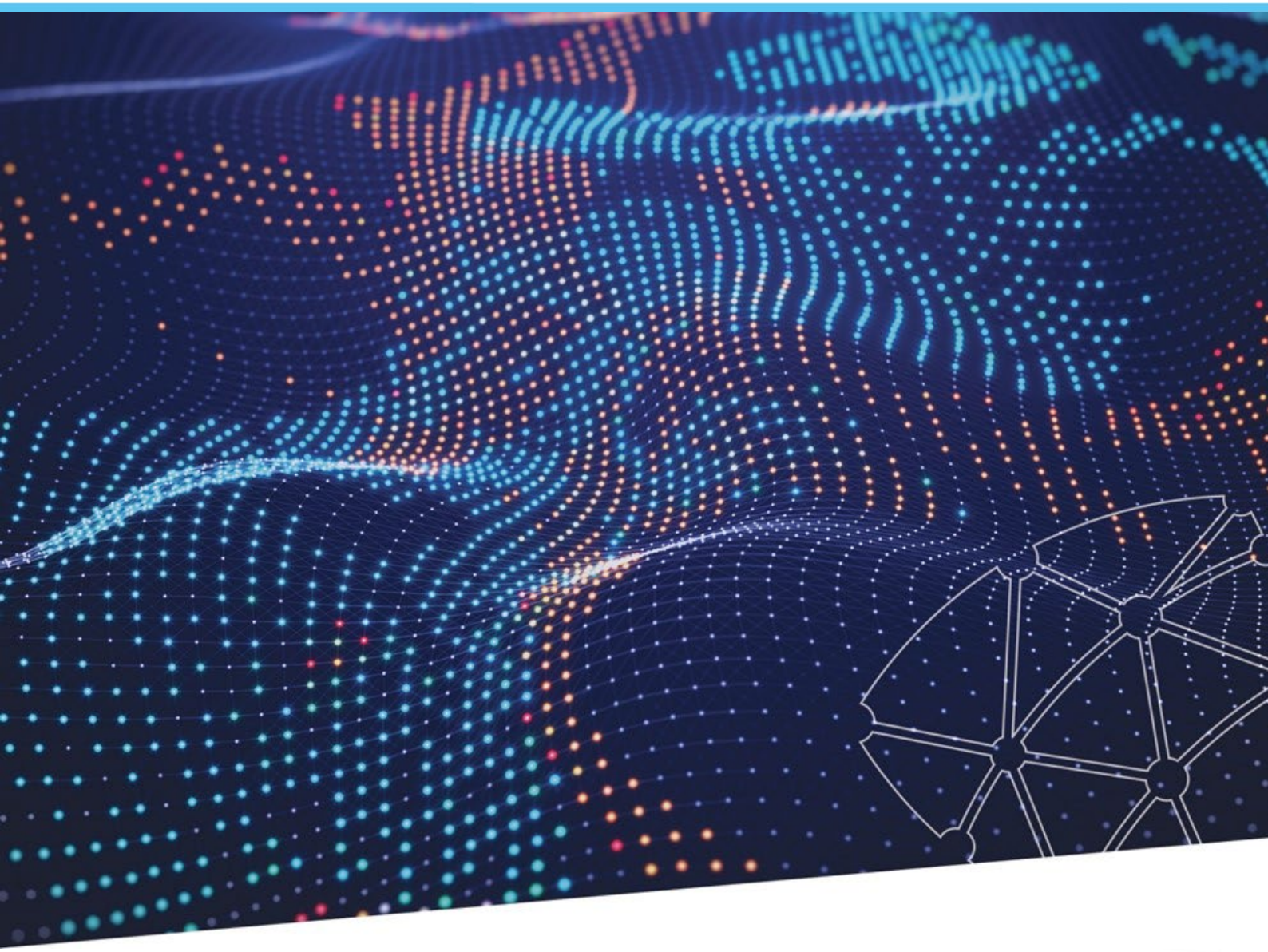
CENTRE FOR
CYBERSECURITY
BELGIUM



LEITFADEN ZUR MELDUNG VON NIS2-SICHERHEITSVORFÄLLEN

Version 10.2024 - 1.2

Centre for Cybersecurity Belgium
Under the authority of the Prime Minister

Einleitung

Das Gesetz vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit („NIS2-Gesetz“) setzt die EU-Richtlinie 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 („NIS2-Richtlinie“) in Belgien um.

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

Eine der wichtigsten Verpflichtungen, die sich aus der NIS2-Richtlinie und -Gesetzgebung ergeben, ist die Pflicht zur Information und Meldung von Sicherheitsvorfällen. Diese Verpflichtung zielt darauf ab, den betroffenen Einrichtungen Hilfe zu leisten, die verschiedenen zuständigen Behörden angemessen zu informieren, Warnmeldungen über bestimmte Bedrohungen an andere Einrichtungen weiterzuleiten und auf nationaler oder europäischer Ebene zusammenzuarbeiten.

Ziel des vorliegenden Dokuments ist es allgemeine Informationen über die Melde- und Informationspflichten gemäß dem NIS2-Gesetz bereitzustellen, das am 18. Oktober 2024 in Kraft getreten ist.

Inhaltsverzeichnis

A. Verpflichtende Meldungen

A.1. WELCHE EREIGNISSE MÜSSEN VON EINRICHTUNGEN, DIE DEM NIS2-GESETZ UNTERLIEGEN, GEMELDET WERDEN?

Die Meldung eines Ereignisses ist verpflichtend, wenn es sich um einen "erheblichen" Sicherheitsvorfall handelt. Dies beinhaltet zwei Elemente.

Erstens muss es sich um **einen Sicherheitsvorfall** im Sinne von Art. 8, 5° des NIS2-Gesetzes handeln: "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".

Zweitens muss es sich bei dem Vorfall um **einen erheblichen Sicherheitsvorfall** im Sinne von Art. 8, 57° des NIS2-Gesetzes handeln: " Jeder Sicherheitsvorfall, der erhebliche Auswirkungen auf die Erbringung einer der in den Anhängen I und II des Gesetzes aufgeführten Dienstleistungen hat und der:

1° schwerwiegende Betriebsstörungen eines der in den in Anhang I und II aufgeführten Sektoren oder Teilsektoren erbrachten Dienstes oder einen finanziellen Verlust für die betreffende Einrichtung verursacht hat oder verursachen kann, oder

2° andere natürliche oder juristische Personen durch erhebliche materielle, körperliche oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann".

A.2. WIE STELLT MAN FEST, OB EIN SICHERHEITSVORFALL ERHEBLICH IST ODER NICHT?

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

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

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

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

Um den Einrichtungen bei dieser Beurteilung eine Orientierungshilfe zu geben, hat das ZCB im Folgenden einige konkrete Situationen genannt, in denen der erhebliche Charakter eines Sicherheitsvorfalls von einer Einrichtung zumindest als gegeben angesehen werden sollte.

Die beschriebenen Situationen sind jedoch weder erschöpfend noch auf die verschiedenen erheblichen Sicherheitsvorfälle beschränkt, die auftreten können.

1) Ein mutmaßlicher böswilliger Vorfall, der die Authentizität, Integrität oder Vertraulichkeit von Daten in den Netz- oder Informationssystemen der Einrichtung gefährdet und zu einer schwerwiegenden Betriebsstörung führt oder führen kann

Ein solches Ereignis kann eintreten, wenn (einer dieser Umstände genügt):

- jemand einen Zugriff auf die Netze, Systemen oder Informationen erhalten hat, die die Erbringung der

Dienstleistung(en) der Einrichtung unterstützen, der größer ist als erwartet;
- ein System oder Netz, das die Erbringung der Dienstleistung(en) der Einrichtung unterstützt, von einer Person konfiguriert wurde oder werden kann, die nicht die Rechte zur Konfiguration des Systems oder Netzes der Einrichtung haben sollte;
- ein System oder Netz, das die Erbringung der Dienstleistung(en) der Einrichtung unterstützt, nicht mehr von privilegierten Benutzern konfiguriert werden kann, die die Rechte zur Konfiguration des Systems oder Netzes haben sollten;
- Konfigurationen oder Informationen der Systeme, die die Erbringung der Dienstleistung(en) der Einrichtung unterstützen, unrechtmäßig geändert, gelöscht, hinzugefügt oder unzuverlässig gemacht wurden;
- ein System oder Netz, das die Erbringung der Dienstleistung(en) der Einrichtung unterstützt, Aufgaben ausführt, die es nicht ausführen soll, oder Aufgaben nicht ausführt, die es ausführen soll, oder Aufgaben nicht ausführt, die es im Zusammenhang mit dem Zugang oder der Integrität des Systems oder Netzes ausführen soll.

