



Bundesministerium
des Innern
und für Heimat

Referentenentwurf für ein NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz

Anhörung von Fachkreisen und Verbänden

Berlin, 3. Juni 2024, 13:30-16:30 Uhr

Einleitung und Überblick

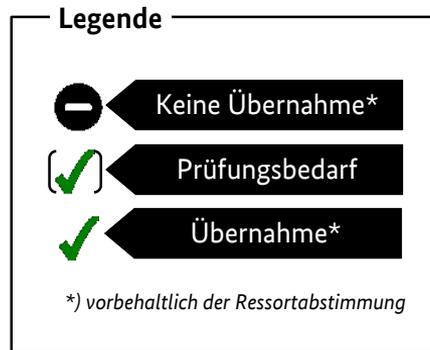
1. Wesentliche Themen der schriftlichen Stellungnahmen
2. Gelegenheit für mündliche Stellungnahmen
3. Nächste Schritte

Angehörte Fachkreise und Verbände

– 62 eingegangene schriftliche Stellungnahmen

HDE e.V.	ISC2	BÖB e.V.	bvse e.V.	BREKO e.V.	Fachverband Biogas e.V.	BVE	UP KRITIS
BWE	ZDH e.V.	GKV	BAH e.V.	UNITI e.V.	VDV	bevh	ZVEI e.V.
eco	DGUV e.V.	MPA	DIHK	Deutscher Städtetag	DRV	DWA	DVGW e.V.
Bundesbank	AG KRITIS	GdP	BEE e.V.	VCI e.V.	DSLTV	dbwv	BVMI e.V.
BUGLAS	DKG e.V.	DVF e.V.	FamPol	TeleTrusT e.V.	GI	BVMW	BDEW e.V.
ABDA	COA	VDMA e.V.	BDI e.V.	VKU e.V.	bwf	BDL	VGMS
bitkom	VATM e.V.	UTV e.V.	bne	BPEX	ASW	TÜV-V	VDA e.V.
DEKRA	DAV	VDR	GDV	ALM e.V.	KZBV		

Wesentliche Themen der schriftlichen Stellungnahmen



Rechtliche Rahmenbedingungen für den Referentenentwurf

- 1:1 Umsetzung der NIS-2-Richtlinie im Bereich Wirtschaft 
- Unterschreitung der Vorgaben der NIS-2-Richtlinie 
- Einbeziehung von Ländern oder Kommunen in den Anwendungsbereich 

Allgemeines

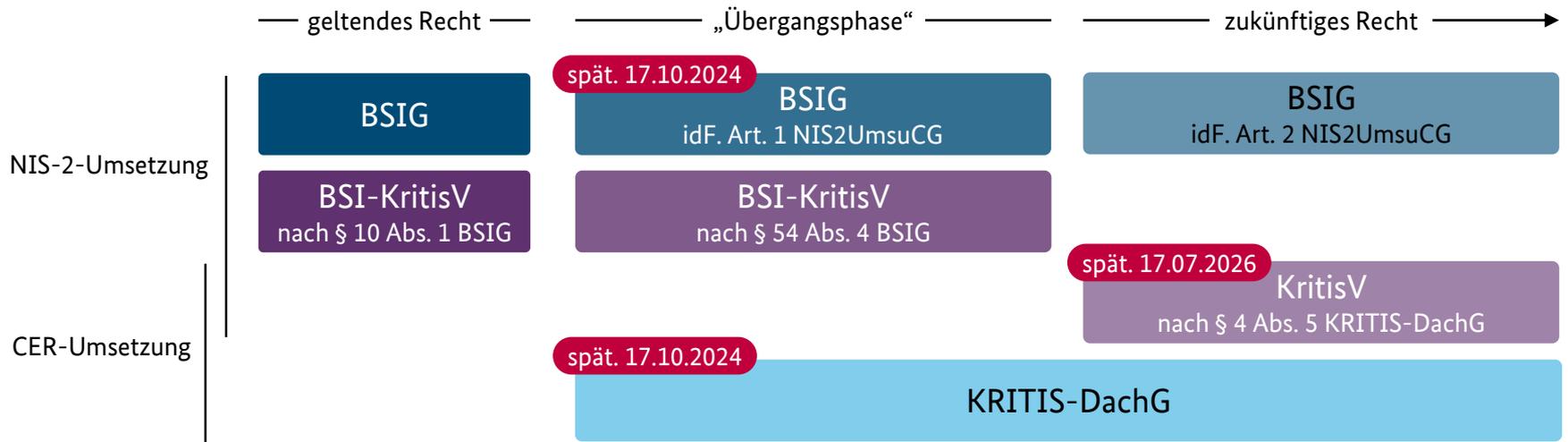
- Ausreichende Beteiligung der betroffenen Unternehmen und Verbände beim Erlass der KritisV sicherstellen 
- Ausreichende Umsetzungsfristen vorsehen  
- § 41 / § 9b: Regelungen für kritische Komponenten überarbeiten 

Harmonisierung mit KRITIS-Dachgesetz

- Harmonisierung von Begrifflichkeiten und Definitionen
- Gemeinsame Registrierungs- und Meldemöglichkeit einrichten
- Effiziente Zusammenarbeit zwischen BBK und BSI sicherstellen
- Einheitliche Rechtsverordnung zur Bestimmung kritischer Anlagen



Zeitliches Zusammenspiel von BSIG / KRITIS-DachG



Mit dem Inkrafttreten der KritisV nach § 4 Abs. 5 KRITIS-DachG findet die Identifizierung von KRITIS (Betreiber kritischer Anlagen) zentral in dieser Rechtsverordnung statt. Grund: Gewährleistung der ununterbrochenen Identifizierung von KRITIS für die Zwecke des BSIG und längere Umsetzungsfrist für die Identifizierung von KRITIS für die Zwecke der Umsetzung der CER-Richtlinie.

