

So kann Ihnen OpenText bei der NIS2-Umsetzung helfen



Was ist NIS2?

NIS2 („Network and Information Security Directive“) ist eine [EU-Richtlinie](#), die Mindeststandards an Cybersicherheit für wichtige Branchen vorschreibt. Sie trat Anfang 2023 in Kraft und muss bis zum 17. Oktober 2024 in nationales Recht überführt werden. Im Vergleich zur ersten NIS-Richtlinie werden deutlich mehr Unternehmen in die Pflicht genommen.

Wer ist von NIS2 betroffen?

Die EU-Richtlinie gilt für zwei Gruppen von Unternehmen. Diese müssen dieselben Vorgaben einhalten, werden jedoch unterschiedlich stark überwacht und sanktioniert:

- ▶ **Besonders wichtige Einrichtungen:** Unternehmen mit mindestens 250 Mitarbeitern oder 50 Mio. € Jahresumsatz, u. a. aus den Sektoren Energie, Transport & Verkehr, Finanzen & Versicherungen, Gesundheit, Wasser & Abwasser, IT & Telekommunikation sowie Weltraum. Ferner Anbieter öffentlicher Telekommunikationsnetze und -dienste mit mindestens 50 Mitarbeitern oder 10 Mio. € Jahresumsatz.
- ▶ **Wichtige Einrichtungen:** Unternehmen mit mindestens 50 Mitarbeitern oder 10 Mio. € Jahresumsatz. Zusätzlich zu den obengenannten Sektoren betrifft dies u. a. auch Post & Kurier, Chemie, Forschung, digitale Dienste, Lebensmittel, Entsorgung sowie bestimmte Bereiche des verarbeitenden Gewerbes.



Wichtig: Die Zuordnung zu NIS2 ist komplex und unterliegt je nach Fall zusätzlichen Anforderungen, Sonderregelungen und Ausnahmen. Selbst wenn die genannten Kriterien nicht erfüllt sind, kann ein Unternehmen von NIS2 betroffen sein – etwa, wenn sogenannte „qualifizierende Faktoren“ vorliegen. Aus diesem Grund ist eine rechtliche Einzelfallbewertung zwingend nötig.



TIPP: Eine erste Einschätzung, ob Ihre Kunden unter NIS2 fallen, können Sie schnell und einfach mit dem [kostenlosen Quick-Check](#) von Prof. Dr. Dennis-Kenji Kipker vornehmen.

Was schreibt NIS2 vor?

Betroffene Unternehmen sind dazu verpflichtet, „geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen“ zu ergreifen. Diese sollen Risiken für die Sicherheit von Informationssystemen minimieren und Auswirkungen von Cyberangriffen eindämmen. Dabei sind u. a. der Stand der Technik sowie die Bedrohungslage zu berücksichtigen.

Konkret schreibt NIS2 **Maßnahmen in folgenden Bereichen** vor:

- ▶ Risikoanalyse und Konzepte für die Sicherheit von Informationssystemen
- ▶ Bewältigung von Sicherheitsvorfällen
- ▶ Backup-, Wiederherstellungs- und Krisenmanagement
- ▶ Absicherung der Lieferkette
- ▶ Sicherheit bei Einkauf, Entwicklung und Wartung von IT-Systemen
- ▶ Schwachstellen-Management
- ▶ Bewertung der Effektivität des Risikomanagements
- ▶ Cyberhygiene und Mitarbeiterschulungen
- ▶ Verschlüsselung
- ▶ Sicherheit des Personals
- ▶ Zugriffskontrolle und Asset-Management
- ▶ Multi-Faktor-Authentifizierung
- ▶ Gesicherte Sprach-, Video-, Text- und Notfallkommunikation

Die Umsetzung soll im Einklang mit internationalen Standards erfolgen. Zudem sind betroffene Unternehmen verpflichtet, erhebliche Sicherheitsvorfälle in mehreren Schritten an das BSI zu melden und gegebenenfalls auch Kunden sowie die Öffentlichkeit zu informieren.



Was droht bei Verstößen gegen NIS2?