Wenn sich beispielsweise ein böswilliger Akteur im Voraus in den Netz- und Informationssystemen einer betroffenen Einrichtung positioniert, um die Dienste in der Zukunft zu stören, muss der Sicherheitsvorfall als erheblich angesehen werden.

2) Ein Ereignis, das die Verfügbarkeit von Daten in den Netz- und Informationssystemen der Einrichtung beeinträchtigt und zu einer schwerwiegenden Betriebsstörung führt oder führen kann

Ein solches Ereignis könnte eintreten, wenn:

- mindestens 20 % der Nutzer mindestens eine Stunde lang keinen Zugang zum Dienst haben;
- die Nutzer den Zugang zum Dienst für mindestens eine Stunde verlieren und die Einrichtung die Zahl der betroffenen Nutzer nicht bestimmen kann (relativ oder absolut);
- das Ereignis eine Verzögerung bei der Lieferung der Produkte über die vertraglich garantierten Lieferzeiten hinaus verursacht.

Im Falle einer geplanten Wartungsabschaltung liegt kein Sicherheitsvorfall vor, wenn sich die Auswirkungen auf das Planmäßige beschränken.

Unter dem Begriff "Nutzer" sind die natürlichen und/oder juristischen Personen, Geschäftskunden und/oder Endkunden zu verstehen, mit denen die betreffende Einrichtung eine Vertragsbeziehung unterhält, die ihnen Zugang zu dem betreffenden Dienst oder den betreffenden Daten verschafft, und welche unter den Folgen des Sicherheitsvorfalls zu leiden haben oder zu leiden drohen. Zur Berechnung der Zahl der betroffenen Nutzer ist die Zahl der betroffenen natürlichen oder juristischen Personen, Geschäftskunden oder Endkunden zu berücksichtigen.

Die Dauer eines Sicherheitsvorfalls, der die Verfügbarkeit eines Dienstes beeinträchtigt, sollte ab dem Beginn der Störung der ordnungsgemäßen Erbringung des Dienstes bis zum Zeitpunkt der Wiederherstellung gemessen werden. Wenn eine betreffende Einrichtung nicht imstande ist, den Zeitpunkt des Beginns der Störung zu bestimmen, sollte die Dauer des Sicherheitsvorfalls ab dem Zeitpunkt gemessen werden, zu dem der Sicherheitsvorfall erkannt wurde, oder ab dem Zeitpunkt, zu dem der Sicherheitsvorfall in Netz- oder Systemprotokollen oder anderen Datenquellen aufgezeichnet wurde, je nachdem, welcher Zeitpunkt früher ist.

Von einer eingeschränkten Verfügbarkeit sollte insbesondere dann ausgegangen werden, wenn ein von einer betreffenden Einrichtung erbrachter Dienst deutlich langsamer als die durchschnittliche Antwortzeit ist oder wenn nicht alle Funktionen eines Dienstes verfügbar sind. Zur Bewertung von Verzögerungen bei der Antwortzeit sollten – soweit möglich – objektive Kriterien auf der Grundlage der durchschnittlichen Antwortzeiten der von den betreffenden Einrichtungen erbrachten Dienste herangezogen werden. Eine Funktion eines Dienstes kann beispielsweise aus einer Chat-Funktion oder einer Bildsuchfunktion bestehen.

3) Ein Ereignis, das einen finanziellen Verlust für die Einrichtung verursacht hat oder verursachen kann

Ein solches Ereignis könnte eintreten, wenn es folgendes bewirkt:

- ein direkter finanzieller Verlust von mehr als 250.000 € oder 5 % des gesamten Jahresumsatzes der betreffenden Einrichtung während des vorangegangenen vollen Geschäftsjahres, je nachdem, welcher

Betrag niedriger ist;
- der Verlust oder die Verbreitung von geistigem Eigentum in einer Weise, die künftige Einnahmen oder Umsätze gefährden könnte;
- den Abfluss von Geschäftsgeheimnissen im Sinne von Artikel 2 Absatz 1 Nummer 1 der Richtlinie (EU) 2016/943 aus der betreffenden Einrichtung.

Um die direkten finanziellen Verluste infolge eines Sicherheitsvorfalls zu bestimmen, müssen die betroffenen Einrichtungen alle finanziellen Verluste berücksichtigen, die sie infolge des Vorfalls erlitten haben, wie etwa:

- Kosten für die Ersetzung oder Verlegung von Software, Hardware oder Infrastruktur;
- Personalkosten, einschließlich Kosten im Zusammenhang mit der Ersetzung oder Verlegung von Personal, der Einstellung zusätzlichen Personals, der Vergütung von Überstunden und der Wiederherstellung verloren gegangener oder beeinträchtigter Kompetenzen;
- Gebühren wegen Nichteinhaltung vertraglicher Verpflichtungen;
- Kosten für Ausgleichs- und Entschädigungszahlungen an Kunden;
- Verluste wegen entgangener Einnahmen;
- Kosten für interne und externe Kommunikation;
- Beratungskosten, einschließlich Kosten im Zusammenhang mit Rechtsberatung, forensischen Dienstleistungen und Behebungsdienstleistungen;
- sonstige Kosten im Zusammenhang mit dem Sicherheitsvorfall.

Geldbußen wie auch Kosten, die für den laufenden Geschäftsbetrieb erforderlich sind, sollten jedoch nicht als finanzielle Verluste infolge eines Sicherheitsvorfalls betrachtet werden, darunter etwa:

- allgemeine Wartungskosten für Infrastruktur, Ausrüstung, Hardware und Software;
- die Qualifikation des Personals auf dem neuesten Stand zu halten;
- interne oder externe Kosten für die Verbesserung des Unternehmens nach dem Sicherheitsvorfall, einschließlich Upgrades;
- Verbesserungen und Initiativen zur Risikobewertung;
- Versicherungsprämien.

Die betreffenden Einrichtungen sollten die Höhe der finanziellen Verluste auf der Grundlage vorliegender Daten berechnen, und wenn die tatsächliche Höhe der finanziellen Verluste nicht bestimmt werden kann, sollten die Einrichtungen solche Beträge schätzen.

4) Ein Ereignis, das einen materiellen oder immateriellen Schaden verursacht hat oder verursachen kann, der andere natürliche oder juristische Personen betrifft

Ein solches Ereignis könnte eintreten, wenn es folgendes bewirkt:

- die teilweise oder vollständige Zerstörung physischer oder digitaler Vermögenswerte;
- Schäden an der physischen Infrastruktur, die zu einer Verzögerung bei der Lieferung von Produkten oder Dienstleistungen über die vertraglich garantierten Lieferzeiten hinaus führen;
- Schäden wie Tod, Krankenhausaufenthalt, Verletzung oder Behinderung;
- erhebliche finanzielle Folgen.

