

# NIS-2 ANTE PORTAS

(Stichdatum 17.10.2024)

## Lösungen der MCSS AG zur NIS-2-Richtlinie

### Was bedeutet NIS-2?

NIS steht für „Network and Information Security“. Es ist eine verpflichtende EU-Richtlinie (2022/2555) und definiert für die betroffenen Einrichtungen, Organisationen und Unternehmen strenge verpflichtende Regelungen für Cyberschutz und Informationssicherheit.

### Für wen ist NIS-2 verpflichtend?

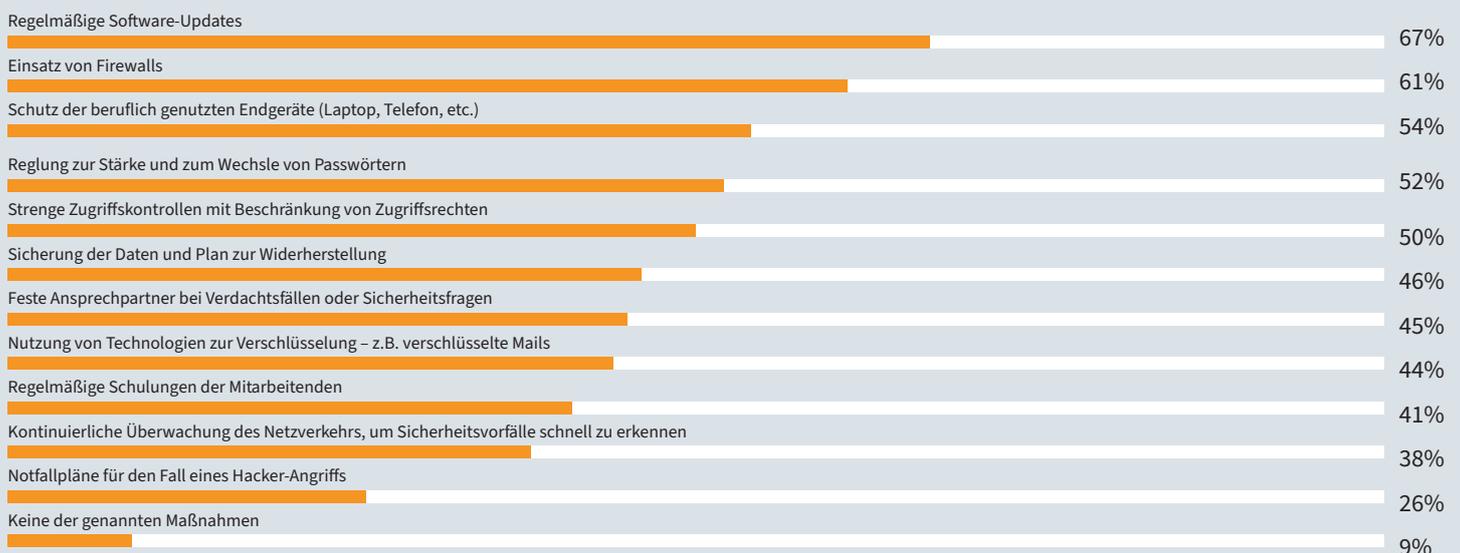
Die NIS-2-Richtlinie zielt darauf ab, in wesentlichen und wichtigen Einrichtungen die Cybersicherheit zu stärken und IT-Vorfälle zu vermeiden. Sie betrifft Unternehmen und Organisationen in 18 verschiedenen Sektoren mit mehr als 50 Mitarbeitenden und/oder einem Jahresumsatz von über 10 Millionen Euro. Auch kleinere Unternehmen können als Teil der Lieferkette von NIS-2-Unternehmen betroffen sein.

### Bis wann müssen die Vorbereitungen abgeschlossen sein?

Das Stichdatum ohne Übergangszeit ist der 17. Oktober 2024.  
Die Übergangsfrist beträgt 3 Monate, wenn vor dem 17.10. die Betroffenheit angezeigt wird.

