MICHAEL WIESNER

# NIS-2 IN DER PRAXIS

## Media IT-SicherheitsForum 2024

Michael Wiesner,
Michael Wiesner GmbH

24.04.2024

Bild generiert mit ChatGPT/DALL-E

# VORSTELLUNG

## Michael Wiesner

*„Pentesting CISO doing Incident Response“*

- Informationssicherheit seit 1994
- Berater & Penetrationstester
- Externer Informationssicherheitsbeauftragter (ISB/CISO)

MICHAEL WIESNER

# VORBEMERKUNG

- Die folgenden Folien basieren auf dem aktuellen Kenntnisstand vom April 2024
- Grundlage ist die „RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES“ – kurz NIS-2-Richtlinie
- Ergänzend fließen Inhalte des Referentenentwurfs zum NIS2UmsuCG vom 22.12.2023 ein
- Unter Vorbehalt / Kein Anspruch auf Vollständigkeit!

MICHAEL WIESNER

# EINLEITUNG

# NIS-2

- Grundsätzliche Maßnahmen in Kapitel IV „Risikomanagementmaßnahmen und Berichtspflichten im Bereich der Cybersicherheit“
  - Artikel 20: Governance
  - Artikel 21: Risikomanagementmaßnahmen im Bereich der Cybersicherheit

MICHAEL WIESNER

# NIS-2

- Darüber hinaus müssen „Betreiber kritischer Anlagen“ und „Besonders wichtige Einrichtung“ zusätzliche Maßnahmen umsetzen
- Dies sind z.B.
  - Registrierungs- und Meldepflichten
  - Nachweiserbringung
  - Unterrichtungspflichten
  - Höhere Maßstäbe für KRITIS sowie besondere Maßnahmen im Bereich „Systeme zur Angriffserkennung (SzA)“
- Auf diese Punkte wird hier nicht im Detail eingegangen

# GRUNDLAGEN

# GRUNDLAGEN

(2) Die Mitgliedstaaten stellen sicher, dass die Mitglieder der Leitungsorgane wesentlicher und wichtiger Einrichtungen an Schulungen teilnehmen müssen, und fordern wesentliche und wichtige Einrichtungen auf, allen Mitarbeitern regelmäßig entsprechende Schulungen anzubieten, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken sowie Managementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Quelle: NIS-2 Artikel 20 (2)

Die in Unterabsatz 1 genannten Maßnahmen müssen unter Berücksichtigung des Stands der Technik und gegebenenfalls der einschlägigen europäischen und internationalen Normen sowie der Kosten der Umsetzung ein Sicherheitsniveau der Netz- und Informationssysteme gewährleisten, das dem bestehenden Risiko angemessen ist. Bei der Bewertung der Verhältnismäßigkeit dieser Maßnahmen sind das Ausmaß der Risikoexposition der Einrichtung, die Größe der Einrichtung und die Wahrscheinlichkeit des Eintretens von Sicherheitsvorfällen und deren Schwere, einschließlich ihrer gesellschaftlichen und wirtschaftlichen Auswirkungen, gebührend zu berücksichtigen.

Quelle: NIS-2 Artikel 21 (1)

# GRUNDLAGEN

§ 30

**Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen**

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Dabei sind das Ausmaß der Risikoexposition die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

Quelle: Referentenentwurf NIS2UmsuCG vom 23.12.2023

# GRUNDLAGEN

- Risikomanagementmaßnahmen stehen im Mittelpunkt
- Maßnahmen sollen den „*Stand der Technik*“ und ggf. „*einschlägige europäische und internationale Normen*“ einhalten
- Einrichtungen sind verpflichtet, „***Verhältnismäßige** und **wirksame** technische und organisatorische Maßnahmen zu ergreifen, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit […] zu vermeiden […]*“

