axians

HERZLICH WILLKOMMEN!

CARRIER INNOVATION DAY 2024

SIMPLIFY. INNOVATE. TRANSFORM.

VINCI ENERGIES

axians

CYBER CURRICULUM

Cyber Security – NIS 2 Ein Segen oder das notwendige Übel?

Niclas Matz, Cyber Curriculum
Founder & CEO

VINCI ENERGIES

CYBER CURRICULUM®

NIS2-Richtlinie

Europaweiter Sicherheitsstandard:
„Segen oder notwendiges Übel?“

cyber-curriculum.com

Ihr heutiger Referent

Niclas Matz
CEO
Cyber Curriculum

Adresse
Alt-Moabit 73a, 10555 Berlin

Telefonnummer
+49 30-577-0068-30

E-Mail Adresse
niclas.matz@cyber-curriculum.com

Dienstleistungen

- 24/7 SOC (Security Operations Center)
- Incident Response & Business Continuity
- Datenschutz & GRC (Governance, Risk, Compliance)
- Schulung & Prozessberatung
- Cloud Security, IAM, SDLC
- Branchenspezifische Beratung – auf Ihre Bedürfnisse zugeschnitten

CYBER CURRICULUM

„NIS 2 – Segen oder notwendiges Übel?“

Volkswirtschaft Cybercrime

Wirtschaftlicher Schaden durch Cybercrime im Vergleich mit den vier größten Volkswirtschaften der Welt

1.	USA	27,7 Bio. USD
2.	China	17,7 Bio. USD
3.	***Cybercrime***	***8,0 Bio. USD****
4.	Deutschland	4,5 Bio. USD
5.	Japan	4,2 Bio. USD

* Quelle: World Economic Forum: https://www.weforum.org/stories/2023/01/global-rules-crack-down-cybercrime/

CYBER CURRICULUM

NIS 2:

Ausgangssituation und Zielsetzung der NIS2-Richtlinie

Ausgangssituation

- **Cyberangriffe** erfolgen häufig und automatisiert, **über Lieferketten, Dienstleister und Zulieferer**.
- **Sicherheitslücken durch Flickenteppich:** Europaweit uneinheitliche Standards öffnen Cyberattacken Tür und Tor
- **EU verschärft Cyberschutz:** Unternehmen müssen wirksame Cybersecurity-Maßnahmen nachweisen.

Zielsetzung

- ✓ **Hohes Cybersicherheitsniveau im europäischen Binnenraum.**
- ✓ Umsetzung eines **europaweiten Security-Standards** und Erhalt der Wettbewerbsfähigkeit des Wirtschaft Standortes
- ✓ **Schutz der Bevölkerung**

CYBER CURRICULUM

NIS 2:

Historische Einordnung des IT- SiG 2.0 und NIS 2 und die Bedeutung für die IT-Sicherheitslandschaft

2015	2017	2021	2023	2024
IT-SiG Inkrafttreten nationales IT-Sicherheitsgesetzes (IT-SiG 1.0)	**NIS-Richtlinie** Inkrafttreten der europäischen Richtlinie	**IT-SiG 2.0** Inkrafttreten nationales IT-Sicherheitsgesetz (IT-SiG 2.0) **Stellt deutsche KRITIS-Regulierung dar.**	**NIS2-Richtlinie** Inkrafttreten der europäischen Richtlinie **Die NIS2-Richtlinie erweitert den Regulierungskreis.**	**NIS2UmsuCG** Referentenentwurf NIS2-Umsetzungsgesetz

CYBER CURRICULUM

NIS 2:

Betroffenen Sektoren und Selektoren zur Einstufung der Regulierung

Sektoren

Energie	Öffentliche Verwaltung
Banking	Post- und Kurierdienste
Gesundheit	Chemieproduktion
Abwasser	Forschungseinrichtungen
ITK-Service-Management	Abfallentsorgung
Weltraum	Lebensmittel
Verkehr	Digitale Dienste
Finanzmärkte	Trinkwasser
Digitale Infrastruktur	

Selektoren

Anzahl Mitarbeitende:	Jahresumsatz oder Jahresbilanzsumme:
≥ 50	> 10 Mio. EUR oder > 10 Mio. EUR
≥ 250	> 50 Mio. EUR oder > 43 Mio. EUR

KRITIS
(Teilmenge von bwE)

bwE
(Besonders wichtige Einrichtung)

wE
(Wichtige Einrichtung)

Nicht betroffen

CYBER CURRICULUM

NIS 2:

NIS2-Umsetzungsgesetz – Referentenentwurf (BSIG-E)

- Statt eines IT-SiG 3.0 wird in Deutschland ein NIS2-Umsetzungsgesetz erarbeitet. Da
- Ziel NIS2-Umsetzungsgesetz : Überführung der EU-Richtlinie NIS2 in deutsches Recht.
- Das NIS2UmsuCG wird als Mantelgesetz bestehende Gesetze wie das BSI-Gesetz, das IT-SiG2.0, das Energiewirtschaftsgesetz und viele andere verändern.
- Alle Mitgliedstaaten sollten die NIS2-Richtlinie bis zum 17. Oktober 2024 in nationales Recht umsetzen.
- Deutschland hat diese Frist nicht eingehalten und plant die Umsetzung, das NIS2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG), bis März 2025.

