CENTRE FOR CYBERSECURITY BELGIUM

TLP:CLEAR

9. April 2026

REF.: NCCA/JK/INS-001

EX-ANTE-AUFSICHT ÜBER WESENTLICHE EINRICHTUNGEN: Aufforderung zur Übermittlung von Informationen mit Frist zum 18. April 2026

An alle wesentlichen NIS2-Einrichtungen,

mit diesem Schreiben **erläutert** der NIS2-Inspektionsdienst[1] des Zentrums für Cybersicherheit Belgien (ZCB)[2], **welche Informationen dem ZCB bis zum 18. April 2026 übermittelt werden müssen**, **und fordert alle wesentlichen NIS2-Einrichtungen formell auf, diese Informationen** per E-Mail über die Adresse certification@ccb.belgium.be **an das ZCB zu übermitteln**. Im Falle sensibler Informationen kann zunächst ein sicherer Link für die Dateiübertragung angefordert werden.

Seit Inkrafttreten des NIS2-Gesetzes am 18. Oktober 2024 müssen alle NIS2-Einrichtungen insbesondere die erforderlichen Cybersicherheitsmaßnahmen ergreifen, um ihre Netzwerke und Informationssysteme zu schützen. Dazu gehören Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit[3]. Gleichzeitig ist der Inspektionsdienst befugt, diese Einrichtungen zu überwachen[4].

Der NIS2-Inspektionsdienst ist befugt, die Einhaltung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit durch wesentliche und wichtige Einrichtungen zu überwachen, insbesondere indem er Zugang zu allen für die Wahrnehmung seiner Aufsichtspflichten erforderlichen Dokumenten oder Informationen verlangt und eine Kopie davon erhält; indem er vor Ort oder aus der Ferne Untersuchungen, Inspektionen oder Anhörungen durchführt; und indem er alle Informationen anfordert, die er für die Bewertung der von der betreffenden Einrichtung getroffenen Risikomanagementmaßnahmen im Bereich der Cybersicherheit für erforderlich hält. Bei der Ausübung dieser Befugnisse zur Anforderung von Informationen muss der Inspektionsdienst den Zweck der Anforderung, die genau benötigten Informationen oder Nachweise sowie die Frist, innerhalb derer diese vorzulegen sind, angeben[5].

Der NIS2-Inspektionsdienst (NCCA) fordert alle wesentlichen Einrichtungen auf, die erforderlichen Informationen, wie nachstehend aufgeführt, bis spätestens 18. April 2026 vorzulegen, damit er die Implementierung der Risikomanagementmaßnahmen im Bereich der Cybersicherheit gründlich überprüfen kann.

---

[1] Siehe das Gesetz vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netzwerk- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (NIS2-Gesetz).
[2] Benannt als nationale Cybersicherheitsbehörde gemäß Artikel 3 § 1 des Königlichen Erlasses vom 9. Juni 2024 zur Implementierung des Gesetzes vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netzwerken und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (NIS2-KE).
[3] Art. 30, § 3, 6° NIS2-Gesetz.
[4] Titel 4 des NIS2-Gesetzes.
[5] Siehe insbesondere Art. 44 § 1 bis 2; 48 § 1 und 50 § 1 des NIS2-Gesetzes.

An das ZCB zu übermittelnde Informationen

Einrichtungen, die sich für ISO/IEC 27001 entschieden haben (3 mögliche Szenarien)[6]

1) Szenario 1: Die Organisation verfügt über ein von einem autorisierten CAB ausgestelltes ISO/IEC 27001-Zertifikat

Ihre Organisation muss keine weiteren Maßnahmen ergreifen. Das CAB wird die administrativen Formalitäten erledigen.

