German OWASP Day 2024

NIS2 entmystifiziert - Was Unternehmen nun tun müssen

Tim Philipp Schäfers, NIS2-Navigator

German OWASP Day 2024

01

Worüber reden wir?

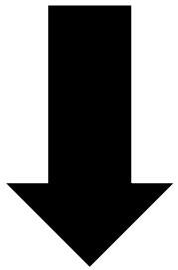
NIS-2-Richtlinie

Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein **hohes gemeinsames Cybersicherheitsniveau** in der Union (27.12.2022 veröffentlicht)

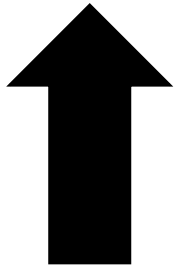
NIS2-Umsetzungsgesetz (NIS2UmsuCG)

NIS-2-Umsetzungs- und **Cybersicherheitsstärkungsgesetz**

Verordnung vs. Richtlinie



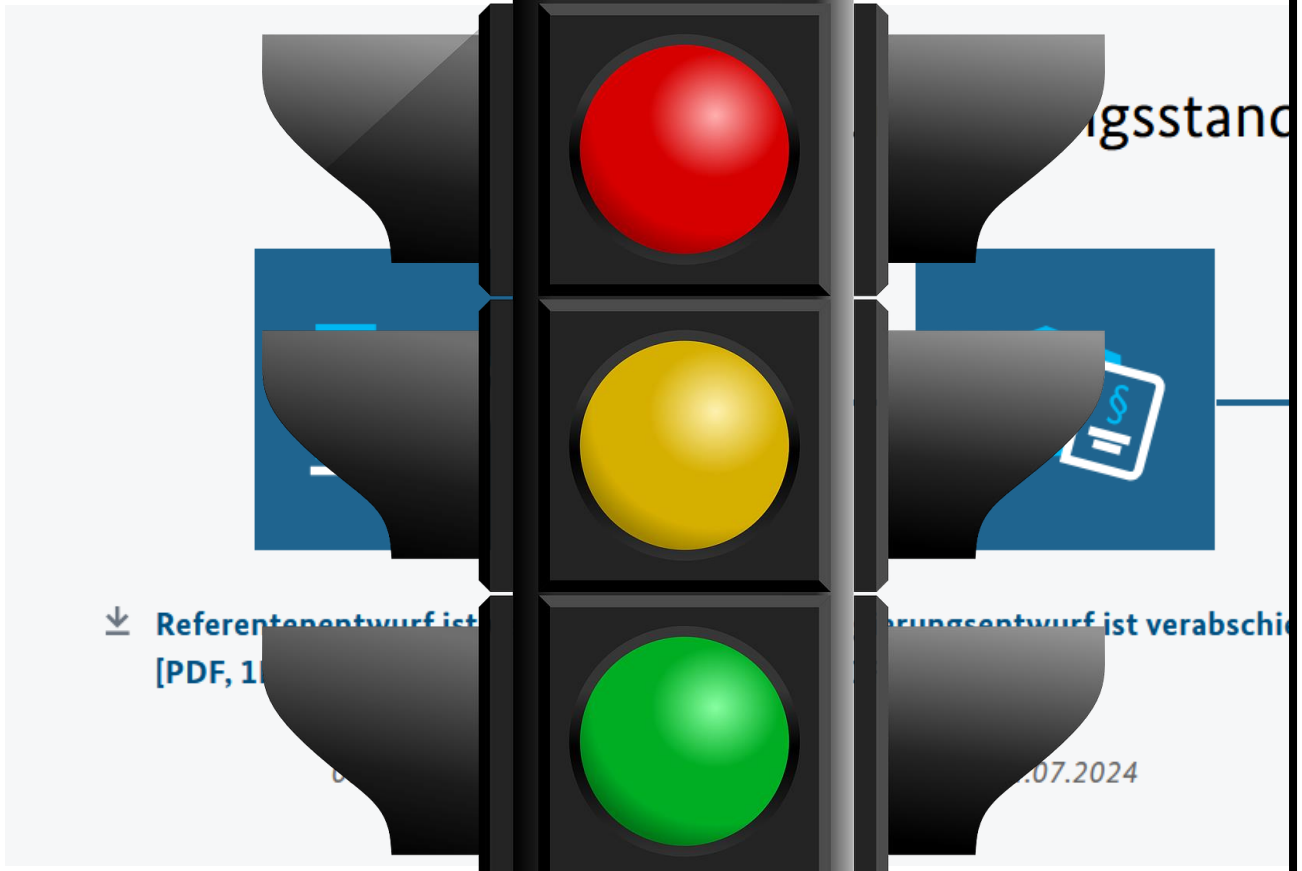
Merkmal	Verordnung (Regulation)	Richtlinie (Directive)
Beispiel	Datenschutzgrundverordnung (DSGVO)	NIS-2-Richtlinie
Geltung	Unmittelbar in allen Mitgliedstaaten	Umsetzung in nationales Recht erforderlich
Zielsetzung	Vollständige Harmonisierung	Zielvorgabe, die in nationales Recht umgesetzt wird



