;
- Einrichtungen der öffentlichen Verwaltung, die von den föderierten Teilstaaten abhängen, identifiziert gemäß Artikel 11, § 2 des Gesetzes;
- Die Hilfeleistungszonen im Sinne von Artikel 14 des Gesetzes vom 15. Mai 2007 über die zivile Sicherheit oder der Dienst für Brandschutz und medizinische Nothilfe der Region Brüssel-Hauptstadt, der durch die Verordnung vom 19. Juli 1990 über die Schaffung eines Dienstes für Brandschutz und medizinische Nothilfe der Region Brüssel-Hauptstadt geschaffen wurde.

Der Begriff der Abhängigkeit (die von X „abhängen“) wurde von Artikel 5 des Gesetzes vom 30. Juli 2018 über den Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten inspiriert. Er ermöglicht es, insbesondere Einrichtungen zu erfassen, die Teil einer Verwaltungsebene sind, weil sie von diesen Behörden gegründet wurden, ihre Tätigkeit mehrheitlich von diesen Behörden finanziert wird, die Verwaltung der Kontrolle dieser Behörden unterliegt, oder weil bei denen mehr als die Hälfte der Mitglieder des Verwaltungs-, Leitungs- oder Aufsichtsorgans von diesen Behörden ernannt werden.

Wie aus der Definition in Art. 8, 34° hervorgeht, unterliegt eine öffentliche Einrichtung, die hauptsächlich eine Dienstleistung erbringt, die in einem anderen Sektor oder Teilsektor in einer der Beilagen des Gesetzes aufgeführt ist (z.B. eine im Energie- oder Trinkwassersektor tätige Interkommunale, ein öffentliches Krankenhaus, eine öffentliche Einrichtung, die einen IKT-Dienst anbietet, usw.), den Regeln dieses Sektors und nicht dem Sektor der öffentlichen Verwaltung.

2.2. Unterliegen lokale öffentliche Einrichtungen den Verpflichtungen des Gesetzes?

Art. 8, 34° Beilage I, Sektor 10 (Öffentliche Verwaltung) NIS2-Gesetz

Lokale öffentliche Einrichtungen (Gemeinden, Provinzen, Interkommunale, ÖSHZ, Regiebetriebe, usw.) unterliegen nicht automatisch den Anforderungen des NIS2-Gesetzes. Gemäß dem in Artikel 162 der Verfassung verankerten Grundsatz der lokalen Selbstverwaltung, werden die lokalen Einrichtungen trotz der Ausübung einer Aufsichts- oder Finanzierungskontrolle nicht als Einrichtung der öffentlichen Verwaltung betrachtet, die im Sinne der Beilage I des NIS2-Gesetzes von den föderierten Teilgebieten oder dem Föderalstaat abhängen.

Diese lokalen Einrichtungen unterliegen jedoch den Bestimmungen des NIS2-Gesetzes, wenn sie eine in Beilage I oder II des Gesetzes aufgeführte Dienstleistung erbringen und größer als ein kleines Unternehmen sind.

Lokale öffentliche Einrichtungen können auch über Artikel 11 § 1 (Identifizierung durch die nationale Cybersicherheitsbehörde - ZCB) identifiziert werden, sofern das in Artikel 11 § 3 vorgesehenen Konzertierungsverfahren eingehalten wird. Die Initiative für eine solche Identifizierung könnte auf Antrag der nationalen Cybersicherheitsbehörde, der betroffenen Einrichtung oder auch einer Region erfolgen.

2.3. Unterliegen regionale oder gemeinschaftliche öffentliche Einrichtungen den Verpflichtungen des Gesetzes?

Art. 11, §2-3 und Beilage I, Sektor 10 (Öffentliche Verwaltung) NIS2-Gesetz

Die regionalen und gemeinschaftlichen öffentlichen Einrichtungen gehören zu den Einrichtungen der öffentlichen Verwaltung, die unter das NIS2-Gesetz fallen. Dennoch muss zuvor ein formelles Identifizierungsverfahren von der nationalen Cybersicherheitsbehörde (ZCB) durchgeführt werden. Dabei werden auf Grundlage einer Risikoanalyse Einrichtungen bewertet, die Dienstleistungen erbringen, deren Störung erhebliche Auswirkungen auf kritische gesellschaftliche oder wirtschaftliche Aktivitäten haben könnte.

Gemäß Artikel 11, § 2 und 3 des NIS2-Gesetzes erfolgt diese Identifizierung in Absprache mit den betroffenen öffentlichen Einrichtungen und den Regierungen der föderierten Einheiten. Nach Abschluss dieses Verfahrens kann die regionale oder gemeinschaftliche öffentliche Einrichtung als wesentliche Einrichtung oder wichtige Einrichtung bezeichnet werden.

3. Verpflichtungen

3.1. Welche rechtlichen Verpflichtungen bestehen für die betroffenen Einrichtungen?

Aus dem NIS2-Gesetz ergeben sich mehrere Pflichten für wesentliche und wichtige Einrichtungen:

- das Ergreifen angemessener Cybersicherheitsmaßnahmen;
- die rechtzeitige Meldung erheblicher Sicherheitsvorfälle;
- die Registrierung bei den zuständigen Behörden;
- die Ausbildung der Führungsorgane (Abschnitt 4.13.);
- die Durchführung regelmäßiger Konformitätsbewertungen (obligatorisch für wesentliche Einrichtungen und freiwillig für wichtige Einrichtungen);
- den Austausch von Informationen und die Zusammenarbeit mit den zuständigen Behörden.

Diese verschiedenen Pflichten werden in den folgenden Abschnitten erläutert.

3.2. Welche Verpflichtungen bestehen hinsichtlich der Cybersicherheitsmaßnahmen?

Art. 30, 31 und 42 NIS2-Gesetz

Wesentliche und wichtige Einrichtungen müssen geeignete und verhältnismäßige (technische, operative und organisatorische) Maßnahmen ergreifen, um Risiken zu bewältigen, die die Sicherheit der Netz- und Informationssysteme bedrohen, die diese Einrichtungen im Rahmen ihrer Geschäftstätigkeit oder bei der Erbringung ihrer Dienste nutzen, und um die Folgen von Sicherheitsvorfällen für die Empfänger ihrer Dienste und für andere Dienste zu beseitigen oder zu verringern.

Es ist wichtig zu betonen, dass sich **der Anwendungsbereich des NIS2-Gesetzes im Gegensatz zum NIS1-Gesetz auf die gesamte betroffene Einrichtung bezieht** und nicht nur auf ihre in den Beilagen des Gesetzes aufgeführten Tätigkeiten.

Um die praktische Umsetzung dieser Cybersicherheitsmaßnahmen zu erleichtern, hat das ZCB bereits einen Referenzkader entwickelt und den betroffenen Einrichtungen kostenlos zur Verfügung gestellt: das "Cyberfundamentals Framework" (CyFun®) mit verschiedenen Stufen und einem Analysetool, das es ermöglicht, die am besten geeignete Stufe für eine Einrichtung zu bestimmen. Das Gesetz und sein Königlicher Erlass werden wesentlichen und wichtigen Einrichtungen, die sich für die Verwendung des CyFun®-Frameworks oder der internationalen Norm ISO/IEC 27001 (mit dem NIS2-konformen Anwendungsbereich - d.h. alle Netz- und Informationssysteme) entscheiden, eine **Konformitätsvermutung** in Bezug auf die Sicherheitsmaßnahmen bieten.

