NIS2-Vorlagen für Vorfallsmeldungen — Artikel 23

Alle Stufen der NIS2-Meldung erheblicher Sicherheitsvorfälle als einreichungsfertige Formulare: die Frühwarnung binnen 24 Stunden, die Vorfallsmeldung binnen 72 Stunden, der Zwischen-/Fortschrittsbericht und der Abschlussbericht binnen eines Monats — die Inhaltsfelder folgen Artikel 23(4)(a)–(e) der Richtlinie (EU) 2022/2555, und die Erheblichkeitskriterien der DVO (EU) 2024/2690 sind in die Bewertungsfelder eingearbeitet.

Dieses PDF ist der Begleiter zum Ausdrucken und Prüfen. Die Arbeitsdateien sind die DOCX-Formulare; für KI-Agenten wird eine maschinenlesbare Markdown-Variante bereitgestellt. Alle drei Dateien sind kostenlos unter orbiqhq.com/templates/nis2-incident-reporting-pack verfügbar — ohne E-Mail-Adresse.

Rechtsgrundlage: Richtlinie (EU) 2022/2555 (NIS2), Artikel 23; Durchführungsverordnung (EU) 2024/2690 der Kommission. Keine Rechtsberatung; nationale Umsetzungsgesetze können zusätzliche Felder oder kürzere Fristen je Sektor vorsehen.

So verwenden Sie dieses Paket

So verwenden Sie dieses Paket: Füllen Sie Formular 0 (Eintrag im Vorfallsregister) einmalig aus und anschließend die Formulare 1–4, sobald die jeweiligen Fristen fällig werden. Reichen Sie die Meldungen über Ihren nationalen Kanal ein (in Deutschland: das Meldeportal des BSI; Österreich: das Meldeportal des BMI/GovCERT; Norwegen: NSM bzw. die zuständige Sektorbehörde; prüfen Sie das Portal Ihres CSIRT) — diese Formulare strukturieren den Inhalt so, dass die Einreichung eine Übertragung ist und kein Verfassen.

Formular 0 — Eintrag im Vorfallsregister (intern)

Einmalig bei Entdeckung ausfüllen und aktuell halten. Dies ist Ihre interne verbindliche Datenquelle, die jede Meldestufe speist.

Feld	Hinweise
Interne Vorfalls-ID	z. B. INC-2026-041
Name und Registrierung der Einrichtung	Rechtseinheit, wie bei der zuständigen Behörde registriert
Einstufung der Einrichtung	wesentliche Einrichtung / wichtige Einrichtung; Sektor und Teilsektor (Anhang I/II)
Einsatzleitung des Vorfalls	Name, Rolle, Telefon, E-Mail
Meldeverantwortliche Person	Person, die die Meldungen an das CSIRT bzw. die zuständige Behörde übermittelt
Datum und Uhrzeit der Entdeckung (mit Zeitzone)	Zeitpunkt, zu dem die Einrichtung KENNTNIS erlangt hat — hiermit beginnt die 24-Stunden-Frist
Quelle der Entdeckung	Monitoring-Alarm / Meldung durch Beschäftigte / Kundenmeldung / Dritte / Behörde
Betroffene Dienste und Systeme	Namen der Dienste, Umgebungen, Regionen
Bewertung der Erheblichkeit	welche Alternative des Art. 23(3) (schwerwiegende Betriebsstörung oder finanzieller Verlust / erheblicher Schaden für andere) oder welches Kriterium der DVO 2024/2690 erfüllt ist, und warum
Grenzüberschreitende Relevanz	Mitgliedstaaten oder Einrichtungen in anderen Mitgliedstaaten, die betroffen oder potenziell betroffen sind
Meldeprotokoll	Stufe / Zeitpunkt der Einreichung / Kanal / von der Behörde vergebenes Aktenzeichen

Formular 1 — Frühwarnung (binnen 24 Stunden)

Artikel 23(4)(a): unverzüglich, in jedem Fall aber binnen 24 Stunden nach Kenntniserlangung von dem erheblichen Sicherheitsvorfall einzureichen. Die Frühwarnung ist bewusst knapp gehalten — warten Sie für ihre Abgabe nicht auf den Abschluss der Analyse.

1. Meldende Einrichtung

Feld	Hinweise
Name der Einrichtung / Kennung bei der Behörde	
Ansprechpartner für diesen Vorfall	Name, Telefon, E-Mail — rund um die Uhr erreichbar

2. Zusammenfassung des Vorfalls

Feld	Hinweise
Interne Vorfalls-ID	
Datum/Uhrzeit der Kenntniserlangung	Zeitzone ausdrücklich angeben
Kurzbeschreibung	2–4 Sätze: was betroffen ist, aktueller Status
Betroffene Dienste	

3. Pflichtangaben der Frühwarnung — Art. 23(4)(a)

Feld	Hinweise
Verdacht auf rechtswidrige oder böswillige Ursache?	ja / nein / unbekannt — mit einzeiliger Begründung
Könnte der Vorfall grenzüberschreitende Auswirkungen haben?	ja / nein / unbekannt — potenziell betroffene Mitgliedstaaten benennen, soweit bekannt

4. Auf dieser Stufe optional

Feld	Hinweise
Unterstützung angefordert?	Einrichtungen können Unterstützung oder Hinweise des CSIRT anfordern
Andauernd / eingedämmt?	

