

NIS-2-Richtlinie & die deutsche Umsetzung

1. Einführender Überblick

- a) Aktuelle Lage der IT-Sicherheit
- b) Aktuelle Beispiele
- c) Schutz der KRITIS

2. NIS-2-Richtlinie

- a) Allgemeines

3. NIS-2-Umsetzungsgesetz

- a) Übersicht
- b) Inhaltliche Vorgaben
- c) Kabinettsentwurf



Überblick über das Ausmaß der Gefahren im vergangenen Jahr

Top 3-Bedrohungen je Zielgruppe:

Gesellschaft



Identitätsdiebstahl
Sextortion
Fake-Shops im Internet

Wirtschaft



Ransomware
Schwachstellen, offene oder falsch konfigurierte Online-Server
IT-Supply-Chain: Abhängigkeiten und Sicherheit

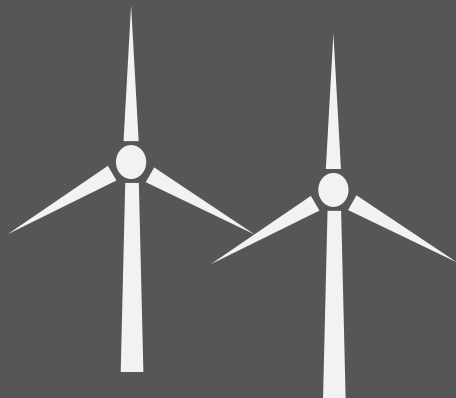
Staat & Verwaltung



Ransomware APT
Schwachstellen, offene oder falsch konfigurierte Online-Server



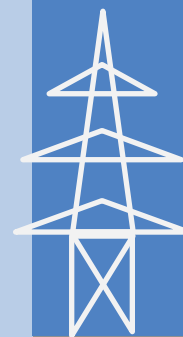
Kollateralschaden nach Angriff auf Satellitenkommunikation



78

Global bekannt gewordene Schwachstellen am Tag

Anstieg von 14% im Vergleich zum Vorjahr



11,5 Millionen neue Malware-Varianten
Anstieg von 26% im Vergleich zum Vorjahr!

22

aktive APT-Gruppen (advances persistent threat) in Deutschland



>100

bekannte Cybercrime-Gruppen in Deutschland

300k-850k \$

durchschnittlich gezahltes Lösegeld bei Angriffen mit Ransomware

Differenzierung nach Verschlüsselung bzw. Exfiltration von Daten



1,1 Mrd. \$

wurden im Jahr 2023 weltweit von Ransomware-Gruppen in Form von Lösegeld erbeutet

2024

Veränderung
zum Vorjahr

Cybercrime-Fälle:

Inland: 131.391

Ausland: 201.877

Inland: - 2,2%

Ausland: + 6%

**In Deutschland durch Cyberattacken
entstandene Schäden:**

→ 178,6 Mrd. Euro

+ 20,51%

Anzahl der Ransomware-Angriffe:

→ 950

- 6,7%

Aufklärungsquote:

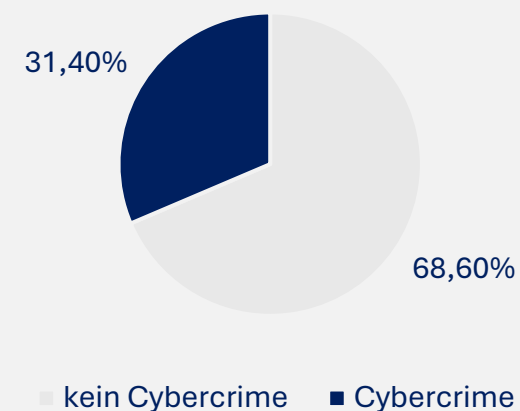
→ 31,9%

- 0,9%

Besondere Gefahr durch Auslandstaaten

- Aufenthaltsort der Täter unbekannt oder nicht in Deutschland
- Schaden/Taterfolg tritt in DE ein

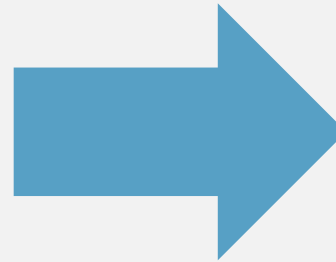
Auslandstaaten



Beispiel 1: CrowdStrike Falcon verursacht weltweit IT-Ausfälle

Sachverhalt:

- Am 19. Juli 2024 verursachte ein Update der EDR-Software Falcon von CrowdStrike weltweit IT-Ausfälle
- In Deutschland waren auch KRITIS-Betreiber und meldepflichtige Organisationen betroffen
 - Nur Unternehmen betroffen, keine Privatpersonen
- Update führte zu Systemabsturz mit Bluescreen of Death (BSOD) auf Windows-Systemen
- Fehler trat nur bei installiertem Falcon EDR Sensor auf
- Ursache war ein Programmierfehler in der in C++ entwickelten Software
 - CrowdStrike veröffentlichte am 19. Juli 2024 einen Workaround
- Etwa 8,5 Millionen Windows-Systeme betroffen (laut Microsoft)
- Cyberkriminelle nutzten Ausfälle für Phishing, Betrugsversuche und Fake-Webseiten
- Ab dem 21. Juli 2024 stabilisierte sich die Lage