### Eine aktuelle Umfrage von Lufthansa IND zum Thema IT-Security in Unternehmen bescheinigt Beschäftigten wie Führungskräften großen Nachholbedarf hinsichtlich der eigenen Gefährdung durch Cyberkriminelle:

#### Welche Maßnahmen zur IT-Sicherheit in Ihrem Unternehmen sind Ihnen bekannt? (Mehrfachantworten sind möglich)



## Welche Risiken bestehen bei Nichteinhaltung von NIS-2?

Je nach Größe und der Wichtigkeit der Einstufung müssen Organisationen, Einrichtungen und Unternehmen bis zu zehn Millionen oder 2 % eines Jahresumsatzes als mögliche Geldstrafe zahlen. Von den Aufsichtsbehörden können Vor-Ort-Kontrollen durchgeführt oder Nachweise angefordert werden.

**Die Unternehmensleitung ist verantwortlich und kann persönlich haftbar gemacht werden. Letztere sind verantwortlich, die Organisation bis zum 17. Oktober 2024 beim BSI zu registrieren.**

|                                   | WESENTLICHE EINRICHTUNGEN  | WICHTIGE EINRICHTUNGEN  |
|-----------------------------------|--|---|
| <b>AUFSICHT DURCH BEHÖRDEN</b>    | Proaktive Aufsicht (z.B. regelmäßige Sicherheitsprüfungen)   | Reaktive Aufsicht nach Hinweisen auf Verstöße (z.B. gezielte Sicherheitsprüfungen)  |
| <b>GELDSTRAFEN BEI VERSTÖSSEN</b> | Höchstbetrag von mind. 10 Mio. EUR oder 2% des weltweiten Umsatzes   | Höchstbetrag von mind. 7 Mio. EUR oder 1,4% des weltweiten Umsatzes   |
| <b>WER ZÄHLT DAZU?</b>            | Große Unternehmen<br><br>> 249 Beschäftigte, oder<br>> 50 Mio. EUR Umsatz und<br>> 43 Mio. EUR Bilanz<br><br>Größenunabhängige Sonderfälle:<br>z.B. DNS-Diensteanbieter, Zentralregierung, KRITIS, und Einrichtungen, die vom Staat als „wesentlich“ eingestuft werden | Mittlere Unternehmen<br><br>mind. 50 Beschäftigte, oder<br>> 10 Mio. EUR Umsatz und<br>> 10 Mio. EUR Bilanz<br><br>Größenunabhängige Sonderfälle:<br>Einrichtungen, die vom Staat als „wichtig“ eingestuft werden |

## Was ist zu beachten?



**Betroffene müssen umfangreiche Maßnahmen im Bereich Cyber- und Informationssicherheit umsetzungsbereit gewährleisten können.**

Dazu zählen bspw. Risikoanalysekonzepte, Gewährleistung der Aufrechterhaltung des Betriebs im Ernstfall und weitere Maßnahmen.



**Es besteht eine Schulungsverpflichtung für die Geschäftsführung.**



**Bedeutende Sicherheitsvorfälle müssen künftig innerhalb von 24 Stunden an die zuständige Behörde gemeldet werden.**



**UMKEHR DER MELDEPFLICHT:**

**Betroffene sind künftig verpflichtet, bis zu einem Stichtag beim BSI nachzuweisen, dass sie die Auflagen erfüllen.**

**Damit liegt eine Bringschuld bei den Unternehmen und Institutionen.**

## Welche Lösungen bietet das MCSS-Expertensystem zu NIS-2?

Die **MCSS-NIS-2-Lösungen** basieren auf dem vom Bundeswirtschaftsminister ausgezeichneten cloudbasierten Expertensystem für kleine und mittlere Unternehmen ab 50 angestellten und freien Mitarbeitenden.

## Das cloudbasierte MCSS-Expertensystem

zum Management von Digitalisierung, Cybersicherheit & Datenschutz



### mit MC-KMU in der Cloud

NIS-2 stellt ab dem 18. Oktober 2024 höchste Anforderungen an alle Organisationen mit mehr als 50 Mitarbeitenden und/oder 10 Mio. Umsatz, auch im Gesundheits- und Sozialwesen.

