NIS2

Orientierung für Unternehmen

Was NIS2 bedeutet und wie Unternehmen jetzt sinnvoll vorgehen

NIS2 ist keine abstrakte Regulierung mehr, sondern ein konkreter Rahmen für Cybersicherheit, Governance und Resilienz. Seit Dezember 2025 ist die entsprechende EU-Richtlinie in deutsches Recht umgesetzt, mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) und weiteren Behörden als Aufsichtsinstanzen. Dieses Point of View ordnet ein, was NIS2 bedeutet, welche Unternehmen betroffen sind und welche Schritte jetzt sinnvoll sind, um die gesetzlichen Regelungen einzuhalten. Vor allem lädt es dazu ein, die Chance zu erkennen, die in den neuen Anforderungen liegt: die Nutzung von NIS2 als integriertes Sicherheits- und Steuerungsmodell, das die Widerstandsfähigkeit des Unternehmens stärkt.

Inhaltsverzeichnis

Einordnung 2

Herausforderungen für Unternehmen 3

Checkliste: Ist Ihr Unternehmen von NIS2 betroffen? 4

Welche Anforderungen stellt NIS2? 5

So können Sie sich auf NIS2 vorbereiten 7

NIS2 umsetzen – und die Resilienz stärken 8

Fazit 9

Einordnung

Kaum ein Thema bewegt die Informationssicherheit derzeit so stark wie NIS2. Viele Unternehmen fragen sich, ob sie betroffen sind, ob die bestehende Cybersicherheitsstrategie ausreicht und welche Pflichten jetzt konkret relevant werden. Gleichzeitig entsteht oft Unsicherheit darüber, wie der Einstieg gelingt und welche Maßnahmen zuerst angegangen werden sollten.

Dieses Point of View vertritt eine klare Position: NIS2 lässt sich nicht durch Einzelmaßnahmen erfüllen. Entscheidend ist, Cybersicherheit als steuerbares und nachvollziehbares Gesamtsystem aufzubauen, das regulatorischen Anforderungen ebenso standhält wie realen Bedrohungsszenarien.

NIS2 ist die Weiterentwicklung der europäischen NIS-Richtlinie und verschärft die Anforderungen an Cybersicherheit, Risikomanagement, Vorfallmeldung und Verantwortung auf Vorstandsebene.

Für viele Unternehmen bedeutet das nicht nur zusätzliche gesetzliche Pflichten, sondern vor allem die Notwendigkeit, Verantwortlichkeiten, Prozesse und Sicherheitsmaßnahmen belastbar zu organisieren.

Es reicht nicht mehr, die Regulierung zu beobachten. Stattdessen gilt es jetzt, Antworten darauf zu finden, was NIS2 konkret für die eigene Organisation bedeutet, welche Pflichten gelten und wie sich eine tragfähige Umsetzungslogik aufbauen lässt.

Herausforderungen für Unternehmen

Mit NIS2 hat sich der regulatorische Rahmen für Cybersicherheit in Deutschland deutlich verändert. Der Kreis der betroffenen Organisationen ist größer als bisher, und die Anforderungen sind konkreter und verbindlicher gefasst. Gefragt sind nicht gute Sicherheitsabsichten, sondern nachvollziehbare und dokumentierte Maßnahmen.

Wer bereits in Informationssicherheit, Business Continuity, Incident Response oder Governance investiert hat, bringt meist eine gute Basis mit. Trotzdem zeigt sich in der Praxis oft, dass Verantwortlichkeiten, Nachweise, Meldewege oder die Einbindung der Lieferkette noch nicht ausreichend strukturiert sind. Hier besteht Handlungsbedarf, um eine NIS2-Konformität zu erreichen.

Hinzu kommt, dass NIS2 mehr Unternehmen betrifft als viele zunächst vermuten. Direkt reguliert sind wichtige und besonders wichtige Einrichtungen. Gleichzeitig steigt auch für Dienstleister, Plattformanbieter und Zulieferer der operative Druck, weil regulierte Unternehmen zunehmend robuste Sicherheits- und Nachweisketten erwarten.