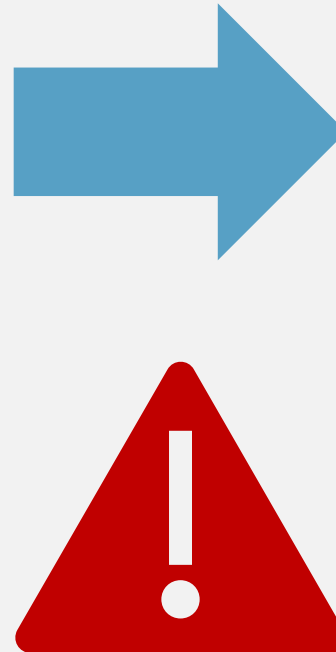
Bewertung durch das BSI:

- Kein Cyberangriff, sondern Qualitätssicherungsfehler des Herstellers
- Enorme wirtschaftliche Schäden, Höhe noch unbekannt
 - Erste Schätzungen: Kosten vermutlich in Milliardenhöhe

Beispiel 2: Cybersicherheitsvorfall bei einem Remote-Screensharing-Anbieter

Sachverhalt:

- Cyberangriff auf bekannten Hersteller für Fernzugriffs- und Screensharing-Software im Februar 2024
- Kompromittierung interner Systeme, dabei Abfluss von:
 - Quellcode
 - Signierzertifikaten
- Hersteller reagierte umgehend mit einem Dienstleister:
 - Systeme bereinigt und wiederhergestellt
 - Zertifikate zurückgezogen
 - Sicherheitsupdates veröffentlicht (Zertifikatsaustausch bei Endnutzern)
- Kein Nachweis für Kompromittierung von Nutzerdaten, aber vorsorglich:
 - Passwort-Reset im Kundenportal

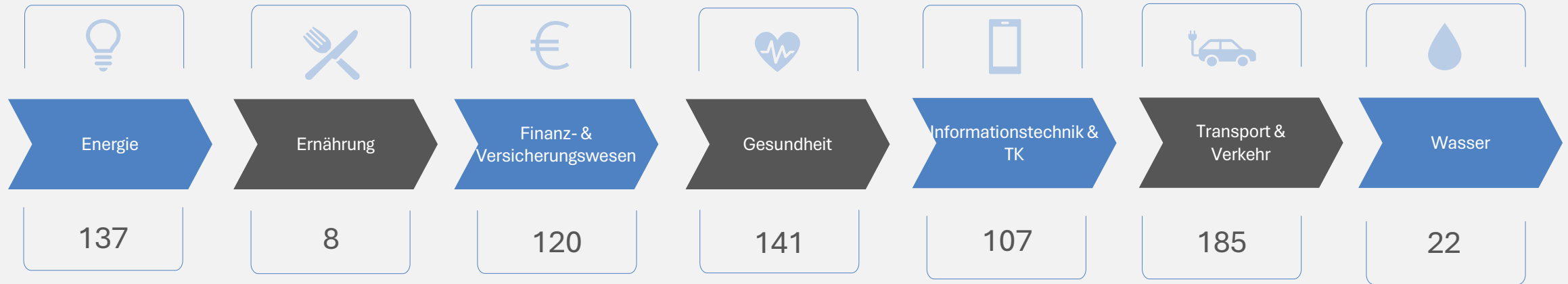


Bewertung durch das BSI:

- Abfluss von Quellcode und Zertifikaten birgt hohes Risiko:
 - Gefahr für Folgeangriffe (z. B. Man-in-the-Middle, Supply-Chain)
 - Potenziell unbemerkte oder bereits erfolgte Angriffe mit kompromittierten Zertifikaten
- Maßnahmen des Herstellers senken Risiko deutlich
- Restrisiko bleibt:
 - Schadhafte Software mit kompromittierten Zertifikaten könnte über Drittseiten oder gezielt verbreitet werden
- Besonders kritisch:
 - Einsatz der Software mit administrativen Rechten im Unternehmensumfeld

- **Kritische Infrastruktur (KRITIS):**
 - Umfasst lebenswichtige Einrichtungen wie Energie, Wasser, Gesundheitswesen & Verkehr
 - Ihr Ausfall oder Beeinträchtigungen könnten schwerwiegende Folgen für die Bevölkerung, Wirtschaft & Sicherheit haben
- Schutz kritischer Infrastrukturen als **Kern** der **deutschen Sicherheitspolitik**
- **Hauptverantwortung** für Schutz bei **Betreibern**
- Absicherung gegen Naturkatastrophen, Terrorismus, Sabotage, menschliches Versagen
 - Zunehmende Bedeutung der **Resilienz kritischer Infrastrukturen**
- **Resilienz:** Fähigkeit zur **Anpassung & schnellen Wiederherstellung** der Funktionalität nach Ereignissen