Formular 2 — Vorfallsmeldung (binnen 72 Stunden)

Artikel 23(4)(b): unverzüglich, in jedem Fall aber binnen 72 Stunden nach Kenntniserlangung einzureichen. Sie aktualisiert die Frühwarnung und ergänzt eine erste Bewertung. Für Vertrauensdiensteanbieter kann das nationale Recht diese Meldung bereits binnen 24 Stunden verlangen.

1. Bezug

Feld	Hinweise
Interne Vorfalls-ID / Aktenzeichen der Frühwarnung	von der Behörde vergebenes Aktenzeichen aus Formular 1
Änderungen seit der Frühwarnung	Zusammenfassung dessen, was neu ist oder korrigiert wurde

2. Erste Bewertung — Art. 23(4)(b)

Feld	Hinweise
Bewertung des Schweregrads	Umfang der Störung, betroffene Nutzer/Empfänger, bisherige Dauer
Bewertung der Auswirkungen	betriebliche und finanzielle Auswirkungen (Schätzung), Auswirkungen auf Vertraulichkeit/Integrität/Verfügbarkeit der Daten
Kompromittierungsindikatoren (soweit verfügbar)	IoCs: Hashwerte, IP-Adressen, Domains, TTPs — bei größerem Umfang als strukturierte Datei beifügen
Erfüllte Erheblichkeitskriterien	Alternativen des Art. 23(3) und, soweit einschlägig, das Kriterium der DVO (EU) 2024/2690 (z. B. direkter finanzieller Verlust von mehr als 500.000 EUR oder 5 % des Jahresumsatzes, je nachdem, welcher Wert niedriger ist)

3. Stand der Reaktion

Feld	Hinweise
Ergriffene Eindämmungs-/Abhilfemaßnahmen	
Aktualisierung zu grenzüberschreitenden Aspekten	betroffene Mitgliedstaaten / benachrichtigte Stellen
Kommunikation gegenüber Empfängern der Dienste	ob die Empfänger über den Vorfall oder über Maßnahmen, die sie ergreifen können, informiert wurden (Art. 23(1)–(2)); etwaige behördliche Anordnungen zur Information der Öffentlichkeit vermerken

Formular 3 — Zwischen-/Fortschrittsbericht (auf Anforderung oder nach einem Monat bei andauerndem Vorfall)

Artikel 23(4)(c): Ein CSIRT oder eine zuständige Behörde kann einen Zwischenbericht mit relevanten Statusaktualisierungen anfordern. Artikel 23(4)(e): Dauert der Vorfall zum Fälligkeitszeitpunkt des Abschlussberichts noch an, reichen Sie stattdessen einen Fortschrittsbericht ein und den Abschlussbericht binnen eines Monats nach Abschluss der Bearbeitung des Vorfalls.

Feld	Hinweise
Bezug	Vorfalls-ID + Aktenzeichen der vorherigen Meldungen
Angefordert von / Auslöser	behördliche Anforderung oder Erreichen der Monatsfrist bei andauerndem Vorfall
Statusaktualisierung	aktueller Betriebszustand; Dienste wiederhergestellt / beeinträchtigt / ausgefallen
Aktualisierte Auswirkungszahlen	betroffene Nutzer, Ausfallzeit, finanzielle Schätzung
Neue Erkenntnisse	Fortschritt bei der Ursachenanalyse, neue IoCs, Änderungen des Umfangs
Nächste Schritte und erwarteter Zeitplan	

Formular 4 — Abschlussbericht (binnen eines Monats nach der 72-Stunden-Meldung)

Artikel 23(4)(d): spätestens einen Monat nach der Vorfallsmeldung aus Formular 2 einzureichen. Alle vier nachstehenden Inhaltselemente sind verpflichtend.

1. Ausführliche Beschreibung — Art. 23(4)(d)(i)

Feld	Hinweise
Darstellung des Vorfalls	Zeitleiste von der ersten Kompromittierung bis zur Behebung
Schweregrad und Auswirkungen	endgültige Zahlen: Dauer, betroffene Nutzer/Empfänger, betroffene Daten, finanzieller Verlust

2. Bedrohung und Ursache — Art. 23(4)(d)(ii)

Feld	Hinweise
Art der Bedrohung	z. B. Ransomware, Kompromittierung der Lieferkette, DDoS, Fehlkonfiguration
Grundursache	die wahrscheinlich auslösende Ursache, mit Nachweisen

3. Abhilfemaßnahmen — Art. 23(4)(d)(iii)

Feld	Hinweise
Umgesetzte Maßnahmen	abgeschlossene Behebung
Laufende Maßnahmen	mit Verantwortlichen und Terminen

4. Grenzüberschreitende Auswirkungen — Art. 23(4)(d)(iv)

Feld	Hinweise
Grenzüberschreitende Auswirkungen, soweit einschlägig	betroffene Mitgliedstaaten und Kategorien von Einrichtungen

5. Gewonnene Erkenntnisse (empfohlen)

Feld	Hinweise
Präventive Änderungen	Änderungen an Kontrollen, die in Ihre Risikomanagementmaßnahmen nach Art. 21 und Ihr ISMS einfließen
Überprüfung des Entdeckungs-/Meldeprozesses	wurden die 24-h-/72-h-Fristen eingehalten; was ist zu verbessern