Status NIS2UmsuCG in DE

Entnommen von: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html

Status NIS2UmsuCG in DE



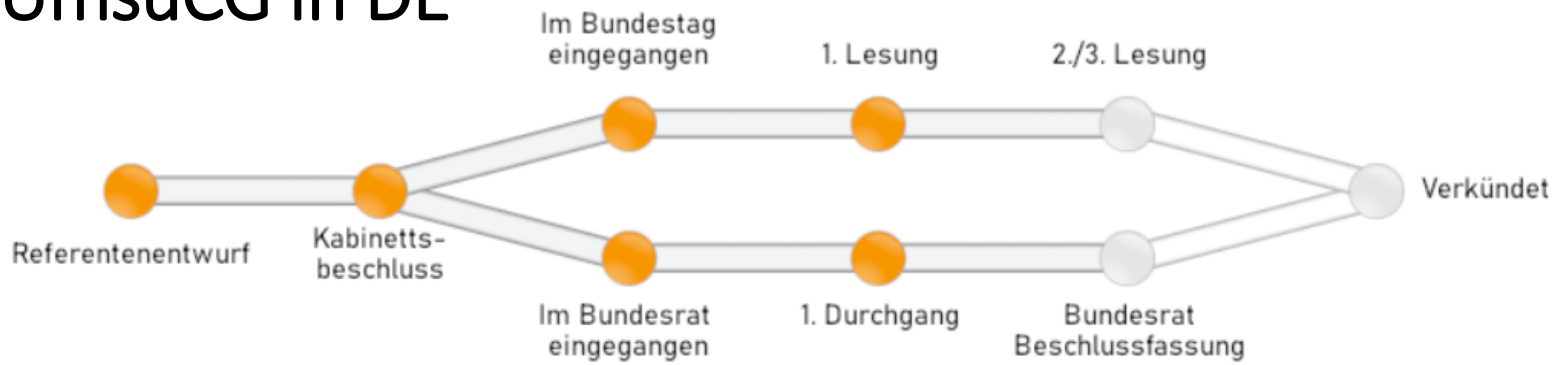
NIS2UmsuCG

1 von 113 Gesetzesvorhaben

Hätte bis 17.10.2024 beschlossen sein müssen (EU-Recht)

Entnommen von: https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html

Status NIS2UmsuCG in DE



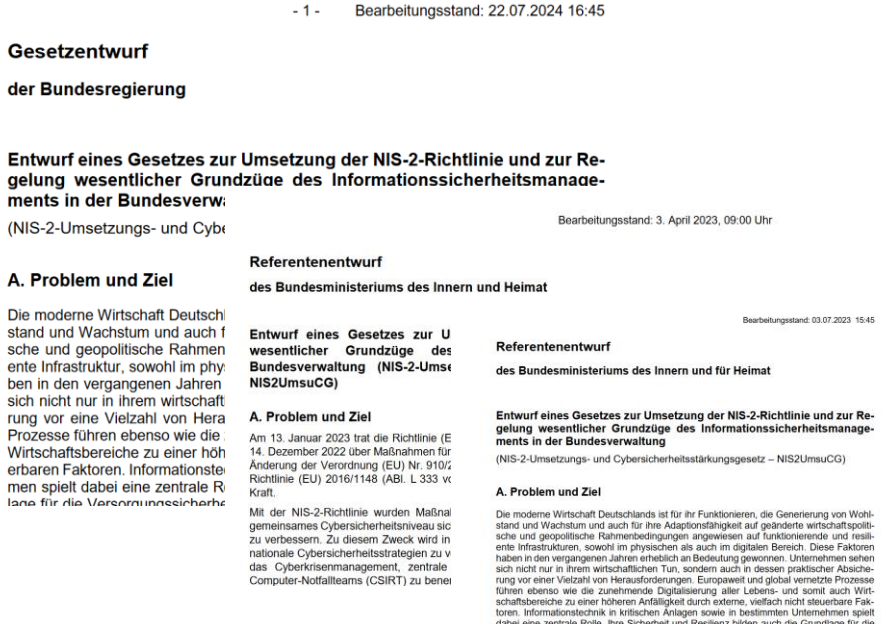
Basics

Offizieller Titel:	Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz)
Initiator:	Bundesministerium für Inneres und Heimat
Status:	In der Ausschussberatung
Letzte Änderung:	10.10.2024
Drucksache:	20/13184 (PDF-Download)
Gesetztyp:	Einspruchsgesetz

