



Bundesministerium
des Innern
und für Heimat

Werkstattgespräch– Diskussionspapier des BMI für wirtschaftsbezogene Regelungen zur Umsetzung der NIS-2-RL

Tagesordnung

1. Begrüßung & Einleitung
2. Auswertung der eingegangenen Stellungnahmen
3. Weiterer Zeitplan
4. Mündliche Stellungnahmen

Angehörte Verbände und Institutionen

37 eingegangene schriftliche Stellungnahmen:

| | | | | |
|------------|----------|----------------|-------------|-----------|
| BDEW e.V. | DVF e.V. | TeleTrust e.V. | BREKO e.V. | VDMA e.V. |
| DVGW e.V. | GDV e.V. | UP KRITIS | eco e.V. | DKG e.V. |
| ARD | HDE e.V. | DIHK | VOICE e.V. | BDI e.V. |
| BVMW e.V. | BWE e.V. | BIEK e.V. | Bitkom e.V. | VKU e.V. |
| VATM e.V. | VDV e.V. | ZVEI e.V. | DSL e.V. | ASW e.V. |
| BVE e.V. | BVR e.V. | ALM e.V. | VDR | |
| UNITI e.V. | UTV e.V. | DEKRA | ZDS e.V. | |
| IDW e.V. | TÜV e.V. | VDA e.V. | BDL e.V. | |

2. Auswertung der eingegangenen Stellungnahmen

Allgemeine Punkte

Allgemeine Punkte- Harmonisierung mit dem KRITIS-Dachgesetz

- Harmonisierung NIS2UmsuCG und KRITIS-DachG: Begrifflichkeiten sowie Schwellenwerte, Zuordnungskriterien, Registrierungsanforderungen 
- §32 Abs. 1: Anpassung des mehrstufigen Meldeprozesses an das KRITIS-DachG (24h, 72h, 1 Monat vs. 24h, 1 Monat) 
- Einheitliche Abstimmungsvorgaben (Benehmen/Einvernehmen) für BBK und BSI sowie weiterer Beteiligter zur Festlegung gemeinsamer branchenspezifischer Standards 

Allgemeine Punkte- Klarstellungen zu verwendeten Begriffen

- § 30 Abs. 2: „Cyberhygiene“: Weitere Klarstellungen ✓
- § 2 Abs. 1 Nr. 30: „Rechenzentrumsdienst“: Weitere Klarstellungen (Housing und/oder Hosting) ✓
- §2 Abs. 1 Nr. 13: Definition von IKT-Produkten Klarstellung, ob hier Software mitgemeint ist ✓
- § 30 Abs. 2 Nr. 3: Einhaltung von relevanten Anforderungen entlang der Lieferkette → Weitere Klarstellungen ✓
- § 30 Abs. 1 „IT Dienste für die Erbringung ihrer Dienste“: Weitere Klarstellungen ✓

Allgemeine Punkte-

Definition besonders wichtige Einrichtung/wichtige Einrichtung

- Bei Qualifizierung als „besonders wichtige Einrichtung“ aufgrund des Betriebs einer „Kritischen Anlage“ gem. § 28 Abs. 1 sollte nur der betroffene Unternehmensteil den speziellen Anforderungen an „Kritische Anlagen“ unterliegen 
- Weitere Erläuterungen für den Umgang mit Querverbundsunternehmen 
- § 30 Abs. 1: Eingrenzung des zu betrachtenden Scopes auf versorgungsrelevante Bereiche (für alle Einrichtungskategorien) 
- § 28 Abs. 3: Bei Hinzurechnung von Daten verbundener Unternehmen sollte die Beweislast der Nichtberücksichtigung beim BSI liegen 
- Ausnahme von konzern-/gruppeneigenen IT-Dienstleistern 