■ Meldungszahlen nach KRITIS-Sektoren (2024) → insgesamt: 726



Störungen, die zu einem Ausfall oder zu einer erheblichen Beeinträchtigung der Funktionsfähigkeit geführt haben

■ Hauptgefahren in einzelnen KRITIS-Sektoren:

Energie

- Phishing,
- DDoS
- Menschliche Fehler

Netzinfrastruktur

- Gefahren durch Schwachstellen in privaten und öffentlichen TK-Netzen

Satellitenkommunikation

- Klassische Angriffsvektoren auf terrestrische Infrastruktur
- Angriffspfade auf die Satelliten selbst

01

Vorbereitung der Mitgliedsstaaten

02

Zusammenarbeit zwischen den Mitgliedsstaaten

03

Schaffung einer Sicherheitskultur in wichtigen Sektoren

04

Sanktionen bei Verstößen

01

Vorbereitung der Mitgliedsstaaten



- Angemessene Ausrüstung der Mitgliedsstaaten mit **Technik & Personal**
- **Beispiele:**
 - Gründung eines Computer Security Incident Response Team (**CSIRT**)
 - Gründung einer nationalen Behörde für Netzwerk- & Informationssicherheit (**NIS**)

02

Zusammenarbeit zwischen den Mitgliedsstaaten



- Einsetzung einer **Kooperationsgruppe**
- **Ziel:**
 - Unterstützung & Erleichterung der strategischen Zusammenarbeit sowie des Informationsaustausches zwischen den Mitgliedsstaaten

03

Schaffung einer Sicherheitskultur in wichtigen Sektoren



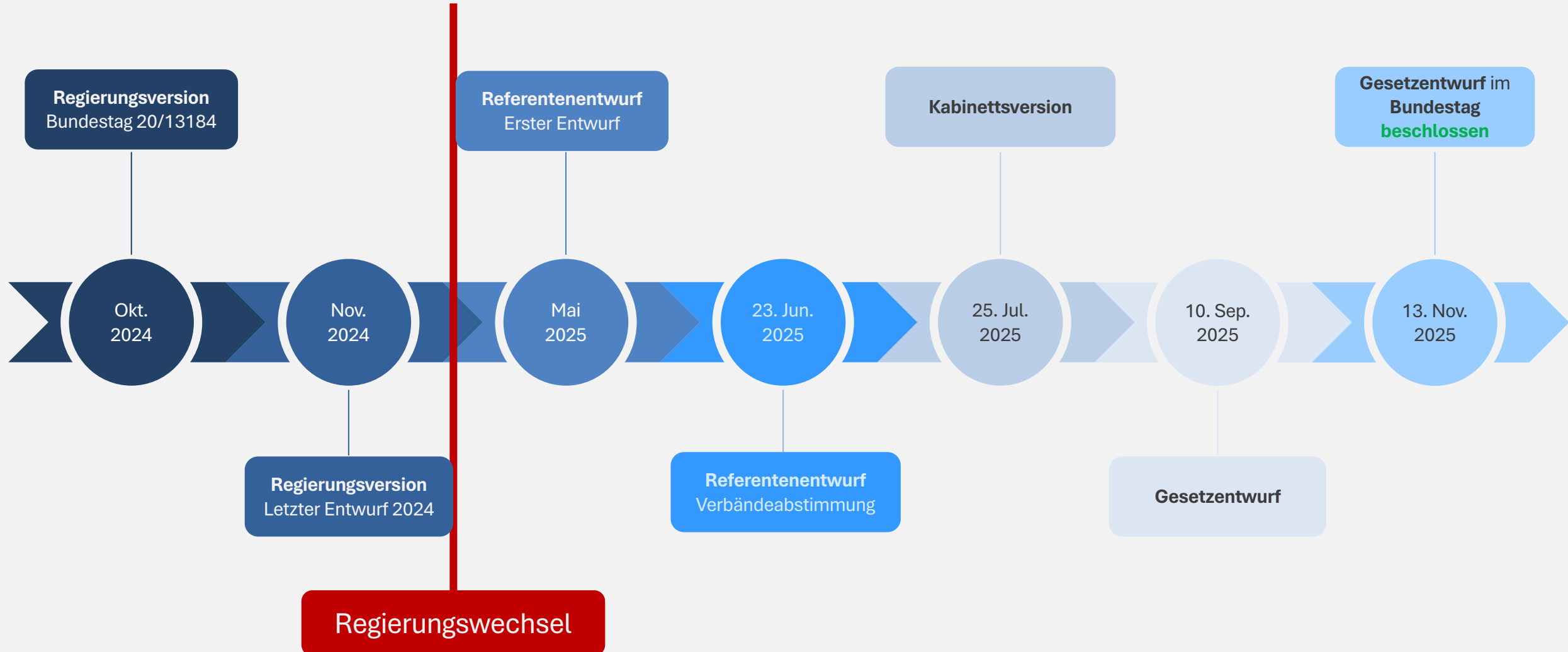
- In Sektoren, die stark auf Informations- und Kommunikationstechnik (ITK) angewiesen sind und für die Wirtschaft und Gesellschaft von entscheidender Bedeutung sind, muss der Sicherheitsaspekt eine besonders tragende Rolle spielen
- Dabei werden insbesondere die **Unternehmen** in die Pflicht genommen
 - Sie müssen geeignete **Sicherheitsmaßnahmen** ergreifen und sich bei schwerwiegenden Fällen an die zuständigen nationalen Behörden wenden
- Die betroffenen **Sektoren** sind insbesondere:
 - **Energie**, Verkehr, Wasser, Banken, Gesundheitsversorgung, **Telekommunikation** und viele weitere