Verschärfte Sicherheitsanforderungen:

NIS2 legt strengere Sicherheitsanforderungen fest, die Unternehmen berücksichtigen müssen. Dazu gehören beispielsweise Maßnahmen zur Risikobewertung, Risikominderung und zur Reaktion auf Sicherheitsvorfälle.

Unternehmen müssen sicherstellen, dass sie über angemessene technische und organisatorische Maßnahmen verfügen, um die Sicherheit der eigenen Netzwerke und Informationssysteme zu gewährleisten.

Dies bietet die Gelegenheit, die eigene Cybersicherheit signifikant zu verbessern, indem in fortschrittliche Technologien und in qualifizierte sowie kompetente Partner investiert wird.

Berichterstattung und Meldepflichten:

Die betroffenen Unternehmen müssen dafür Sorge tragen, dass sie in der Lage sind, Sicherheitsvorfälle innerhalb kurzer Zeiträume zu melden. NIS2 verschärft diese Meldepflichten und verlangt eine schnellere und detailliertere Berichterstattung. Dies setzt voraus, dass Unternehmen robuste Incident-Management-Prozesse und -Systeme implementieren, die eine effiziente Erkennung und Meldung von Vorfällen ermöglichen.

Interne und externe Sensibilisierung:

NIS2 betont die Bedeutung der Zusammenarbeit zwischen verschiedenen Akteuren, einschließlich anderen Unternehmen, Branchenverbänden und nationalen Behörden. Es gilt, Kommunikations- und Kooperationsmechanismen zu etablieren, um Informationen über Bedrohungen und Best Practices auszutauschen. Dies ist besonders herausfordernd für Unternehmen, die bisher wenig Erfahrung in der Zusammenarbeit im Bereich der Cybersicherheit haben. Zudem erfordert NIS2 eine umfassende Sensibilisierung und Schulung aller Mitarbeitenden in Bezug auf Cybersicherheitsrisiken und die spezifischen Anforderungen des Gesetzes.

Für Unternehmen entstehen daraus vor allem vier Herausforderungen: die eigene Betroffenheit einzuordnen, den bestehenden Umsetzungsstand realistisch zu bewerten, kritische Lücken zu priorisieren und daraus einen tragfähigen Umsetzungsweg abzuleiten.

Checkliste: Ist Ihr Unternehmen von NIS2 betroffen?

Um eine erste Einschätzung zu erhalten, ob Ihr Unternehmen von NIS2 betroffen sein könnte, helfen die folgenden Leitfragen. Bereits eine einzige bejahte Antwort ist ein Signal dafür, dass eine vertiefte Prüfung sinnvoll ist.

Sektorzugehörigkeit

- Ist Ihr Unternehmen in einem relevanten Sektor tätig, zum Beispiel in Energie, Transport und Verkehr, Finanzwesen, Gesundheitswesen, Trinkwasser- und Abwasserwirtschaft, digitale Infrastruktur oder Telekommunikation?
- Sind Sie in Bereichen wie Post und Kurierdiensten, Abfallbewirtschaftung, Chemie, Lebensmittel oder im verarbeitenden Gewerbe tätig also in der industriellen Produktion und Weiterverarbeitung von Gütern sowie in digitalen Diensten, im Gesundheitswesen oder in der Forschung aktiv?

Größenkriterien

- Erreichen einzelne Gesellschaften oder Geschäftsbereiche typische Schwellenwerte für Beschäftigte, Umsatz oder Bilanzsumme?
- Bei besonders wichtigen Einrichtungen gelten 250 Mitarbeitende oder ein Jahresumsatz von über 50 Mio. Euro bei einer Jahresbilanzsumme von über 43 Mio. Euro als relevant.
- Bei wichtigen Einrichtungen liegen typische Schwellenwerte bei mindestens 50 Mitarbeitenden oder bei einem Jahresumsatz und einer Jahresbilanzsumme von jeweils über 10 Mio. Euro.

Je nach Sektor und Einrichtungsart können Sonderregelungen gelten. Gerade bei mehreren Gesellschaften, internationalen Set-ups oder Grenzfällen ist eine strukturierte Einordnung ratsam.