2) Szenario 2: Die Organisation verfügt über ein ISO/IEC 27001-Zertifikat, das von einem nicht autorisierten CAB ausgestellt wurde

Ihre Organisation muss die folgenden Dokumente an das ZCB senden[7]:

a. Anwendungsbereich des Zertifikats
b. Statement of Applicability – SoA des Zertifikats (einschließlich aller Cybersicherheitsmaßnahmen, die derzeit implementiert werden oder bereits implementiert wurden, entsprechend der CyFun®-Basic Sicherheitsstufe)
c. Aktueller (interner) Auditbericht, in dem die Implementierung dieser Cybersicherheitsmaßnahmen bewertet wird

Hinweis: Ab dem 18. April 2027 muss die Organisation ein Zertifikat von einem akkreditierten und autorisierten CAB erhalten (die Übertragung bestehender Zertifizierungen kann bei Bedarf erfolgen; CABs verfügen über entsprechende Verfahren).

3) Szenario 3: Die Organisation verfügt noch nicht über eine aktuelle ISO/IEC 27001-Zertifizierung

Ihre Organisation muss die folgenden Dokumente an das ZCB senden[8]:

a. Anwendungsbereich des zukünftigen Zertifikats
b. Statement of Applicability – SoA des zukünftigen Zertifikats (einschließlich aller Cybersicherheitsmaßnahmen, die derzeit implementiert werden oder bereits implementiert wurden, entsprechend der CyFun®-Basic Sicherheitsstufe)
c. Aktueller (interner) Auditbericht, in dem die Implementierung dieser Cybersicherheitsmaßnahmen bewertet wird

Hinweis: Ab dem 18. April 2027 muss die Organisation ein Zertifikat von einem akkreditierten und autorisierten CAB erhalten.

Einrichtungen, die sich für das CyberFundamentals Framework (CyFun®) entschieden haben (2 mögliche Szenarien)[9]

1) Szenario 1: Die Organisation hat bereits von einem autorisierten CAB einen Nachweis über die Einhaltung mindestens der CyFun®-Sicherheitsstufe „Basic“ erhalten

Das CAB kümmert sich um die administrativen Formalitäten. Ihre Organisation muss nichts weiter unternehmen.

[6] Art. 39, Abs. 1, 1° NIS2-Gesetz und Art. 5, § 1, 2° NIS2-KE.
[7] Art. 22, § 1, 2° NIS2-KE, in Verbindung mit Art. 44, § 1 bis 2; 48, § 1; und 50, § 1 NIS2-Gesetz.
[8] Art. 22, § 1, 2° NIS2-KE, in Verbindung mit Art. 44, § 1 bis 2; 48, § 1; und 50, § 1 NIS2-Gesetz.
[9] Art. 39, Abs. 1, 1° NIS2-Gesetz und Art. 5, § 1, 1° NIS2-KE.

2) Szenario 2: Die Organisation hat noch keinen Nachweis über die Einhaltung mindestens der CyFun®-Sicherheitsstufe „Basic“ von einem autorisierten CAB erhalten

Wir verlangen, dass bis zum Stichtag vom 18. April 2026 mindestens eine unterzeichnete Vereinbarung mit einem CAB für die Sicherheitsstufe CyFun® Basic vorliegt, auch wenn die eigentliche Verifizierung erst später erfolgt. Sie müssen keine weiteren Maßnahmen ergreifen als die genannte Verifizierung[10].

Einrichtungen, die sich für eine direkte Inspektion durch das ZCB entschieden haben[11]

Ihre Organisation muss einen formellen Antrag auf eine Inspektion beim ZCB einreichen (inspection@ccb.belgium.be).

Die Inspektion durch das ZCB ist eine alternative Option, die wesentlichen Einrichtungen im Rahmen des regulären Konformitätsbewertungsverfahrens angeboten wird und bei der kein CAB hinzugezogen wird. Es ist jedoch zu beachten, dass diese Option für die betroffenen Einrichtungen weniger vorteilhaft ist, da sie **keine Konformitätsvermutung begründet**. Es handelt sich daher um eine rein punktuelle Kontrolle, auf die sich die Einrichtung im Falle eines Sicherheitsvorfalls nicht in gleicher Weise berufen kann wie auf eine von einer CAB durchgeführte Verifizierung oder Zertifizierung, um sich zu verteidigen. Tatsächlich **obliegt es weiterhin der Einrichtung, nachzuweisen, dass sie ihren Verpflichtungen nachkommt**[12]. Verfügt eine wesentliche Einrichtung beispielsweise über eine Zertifizierung, so obliegt es dem ZCB, nachzuweisen, dass die Einrichtung ihren Verpflichtungen nicht nachkommt. Es ist daher ein erheblicher Vorteil, über eine solche Konformitätsvermutung zu verfügen.