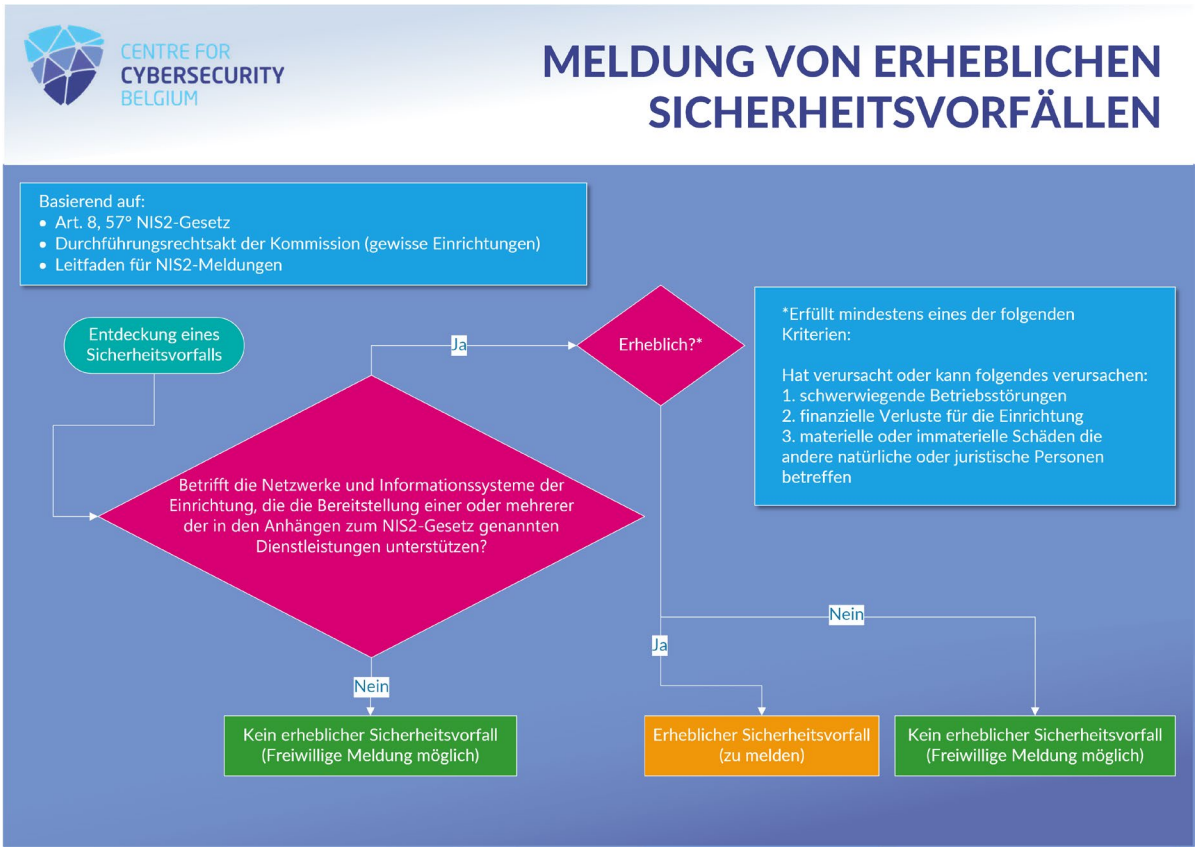
Die betreffenden Einrichtungen sollten auch verpflichtet sein, Sicherheitsvorfälle zu melden, die den Tod natürlicher Personen oder erhebliche Schädigungen der Gesundheit natürlicher Personen verursacht haben oder verursachen können, denn bei solchen Vorfällen handelt es sich um besonders schwere Fälle, die erhebliche materielle oder immaterielle Schäden verursachen. So könnte beispielsweise ein Sicherheitsvorfall, der eine betreffende Einrichtung beeinträchtigt, dazu führen, dass Gesundheits- oder Notdienste nicht zur Verfügung stehen oder dass die Vertraulichkeit oder Integrität von Daten verloren geht und sich dies auf die Gesundheit natürlicher Personen auswirkt.

Bei der Feststellung, ob ein Sicherheitsvorfall erhebliche Schädigungen der Gesundheit einer natürlichen Person verursacht hat oder verursachen kann, sollten die betreffenden Einrichtungen berücksichtigen, ob der Vorfall schwere Verletzungen und Erkrankungen verursacht hat oder verursachen kann. In dieser Hinsicht sollten die betreffenden Einrichtungen nicht dazu verpflichtet sein, zusätzliche Informationen einzuholen, die ihnen nicht zugänglich sind.

5) Ein wiederkehrendes Ereignis

Wiederholte Sicherheitsvorfälle, die offensichtlich dieselbe Ursache haben und einzeln betrachtet die Kriterien für einen erheblichen Sicherheitsvorfall nicht erfüllen, sollten zusammen dennoch als erheblicher Sicherheitsvorfall betrachtet werden, sofern sie zusammen das Kriterium für finanzielle Verluste erfüllen und zumindest zweimal innerhalb von sechs Monaten aufgetreten sind.

Solche wiederholten Sicherheitsvorfälle können auf erhebliche Mängel und Schwächen in den Verfahren für das Cybersicherheitsrisikomanagement der betreffenden Einrichtung und deren Reifegrad im Bereich der Cybersicherheit hindeuten. Darüber hinaus können solche wiederholten Sicherheitsvorfälle erhebliche finanzielle Verluste bei der betreffenden Einrichtung verursachen.



A.3. GIBT ES BESONDERE REGELN?

In der Durchführungsverordnung vom 17. Oktober 2024[1] hat die Europäische Kommission die Kriterien für die Beurteilung, ob ein Sicherheitsvorfall als "erheblich" anzusehen ist, für die folgenden Arten von Einrichtungen festgelegt:

- DNS-Dienstanbieter;
- TLD-Namenregister;
- Anbieter von Cloud-Computing-Diensten;
- Anbieter von Rechenzentrumsdiensten;
- Betreiber von Inhaltszustellnetzen;
- Anbieter verwalteter Dienste;
- Anbieter verwalteter Sicherheitsdienste;
- Anbieter von Online-Marktplätzen;
- Anbieter von Online-Suchmaschinen;
- Anbieter von Plattformen für Dienste sozialer Netzwerke;

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=pi_com%3AC(2024)7151

- Vertrauensdiensteanbieter.

Für die Einrichtungen, die von der Durchführungsverordnung betroffen sind, gelten diese besonderen Vorschriften (siehe Anhang 3). Im Falle von Widersprüchen zwischen diesem Leitfaden und den Bestimmungen der Durchführungsverordnung haben letztere für diese Einrichtungen Vorrang.

Einrichtungen des Banken- und Finanzmarktinfrastruktursektors im Sinne von Anhang I des NIS2-Gesetzes, die in den Anwendungsbereich der Verordnung (EU) 2022/2554 vom 14. Dezember 2022 über die digitale operationelle Widerstandsfähigkeit des Finanzsektors (DORA) fallen, einschließlich der von der Belgischen Nationalbank ausgeübten Tätigkeit als Zentralverwahrer, sind nicht den oben genannten Meldeverfahren verpflichtet.[2]

Darüber hinaus verwenden die als kritisch eingestuften Betreiber elektronischer Kommunikationsdienste die vom BIPT erstellte Eskalationsmatrix und implementieren die darin vorgesehenen Redundanzmittel. Darüber hinaus sollten die Artikel 34 und 35 des NIS2-Gesetzes dahingehend ausgelegt werden, dass eine Frühwarnung so schnell wie möglich erfolgen muss, wenn der zugrunde liegende Sicherheitsvorfall die Verfügbarkeit von Notfallkommunikation im Sinne von Artikel 2, 60° des Gesetzes vom 13. Juni 2005 über elektronische Kommunikation beeinträchtigt, da diese Kommunikation von großer Bedeutung ist und die Nichtverfügbarkeit dieser Kommunikation Auswirkungen auf das Leben oder die körperliche Unversehrtheit von Personen haben kann.

A.4. WANN MUSS EIN ERHEBLICHER SICHERHEITSVORFALL GEMELDET WERDEN?

Diese Meldefristen laufen ab dem Zeitpunkt, zu dem die Einrichtung Kenntnis von solchen erheblichen Vorfällen erlangt. Die betreffende Einrichtung muss daher Sicherheitsvorfälle melden, die nach der von ihr vorgenommenen Anfangsbewertung schwerwiegende Betriebsstörungen des Dienstes oder finanzielle Verluste für diese Einrichtung verursachen oder andere natürliche oder juristische Personen beeinträchtigen könnten, indem sie erhebliche materielle oder immaterielle Schäden nach sich ziehen.

Wenn also eine betreffende Einrichtung ein verdächtiges Ereignis feststellt oder ihr ein mutmaßlicher Sicherheitsvorfall von einem Dritten, z. B. von einer Person, einem Kunden, einer Einrichtung, einer Behörde, einer Medienorganisation oder aus anderer Quelle, zur Kenntnis gebracht wird, sollte sie das verdächtige Ereignis zeitnah bewerten, um festzustellen, ob es sich um einen Sicherheitsvorfall handelt, und, falls dies der Fall ist, seine Art und Schwere zu bestimmen. Es ist daher davon auszugehen, dass die betreffende Einrichtung von dem erheblichen Sicherheitsvorfall Kenntnis hatte, sobald sie nach einer solchen Anfangsbewertung mit hinreichender Gewissheit feststellt, dass ein erheblicher Sicherheitsvorfall vorliegt.

