NIS2UmsuCG

Aktueller Stand der deutschen Umsetzung

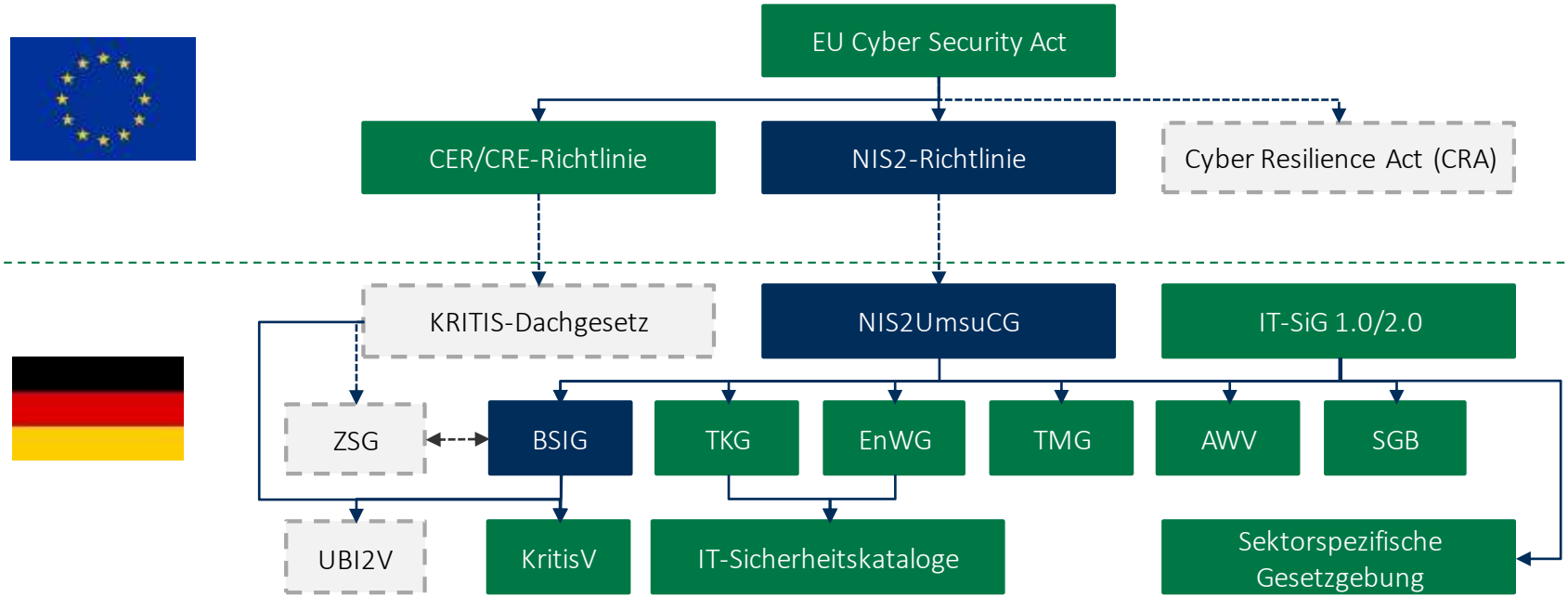
Manuel Atug

Über mich

Manuel Atug

- Principal bei HiSolutions
- Diplom-Informatiker, Master of Science in Applied IT Security, Ingenieur
- begleitet KRITIS-Betreiber bei der Umsetzung der Anforderungen:
  - ISMS, BCM, branchenspezifischer Stand der Technik (B3S)
  - Notfall- und Continuity-Management
- prägender Berater des BSI für § 8a BSIG

Übersicht zur Regulierungsstruktur



Grün: verabschiedet **Blau**: Scope NIS2 **Grau**: In Arbeit

Die Aufregung

- Erweiterung des Geltungsbereiches um den Faktor 7-10
- Inklusion der Lieferkette
- wenige Ausnahmeregelungen
- weitreichende Befugnisse für das BSI
- empfindliche Strafen

Wer fällt unter das Gesetz? (1)

