Willkommen & Warum NIS2 wichtig ist

Willkommen bei NIS2 Ready. In den nächsten fünfundzwanzig Minuten erfahren Sie, was die NIS2-Richtlinie ist, warum es sie gibt und warum sie höchstwahrscheinlich relevanter für Ihre tägliche Arbeit ist, als Sie denken. Es sind keine Vorkenntnisse nötig — weder im Recht noch in der IT.

NIS2 Ready — Cybersicherheits-Compliance für die öffentliche Verwaltung & kritische Infrastruktur

Einheit 1 von 6 · Modul · ~25 Minuten · keine juristischen oder technischen Vorkenntnisse erforderlich

Ein Montagmorgen in der Stadtverwaltung Nordholm

Fangen wir nicht mit dem Gesetz an. Fangen wir mit einem ganz gewöhnlichen Montagmorgen in einer ganz gewöhnlichen Stadtverwaltung an — denn genau dort lebt NIS2 tatsächlich.

Es ist 8:14 Uhr an einem Montagmorgen in der **Stadtverwaltung Nordholm**, einer mittelgroßen deutschen Kommunalverwaltung — Bürgerservice, Genehmigungen, Sozialleistungen, all die Systeme, auf die sich eine ganze Stadt still und leise verlässt.

Eine IT-Administratorin bemerkt eine Häufung fehlgeschlagener Anmeldeversuche gegen das Bürgerportal, die sich über Nacht angesammelt haben. Es ist noch nichts kaputtgegangen — noch nicht. Aber achten Sie darauf, was als Nächstes passiert, denn das ist der entscheidende Punkt: Niemand im Gebäude kann drei einfache Fragen sofort beantworten.

> 08:14 — Etwas Seltsames
>
> *Ist das ernst? Wen informieren wir? Wie viel Zeit haben wir?*

Drei angespannte Stunden später: Entwarnung. Die Ursache war ein falsch konfigurierter Überwachungs-Bot, kein Angreifer — keine Daten offengelegt, kein Bürger betroffen. Alle machen sich wieder an die Arbeit.

> 11:05 — Entwarnung
>
> Fehlalarm. Keine Daten offengelegt, kein Bürger betroffen.

Aber die eigentliche Geschichte ist nicht der Fehlalarm. Es ist die Tatsache, dass ein ganz gewöhnlicher Montag eine Lücke offenbart hat: Niemand hatte eine klare Antwort parat — und wäre es echt gewesen, hätten diese drei fehlenden Stunden entscheidend sein können.

Kommt Ihnen das bekannt vor? Wenn Ihre Organisation je einen *„Moment, wer ist dafür eigentlich zuständig?“*-Moment hatte, dann sind Sie genau die Person, für die dieser Kurs gemacht ist.

Warum das wichtig ist, bevor wir über das Gesetz sprechen

Sie müssen sich nicht um ihrer selbst willen für eine EU-Richtlinie mit 46 Artikeln interessieren. Sie brauchen genau drei Dinge — und diese drei Dinge sind dieser ganze Kurs in komprimierter Form.

Drei Dinge — das ist der ganze Kurs, komprimiert:

1. Zu wissen, ob NIS2 **auf Sie zutrifft** — *das ist Einheit 2.*
2. Zu wissen, was es **tatsächlich von Ihnen verlangt** — *das sind die Einheiten 3 bis 5.*
3. Zu wissen, was zu tun ist, **wenn der Montagmorgen-Moment kein Fehlalarm ist** — *das ist Einheit 4.*

Was NIS2 tatsächlich ist (und warum es das gibt)

Zuerst in klaren Worten — der offizielle Name kann einen Absatz warten.

Einfach ausgedrückt: NIS2 ist das Regelwerk der EU, um jene Organisationen, auf die sich alle verlassen — Krankenhäuser, Energienetze, öffentliche Verwaltungen, Verkehrsbetreiber, digitale Infrastruktur — angemessen vor Cybervorfällen zu schützen und sicherzustellen, dass, wenn doch etwas schiefgeht, die richtigen Leute schnell genug davon erfahren, um handeln zu können.

Nun der formelle Name — einmal, damit Sie ihn wiedererkennen, wenn Sie ihm in einem Vermerk oder einer Schlagzeile begegnen.

> Der formelle Name — einmal, zum Wiedererkennen
>
> Offiziell heißt dieses Regelwerk **Richtlinie (EU) 2022/2555**, bekannt als **NIS2** — kurz für die zweite *„Network and Information Security"*-Richtlinie. Sie werden diesen Namen wiedersehen, aber Sie werden selten direkt über ihn nachdenken müssen: Dieser Kurs übersetzt ihn in Entscheidungen, die Sie tatsächlich treffen können.