Einrichtungsart und Sonderfälle

- Betreiben Sie kritische Anlagen oder erbringen Sie Leistungen in einem besonders regulierten Umfeld?
- Sind Sie Anbieter oder Betreiber von Top-Level-Domain-Registries, DNS-Diensten oder öffentlichen Telekommunikationsnetzen oder -diensten

Geschäftsbeziehungen und Lieferkette

- Arbeiten Sie eng mit Unternehmen zusammen, die selbst reguliert sind?
- Erbringen Sie Leistungen, die für Betrieb, Versorgung oder digitale Prozesse regulierter Unternehmen wesentlich sind?

Die Sicherheit der Lieferkette ist ein ausdrücklicher Bestandteil der Anforderungen. Das bedeutet nicht automatisch, dass jeder Zulieferer selbst direkt reguliert ist, erhöht aber den Nachweis- und Erwartungsdruck in der Praxis.

Könnte Ihr Unternehmen von NIS2 betroffen sein, sollten Sie sich eingehend mit den spezifischen Anforderungen der NIS2-Richtlinie befassen. In den folgenden Abschnitten dieses Point of View erhalten Sie eine detaillierte Übersicht über die Anforderungen und wie Sie diese in Ihrem Unternehmen angehen können.

Welche Anforderungen stellt NIS2?

Für betroffene Unternehmen lassen sich die zentralen Anforderungen in mehrere miteinander verbundene Pflichtenblöcke einordnen. Wichtig ist, diese nicht isoliert zu betrachten, sondern als Teil eines tragfähigen Sicherheits- und Steuerungsmodells.

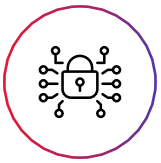
Registrierung und Datenpflege

Betroffene Einrichtungen müssen sich beim digitalen Dienst „Mein Unternehmenskonto“ (MUK) sowie im zweiten Schritt beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren und ihre Daten aktuell halten. Gesonderte Registrierungspflichten gibt es für Betreiber kritischer Anlagen und für Einrichtungen der Sektoren digitale Dienste und digitale Infrastrukturen. Änderungen sind zeitnah vorzunehmen. Die Registrierung ist damit kein Einmalvorgang, sondern Teil einer laufenden Verpflichtung.

Maßnahmen zum Risikomanagement

Die betroffenen Unternehmen müssen geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen etablieren und dokumentieren. Dazu gehören insbesondere:

- Konzepte zur Risikoanalyse und Sicherheit für Informationssysteme
- Business Continuity Management, Backup-Management, Krisenmanagement und Wiederherstellungsfähigkeit
- Prävention, Erkennung und Bewältigung von Sicherheitsvorfällen
- Bewertung der Wirksamkeit vorhandener Cybersicherheitsmaßnahmen, zum Beispiel durch Tests und Übungen
- Technologien für Kryptographie und Verschlüsselung
- Identitäts- und Zugriffsmanagement sowie Personalsicherheit
- Lösungen zur Multi-Faktor-Authentifizierung oder zu vergleichbaren Authentifizierungsverfahren
- Sicherheit in der Lieferkette und im Umgang mit Dienstleistern
- Sichere Kommunikation sowie Sicherheitsanforderungen für Beschaffung, Entwicklung und Wartung von IT-Systemen



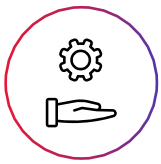
Cyberhygiene und Sensibilisierung

Neben formalen Pflichten bleibt die operative Sicherheitsbasis entscheidend. Dazu gehören beispielsweise:

- die Implementierung von Zero-Trust-Prinzipien
- das Asset-Management
- sichere Gerätekonfigurationen
- die Durchführung kontrollierter Software-Updates (Patch- und Updatemanagement)
- die Sensibilisierung und Schulung von Mitarbeitenden und Leitungspersonen durch Workshops und Trainings

Meldepflichten bei Sicherheitsvorfällen

Erhebliche Sicherheitsvorfälle müssen fristgerecht gemeldet werden. Der Prozess ist gestuft: Zunächst ist innerhalb von 24 Stunden eine frühe Meldung erforderlich. Danach folgen eine weitergehende Meldung innerhalb von 72 Stunden sowie eine Abschluss- oder Fortschrittsmeldung innerhalb eines Monats. Unternehmen sollten diese Abläufe nicht erst im Ernstfall definieren.