NIS 2:

Referentenentwurf (BSIG-E) – Lieferketten-Sicherheit – § 30.2.4

NIS 2 und KRITIS-Dachgesetz fokussiert Themen wie die Lieferketten-Sicherheit . Dies umfasst den Schutz der Supply Chain – also das Vorhandensein und die Resilienz der eigenen Zulieferer und Dienstleister.

Supply Chain Security:

- Vorgaben zum Schutzniveau bei Providern
- Resilienz der Lieferkette sollte zusammen mit dem ISMS erarbeitet werden
- Diversifizierung von Lieferketten
- Dienstleister und Serviceprovider sollten so ausgewählt werden, dass es keinen SPOF (*Single Point of Failure*) gibt.

Analyse der Resilienz:

- Die Abhängigkeit von Lieferanten und Dienstleistern sollte strategisch erfasst und im Rahmen des BCMs analysiert werden.

Nachweispflicht:

- Einhaltung der Vorgaben muss durch Zulieferer und Dienstleister nachgewiesen werden.

NIS 2:

NIS2UmsuCG – *Kritik am Referentenentwurf (BSIG-E)*

- Gesetzentwurf zur NIS-2-Umsetzung:
  Der aktuelle Entwurf enthält viele Schwächen und Unklarheiten.
  Risiko: Keine klare Vereinheitlichung des Cybersicherheitsrechts.

- Begriffliche Unschärfen:
  Unbestimmte Begriffe wie „erhebliche Cyberbedrohung“, „immaterieller Schaden“, „Sicherheitsvorfall“ und „Erheblichkeit“.
  Risiko: Rechtsunsicherheiten bei Betroffenen.

- Betroffenheit:
  Wissenslücke bei KMUs und Zulieferern, die bisher keine Informationssicherheitsmaßnahmen ergreifen mussten.
  Risiko: Unsicherheiten bezüglich Betroffenheit vom Gesetz und Weg zur Umsetzung.

- Meldepflichten:
  Unsicherheit wie das Meldeverfahren in der Praxis umgesetzt wird.
  Risiko: Zusätzliche Belastungen für Unternehmen bei hoch-bürokratischem Meldeverfahren.

[1] https://www.bundestag.de/resource/blob/1027334/3e421efc0ba6e141725e9f9f18a5b318/20-4-528
[2] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/CI1/NIS-2-umsetzungs-cybersicherheit/NIS2UmsuCG070524_Bitkom_pdf.pdf?__blob=publicationFile&v=2.df

NIS 2:

NIS2UmsuCG – *Kritik am Referentenentwurf (BSIG-E)*

- Nachweispflicht für Betreiber kritischer Anlagen:
  Hohe Nachweispflichten für Betreiber kritischer Anlagen, die teilweise redundant erscheinen.
  Risiko: Höhere interne Aufwände = höhere wirtschaftliche Aufwände für Unternehmen .

- Systeme zur Angriffserkennung (SzA):
  Unklarheit ob Zwang zum Einsatz von SzA auch für (besonders) wichtige Einrichtungen gilt.
  Risiko: Unsicherheiten auf Seiten der Unternehmen.

- Lieferkettenmanagement:
  Risikobasierte Anforderungen an die Lieferkette können erhebliche Aufwände verursachen.
  Risiko: Benachteiligung kleiner Zulieferer und Dienstleister.

- Unklarheiten für Geschäftsführung:
  Fehlende Vorgaben für Schulungs- oder Handlungsnachweise bei hohen Anforderungen.
  Risiko: Unsicherheiten bei Geschäftsführer*innen.

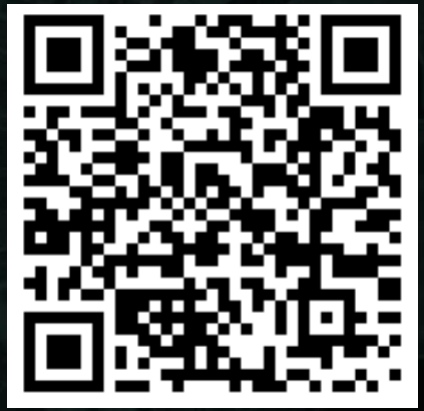
[1] https://www.bundestag.de/resource/blob/1027334/3e421efc0ba6e141725e9f9f18a5b318/20-4-528
[2] https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/stellungnahmen/CI1/NIS-2-umsetzungs-cybersicherheit/NIS2UmsuCG070524_Bitkom_pdf.pdf?__blob=publicationFile&v=2.df

NIS 2:

Fazit: „Segen oder notwendiges Übel?“

- NIS 2 stärkt europäische Lieferketten und sichert die Wettbewerbsfähigkeit von Unternehmen im europäischen Binnenraum.
- Die NIS 2 erhöht das Sicherheitsniveau ganzheitlich, indem auch die Lieferkette verpflichtet wird Maßnahmen nachzuweisen.
- NIS2UmsuCG in der praktischen Umsetzung eine Katastrophe.
- BSI keine unabhängige Behörde (BMI) und mit der Auditierung überfordert.

Befragen Sie unseren AI-Chatbot zu Ihren NIS2-Fragen.



CYBER CURRICULUM