Allgemeine Punkte- Anwendung des Size-Caps

- § 28 Abs. 3: Es sind nur diejenigen Teile der Einrichtung einzubeziehen, die tatsächlich im Bereich der in den Anlagen 1 und 2 genannten Definitionen der Einrichtungskategorien tätig sind → Einschränkung sollte für alle Einrichtungen gelten 
- Bei der Anwendung des Size-Caps sollte auf die Haupttätigkeit des Unternehmens abgestellt werden 
- § 28: ergänzende Regelung bzgl. Unverhältnismäßigkeit bei Hinzurechnung der Daten von Partner- oder verbundenen Unternehmen → Konkretisierung, wann bestimmender Einfluss auf die informationstechnischen Systeme vorliegt 

Allgemeine Punkte- Anwendung des Size-Caps

- Kleine und mittlere Unternehmen umfänglich aus der Regulierung ausnehmen 
- Size Cap Kriterien für Mitarbeiterzahl und Umsatz nach Kommissionsempfehlung 2003/361 EC(1): „und“ statt „oder“ 
- Kritikalität als Bewertungsfaktor zur Kategorisierung in besonders wichtige Einrichtungen zusätzlich mit einbeziehen 

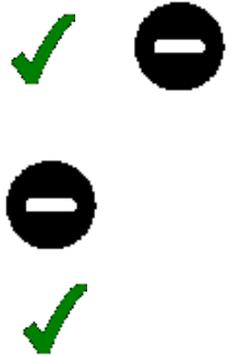
Allgemeine Punkte- Bereichsausnahmen

- Anpassung der Bereichsausnahmen (Finanzunternehmen nach DORA-VO, Betreiber von öffentlichen Telekommunikationsnetzen, Energieversorgungsnetzen und Energieanlagen)



Allgemeine Punkte- Zusammenspiel mit anderen EU Mitgliedsstaaten

- Vermeidung nationaler Sonderregelungen → 1:1 Umsetzung in nationales Recht
- Meldepflichten nur an eine Stelle (EU weit)
- EU-weit einheitliche Regulierung anstreben



Allgemeine Punkte- Registrierungs- und Meldepflichten

- Registrierungspflichten §33: Klarstellung, dass Pflichten erst gelten, wenn Melde- und Registrierungsmöglichkeiten vorhanden sind
- Kommunikation auf Englisch mit dem BSI ermöglichen
- § 32: Konkretisierung der Meldepflichten – substantiierte Kenntnis
- § 32: Meldemöglichkeiten vollumfänglich digital gestalten



Allgemeine Punkte- Registrierungs- und Meldepflichten

- §32 Abs. 1: Längere Fristen für Erstmeldung von Cybersicherheitsvorfällen (24 Stunden) 
- § 32 Abs. 1: Erhebliche Cybersicherheitsvorfälle sollten nur vorliegen bei „erheblichen“ finanziellen Auswirkungen 
- Registrierungspflichten §34 Weitere Klarstellungen im Umgang mit Konzernstrukturen 
- § 2 Abs. 2 Streichung der Verordnungsermächtigung zur weiteren Eingrenzung von „erheblichen“ Sicherheitsvorfällen 

Allgemeine Punkte- Nachweispflichten

- Nachweispflichten mit Übergangsfrist nach Inkrafttreten verlängern und konkretisieren (frühestens drei Jahre, sowohl für KRITIS als auch für wichtige und besonders wichtige Einrichtungen) ✓
- Bürokratieabbau bei den Nachweispflichten – unnötige Nachweispflichten sollten vermieden werden ✓
- Widersprüchliche Umsetzungs- und Nachweisfristen deutlicher darstellen ✓
- Einführung einer Dokumentationspflicht für wichtige und besonders wichtige Einrichtungen analog zu Art. 5 Abs. 2 DSGVO ✓

