KBV KASSENÄRZTLICHE BUNDESVEREINIGUNG

Neue Vorgaben für Cybersicherheit: Hinweise für betroffene Praxen und MVZ

Für schätzungsweise 1.000 Praxen und Medizinische Versorgungszentren (MVZ) gelten seit 6. Dezember 2025 strengere Vorgaben für die Stärkung der Cybersicherheit – also für den Schutz vor Angriffen auf das eigene Netzwerk und die Informationssicherheit. Grund ist das in Kraft getretene Gesetz zur Umsetzung der europäischen NIS-2-Richtlinie (siehe unten). Betroffen sind größere und umsatzstarke Praxen und MVZ. Wer genau dazu zählt und was in diesem Fall zu beachten ist, fasst diese PraxisInfo zusammen.

Schutz vor Angriffen auf das eigene Netzwerk

AUF EINEN BLICK

NIS-2 – DARUM GEHT ES

NIS-2 steht für die zweite Richtlinie zur Netzwerk- und Informationssicherheit („Network and Information Security Directive 2“). Es handelt sich um eine EU-Richtlinie zur Harmonisierung und Stärkung der Cybersicherheit, die im Vergleich zur ersten Direktive den Geltungsbereich auf mehr Sektoren ausdehnt, strengere Sicherheitsanforderungen und Meldepflichten festlegt und auch höhere Bußgelder androht. In Deutschland trat das zugehörige NIS-2-Umsetzungsgesetz am 6. Dezember 2025 in Kraft. Die neuen Regelungen finden sich im novellierten BSI-Gesetz (siehe Serviceteil am Ende dieser PraxisInfo).

Betroffen nur, wenn Praxis oder MVZ als „wichtig“ gilt

WELCHE PRAXEN/MVZ SIND BETROFFEN?

Alle, die mindestens als „wichtige Unternehmen“ gelten

Betroffen von der NIS-2-Richtlinie sind größere und/oder umsatzstarke Praxen (inkl. Berufsausübungsgemeinschaften/BAG) und MVZ, die eines dieser beiden Kriterien erfüllen und damit als wichtige Unternehmen gelten:

- es arbeiten dort mindestens 50 Personen oder
- es wird ein Jahresumsatz von über 10 Millionen Euro ausgewiesen

Bei 50 Personen oder 10 Mio. Euro Umsatz

Weitere Verschärfung für „besonders wichtige Unternehmen“

Es kann sein, dass eine Praxis oder ein MVZ als besonders wichtiges Unternehmen entsprechend der EU-Richtlinie gilt. Dann gelten noch strengere oder zusätzliche Regelungen. Dies ist der Fall, wenn sie eines der beiden Kriterien erfüllen:

- es arbeiten dort mindestens 250 Personen oder
- es wird ein Jahresumsatz von über 50 Millionen Euro und eine Jahresbilanzsumme von 43 Millionen Euro ausgewiesen

Der Bundesverband Medizinische Versorgungszentren schätzt, dass insgesamt etwa 1.000 Praxen und MVZ unter die NIS-2-Richtlinie fallen könnten.

Betrifft etwa 1.000 Praxen und MVZ

Mehr Schutz vor Hackerangriffen

Bereits jetzt gibt es in puncto Datenschutz und Datensicherheit Vorgaben für Unternehmen und Einrichtungen – auch für den Gesundheitsbereich und somit für Praxen und MVZ. Zu nennen sind etwa die Datenschutzgrundverordnung auf EU-Ebene oder nationale berufsrechtliche Vorschriften wie die ärztliche Schweigepflicht.

EU-Richtlinie und Gesetz in Deutschland

Weil es immer häufiger zu Hackerangriffen auf Unternehmen und Einrichtungen kommt, hat die EU bereits im Jahr 2022 die zweite Richtlinie zur Netzwerk- und Informationssicherheit veröffentlicht (NIS-2-Richtlinie). Die EU-Mitgliedstaaten mussten sie in nationales Recht umsetzen, so nun auch in Deutschland.

Konkret erfolgte es durch das „Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung“. Die Regelungen gelten nicht nur für Krankenhäuser, sondern auch für größere Praxen und MVZ, wenn sie einen Schwellenwert überschreiten. Denn dann sind sie „wichtige Unternehmen“ oder „besonders wichtige Unternehmen“ im Sinne der NIS-2-Richtlinie.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) informiert ausführlich darüber: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/kritis_node.html

EMPFEHLUNG FÜR ALLE: ZUERST NIS-2-BETROFFENHEITSPRÜFUNG

Prüfen, ob Praxis/MVZ überhaupt betroffen ist

Zunächst sollten Inhaberinnen und Inhaber von Praxen und MVZ prüfen, ob die eigene Einrichtung von den neuen Vorgaben betroffen ist. Dazu müssen sie eigenständig die NIS-2-Betroffenheitsprüfung durchführen, die online beim BSI möglich ist:

Prüfung online absolvieren

Prüfung ist online möglich

- Auf der Internetseite des BSI kann die **NIS-2-Betroffenheitsprüfung** online durchgeführt werden: https://betroffenheitspruefung-nis-2.bsi.de/.
- Grundlage ist ein allgemeines Schema, das als PDF abrufbar ist: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-betroffenheit-entscheidungsbaum.pdf?__blob=publicationFile&v=9

Registrierung und Hinweise für die Umsetzung

- Wer betroffen ist, kann sich beim BSI registrieren: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html
- Das BSI stellt für die Umsetzung Hinweise bereit: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-was-tun/NIS-2-was-tun_node.html

DIESE PFLICHTEN HABEN BETROFFENE

Pflichten

1. Die Praxis oder das MVZ gilt als „wichtiges Unternehmen“

Sobald die eigene Praxis oder das MVZ als wichtiges Unternehmen im Sinne der EU-Vorgaben gilt, sind bestimmte Pflichten zu erfüllen.