Sobald eine NIS2-Einrichtung mit hinreichender Gewissheit weiß, dass ein erheblicher Sicherheitsvorfall vorliegt, muss sie das nationale CSIRT (das ZCB) darüber informieren. Diese Meldung erfolgt in mehreren Schritten[3] :

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

Der Begriff "unverzüglich" bedeutet, dass die Einrichtung, die dazu in der Lage ist, den Sicherheitsvorfall so schnell wie möglich melden muss, ohne die Höchstfristen von 24 und 72 Stunden abzuwarten. Nur ordnungsgemäß begründete besondere Umstände können dazu führen, dass bis zum Ende dieser Fristen gewartet wird. Die Einhaltung der internen Verfahren der Organisation darf nicht zu einer unangemessenen Verzögerung der Meldung des Sicherheitsvorfalls führen.

[2] Art. 6, § 3 des NIS2-Gesetzes.
[3] Art. 35 des NIS2-Gesetzes und das untenstehende Bild.

Sollte der erhebliche Sicherheitsvorfall die Erbringung der in den Anhängen des Gesetzes aufgeführten Dienstleistungen beeinträchtigen, muss die Einrichtung auch die Empfänger ihrer Dienstleistungen (soweit diese identifizierbar sind) unverzüglich informieren. Diese Informationspflicht kann mit allen zur Verfügung stehenden Mitteln erfüllt werden (Informationen auf der Website, Mailingliste, Mitteilung in einer Anwendung, Mitteilungen auf Papier, usw.).

Die NIS2-Einrichtung muss außerdem den Empfängern ihrer Dienste, die potenziell von einer erheblichen Cyberbedrohung betroffen sind (siehe hiernach die Definition im Abschnitt "Freiwillige Meldungen"), unverzüglich alle Maßnahmen oder Korrekturen mitteilen, die diese Empfänger als Reaktion auf diese Bedrohung ergreifen können.

Das ZCB kann die von der Einrichtung erhaltenen Informationen im erforderlichen Umfang mit anderen Behörden teilen.

A.5. WIE SOLLTE DIE EINRICHTUNG EINEN SICHERHEITSVORFALL MELDEN?

Für jede der unter dem vorherigen Punkt genannten Stufen erfolgt die Meldung durch die betreffende Einrichtung über ein Online-Formular: **https://notif.safeonweb.be** (es sei denn, es ist nicht verfügbar oder technisch unmöglich). Die verschiedenen Felder des Online-Meldeformulars werden in Anhang 2 dieses Leitfadens erläutert.

Um mögliche Hindernisse bei der Meldung zu vermeiden und in Anbetracht der mutmaßlichen Notlage, in der sich eine Einrichtung befindet, ist für die Nutzung des Meldeformulars keine Authentifizierung erforderlich.

Eine Notrufnummer **(+32 (0)2 501 05 60)** ist ebenfalls verfügbar. Dieser Kanal soll es den Einrichtungen, die dies wünschen, ermöglichen, das nationale CSIRT im Notfall zu kontaktieren, wenn bei einem Sicherheitsvorfall ein sofortiges Eingreifen des nationalen CSIRT erforderlich ist. Wenn das Formular nicht verfügbar oder für die Einrichtung technisch nicht erreichbar ist, kann ein solcher Notruf als gleichwertig mit den in Artikel 35 des NIS2-Gesetzes genannten Meldungen angesehen werden.

A.6. BEI DER MELDUNG EINES ERHEBLICHEN SICHERHEITSVORFALLS ZU ÜBERMITTELNDE INFORMATIONEN

In den verschiedenen Phasen der Anmeldung sind unterschiedliche Arten von Informationen zu übermitteln (siehe Online-Formular):

- Die **Frühwarnung** (*Early Warning*) gibt an, ob der Verdacht besteht, dass der Sicherheitsvorfall durch illegale oder böswillige Handlungen verursacht wurde oder ob er grenzüberschreitende Auswirkungen haben könnte (d. h. Auswirkungen in einem anderen EU-Land). Diese Frühwarnung enthält nur die Informationen, die notwendig sind, um das CSIRT auf den Sicherheitsvorfall aufmerksam zu machen, und ermöglicht es der betroffenen Einrichtung, gegebenenfalls Unterstützung anzufordern.
  Eine solche Warnung sollte die Ressourcen der meldenden Einrichtung nicht von Aktivitäten zur Bewältigung von Sicherheitsvorfällen ablenken, die Vorrang haben sollten.
- Die **Meldung des Sicherheitsvorfalls** innerhalb von 72 Stunden dient dazu, die im Rahmen der Frühwarnung übermittelten Informationen zu aktualisieren. Sie enthält auch eine erste Bewertung des Sicherheitsvorfalls, einschließlich seines Schweregrads und seiner Auswirkungen, sowie Indikatoren für eine Kompromittierung (IOCs), sofern vorhanden.
  Wie bei der Frühwarnung sollten auch bei der Meldung von Sicherheitsvorfällen die Ressourcen der Einrichtung nicht von der Bewältigung erheblicher Sicherheitsvorfälle abgezogen werden.
- Der **Zwischenbericht** enthält relevante Aktualisierungen der Situation.
- Der **Abschlussbericht** sollte eine detaillierte Beschreibung des Sicherheitsvorfalls enthalten, einschließlich seiner Schwere und seiner Auswirkungen, der Art der Bedrohung oder der Ursache, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat, der angewandten und laufenden Abhilfemaßnahmen und gegebenenfalls der grenzüberschreitenden Auswirkungen des Vorfalls.
- Der **Fortschrittsbericht** enthält so viele Informationen wie möglich, die im Abschlussbericht enthalten sein sollten und die der Einrichtung zum Zeitpunkt der Vorlage des Fortschrittsberichts vorliegen.

B. Freiwillige Meldungen

Wesentliche und wichtige Einrichtungen können (nicht-erhebliche) Sicherheitsvorfälle, Cyberbedrohungen und Beinaheunfälle melden.

Eine Cyberbedrohung ist „ein möglicher Umstand, ein mögliches Ereignis oder eine mögliche Handlung, der/das/die Netz- und Informationssysteme, die Nutzer dieser Systeme und andere Personen schädigen, stören oder anderweitig beeinträchtigen könnte".[4]

Ein Beinahe-Vorfall ist „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 haben könnte, dessen Eintritt jedoch erfolgreich verhindert wurde bzw. das nicht eingetreten ist".[5]

Einrichtungen, die weder wesentlich noch wichtig sind, können erhebliche Sicherheitsvorfälle, Cyberbedrohungen und Beinahe-Unfälle melden.

Diese freiwilligen Meldungen werden auf die gleiche Weise bearbeitet wie verpflichtende Meldungen, aber verpflichtende Meldungen können dennoch vorrangig behandelt werden.

Eine freiwillige Meldung führt nicht unmittelbar zu einer Inspektion der Einrichtung, die die Meldung vorgenommen hat, und erlegt ihr keine zusätzlichen Verpflichtungen auf, denen sie ohne die Meldung nicht unterworfen gewesen wäre.[6]

[4] Art. 8, 10° des NIS2-Gesetzes und Art. 2, Punkt 8), der Verordnung (EU) 2019/881 - "CSA".
[5] Art. 8, 6° des NIS2-Gesetzes.
[6] Art. 38, § 2, Absatz 3 des NIS2-Gesetzes - unbeschadet der Vorbeugung, Erkennung, Untersuchung und Verfolgung von Straftaten.

C. Vertraulichkeitsregeln für Informationen, die bei einer Meldung übermittelt werden

Die NIS2-Einrichtung und ihre Unterauftragnehmer beschränken den Zugang zu Informationen über Sicherheitsvorfälle im Sinne des NIS2-Gesetzes auf diejenigen Personen, die davon Kenntnis haben müssen und diejenigen die Zugang zu diesen Informationen haben müssen, um ihre Funktionen oder Aufgaben im Zusammenhang mit diesem Gesetz wahrzunehmen. Diese Regel gilt auch für das ZCB (als nationales CSIRT), das nationale Krisenzentrum (NCCN) und jede zuständige sektorale Behörde.