Es ist hervorzuheben, dass der CyFun®-Kader des ZCB an die diesbezügliche Arbeit der NIS-Kooperationsgruppe angeglichen ist.

Die im Gesetz enthaltenen Mindestmaßnahmen basieren auf einem gefahrenübergreifenden Ansatz, der darauf abzielt, Netz- und Informationssysteme sowie deren physische Umgebung vor Sicherheitsvorfällen zu schützen, und zumindest folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
2. Bewältigung von Sicherheitsvorfällen;
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
7. grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
8. Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung;
11. Eine Politik für die koordinierten Offenlegung von Schwachstellen.

Die von wesentlichen und wichtigen Einrichtungen zu treffenden Maßnahmen müssen **geeignet und verhältnismäßig** sein. In diesem Zusammenhang ist es wichtig, klarzustellen, dass die Maßnahmen zum Management von Cybersicherheitsrisiken in einem **angemessenen Verhältnis zu den Risiken stehen sollten,** denen das betreffende Netz- und Informationssystem ausgesetzt ist, um zu verhindern, dass die finanzielle und administrative Belastung der wesentlichen und wichtigen Einrichtungen unverhältnismäßig hoch ist. In diesem Zusammenhang berücksichtigen die Einrichtungen insbesondere **den Stand der Technik** dieser Maßnahmen sowie gegebenenfalls einschlägige europäische oder internationale **Normen** und die **Kosten für die Umsetzung** dieser Maßnahmen.

3.3. Welche Verpflichtungen bestehen hinsichtlich der Meldung von Sicherheitsvorfällen?

3.3.1. Allgemeine Regeln

Art. 8, 5° und 57°; 34 und 35 NIS2-Gesetz

Ein Sicherheitsvorfall ist gesetzlich definiert als *"ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über Netz- und Informationssysteme angeboten werden bzw. zugänglich sind, beeinträchtigt"*.

Im Falle eines erheblichen Sicherheitsvorfalls muss die Einrichtung diesen dem nationalen CSIRT (ZCB) und in einigen Fällen auch den Empfängern ihrer Dienstleistungen melden.

Die Benachrichtigung erfolgt in mehreren Schritten (siehe Abschnitt 3.3.3.): zunächst eine Frühwarnung innerhalb von 24 Stunden nach Entdeckung des Sicherheitsvorfalls (*Early warning)*, dann eine ordnungsgemäße Meldung des Sicherheitsvorfalls innerhalb von 72 Stunden nach Entdeckung des Vorfalls (*Initial assessment of the incident)* und schließlich ein Abschlussbericht spätestens einen Monat nach der Meldung des Sicherheitsvorfalls (*Final report*). In der Zwischenzeit kann der nationale CSIRT Zwischenberichte anfordern.

Ein erheblicher Sicherheitsvorfall ist definiert als: "*jeder Vorfall, der erhebliche Auswirkungen auf die Erbringung von Dienstleistungen in den in den Anhängen des NIS2-Gesetzes aufgeführten Sektoren oder Teilsektoren hat und der:*

1. *schwerwiegende Betriebsstörungen eines der in den in Anhang I und II aufgeführten Sektoren oder Teilsektoren erbrachten Dienstes oder einen finanzielle Verluste 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.*"

In der Praxis wird das ZCB Empfehlungen dazu abgeben, in welchen Fällen eine Meldung erforderlich ist und wie das Verfahren aussehen sollte.

3.3.2. Empfänger einer obligatorischen Meldung eines erheblichen Sicherheitsvorfalls

Grundsätzlich muss jede NIS2-Einrichtung einen Sicherheitsvorfall nur dem ZCB melden. Das ZCB leitet die Meldungen an etwaige sektorale Behörden sowie an das Krisenzentrum (für wesentliche Einrichtungen) weiter.

Art. 34, §1 NIS2-Gesetz

Diese Regel gilt jedoch nicht für Einrichtungen, die unter die DORA-Verordnung im Banken- und Finanzsektor fallen. Die Einrichtungen in diesen beiden Sektoren melden ihren Sicherheitsvorfall je nach Fall der Belgischen Nationalbank (BNB) oder der Finanzdienstleistungs- und Marktaufsichtsbehörde (FSMA), die die Meldung des Vorfalls automatisch an das ZCB weiterleiten.

Gegebenenfalls teilt die Einrichtung den Empfängern ihres Dienstes erhebliche Sicherheitsvorfälle mit, die die von der Einrichtung erbrachten Dienste beeinträchtigen könnten. Sie teilt den Empfängern, die potenziell von einer bedeutenden Cyberbedrohung betroffen sind, auch alle Korrekturen und Maßnahmen mit, die sie als Reaktion darauf anwenden können.

Art. 34, §2 NIS2-Gesetz

3.3.3. Verfahren zur Meldung eines Sicherheitsvorfalls

Die Meldung von erheblichen Sicherheitsvorfällen erfolgt in mehreren Schritten:

Art. 35 NIS2-Gesetz

1. unverzüglich, in jedem Fall aber innerhalb von 24 Stunden nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, übermittelt die Einrichtung eine Frühwarnung;

2. unverzüglich, in jedem Fall aber innerhalb von 72 Stunden (24h für Vertrauensdienstanbieter) nach Kenntnisnahme des erheblichen Sicherheitsvorfalls, übermittelt die Einrichtung eine Meldung über den Sicherheitsvorfall;
3. auf Ersuchen eines CSIRT oder gegebenenfalls der zuständigen Behörde übermittelt die Einrichtung einen Zwischenbericht über relevante Statusaktualisierungen;
4. spätestens einen Monat nach Übermittlung der Meldung des Sicherheitsvorfalls gemäß Punkt 2, übermittelt die Einrichtung einen Abschlussbericht;
5. im Falle eines andauernden Sicherheitsvorfalls zum Zeitpunkt der Vorlage des Abschlussberichts, übermittelt die betroffene Einrichtung einen Fortschrittsbericht und dann, innerhalb eines Monats nach Behandlung des Sicherheitsvorfalls, einen Abschlussbericht.

In der Praxis wird die Benachrichtigung über das auf der ZCB-Website eingerichtete Verfahren erfolgen.

3.3.4. Informationen, die bei der Meldung eines Sicherheitsvorfalls übermittelt werden müssen

Die verschiedenen Schritte der Meldung beinhalten unterschiedliche Informationen, die übermittelt werden müssen :