- Inklusion und Aufteilung über Einrichtungsgrößen (EU Size Cap) und Sektorenzugehörigkeit:

BESONDERS WICHTIG

a) mindestens **250 Mitarbeiter**, oder

b) Jahresumsatz **über 50 Millionen Euro** und Jahresbilanzsumme **über 43 Millionen Euro**

c) Zugehörigkeit zu Anlage 1 NIS2UmsuCG

ODER

Betreiber kritischer Anlagen, unabhängig von der Unternehmensgröße (Richtwert: Versorgung von mehr als 500.000 Personen)

WICHTIG

a) mindestens **50 Mitarbeiter**, oder

b) einen Jahresumsatz und eine Jahresbilanzsumme jeweils **über 10 Millionen Euro**

c) Zugehörigkeit zu Anlage 1 oder 2 NIS2UmsuCG

Wer fällt unter das Gesetz? (2)

Unabhängig von der Einrichtungsgröße und als „besonders wichtig“ klassifiziert sind

- qualifizierte Vertrauensdiensteanbieter, Top Level Domain Name Registries oder DNS-Diensteanbieter
- Betreiber kritischer Anlagen (Richtwert: Versorgung von mehr als 500.000 Menschen)
- Einrichtungen der Zentralregierung

Abhängigkeiten zu anderen EU-Regularien

- Unternehmen, die unter DORA erfasst werden, sind voraussichtlich von NIS2 exkludiert

Wer fällt unter das Gesetz? (3)

WICHTIGE EINRICHTUNGEN

ca. 25.000 betroffene Unternehmen

BESONDERS WICHTIGE EINRICHTUNGEN

ca. 5.000-10.000
betroffene Unternehmen

BETREIBER KRITISCHER ANLAGEN

Ca. 2.500-5.000
betroffene Unternehmen

Sicherheit in der Lieferkette

unbekannte Anzahl betroffener Unternehmen weltweit!

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

- **Geschäftsleitungen besonders wichtiger Einrichtungen** und wichtiger Einrichtungen sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden **Risikomanagement-maßnahmen** im Bereich der **Cybersicherheit** zu **billigen und ihre Umsetzung zu überwachen**

- Die **Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen regelmäßig an Schulungen teilnehmen**, um ausreichende Kenntnisse und Fähigkeiten zur **Erkennung und Bewertung von Risiken sowie Risikomanagementpraktiken** im Bereich der Sicherheit in der Informationstechnik und zu **Auswirkungen von Risiken sowie Risikomanagementpraktiken** auf die von der Einrichtung erbrachten Dienste zu erwerben

Das Risikomanagement (1)

- **ISMS:** Konzepte in Bezug auf Risikoanalyse, Sicherheit für Informationssysteme, Bewertung der Wirksamkeit von Maßnahmen, Kryptografie, Identitäts- und Berechtigungsmanagement
- **BCM** und **Krisenmanagement**: Aufrechterhaltung des Betriebs, z. B. Backup-Management und Wiederherstellung nach einem Notfall, Krisenmanagement, gesicherte Notfallkommunikation
- **Lifecycle Management**: Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen (…)
- **Bewältigung von Sicherheitsvorfällen**
- **Awareness**: grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit, Clean Desk
- **Sicherheit des Personals**
- **Sichere Authentifizierung**: Verwendung von Lösungen zu MFA oder zur kontinuierlichen Authentifizierung
- **Sichere Kommunikation**: gesicherte Sprach-, Video- und Textkommunikation
- **Dienstleistersteuerung**: Sicherheit der Lieferkette (…)
- **Krypographie** und **Verschlüsselung**

Das Risikomanagement (2)

Einrichtungen

Technische und organisatorische Maßnahmen (TOMs)

