

kaspersky

So kann Ihnen
Kaspersky 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.

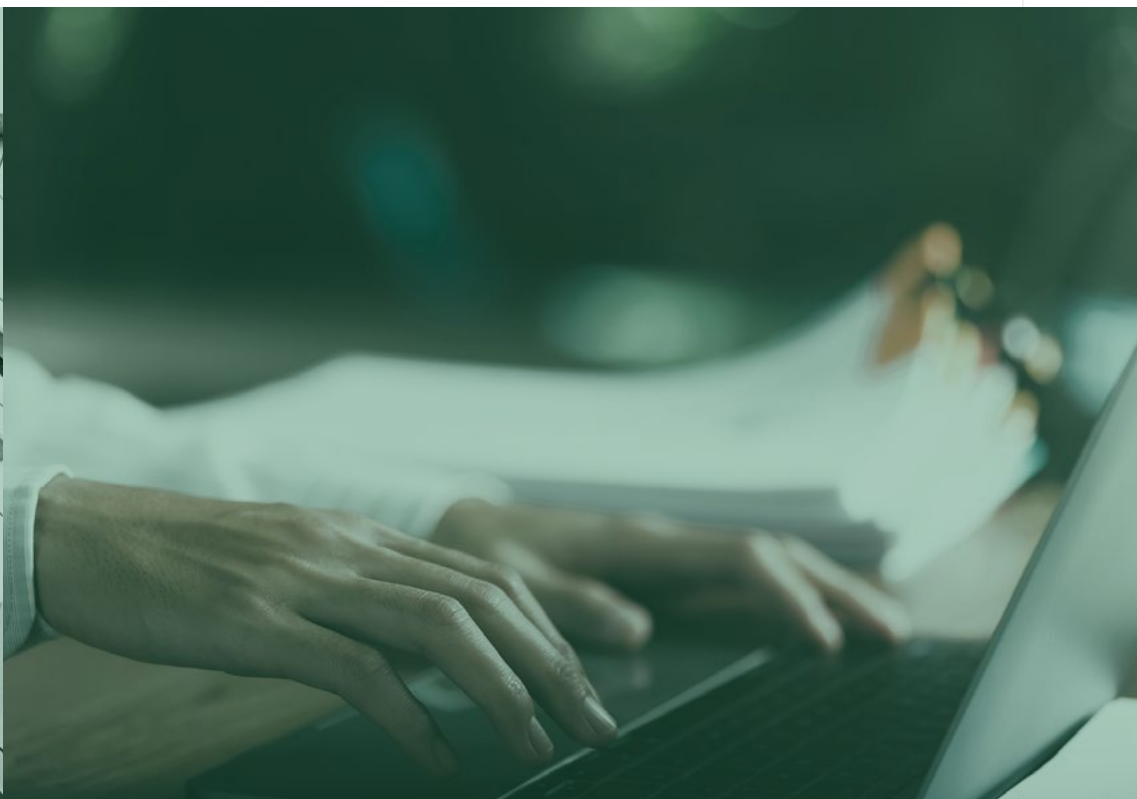
Was schreibt NIS2 vor?

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 Kaspersky 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.

Unser Security-Experte [Kaspersky](#) bietet Ihnen ein umfassendes Portfolio an vielfach ausgezeichneten Sicherheitslösungen, auf das weltweit 220.000 Unternehmen vertrauen und das Ihnen dabei helfen kann, NIS2 bei Ihren Kunden umzusetzen:

- ▶ **[Kaspersky Endpoint Security](#):** Endpoint-Schutz, der sich flexibel an die Bedürfnisse Ihrer Kunden anpassen lässt. Die Varianten Endpoint Security for Business Advanced sowie Endpoint Security Cloud Plus enthalten u. a. das Vulnerability & Patch Management-Modul, welches ein zentrales Patching von Software-Schwachstellen ermöglicht.
- ▶ **[Kaspersky Endpoint Detection and Response \(EDR\)](#):** scannt das Netzwerk und leitet bei Bedarf automatisierte Gegenmaßnahmen ein. Dank Verhaltensanalysen lassen sich sogar unbekannte Bedrohungen identifizieren. Wird ein System kompromittiert, stellt die Lösung im Anschluss wertvolle Daten zur Ursachenforschung bereit. Damit leistet sie nicht nur einen wichtigen Beitrag zur Bewältigung von Sicherheitsvorfällen, sie eignet sich auch für den Einsatz in Betrieben mit kritischen Infrastrukturen.
- ▶ **[Kaspersky Managed Detection and Response \(MDR\)](#):** geeignet für alle IT-Dienstleister, die von den Vorteilen der EDR-Lösung profitieren möchten, aber

nicht die nötigen Ressourcen hierfür besitzen. Das Threat Hunting-Team des Herstellers behält die Endpoints Ihrer Kunden jederzeit im Blick.

- ▶ **Kaspersky Automated Security Awareness Platform:** realitätsnahe E-Trainings und Phishing-Simulationen für verschiedenste Anwendergruppen, mit denen Sie das Sicherheitsniveau bei Ihren Kunden nachhaltig steigern. In der NIS2-Richtlinie werden Schulungen zur Schärfung des Bewusstseins von Cyberbedrohungen explizit genannt.

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 Security-Spezialisten näher kennen!



Sprechen Sie uns an:
[+49 6441 67118-842](tel:+49644167118842)



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



Kostenfreies **Webinar**:
ebertlang.com/akademie




Testversionen:
ebertlang.com/technologie/testversion

Über Kaspersky

Kaspersky ist eines der führenden Security-Unternehmen weltweit mit einer umfassenden Palette an Sicherheitslösungen zur Abwehr komplexer sowie neuer Cyberbedrohungen. Die tiefgreifende Threat Intelligence ist Basis für alle Produkte und schützt Unternehmen, kritische Infrastrukturen, staatliche Einrichtungen sowie Privatanwender. Rund 220.000 Unternehmenskunden weltweit vertrauen auf die Sicherheit durch die vielfach ausgezeichneten Kaspersky-Technologien.

 www.ebertlang.com/kaspersky

 +49 6441 67118-842

 kaspersky@ebertlang.com

 **EBERTLANG**