Entnommen von: Bundestagszusammenfasser.de / https://bundestagszusammenfasser.de/details?docid=71

Status NIS2UmsuCG in DE

Regierungsentwurf, Bearbeitungsstand 22.07.2024
offizieller Entwurf (BMI) 07.05.2024
Diskussionspapier, Bearbeitungsstand 27.09.2023
Referentenentwurf, Bearbeitungsstand 03.07.2023
Referentenentwurf, Bearbeitungsstand 03.04.2023



- 1 - Bearbeitungsstand: 22.07.2024 16:45

Gesetzentwurf

der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwa

(NIS-2-Umsetzungs- und Cybe

A. Problem und Ziel

Die moderne Wirtschaft Deutschl
stand und Wachstum und auch f
sche und geopolitische Rahmen
ente Infrastruktur, sowohl im phy
ben in den vergangenen Jahren
sich nicht nur in ihrem wirtschaft
rung vor eine Vielzahl von Hera
Prozesse führen ebenso wie die
Wirtschaftsbereiche zu einer höh
erbaren Faktoren. Informationste
men spielt dabei eine zentrale R
lage für die Versorgungssicherhe

Bearbeitungsstand: 3. April 2023, 09:00 Uhr

Referentenentwurf

des Bundesministeriums des Innern und Heimat

**Entwurf eines Gesetzes zur U
wesentlicher Grundzüge des
Bundesverwaltung (NIS-2-Umse
NIS2UmsuCG)**

A. Problem und Ziel

Am 13. Januar 2023 trat die Richtlinie (E
14. Dezember 2022 über Maßnahmen für
Änderung der Verordnung (EU) Nr. 910/
Richtlinie (EU) 2016/1148 (ABl. L 333 v
Kraft.

Mit der NIS-2-Richtlinie wurden Maßnal
gemeinsames Cybersicherheitsniveau sic
zu verbessern. Zu diesem Zweck wird in
nationale Cybersicherheitsstrategien zu v
das Cyberkrisenmanagement, zentrale
Computer-Notfallteams (CSIRT) zu benei

Bearbeitungsstand: 03.07.2023 15:45

Referentenentwurf

des Bundesministeriums des Innern und für Heimat

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

(NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG)

A. Problem und Ziel

Die moderne Wirtschaft Deutschlands ist für ihr Funktionieren, die Generierung von Wohlstand und Wachstum und auch für ihre Adaptionsfähigkeit auf geänderte wirtschaftspolitische und geopolitische Rahmenbedingungen angewiesen auf funktionierende und resiliente Infrastrukturen, sowohl im physischen als auch im digitalen Bereich. Diese Faktoren haben in den vergangenen Jahren erheblich an Bedeutung gewonnen. Unternehmen sehen sich nicht nur in ihrem wirtschaftlichen Tun, sondern auch in dessen praktischer Absicherung vor einer Vielzahl von Herausforderungen. Europaweit und global vernetzte Prozesse führen ebenso wie die zunehmende Digitalisierung aller Lebens- und somit auch Wirtschaftsbereiche zu einer höheren Anfälligkeit durch externe, vielfach nicht steuerbare Faktoren. Informationstechnik in kritischen Anlagen sowie in bestimmten Unternehmen spielt

Abgeordnete Parlament Ausschüsse Internationales Dokumente

Anhörung zum NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Zeit: Montag, 4. November 2024, 11 Uhr
Ort: Berlin, Paul-Löbe-Haus, Sitzungssaal E 800

Quellen: https://nis2-navigator.de/aktueller-stand-nis2/ / https://www.bundestag.de/ausschuesse/a04_inneres/anhoerungen/1026172-1026172

German OWASP Day 2024

02

Was heißt das alles konkret?

