zvdh -kompakt

06/2026

Cybersicherheitsgesetz (NIS-2): Was Dachdeckerbetriebe wissen müssen

Köln, 12. Februar 2026

Am 21. November 2025 trat das neue Cybersicherheitsgesetz (NIS-2) in Kraft. Es stärkt die IT-Sicherheit in den sogenannten kritischen Sektoren wie Energie, Verkehr oder Gesundheitswesen. Dachdeckerbetriebe sind meist nicht direkt betroffen – es gibt aber wichtige Ausnahmen und indirekte Pflichten. Um eine Betroffenheit zu prüfen können Tools wie der NIS-2-Navigator des BSI oder der Check von Deutschland sicher im Netz genutzt werden.

Direkt betroffen

ist nur, wenn der Betrieb mehr als 50 Mitarbeiter oder über zehn Millionen Euro Umsatz hat und in einem kritischen Sektor tätig ist (z. B. digitale Dienstleistungen für kritische Infrastrukturen). Diese Schritte müssen dann umgesetzt werden:

- Risikomanagement für IT-Systeme einführen
- Sicherheitsvorfälle an das BSI melden
- Technische Schutzmaßnahmen (Backups, Updates) umsetzen
- Mitarbeiter schulen und Maßnahmen dokumentieren

Indirekt betroffen

sind Betriebe, die für große Auftraggeber aus kritischen Sektoren (z. B. kommunale Energieversorger, Krankenhäuser) arbeiten. Diese können IT-Sicherheitsnachweise verlangen. Auch ohne direkte Betroffenheit sollten Sie handeln, um bei möglichen Anforderungen von betroffen Auftraggebern schnell reagieren zu können:

- Kundenanforderungen vorbereiten, z. B. IT-Sicherheits-Selbstauskunft
- Grundlegende Maßnahmen wie MFA, Backups und Phishing-Schulungen umsetzen

Fazit fürs Dachdeckerhandwerk

Auch wenn NIS-2 für die meisten Dachdeckerbetriebe keine direkten Pflichten mit sich bringt, lohnt es sich, die indirekten Auswirkungen im Blick zu behalten – besonders bei Großkunden. Einfache Maßnahmen wie 2-Faktor-Authentifizierung oder Backups stärken die IT-Sicherheit und bereiten Sie auf mögliche Anforderungen vor. Aber auch um Ihr Unternehmen vor Angriffen zu schützen, lohnt es sich, vorzusorgen. Im letzten Jahr war bereits jedes 2. KMU-Unternehmen von einem Hackerangriff betroffen.

Checkliste: Cybersicherheit für Betriebe

1. MFA (Multi-Faktor-Authentifizierung) einschalten für E-Mail, Office/Cloud, Buchhaltungstools: MFA ist ein Sicherheitsverfahren, bei dem man zwei verschiedene Nachweise eingeben muss, um sich einzuloggen, z.B. etwas, das man weiß (Passwort) und etwas, das man hat (z. B. Einmalcode per App/SMS oder Sicherheitsschlüssel)
2. Backups prüfen: täglich, getrennt aufbewahrt; Wiederherstellung dokumentieren
3. Updates automatisieren: Betriebssysteme, Browser
4. Phishing-Schulung für die Mitarbeitenden
5. IT-Notfallkarte mit Notfall-Telefonnummer ausfüllen und sichtbar im Büro aufhängen.
6. IT-Kontakt und Vertretung benennen; Lieferantenliste und AV-Verträge aktualisieren.
7. Auf Kundenanforderungen vorbereiten: Eine Dokumentation 1–2 Seiten „IT-Sicherheits-Selbstauskunft“ für Ausschreibungen und Kunden
8. IT-Sicherheitsverantwortliche und Vertretung festlegen.

Weiterführende Infos und Checklisten finden Innungsbetriebe im internen Mitgliederbereich (Aktuelles/Cybersicherheit).

Herausgeber: Zentralverband des Deutschen Dachdeckerhandwerks e.V., Fritz-Reuter-Straße 1, 50968 Köln
☎ 0221-398038-0 E-Mail zvdh@dachdecker.de // Internet www.dachdecker.de // verantwortlich: Claudia Büttner