Die direkt vom ZCB durchgeführte Konformitätsbewertung **erfolgt in Form eines Inspektionsverfahrens (mit möglichen Verwaltungsmaßnahmen und Sanktionen)**[13] **und ist nicht kostenlos**[14] – mit Ausnahme von Einrichtungen im Sektor der öffentlichen Verwaltung, die in Anhang I des NIS2-Gesetzes genannt sind und nicht unter Artikel 1 des Königlichen Erlasses vom 4. Mai 2016 zur Einrichtung des Föderalen Internen Auditdienstes liegen (Prüfung durch den FIA als NIS2-CAB).

Mit freundlichen Grüßen,

Johan Klykens (Signature)

Digitally signed by Johan Klykens (Signature)
Date: 2026.04.09 13:18:08 +02'00'

Johan KLYKENS
Direktor
Nationale Behörde für Cybersicherheitszertifizierung (NCCA) – NIS2-Inspektionsdienst
Zentrum für Cybersicherheit Belgien

[10] Art. 22, § 1, 1° NIS2-KE.
[11] Art. 39 Abs. 1, 2° NIS2-Gesetz; Art. 5, § 1 und 23, § 1 NIS2-KE.
[12] Art. 42 NIS2-Gesetz.
[13] Art. 48 ff. NIS2-Gesetz.
[14] Art. 20 NIS2-KE.

Wie lautet Ihre Antwortfrist?

Sie sind verpflichtet, innerhalb der festgelegten Frist zu antworten[15]. Wir können die Antwortfrist auf Ihren formellen schriftlichen Antrag hin verlängern. Sie müssen jedoch nachweisen, dass Sie berechtigte Gründe dafür haben:

- ein triftiger Grund, der belegt, dass mehr Zeit für die Sammlung von Beweismitteln benötigt wird
- eine schwere Erkrankung oder eine längere Abwesenheit
- ein Fall höherer Gewalt

Wie sollten Sie antworten?

Sie können Ihre Antwort an uns senden:

- per Post: CCB – NCCA – NIS2-Inspektionsdienst
  Rue de la Loi 18, 1000 Brüssel

- per E-Mail: certification@ccb.belgium.be

  Enthält Ihre Antwort Dateien, die zu groß oder zu sensibel sind, um per E-Mail versendet zu werden? In diesem Fall kontaktieren Sie uns bitte, damit wir Ihnen einen Datentransferdienst zur Verfügung stellen können.

Sind Sie in Verzug, haben nicht geantwortet oder haben eine unvollständige Antwort übermittelt?

Da Sie gesetzlich verpflichtet sind, innerhalb der festgelegten Frist zu antworten, können wir in diesem Fall eine Verwaltungsmaßnahme[16] oder eine Geldbuße[17] verhängen.

Welche Belege sind erforderlich?

Sie können sich dafür entscheiden, die angeforderten Belege nicht mit Ihrer Antwort einzureichen. In diesem Fall werden wir diese Unterlagen an Ihrer Adresse überprüfen. Dies hat keine administrativen Maßnahmen und Geldbußen zur Folge. Sie müssen uns jedoch innerhalb der festgelegten Frist kontaktieren, um einen Termin zu vereinbaren.

Haben Sie Fragen?

Für weitere Informationen können Sie sich jederzeit an uns wenden. Die in diesem Schreiben genannten Rechtsvorschriften können unter folgender Adresse eingesehen werden: https://www.ejustice.just.fgov.be/.

Schutz Ihrer personenbezogenen Daten?

Weitere Informationen darüber, wie wir Ihre personenbezogenen Daten gemäß den Datenschutzbestimmungen verarbeiten, finden Sie auf der Website des ZCB: https://ccb.belgium.be/de/personenbezogener-daten.

[15] Artikel 44, § 2 NIS2-Gesetz.
[16] Artikel 58 NIS2-Gesetz.
[17] Artikel 59 NIS2-Gesetz.