Warum die EU eingegriffen hat

NIS2 ist nicht aus dem Nichts entstanden. Drei Entwicklungen machten ein gemeinsames europäisches Regelwerk unumgänglich.

- **Digitale Abhängigkeit.** Öffentliche Dienste, Gesundheitswesen, Verkehr und Versorgungsbetriebe laufen heute auf vernetzter Software — für das meiste, was sie tun, gibt es keine „Offline-Rückfallebene".
- **Kaskadierende Ausfälle.** Ein einziges schwaches Glied in den Systemen einer Organisation kann zu einem Problem für Bürgerinnen und Bürger, Patienten, Fahrgäste oder eine ganze Region werden.
- **Ungleiche Vorbereitung.** Die erste NIS-Richtlinie (2016) wurde in den Mitgliedstaaten sehr unterschiedlich angewandt — wie gut ein wesentlicher Dienst geschützt war, hing davon ab, wo er sich zufällig befand.

> In Zahlen
>
> NIS2 — Richtlinie (EU) 2022/2555 — trat am 16. Januar 2023 in Kraft und ersetzte die ursprüngliche NIS-Richtlinie von 2016. Die EU-Mitgliedstaaten hatten bis zum 17. Oktober 2024 Zeit, sie in nationales Recht umzusetzen.

Nicht nur ein weiteres Compliance-Kästchen zum Abhaken

NIS2 ist die Antwort der EU auf dieses Risiko: kein Papierkram um seiner selbst willen, sondern ein **gemeinsamer Mindeststandard**, damit *„wir wussten nicht, dass wir das prüfen müssen"* aufhört, eine akzeptable Ausrede zu sein — überall in der EU, in jedem Sektor, von dem das tägliche Leben der Menschen abhängt.

Was„gemeinsamer Mindeststandard“in Zahlen bedeutet

Nach Art. 34 können Aufsichtsbehörden gegen **wesentliche Einrichtungen** Geldbußen von bis zu 10 Millionen € oder 2 % des weltweiten Jahresumsatzes verhängen — je nachdem, welcher Betrag höher ist. Für **wichtige Einrichtungen** sind es bis zu 7 Millionen € oder 1,4 % des Umsatzes. *(Einheit 5 behandelt genau, wer dafür persönlich in der Verantwortung steht.)*

Sie werden niemals alle 46 Artikel lesen müssen.

Das ist die Aufgabe dieses Kurses — diesen Teil haben wir bereits für Sie erledigt.

„Wahrscheinlich nicht ich“ — die teuerste erste Vermutung

Hier ist die mit Abstand häufigste erste Reaktion auf NIS2 — und warum sie meistens falsch ist.

Die häufigste erste Reaktion auf NIS2 ist eine Variante von: *„Das klingt nach etwas für große Tech-Konzerne oder Bundesbehörden. Wahrscheinlich nicht ich.“* Das ist eine verständliche Vermutung. Sie ist aber, häufiger als nicht, falsch — und hier ist der Grund.

Nehmen wir die vier häufigsten Varianten von „wahrscheinlich nicht ich“. Entscheiden Sie bei jeder zuerst selbst — wahr oder falsch? — und öffnen Sie sie dann, um sie mit der Realität abzugleichen.

❓ *„Wir sind zu klein dafür.“* — wahr oder falsch? ›

❓ *„Wir sind öffentliche Verwaltung, keine Industrie.“* — wahr oder falsch? ›

❓ *„Wir haben unsere IT ausgelagert.“* — wahr oder falsch? ›

❓ *„Wir sind nicht kritisch — wir betreiben nur Busse / die Abrechnung / eine Klinikstation.“* — wahr oder falsch? ›

> In Zahlen
>
> Anhang I und Anhang II führen zusammen **18 Sektoren** auf — 11 Sektoren „hoher Kritikalität“ (Energie, Verkehr, Bankwesen, Gesundheit, digitale Infrastruktur, öffentliche Verwaltung und mehr) und 7 „sonstige kritische“ Sektoren (von Postdiensten über die Lebensmittelproduktion bis zu digitalen Marktplätzen). Genau diese Breite ist der Grund, warum „wahrscheinlich nicht ich“ so oft danebenliegt.

Und „im Anwendungsbereich“ ist nicht nur eine Kennzeichnung für die Organisation. Sie landet auf einzelnen Schreibtischen — durchaus möglicherweise auch auf Ihrem.