Das MCSS-Expertensystem **MC-KMU** bietet einfache, schnelle und kostengünstige Lösungen für die organisatorische Umsetzung von NIS-2.

## Wie werden NIS-2-Lösungen der MCSS AG eingesetzt?

Die **MCSS-Expertensysteme** sind installationsfrei und innerhalb von 24 Stunden nach Lizenzierung einsatzbereit.

|   |  |  |   |  |  |
|---|--|--|---|--|--|
| <br>Wofür steht NIS-2?<br>Einführung | 1<br>Risikobewertungen und<br>Sicherheitsrichtlinien       | 2<br>Bewertung der Wirksamkeit von<br>Sicherheitsmaßnahmen         | 3<br>Einsatz von Kryptographie und<br>Verschlüsselung | 4<br>Umgang und Meldepflicht mit<br>Sicherheitsvorfällen | 5<br>Beschaffung von Systemen  |
| 6<br>Cybersicherheits Schulungen<br>und Computerhygiene   | 7<br>Sicherheitsverfahren für<br>Zugang zu sensiblen Daten | 8<br>Betriebskontinuität und<br>Strategien zum<br>Krisenmanagement | 9<br>Einsatz von Mehrfaktor-<br>Authentifizierung     | 10<br>Sicherheit im Zusammenhang<br>mit Lieferketten     | <br>Zusammenfassung |



**MCSS** AG  
**MioCloud**  
Solution Systems

A Robert-Perthel-Straße 77a  
50739 Köln  
T 0221/47 44 77 44  
F 0221/47 44 77 55  
E [info@mcss-ag.de](mailto:info@mcss-ag.de)  
W [mcss-ag.de](http://mcss-ag.de)

Gefördert durch:



Bundesministerium  
für Wirtschaft  
und Klimaschutz

aufgrund eines Beschlusses  
des Deutschen Bundestages

# Wie werden mit dem MCSS-Expertensystem die Pflichten und Aufgaben zu NIS-2 für die verschiedenen Abteilungen gelöst?

Die wichtigsten Pflichten und Aufgaben zu NIS-2 in verpflichteten Einrichtungen betreffen die Geschäftsleitung. Die verantwortliche Leitung kann ein NIS-Team etablieren, das der Geschäftsleitung zuarbeitet und delegierbare Aufgaben übernimmt.

Dabei unterstützt das MCSS-System mit Vorlagen nach dem folgenden Katalog:

| Pflicht   | Verantwortung   | Umsetzung  | Zeitpunkt  |
|---|---|--|--|
| Analyse der Betroffenheit, evtl. mit abhängigen Organisationen                      | Geschäftsleitung, Rechtsabteilung, Wirtschaftsprüfer    | Geschäftsleitung, NIS-Team   | Bei in Krafttreten und danach jährlich                 |
| Registrierung beim Bundesamt für Sicherheit in der Informationstechnik (BSI)        | Geschäftsleitung, Verwaltungsabteilung, Rechtsabteilung | Verwaltung, NIS-Team   | Nach Feststellung der Betroffenheit und bei Änderungen |
| Definition der Geltungsbereiche   | KRITIS-Team, HR-Abteilung, IT-Leitung                   | KRITIS-Team, HR-Abteilung, IT-Abteilung                            | Nach Registrierung                                     |
| Umsetzung technischer, organisatorischer, rechtlicher Maßnahmen zur Cybersicherheit | Geschäftsleitung, NIS-Team                              | NIS-Team, HR-Abteilung, IT-Abteilung, Rechtsabteilung              | Regelmäßig nach Curriculum                             |
| Prüfung Lieferkettensicherheit  | Geschäftsleitung, Einkaufsabteilung                     | NIS-Team, Einkaufsabteilung, Verwaltungsabteilung, Rechtsabteilung | Regelmäßig nach Curriculum                             |
| Prüfung der Cyber Security  | Geschäftsleitung, NIS-Team, IT-Leitung                  | Geschäftsleitung, NIS-Team, IT-Leitung                             | Zur ersten Einführung und anschließend alle 2 Jahre    |

Weitere Unterstützungen können individuell gebucht werden:

✔ **Dokumenten-Audits** (Prüfung von Leitlinien, Verfahrensanweisungen, Vertragszusätze etc.)