Begriffsdefinitionen – Konkretisierungen und Klarstellungen

- Wiedereinfügung „Authentizität“ bei den Schutzzielen „Vertraulichkeit, Integrität, Verfügbarkeit“ 
- Einheitliche Verwendung von „Informationssicherheit“ vs. „Cybersicherheit“ 
- „Erheblicher Cybersicherheitsvorfall“ (§ 2 Abs. 1 Nr. 10): finanzielle Verluste näher qualifizieren (z.B. „existenzbedrohende finanzielle Verluste“) 

Begriffsdefinitionen – Konkretisierungen und Klarstellungen

- Abgrenzung „Cloud Computing Dienst“ und „Rechenzentrumsdienst“
- Begriff der „Cyberhygiene“ weiter konkretisieren
- Managed Service Provider („MSP“) stärker eingrenzen



Anwendungsbereich

- Anwendungsbereich bei wichtigen und besonders wichtigen Einrichtungen auf „versorgungsrelevante IT“ beschränken 
- Anwendungsbereich hinsichtlich Rechenzentrumsdienstleistern enger fassen 
- Doppelregulierung zwischen § 28 BSIG-E und § 5c EnWG-E vermeiden 
- Einrichtungsart Ladepunktbetreiber: Verweis auf AFIR statt LSV 

Registrierungs- und Meldepflichten

- Aufwand begrenzen - Einheitliche und voll digitalisierte Melde- und Registrierungsmöglichkeiten
- Klare Meldeprozesse etablieren
- Grundsatz „Ein Vorfall, eine Meldung“ sicherstellen



Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen (§ 38 BSIG-E)

- 1:1 Umsetzung von Artikel 20 NIS-2-Richtlinie (Cybersicherheit „zur Chefsache“ zu machen ist Ziel der NIS-2-Richtlinie) 
- Streichung Unabdingbarkeit Schadensersatzanspruch Geschäftsleitung – Einrichtung 

Datenbanken der Domain-Name-Registrierungsdaten (§§ 51-53 BSIG-E)

- Arbeitsergebnisse der NIS-Kooperationsgruppe zur auf EU-Ebene abgestimmten Konkretisierung der Richtlinienvorschriften werden eingearbeitet
- Streichung der Vorschriften



Risikomanagementmaßnahmen und Aufsicht

- § 30 Abs. 6: mögliche Nachteile durch den verpflichtenden Einsatz von zertifizierten Produkten vermeiden ✓
- Zuständigkeitsverteilung zwischen BSI und weiteren zuständigen Behörden (insb. BNetzA) klarstellen ✓
- Anforderungen an KRITIS, besonders wichtigen Einrichtungen und wichtigen Einrichtungen stärker abstufen (✓)
- § 30 Abs. 2: Liste der Risikomanagementmaßnahmen weiter präzisieren (✓)

Gelegenheit für Stellungnahmen

Gelegenheit für Stellungnahmen

- | | | | | |
|--------------|------------|---------------|---------------|-------------------------------|
| 1. ABDA | 11. BPEX | 21. DRV | 31. TeleTrusT | 41. Wertpapier-
firmen |
| 2. AG KRITIS | 12. BREKO | 22. DSLV | 32. TÜV | 42. Wirtschaftsrat
der CDU |
| 3. ALM | 13. BUGLAS | 23. DVF | 33. UP KRITIS | 43. ZDH |
| 4. BAH | 14. BVMW | 24. eco | 34. VATM | 44. ZVEI |
| 5. BDB | 15. BWE | 25. GDV | 35. VDA | |
| 6. BDEW | 16. DAV | 26. GKV-Sv. | 36. VDMA | |
| 7. BDI | 17. Dekra | 27. HDE | 37. VDV | |
| 8. BDL | 18. DENIC | 28. IDW | 38. VKU | |
| 9. BEE | 19. DIHK | 29. KZBV | 39. VOICE | |
| 10. Bitkom | 20. DKGEV | 30. Spectaris | 40. VUD | |

Nächste Schritte

1. Erstellung 4. Referentenentwurf
2. Finale Abstimmung des 4. Referentenentwurfs
3. Kabinettsbeschluss
4. Parlamentarisches Verfahren
5. Verkündung, Inkrafttreten

Vielen Dank für Ihre Teilnahme!



Bundesministerium
des Innern
und für Heimat

Kontakt

Referat CI 1 – Grundsatz; Cyber- und Informationssicherheit
Referat CI 3 – Cybersicherheit für Wirtschaft und Gesellschaft
Referat CI 4 – Cybersicherheit in der Bundesverwaltung