MICHAEL WIESNER

# GRUNDLAGE ZUR UMSETZUNG DER NIS-2 ANFORDERUNGEN IST EIN INFORMATIONSSICHERHEITS-MANAGEMENTSYSTEM (ISMS)!




Bild generiert mit ChatGPT/DALL-E

MICHAEL WIESNER

# EXKURS: ISMS

- Leitdokumente und Richtlinien
- ISMS-Prozesse (Anforderungsmanagement, Risikomanagement, Verbesserungsmanagement, Maßnahmenmanagement)
- Maßnahmen (technische, personalbezogene, physische, organisatorische)

MICHAEL WIESNER

# EXKURS: ISMS

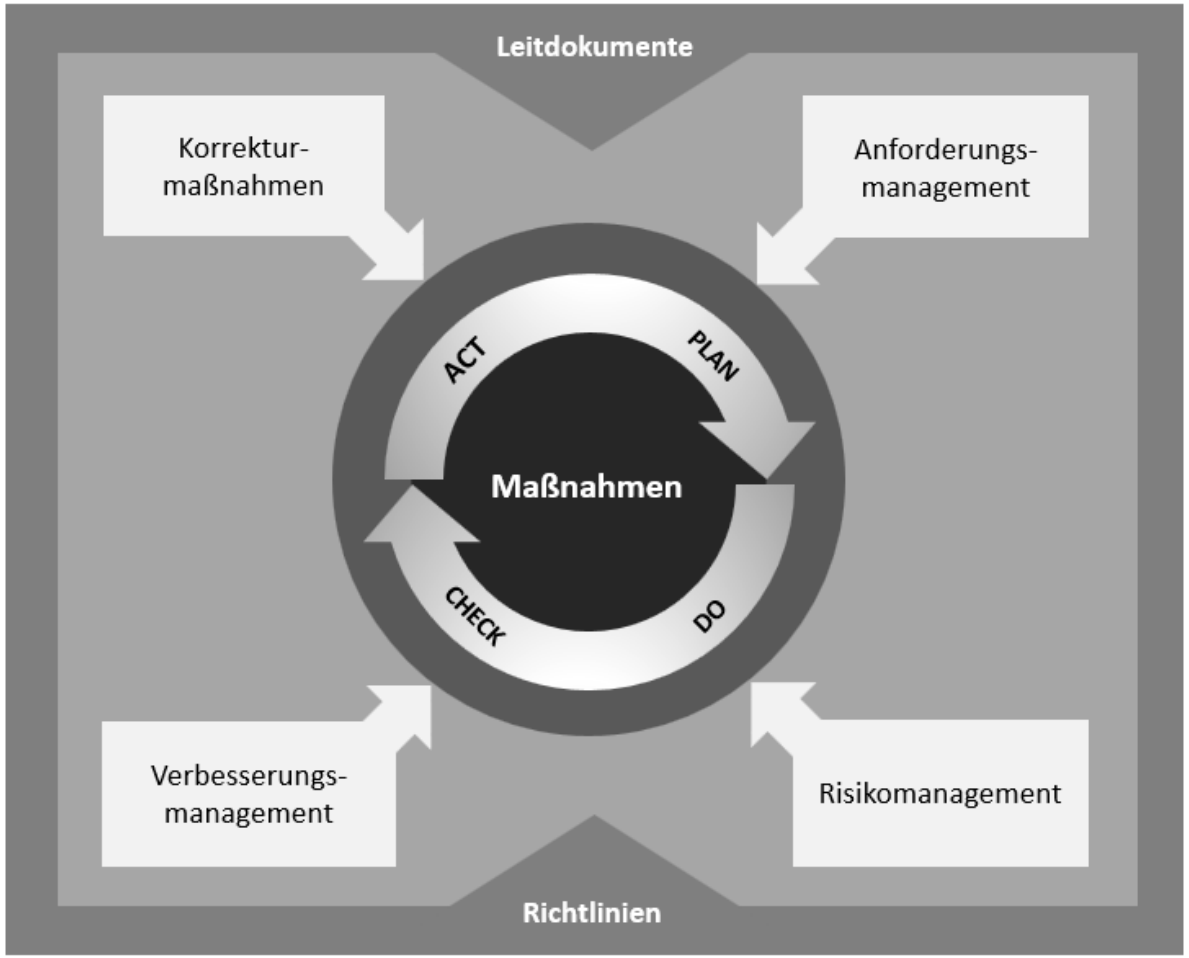


Abb.: Informationssicherheitsprozess

MICHAEL WIESNER

# EXKURS: ISMS

- Anerkannte Normen:
  - ISO 27001 sowie Ergänzungen
  - BSI IT-Grundschutz / C5
  - Für KMU: VdS 10000 (NIS-2 Ergänzung in Arbeit)
  - B3S (KRITIS Branchenstandards)
  - IEC 62443 (OT)

MICHAEL WIESNER

# UMSETZUNG NIS-2 MAßNAHMEN

MICHAEL WIESNER

# UMSETZUNG NIS-2 MAßNAHMEN

1. ISMS implementieren (Auswahl einer geeigneten Norm – Angemessenheit beachten!)
2. Abgleich mit den konkreten NIS-2 Anforderungen (insbesondere Artikel 20/21 bzw. NIS2UmsuCG)
3. Umsetzung ggf. zusätzlicher Maßnahmen

MICHAEL WIESNER

# UMSETZUNG NIS-2 MAßNAHMEN

a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;

b) Bewältigung von Sicherheitsvorfällen;

c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;

d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;

e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;

f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;

g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;

h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;

i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;

j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

Quelle: NIS-2 Artikel 21 (2)

MICHAEL WIESNER

# UMSETZUNG NIS-2 MAßNAHMEN MIT ISO 27001:2022

MICHAEL WIESNER

# UMSETZUNG NIS-2 MAßNAHMEN MIT ISO 27001:2022

- Die Maßnahmen der ISO 27001/27002 erfüllen die Anforderungen der NIS-2 (Artikel 20/21)
- ACHTUNG: Zertifizierung nach ISO 27001 bedeutet nicht zwingend Erfüllung der NIS-2 Richtlinie/NIS2UmsuCG