Störungen von VIVA in informationstechnischen Systemen

TOMs

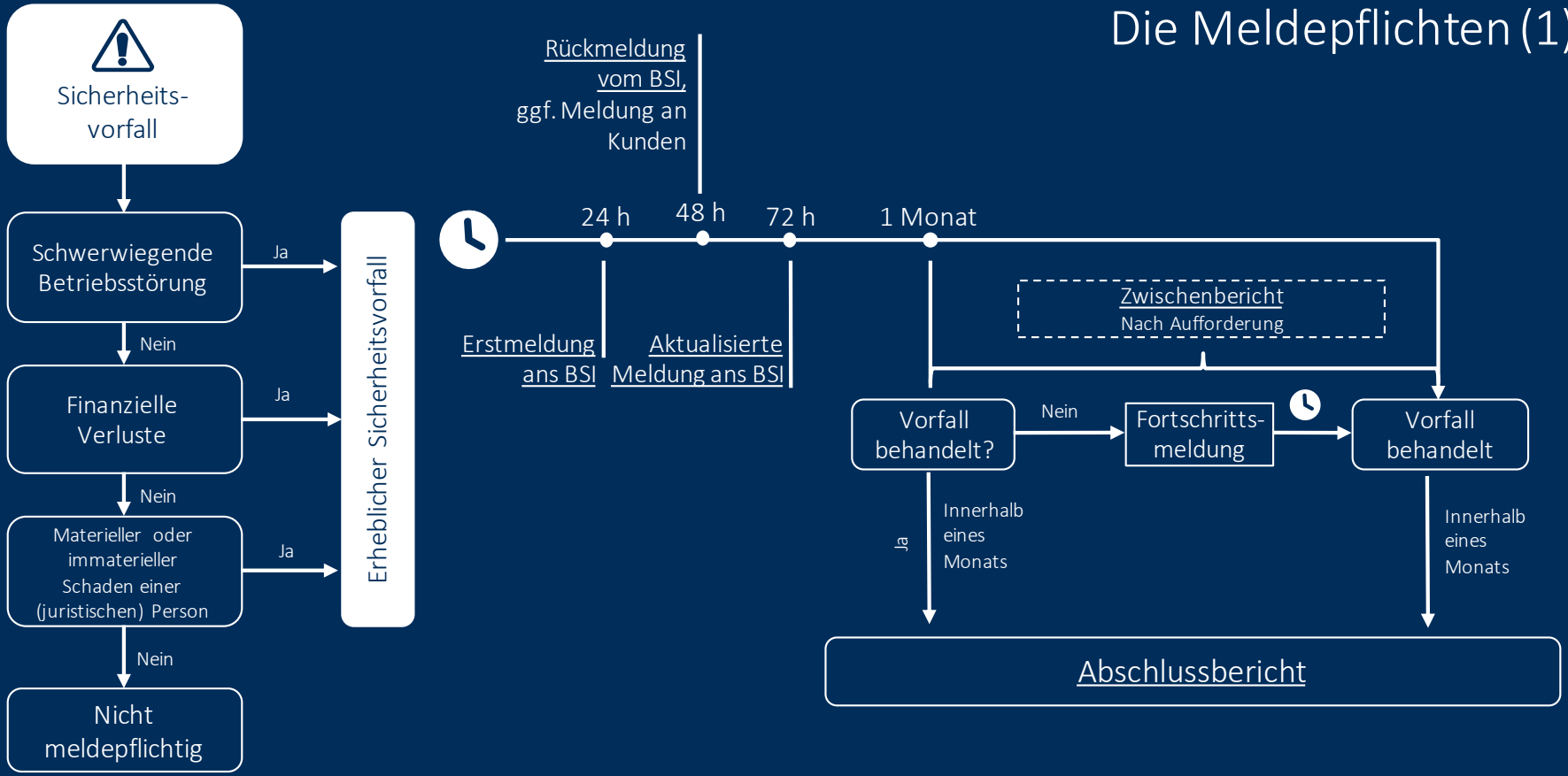
Für **besonders wichtige** und **wichtige Einrichtungen** müssen die Maßnahmen

- geeignet, verhältnismäßig, wirksam, nach Stand der Technik und auf Standards bzw. Normen basierend sein
- ausgewählt werden nach Risikoexposition, Größe der Einrichtung, Umsetzungskosten, Eintrittswahrscheinlichkeit, Schwere von Sicherheitsvorfällen und gesellschaftlichen bzw. wirtschaftlichen Auswirkungen