Meldungen werden vom nationalen CSIRT unverzüglich an alle zuständigen sektoralen Behörden und an das NCCN weitergeleitet, wenn die Meldung von einer wesentlichen Einrichtung stammt.[7]

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

Diese Übermittlung von Informationen beschränkt sich jedoch auf das, was im Hinblick auf den Zweck dieses Austauschs relevant und verhältnismäßig ist, unter Einhaltung der Verordnung (EU) 2016/679 (DSGVO), der Vertraulichkeit der betreffenden Informationen, der Sicherheit und der geschäftlichen Interessen der NIS2-Einrichtungen.

D. Was geschieht, wenn ein Sicherheitsvorfall eintritt, der auch personenbezogene Daten betrifft?

Wie bereits bisher ersetzt die Meldung von Sicherheitsvorfällen nach dem NIS2-Gesetz nicht die Meldung einer Verletzung des Schutzes personenbezogener Daten, beispielsweise an die Datenschutzbehörde (DSB). Es sind nach wie vor zwei getrennte Meldungen erforderlich.

Das Gesetz sieht jedoch eine engere Zusammenarbeit zwischen der nationalen Cybersicherheitsbehörde und den Datenschutzbehörden vor. Diese Zusammenarbeit könnte zur Entwicklung von gemeinsamen Instrumenten führen.

Die DSB kann über ihre Website benachrichtigt werden.[8]

[7] Art. 34 des NIS2-Gesetzes.
[8] https://www.datenschutzbehorde.be/professionell/aktionen/datenverlust.

Anhang 1 - Übersichtstabelle - erheblicher Sicherheitsvorfall

Art des Ereignisses	Beispiele
Ein mutmaßlicher böswilliger Vorfall, der die Authentizität, Integrität oder Vertraulichkeit von Daten in den Netz- oder Informationssystemen der Einrichtung gefährdet und zu einer schwerwiegenden Betriebsstörung führt oder führen kann.	• jemand einen Zugriff auf die Netze, Systemen oder Informationen erhalten hat, die die Erbringung der Dienstleistung(en) der Einrichtung unterstützen, der größer ist als erwartet; • ein System oder Netz, das die Erbringung der Dienstleistung(en) der Einrichtung unterstützt, von einer Person konfiguriert wurde oder werden kann, die nicht die Rechte zur Konfiguration des Systems oder Netzes der Einrichtung haben sollte; • ein System oder Netz, das die Erbringung der Dienstleistung(en) der Einrichtung unterstützt, nicht mehr von privilegierten Benutzern konfiguriert werden kann, die die Rechte zur Konfiguration des Systems oder Netzes haben sollten; • Konfigurationen oder Informationen der Systeme, die die Erbringung der Dienstleistung(en) der Einrichtung unterstützen, unrechtmäßig geändert, gelöscht, hinzugefügt oder unzuverlässig gemacht wurden; • ein System oder Netz, das die Erbringung der Dienstleistung(en) der Einrichtung unterstützt, Aufgaben ausführt, die es nicht ausführen soll, oder Aufgaben nicht ausführt, die es ausführen soll, oder Aufgaben nicht ausführt, die es im Zusammenhang mit dem Zugang oder der Integrität des Systems oder Netzes ausführen soll.
Ein Ereignis, das die Verfügbarkeit von Daten in den Netz- und Informationssystemen der Einrichtung beeinträchtigt und zu einer schwerwiegenden Betriebsstörung führt oder führen kann	• mindestens 20 % der Nutzer mindestens eine Stunde lang keinen Zugang zum Dienst haben; • die Nutzer den Zugang zum Dienst für mindestens eine Stunde verlieren und die Einrichtung die Zahl der betroffenen Nutzer nicht bestimmen kann (relativ oder absolut); • das Ereignis eine Verzögerung bei der Lieferung der Produkte über die vertraglich garantierten Lieferzeiten hinaus verursacht; • geplante Wartungsarbeiten sollten nicht berücksichtigt werden (z. B. geplante Wartungsabschaltungen).
Finanzielle Verluste für die betroffene Einrichtung	• ein direkter finanzieller Verlust von mehr als 250.000 € oder 5 % des gesamten Jahresumsatzes der betreffenden Einrichtung während des vorangegangenen vollen Geschäftsjahres, je nachdem, welcher Betrag niedriger ist; • der Verlust oder die Verbreitung von geistigem Eigentum in einer Weise, die künftige Einnahmen oder Umsätze gefährden könnte; • den Abfluss von Geschäftsgeheimnissen im Sinne von Artikel 2 Absatz 1 Nummer 1 der Richtlinie (EU) 2016/943 aus der betreffenden Einrichtung.
Erheblicher materieller, physischer oder moralischer Schaden für andere natürliche oder juristische Personen	• die teilweise oder vollständige Zerstörung physischer oder digitaler Vermögenswerte; • Schäden an der physischen Infrastruktur, die zu einer Verzögerung bei der Lieferung von Produkten oder Dienstleistungen über die vertraglich garantierten Lieferzeiten hinaus führen; • Schäden wie Tod, Krankenhausaufenthalt, Verletzung oder Behinderung; • erhebliche finanzielle Folgen.

Ein wiederkehrendes Ereignis	• mindestens zweimal innerhalb eines Zeitraums von sechs Monaten; • die auf dieselbe offensichtliche Ursache zurückzuführen sind; • zusammen das Kriterium des finanziellen Verlustes (für die Einrichtung oder für Dritte) oder der Nichtverfügbarkeit erfüllen.

Anhang 2 - Erläuterung des Meldeformulars

Die verschiedenen Felder des Meldeformulars werden im Folgenden beschrieben. Die linke Spalte enthält den technischen Titel des Feldes (in eckigen Klammern) und den für die Benutzer sichtbaren Titel (in Fettdruck). Die rechte Spalte enthält die Beschreibung des Feldes. Die Felder sind in Abschnitte unterteilt, die jeweils einen eigenen technischen Titel haben (in eckigen Klammern und großgeschrieben).

[EINRICHTUNG, DIE DEN SICHERHEITSVORFALL MELDET]	
[A. Feldname: 1-Submission_Type] **Handelt es sich um eine Meldung, die unter das NIS2-Gesetz fällt?**	In diesem Feld können Sie angeben, ob Ihre Meldung in den Anwendungsbereich des NIS2-Gesetzes fällt (Pflichtfeld).
[B. Feldname: 2-Submitter] **Ich bin...**	In diesem Feld können Sie angeben, ob Sie eine NIS2-Einrichtung sind (Pflichtfeld).
[SPEZIFISCHE MERKMALE NIS]	
[C. Feldname: 3-NIS_Type] **Wie wird die Organisation im Rahmen des NIS2-Gesetzes kategorisiert?**	In diesem Feld können Sie angeben, ob Sie eine wichtige oder wesentliche Einrichtung im Sinne des NIS2-Gesetzes sind (Pflichtfeld).
[D. Feldname: 4-Sector] **In welchem/welchen Hauptsektor(en) ist die Organisation tätig?**	In diesem Feld können Sie den/die Sektor(en) angeben, in dem/denen Sie tätig sind. Es ist möglich, mehr als ein Kästchen anzukreuzen (Pflichtfeld).
[E. Feldname: 5-NIS_Notification] **Welche Art von NIS2-Sicherheitsvorfallmeldung reichen Sie ein?**	In diesem Feld können Sie angeben, in welchem Stadium des Meldeverfahrens Sie sich befinden. Zur Erinnerung: Die Phasen sind unter Punkt A. "Wann muss ein erheblicher Sicherheitsvorfall gemeldet werden?" beschrieben (Pflichtfeld).
[DETAILS ZUM SICHERHEITSVORFALL]	
[F. Feldname: 6-Malicious_Intent] **Vermuten eine böswillige Absicht hinter dem Sicherheitsvorfall?**	In diesem Feld können Sie angeben, ob der Sicherheitsvorfall Ihrer Meinung nach böswillig war. Wenn Sie es nicht wissen oder nicht überzeugt sind, kreuzen Sie bitte "Unsicher" an (Pflichtfeld).
[G. Feldname: 7-Incident_Type] **Art des Sicherheitsvorfalls**	In diesem Feld können Sie aus einer Liste von Ereignisarten diejenige(n) auswählen, die dem Sicherheitsvorfall entspricht/entsprechen, den Sie melden möchten. Es ist möglich, mehrere Kästchen anzukreuzen (Pflichtfeld).
[H. Feldname: 8-Incident_Date] **Wann hat sich der Vorfall ereignet?**	In diesem Feld können Sie das Datum im Format Monat/Tag/Jahr eingeben. Wenn Sie sich nicht sicher sind, können Sie in das folgende Feld (I.) alle Informationen über den Zeitpunkt des Sicherheitsvorfalls eingeben (optionales Feld).