Verantwortung der Geschäftsleitung

Die Geschäftsleitung trägt Verantwortung für die Umsetzung und Überwachung der Maßnahmen. Dazu gehören die aktive Unterstützung bei der Umsetzung, die Genehmigung wesentlicher Maßnahmen, die Verankerung von Zuständigkeiten sowie die Teilnahme an geeigneten Schulungen. NIS2 ist damit auch ein Governance-Thema.

Diese Maßnahmen sind wesentlich, um die Anforderungen der NIS2-Richtlinie zu erfüllen und die Cybersicherheit im Unternehmen zu stärken. Die Unterstützung durch eine engagierte Geschäftsführung ist unumgänglich.

Aufsicht, Nachweise und Folgen bei Verstößen

Unternehmen müssen ihre Maßnahmen und Prozesse nachvollziehbar dokumentieren und mit einer risikoorientierten Aufsicht rechnen. Bei Verstößen drohen aufsichtsrechtliche Maßnahmen, Bußgelder und erheblicher Reputationsdruck. Schon deshalb ist eine durchdachte Umsetzungsstrategie sinnvoller als punktuelle Einzelmaßnahmen.

So können Sie sich auf NIS2 vorbereiten

Ein strukturierter und schrittweiser Ansatz hat sich in der Praxis als entscheidend erwiesen.

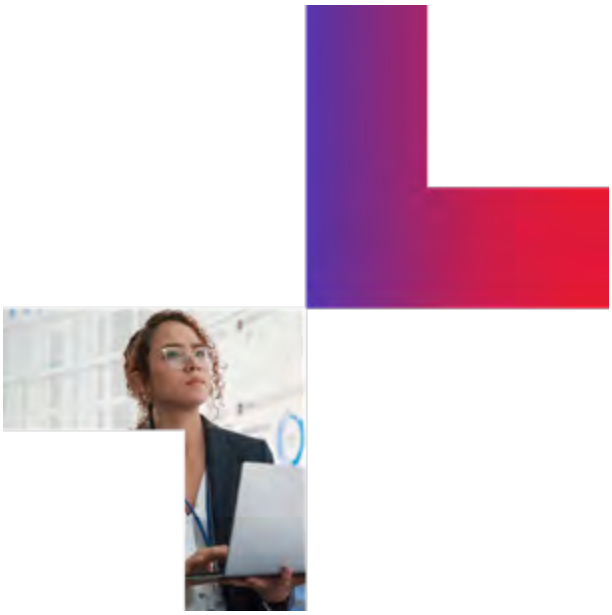
1. Betroffenheit prüfen: Klären Sie, welche Gesellschaften, Standorte, Services und Abhängigkeiten in den relevanten Scope fallen.
2. Security Audit durchführen: Analysieren Sie, welche Sicherheitsmaßnahmen bereits vorhanden sind und wo Lücken bestehen.
3. Geschäftsleitung sensibilisieren: NIS2 schafft klare Verantwortlichkeiten für die Leitungsebene. Diese Rolle sollte frühzeitig verstanden und verankert werden.
4. Verantwortlichkeiten identifizieren: Klären Sie, welche Mitarbeitenden und Funktionen für IT-Sicherheit, Risiko-Management, Meldeprozesse und Lieferkette verantwortlich sind.
5. Sicherheitslücken und Risiken priorisieren: Bewerten Sie, welche Abweichungen zwischen bestehender Sicherheitsarchitektur und den Anforderungen besonders kritisch sind.
6. Meldekonzept etablieren: Definieren Sie Verantwortlichkeiten, Eskalationspfade, Vorlagen und Kriterien, damit erhebliche Vorfälle fristgerecht bewertet und gemeldet werden können.
7. Lieferkette einbeziehen: Bewerten Sie kritische Dienstleister, Plattformen und Software-Lieferanten systematisch und sprechen Sie erkannte Risiken aktiv an.
8. Umsetzungsstrategie entwickeln: Leiten Sie aus der Einordnung eine realistische Roadmap ab, inklusive Budget, Prioritäten und zeitlicher Staffelung.
9. Workshops und Trainings durchführen: Sensibilisieren Sie Management, Fachbereiche und Mitarbeitende für ihre Rolle in der Umsetzung.

