Checkliste

NIS2 MAßNAHMEN

Die deutsche Regierung plant, Anfang 2026 die europäische NIS2-Richtlinie in einem deutschen Gesetz zu etablieren.

Viele Firmen fragen sich, ob ihr ISMS, eine evtl. vorhandene ISO 27001-Zertifizierung oder ein ehemaliger IT-Audit ausreicht oder ob letztendlich ihre IT und Organisation dann gesetzeskonform operieren wird.

Diese Checkliste ist eine Zusammenfassung der NIS2-TOMs („NIS2 – Technische und Organisatorische Maßnahmen“) für eine kurze Eigenüberprüfung, ohne die Gesetzestexte zu lesen. Das meiste müsste dann in einem ISMS oder Mini-ISMS abgebildet und „gelebt“ werden.

NIS2 TOMS

Das Dokument „NIS2 - Technische und Methodische Voraussetzungen“ legt die technischen und organisatorischen Anforderungen fest, die nach der NIS-2-Richtlinie im Bereich Cybersicherheit und nach § 30 BSIG-E erfüllt werden müssen.

Es behandelt spezifische Anforderungen in verschiedenen Bereichen:

1. Sicherheitsrichtlinien: Die Erstellung und Pflege einer Sicherheitsrichtlinie für Netzwerk- und Informationssysteme, die mit der Geschäftsstrategie abgestimmt ist und in den klaren Verantwortlichkeiten für Cybersicherheitsmaßnahmen definiert sind.

CAIRO-Tipp: *Organisation und Stellenbeschreibungen konkretisieren,* ***ISB*** *und* ***DSM*** *benennen.*

2. Risikomanagement: Die Einführung eines Risikomanagement-Frameworks, das regelmäßige Risikoanalysen und -bewertungen umfasst, um geeignete Maßnahmen zu priorisieren und sicherzustellen, dass Sicherheitsbedrohungen effektiv behandelt werden.

CAIRO-Tipp: *Eintrittswahrscheinlichkeit x Schadenshöhe – mindestens für die kritischen Systeme im Detail zu analysieren! Das ganze Risikomanagement ist Fokus von NIS2 und muss in einem Risikomanagement-Framework als Teil des ISMS vorhanden sein. Die Umsetzung und Dokumentation von IT-Risikomanagementmaßnahmen sind eine Kernpflicht der Geschäftsführung.*

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim

3. Vorfallmanagement: Die Einrichtung einer Richtlinie zur Behandlung von Sicherheitsvorfällen, einschließlich deren Kategorisierung sowie der Überwachung, Protokollierung und Bewertung verdächtiger Aktivitäten. Sie umfasst auch Anforderungen zur Meldung von Ereignissen an die zuständigen Behörden.

CAIRO-Tipp: *Meldewege und Prozesse im Detail festlegen – am besten als Teil von Notfallplänen, aber auch für „Continuous Improvement" in Systemen zur Störungserfassung und -behebung.*

4. Krisenmanagement: Entwicklung eines Krisenmanagementplans, der die kontinuierliche Kommunikation zwischen Unternehmen und Behörden sowie eine Notfallwiederherstellungsplanung sicherstellt.

CAIRO-Tipp: *Notfallpläne mit klaren Handlungsfolgen, einschließlich Beweissicherung, müssen erarbeitet werden. Für den Fall von erfolgreichen Einbrüchen, Ransomware-Attacken oder ähnlichem sind separate Notfallwiederherstellungspläne für die kritischen Systeme nötig, mit Details zur Wiederherstellung. Nur Restore-/Recovery-Pläne decken Schwachstellen auf, wie z. B. ein nicht vorhandenes 3-2-1-Backup oder fehlende Restore-Tests!*

5. Lieferketten-Sicherheit: Einführung einer Sicherheitsrichtlinie für Lieferketten, um sicherzustellen, dass die Anbieter die Cybersicherheitsanforderungen der Organisation erfüllen und Risiken entlang der Lieferkette minimiert werden.

CAIRO-Tipp: *Das Lieferantenmanagement ist oft schon durch die DSGVO-Regelungen (2015) im Sinne von Auftragsverarbeitungsverträgen (AVV) zum Schutz personenbezogener Daten abgebildet. Auch diese AVV enthalten TOM-Listen. Es reicht aus, diese AVV/TOM-Listen, um einige sicherheitsrelevante Punkte zu ergänzen, und man kommt nicht darum herum, die Gespräche mit den Lieferanten erneut zu führen.*

Hier sollten auch gleich Standardinformationen für den Support durch Lieferanten wie SLA, Kontaktdaten usw. aktualisiert werden, um den Aufwand gering zu halten.

6. Schulung und Bewusstsein: Regelmäßige Schulungen und Sensibilisierungsprogramme für Mitarbeiter und Lieferanten, um grundlegende Cybersicherheitshygiene und die richtige Reaktion auf Sicherheitsbedrohungen zu fördern.

CAIRO-Tipp: *NIS2 fordert auch Security-Awareness-Schulungen für das Top-Management (Stellvertreter nicht erlaubt). Kein Training ohne Lernkontrolle (Phishing-Kurs ⇒ Phishing-Simulation). Alle Trainings müssen geprüft und abgezeichnet werden.*

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim

7. Verschlüsselung und Zugangskontrolle: Vorschriften zur sicheren Handhabung von Daten durch Verschlüsselungsstandards und Multi-Faktor-Authentifizierung für den Zugang zu sensiblen Netzwerken und Systemen.

CAIRO-Tipp: *Kryptographie ist ein weites und komplexes Feld und weit mehr als nur sichere Netzwerkprotokolle und VPN. So kann man z. B. E-Mails wirklich verschlüsseln, Systeme nachträglich mit MFA-Fähigkeiten ausstatten (ADFS, KeyCloak) oder mit Conditional Access die Anmeldungen noch sicherer machen.*

8. Schwachstellen- und Patch-Management: Regelmäßige Überwachung und Behandlung von Schwachstellen sowie das zeitnahe Einspielen von Sicherheitsupdates, um Sicherheitslücken zu schließen.

CAIRO-Tipp: *Dies betrifft nicht nur Client-Systeme (Laptops, Mobilgeräte), sondern auch Server-Systeme oder Netzwerke. Inwiefern man dies automatisieren kann oder sollte, ist eine subtile Entscheidung in der Praxis.*

Insgesamt gesehen verlangt die NIS2-Richtlinie, dass ein Informationssicherheits-Managementsystem **(ISMS)** eingeführt und betrieben wird.

Die Anforderung beinhaltet als Teil des ISMS (oder Mini-ISMS) den Aufbau und die Pflege eines **Risikomanagement-Frameworks**, das auf Netzwerk- und Informationssicherheitsrichtlinien basiert und durch kontinuierliche Überprüfung und Anpassung sicherstellt, dass die Cybersicherheitsmaßnahmen auch wirklich effektiv sind.

Dies ist insbesondere in Artikel 21(2), Punkt (a) der Richtlinie definiert, der die Umsetzung und Pflege eines Risikomanagementprozesses vorsieht.

Eine sehr gute Referenz ist auch das jüngst publizierte BSI-Dokument zur „NIS2-Geschäftsleitungsschulung“.

+49 (0)621 867510 info@cairo.ag www.cairo.ag Hermsheimer Straße 3 68163 Mannheim