

IT-Sicherheit: NIS-2-Richtlinie maßvoll umsetzen

Stand: Juni 2025

Einordnung

Der Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung wird die zweite EU-Richtlinie zur Netzwerk- und Informationssicherheit (NIS-2) in deutsches Recht umsetzen. Diese Umsetzung hätte bereits bis zum Oktober 2024 erfolgen müssen, scheiterte jedoch aufgrund der vorgezogenen Neuwahlen des Bundestages aufgrund des Scheiterns der früheren Regierungskoalition.

Ziele

Alle betroffenen Unternehmen sollen künftig zentrale Schutzmaßnahmen etablieren. Etwa Risikoanalysen, Notfallpläne, Backup-Konzepte oder Verschlüsselungslösungen. Der Umfang richtet sich nach der Bedeutung der Einrichtung.

U.a. wird auch das Meldeverfahren bei einem Cyberangriff in ein gestuftes Verfahren geändert: zunächst soll eine kurze Erstmeldung innerhalb von 24 Stunden, dann ein Zwischenstand nach 72 Stunden und schließlich ein Abschlussbericht innerhalb eines Monats erfolgen.

Des Weiteren wird die Rolle für des BSI durch mehr Befugnisse zur Aufsicht und Durchsetzung gestärkt. Bei schwerwiegenden Verstößen können künftig auch Bußgelder verhängt werden, die sich am Jahresumsatz orientieren.

Forderungen

- Die Unternehmen müssen rechtssicher feststellen können, ob sie von dem Gesetz betroffen sind und damit auch den Verpflichtungen nachkommen müssen.
- Die Umsetzung des NIS-2-Gesetzes und des KRITIS-Dachgesetzes müssen Hand in Hand gehen. Es darf keine Doppel-Strukturen und Doppel-Meldungen geben.
- Es darf zudem keine Ungleichbehandlung zwischen Wirtschaft und staatlicher Verwaltung geben, wenn diese zumindest teilweise vom Anwendungsbereich ausgenommen wird.
- Die Umsetzung muss eins zu eins zur Richtlinie erfolgen und es dürfen keine weiteren unnötigen bürokratischen Regelungen aufgebaut werden.