✔ **QM-Dokumentations-Audits** im NIS-2-Kontext (Rechtskonformität)

✔ **Lieferanten-Audits** mit NIS-2-Prüfungen der Lieferketten mit Prüfungsbestätigung

✔ **Coaching von NIS-Teams** zur Umsetzung der NIS-2-Anforderungen

# Welche Inhalte bietet das MCSS-NIS-2-Coaching für Führungskräfte in kleinen und mittleren Unternehmen?

|   |         |
|---|---------|
| <b>① Einführung</b>   | 15 min. |
| <ul style="list-style-type: none"><li>• Überblick EU-RL 2022/2555, NIS-2</li><li>• Einordnung und rechtliche Rahmenbedingungen</li><li>• Ermittlung der Betroffenheit</li></ul>   |         |
| <b>② Organisatorische Einordnung</b>  | 30 min. |
| <ul style="list-style-type: none"><li>• Die Rolle der Leitungsorgane</li><li>• Das NIS-2-Netzwerk<ul style="list-style-type: none"><li>– Die Geschäftsleitung in der Gesamtheit (Gesamtverantwortung)</li><li>– Die Rechtsabteilung oder der Justiziar (Einordnung und Verträge)</li><li>– Die Personalabteilung (Schulung, On- und Outboarding)</li><li>– Die IT-Abteilung (Technische Maßnahmen)</li><li>– Die Verwaltungs- und Einkaufsabteilung (QM &amp; Lieferketten)</li></ul></li></ul> |         |
| <b>③ Die konkreten Anforderungen</b>  | 75 min. |
| <ul style="list-style-type: none"><li>• Risikobewertungen und Sicherheitsleitlinien</li><li>• Einsatz von Kryptographie</li><li>• Umgang mit Sicherheitsvorfällen</li><li>• Cybersicherheitsschulungen und Computerhygiene</li><li>• Zugang zu sensiblen Daten</li><li>• Kontinuität und Krisenmanagement</li><li>• Einsatz von Mehrfaktor-Authentifizierung</li><li>• Sicherheit mit Lieferketten</li></ul>  |         |
| <b>Pause</b>  | 10 min. |
| <b>④ Die Management- und Expertensysteme</b>  | 30 min. |
| <ul style="list-style-type: none"><li>• ISMS</li><li>• DSMS (DSGVO)</li><li>• QMS (QM-Richtlinie)</li><li>• Synergien durch digitale Integration</li><li>• Onboarding MCSS-Expertensystem</li></ul>   |         |
| <b>⑤ Melde-, Nachweispflichten &amp; Aufsichtskompetenzen</b>   | 15 min. |
| <ul style="list-style-type: none"><li>• Registrierung und Veränderungsmeldungen</li><li>• Einordnung von Sicherheitsvorfällen</li><li>• Meldeverfahren bei Störungen</li><li>• Sanktionen, Strafen und Haftung der Verantwortlichen</li><li>• Cyberversicherungen</li></ul>   |         |
| <b>Zusammenfassung &amp; Empfehlungen</b>   | 5 min.  |

180 min.

**Zielgruppen:** Gesamtmanagement, Vorstand, Geschäftsführer, Aufsichtsrat, Betriebsrat, CIO, CTO, CISO, QMB, ISB, DSB und alle schulenden Rollen

**Abschluss:** Teilnahmebestätigung (Zertifikat) nach NIS-2-Anforderung

**Material:** Schulungsvideos (12 á 5 min.), Verfahrensanweisungen (ISO 9001), Vorlagen für Leitlinien, Curricula, Checklisten