Art. 35 NIS2-Gesetz

- Die Frühwarnung gibt an, ob der Verdacht besteht, dass der erhebliche Sicherheitsvorfall durch rechtswidrige oder böswillige Handlungen verursacht worden sein könnte, und ob er grenzüberschreitende Auswirkungen haben könnte. Diese Frühwarnung umfasst nur die Informationen, die erforderlich sind, um den Sicherheitsvorfall dem CSIRT zur Kenntnis zu bringen, und ermöglicht es der betroffenen Einrichtung gegebenenfalls Unterstützung anzufordern.
  Diese Warnung darf die Ressourcen der meldenden Einrichtung nicht von den Tätigkeiten im Zusammenhang mit der Bewältigung von Sicherheitsvorfällen abziehen. Diese sollten Vorrang haben, um zu verhindern, dass die Meldepflichten für Sicherheitsvorfälle die Ressourcen von der Bewältigung wichtiger Sicherheitsvorfälle abziehen oder die diesbezüglichen Bemühungen der Einrichtung auf andere Weise gefährden.
- Die Meldung eines Sicherheitsvorfalls innerhalb von 72 Stunden dient dazu, die im Rahmen der Frühwarnung mitgeteilten Informationen zu aktualisieren. Sie liefert außerdem eine erste Bewertung des Sicherheitsvorfalls, einschließlich des Schweregrads und der Auswirkungen, sowie Kompromittierungsindikatoren, sofern diese verfügbar sind.
  Wie bei der Frühwarnung dürfen auch bei der Meldung von Vorfällen keine Ressourcen der Einrichtung abgezogen werden, um zu vermeiden, dass die Meldepflichten für Vorfälle Ressourcen von der Bewältigung erheblicher Sicherheitsvorfälle abziehen oder die diesbezüglichen Bemühungen der Einrichtung auf andere Weise beeinträchtigen.
- Der Zwischenbericht enthält relevante Aktualisierungen der Situation.
- Der Abschlussbericht sollte eine detaillierte Beschreibung des Sicherheitsvorfalls enthalten, einschließlich der Schwere und der Auswirkungen, der Art der Bedrohung oder der tieferen Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat, der angewandten und laufenden Maßnahmen zur Schadensbegrenzung und gegebenenfalls der grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls.

- Der Fortschrittsbericht enthält so weit wie möglich die Informationen, die im Abschlussbericht enthalten sein sollten und die sich zum Zeitpunkt der Übermittlung des Fortschrittsberichts im Besitz der Einrichtung befanden.

3.3.5. Vertraulichkeitsregeln, die für die bei einem Sicherheitsvorfall übermittelten Informationen gelten

Art. 26, §3-4 NIS2-Gesetz

Die NIS2-Einrichtung und ihre Auftragsverarbeiter beschränken den Zugang zu Informationen über Sicherheitsvorfälle im Sinne des NIS2-Gesetzes auf diejenigen Personen, die zur Wahrnehmung ihrer Aufgaben oder Pflichten im Zusammenhang mit diesem Gesetz davon Kenntnis haben müssen und Zugang dazu benötigen.

Dies gilt auch für das ZCB (nationaler CSIRT), dem NCCN und der sektoralen Behörde.

Die dem ZCB, dem NCCN und der sektoralen Behörde von einer NIS2-Einrichtung zur Verfügung gestellten Informationen können mit Behörden anderer EU-Mitgliedstaaten und mit anderen belgischen Behörden ausgetauscht werden, wenn dieser Austausch für die Anwendung gesetzlicher Bestimmungen erforderlich ist.

Diese Informationsweitergabe beschränkt sich jedoch auf das, was für den Zweck dieses Austauschs relevant und verhältnismäßig ist, wobei die EU-Verordnung 2016/679 (DSGVO), die Vertraulichkeit der betroffenen Informationen, die Sicherheit und die Geschäftsinteressen der NIS2-Einrichtungen beachtet werden müssen.

3.4. Was passiert, wenn es zu einem Sicherheitsvorfall kommt, bei dem auch personenbezogene Daten betroffen sind?

Wie bereits jetzt werden die Sicherheitsvorfallmeldungen im Rahmen des Gesetzes nicht die möglichen Meldungen im Falle einer Verletzung personenbezogener Daten, z. B. an die belgische Datenschutzbehörde (DSB), ersetzen. Es werden weiterhin zwei getrennte Meldungen erforderlich sein.

Das Gesetz sieht jedoch eine verstärkte Zusammenarbeit zwischen der nationalen Behörde für Cybersicherheit und den Datenschutzbehörden vor. Diese Zusammenarbeit könnte zur Entwicklung gemeinsamer Instrumente führen.

Eine Benachrichtigung an die DSB kann auf deren Website erfolgen.

3.5. Ist es möglich, Sicherheitsvorfälle oder Cyberbedrohungen freiwillig zu melden?

Art. 38 NIS2-Gesetz

Ja. Das nationale CSIRT (ZCB) kann auch auf freiwilliger Basis, von NIS oder nicht-NIS2 Einrichtungen, Meldungen über Sicherheitsvorfälle, Cyberbedrohungen oder auch verhinderte Vorfälle erhalten.

Siehe dazu das in Abschnitt 3.3. erläuterte Verfahren.

3.6. Welche rechtlichen Bedingungen gelten für die Nutzung des Schutzrahmens bei der Suche und Meldung von Schwachstellen (ethisches Hacking)?

Das NIS2-Gesetz übernimmt die Bestimmungen des NIS1-Gesetzes, das einen Schutzrahmen (*safe harbour*) für "ethische Hacker" oder "digitale Whistleblower" vorsieht.

Art. 22 und 23 NIS2-Gesetz

Um von dem Schutzrahmen zu profitieren, muss eine Person :

- Ohne betrügerische oder schädliche Absicht handeln;
- Innerhalb von 24 Stunden nach der Entdeckung der Schwachstelle eine vereinfachte Meldung sowohl an das nationale CSIRT als auch an die verantwortliche Organisation senden;
- Innerhalb von 72 Stunden nach der Entdeckung eine vollständige Benachrichtigung an dieselben Adressaten senden;
- Nur innerhalb der Grenzen des Notwendigen und der Verhältnismäßigkeit handeln, um die Existenz einer Schwachstelle zu überprüfen und zu berichten;
- Es unterlassen eine Schwachstelle ohne Zustimmung des nationalen CSIRT öffentlich zu machen.

Außerdem müssen ethische Hacker, um die Netz- und Informationssysteme bestimmter Behörden wie Nachrichtendienste, dem Verteidigungsministerium, Justizbehörden, usw. nach Schwachstellen durchsuchen zu können, zunächst eine Vereinbarung mit diesen Einrichtungen treffen.

Das ZCB bietet auf ihrer Website allgemeine Informationen über ethisches Hacking an, einschließlich einer Seite, die dem Meldeverfahren gewidmet ist.

3.7. Wie registrieren sich NIS2-Einrichtungen?

Wesentliche und wichtige Einrichtungen müssen sich auf dem ZCB-Portal Safeonweb@Work registrieren.

Art. 13 NIS2-Gesetz

Die Frist für die Registrierung hängt von der Art der Einrichtung ab. Grundsätzlich haben wesentliche und wichtige Einrichtungen sowie Einrichtungen, die Domänennamen-Registrierungsdienste erbringen, **fünf Monate** nach Inkrafttreten des Gesetzes, d.h. bis zum **18. März 2025**, Zeit, sich zu registrieren. Bei der Registrierung müssen sie die folgenden Informationen bereitstellen:

1) Ihr Name und die Registrierungsnummer der Zentralen Datenbank der Unternehmen (ZDU) oder eine gleichwertige Registrierung in der Europäischen Union;
2) Ihre aktuelle Adresse und Kontaktangaben, einschließlich E-Mail-Adresse, IP-Adresse und Telefonnummer;
3) Gegebenenfalls der betreffende Sektor und Teilsektor gemäß Anhang I oder II des Gesetzes;
4) Gegebenenfalls eine Liste der Mitgliedstaaten, in denen sie Dienstleistungen erbringen, die in den Geltungsbereich des Gesetzes fallen.

Eine Ausnahme besteht für Einrichtungen, die diese Informationen bereits aufgrund einer gesetzlichen Verpflichtung einer sektoralen NIS2-Behörde mitgeteilt haben. In diesem Fall müssen die Informationen bei dieser Behörde lediglich vervollständigt werden. Wenn sich die Informationen ändern, müssen sie innerhalb von zwei Wochen nachgereicht werden.

