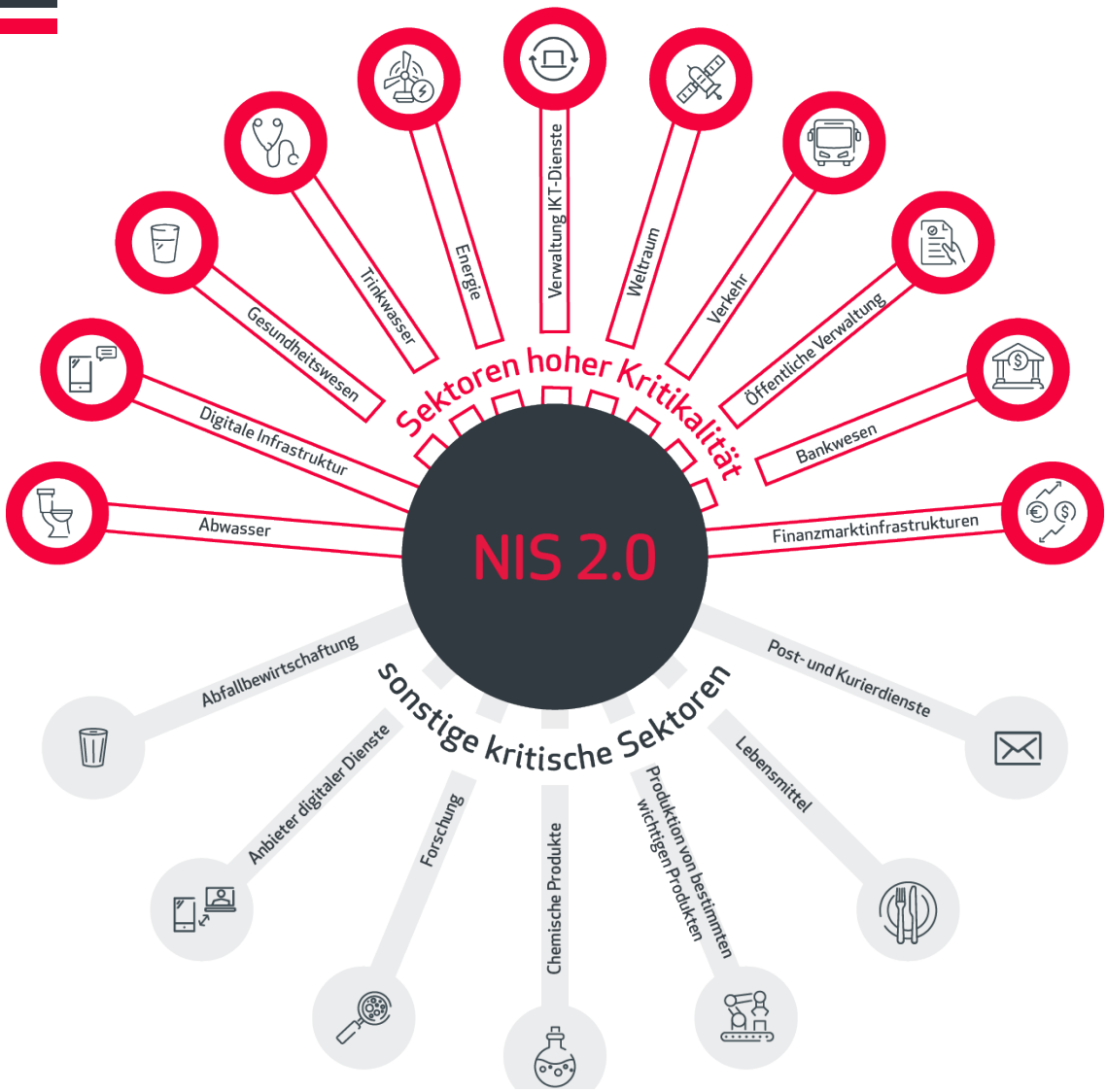
ACP



Checkliste

Fit für die EU NIS 2 Richtlinie

Fit für die EU NIS 2 Richtlinie

Aufgrund der stetig wachsenden Gefahr von Cyberangriffen verabschiedete die EU eine Richtline für Netz- und Informationssystemsicherheit. Dadurch werden Regelungen für mehr Cybersicherheit im Bereich der kritischen Infrastruktur geschaffen. Im Oktober 2024 tritt die Novellierung des NIS-Gesetzes, NIS 2.0 in Kraft, die Unternehmen mit zusätzlichen Anforderungen an die Informationssicherheit konfrontiert.

Unsere Checkliste bietet einen Überblick über die Anforderungen und Schritte in Bezug auf die NIS 2 Richtlinie. Sie dient als nützliche Grundlage, um sicherzustellen, dass Ihre Organisation die erforderlichen Maßnahmen zur Verbesserung der Cybersicherheit und zur Einhaltung der EU-Vorschriften ergriffen hat. Erfahren Sie, wie Sie die NIS2-Richtlinie umsetzen können und die digitale Resilienz Ihres Unternehmens stärken können.

