Risikoanalyse nach NIS2

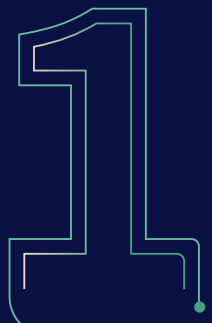
Athereon GRC

Athereon GRC

Risikoanalyse nach **NIS2**

Schritt für Schritt

Die NIS2-Richtlinie verpflichtet Unternehmen und Organisationen, geeignete und verhältnismäßige Maßnahmen zum Risikomanagement der Informationssicherheit umzusetzen (Art. 21). Zentrale Grundlage ist eine systematische Risikoanalyse. Sie ermöglicht es, Bedrohungen und Schwachstellen zu erkennen, Auswirkungen zu bewerten und angemessene Schutzmaßnahmen einzuleiten.



Kontext und Geltungsbereich festlegen

Bevor Risiken bewertet werden können, muss klar sein, welche Systeme, Prozesse und Informationen betrachtet werden. Dazu gehört die Abgrenzung des Untersuchungsbereichs: Welche IT-Systeme, Dienste und Daten sind für die Erfüllung geschäftskritischer Aufgaben oder gesetzlicher Pflichten relevant? NIS2 fordert, dass alle wesentlichen und wichtigen Einrichtungen ihre kritischen Abhängigkeiten systematisch erfassen.

Bedrohungen und Schwachstellen identifizieren

Im zweiten Schritt werden potenzielle Gefahrenquellen ermittelt – von Cyberangriffen über technische Ausfälle bis hin zu organisatorischen Mängeln. Ebenso wichtig ist es, bestehende Schwachstellen zu dokumentieren, die Angriffe oder Störungen erleichtern könnten. Dieser Schritt schafft Transparenz über das gesamte Risikoumfeld.

Risiken bewerten

Die identifizierten Risiken müssen nach Eintrittswahrscheinlichkeit und Auswirkung bewertet werden. Ziel ist es, eine Priorisierung vorzunehmen: Welche Risiken gefährden die Verfügbarkeit, Integrität, Vertraulichkeit oder Authentizität besonders stark? NIS2 fordert, dass Organisationen Risiken anhand ihrer möglichen betrieblichen und gesellschaftlichen Folgen einschätzen.

Maßnahmen ableiten und umsetzen

Aus der Bewertung werden technische und organisatorische Schutzmaßnahmen (TOMs) abgeleitet. Dazu zählen z. B. Zugriffskontrollen, Backup-Strategien, Notfallpläne oder Sensibilisierung der Mitarbeitenden. NIS2 verlangt, dass diese Maßnahmen angemessen und verhältnismäßig zur Risikolage ausgestaltet werden.

Dokumentation und kontinuierliche Überprüfung

Alle Ergebnisse der Risikoanalyse müssen nachvollziehbar dokumentiert werden. Dazu gehören Annahmen, Bewertungskriterien, Entscheidungen und getroffene Maßnahmen. Da sich Bedrohungslage und Unternehmensumfeld laufend ändern, ist die Risikoanalyse regelmäßig zu überprüfen und zu aktualisieren. NIS2 betont die Pflicht zur kontinuierlichen Anpassung.

Fazit

Die Risikoanalyse ist das Herzstück des Risikomanagements nach NIS2. Sie hilft Organisationen, Informationssicherheit systematisch anzugehen und die gesetzlichen Vorgaben nachweisbar zu erfüllen. Wer frühzeitig beginnt, schafft eine belastbare Grundlage für weitere Sicherheitsmaßnahmen – und erhöht zugleich die Resilienz des eigenen Unternehmens.

Athereon GRC

Athereon GRC GmbH
Innovationsring 7-9
66115 Saarbrücken

grc@athereon.de

+49 681 9697 297

www.athereon.de