Allgemeine Punkte-

Verpflichtender Einsatz zertifizierter Produkte

- Streichung des § 30 Abs. 6 sowie der Verordnungsermächtigung in § 57 Abs. 3
- Vorschrift sollte eine Kann-Vorschrift sein, analog zur NIS-2 Richtlinie („Mitgliedstaaten können wesentliche und wichtige Einrichtungen dazu verpflichten(...).“)



Allgemeine Punkte- Billigung-, Überwachungs- und Schulungspflicht für Geschäftsleiter

- § 38 Abs. 1: u.U. unbillige Haftungsrisiken für Leiter nationaler Unternehmensteile eines multinationalen Konzerns 
 - Streichung des § 38 Abs. 2 zu Ersatzansprüchen der Einrichtung 
 - § 38 Abs. 3: Unklare Schulungspflichten für Geschäftsleiter 
 - Möglichkeit der Delegation an IT-Fachkräfte ermöglichen  
 - Streichung des § 64 Abs. 10: Möglichkeit, die Geschäftsführung/gesetzl. Vertretung für Leitungsaufgaben der Aufgaben zu entheben → Konsequenzen 
- Pflichten der Geschäftsführung insgesamt als nicht verhältnismäßig angesehen 

Allgemeine Punkte- Informationsaustausch

- § 6 Informationsaustausch: Zusammenarbeit zwischen Behörden und Betreibern erhöhen → Informations- und Meldepflichten ggü. den Betreibern einführen (Lageinformationen) → BSI Information Sharing Portal 
- Unterstützung bei Umsetzung der Anforderungen insbesondere bei kleineren Unternehmen – RL, Leitfäden, Muster, Ansprechpartner, etc. 
- Informationsaustausch sollte auf freiwilliger Basis erfolgen und mögliche Nutzung des Angebots ausgeweitet werden (Teilnahmebedingungen) 

Allgemeine Punkte-

Weitere Punkte

- § 30: Nutzung der branchenspezifischen Sicherheitsstandards(B3S) auch für wichtige Einrichtungen ermöglichen  
- § 33 Abs. 2: Streichung der Pflicht zur Übermittlung von IP-Adressbereichen 
- Klarstellung, dass nur öffentliche IP-Adressbereiche zu übermitteln sind 
- Absenkung der Bußgeldgrenzen 
- Aufnahme der Länder und Kommunen in den Anwendungsbereich 

Sektorspezifische Themen

Gesundheit

- Ausnahmeregelung gem. § 28 Abs. 4 aufgrund spezialgesetzlicher Regelungen im SGB V für Krankenhäuser
- Branchenspezifische Lösung für die Anforderungen des § 30 Abs. 2
- § 40 Abs. 4 Übermittlungspflichten von Informationen – Klärung der Vereinbarkeit bei personenbezogenen Daten gem. Art. 9 DSGVO



Sektorspezifische Themen

Transport und Verkehr

- Angleichung der von der Richtlinie erfassten Einrichtungsdefinitionen für die Schifffahrt an die derzeitigen Begriffsbestimmungen der BSI-KritisV
- Harmonisierung bestehender Cybersicherheitsverpflichtungen im Bereich der Luftfahrt



Sektorspezifische Themen

Energie

- Anpassung der Definitionen für Wasserstoff 
- Begrifflichkeiten in der Strom- und Gasversorgung an das EnWG anlehnen 

3. Weiteres Vorgehen

- Erstellung des zweiten Referentenentwurfs und Einleitung der zweiten Runde der Ressortabstimmung
- Länder- und Verbändeanhörung
- Einleitung des parlamentarischen Verfahrens
- Inkrafttreten, anschließend Start der 3 Jahresfrist für Nachweise

Ende der Umsetzungsfrist der NIS-2-Richtlinie: 17. Oktober 2024

4. Anhörung zu den Stellungnahmen

Mündliche Stellungnahmen

Vielen Dank für Ihre Aufmerksamkeit!



Bundesministerium des Innern und für Heimat

Referat CI 3

ci3@bmi.bund.de