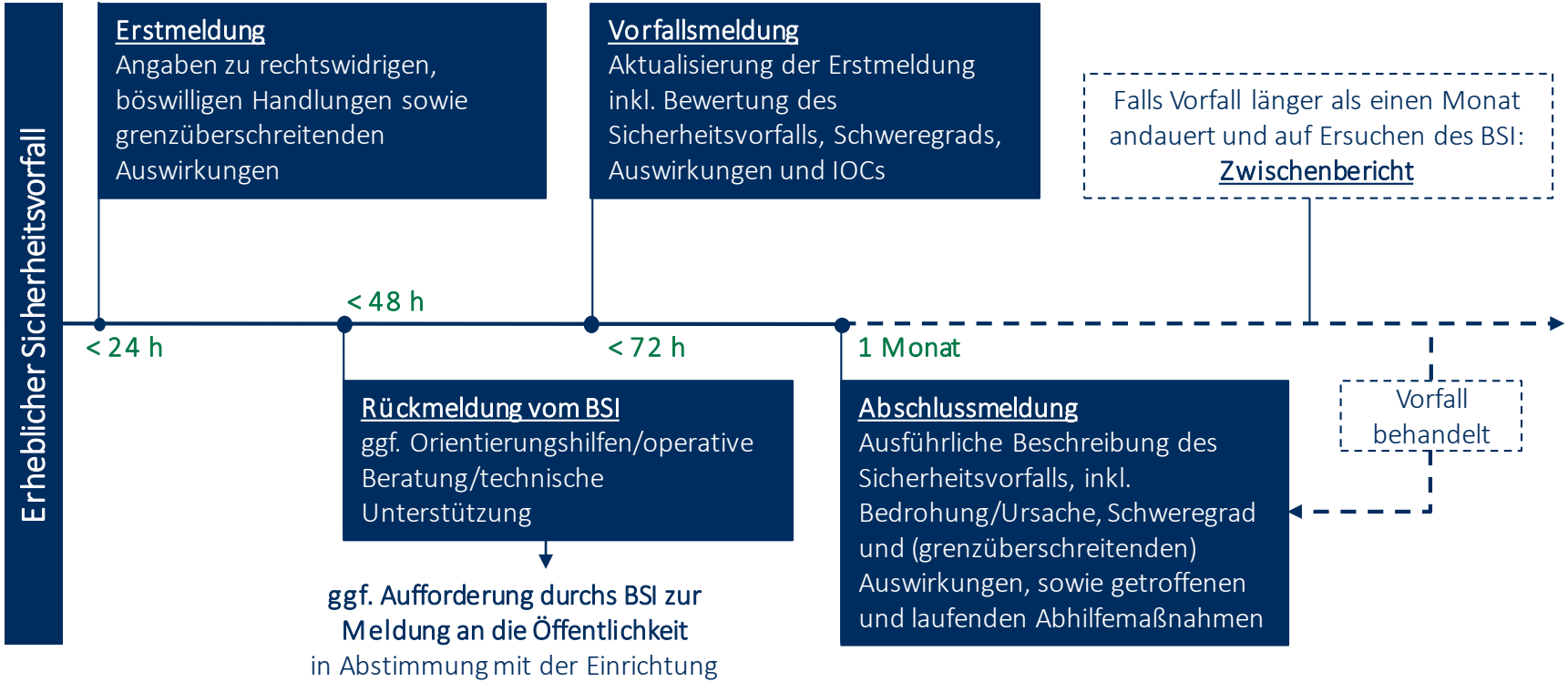
Zusätzlich müssen sie für **Betreiber kritischer Anlagen**:

- geeignet sein, um den in Lageberichten, Bewertungen und Bedrohungsszenarien des BSI geschilderten Szenarien standzuhalten
- Versorgungssicherheit der Dienste auf möglichst hohem Niveau garantieren
- bei aufwändigeren Maßnahmen verhältnismäßig sein, wenn der erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht

Die Meldepflichten (1)



Die Meldepflichten (2)