1

☐

Eigene Betroffenheit sowie Registrierungs- und Meldepflicht klären

Ist Ihr Unternehmen in einer der wesentlichen oder wichtigen Sektoren tätig? Häufig ist die Zuordnung nicht eindeutig möglich, weshalb die Meinung von Expert*innen unterstützen kann.

2

☐

Betroffenheit von Kunden und Lieferanten klären (Lieferkettensicherheit ist laut NIS 2 zu gewährleisten)

NIS 2 geht uns alle an! Finden Sie Ihr Unternehmen in einer der Sektoren wieder oder sind Ihre Kunden von NIS 2 betroffen? Dann sollte innerhalb Ihres Unternehmens ein adäquates Maß an Cybersicherheit umgesetzt sein. Damit sind Sie optimal für entsprechende Überprüfungen vorbereitet. Dies gilt übrigens auch für Ihre Lieferanten.

3

☐

Überblick über Anforderungen und Strafen der NIS 2-Richtlinie verschaffen

Auch die Geschäftsführung sollte mit den Anforderungen und möglichen Sanktionen von NIS 2 vertraut gemacht werden. Besonders zu erwähnen ist hier, dass die Geschäftsführung bei Verstößen direkt haftbar gemacht werden kann.

4

Management in Bezug auf Cybersecurity und Risikomanagement schulen

Das obere Management muss kontinuierlich über mögliche Risiken und Gefahren informiert werden. Das Management, aber auch alle anderen Mitarbeiter*innen müssen in regelmäßigen Abständen nachweisbare Security Awareness Schulungen durchlaufen.

5

11 Kategorien und Sicherheitsmaßnahmen überprüfen

Von der Erkennung von Cybersicherheitsvorfällen bis hin zu einem funktionierenden Krisenmanagement: die zu erfüllenden Anforderungen sind weitgreifend. Eine Security-GAP-Analyse kann Aufschluss darüber geben, wo Handlungsbedarf besteht.

6

Die notwendigen Ausgaben planen

Security erfordert Ressourcen. Ermitteln und planen Sie rechtzeitig Maßnahmen und das erforderliche Budget, um NIS 2-compliant zu werden.

7

Lieferketten-Sicherheit bewerten

Regelmäßige Audits und Lieferantenbewertungen geben Ihnen die notwendige Information, wie es um die Cybersicherheit in Ihrer Lieferkette steht.

8

Prozesse und Vorfallmanagement definieren

Wie reagieren Sie im Falle eines Angriffs? Unser Security Operations Center kann Sie dabei unterstützen, Vorfälle rechtzeitig zu erkennen und frühzeitig notwendige Gegenmaßnahmen zu setzen.

9

Geschäftskontinuität und Krisenmanagement planen

Sind Prozesse und Verantwortlichkeiten definiert, wenn die Geschäftskontinuität gefährdet ist? Wer ist im Krisenfall zu informieren und wie ist das Krisenmanagement abgebildet? Krisenübungen können helfen, einen Plan auf seine Wirksamkeit zu überprüfen.

10

Informationssicherheitsmanagementsystem (ISMS) realisieren und implementieren

Verfahren und Regeln innerhalb einer Organisation, die dazu dienen, die Informationssicherheit dauerhaft zu definieren, zu steuern, zu kontrollieren, aufrechtzuerhalten und fortlaufend zu verbessern, müssen vorhanden sein. Sie bilden die Basis, um das Informationssicherheitsniveau dauerhaft zu erhalten und weiterzuentwickeln.

ACP ist qualifizierte Stelle gemäß NIS-Gesetz

ACP erfüllt als qualifizierte Stelle alle Anforderungen gemäß dem NIS-Gesetz. Unsere Experten*innen haben langjährige Erfahrung im Bereich der Information Security und begleiten Sie gerne mit einem ganzheitlichen Ansatz, der sich über technische und organisatorische Sicherheitsvorkehrungen erstreckt. So erhöhen Sie das Sicherheitsniveau Ihrer IT - auch unter Berücksichtigung der gesetzlichen Anforderungen.

Starten Sie den kostenlosen NIS 2 Readiness Check

Mit dem kostenlosen Cyber Security Rating sind Sie in der Lage, das aktuelle Sicherheitsniveau Ihrer Organisation festzustellen. Das Rating basiert auf der Beantwortung eines kurzen Fragebogens und einem optional automatisierten technischen Assessment.

Im Anschluss erhalten Sie eine Ergebnisübersicht, die Ihnen einen ganzheitlichen Überblick über Ihren Sicherheitsstatus liefert. Darauf aufbauend beraten wir Sie gerne für gezielte Maßnahmen, um das Sicherheitsniveau in Ihrem Unternehmen Schritt für Schritt zu erhöhen.

Zum Cyber Security Rating

Stellen Sie Informationssicherheit in den Fokus!

Machen Sie jetzt den ersten Schritt in Richtung NIS 2: Mit den ACP Beratungs- und Prüfleistungen steigern Sie Ihre Cybersicherheit nachhaltig.

Jetzt Kontakt aufnehmen!

acp.at/nis
security@acp.at