[I. Feldname: 9-Incident_Description] **Beschreiben Sie den Sicherheitsvorfall (Ursache, Auswirkungen auf das Unternehmen, Name des Virus/der Malware, betroffene Daten und Systeme, ergriffene Maßnahmen, betroffene Betriebssysteme/Software, usw.)**	In diesem Feld können Sie die in Ihrem Besitz befindlichen Informationen über den Sicherheitsvorfall angeben, einschließlich Kompromittierungsindikatoren. Welche Informationen vorrangig zu übermitteln sind, entnehmen Sie bitte Punkt A.6. "Bei der Meldung eines erheblichen Sicherheitsvorfalls zu übermittelnde Informationen", in dem beschrieben wird, welche Informationen in den einzelnen Phasen der Meldung zu übermitteln sind. Bitte beachten Sie, dass das Formular spezifische Felder für die Ursachen, die Folgen und die Schwere des Sicherheitsvorfalls enthält. Sie haben maximal 500 Zeichen zur Verfügung (Pflichtfeld).
[J. Feldname: 9-Assessment_Severity] **Bitte geben Sie eine Einschätzung der Schwere des Sicherheitsvorfalls an**	In diesem Feld können Sie den Schweregrad des Sicherheitsvorfalls beschreiben. Im Rahmen der Frühwarnung kann eine solche Einschätzung sehr kurz und/oder unvollständig sein. Im Rahmen der Meldung innerhalb von 72 Stunden nach dem Sicherheitsvorfall müssen Sie eine erste Einschätzung des Schweregrads des Vorfalls abgeben. Im Rahmen des Abschlussberichts muss diese Bewertung detailliert sein. Sie haben maximal 500 Zeichen zur Verfügung (Pflichtfeld).
[K. Feldname: 11-Assessment_Consequence] **Was sind die Folgen des Sicherheitsvorfalls?**	In diesem Feld können Sie die Auswirkungen des Sicherheitsvorfalls beschreiben. Im Rahmen der Frühwarnung kann eine solche Bewertung sehr kurz und/oder unvollständig sein. Im Rahmen der Meldung innerhalb von 72 Stunden nach dem Sicherheitsvorfall müssen Sie eine erste Einschätzung der Auswirkungen des Vorfalls abgeben. Im Rahmen des Abschlussberichts muss diese Bewertung detailliert sein. Bitte beachten Sie, dass das Formular spezielle Felder zu den möglichen grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls enthält. Sie haben maximal 500 Zeichen zur Verfügung (Pflichtfeld).
[L. Feldname: 12-Threat_Type_Root_Cause] **Was war die Ursache des Sicherheitsvorfalls?**	In diesem Feld können Sie angeben, ob die Ursache des Sicherheitsvorfalls bekannt ist, und, falls ja, Informationen dazu liefern. Bitte beachten Sie, dass Sie in der endgültigen Berichtsphase die Art der Bedrohung oder die Ursache angeben müssen, die den Sicherheitsvorfall wahrscheinlich ausgelöst hat. Sie haben maximal 500 Zeichen zur Verfügung (Pflichtfeld).
[Mr Field Name: 13-Cross_Border_Impact**] Glauben Sie, dass dieser Sicherheitsvorfall zu grenzüberschreitenden Problemen führen könnte?**	In diesem Feld können Sie angeben, ob der Sicherheitsvorfall Ihrer Meinung nach grenzüberschreitende Auswirkungen hat. Wenn Sie es nicht wissen oder sich nicht sicher sind, kreuzen Sie "Unsicher" an. Bitte beachten Sie, dass Sie in der Abschlussberichtsphase gegebenenfalls die grenzüberschreitenden Auswirkungen des

	Sicherheitsvorfalls angeben müssen (Pflichtfeld).
[N. Feldname: 14-Cross_Border_Impact_Description **Bitte geben Sie Einzelheiten zu den grenzüberschreitenden Problemen an, die dieser Sicherheitsvorfall möglicherweise auslöst.**	In diesem Feld können Sie Angaben zu den grenzüberschreitenden Auswirkungen des Sicherheitsvorfalls machen. Bitte beachten Sie, dass dieses Feld nur erscheint, wenn Sie im vorherigen Feld (M.) "Ja" angekreuzt haben (optionales Feld).
[O. Feldname: 15-Police_Involved] **Haben Sie den Sicherheitsvorfall der Polizei gemeldet? (Wenn Sie Opfer eines Cyberangriffs geworden sind, raten wir Ihnen diesen bei der Polizei zu melden)**	In diesem Feld können Sie angeben, ob Sie den Sicherheitsvorfall bereits bei der Polizei gemeldet haben. Es ist ratsam, dies zu tun, wenn der Sicherheitsvorfall böswillig oder absichtlich herbeigeführt wurde (optionales Feld).
[P. Feldname: 16-Help_Needed] **Benötigen Sie eine Unterstützung, Untersuchung oder Beratung durch das ZCB?**	In diesem Feld können Sie gegebenenfalls ausdrücklich Unterstützung durch das ZCB anfordern, indem Sie das Feld "Ja" ankreuzen. Diese Unterstützung besteht in einer operativen Anleitung oder Beratung bei der Implementierung möglicher Abhilfemaßnahmen oder auch in zusätzlicher technischer Unterstützung (Pflichtfeld).
[Q. Feldname: 17-Help_Type_Needed**] Spezifizieren Sie so genau wie möglich, welche Unterstützung Sie vom ZCB benötigen**	In diesem Feld können Sie die Art der Unterstützung beschreiben, die Sie bei der Bewältigung des Sicherheitsvorfalls, der Anlass für die Meldung war, benötigen würden. Diese Unterstützung besteht aus operativen Leitlinien oder Ratschlägen für die Implementierung möglicher Abhilfemaßnahmen oder auch aus zusätzlicher technischer Unterstützung. Maximal 500 Zeichen (Pflichtfeld).
[R. Field Name: 18-Actions_Taken] **Welche Maßnahmen haben Sie ergriffen?**	In diesem Feld können Sie die Maßnahmen beschreiben, die zur Abschwächung und/oder Behebung des Sicherheitsvorfalls ergriffen wurden. Bitte beachten Sie, dass dieses Feld optional ist, Sie aber im Abschlussbericht die angewandten und laufenden Abhilfemaßnahmen beschreiben müssen. Sie haben 500 Zeichen zur Verfügung (optionales Feld).
[S. Field Name: 19-Resolved] **Ist der Sicherheitsvorfall jetzt gelöst?**	In diesem Feld können Sie angeben, ob der Sicherheitsvorfall zum Zeitpunkt der Meldung behoben wurde (Pflichtfeld).
[KONTAKTANGABEN DER EINRICHTUNG]	
[T. Feldname: 20-Anonymous]	Dieses Feld ist nicht sichtbar und gibt an, ob die Meldung anonym erfolgt.
[U. Field Name: 21-Contact_Person] **Kontaktperson**	In diesem Feld können Sie den Namen der Kontaktperson für die Verwaltung von

	Sicherheitsvorfällen eingeben (optionales Feld).
[V. Feldname: 22-Organization] **Name der Organisation**	In diesem Feld können Sie den Namen der Organisation angeben, in deren Namen die Meldung gemacht wird (Pflichtfeld).
[W. Feldname: 23-Email] **E-Mail**	In diesem Feld können Sie die E-Mail-Adresse eingeben, die vom ZCB verwendet werden kann, um die Organisation, die Opfer des Sicherheitsvorfalls ist, zu kontaktieren (Pflichtfeld).
[X. Feldname: 24-Telephone] **Telefonnummer**	In diesem Feld können Sie die Telefonnummer angeben, über die das ZCB die Organisation, die Opfer des Sicherheitsvorfalls ist, kontaktieren kann (Pflichtfeld).
[Y. Feldname: 25-Location] **Wo hat sich der Sicherheitsvorfall ereignet?**	In diesem Feld können Sie angeben, wo sich der Sicherheitsvorfall ereignet hat (optionales Feld).