Die Registrierungspflichten

Besonders wichtige, wichtige Einrichtungen sowie Domain-Name-Registry-Dienste

Frist: innerhalb von drei Monaten

Zu meldende Inhalte

- Name der Einrichtung, Rechtsform und Handelsregisternummer
- Anschrift und aktuelle Kontaktdaten, einschließlich E-Mail-Adresse, IP-Adressbereichen und Telefonnummern,
- Sektor und Teilsektor
- Auflistung der Mitgliedstaaten der EU, in denen die Einrichtung Dienste erbringt

Betreiber kritischer Anlagen

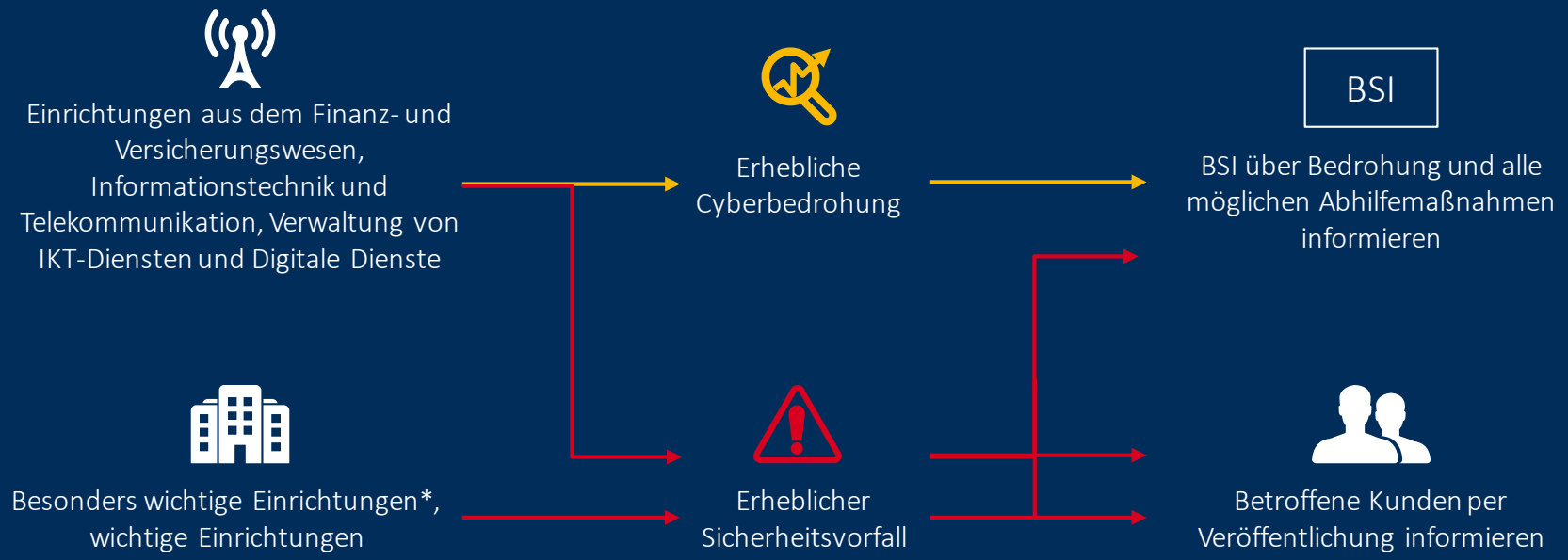
Frist: zum 17. Januar 2025

zusätzlich zu meldende Inhalte

- IP-Adressbereiche der kritischen Anlagen
- Anlagenkategorie
- Versorgungskennzahlen
- Informationen zur jederzeit erreichbaren Kontaktstelle

- Bei ausbleibender Registrierung kann diese durchs BSI vorgenommen werden
- Nachweise über die Registrierung können vom BSI eingefordert werden
- Bei Änderungen sind Versorgungs-kennzahlen einmal jährlich, alle anderen Angaben unverzüglich, spätestens zwei Wochen ab dem Zeitpunkt der Änderung, zu übermitteln

Die Unterrichtungspflichten



***Partizipationspflicht** für besonders wichtige Einrichtungen und Betreiber kritischer Anlagen im **Onlineportal des BSI**

