**CHECKLISTE: Schritt-für-Schritt-Anleitung NIS-2-Richtlinie**

**Ablauf**

**Achten Sie hierauf**

**Umgesetzt?**

Schritt 1: Klären Sie, inwieweit Ihr Unternehmen be- troffen ist.

* Prüfen Sie, ob die Festlegungen aus der NIS-2-RL dazu führen, dass Ihr Unternehmen aller Voraussicht nach die Anforderungen umsetzen muss. Diese werden sich insbesondere aus dem angepassten BSIG ergeben.
* Schauen Sie, inwieweit Ihr Unternehmen indirekt betroffen ist. So kann Ihr Unternehmen ggf. nicht direkt den Anforderungen der NIS-2-RL und der deutschen Umsetzung unterliegen. Ggf. werden die Anforderungen an Ihr Unternehmen im Rahmen von Aufträgen weitergegeben.

q Ja q Nein

Schritt 2: Verant- wortliche festlegen und Projekt starten

* Steht fest, dass Ihr Unternehmen die Anforderungen umsetzen muss, ist es unumgänglich, die Sache anzugehen. Aussitzen ist nicht drin.
* Ihr Unternehmen sollte ein Projektteam zusammenstellen, damit der nötige Handlungsbedarf ausgemacht wird. Zudem müssen Entscheidungen getroffen und Maßnahmen umgesetzt werden.

q Ja q Nein

Schritt 3: Gefah- ren und Risiken analysieren und bewerten

* Ihr Unternehmen muss die Risiken an sich ausmachen, die sich aus der Geschäftstätigkeit bzw. etwa aus der Bedrohungssituation durch Cyberkriminelle ergeben. Risiken können sich aber auch aus Dienstleistungen ergeben, die man gegenüber anderen erbringt.
* Auch die Umsetzung der Vorgaben an sich sollte unter Risikoaspekten betrachtet werden. Ggf. wird es keine oder nur kurze Übergangsfristen in Deutschland geben.
* Es müssen Maßnahmen abgeleitet werden, um mit den Risiken angemessen umzugehen.

q Ja q Nein

Schritt 4: Bestands- aufnahme durch- führen

* Überblick zu gewinnen ist wichtig. Ggf. ist schon vieles in Ihrem Unternehmen vorhanden und manche Maßnahmen sind ausreichend.
* Ideal ist ein Soll-Ist-Abgleich bzw. eine Analyse der Lücken (sogenannte Gap-Analyse). Passt das Ist noch nicht, müssen Maßnahmen festgelegt werden, um das Soll zu erreichen.

q Ja q Nein

Schritt 5: Regelun- gen, Standards und Prozesse etablieren

* Diese Festlegungen sind entscheidend, damit die Sache insgesamt funktionieren kann.
* Prozesse dürfen nicht nur auf dem Papier funktionieren. Hier ist die Praxis entscheidend.

q Ja q Nein

Schritt 6: Beschäf- tigte sensibilisieren und qualifizieren

* Relevante Beschäftigte müssen über das erforderliche Know-how verfügen. Auch das ist nötig, um Risiken zu minimieren. Schulungen und Sensibilisierungsmaßnahmen sind unerlässlich.
* IT-Sicherheit ist meist etwas für Spezialisten. Laienhafte Kenntnisse führen früher oder später zu Schäden. Hinterfragen Sie die Qualifikation der zuständigen Kollegen.

q Ja q Nein

Schritt 7: Melde- pflichten organi- sieren

* Zukünftig wird es besondere Meldepflichten geben, etwa zu IT-Sicherheitsvorfällen. Hierzu müs- sen Prozesse festgelegt und Verantwortliche benannt werden.
* Empfehlen Sie, dass man die zukünftigen Regelungen des BSIG im Auge behält. Hier wird es Vor- gaben zu Meldepflicht und Meldeweg geben.

q Ja q Nein

Schritt 8: Doku- mentation erstellen

* Die ergriffenen Maßnahmen müssen dokumentiert sein. Damit kann Ihr Unternehmen belegen, welche Umsetzungsmaßnahmen ergriffen wurden.
* Die Dokumentation darf keine Lücken aufweisen. Außerdem ist Aktualität entscheidend.

q Ja q Nein

Schritt 9: Prüfung der Umsetzung

* Dass Maßnahmen wirksam umgesetzt sind und funktionieren, muss durch Kollegen geprüft wer- den, die das fachlich gut beurteilen können.
* Ggf. ist eine Prüfung durch externe Spezialisten oder eine Zertifizierung nötig, etwa weil ein Ge- schäftspartner eine unabhängige Bewertung fordert.

q Ja q Nein

Schritt 10: Anpas- sungsbedarf fort- laufend ermitteln

* Es ist vieles noch im Fluss. Insofern muss fortlaufend geprüft werden, inwieweit aufgrund ver- änderter Rahmenbedingungen Anpassungsbedarf besteht.
* Auch Risiken können sich verändern. Insofern müssen auch die Maßnahmen angepasst werden.

q Ja q Nein