



# NIS2-Richtlinie: neue Vorschriften für die Cybersicherheit von Netz- und Informationssystemen

Cybersicherheit umfasst den Schutz von **Netzwerk- und Informationssystemen** (NIS), ihren Nutzern und anderen betroffenen Personen vor Cyberfällen und Bedrohungen. Um auf die zunehmende Gefährdung Europas durch Cyberbedrohungen zu reagieren, ersetzte die [Richtlinie 2022/2555, auch bekannt als NIS2](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555) (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555>) ihre Vorgängerrichtlinie, die Richtlinie 2016/1148 oder NIS1. NIS2 erhöht das gemeinsame Ambitionsniveau der EU im Bereich der Cybersicherheit durch einen breiteren Anwendungsbereich, klarere Vorschriften und stärkere Aufsichtsinstrumente. Sie verpflichtet die Mitgliedstaaten, **ihre Cybersicherheitskapazitäten zu verbessern** und gleichzeitig Risikomanagementmaßnahmen und Berichtspflichten für Einrichtungen aus mehr Sektoren einzuführen und Vorschriften für die Zusammenarbeit, den Informationsaustausch, die Beaufsichtigung und die Durchsetzung von Cybersicherheitsmaßnahmen festzulegen.

Die Richtlinie schreibt vor, dass jeder Mitgliedstaat eine nationale Cybersicherheitsstrategie annimmt, die Strategien für die Sicherheit der Lieferkette, das Schwachstellenmanagement und die Aufklärung und Sensibilisierung im Bereich Cybersicherheit umfasst. Die Mitgliedstaaten müssen auch eine Liste der Betreiber wesentlicher Dienste erstellen und regelmäßig aktualisieren, um sicherzustellen, dass diese Einrichtungen die Anforderungen der Richtlinie erfüllen.

Zusätzlich zu den Sektoren, die bereits unter NIS 1 fallen, wie Energie, Verkehr, Gesundheitswesen, Finanzen, Wasserwirtschaft und digitale Infrastruktur, gelten diese Vorschriften für Anbieter öffentlicher elektronischer Kommunikationsdienste, mehr digitale Dienste wie soziale Plattformen, Abwasser- und Abfallbewirtschaftung, Herstellung kritischer Produkte, Post- und Kurierdienste, öffentliche Verwaltung sowohl auf zentraler als auch auf regionaler Ebene oder im Weltraum. In der Regel müssen mittlere und große Einrichtungen in diesen kritischen Sektoren geeignete Maßnahmen zum Cybersicherheitsrisikomanagement ergreifen und die zuständigen nationalen Behörden über erhebliche Sicherheitsvorfälle informieren. Dabei handelt es sich um Vorfälle, die erhebliche Störungen oder Schäden verursachen können.

Die Richtlinie enthält auch Bestimmungen für Aufsicht, Durchsetzung und freiwillige Peer Reviews, um das gegenseitige Vertrauen und die Cybersicherheitskapazitäten in der gesamten EU zu stärken. Es führt auch die Rechenschaftspflicht des Top-Managements für die Nichteinhaltung von Maßnahmen zum Cybersicherheitsrisikomanagement ein und macht den Vorstand auf die Cybersicherheit aufmerksam.

Mit der Richtlinie wird ein Netzwerk von [Computer Security Incident Response Teams \(CSIRTs\)](https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/csirts-network) (<https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/csirts-network>) eingerichtet, um Informationen über Cyberbedrohungen auszutauschen und auf Vorfälle zu reagieren. Diese Teams sind entscheidend für die Aufrechterhaltung des Situationsbewusstseins und die Bereitstellung von Unterstützung. Um Cybersecurityvorfälle oder -krisen großen Ausmaßes zu bewältigen, wird mit der Richtlinie das [europäische Netz der Verbindungsorganisationen für Cyberkrisen \(EU-CyCLONE\)](https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone) (<https://www.enisa.europa.eu/topics/eu-cyber-crisis-and-incident-management/eu-cyclone>) geschaffen. Dieses Netz unterstützt ein koordiniertes Management und gewährleistet einen regelmäßigen Informationsaustausch zwischen den Mitgliedstaaten und den EU-Organen im Falle von Vorfällen und Krisen großen Ausmaßes.

Parallel dazu ist die [NIS-Kooperationsgruppe](https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group) (<https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group>) eine Plattform, die mit der NIS-Richtlinie eingerichtet wurde, um die strategische Zusammenarbeit und den Informationsaustausch zwischen den EU-Mitgliedstaaten, der Europäischen Kommission und der Agentur der Europäischen Union für Cybersicherheit (ENISA) zu erleichtern. Die Gruppe veröffentlicht unverbindliche Leitlinien und Empfehlungen zur Unterstützung der Umsetzung der NIS-Richtlinie.

## Hintergrund

Die [NIS 1 \(Richtlinie 2016/1148\)](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148) (<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32016L1148>) war die erste umfassende EU-Rechtsvorschrift, die darauf abzielte, die Cybersicherheit von Netz- und Informationssystemen zu erhöhen, um lebenswichtige Dienste für die Wirtschaft und Gesellschaft der EU zu schützen. Im Dezember 2020 schlug die Kommission vor, NIS 1 zu überarbeiten, was zur Annahme von NIS 2 führte, das im Januar 2023 in Kraft trat. Die Mitgliedstaaten hatten bis zum 17. Oktober 2024 Zeit, die NIS2-Richtlinie in nationales Recht umzusetzen. NIS 2 hob NIS1 mit Wirkung vom 18. Oktober 2024 auf.

Die Kommission hat [Vertragsverletzungsverfahren](#)

[https://commission.europa.eu/law/application-eu-law/implementing-eu-law/infringement-procedure\\_en](https://commission.europa.eu/law/application-eu-law/implementing-eu-law/infringement-procedure_en)) eingeleitet und [Aufforderungsschreiben an 23 Mitgliedstaaten gerichtet, weil diese die NIS2-Richtlinie nicht bis zum 17. Oktober 2024 vollständig in nationales Recht umgesetzt](#) (<https://digital-strategy.ec.europa.eu/en/news/commission-calls-23-member-states-fully-transpose-nis2-directive>) haben. Die Mitgliedstaaten müssen reagieren und ihre Umsetzung der Richtlinie abschließen. Andernfalls kann die Kommission eine mit Gründen versehene Stellungnahme abgeben, bei der es sich um einen förmlichen Antrag auf Einhaltung des EU-Rechts handelt. Ein fortgesetzter Verstoß könnte schließlich dazu führen, dass der Fall an den Gerichtshof der Europäischen Union verwiesen wird, der finanzielle Sanktionen verhängen kann.

Dies ist eine maschinelle Übersetzung durch den eTranslation-Dienst der Europäischen Kommission, der Ihnen hilft, diese Seite zu verstehen. [Bitte lesen Sie die Nutzungsbedingungen](#) ([https://ec.europa.eu/info/use-machine-translation-europa-exclusion-liability\\_en](https://ec.europa.eu/info/use-machine-translation-europa-exclusion-liability_en)). Um die Originalfassung zu lesen, [gehen Sie zur Quellenseite](#) (<https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>).

---

**Source URL:** <https://digital-strategy.ec.europa.eu/policies/nis2-directive>

© European Union, 2025 - [Gestaltung der digitalen Zukunft Europas \(https://digital-strategy.ec.europa.eu/de\)](#) - PDF generated on 01/04/2025

Reuse of this document is allowed, provided appropriate credit is given and any changes are indicated (Creative Commons Attribution 4.0 International license).

For any use or reproduction of elements that are not owned by the EU, permission may need to be sought directly from the respective right holders.