Die Ausweitung der Befugnisse für das BSI (1)

Prüfung der Konformität

- Prüfung der Einhaltung der Maßnahmen
- Prüfung mittels schriftlicher Nachweise und/oder Begehungen
- Unabhängige Dritte dürfen zur Prüfung beauftragt werden
- Kommunikation dieser Dritten erfolgt über das BSI

Anordnung von Maßnahmen

- Das BSI darf Maßnahmen anordnen, ggf. mittels behördenübergreifender Zusammenarbeit (Amtshilfe)
- Maßnahmen dürfen die Umsetzung der Inhalte des NIS2UmsuCG und/oder die Art der Behebung eines Sicherheitsvorfalls vorgeben
- In diesem Zuge können Nachweise eingefordert werden

Die Ausweitung der Befugnisse für das BSI (2)

Veröffentlichung von Informationen

- Anordnung an Einrichtungen zur Information von Kunden über Abwehr- oder Abhilfemaßnahmen bei Cyberbedrohungen
- Veröffentlichung von Verstößen gegen das NIS2UmsuCG durch das BSI möglich

Ernennung von Überwachungsbeauftragten

- Benennung eines Überwachungsbeauftragten für die Einhaltung der Pflichten aus dem NIS2UmsuCG, ggf. mittels behördenübergreifender Zusammenarbeit (Amtshilfe)
- Überwachungsbeauftragte können Interne und Externe sein

Die Ausweitung der Befugnisse für das BSI (3)