04

Sanktionen bei Verstößen



- Sanktionen in Form von Bußgeld:
 - Stufenkonzept für Bußgeldtatbestände bis zu **20 Millionen EUR**.
 - Berücksichtigung von **fahrlässigem & vorsätzlichem Verschulden**.
- Bußgeldrahmen für wichtige Einrichtungen:
 - Bis zu **7 Mio. EUR** oder mindestens **1,4 % des weltweiten Umsatzes im vorangegangenen Geschäftsjahr**.
- Bußgeldrahmen für besonders wichtige Einrichtungen:
 - Bis zu **10 Mio. EUR** oder mindestens **2 % des weltweiten Umsatzes im vorangegangenen Geschäftsjahr**.
- Keine Differenzierung:
 - Zwischen besonders wichtigen Einrichtungen & Kritischen Anlagen erfolgt keine spezifische Differenzierung.



Übersicht der relevanten finalen Änderungen vor Abschluss im Bundestag

Kritische Komponenten (§ 41 BSIG; Art.1 NIS2-Umsetzungsgesetz)

- Die Pflicht zur **vorherigen Anzeige kritischer Komponenten** beim Bundesinnenministerium (BMI) entfällt
- Die **Zertifizierungspflicht** kritischer Komponenten nach **§ 165 Abs. 4 TKG** für Betreiber von Netzen mit erhöhtem **Gefährdungspotenzial** besteht jedoch weiterhin unverändert
- Die Vorlage einer **Garantieerklärung** der Hersteller ist **nicht mehr erforderlich**
- Insgesamt kommt es damit zu einem **Abbau** von **Bürokratie** für Betreiber und Hersteller



- Das **BMI** erhält **erweiterte Befugnisse**, den Einsatz kritischer Komponenten in kritischen Anlagen zu untersagen
- Eine **Untersagung** kann erfolgen, wenn der Einsatz die öffentliche Sicherheit oder Ordnung voraussichtlich beeinträchtigt (**§ 41 Abs. 1 BSIG**)
- Die Entscheidung erfolgt im Benehmen mit dem **BMF** und dem **Auswärtigen Amt**
- Ein Katalog nicht abschließender Regelbeispiele beschreibt, wann eine „**voraussichtliche Beeinträchtigung**“ vorliegen kann
- Regelbeispiele sind **weit** und **offen** (**drohende Rechtsunsicherheit**)