Für die folgenden Arten von Einrichtungen aus den digitalen Sektoren gibt es eine leicht angepasste Regelung:

Art. 14 NIS2-Gesetz

- DNS-Dienstanbieter;
- TLD- Namensregister;
- Einrichtungen, die Domänennamen-Registrierungsdienste erbringen;
- Anbieter von Cloud-Computing-Diensten;
- Anbieter von Rechenzentrumsdienstleistungen;
- Anbieter von Inhaltszustellnetzen;
- Anbieter verwalteter Dienste;
- Anbieter verwalteter Sicherheitsdienste;
- Anbieter von Online-Marktplätzen;
- Anbieter von Online-Suchmaschinen; und
- Anbieter von Plattformen für Dienste sozialer Netzwerke.

Sie müssen sich innerhalb von **zwei Monaten** nach Inkrafttreten des Gesetzes, d.h. bis zum **18. Dezember 2024**, registrieren und die folgenden Informationen mitteilen:

1) Ihr Name;
2) Ihr Sektor, Teilsektor und die Art der Einrichtung, wie in Anhang I bzw. II aufgeführt;
3) Die Anschrift ihres Hauptgeschäftssitzes und ihrer sonstigen Niederlassungen in der Union oder, falls sie nicht in der Union niedergelassen sind, die Anschrift ihres Vertreters;
4) Ihre aktuellen Kontaktdaten, einschließlich E-Mail-Adressen und Telefonnummern, sowie ggf. die ihres Vertreters;
5) Die Mitgliedstaaten, in denen sie ihre Dienstleistungen erbringen, die in den Geltungsbereich des Gesetzes fallen;
6) Ihre IP-Adressbereiche.

Auch hier ist jede Einrichtung verpflichtet, das ZCB unverzüglich über jede Änderung ihrer Angaben zu informieren.

In der Praxis werden einige dieser Informationen direkt von der Zentralen Datenbank der Unternehmen (ZDU) während des Registrierungsprozesses eingeholt.

3.8. Wie verwaltet man als Einrichtung die Beziehungen zu seinen direkten Lieferanten und Auftragnehmern (*supply chain*)?

Die unter das NIS2-Gesetz fallenden Einrichtungen müssen geeignete und verhältnismäßige Maßnahmen ergreifen, um ihre Netz- und Informationssysteme zu sichern.

Art. 30, §3, 4° NIS2-Gesetz

Eine dieser Maßnahmen ist die Sicherheit der Lieferkette der betreffenden Einrichtung. Diese umfasst die sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern.

Auch wenn die Anforderungen des NIS2-Gesetzes nur für NIS2-Einrichtungen gelten, müssen diese dennoch sicherstellen, dass ihre unmittelbaren Anbieter und Diensteanbieter ähnliche Maßnahmen umsetzen. Um die Einhaltung ihrer gesetzlichen Verpflichtungen zu gewährleisten, kann eine NIS2-Einrichtung von ihren unmittelbaren Anbietern und Diensteanbietern vertraglich verlangen, dass sie über eine der im Rahmen des NIS2-Gesetzes anerkannten Zertifizierungen verfügen: CyFun® oder ISO 27001.

3.9. Wie vertraulich sind die ausgetauschten Informationen?

Art. 26 NIS2-Gesetz

Die zuständigen Behörden, wesentliche oder wichtige Einrichtungen und ihre Auftragsverarbeiter beschränken den Zugang zu Informationen im Rahmen des NIS2-Gesetzes auf Personen, die zur Wahrnehmung ihrer Aufgaben oder Pflichten im Zusammenhang mit der Durchführung des Gesetzes Kenntnis von den Informationen haben und/oder Zugang zu ihnen haben müssen.

Informationen, die den zuständigen Behörden von wesentlichen oder wichtigen Einrichtungen zur Verfügung gestellt werden, können jedoch mit Behörden in der Europäischen Union, mit belgischen Behörden oder mit ausländischen Behörden ausgetauscht werden, wenn ein solcher Austausch für die Anwendung von Rechtsvorschriften erforderlich ist.

Die ausgetauschten Informationen beschränken sich auf das, was relevant ist, und stehen in einem angemessenen Verhältnis zum Zweck des Informationsaustauschs, insbesondere im Einklang mit der Verordnung (EU) 2016/679 (DSGVO). Dieser Informationsaustausch wahrt die Vertraulichkeit der relevanten Informationen und schützt die Sicherheit und die Geschäftsinteressen wesentlicher oder wichtiger Einrichtungen.

Art. 27 NIS2-Gesetz

Das Gesetz sieht jedoch die Möglichkeit vor, freiwillig Informationen auszutauschen, die für die Cybersicherheit relevant sind, darunter insbesondere Informationen über Cyberbedrohungen, verhinderte Sicherheitsvorfälle, Schwachstellen, etc. Dieser Austausch findet unter bestimmten Bedingungen im Rahmen von Informationsaustauschgemeinschaften statt, die durch Vereinbarungen über die gemeinsame Nutzung von Informationen umgesetzt werden.

4. Kontrolle / Aufsicht

4.1. Wer sind die zuständigen Behörden?

Art. 15, 16 ff. NIS2-Gesetz und Art. 3 NIS2 Königlicher Erlass

4.1.1. Das Zentrum für Cybersicherheit Belgien (ZCB)

Die nationale Cybersicherheitsbehörde (ZCB) ist für die Koordinierung und Überwachung des Gesetzes zuständig. Zu diesem Zweck kombiniert das Gesetz die bestehenden Aufgaben der ZCB mit den in der NIS2-Richtlinie vorgesehenen Ergänzungen, insbesondere in Bezug auf die Aufsicht über Einrichtungen. Der ZCB ist für die Aufsicht über wesentliche und wichtige Einrichtungen zuständig (mit Unterstützung der sektoralen Behörden) und ist die zentrale Kontaktstelle für die Umsetzung von NIS2.

Das nationale Computersicherheits-Ereignis- und Reaktionsteam (*National Computer Security Incident Response Team*, CSIRT) ist ebenfalls Teil der nationalen Cybersicherheitsbehörde. Die NIS2-Einrichtungen sind verpflichtet, diesem CSIRT erhebliche Sicherheitsvorfälle zu melden.

4.1.2. Sektorspezifische Behörden

Die folgenden sektoralen Behörden wurden benannt:

1. **für den Energiesektor**: der für Energie zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Verwaltung (gegebenenfalls kann der Minister für jeden Teilsektor einen anderen Delegierten ernennen);
2. **für den Verkehrssektor** :
    a. In Bezug auf den Transportsektor, mit Ausnahme des Wassertransports: der für den Transport zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Verwaltung (gegebenenfalls kann der Minister für jeden Teilsektor einen anderen Delegierten ernennen);
    b. In Bezug auf den Wassertransport: der für die maritime Mobilität zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Verwaltung (gegebenenfalls kann der Minister für jeden Teilsektor einen anderen Delegierten ernennen);
3. **für den Gesundheitswesen-Sektor** :
    a. In Bezug auf Einrichtungen, die Einrichtungen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel ausüben; Einrichtungen, die pharmazeutische Erzeugnisse herstellen; und Einrichtungen, die Medizinprodukte herstellen, die während einer Notlage im Bereich der öffentlichen Gesundheit als kritisch eingestuft werden: die Föderale Agentur für Arzneimittel und Gesundheitsprodukte (AFMPS/FAGG);
    b. Der für Volksgesundheit zuständige Föderalminister, oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Verwaltung;
4. **für den Bereich digitale Infrastruktur: das** Belgische Institut für Postdienste und Telekommunikation (BIPT);

5. **in Bezug auf Vertrauensdienstanbieter**: der für Wirtschaft zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Behörde;
6. **für den Bereich der digitalen Anbieter**: der für Wirtschaft zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Behörde;
7. **für die Bereiche Raumfahrt und Forschung**: der für Wissenschaftspolitik zuständige Föderalminister oder, in seinem Auftrag, ein leitender Mitarbeiter seiner Behörde;
8. **für Trinkwasser**: das Nationale Sicherheitskomitee für die Bereitstellung und Verteilung von Trinkwasser;
9. **für den Bankensektor**: die Belgische Nationalbank (BNB);
10. **für den Bereich der Finanzmarktinfrastruktur**: die Finanzdienstleistungs- und Marktaufsichtsbehörde (FSMA).