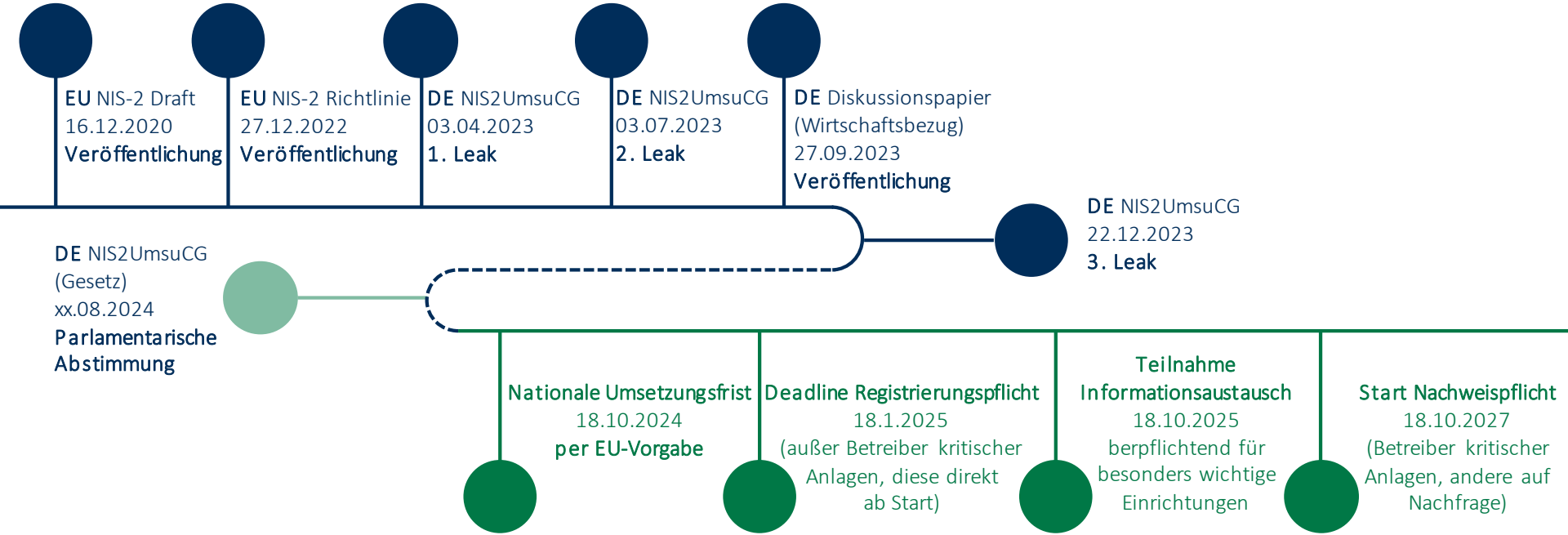
Fristen und Sanktionen

- Fristsetzung für die Umsetzung der angeordneten Maßnahmen
- Möglichkeit der Aussetzung der Genehmigung von Teilen oder aller Dienste/Tätigkeiten einer Einrichtung, ggf. auch mittels behördenübergreifender Zusammenarbeit (Amtshilfe)
- Möglichkeit der Untersagung der Tätigkeiten der Geschäftsführung/der gesetzlichen Vertreter bei Nicht-Erfüllung der Anforderungen, ggf. auch mittels behördenübergreifender Zusammenarbeit (Amtshilfe)
- Sanktionen mit einer Geldbuße bis zu **10 Mio. €** oder einem Höchstbetrag von **min. 2 %** des globalen Jahresumsatzes (besonders wichtige Einrichtungen) bzw. einer Geldbuße bis zu **7 Mio. €** oder **min. 1,4 %** des globalen Jahresumsatzes (wichtige Einrichtungen)

Die potenziellen Strafen (1)

Bereich	Detaillierte Ordnungswidrigkeit	Kritisch	Besonders Wichtig	Wichtig
Risikomanagement	Nachweis wurde nicht, nicht richtig, nicht vollständig, nicht rechtzeitig übermittelt	10.000.000	10.000.000	500.000
	Ungeeignete TOMs	10.000.000	10.000.000	7.000.000
Meldepflicht	Meldepflicht wurde nicht, nicht richtig, nicht vollständig, nicht rechtzeitig befolgt	10.000.000	10.000.000	7.000.000
Anordnung vom BSI	Wiederherstellung der informationstechnischen Systeme nach Aufforderung	2.000.000	2.000.000	2.000.000
	Einschränkung der Telekommunikation bei Störung	2.000.000	2.000.000	2.000.000
	Anweisung zur Umleitung an eine dem BSI bekannte Anschlusskennung	2.000.000	2.000.000	2.000.000
	Anweisung des BSI, Telemedien per TOM wiederherzustellen	2.000.000	2.000.000	2.000.000
	Vorlage eines Mängelbeseitigungsplans	-	2.000.000	-
Urkunden	Handlung als Konformitätsbewertungsstelle ohne Qualifikation dafür	500.000	500.000	500.000
	IT-Sicherheitskennzeichen	500.000	500.000	500.000
	Fälschliche Angabe von BSI-Zertifizierungen	500.000	500.000	500.000
Registrierung	Verzug bei der Frist von 3 Monaten oder bei kritischen Einrichtungen von einem Tag	500.000	500.000	500.000
	Änderung bei Registrierungsdaten nicht innerhalb von zwei Wochen mitgeteilt	500.000	500.000	100.000
	Bei kritischen Einrichtungen Kontaktdaten nicht erreichbar	100.000	-	-
Kooperation mit BSI	Zugang zu Räumlichkeiten nicht gewährt	500.000	500.000	-
	Unzureichende Informationenweitergabe	500.000	500.000	500.000
	Verbindliche Anweisung zur Umsetzung von NIS2UmsuCG nicht Folge geleistet	500.000	500.000	100.000
	Mitwirkungspflicht gegenüber Überwachungsbeauftragten	100.000	100.000	100.000
Hersteller von IKT-Produkten	Fehlende Auskunft (inkl. technischer Details) über verwendete IKT-Produkte ans BSI	100.000	100.000	100.000
	Fehlende Beseitigung von Schwachstellen bei IKT-Produkten, die zu Vorfällen bei kritischen Einrichtungen führen können	100.000	500.000	100.000
Unterrichtungspflicht	Fehlende Unterstützung von Kunden	100.000	100.000	100.000

So geht es weiter



NIS2-Kompass

Betroffenheitsanalyse leicht gemacht!

Schnelle und freie Kurzanalyse unter:

- https://www.hisolutions.com/detail/nis2-kompass

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com