  - Der Anwendungsbereich des ISMS muss das gesamte Unternehmen umfassen
  - Risikoanalyse muss All-Gefahren-Ansatz und gesellschaftliche Auswirkungen berücksichtigen (§ 30 RefE NIS2UmsuCG)
  - Maßnahmen müssen umgesetzt und nicht „nur“ geplant sein
  - Ggf. kann die Umsetzung weiterer Maßnahmen (Stand der Technik, z.B. BSI IT-Grundschutz) notwendig werden

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**Artikel 21: Risikomanagementmaßnahmen im Bereich der Cybersicherheit**

**a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme**

- 6.1 Maßnahmen zum Umgang mit Risiken und Chancen
- 8.2 Informationssicherheitsrisikobeurteilung
- 8.3 Informationssicherheitsrisikobehandlung
- A.5.1 Informationssicherheitsrichtlinien

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**b) Bewältigung von Sicherheitsvorfällen**

- A.5.5 Kontakt mit Behörden
- A.5.6 Kontakt mit speziellen Interessensgruppen
- A.5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- A.5.25 Beurteilung und Entscheidung über Informationssicherheitsereignisse
- A.5.26 Reaktion auf Informationssicherheitsvorfälle
- A.5.27 Erkenntnisse aus Informationssicherheitsvorfällen
- A.5.28 Sammeln von Beweismaterial
- A.6.8 Meldung von Informationssicherheitsereignissen
- A.8.16 Überwachung von Aktivitäten

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement**

- A.5.29 Informationssicherheit bei Störungen
- A.5.30 IKT-Bereitschaft für Business Continuity
- A.8.13 Sicherung von Information
- A.8.14 Redundanz von informationsverarbeitenden Einrichtungen
- A.8.15 Protokollierung
- A.8.16 Überwachung von Aktivitäten

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern**

- A.5.19 Informationssicherheit in Lieferantenbeziehungen
- A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
- A.5.21 Umgang mit der Informationssicherheit in der IKT-Lieferkette
- A.5.22 Überwachung, Überprüfung und Änderungsmanagement von Lieferantendienstleistungen
- A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen**