Die sektoralen Behörden haben eine Reihe von Kompetenzen. Weitere Informationen finden Sie in Abschnitt 4.5.

Einrichtungen, die unter eine sektorale Behörde fallen, können sich an diese wenden, um Informationen und Unterstützung zu erhalten, usw.

4.1.3. Das Nationale Krisenzentrum (NCCN)

Das Nationale Krisenzentrum ist auch an der Umsetzung des NIS2-Gesetzes beteiligt, insbesondere in Bezug auf die Meldung von Sicherheitsvorfällen, das Cyber-Krisenmanagement und die von den Betreibern kritischer Infrastrukturen und kritischen Einrichtungen (die der CER-Richtlinie unterliegen) umgesetzten Maßnahmen zur Gewährleistung der physischen Sicherheit.

4.2. Können bestimmte Rahmenwerke von NIS2-Einrichtungen zum Nachweis ihrer Konformität verwendet werden?

Art. 5, §1 NIS2 Königlicher Erlass

Wesentliche Einrichtungen, die einer Pflicht zur regelmäßigen Konformitätsbewertung unterliegen, können sich für die Verwendung eines der beiden im Königlichen Erlass von NIS2 genannten Rahmenwerk entscheiden.

Die Verwendung dieser Rahmen zur Kontrolle wird im nächsten Abschnitt erläutert (4.3.).

4.2.1. Das CyberFundamentals (CyFun®) Framework

Das vom ZCB entwickelte Rahmenwerk der CyberFundamentals basiert auf mehreren gängig verwendeten Rahmenwerken oder Standards für Cybersicherheit, darunter NIST CSF, ISO 27001 / ISO 27002, CIS Controls und IEC 62443.

Es besteht aus der Ausgangsstufe Small und mehreren Sicherheitsstufen: Basic, Important und Essential (um den Risiken, denen eine Organisation ausgesetzt sein kann, am besten gerecht zu werden). Es gibt ein Tool, mit dem man die am besten geeignete Stufe auswählen kann.

Dieses Rahmenwerk ist kostenlos und öffentlich auf unserer Safeonweb@Work-Website verfügbar.

4.2.2. ISO/IEC 27001

Die europäische Norm ISO/IEC 27001 ist eine international anerkannte technische Norm, die den allgemeinen und strukturierten Ansatz für ein Sicherheitsmanagement für jedes Informationssystem festlegt. Es handelt sich also um eine Grundnorm, die die allgemeinen Grundsätze für die Umsetzung aller Sicherheitsmaßnahmen eines Informationssystems festlegt und in allen Sektoren anwendbar ist.

Die letzte Fassung stammt aus dem Jahr 2022, wurde aber ohne Angabe eines Datums in den Königlichen Erlass übernommen, damit immer die neueste Fassung angewendet werden kann.

4.3. Wie wird die Kontrolle der betroffenen Einrichtungen durchgeführt?

Wenn man im Zusammenhang mit dem Gesetz von Kontrolle/Aufsicht spricht, muss man zwischen zwei Kategorien von Einrichtungen unterscheiden: wesentliche Einrichtungen und wichtige Einrichtungen.

Art. 39 ff. NIS2-Gesetz
Art. 6-13 NIS2 Königlicher Erlass

Wesentliche Einrichtungen müssen sich einer regelmäßigen Konformitätsbewertung unterziehen. Diese Bewertung wird auf der Grundlage der von der Einrichtung getroffenen Wahl zwischen drei Optionen durchgeführt:

- entweder eine CyberFundamentals (CyFun®)-Zertifizierung, die von einer vom ZCB zugelassenen Konformitätsbewertungsstelle (KBS/CAB) vergeben wird (nach Akkreditierung durch BELAC);
- oder eine ISO/IEC 27001-Zertifizierung, die von einem CAB ausgestellt wurde, das von einer Akkreditierungsstelle akkreditiert wurde, die das Abkommen über die gegenseitige Anerkennung (MLA), unter das die ISO 27001-Norm fällt, im Rahmen der Europäischen Kooperation für Akkreditierung (EA) oder des Internationalen Akkreditierungsforums (IAF) unterzeichnet hat, und vom ZCB zugelassen wurde;
- oder eine Inspektion durch den Inspektionsdienst das ZCB (oder durch einen sektoralen Inspektionsdienst).

Der Inspektionsdienst kann auch jederzeit wesentliche Einrichtungen kontrollieren (wenn kein Sicherheitsvorfall vorliegt - *ex ante* - und nach einem Vorfall oder wenn genügend Beweise für die Nichteinhaltung des Gesetzes vorliegen - *ex post*).

Bei wichtigen Einrichtungen erfolgt die Aufsicht nur "*ex post*" durch den Inspektionsdienst, d.h. nach einem Sicherheitsvorfall oder aufgrund von Beweisen, Hinweisen oder Informationen, dass eine wichtige Einrichtung ihren Verpflichtungen nicht nachkommt (Art. 48, §2 NIS2-Gesetz). Daher unterliegen sie grundsätzlich keiner regelmäßigen Konformitätsbewertung. Diese Einrichtungen können sich jedoch freiwillig denselben Regelungen unterziehen wie wesentliche Einrichtungen.

Für die Modalitäten der vom Inspektionsdienst durchgeführten Inspektion siehe Abschnitt 4.10.

4.4. Was ist eine Konformitätsbewertungsstelle (KBS/CAB)?

Eine Konformitätsbewertungsstelle (*Conformity Assessment Body* - "CAB") ist eine Stelle, die die Einhaltung der Anforderungen des CyFun®-Rahmenwerks oder der ISO 27001 Norm (die im Rahmen des NIS2-Gesetzes angewendet wird) durch NIS2-Einrichtungen, die der regelmäßigen Konformitätsbewertung unterliegen (obligatorisch für wesentliche, freiwillig für wichtige Einrichtungen), überwacht und zertifiziert.

Im Rahmen von CyFun® ist ein CAB von der belgischen Akkreditierungsbehörde (BELAC) akkreditiert und von der ZCB zugelassen. Im Rahmen von ISO 27001 ist es von einer Akkreditierungsstelle akkreditiert, die das Abkommen über gegenseitige Anerkennung (MLA), unter das die Norm ISO 27001 fällt, im Rahmen der Europäischen Kooperation für Akkreditierung (EA) oder des Internationalen Akkreditierungsforums (IAF) unterzeichnet hat, und vom ZCB zugelassen.

CABs spielen in unserer Wirtschaft eine wichtige Rolle, um sicherzustellen, dass Unternehmen die ihnen auferlegten regulatorischen Anforderungen ordnungsgemäß erfüllen.