Bei Verstößen können u. a. folgende Bußgelder verhängt werden (es gilt jeweils der höhere Betrag):

- ▶ **Besonders wichtige Einrichtungen:** Maximal 10 Mio. € oder 2 % des weltweiten Umsatzes aus dem letzten Geschäftsjahr
- ▶ **Wichtige Einrichtungen:** Maximal 7 Mio. € oder 1,4 % des weltweiten Umsatzes aus dem letzten Geschäftsjahr

In bestimmten Fällen kann das BSI zudem Führungskräften zeitweise die Ausübung Ihrer Tätigkeit untersagen.

Wie kann OpenText bei der NIS2-Umsetzung helfen?

Sofern Ihre Kunden von NIS2 betroffen sind, empfiehlt sich grundsätzlich u. a. Folgendes:

- ▶ Führen Sie eine **Risikoanalyse** durch und dokumentieren Sie diese.
- ▶ Nehmen Sie **fachliche Hilfe** von auf IT-Sicherheitsrecht spezialisierten Anwaltskanzleien in Anspruch
- ▶ Wenden Sie sich bei komplexeren Fragen an das [Bundesamt für Sicherheit in der Informationstechnik \(BSI\)](#) oder zuständige Ministerien der Länder.

[OpenText Cybersecurity](#), unser Experte für Cyber-Resilienz, bietet Ihnen ein breites Portfolio an Security-, Backup- und Disaster Recovery-Lösungen. Dieses kann Ihnen dabei helfen, wichtige Aspekte von NIS2 abzudecken – insbesondere aus den Bereichen Backup-, Wiederherstellungs- und Krisenmanagement sowie Mitarbeiterschulungen.

- ▶ **Backup:** Sichern Sie Daten auf verschiedensten Plattformen und stellen Sie diese bei Bedarf schnell wieder her – seien es Laptops und Workstations ([Carbonite Endpoint](#)), physische, hybride sowie virtuelle Server ([Carbonite Server Backup](#)) oder SaaS-Anwendungen wie Microsoft 365, Google Workspace, Salesforce, Dropbox und Box ([Carbonite Cloud-to-Cloud Backup](#)).
- ▶ **Hochverfügbarkeit:** Mit [Carbonite Availability](#) sorgen Sie dafür, dass kritische Systeme jederzeit verfügbar sind. Im Ernstfall lässt sich der Geschäftsbetrieb nahezu ohne Unterbrechungen oder Datenverluste fortführen. Noch einen Schritt weiter geht [Carbonite Recover](#), mit dem MSPs Ihren Kunden Disaster Recovery as a Service dank Echtzeit-Replikation in die Cloud anbieten können.
- ▶ **Security Awareness-Trainings:** Schulen Sie die Mitarbeiter Ihrer Kunden mit [Webroot Security Awareness Training](#) durch realitätsnahe Phishing-Simulationen, E-Trainings und Compliance-Kurse für den täglichen Umgang mit Cyberbedrohungen.

Wichtiger Hinweis:

Dieser Leitfaden ist ein Informationsdokument und stellt keine Rechtsberatung dar. In konkreten Einzelfällen wenden Sie sich bitte an einen spezialisierten Fachanwalt. Trotz sorgfältiger Prüfung übernehmen wir keine Gewähr und Haftung für die Richtigkeit aller Angaben.

Lernen Sie den Cyber-Resilienz-Spezialisten näher kennen!



Sprechen Sie uns an:
[+49 6441 67118-841](tel:+49644167118841)



Ihr individuelles **Angebot**:
carbonite@ebertlang.com



Kostenfreie **Webinare**:
ebertlang.com/akademie




Testversionen:
ebertlang.com/technologie/testversion

Über OpenText Cybersecurity

In einer Zeit ständiger Cyberbedrohungen hilft OpenText Cybersecurity Unternehmen jeder Größe, widerstandsfähiger gegen Cyberattacken zu werden, IT-Systeme jederzeit betriebsbereit zu halten und damit Cyber-resilient zu werden. Mehrschichtige Data Security- und Data Management-Lösungen helfen bei der Prävention, Erkennung und Reaktion auf Cybervorfälle sowie bei der Wiederherstellung, Überprüfung und Compliance.

 ebertlang.com/carbonite

 +49 6441 67118-841

 carbonite@ebertlang.com

 **EBERTLANG**