Konkret an drei Stellen landet sie:

- **Entscheidungsträger** tragen persönliche Governance-Verantwortung für die Cybersicherheit. *Einheit 5 behandelt genau, was das bedeutet.*
- **IT- und Sicherheitspersonal** setzt die konkreten Maßnahmen um, die die Richtlinie verlangt. *Einheit 3 geht alle zehn durch.*
- **Alle anderen** sind Teil davon, wie Vorfälle bemerkt und gemeldet werden — erinnern Sie sich, wer in Nordholm die seltsamen Anmeldungen entdeckt hat. *Einheit 4 zeigt, wie diese Kette funktioniert.*

Um es klar zu sagen: Ob NIS2 auf Ihre Organisation zutrifft, ist keine Frage des Bauchgefühls. Es ist eine präzise, überprüfbare Frage — und die nächste Einheit gibt Ihnen den Test dazu an die Hand.

> „Wahrscheinlich nicht ich“ist eine Vermutung. Einheit 2 ersetzt sie durch einen Test.
>
> Ob NIS2 auf Ihre Organisation zutrifft, ist eine **präzise, überprüfbare Frage** — zuerst der Sektor, dann die Größe. Einheit 2 führt Sie anhand eines echten Grenzfalls durch diesen zweistufigen Test. Behandeln Sie bis dahin „wahrscheinlich nicht ich“ als ungeprüft.

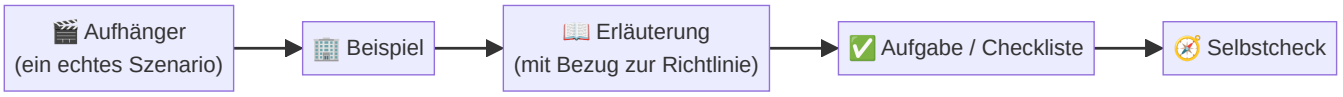
Wie dieser Kurs funktioniert

Dieser Kurs ist so aufgebaut, dass er sich um Ihre eigentliche Arbeit herum fügt — nicht umgekehrt. Vier Dinge sollten Sie wissen, bevor Sie fortfahren.

- **Sechs Einheiten im eigenen Tempo**, insgesamt etwa vier bis sechs Stunden, in Einheiten von jeweils 20–40 Minuten.
- **Sie bestimmen die Reihenfolge.** Jede Einheit ist in sich abgeschlossen — nehmen Sie sie der Reihe nach, oder springen Sie direkt zu der, die Ihre Rolle am dringendsten braucht.
- **Jede Einheit folgt demselben Rhythmus** — tatsächlich stecken Sie gerade mittendrin: Diese Einheit begann mit einem Szenario, nicht mit einer juristischen Definition.
- **Selbstchecks sind für Sie, nicht für eine Note.** Niemand besteht oder fällt durch diesen Kurs. Eine „falsche“ Antwort ist nützliche Information, kein Problem.

Der Rhythmus, dem jede Einheit folgt

Jede Einheit durchläuft dieselben fünf Takte: zuerst ein echtes Szenario, dann ein Beispiel, dann die dahinterstehende Erklärung, dann eine kurze Aufgabe oder Checkliste und schließlich ein schneller Selbstcheck.



Ihr Weg durch den Kurs

Hier ist der vollständige Weg. Beachten Sie die letzte Spalte — jede Einheit endet mit etwas Konkretem in Ihren Händen, und Einheit 6 macht daraus eine einzige Zahl: Ihren persönlichen NIS2-Readiness-Score.

#	Einheit	Typ	~Zeit	Sie gehen d hervor mit
1	Willkommen & Warum NIS2 wichtig ist	Modul	25 Min	Orientierun Bedeutung Rhythmus d
2	Sind Sie im Anwendungsbereich? Wesentliche vs. wichtige Einrichtungen	Übung	40 Min	der Einstufu Organisatio der Begrün dahinter
3	Die 10 Maßnahmen, die Sie wirklich brauchen	Übung	50 Min	dem Maßnahme zugeordnet eigenen Verantwort
4	Sicherheitsvorfälle behandeln & melden	Modul	45 Min	dem Melde- angewandt realistische
5	Wer ist verantwortlich? Governance & Konsequenzen	Modul	40 Min	Klarheit dar persönlich i Verantwort und wofür
6	Ihr NIS2-Readiness-Score	Übung	35 Min	einem bere Readiness-S Ihrer eigene Selbsteinsc

> Das Ziel ist konkret.
>
> Am Ende von Einheit 6 haben Sie Ihren eigenen **NIS2-Readiness-Score** — erstellt aus einer kurzen Selbsteinschätzung, die Sie unterwegs ausfüllen, nicht aus der Theorie.