4.5. Was sind die Aufgaben der sektoralen Behörden?

Die sektoralen Behörden spielen im Rahmen des NIS2-Gesetzes ebenfalls eine Rolle, da sie über besonderes Wissen und Fachkenntnisse in den jeweiligen Sektoren verfügen. Sie können ggf. bei den folgenden Aufgaben tätig werden:

Art. 11, 13, 24, 25, 33, 34, 39, 44, 51 und 52 NIS2-Gesetz

- Zusätzliche Identifikation;
- Registrierung von Einrichtungen;
- Organisation von sektoralen Übungen;
- Analyse und Bewältigung der Folgen eines Sicherheitsvorfalls für einen Sektor;
- Teilnahme an einigen Arbeiten der NIS-Kooperationsgruppe;
- Sensibilisierung der Einrichtungen in ihren Sektoren;
- Zusammenarbeit auf nationaler Ebene;
- Zusätzliche Maßnahmen zum Management von Cybersicherheitsrisiken;
- Benachrichtigung über Sicherheitsvorfälle;
- Aufsicht und Inspektion (gemeinsam oder delegiert);
- Administrative Bußgelder.

4.6. Wie kann eine Einrichtung nachweisen, dass sie ihre Pflichten erfüllt?

Im Rahmen der regelmäßigen Konformitätsbewertung - die für wesentliche Einrichtungen obligatorisch ist - wird es für die Einrichtung möglich sein, eine Zertifizierung oder ein Siegel zu erhalten, bei dem bis zum Beweis des Gegenteils davon ausgegangen werden kann, dass die Einrichtung ihre Verpflichtungen in Bezug auf die Cybersicherheit erfüllt.

Art. 42 NIS2-Gesetz

Art. 5, §1 NIS2 Königlicher Erlass

Diese Zertifizierung wird auf den beiden im Königlichen Erlass genannten Rahmenwerken basieren: den CyberFundamentals oder der internationalen Norm ISO 27001 (mit dem richtigen Anwendungsbereich und *Statement of Applicability*). Siehe in diesem Zusammenhang Abschnitt 4.2.

Selbstverständlich kann eine Einrichtung auch einen anderes Rahmenwerk oder technischen Standard verwenden, um ihre rechtlichen Anforderungen an die Cybersicherheit umzusetzen. In diesem Fall gibt es jedoch keine Konformitätsvermutung, und dem Inspektionsdienst muss anhand einer Mapping-Tabelle mit einem der beiden genannten Standards nachgewiesen werden, dass alle erforderlichen Maßnahmen umsetzt wurden.

4.7. Kann eine Einrichtung eine niedrigere CyFun® Sicherheitsstufe als die ihrer Kategorie entsprechende verwenden?

Art. 7 NIS2 Königlicher Erlass

Ja, der Königliche Erlass lässt einer Einrichtung die Möglichkeit, eine niedrigere CyFun®-Stufe zu verwenden (z.B. die Verwendung der Sicherheitsstufe Important für eine wesentliche Einrichtung), sofern sie dies auf Grundlage ihrer Risikoanalyse objektiv rechtfertigen kann. Diese Entscheidung liegt in der alleinigen Verantwortung der betreffenden Einrichtung und hat keinen Einfluss auf ihre rechtliche Einstufung als wesentliche oder wichtige Einrichtung. Es ist zu betonen, dass diese Wahl jederzeit vom Inspektionsdienst im Rahmen seiner Kontrollaufgaben in Frage gestellt werden kann.

Die ZCB bietet ein auf Safeonweb@Work verfügbares Risikobewertungstool an, damit eine Einrichtung eine fundierte Auswahl der für sie geeigneten CyFun®-Sicherheitsstufe treffen kann.

4.8. Kann eine Einrichtung, die unter NIS1 ein Betreiber wesentlicher Dienste (BWD) war, ihre ISO27001-Zertifizierung behalten?

Art. 8, 12 und 14-15 NIS2 Königlicher Erlass

Wenn eine Einrichtung, die unter NIS1 Betreiber eines wesentlichen Dienstes (BWD) war, über eine ISO 27001 Zertifizierung verfügt, kann sie ihre Zertifizierung im Rahmen der von NIS2 ausgelegten regelmäßigen Konformitätsbewertung vorlegen. Bei Bedarf muss der Geltungsbereich der Zertifizierung erweitert werden, um sicherzustellen, dass sie alle Netz- und Informationssysteme der betreffenden Einrichtung abdeckt.

Die Zertifizierung muss von einer Konformitätsbewertungsstelle durchgeführt werden, die von BELAC in Belgien (oder von einer anderen akkreditierten europäischen nationalen Stelle, wenn die Zertifizierung aus einem anderen Mitgliedstaat stammt) akkreditiert und vom ZCB zugelassen ist.

4.9. Ab wann müssen die betroffenen Einrichtungen die Verpflichtungen aus dem Gesetz umsetzen?

Art. 13 & 75 NIS2-Gesetz

Art. 22-23 NIS2 Königlicher Erlass

Das NIS2-Gesetz und der NIS2 Königliche Erlass werden ab dem 18. Oktober 2024 in Kraft treten. **Ab diesem Zeitpunkt gelten** für wesentliche und wichtige Einrichtungen **alle Verpflichtungen** aus dem Gesetz und dem KE, sofern keine Ausnahmen bestehen (Cybersicherheitsmaßnahmen, Meldung von Sicherheitsvorfällen, usw.).

Abweichend davon wird die Registrierungspflicht zeitlich gestaffelt umgesetzt. Die Frist hängt von der Art der Einrichtung ab (siehe Abschnitt 3.7.) :

- Grundsätzlich haben die Einrichtungen nach Inkrafttreten des Gesetzes **fünf Monate Zeit,** um sich zu registrieren.
- Für Einrichtungen in bestimmten Sektoren, die mit Informations- und Kommunikationstechnologien zu tun haben (Cloud-Anbieter, DNS-Dienste, Datenzentren usw.), beträgt die Frist für die Registrierung **2 Monate** nach Inkrafttreten des Gesetzes.

Abweichend davon wird auch die regelmäßige Konformitätsbewertung wesentlicher Einrichtungen je nach gewähltem Referenzsystem schrittweise und differenziert umgesetzt:

- **18 Monate nach Inkrafttreten des Gesetzes,** d.h. vor dem 18. April 2026 :
  - Wer festlegt, dass er die Sicherheitsstufen CyFun® Basic oder Important einhalten muss, muss eine Überprüfung durch ein für CyFun® akkreditiertes und zugelassenes CAB durchführen lassen. Wer festlegt, dass er die Sicherheitsstufe CyFun® Essential einhalten muss, muss ebenfalls eine solche Basic oder Important Überprüfung ausführen lassen;
  - Diejenigen, die sich für eine Zertifizierung nach ISO 27001 entschieden haben, müssen den Anwendungsbereich und das *Statement of Applicability* an das ZCB übermitteln;
  - Diejenigen, die sich für die Inspektion durch das ZCB entschieden haben, müssen die CyFun®-Selbstbewertung oder die Informationssicherheitspolitik, den Anwendungsbereich und das *Statement of Applicability* von ISO 27001 an das ZCB übermitteln.
- **30 Monate nach Inkrafttreten des Gesetzes,** d.h. vor dem 18. April 2027 :
  - Wer festlegt, dass er die Sicherheitsstufe CyFun® Essential einhalten muss, muss zusätzlich zu der oben genannten Basic- oder Important-Verifizierung eine Zertifizierung durch ein CAB erhalten, das für CyFun® akkreditiert und zugelassen ist;
  - Diejenigen, die sich für eine ISO 27001-Zertifizierung entschieden haben, müssen eine Zertifizierung durch ein CAB erhalten, das für ISO 27001 akkreditiert und zugelassen ist;
  - Diejenigen, die sich für die Inspektion durch das ZCB entschieden haben, müssen einen Fortschrittsbericht über die Einhaltung der Vorschriften übermitteln.