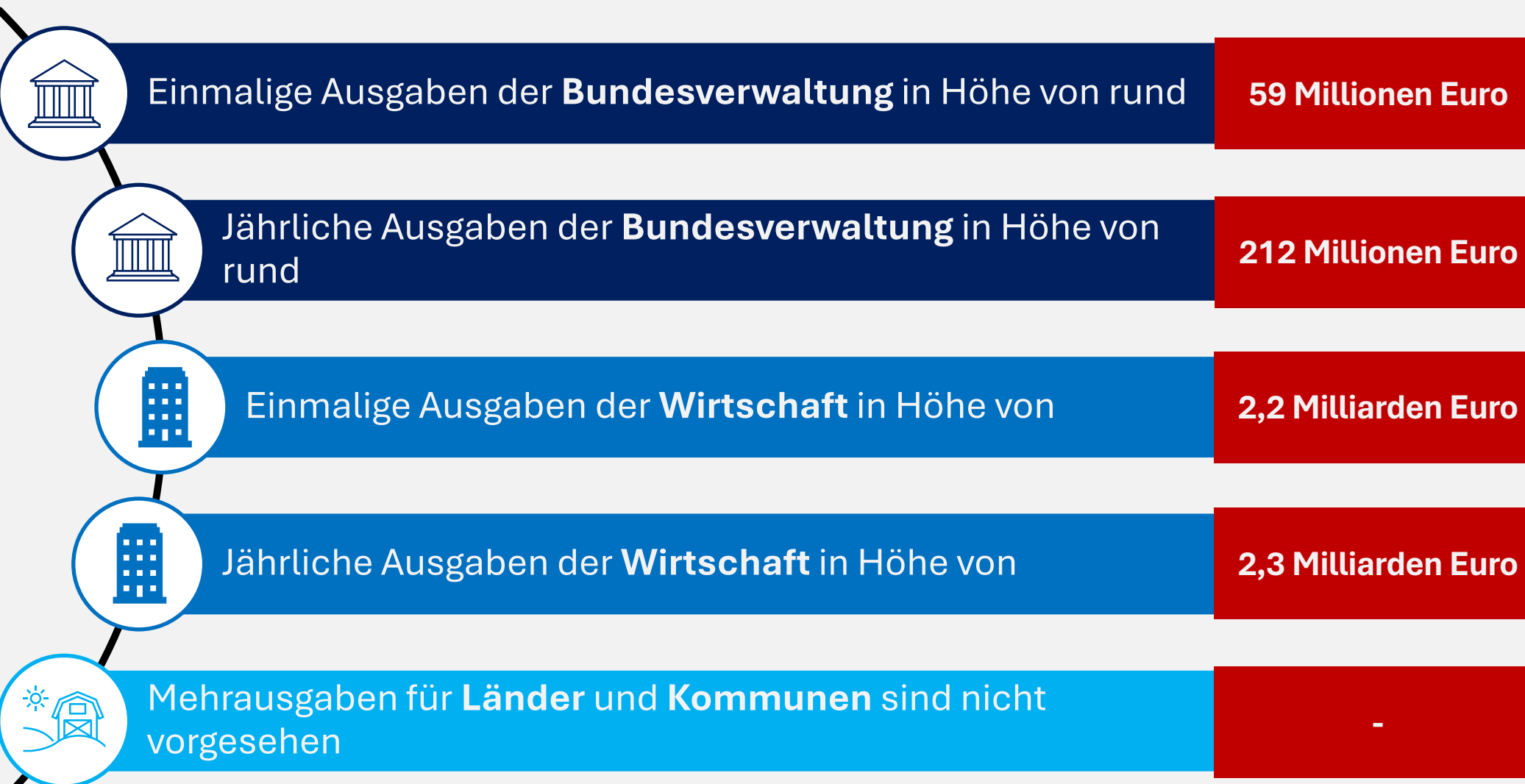


- Nach einer **Untersagung** kann das BMI auch den künftigen Einsatz weiterer kritischer Komponenten desselben Herstellers **untersagen**
- Das BMI kann zudem per **Allgemeinverfügung** allen Betreibern kritischer Anlagen den Einsatz derselben Komponente oder desselben Komponententyps untersagen
- Ein **Verbot** kann – muss aber nicht – mit einer **Umsetzungsfrist** versehen werden
- Widerspruch** und **Klage** haben **keine aufschiebende Wirkung**
- Betreiber kritischer Anlagen sind nun verpflichtet, bei der **Sachverhaltsaufklärung mitzuwirken** (im Gegensatz zur bisherigen Rechtslage)



Wegfall der De-Minimis-Regelung bei der Anordnung von Maßnahmen nach § 169 TKG (§ 16 BSIG; Art.1 NIS2-Umsetzungsgesetz)

- Die **100.000-Kunden-Schwelle** für Anordnungen des BSI nach **§ 169 Abs. 6 und 7 TKG** entfällt
- Das BSI kann nun jeden Netzbetreiber adressieren – unabhängig von der Kundenzahl
- Anordnungen** betreffen insbesondere:
 - Einschränkung, Umleitung** oder **Unterbindung von Telekommunikationsdiensten** zur Behebung von Störungen,
 - Einschränkung des Datenverkehrs** von und zu Störungsquellen
- Bei der Anordnung müssen die **technischen Möglichkeiten** des Netzbetreibers und die **wirtschaftliche Zumutbarkeit** berücksichtigt werden



Betroffene Unternehmen/Einrichtungen in Deutschland

Normen entsprechen dem aktuellen Gesetzesentwurf des NIS-2-Umsetzungsgesetz

Besonders wichtige Einrichtungen nach Größe des Unternehmens in Sektoren aus Anlage 1

- Unternehmen ab 250 Mitarbeitern oder
- Unternehmen über 50 Mio. EUR Umsatz und Bilanz über 43 Mio. EUR
- **Größenunabhängig:** qTSP, TLD, DNS, TK-Anbieter, kritische Anlagen
- **Sonderfall:** TK-Anbieter ab mittlerer Größe

§ 28 I S

Wichtige Einrichtungen nach Größe des Unternehmens in Sektoren aus Anlage 1 und 2

- Unternehmen ab **50 Mitarbeitern** oder
- Unternehmen über **10 Mio. EUR Umsatz** und Bilanz über **10 Mio. EUR**
- Vertrauensdienste und TK-Anbieter