NIS2 auf einen Blick

- Weitreichende Anforderungen im Bereich Informationssicherheit
- ca. 30.000 betroffene Unternehmen in Deutschland + Lieferkette
- Zahlreiche Anforderungen und Pflichten für Organisationen
- Empfindliche Strafen bei Verstößen
- Befugniserweiterung für Behörden

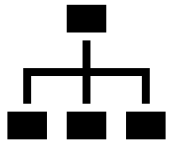
Betroffenheit nach NIS2 (Sektoren)


Energie


Transport & Verkehr

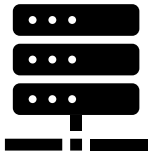

Finanzmarkt


Gesundheits-wesen


Öffentliche Verwaltung

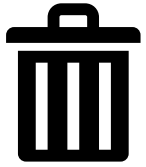

Weltraum

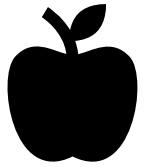

Wasser & Abwasser


Digitale Infrastruktur

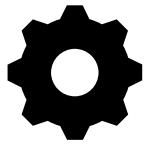

Post & Kurierdienste


Chemie


Abfallbewirt-schaftung


Ernährung / Lebensmittel


Forschung


Verarbeitendes Gewerbe


Verwalten von IKT-Diensten

Besonders wichtige Einrichtungen

>250 Mitarbeitende ODER
>50 Mio € Umsatz und Bilanz >43 Mio. €

Wichtige Einrichtungen

>50 Mitarbeitende ODER
>10 Mio € Umsatz und Bilanz >10 Mio.

KRITIS Betreiber

KRITIS Sektor + Schwellwerte (>500.000 versorgte Personen) erzielt

Bundeseinrichtung

Bundesbehörde oder IT-Dienstleister v. d. (einige Ausnahmen vorhanden)

Betroffenheit nach NIS2 - Betroffenheitschecks

Bundesamt
für Sicherheit in der
Informationstechnik

Ist das Unternehmen Betreiber einer kritischen Anlage?

Gemäß § 2 Absatz 10 BSIG sind Kritische Infrastrukturen im Sinne dieses Gesetzes Einrichtungen, Anlagen oder Teile davon, die den Sektoren

- Energie
- Informationstechnik und Telekommunikation
- Transport und Verkehr
- Gesundheit
- Wasser
- Ernährung
- Finanz- und Versicherungswesen
- Siedlungsabfallentsorgung

angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebl
Gefährdungen für die öffentliche Sicherheit eintreten würden.

Die Kritischen Infrastrukturen im Sinne dieses Gesetzes werden durch die Rechtsverordnung nach § 10 Absatz 1 BSIG (BSI-Kritisverordnung) näh

1 → Ist Ihr Unternehmen in einem oder mehreren der folgenden Sektoren tätig? (Sektorauswahl 1/2)

Mehr Infos zu den Sektoren: https://simplisec.de/nis2-sektoren/

Wählen Sie ein oder Mehrere

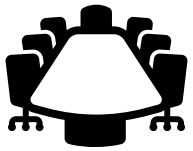
https://betroffenheitspruefung-nis-2.bsi.de/ & https://nis2-navigator.de/nis2-betroffenheitsanalyse/

Wichtige Pflichten nach NIS2

Registrierungspflicht (§§ 33, 34)

Pflicht zum Risikomanagement (§ 30)

Nachweispflicht (§ 39)



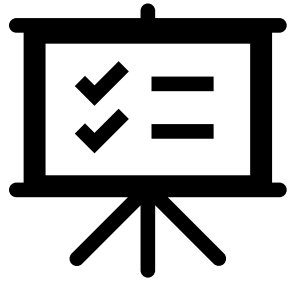
Pflicht zur Einbindung der Geschäftsführung (§ 38)

Meldepflicht (§ 32)

Einhaltung: „Stand der Technik“ (§ 30)

Einhaltung: „Stand der Technik“ (§ 30)

„branchenübliche und angemessene Schutzmaßnahmen“ (ISMS)

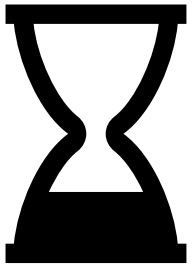


Mindestens (aus § 30):

1. Konzepte in Bezug auf die **Risikoanalyse** und auf die Sicherheit in der Informationstechnik,
2. **Bewältigung von Sicherheitsvorfällen**,
3. Aufrechterhaltung des Betriebs, wie **Backup-Management** und Wiederherstellung nach einem **Notfall**, und **Krisenmanagement**,
4. **Sicherheit der Lieferkette** einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern,
5. **Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen**, einschließlich **Management und Offenlegung von Schwachstellen**,
6. Konzepte und Verfahren zur **Bewertung der Wirksamkeit von Risikomanagementmaßnahmen** im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Verfahren im Bereich der **Cyberhygiene und Schulungen** im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Verfahren für den Einsatz von **Kryptografie und Verschlüsselung**,
9. Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle** und für das Management von Anlagen,
10. Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung** oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls **gesicherte Notfallkommunikationssysteme** innerhalb der Einrichtung.