Wichtige Einrichtungen sind nicht Gegenstand einer regelmäßigen obligatorischen Konformitätsbewertung (Ex-post-Aufsicht). Unter Beachtung der Angemessenheit und

Verhältnismäßigkeit der Cybersicherheitsmaßnahmen wird der Inspektionsdienst wichtige Einrichtungen beaufsichtigen, wobei ein ähnlicher Zeitraum von 18 Monaten nach Inkrafttreten des Gesetzes eingehalten werden muss (damit sie das erforderliche Niveau vollständig erreichen können).

Wenn sich beispielsweise Anfang 2025 ein bedeutender Cybervorfall ereignet, muss die betreffende Einrichtung die erforderlichen Maßnahmen zur Bewältigung dieses Vorfalls ergreifen und ihn dem ZCB melden, möglicherweise unter der Aufsicht der zuständigen Inspektionsdienste. Aus diesem Grund fordern wir alle NIS2-Einrichtungen auf, mit der Umsetzung der erforderlichen Maßnahmen nicht bis zum Ablauf der Registrierungsfrist und ihrer ersten Konformitätsbewertungen zu warten.

4.10. Wie wird die Inspektion durchgeführt?

Art. 44 ff. NIS2-Gesetz

Der Inspektionsdienst der nationalen Cybersicherheitsbehörde ist zuständig für das Durchführen von Inspektionen zur Überprüfung, ob wesentliche und wichtige Einrichtungen die Maßnahmen zum Management von Cybersicherheitsrisiken und die Vorschriften für die Meldung von Sicherheitsvorfällen einhalten.

Inspektionen wesentlicher Einrichtungen können sowohl *ex ante* (proaktiv) als auch *ex post* (reaktiv) durchgeführt werden. Sie werden vom Inspektionsdienst das ZCB oder vom benannten sektorielle Inspektionsdienst (spezifische/ergänzende sektorielle Maßnahmen) durchgeführt. Diese Inspektionen können auf Antrag der sektoriellen Behörde gemeinsam von den oben genannten Behörden durchgeführt werden.

Wesentliche Einrichtungen sind darüber hinaus verpflichtet, sich regelmäßigen Konformitätsbewertungen zu unterziehen. Wichtige Einrichtungen können sich auch freiwillig einer Konformitätsbewertung auf der Grundlage von ISO 27001 oder den CyberFundamentals unterziehen (siehe Abschnitt 4.3.).

Ex-post-Inspektionen wichtiger Einrichtungen werden auf der Grundlage von Indikatoren durchgeführt, wie z.B. dem Auftreten eines Sicherheitsvorfalls oder objektiven Beweisen für mögliche Mängel. Auch hier kann die Inspektion vom Inspektionsdienst des ZCB, dem benannten sektorielle Inspektionsdienst oder von beiden durchgeführt werden. Das Ziel der gemeinsamen Kontrollen oder der an den sektorielle Inspektionsdienst delegierten Kontrollen ist es zu vereinfachen und die staatlichen Ressourcen zu rationalisieren.

Die Inspektoren können sich vor Ort begeben, Feststellungen durch Protokolle treffen und Berichte verfassen. Auf der Grundlage dieser Feststellungen kann ein Verfahren eingeleitet werden, in dem die Einrichtung aufgefordert wird, einen Verstoß abzustellen und gegebenenfalls geeignete Verwaltungsmaßnahmen zu ergreifen, die von einer Verwarnung bis hin zu einem Bußgeld reichen können.

4.11. Sind Verwaltungsmaßnahmen und Geldstrafen verhältnismäßig? Wie hoch sind die Bußgelder?

Art. 59 NIS2-Gesetz

Das Ziel von Verwaltungsmaßnahmen und Geldstrafen ist es, die Cybersicherheit wesentlicher und wichtiger Einrichtungen zu

erhöhen. Unter Einhaltung der gesetzlich vorgeschriebenen Verfahren (einschließlich der Anhörung der betroffenen Einrichtung, siehe Art. 51-57) können verhältnismäßige Verwaltungsmaßnahmen oder Geldbußen verhängt werden, wobei die Schwere der Verstöße, das Verhalten der Einrichtung und mögliche Wiederholungsfälle berücksichtigt werden.

Die folgenden Verwaltungsmaßnahmen können verhängt werden:

1. 500 bis 125.000 Euro für jeden, der den Informationspflichten nach Artikel 12 nicht nachkommt;
2. 500 bis 200.000 Euro für die Einrichtung, die eine für sie handelnden Person negative Konsequenzen erleiden lässt, weil diese in gutem Glauben und im Rahmen ihrer Aufgaben ihren Verpflichtungen aus diesem Gesetz nachkommt;
3. 500 bis 200.000 Euro für jene, die ihren Kontrollpflichten nicht nachkommen;
4. 500 bis 7.000.000 Euro oder 1,4% des gesamten weltweit im vorangegangenen Geschäftsjahr erzielten Jahresumsatzes des Unternehmens, zu dem die wichtige Einrichtung gehört (je nachdem, welcher Betrag höher ist): für die wichtige Einrichtung, die ihren Verpflichtungen in Bezug auf Maßnahmen zum Management von Cybersicherheitsrisiken und/oder zur Meldung von Sicherheitsvorfällen nicht nachkommt;
5. 500 bis 10.000.000 Euro oder 2% des gesamten weltweit im vorangegangenen Geschäftsjahr erzielten Jahresumsatzes des Unternehmens, dem die wesentliche Einrichtung angehört (je nachdem, welcher Betrag höher ist): für die wesentliche Einrichtung, die ihren Verpflichtungen in Bezug auf Maßnahmen zum Management von Cybersicherheitsrisiken und/oder zur Meldung von Sicherheitsvorfällen nicht nachkommt.

Die Verwaltungsstrafe wird verdoppelt, wenn innerhalb von drei Jahren ein Rückfall für denselben Sachverhalt vorliegt.

Das Zusammentreffen mehrerer Verstöße kann zu einer einzigen Verwaltungsstrafe kommen, die der Schwere der gesamten Tat angemessen ist.

