

Der Countdown läuft

NIS2 und die Kunst der Meldepflicht

Stand: Juni 2026 · 150 Tage NIS2

25 Jahre ho.Systeme

Wo stehen wir heute?

06.12.

2025

Inkrafttreten
NIS2UmsuCG

50

TAGE

in Kraft seit
Verkündung

0

TAGE

Übergangsfrist
für Unternehmen

30K+

FIRMEN

neu unter
Regulierung

Die Kernbotschaft

Wer heute noch keine Gap-Analyse gemacht hat, ist faktisch bereits in einer Compliance-Lücke. Das Gesetz kennt keine Schonfrist.

Montag, 07:03 Uhr



„Die Systeme sind verschlüsselt. Die Produktion steht. Niemand kommt mehr an die Patientendaten.“

Drei Fragen, die jetzt **sofort** beantwortet sein müssen:

01

Sind wir meldepflichtig – und an wen?

02

Wer trifft die Entscheidung zu melden?

03

Was schreiben wir in den ersten 24 Stunden?

Die 24-72-30 Regel

Drei Meldungen. Drei Fristen. Keine Verhandlungsbasis.

24h

72h

30 Tage



FRÜHE ERSTMELDUNG

Erstmeldung an das BSI. Wurde der Vorfall wahrscheinlich durch eine rechtswidrige Handlung verursacht?

VORFALLSBERICHT

Erste Bewertung: Schwere, Auswirkungen, betroffene Systeme, erste Indikatoren der Kompromittierung.

ABSCHLUSSMELDUNG

Vollständiger Bericht inkl. Ursachen, ergriffener Maßnahmen, grenzüberschreitender Auswirkungen.



Die Uhr startet, sobald die **Kenntnisnahme** des Vorfalls vorliegt. **Nicht erst nach interner Klärung.**

Was ist „erheblich“?

Die schwierigste Frage: Wann ist ein Sicherheitsvorfall meldepflichtig?



MELDEPFLICHTIG

Erhebliche Sicherheitsvorfälle nach § 32 BSIG

- Schwerwiegende Betriebsstörung der Dienste
- Finanzielle Verluste für die Einrichtung
- Erhebliche Auswirkungen auf andere natürliche oder juristische Personen
- Ausnutzbare Schwachstelle wird aktiv ausgenutzt
- Kritische Infrastrukturen sind betroffen



INTERN DOKUMENTIEREN

Vorfälle ohne erhebliche Auswirkung

- Erfolgreich abgewehrte Angriffsversuche
- Phishing-Mails ohne Klick / ohne Kompromittierung
- Patches geschlossener Schwachstellen ohne Vorfall
- Kurzzeitige Störungen ohne Geschäftsauswirkung
- Aber: Lückenlos im Sicherheitsjournal dokumentieren!

Wer meldet? Wer haftet?

NIS2 trifft eine klare Antwort – und sie betrifft die Chefetage



CHEFSACHE

Die Geschäftsführung haftet
persönlich.

§ 38 BSIG verpflichtet die Geschäftsleitung, die
Umsetzung der Risikomanagement-Maßnahmen zu billigen
und ihre Umsetzung zu überwachen – persönlich, nicht
delegierbar.



GESCHÄFTSFÜHRUNG

Trifft die Entscheidung zu melden. Trägt die persönliche
Haftung. Kann Schulungspflicht nicht delegieren.



CISO / IT-SICHERHEIT

Bewertet Vorfall, koordiniert Reaktion, bereitet die Meldung
inhaltlich vor – auf Knopfdruck verfügbar.



KOMMUNIKATION & RECHT

Externe Kommunikation, ggf. Information der Nutzer,
Abstimmung mit Datenschutz (DSGVO-Schnittmenge).

Wenn die Meldung ausbleibt...

10 Mio. €

oder 2 % vom weltweiten Jahresumsatz

für besonders wichtige Einrichtungen

7 Mio. €

oder 1,4 % vom weltweiten Jahresumsatz

für wichtige Einrichtungen

Persönlich

Haftung der Geschäftsleitung

bei grober Pflichtverletzung

Reputationsschäden, Kundenverlust und Versicherungsprobleme sind in diesen Zahlen NICHT enthalten.

Der Meldeweg in der Praxis

Von der Detektion bis zur BSI-Meldung – fünf Schritte unter Zeitdruck



Faustregel: Wer den Meldeprozess nicht VORHER eingeübt hat, schafft die 24 Stunden nicht.

Die 5 häufigsten Fehler

Was Unternehmen unter Zeitdruck immer wieder falsch machen

01

„Wir warten erst ab“

Die Uhr läuft ab Kenntnisnahme, nicht ab forensischer Klarheit. Vorläufige Meldung ist Pflicht.

02

Niemand fühlt sich zuständig

Ohne festgelegte Meldekette verstreichen die ersten 6 Stunden mit interner Klärung.

03

Keine Vorlagen vorbereitet

Im Ernstfall fehlen Templates, Kontakte und Zugang zum BSI-Meldeportal.

04

DSGVO und NIS2 getrennt gedacht

Beide Meldepflichten greifen parallel – aber mit unterschiedlichen Fristen und Adressaten.

05

Lieferkette vergessen

Vorfälle bei Dienstleistern lösen ebenfalls Pflichten aus. Wer informiert wen?



Die Lösung:

Tabletop-Übungen. Mindestens zweimal im Jahr. Mit echter Stoppuhr.

Ihr 5-Punkte-Plan

Was Sie nach diesem Vortrag in 90 Tagen umsetzen können

WOCHE 1-2

● **Betroffenheit prüfen**

Sektor, Größe, Schwellenwerte gegen § 28 BSIg abgleichen. BSI-Betroffenheitsprüfung nutzen.

WOCHE 3-4

● **Meldekette definieren**

Wer detektiert, wer eskaliert, wer entscheidet, wer meldet. 24/7-Erreichbarkeit sicherstellen.

WOCHE 5-6

● **BSI-Registrierung**

Beim BSI registrieren. Frist für besonders wichtige Einrichtungen war 06. März 2026.

WOCHE 7-10

● **Templates & Tools**

Meldevorlagen für 24h/72h/30-Tage-Berichte vorbereiten. Zugriff auf Meldeportal testen.

WOCHE 11-12

● **Tabletop-Übung**

Realistisches Szenario mit Stoppuhr. Dokumentieren, was nicht funktioniert, und nachschärfen.

Was Sie heute mitnehmen

1

**Die Zeit ist
abgelaufen.**

NIS2 gilt in Deutschland seit dem 6.
Dezember 2025.
Ohne Übergangsfrist.
Wer wartet, ist schon zu spät.

2

**Melden ist
Chefsache.**

Die Geschäftsführung haftet
persönlich. Die 24-Stunden-Frist ist
nicht delegierbar.

3

**Ohne Probelauf
kein Ernstfall.**

Wer den Meldeprozess nicht
eingeübt hat, schafft die Frist im
Ernstfall nicht.

24

DIE FRAGE BLEIBT

Wissen Sie heute, wen Sie morgen früh anrufen müssen?

Wenn die Antwort „Nein“ lautet, ist das Ihr Auftrag für die nächsten 30 Tage.



Wir sind ho.Systeme



Martin Cerednik
Cyber Security Engineer

Kreisstraße 10
33790 Halle (Westf.)

Telefon: 05201 97177-354

E-Mail: martin.cerednik@hosysteme.de