Meldepflicht (§ 32)

Bei einem „erheblichen Sicherheitsvorfall“:



- Erstinformation innerhalb von 24 Stunden nach Kenntnisnahme
- Nach 72 Stunden Statusbericht (Aktualisierung der Erstmeldung)
- ggfs. weitere Zwischenmeldungen (auf Anfrage des BSI, etc.)
- Nach 1 Monat umfassender Bericht (inkl. Schweregrad, Auswirkungen, Art der Bedrohung, Ursache, Abhilfemaßnahmen, etc.)

BSI und Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BKK) als zentrale Meldestelle

Strafen nach NIS2

	Von	Bis
KRITIS-Betreiber	100.000 €	10 Mio € oder 2% Umsatz
Besonders wichtige Einrichtungen		
Wichtige Einrichtungen	100.000 €	7 Mio € oder 1.4% Umsatz
Allgemeine Tatbestände	100.000 €	2 Mio €

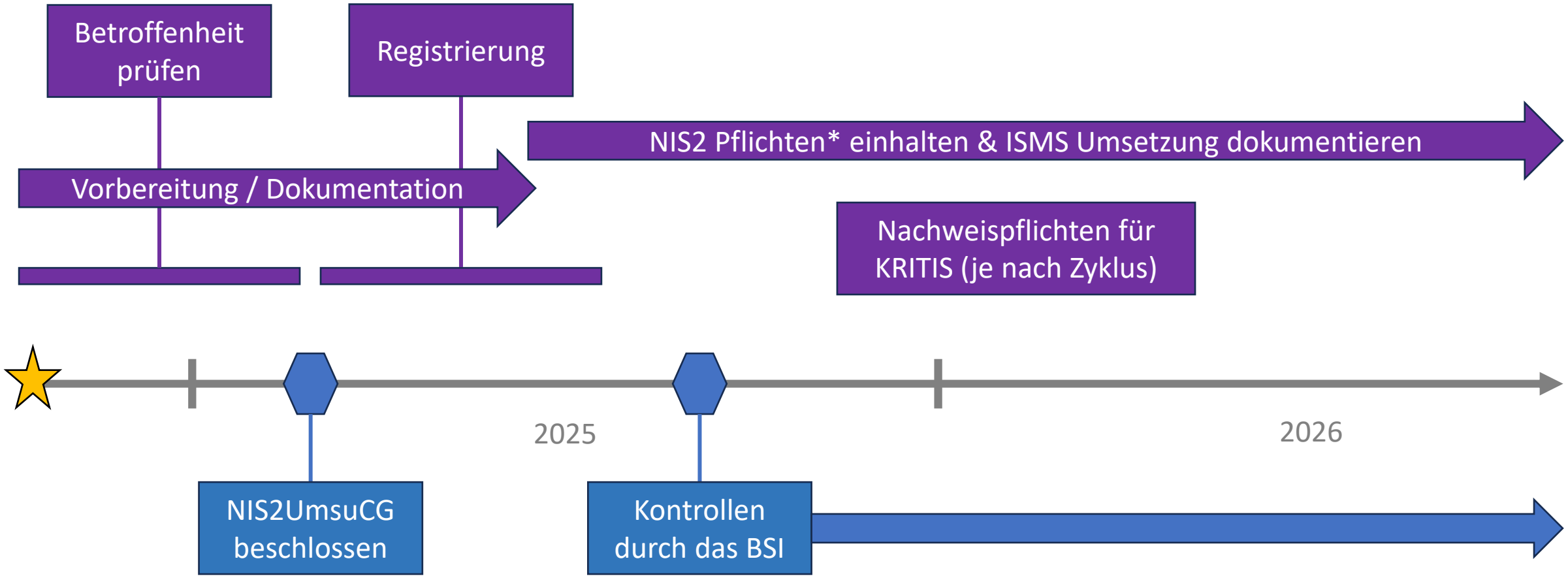
German OWASP Day 2024

03

Was ist zu tun?

Timeline

*Beinhaltet insbesondere: Risikomanagement, Registrierung, Vorfallsmeldung, Nachweise, Informationspflicht, Governance, Stand der Technik, etc.



Quellen / weitere Informationen

OpenKRITIS	https://openkritis.de
NIS2-Navigator	https://nis2-navigator.de/
BSI NIS2	https://www.bsi.bund.de/dok/nis-2
BMI	https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html
ENISA	https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/network-and-information-systems-directive-2-nis2

Vielen Dank!

Tim Philipp Schäfers

tim@nis2-navigator.de

https://nis2-navigator.de