4.12. Welche anderen Verwaltungsmaßnahmen können ergriffen werden?

4.12.1. Grundlegende Maßnahmen

Gegen wesentliche und wichtige Einrichtungen können folgende Verwaltungsmaßnahmen verhängt werden:

Art. 58 NIS2-Gesetz

1. Warnungen wegen Gesetzesverstößen der betreffenden Einrichtungen aussprechen;
2. verbindliche Anweisungen oder eine Anordnung erlassen, in denen die betroffenen Einrichtungen aufgefordert werden, die festgestellten Mängel oder Rechtsverstöße zu beheben;
3. die betroffenen Einrichtungen anweisen, ein Verhalten, das gegen das Gesetz verstößt, zu beenden und es nicht zu wiederholen;
4. die betroffenen Einrichtungen anweisen, die Einhaltung ihrer Maßnahmen zum Management von Cybersicherheitsrisiken zu gewährleisten oder die festgelegten

Verpflichtungen zur Meldung von Sicherheitsvorfällen konkret und innerhalb einer bestimmten Frist zu erfüllen;
5. die betroffenen Einrichtungen anweisen, die natürlichen oder juristischen Personen, für die sie Dienstleistungen erbringen oder Tätigkeiten ausüben und die von einer erheblichen Cyberbedrohung betroffen sein könnten, über die Art der Bedrohung sowie über alle Präventiv- oder Abhilfemaßnahmen zu informieren, die diese natürlichen oder juristischen Personen als Reaktion auf die Bedrohung ergreifen könnten;
6. die betroffenen Einrichtungen anweisen, die nach einem Sicherheitsaudit ausgesprochenen Empfehlungen innerhalb einer angemessenen Frist umzusetzen;
7. die betroffenen Einrichtungen anweisen, die Aspekte von Gesetzesverstößen in besonderer Weise zu veröffentlichen;

Wenn es sich bei der betroffenen Einrichtung um eine wesentliche Einrichtung handelt :

- Das ZCB kann für einen bestimmten Zeitraum einen Kontrollbeauftragten mit genau festgelegten Aufgaben ernennen, der die Aufsicht darüber führt, dass die betreffenden Einrichtungen die Maßnahmen zum Management von Cybersicherheitsrisiken und zur Meldung von Sicherheitsvorfällen einhalten;
- Die verbindlichen Anweisungen nach Nummer 2 beziehen sich auch auf die Maßnahmen zur Vermeidung oder Behebung eines Sicherheitsvorfalls, sowie auf die Fristen für die Durchführung dieser Maßnahmen und die Berichterstattung über die Durchführung.

4.12.2. Zusätzliche Maßnahmen

Werden die geforderten Maßnahmen nicht innerhalb der gesetzten Frist ergriffen, können den wesentlichen Einrichtungen die folgenden Verwaltungsmaßnahmen auferlegt werden:

Art. 60 NIS2-Gesetz

1. das vorrübergehende Aussetzen eine Zertifizierung oder Genehmigung in Bezug auf alle oder einen Teil der von der betreffenden Einrichtung erbrachten einschlägigen Dienstleistungen oder durchgeführten Tätigkeiten;
2. das vorrübergehende Aussetzen der Führungsaufgaben einer natürlichen Person, die in der betreffenden Einrichtung auf der Ebene des Geschäftsführers oder des gesetzlichen Vertreters Führungsaufgaben wahrnimmt.

Die in Nummer 1 genannten vorübergehenden Aussetzungen oder Verbote werden nur so lange angewandt, bis die betreffende Einrichtung die erforderlichen Maßnahmen ergriffen hat, um die Mängel zu beheben oder den Anforderungen der zuständigen Behörde nachzukommen, die die Anwendung dieser Maßnahmen veranlasst hat.

4.13. Welche Pflichten und Verantwortlichkeiten hat das Management?

Die Leitungsorgane der NIS2-Einrichtungen müssen die Maßnahmen zum Management von Cybersicherheitsrisiken genehmigen und deren Umsetzung überwachen. Verstößt die Einrichtung gegen ihre Verpflichtung zur Durchführung von Risikomanagementmaßnahmen, ist das Leitungsorgan dafür verantwortlich.

Art. 31 & 61 NIS2-Gesetz

Die Mitglieder des Leitungsorgans müssen eine Schulung absolvieren, um sicherzustellen, dass sie über ausreichende Kenntnisse und Fähigkeiten verfügen, um Risiken zu ermitteln und das Management von Cybersicherheitsrisiken und deren Auswirkungen auf die von der Einrichtung erbrachten Dienstleistungen zu bewerten.

Die Verantwortlichen und/oder gesetzlichen Vertreter einer NIS2-Einrichtung müssen befugt sein, die Einhaltung des NIS2-Gesetzes durch die Einrichtung zu gewährleisten. Sie haften für die Nichterfüllung dieser Pflicht.

Das Ziel dieser Verantwortlichkeit ist es, die Cybersicherheit zu einem Thema zu machen, das für die betroffenen Einrichtungen wirklich wichtig ist.

4.14. Was ist ein "Leitungsorgan"?

Der Begriff "Leitungsorgan" wird in der Richtlinie nicht definiert.

Aus europarechtlicher Sicht hat der Europäische Gerichtshof mehrfach darauf hingewiesen, dass erstens, wenn ein Wort oder ein Begriff im Rechtsinstrument nicht definiert ist, seine übliche Bedeutung zugrunde zu legen ist, und zweitens, wenn nicht anders angegeben, jeder Begriff im europäischen Recht dieselbe Definition haben sollte. Eine solche Definition kann in der Richtlinie 2013/36 in Artikel 3, §1, (7) gefunden *werden*: "*das Organ oder die Organe eines Instituts, das (die) nach nationalem Recht bestellt wurde (wurden) und befugt ist (sind), Strategie, Ziele und Gesamtpolitik des Instituts festzulegen und die Entscheidungen der Geschäftsleitung zu kontrollieren und zu überwachen, und dem die Personen angehören, die die Geschäfte des Instituts tatsächlich führen"*.

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.

5. Andere

5.1. Muss die Europäische Kommission noch Durchführungsrechtsakte erlassen?

Ja, ein Durchführungsrechtsakt, der von der Europäischen Kommission bis zum 17. Oktober 2024 angenommen werden muss, betrifft eine begrenzte Anzahl von Einrichtungen, die der Richtlinie unterliegen und für die bestimmte Modalitäten auf europäischer Ebene in harmonisierter Weise vorgesehen sind.

Artikel 21, § 5, Abschn. 1 der Richtlinie betrifft die technischen und methodischen Anforderungen im Zusammenhang mit Risikomanagementmaßnahmen für DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdiensteanbieter.

Artikel 23, § 11 der Richtlinie befasst sich mit dem Begriff des erheblichen Sicherheitsvorfalls für DNS-Diensteanbieter, TLD-Namenregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten sowie Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke.

In diesen Bestimmungen wird auch erwähnt, dass die Kommission soweit wie möglich europäische und internationale Normen und einschlägige technische Spezifikationen befolgen soll. Außerdem soll die Kommission mit der Kooperationsgruppe und der ENISA bei diesen Entwürfen für Durchführungsrechtsakte Ratschläge austauschen und zusammenarbeiten.

Konkret sollte der künftige Durchführungsrechtsakt ausschließlich auf Folgendes abzielen (die Kommission hat ihre Bereitschaft bekundet, wenn möglich beide Arten von Präzisierungen in einem einzigen Rechtsakt zu verabschieden):

- Einzelheiten zu den technischen und methodischen Anforderungen an die Risikomanagementmaßnahmen für diese spezifischen Einrichtungen;
- Einzelheiten zum Begriff des erheblichen Sicherheitsvorfalls für diese spezifischen Einrichtungen, mit Ausnahme der Vertrauensdiensteanbieter.

Die ENISA und die Arbeitsgruppen (*Workstreams*) der NIS-Kooperationsgruppe arbeiten derzeit daran, die Kommission bei der Vorbereitung des Komitologieverfahrens zu beraten.

Auf der Grundlage dieses Austauschs wird die Kommission einen Vorschlag für einen Durchführungsrechtsakt formulieren, der dann im NIS2-Ausschuss (sobald dieser formell eingesetzt ist) geteilt und diskutiert wird. Der Ausschuss wird die in der Verordnung (EU) Nr. 182/2011 genannten Komitologieregeln befolgen müssen.