Wichtige Punkte:

Registrieren

- **Registrierungspflicht** (§ 33 BSI-Gesetz neue Fassung[1]) bei der neuen Meldestelle beim BSI.

Vorfälle innerhalb von Fristen melden

- **Meldepflicht bei erheblichen Sicherheitsvorfällen** (§ 32 BSI-Gesetz neue Fassung) gegenüber der Meldestelle beim BSI:
  - **Binnen 24 Stunden** nach Kenntnisnahme eines Vorfalls Erstmeldung,
  - **Binnen 72 Stunden** nach Kenntnisnahme eines Vorfalls Bewertung von Schwere und Auswirkungen
  - **Binnen eines Monats** eine Abschlussmeldung.
- **Mindestanforderungen an die IT-Sicherheit** (§ 30 BSI-Gesetz neue Fassung), zum Beispiel:
  - Einsatz moderner Verschlüsselungstechnik
  - Multi-Faktor-Authentifizierung
  - regelmäßige Mitarbeiterschulungen zur Cybersicherheit
- **Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen** (§ 38 BSI-Gesetz neue Fassung)
- **Aufsichts- und Durchsetzungsmaßnahmen** (§§ 61, 62 BSI-Gesetz neue Fassung)
- **Bußgeldvorschriften** (§ 65 BSI-Gesetz neue Fassung): Es kann zu Bußgeldern von bis zu 7 Millionen Euro kommen.

2. Die Praxis oder das MVZ gilt als „besonders wichtiges Unternehmen“

Zählt die eigene Praxis oder das MVZ sogar zu den besonders wichtigen Unternehmen, gelten weitere Aufsichts- und Durchsetzungsmaßnahmen (§ 61 BSI-Gesetz neue Fassung) und teilweise höhere Geldbußen (§ 65 BSI-Gesetz neue Fassung). Einige besonders wichtige Einrichtungen sind Betreiber kritischer Anlagen. Diese haben weitere Pflichten zu erfüllen (nach § 31 und § 39 BSI-Gesetz neue Fassung).

Alle Vorschriften stehen im novellierten BSI-Gesetz in den Teilen 3 bis 8 (§§ 30 ff. BSI-Gesetz): https://www.gesetze-im-internet.de/bsig_2025/index.html

Beraten lassen

Es kann ratsam sein, sich je nach individueller Gesellschaftsform beraten zu lassen. Diese Rechtsberatung darf nur von Volljuristen durchgeführt werden.

BSI-Gesetz

Novelliertes BSI-Gesetz: www.gesetze-im-internet.de/bsig_2025/index.html

Veröffentlichung im Bundesgesetzblatt (BGBl). 2025 I Nr. 301 vom 5.12.2025: www.recht.bund.de/bgbl/1/2025/301/VO

Informationen des BSI

NIS-2-Betroffenheitsprüfung: https://betroffenheitspruefung-nis-2.bsi.de/

NIS-2-Registrierung: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/nis-2-regulierte-unternehmen_node.html

Informationen des BSI zur kritischen Infrastruktur: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/kritis_node.html

Weitere Informationen des BSI

MEHR FÜR IHRE PRAXIS

www.kbv.de

↗ **PraxisWissen**
↗ **PraxisWissenSpezial**
Themenhefte für Ihren Praxisalltag

Abrufbar und kostenfrei bestellbar unter:
www.kbv.de/838223

↗ **PraxisInfo**
↗ **PraxisInfoSpezial**
Themenpapiere mit Informationen für Ihre Praxis

Abrufbar unter:
www.kbv.de/605808

↗ **PraxisNachrichten**
Der wöchentliche Newsletter per E-Mail oder App

Abonnieren unter:
www.kbv.de/PraxisNachrichten
www.kbv.de/kbv2go

IMPRESSUM

Herausgeberin:
Kassenärztliche Bundesvereinigung
Herbert-Lewin-Platz 2, 10623 Berlin
Tel.: 030 4005-0, Fax: 030 4005-1590
info@kbv.de, www.kbv.de

Redaktion:
Interne Kommunikation im Stabsbereich Strategie, Politik und Kommunikation

Fachliche Betreuung:
Abteilung Informationssicherheit / IT-Security

Stand:
Dezember 2025

Hinweise:
Aus Gründen der Lesbarkeit wurde meist eine Form der Personenbezeichnung verwendet. Hiermit sind auch alle anderen Formen gemeint.

---

[1] Das bestehende BSI-Gesetz wird durch das NIS2UmsuCG geändert zum BSI-Gesetz (neue Fassung).