Lernen Sie Ihre Begleitung kennen

Noch eine Vorstellung, bevor es losgeht: ich.
Ich bin Mika Reinhardt. Ich habe das letzte Jahrzehnt damit verbracht, öffentlichen Verwaltungen und Betreibern kritischer Infrastruktur in ganz Europa dabei zu helfen, genau diese Art von Richtlinie zu verstehen. Ich bin keine Juristin und keine Hackerin — ich sitze zwischen IT, Recht und Leitung, und meine Aufgabe ist es, dichte Regelungen für Menschen verständlich zu machen, die einen Vollzeitjob haben, der nicht „EU-Richtlinien lesen“ heißt.

> ***Ich zeige Ihnen immer, wo das echte Risiko sitzt, nicht nur, wo der Papierkram sitzt.***
>
> — Mika Reinhardt

Zusammenfassung & Selbstcheck

Bevor Sie weitergehen, drei kurze Fragen und zwei Reflexionen. Nichts davon wird benotet — es ist ein privater Selbstcheck, nur für Sie.

> Nicht benotet. Wenn Sie etwas anderes gewählt haben, ist das kein Problem — lesen Sie die klarsprachliche Umschreibung in *Was NIS2 tatsächlich ist* noch einmal und gehen Sie weiter, sobald es einleuchtet.

1. Was ist NIS2, in einem Satz?

- ◯ Eine EU-Richtlinie, die wesentliche und wichtige Organisationen verpflichtet, Cybersicherheitsrisiken zu managen und erhebliche Sicherheitsvorfälle zu melden
- ◯ Eine freiwillige EU-Zertifizierung, die Sie beantragen können, wenn Sie ein Sicherheits-Siegel möchten
- ◯ Ein rein deutsches Cybersicherheitsgesetz, das auf Bundesministerien beschränkt ist

2. Sie beantworten eine Selbstcheck-Frage in diesem Kurs falsch. Was passiert?

- ◯ Die Einheit gilt als nicht bestanden und muss wiederholt werden
- ◯ Das Ergebnis wird an Ihre Fortbildungskoordination gemeldet
- ◯ Nichts — es ist eine private Selbstdiagnose und ein nützlicher Hinweis darauf, was Sie noch einmal lesen sollten

3. Welche dieser Organisationen könnten plausibel unter NIS2 fallen? Wählen Sie alle Zutreffenden aus.

- ☐ Eine mittelgroße Kommunalverwaltung
- ☐ Ein regionaler Krankenhausverbund
- ☐ Der öffentliche Nahverkehrsbetreiber einer Stadt
- ☐ Nur große multinationale Tech-Konzerne

Bevor Sie gehen: Zwei kurze Reflexionen

Nennen Sie ein System oder einen Dienst, auf den sich Ihre Organisation täglich verlässt. Könnte dessen Ausfall innerhalb von 24 Stunden zu „eines jeden Problem“ werden?

Texteingabe ...

Welche Einheit werden Sie für Ihre Rolle voraussichtlich am meisten brauchen? (Keine falsche Antwort — das hilft Ihnen nur, Ihren Weg durch den Kurs zu planen.)

- ☐ Einheit 2 — Sind Sie im Anwendungsbereich?
- ☐ Einheit 3 — Die 10 Maßnahmen, die Sie wirklich brauchen
- ☐ Einheit 4 — Sicherheitsvorfälle behandeln & melden
- ☐ Einheit 5 — Governance & Konsequenzen
- ☐ Einheit 6 — Ihr NIS2-Readiness-Score

Als Nächstes

Einheit 2 — Sind Sie im Anwendungsbereich? Wesentliche vs. wichtige Einrichtungen. Wir lernen Nordholm Nahverkehr kennen, den Verkehrsbetreiber der Stadt, und finden — anhand eines einfachen zweistufigen Tests — genau heraus, wo die Grenze verläuft und auf welcher Seite von ihr Sie stehen.

Quellen:

1. Richtlinie (EU) 2022/2555 (NIS2), Erwägungsgründe 1–10 (Kontext und Begründung) — vollständiger deutscher Text in `data/cybersichert.pdf`
2. Richtlinie (EU) 2022/2555 (NIS2), Art. 34 (Geldbußen), Art. 41 (Umsetzungsfrist), Art. 45 (Inkrafttreten) — `data/cybersichert.pdf`
3. Richtlinie (EU) 2022/2555 (NIS2), Anhänge I–II (Sektorenlisten) — `data/cybersichert.pdf`
4. Kurs-Agenda — `journal.md` → `## Agenda`