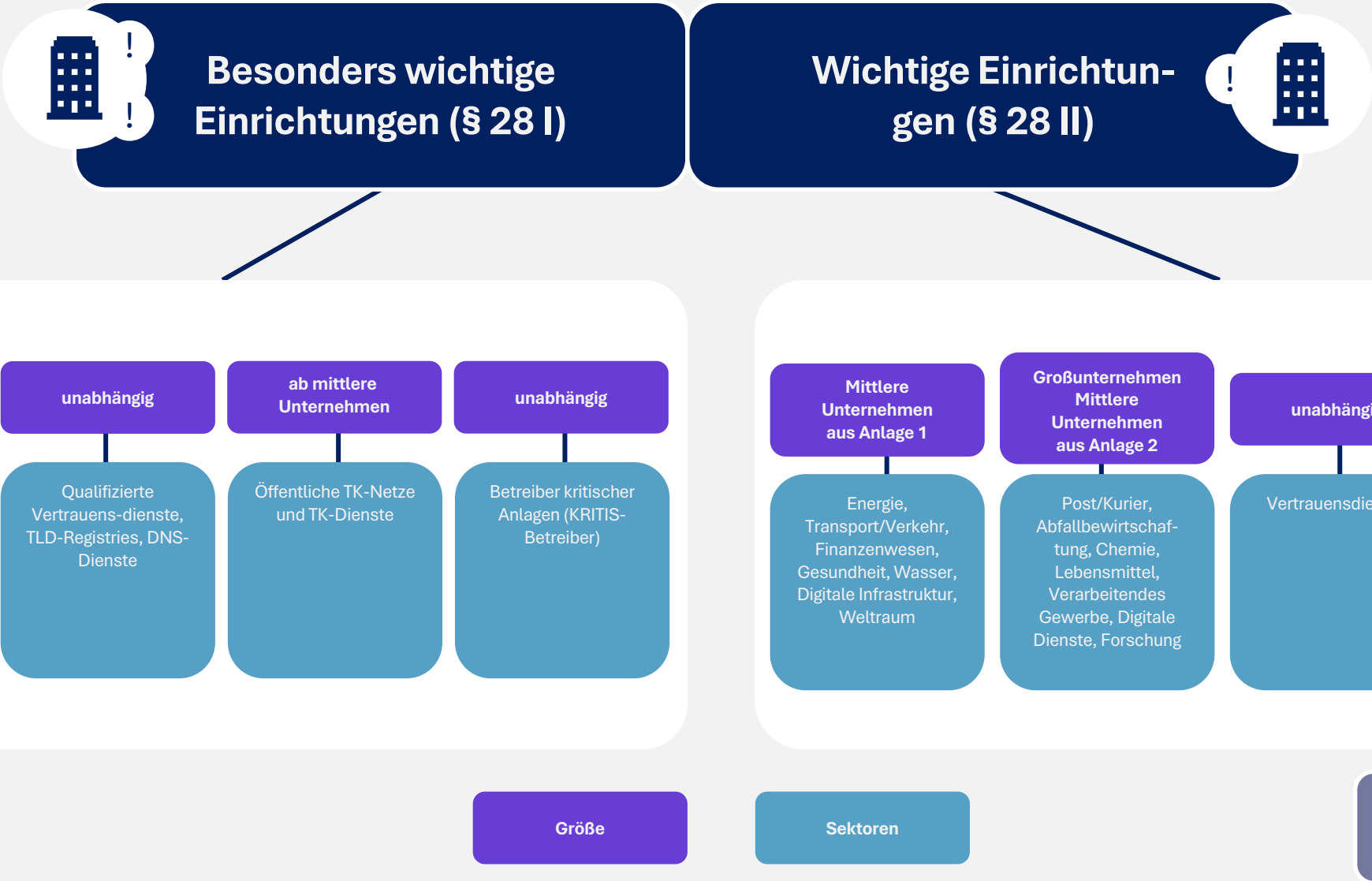
§ 28 II S

Von KRITIS-Betreibern nach der KRITIS-Methodik einzeln festgestellte Anlagen

- KRITIS-Anlage über Schwellenwert, in der Regel ≥ 500 Tsd. versorgte Personen

Einrichtungen der Bundesverwaltung

§ 29 I S



Pflichten von Betreibern und Einrichtungen

Pflicht	Betreiber kritischer Anlagen	Besonders wichtige Einrichtung	Wichtige Einrichtung
Geltungsbereich	Anlage	Unternehmen	Unternehmen
Maßnahmen Risikomanagement § 30	*	+	+
Höhere Maßstäbe für KRITIS §31 (1)	+	-	-
Besondere Maßnahmen SzA §31 (2)	+	-	-
Meldepflichten §32	*	+	+
Registrierung §33 §34	+	+	+
Unterrichtungspflichten (Kunden) § 35	*	+	+
Geschäftsleitung Umsetzung §38	*	+	+
Nachweise und Prüfungen §39	+	tw. (§ 61)	tw. (§ 62)

*
implizit, da Betreiber kritischer Anlagen auch besonders wichtige Einrichtungen sind

Wesentliche Kritik am aktuellen Gesetzentwurf des NIS2UmsuCG

§ 1 – BSI-Kritisverordnung

In § 1 der BSI-Kritisverordnung wurden die Definitionen von „Betreiber“ und „kritischer Dienstleistung“ gestrichen, obwohl beide Begriffe an vielen Stellen weiterverwendet werden – was zu Unklarheiten führt.