Grundsätzlich gilt: Cybersicherheit sollte ganzheitlich gedacht werden – als Ende-zu-Ende-Sicherheit, die alle Faktoren berücksichtigt. Sie ist kein isolierter Aspekt, sondern ein Thema, das Governance, Prozesse, Technik und Zusammenarbeit gleichermaßen betrifft.

Mitarbeitende sollten regelmäßig geschult und sensibilisiert werden, um ein Bewusstsein für Sicherheitsrisiken zu entwickeln und verantwortungsvoll mit sensiblen Daten umzugehen. Dies kann durch eine Kombination aus regelmäßigen Schulungen, Workshops und klaren Sicherheitsrichtlinien erreicht werden. Ein gut informiertes und wachsames Team ist ein wesentlicher Faktor, um Sicherheitsvorfälle zu verhindern und schnell auf Bedrohungen reagieren zu können.

NIS2 umsetzen – und die Resilienz stärken

NIS2 muss als integriertes Sicherheits- und Steuerungsmodell verstanden werden, nicht als Sammlung einzelner Anforderungen. Das ist der Grundgedanke, mit dem CGI seine Kunden bei der Umsetzung von NIS2 berät.



Wir unterstützen dabei, NIS2 als operative Aufgabe greifbar zu machen. Im Mittelpunkt steht nicht die abstrakte Erläuterung der Regulierung, sondern die Frage, wie Betroffenheit, Reifegrad und Handlungsbedarf belastbar eingeordnet werden können. Ein sinnvoller Einstieg ist eine detaillierte Standortbestimmung. Darauf aufbauend, lassen sich vorhandene Maßnahmen bewerten, Lücken priorisieren und eine realistische Roadmap festlegen. Die Schritte im Einzelnen:

Einordnung der Betroffenheit und des organisatorischen Scopes

- Assessment des aktuellen Reifegrads von Governance, Prozessen und Sicherheitsmaßnahmen unter Verwendung eines eigens hierfür entwickelten Tools
- Identifikation und Priorisierung von Lücken
- Ausgestaltung von Melde- und Eskalationsprozessen
- Bewertung von Lieferketten- und Dienstleisterrisiken
- Ableitung einer Roadmap für die NIS2-Umsetzung
- Schulungen und Sensibilisierung für Management, Fachbereiche und Mitarbeitende

Ein strukturiertes Vorgehen schafft nicht nur regulatorische Orientierung, sondern ermöglicht ein Sicherheitsmodell, das steuerbar, nachvollziehbar und im Ernstfall wirksam ist.

Fazit

NIS2 ist für viele Unternehmen operative Realität. Entscheidend ist jetzt nicht, möglichst viele Einzelmaßnahmen parallel zu starten, sondern die eigene Betroffenheit belastbar einzuordnen, den Umsetzungsstand realistisch zu bewerten und Prioritäten sinnvoll festzulegen.

Wer NIS2 als integriertes Sicherheits- und Steuerungsmodell nutzt, adressiert nicht nur regulatorische Anforderungen, sondern stärkt auch die Widerstandsfähigkeit der eigenen Organisation. Genau darin liegt der eigentliche Mehrwert.

About CGI

Insights you can act on

Als globaler Dienstleister für IT- und Geschäftsprozesse sind wir auf Nachhaltigkeit ausgerichtet und bieten unseren Kunden mit weltweit über 94.000 Mitarbeitenden strategische IT- und Business-Beratung, Systemintegration, Managed IT, Business Process Services und Intellectual Property auf Topniveau. Unsere Teams orientieren sich konsequent an den Geschäftsstrategien unserer Kunden, entwickeln innovative Lösungen wie KI entlang der gesamten Wertschöpfungskette und werden im Hinblick auf Zeit- und Budgettreue regelmäßig mit Bestnoten bewertet.

cgi.com/de/cybersecurity/nis2