KBV KASSENÄRZTLICHE BUNDESVEREINIGUNG

GESETZLICHE VORGABEN FÜR CYBERSICHERHEIT
HINWEISE FÜR BETROFFENE PRAXEN UND MVZ

Schutz vor Angriffen auf das eigene Netzwerk

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

AUF EINEN BLICK

NIS-2 – DARUM GEHT ES

EU-Richtlinie

Umsetzung in Deutschland

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).

WELCHE PRAXEN/MVZ SIND BETROFFEN?

Alle, die mindestens als „wichtige Unternehmen“ gelten

Wann Praxis oder MVZ als „wichtig“ gilt

Betroffen sind Praxen (inkl. Berufsausübungsgemeinschaften/BAG) und MVZ, die:

- mindestens 50 Personen beschäftigen
- oder mindestens 10 Millionen Euro Jahresumsatz **und** mindestens 10 Millionen Euro Jahresbilanz haben

Schwellenwerte

Wenn eine Praxis oder ein MVZ ein „besonders wichtiges Unternehmen“ entsprechend der EU-Richtlinie ist, gelten noch strengere Vorgaben. Dies ist der Fall, wenn sie:

- mindestens 250 Personen beschäftigen
- oder mindestens 50 Millionen Euro Jahresumsatz und mindestens 43 Millionen Euro Jahresbilanzsumme haben

Betrifft etwa 1.000 Praxen und MVZ

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

PraxisInfo

Hintergrund und Ziel: Mehr Schutz vor Hackerangriffen

In puncto Datenschutz und Datensicherheit gibt es schon seit längerem Vorgaben für Unternehmen und Einrichtungen – auch im Gesundheitsbereich und somit für Praxen/MVZ. Zu nennen sind etwa die Datenschutzgrundverordnung auf EU-Ebene oder nationale berufsrechtliche Vorschriften wie die ärztliche Schweigepflicht.

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 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 und mindestens als „wichtige Unternehmen“ gelten.

Sie müssen sich dann beim Bundesamt für Sicherheit in der Informationstechnik (BSI) registrieren und erhebliche Sicherheitsvorfälle innerhalb von 24 Stunden nach Bekanntwerden beim BSI melden.

SO GEHEN PRAXEN VOR

1. Betroffenheit prüfen

Im ersten Schritt sollten Praxen/MVZ prüfen, ob die eigene Einrichtung überhaupt von den Vorgaben betroffen ist. Dazu führen sie eigenständig die NIS-2-Betroffenheitsprüfung durch, was sie online beim BSI tun können:

Prüfen, ob Praxis/MVZ betroffen ist

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

2. Betroffene Praxis registrieren

Alle Praxen und MVZ, die betroffen sind, müssen sich beim BSI registrieren. Dabei werden unter anderem Name und Anschrift, die Rechtsform, Kontaktdaten sowie Angaben zur Anzahl der Beschäftigten und zum Jahresumsatz abgefragt. Durch die Registrierung erhält die Praxis individuelle Zugangsdaten. Das BSI bietet hierzu eine Anleitung an, von der Praxen auch zur Registrierung gelangen:

Registrieren und Kontaktdaten hinterlegen

Schritt-für-Schritt-Anleitung zur Registrierung:

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

3. Erhebliche Sicherheitsvorfälle melden und Fristen einhalten

Kommt es zu einem erheblichen IT-Sicherheitsvorfall, muss dieser innerhalb von 24 Stunden, nachdem er der Praxis bekannt wurde, an das BSI gemeldet werden:

Vorfälle melden

- spätestens 24 Stunden nach Kenntnis: frühe Erstmeldung
- spätestens 72 Stunden nach Kenntnis: ausführliche Meldung
- spätestens 30 Tage nach Kenntnis: Folgemeldung oder Abschlussmeldung

Ein erheblicher Sicherheitsvorfall liegt vor, wenn dieser:

› schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann oder
› andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann.

(BSI-Gesetz § 2 Begriffsbestimmungen Nr. 11 erheblicher Sicherheitsvorfall)

Erhebliche Sicherheitsvorfälle

Beispiele

Ausfall des Praxisnetzwerks durch Cyberangriff:

Die Server und Netzwerkgeräte einer Praxis werden durch einen Angriff lahmgelegt, die Praxis muss schließen, Patienten werden abgewiesen, die Versorgung ist akut eingeschränkt.

Beispiel: Netzwerk fällt aus und Praxis muss schließen

Manipulation eines medizinischen Großgeräts durch Cyberkriminelle:

In einem MVZ wurde der Magnetresonanztomograph (MRT) durch Cyberkriminelle manipuliert, das bildgebende System arbeitet dadurch fehlerhaft und die Patientensicherheit ist gefährdet.

Verlust großer Mengen sensibler Patientendaten durch einen Cyberangriff:

Hacker stehlen Stammdaten, Diagnosen, Befunde, Medikationslisten, es drohen Erpressung und/oder Veröffentlichung der sensiblen Daten, die Integrität und Vertraulichkeit sind gefährdet.

ALLE PFLICHTEN IM ÜBERBLICK

Praxen/MVZ, die als „wichtige Unternehmen“ eingestuft sind

Pflichten für „wichtige Unternehmen“

› Registrierungspflicht beim BSI (§ 33 BSI-Gesetz neue Fassung[1])
› Meldepflicht bei erheblichen Sicherheitsvorfällen (§ 32 BSI-Gesetz neue Fassung) bei 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.
› Erfüllen von Mindestanforderungen zur 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)
› Bei Verstößen Zahlung von Bußgeldern (§ 65 BSI-Gesetz neue Fassung): Es kann zu Bußgeldern von bis zu 7 Millionen Euro kommen.

Praxen/MVZ, die als „besonders wichtige Unternehmen“ gelten

Pflichten für „besonders wichtige Unternehmen“

In dem Fall 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 (§ 31 und § 39 BSI-Gesetz neue Fassung). Alle Vorschriften stehen in Teil 3 bis 8 des novellierten BSI-Gesetzes: 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.

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 zur 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

[1] Das bestehende BSI-Gesetz wurde durch das NIS-2-Umsetzungsgesetz geändert zum BSI-Gesetz (neue Fassung).

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, E-Mail: info@kbv.de, www.kbv.de

Redaktion:

Interne Kommunikation im Stabsbereich Strategie,
Politik und Kommunikation

Fachliche Betreuung:

Abteilung Informationssicherheit / IT-Security

Stand: März 2026

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