Anhang 3 - Zusammenfassung der Regeln der Durchführungsverordnung der Kommission vom 17. Oktober 2024 (2024/7151) über die Meldung erheblicher Sicherheitsvorfälle

<table>
<tr><td colspan="2">Eine Einrichtung, die von der Durchführungsverordnung der Kommission vom 17. Oktober 2024 betroffen ist, muss einen Sicherheitsvorfall als "erheblich" betrachten, wenn entweder einer der Umstände, die allen Einrichtungen gemeinsam sind, oder einer der unten genannten spezifischen Umstände eintritt.</td></tr>
<tr><td colspan="2"><u>Gemeinsame Umstände für alle Einrichtungen, die von der Durchführungsverordnung betroffen sind</u> (Art. 3)

Planmäßige Betriebsunterbrechungen und geplante Folgen planmäßiger Wartungsarbeiten, die von oder im Auftrag der betreffenden Einrichtungen durchgeführt werden, gelten nicht als erhebliche Sicherheitsvorfälle.</td></tr>
<tr><td>Finanzielle Verluste für die betroffene Einrichtung</td><td>(a) der Vorfall hat der betreffenden Einrichtung einen direkten finanziellen Verlust in Höhe von mehr als 500 000 EUR oder 5 % ihres jährlichen Gesamtumsatzes im vorangegangenen Geschäftsjahr – je nachdem, welcher Wert niedriger ist – verursacht oder kann einen solchen Verlust verursachen;

(b) der Vorfall hat den Abfluss von Geschäftsgeheimnissen der betreffenden Einrichtung im Sinne von Artikel 2 Nummer 1 der Richtlinie (EU) 2016/943 verursacht oder kann einen solchen Abfluss verursachen.</td></tr>
<tr><td>Erheblicher materieller, physischer oder immaterieller Schaden für andere natürliche oder juristische Personen</td><td>c) der Vorfall hat den Tod einer natürlichen Person verursacht oder kann einen solchen Tod verursachen;

d) der Vorfall hat eine schwere Schädigung der Gesundheit einer natürlichen Person verursacht oder kann eine solche Schädigung verursachen.</td></tr>
<tr><td>Ein <u>mutmaßlicher böswilliger</u> Vorfall, der die Authentizität, Integrität oder Vertraulichkeit von Daten in den Netz- oder Informationssystemen der Einrichtung gefährdet und zu einer schwerwiegenden Betriebsstörung führt oder führen kann</td><td>(e) es hat einen erfolgreichen, mutmaßlich böswilligen und unbefugten Zugriff auf Netz- und Informationssysteme gegeben, der geeignet ist, schwerwiegende Betriebsstörungen zu verursachen.</td></tr>
<tr><td>Wiederkehrendes Ereignis (Art. 4)</td><td>(f) Sicherheitsvorfälle, die einzeln betrachtet nach Artikel 3 nicht als erhebliche Sicherheitsvorfälle angesehen werden, gelten zusammengenommen als ein erheblicher Sicherheitsvorfall, wenn sie alle folgenden Kriterien erfüllen:

- sie sind innerhalb von sechs Monaten mindestens zwei Mal aufgetreten;
- sie haben dieselbe offensichtliche Ursache;
- sie erfüllen zusammengenommen die in Artikel 3 Absatz 1 Buchstabe a aufgeführten Kriterien.

[der Vorfall hat der betreffenden Einrichtung einen direkten finanziellen Verlust in Höhe von mehr als 500 000 EUR oder 5 % ihres jährlichen Gesamtumsatzes im vorangegangenen Geschäftsjahr – je nachdem, welcher Wert niedriger ist – verursacht oder kann einen solchen Verlust verursachen.]</td></tr>
</table>

Besondere Umstände nach Art der Einrichtung (Art. 5 bis 14)

Bei der Berechnung der Zahl der von einem Sicherheitsvorfall betroffenen Nutzer für die Zwecke der Artikel 7 und Artikel 9 bis 14 berücksichtigen die betreffenden Einrichtungen Folgendes:

(a) die Zahl der Kunden, die mit der betreffenden Einrichtung einen Vertrag geschlossen haben, der ihnen Zugang zu den Netz- und Informationssystemen der betreffenden Einrichtung oder über diese Netz- und Informationssysteme angebotenen oder zugänglichen Diensten verschafft;

(b) die Zahl der natürlichen oder juristischen Personen, die mit Geschäftskunden verbunden sind, die Netz- und Informationssysteme der betreffenden Einrichtung oder über diese Netz- und Informationssysteme angebotene oder zugängliche Diensten nutzen.

DNS-Diensteanbieter (Art. 5)

(a) ein rekursiver oder autoritativer Dienst zur Auflösung von Domänennamen ist mehr als 30 Minuten lang vollständig nicht verfügbar;
(b) mehr als eine Stunde lang beträgt die durchschnittliche Antwortzeit eines rekursiven oder autoritativen Dienstes zur Auflösung von Domänennamen auf DNS-Anfragen mehr als 10 Sekunden;
(c) die Integrität, Vertraulichkeit oder Authentizität der Daten, die im Zusammenhang mit der Bereitstellung des autoritativen Dienstes zur Auflösung von Domänennamen gespeichert, übermittelt oder verarbeitet werden, ist beeinträchtigt, außer falls die Daten von weniger als 1 000 Domänennamen, die von dem DNS-Diensteanbieter verwaltet werden und die höchstens 1 % der von dem DNS-Diensteanbieter verwalteten Domänennamen ausmachen, aufgrund einer Fehlkonfiguration nicht korrekt sind.

TLD-Namenregister (Artikel 6)

(a) ein autoritativer Dienst zur Auflösung von Domänennamen ist vollständig nicht verfügbar;
(b) mehr als eine Stunde lang beträgt die durchschnittliche Antwortzeit eines autoritativen Dienstes zur Auflösung von Domänennamen auf DNS-Anfragen mehr als 10 Sekunden;
(c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem technischen Betrieb der TLD gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt.

Anbieter von Cloud-Computing-Diensten (Art. 7)

(a) ein erbrachter Cloud-Computing-Dienst ist mehr als 30 Minuten lang vollständig nicht verfügbar;
(b) die Verfügbarkeit eines Cloud-Computing-Dienstes eines Anbieters ist für mehr als 5 % der Nutzer des Cloud-Computing-Dienstes in der Union oder für mehr als 1 Million Nutzer des Cloud-Computing-Dienstes in der Union – je nachdem, welche Zahl niedriger ist – für eine Dauer von mehr als einer Stunde eingeschränkt;
(c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit der Erbringung eines Cloud-Computing-Dienstes gespeicherten, übermittelten oder verarbeiteten Daten ist infolge einer mutmaßlich böswilligen Handlung beeinträchtigt;
(d) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit der Erbringung eines Cloud-Computing-Dienstes gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt, und dies wirkt sich auf mehr als 5 % der Nutzer des Cloud-Computing-Dienstes in der Union oder auf mehr als 1 Million Nutzer des Cloud-Computing-Dienstes in der Union – je nachdem, welche Zahl niedriger ist – aus.

Anbieter von Rechenzentrumsdiensten (Art. 8)

(a) ein Rechenzentrumsdienst eines vom Anbieter betriebenen Rechenzentrums ist vollständig nicht verfügbar;
(b) die Verfügbarkeit eines Rechenzentrumsdienstes eines vom Anbieter betriebenen Rechenzentrums ist für eine Dauer von mehr als einer Stunde eingeschränkt;
(c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit der Erbringung eines Rechenzentrumsdienstes gespeicherten, übermittelten oder verarbeiteten Daten ist infolge einer mutmaßlich böswilligen Handlung beeinträchtigt;
(d) der physische Zugang zu einem von dem Anbieter betriebenen Rechenzentrum ist beeinträchtigt.