- A.5.20 Behandlung von Informationssicherheit in Lieferantenvereinbarungen
- A.5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- A.5.37 Dokumentierte Betriebsabläufe
- A.6.8 Meldung von Informationssicherheitsereignissen
- A.8.8 Handhabung von technischen Schwachstellen
- A.8.9 Konfigurationsmanagement
- A.8.20 Netzwerksicherheit
- A.8.21 Sicherheit von Netzwerkdiensten

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit**

- 9 Bewertung der Leistung
- A.5.35 Unabhängige Überprüfung der Informationssicherheit
- A.5.36 Einhaltung von Richtlinien, Vorschriften und Normen für die Informationssicherheit

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit**

- 7.3 Bewusstsein
- 7.4 Kommunikation
- A.5.15 Zugangssteuerung
- A.5.16 Identitätsmanagement
- A.5.18 Zugangsrechte
- A.5.24 Planung und Vorbereitung der Handhabung von Informationssicherheitsvorfällen
- A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

- A.6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung
- A.6.8 Meldung von Informationssicherheitsereignissen
- A.8.2 Privilegierte Zugangsrechte
- A.8.3 Informationszugangsbeschränkung
- A.8.5 Sichere Authentifizierung
- A.8.7 Schutz gegen Schadsoftware
- A.8.9 Konfigurationsmanagement
- A.8.13 Sicherung von Information
- A.8.15 Protokollierung
- A.8.19 Installation von Software auf Systemen im Betrieb
- A.8.22 Trennung von Netzwerken

# ZUORDNUNG NIS-2/ISO 27001:2022

**h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung**

- A.8.24 Verwendung von Kryptographie

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen**

- A.5.9 Inventar der Informationen und anderen damit verbundenen Werten
- A.5.10 Zulässiger Gebrauch von Informationen und anderen damit verbundenen Werten
- A.5.11 Rückgabe von Werten
- A.5.15 Zugangssteuerung
- A.6.16 Identitätsmanagement
- A.5.17 Informationen zur Authentifizierung

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

- A.5.18 Zugangsrechte
- A.6.1 Sicherheitsüberprüfung
- A.6.2 Beschäftigungs- und Vertragsbedingungen
- A.6.4 Maßregelungsprozess
- A.6.5 Verantwortlichkeiten bei Beendigung oder Änderung der Beschäftigung
- A.6.6 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

MICHAEL WIESNER

# ZUORDNUNG NIS-2/ISO 27001:2022

**j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.**

- A.5.14 Informationsübertragung
- A.5.16 Identitätsmanagement
- A.5.17 Informationen zur Authentifizierung

MICHAEL WIESNER

# WAS KOMMT NOCH?

- CRA
  https://en.wikipedia.org/wiki/Cyber_Resilience_Act
- DORA
  https://de.wikipedia.org/wiki/Verordnung_(EU)_2022/2554_(DORA)
- KRITIS-Dachgesetz
  https://www.openkritis.de/it-sicherheitsgesetz/kritis-dachgesetz-sicherheitsgesetz-3-0.html

MICHAEL WIESNER

# REFERENZEN

- NIS-2 Richtlinie: https://digital-strategy.ec.europa.eu/de/policies/nis2-directive
- Diskussionspapier zum NIS2UmsuCG: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/referentenentwuerfe/CI1/NIS-2-UmsetzungWirtschaft_DisP.html
- ISO 27001:2022: https://www.beuth.de/de/norm/iso-iec-27001/360980333
- ISO 27002:2022: https://www.beuth.de/de/norm/iso-iec-27002/352094880
- Zuordnungstabelle NIS-2 – ISO 27001:2022: https://wiesner.eu/2024/02/28/nis-2-und-iso-27001-27002/

MICHAEL WIESNER

# KONTAKT

Michael Wiesner GmbH

Am Flachsacker 4

35708 Haiger

T: +49 2773 8132623 0

M: mail@wiesner.eu

W: https://wiesner.eu