§ 2 – Begriffsbestimmungen (zu „kritische Infrastrukturen“ und „DNS-Diensteanbieter“)

- Kritisierung nationaler Begriffsbestimmungen bei der Umsetzung von **Artikel 23 der NIS-2-Richtlinie**; gefordert wird ein gemeinsames europäisches Begriffsverständnis
- Beanstandung der uneinheitlichen Auslegungspraxis zu Meldepflichten in den EU-Mitgliedstaaten; Notwendigkeit einer kohärenten Umsetzung
- Problematisierung des Begriffswechsels von „kritischer Infrastruktur“ zu „kritischer Anlage“ im **BSIG-E** und **TKG**; unklare Auswirkungen auf die Rechtsanwendung
- Die Definition von DNS-Diensteanbietern in **§ 2 BSIG-E** entspricht wortgleich der NIS-2-Richtlinie; die in der Begründung enthaltene Einschränkung bleibt ohne rechtliche Wirkung
- Um Doppelregulierung zu vermeiden, sollte die Ausnahme für Telekommunikationsanbieter ausdrücklich im Gesetzestext verankert werden



§ 28 – Anwendungsbereich

- **§ 28 Abs. 3 BSIG-E** ist europarechtlich genauso zweifelhaft wie die Formulierung des vorherigen Entwurfes
 - Praktisch auch weitestgehend wirkungslos, da Unternehmen, die nur wegen einer Solarstromanlage auf dem Dach in den Anwendungsbereich zu fallen drohen, ein seltener Ausnahmefall sein dürften
- Die neue Regelung erweitert den Anwendungsbereich erheblich, da nun alle Geschäftstätigkeiten eines Unternehmens berücksichtigt werden
- Unklar ist, was als „vernachlässigbar“ gilt – fehlende Definition führt zu Rechtsunsicherheit für betroffene Unternehmen
- Es wird eine Klarstellung durch konkrete Schwellenwerte oder Abgrenzungskriterien gefordert



Wesentliche Kritik am aktuellen Gesetzentwurf des NIS2UmsuCG

§ 29 – Einrichtungen der Bundesverwaltung

- Die geplanten IT-Sicherheitsregelungen für die Bundesverwaltung schwächen das bestehende Schutzniveau, da nur Ministerien und das Kanzleramt verbindlich § 30 unterliegen sollen, während für andere Behörden lediglich Mindeststandards gelten, die hinter dem IT-Grundschutz zurückbleiben
- Eine solche Absenkung widerspricht früheren Forderungen und gefährdet die Vorbildfunktion des Bundes – insbesondere gegenüber Unternehmen im Zuge der NIS-2-Umsetzung; der IT-Grundschutz sollte daher für alle Bundesbehörden verbindlich vorgeschrieben werden



§ 30 – Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen (Begriff „Cyberhygiene“)

- Die Streichung des Begriffs „Cyberhygiene“ in § 30 Abs. 2 Nr. 7 BSIG-E widerspricht der NIS-2-Richtlinie und ist formal fehlerhaft
- Der Ersatz durch „Sensibilisierungsmaßnahmen“ stellt einen Kategorienfehler dar, da „Cyberhygiene“ konkrete technische Maßnahmen umfasst
- Die Richtlinie unterscheidet ausdrücklich zwischen Cyberhygiene (Erwägungsgrund 49) und Sensibilisierung (Erwägungsgrund 50)
- Die Streichung ist zudem inkonsequent, da „Cyberhygiene“ im EnWG (§ 5c) weiterhin genannt wird



Wesentliche Kritik am aktuellen Gesetzentwurf des NIS2UmsuCG

§ 38 – Umsetzung-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

- Änderung in **§ 38 Abs. 1 BSIG-E** von „Risikomanagementmaßnahmen zu genehmigen“ zu „umzusetzen“ wird kritisiert, da die Umsetzung spezifisches Fachwissen erfordert
- Die Verantwortung für die Umsetzung sollte bei Fachabteilungen liegen; empfohlen wird die Rückkehr zur ursprünglichen Formulierung
- Klarstellung gefordert, dass die Geschäftsleitung geeignete Dritte beauftragen kann, die Verantwortung aber weiterhin bei ihr verbleibt



§ 44 – Vorgaben des Bundesamtes

- Der aktuelle Regierungsentwurf zeigt kaum Fortschritte gegenüber dem Referentenentwurf, während **§ 44 BSIG-E** sogar einen deutlichen Rückschritt darstellt
 - Die neue Fassung verzichtet auf die ausdrückliche Verankerung des IT-Grundschatzes, der ursprünglich als zentrale Grundlage der IT-Mindestanforderungen vorgesehen war
 - Stattdessen wird nur noch auf die vom BSI festgelegten Mindeststandards verwiesen, was die rechtliche Verbindlichkeit und Transparenz schwächt
- Diese Änderung legitimiert bestehende Umsetzungsdefizite, anstatt sie zu beheben, und droht, das bislang unzureichende Sicherheitsniveau dauerhaft zu verfestigen
- Ein verbindlicher Verweis auf den IT-Grundschatz wäre notwendig, um ein einheitliches, hohes Sicherheitsniveau in der Bundesverwaltung sicherzustellen