Betreiber von Inhaltszustellnetzen (Art. 9)

(a) ein Inhaltszustellnetz ist mehr als 30 Minuten lang vollständig nicht verfügbar;
(b) die Verfügbarkeit eines Inhaltszustellnetzes ist für mehr als 5 % der Nutzer des Inhaltszustellnetzes in der Union oder für mehr als 1 Million Nutzer des Inhaltszustellnetzes in der Union – je nachdem, welche Zahl niedriger ist – für eine Dauer von mehr als einer Stunde eingeschränkt;
(c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem Betrieb eines Inhaltszustellnetzes gespeicherten, übermittelten oder verarbeiteten Daten ist infolge einer mutmaßlich böswilligen Handlung beeinträchtigt;;
(d) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem Betrieb eines Inhaltszustellnetzes gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt, und dies wirkt sich auf mehr als 5 % der Nutzer des Inhaltszustellnetzes in der Union oder auf mehr als 1 Million Nutzer des Inhaltszustellnetzes in der Union – je nachdem, welche Zahl niedriger ist – aus.

Anbieter verwalteter Dienste und Anbieter verwalteter Sicherheitsdienste (Art. 10)

(a) ein verwalteter Dienst oder ein verwalteter Sicherheitsdienst ist mehr als 30 Minuten lang vollständig nicht verfügbar;
(b) die Verfügbarkeit eines verwalteten Dienstes oder verwalteten Sicherheitsdienstes ist für mehr als 5 % der Nutzer des Dienstes in der Union oder für mehr als 1 Million Nutzer des Dienstes in der Union – je nachdem, welche Zahl niedriger ist – für eine Dauer von mehr als einer Stunde eingeschränkt;
(c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit der Erbringung eines verwalteten Dienstes oder verwalteten Sicherheitsdienstes gespeicherten, übermittelten oder verarbeiteten Daten ist infolge einer mutmaßlich böswilligen Handlung beeinträchtigt;
(d) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit der Erbringung eines verwalteten Dienstes oder verwalteten Sicherheitsdienstes gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt, und dies wirkt sich auf mehr als 5 % der Nutzer des Dienstes in der Union oder auf mehr als 1 Million Nutzer des Dienstes in der Union – je nachdem, welche Zahl niedriger ist – aus.

Anbieter von Online-Marktplätzen (Art. 11)

(a) ein Online-Marktplatz ist für mehr als 5 % der Nutzer des Online-Marktplatzes in der Union oder für mehr als 1 Million Nutzer des Online-Marktplatzes in der Union – je nachdem, welche Zahl niedriger ist – vollständig nicht verfügbar;
(b) mehr als 5 % der Nutzer eines Online-Marktplatzes in der Union oder mehr als 1 Million Nutzer eines Online-Marktplatzes in der Union – je nachdem, welche Zahl niedriger ist – sind von einer eingeschränkten Verfügbarkeit des Online-Marktplatzes betroffen;
(c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem Betrieb eines Online-Marktplatzes gespeicherten, übermittelten oder verarbeiteten Daten ist infolge einer mutmaßlich böswilligen Handlung beeinträchtigt;
(d) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem Betrieb eines Online-Marktplatzes gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt, und dies wirkt sich auf mehr als 5 % der Nutzer des Online-Marktplatzes in der Union oder auf mehr als 1 Million Nutzer des Online-Marktplatzes in der Union – je nachdem, welche Zahl niedriger ist – aus.

Anbieter von Online-Suchmaschinen (Art. 12)

(a) eine Online-Suchmaschine ist für mehr als 5 % der Nutzer der Online-Suchmaschine in der Union oder für mehr als 1 Million Nutzer der Online-Suchmaschine in der Union – je nachdem, welche Zahl niedriger ist – vollständig nicht verfügbar;
(b) mehr als 5 % der Nutzer einer Online-Suchmaschine in der Union oder mehr als 1 Million Nutzer einer Online-Suchmaschine in der Union – je nachdem, welche Zahl niedriger ist – sind von einer eingeschränkten Verfügbarkeit der Online-Suchmaschine betroffen;
(c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem Betrieb einer Online-Suchmaschine gespeicherten, übermittelten oder verarbeiteten Daten ist infolge einer mutmaßlich böswilligen Handlung beeinträchtigt;
(d) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem Betrieb einer Online-Suchmaschine gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt, und dies wirkt sich auf mehr als 5 % der Nutzer der Online-Suchmaschine in der Union oder auf mehr als 1 Million Nutzer der Online-Suchmaschine in der Union – je nachdem, welche Zahl niedriger ist – aus.

Anbieter von Plattformen für Dienste sozialer Netzwerke (Art. 13)

(a) eine Plattform für Dienste sozialer Netzwerke ist für mehr als 5 % der Nutzer der Plattform für Dienste sozialer Netzwerke in der Union oder für mehr als 1 Million Nutzer der Plattform für Dienste sozialer Netzwerke in der Union – je nachdem, welche Zahl niedriger ist – vollständig nicht verfügbar;
(b) mehr als 5 % der Nutzer einer Plattform für Dienste sozialer Netzwerke in der Union oder mehr als 1 Million Nutzer einer Plattform für Dienste sozialer Netzwerke in der Union – je nachdem, welche Zahl niedriger ist – sind von einer eingeschränkten Verfügbarkeit der Plattform für Dienste sozialer Netzwerke betroffen;
(c) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem Betrieb einer Plattform für Dienste sozialer Netzwerke gespeicherten, übermittelten oder verarbeiteten Daten ist infolge einer mutmaßlich böswilligen Handlung beeinträchtigt;
(d) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit dem Betrieb einer Plattform für Dienste sozialer Netzwerke gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt, und dies wirkt sich auf mehr als 5 % der Nutzer der Plattform für Dienste sozialer Netzwerke in der Union oder auf mehr als 1 Million Nutzer der Plattform für Dienste sozialer Netzwerke in der Union – je nachdem, welche Zahl niedriger ist – aus.

Vertrauensdiensteanbieter (Art. 14)

(a) ein Vertrauensdienst ist mehr als 20 Minuten lang vollständig nicht verfügbar;
(b) ein Vertrauensdienst ist für Nutzer oder vertrauende Beteiligte im Laufe einer Kalenderwoche mehr als eine Stunde lang nicht verfügbar;
(c) mehr als 1 % der Nutzer oder vertrauenden Beteiligten in der Union oder mehr als 200 000 Nutzer oder vertrauende Beteiligte in der Union – je nachdem, welche Zahl niedriger ist – sind von einer eingeschränkten Verfügbarkeit eines Vertrauensdienstes betroffen;
(d) der physische Zugang zu einem Bereich, in dem sich Netz- und Informationssysteme befinden und zu dem nur vertrauenswürdiges Personal des Vertrauensdiensteanbieters Zugang hat, oder der Schutz dieses physischen Zugangs ist beeinträchtigt;
(e) die Integrität, Vertraulichkeit oder Authentizität der im Zusammenhang mit der Erbringung eines Vertrauensdienstes gespeicherten, übermittelten oder verarbeiteten Daten ist beeinträchtigt, und dies wirkt sich auf mehr als 0,1 % der Nutzer oder vertrauenden Beteiligten oder auf mehr als 100 Nutzer oder vertrauende Beteiligte des Vertrauensdienstes in der Union – je nachdem, welche Zahl niedriger ist – aus.

LEITFADEN ZUR MELDUNG VON NIS2-SICHERHEITSVORFÄLLEN

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

Alle Texte, Layouts, Designs und sonstigen Elemente jeglicher Art, die in diesem Dokument enthalten sind, sind dem Urheberrecht verpflichtet. Auszüge aus diesem Dokument dürfen nur für nicht-kommerzielle Zwecke und unter Angabe der Quelle vervielfältigt werden.

Das ZCB lehnt jegliche Haftung im Zusammenhang mit dem Inhalt dieses Dokuments ab.

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

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

Pflichtexemplar:
D/2024/14828/008