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?

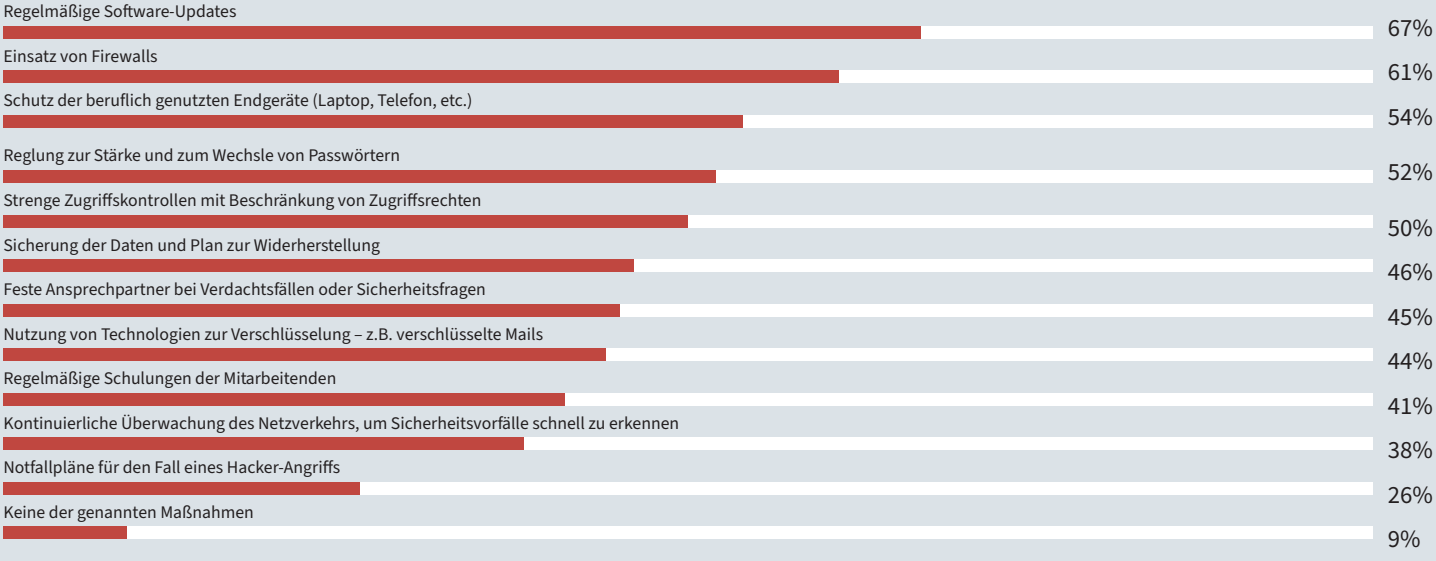
Die NIS-2-Richtlinie zielt darauf ab, in wesentlichen und wichtigen Einrichtungen die Cybersicherheit zu stärken und IT-Vorfälle zu vermeiden. Sie betrifft Unternehmen, Organisationen und Gesundheitsdienstleister in 18 verschiedenen Sektoren mit mehr als 50 Mitarbeitenden und/oder einem Jahresumsatz 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
AUFSICHT DURCH BEHÖRDEN	Proaktive Aufsicht (z.B. regelmäßige Sicherheitsprüfungen)	Reaktive Aufsicht nach Hinweisen auf Verstöße (z.B. gezielte Sicherheits-prüfungen)
GELDSTRAFEN BEI VERSTÖSSEN	Höchstbetrag von mind. 10 Mio. EUR oder 2% des weltweiten Umsatzes	Höchstbetrag von mind. 7 Mio. EUR oder 1,4% des weltweiten Umsatzes
WER ZÄHLT DAZU?	Große Unternehmen (Sektor Gesundheit) > 249 Beschäftigte, oder > 50 Mio. EUR Umsatz und > 43 Mio. EUR Bilanz Größenunabhängige Sonderfälle: z.B. DNS-Diensteanbieter, Zentralregierung, KRITIS, und Einrichtungen, die vom Staat als „wesentlich“ eingestuft werden	Mittlere Unternehmen (Sektor Gesundheit) mind. 50 Beschäftigte, oder > 10 Mio. EUR Umsatz und > 10 Mio. EUR Bilanz Größenunabhängige Sonderfälle: 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.