Wesentliche Kritik am aktuellen Gesetzentwurf des NIS2UmsuCG

§ 56 – Ermächtigung zum Erlass von Rechtsverordnung



- Kritisiert wird die ersatzlose Streichung der Beteiligungsrechte von Wissenschaft, KRITIS-Betreibern und Wirtschaftsverbänden bei der Ausgestaltung von **§ 56 Abs. 4** und **5 BSIG-E**; die bisherige Anhörungspraxis sollte fortgeführt werden
- Die Einbindung der Wirtschaft wird als wesentlich für praxistaugliche und akzeptierte Regelungen angesehen
- Die Festlegung von Schwellenwerten für „kritische Anlagen“ ausschließlich durch Rechtsverordnung im Gesetzgebungsverfahren wird kritisch bewertet; sektorspezifische Schwellenwerte der bestehenden BSI-KritisV sollten beibehalten werden
- Das Bundesministerium für Digitales und Staatsmodernisierung (BMDS) fehlt in der Vertreterliste des **§ 56 Abs. 4** trotz fachlicher Relevanz, insbesondere im Bereich TK-Netzausbau; eine Ergänzung wird als notwendig erachtet

Zum Artikel 25: Änderung des Telekommunikationsgesetzes



- Die Neugestaltung von **§ 165 Abs. 2** und die Ergänzung um **Abs. 2a** im **TKG** legen Mindestanforderungen für Risikomanagementmaßnahmen im Bereich Cybersicherheit fest
- Ein Abgleich mit dem bestehenden Sicherheitskatalog der BNetzA ist daher zwingend erforderlich und eine Überarbeitung des Katalogs wird erwartet
- Dabei sind verschiedene neue Anforderungen und Abwägungskriterien zu berücksichtigen; relevante Normen sind insb.:
 - **§ 165 Abs. 2 Satz 3 (neu); § 165 Abs. 2a; § 165 Abs. 2a Nr. 4; § 165 Abs. 2 (2b)**
- Überarbeitung der Meldepflicht in **§ 168 Abs. 1 TKG-E** erforderlich
 - Gefahr der **Doppelregulierung**

Chancen des Gesetzentwurfs

§ 6 – Informationsaustausch

- Begrüßung des Aufbaus der BSI-Online-Plattform zum Informationsaustausch mit wichtigen Einrichtungen und Bundesverwaltung
 - Empfehlung frühzeitige und transparente Veröffentlichung der Plattformfunktionen
- Teilnahmebedingungen nach **§ 6 Abs. 2** sollten niedrigschwellig und KMU-tauglich gestaltet sein
- Vereinheitlichung mit Plattformen aus anderen Gesetzesvorhaben (z. B. **CER-Richtlinie**) wird befürwortet
- Eine engere Verzahnung mit gesetzlichen Informationspflichten (z. B. **CER-Richtlinie**) stärkt Effizienz und Anwenderfreundlichkeit; die Fortführung der UP KRITIS bleibt für den Austausch zwischen Staat und Wirtschaft wichtig
- Eine europäische Harmonisierung soll den Aufwand für international tätige Unternehmen verringern

§ 41 – Untersagung des Einsatzes kritischer Komponenten

- Ziel, kritische Infrastrukturen effektiv zu schützen, ist positiv zu sehen
- **§ 41 NIS2UmsuCG** enthält strenge Vorgaben für den Einsatz kritischer Komponenten
- Eine ausgewogene Entscheidung unter Federführung des BMI wird begrüßt
- Festlegung kritischer Komponenten sollte im Einvernehmen mit BNetzA und BSI sowie unter Beteiligung von Wirtschaft und Wissenschaft erfolgen; nationale Sonderlösungen oder „Goldplating“ sind zu vermeiden, bis die EU-weit abgestimmte „ICT Supply Chain Toolbox“ vorliegt



www.wr-recht.de



info@wr-recht.de



Tel.: 040 / 350036-0



Standort Hamburg

Bleichenbrücke 11

20354 Hamburg

Hinweise

© Der gesamte Inhalt dieser Präsentation mit Ausnahme des Titelfotos ist ausschließliches Eigentum der WIRTSCHAFTSRAT Recht – Bremer Woitag Rechtsanwaltsgesellschaft mbH. Ohne Einwilligung der Rechtsinhaberin ist jegliche Übernahme zur Vervielfältigung und zur Nutzung für werbliche Zwecke oder die Änderung des Inhalts bei Beibehaltung der wesentlichen strategischen Aussagen – auch einzelner – Vorschläge unzulässig, wenn nicht dafür die schriftliche Genehmigung der Rechtsinhaberin eingeholt wurde.

Das Titelfoto wird unter einer CC 0 Lizenz über die Plattform Unsplash bereitgestellt. Weitere Bilder und Icons stammen von Flaticon.