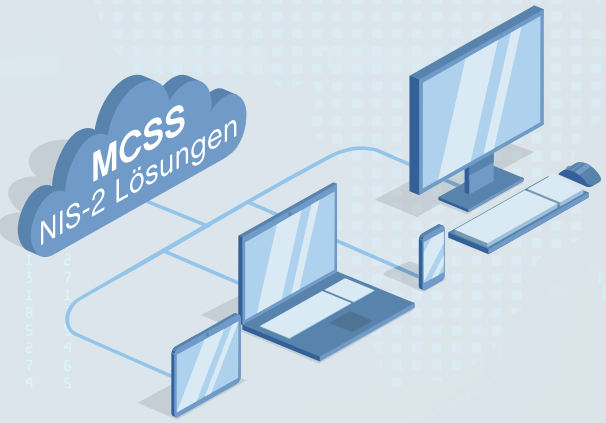
Welche Lösungen bietet das MCSS-Expertensystem zu NIS-2?

Die **MCSS-NIS-2-Lösungen** basieren auf dem vom Bundeswirtschaftsminister ausgezeichneten cloudbasierten Expertensystem für Krankenhäuser, Kliniken, große Pflege- und Sozialeinrichtungen ab 50 angestellten und freien Mitarbeitenden.

Das cloudbasierte **MCSS-Expertensystem**

zum Management von Digitalisierung, Cybersicherheit & Datenschutz

Zielgruppen: Medizinische und pflegende Einrichtungen sowie Organisationen



mit **MCSS-Expertensystemen** in der Cloud

MC-KLINIK MC-CURA MC-ORG

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.

Die MCSS-Expertensysteme mit **MC-KLINIK** (Krankenhäuser), **MC-CURA** (Pflegeeinrichtungen) und **MC-ORG** (für gemeinnützige Organisationen) bieten 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.

1 Wofür steht NIS-2? Einführung	2 Risikobewertungen und Sicherheitsrichtlinien	3 Bewertung der Wirksamkeit von Sicherheitsmaßnahmen	4 Einsatz von Kryptographie und Verschlüsselung	5 Umgang und Meldepflicht mit Sicherheitsvorfällen	6 Beschaffung von Systemen
7 Cybersicherheitsschulungen und Computerhygiene	8 Sicherheitsverfahren für Zugang zu sensiblen Daten	9 Betriebskontinuität und Strategien zum Krisenmanagement	10 Einsatz von Mehrfaktor-Authentifizierung	11 Sicherheit im Zusammenhang mit Lieferketten	12 Zusammenfassung

AUSGEZEICHNET DURCH DEN BUNDESWIRTSCHAFTSMINISTER
JUNI INNOVATIONSPROJEKT 2022

MCSS AG
MioCloud Solution Systems

A Robert-Perthel-Straße 77a
50739 Köln
T 0221/47447744
F 0221/47447755
E info@mcss-ag.de
W 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

ANMERKUNG:

Für Krankenhäuser und vergleichbare Einrichtungen stehen B3S-Vorlagen in der **MC-KLINIK** Version zur Verfügung.

Welche Inhalte bietet das MCSS-NIS-2-Coaching für Führungskräfte im Gesundheits- und Sozialwesen?

① Einführung — 15 min.

- Überblick EU-RL 2022/2555, NIS-2
- Einordnung und rechtliche Rahmenbedingungen
- Ermittlung der Betroffenheit im Gesundheits- und Sozialwesen

② Organisatorische Einordnung — 30 min.

- Die Rolle der Leitungsorgane
- Das NIS-2-Netzwerk
  - Die Geschäftsleitung in der Gesamtheit (Gesamtverantwortung)
  - Die Rechtsabteilung oder der Justiziar (Einordnung und Verträge)
  - Die Personalabteilung ((Schulung, On- und Outboarding)
  - Die IT-Abteilung (Technische Maßnahmen)
  - Die Verwaltungs- und Einkaufsabteilung (QM & Lieferketten)

③ Die konkreten Anforderungen — 75 min.

- Risikobewertungen und Sicherheitsleitlinien
- Einsatz von Kryptographie
- Umgang mit Sicherheitsvorfällen
- Cybersicherheitsschulungen und Computerhygiene
- Zugang zu sensiblen Daten
- Kontinuität und Krisenmanagement
- Einsatz von Mehrfaktor-Authentifizierung
- Sicherheit mit Lieferketten

Pause — 10 min.

④ Die Management und Expertensysteme — 30 min.

- ISMS incl. B3S für Krankenhäuser
- DSMS (DSGVO)
- QMS (QM-Richtlinie)
- Synergien durch digitale Integration
- Onboarding MCSS Expertensystem

⑤ Melde-, Nachweispflichten & Aufsichtskompetenzen — 15 min.

- Registrierung und Veränderungsmeldungen
- Einordnung von Sicherheitsvorfällen
- Meldeverfahren bei Störungen
- Sanktionen, Strafen und Haftung der Verantwortlichen
- Cyberversicherungen

Zusammenfassung & Empfehlungen — 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