

Umsetzung der EU-NIS2 und des kommenden deutschen Umsetzungsgesetzes (NIS2UmsuCG) in der Deutschen Telekom

ECO-Verband | Christian Sachgau | 17.10.2024



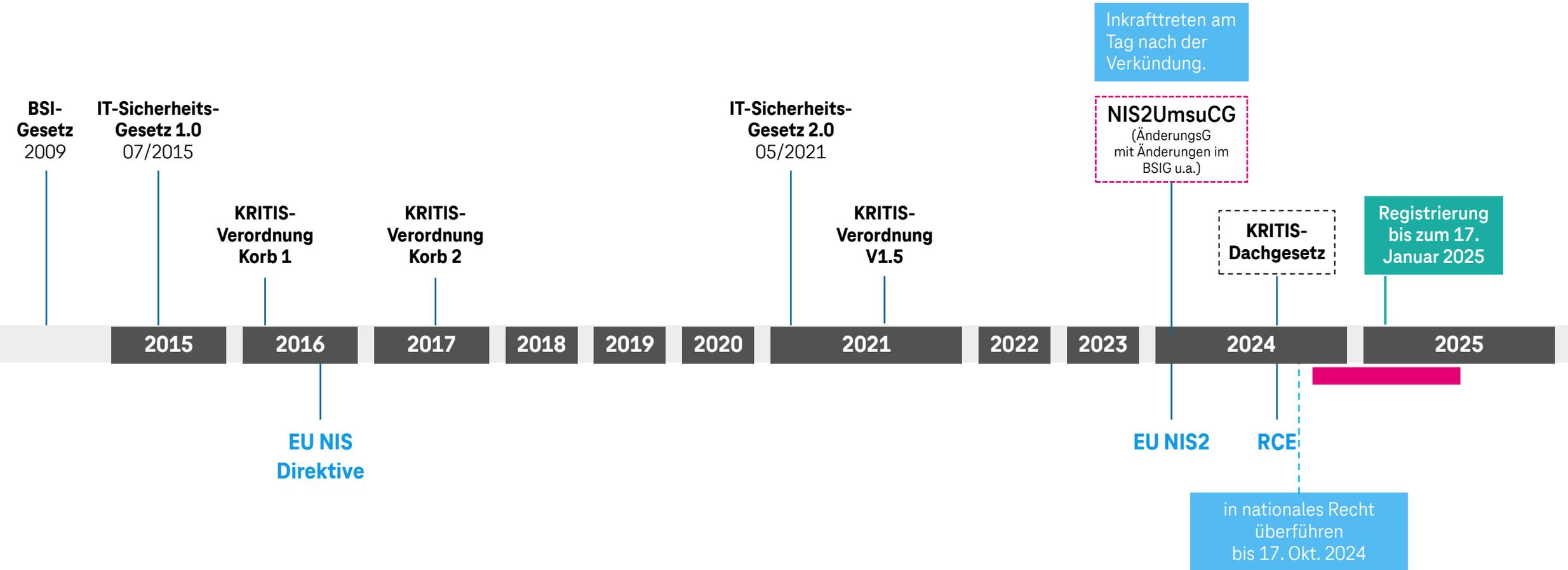
Agenda

- 01** Ausgangssituation
- 02** NIS2 Anforderungen (neu)
- 03** NIS2 Betroffenheits-analyse – Nächste Schritte
- 04** Q&A

01

Ausgangssituation

Zeitstrahl zur Umsetzung der EU NIS und EU NIS2

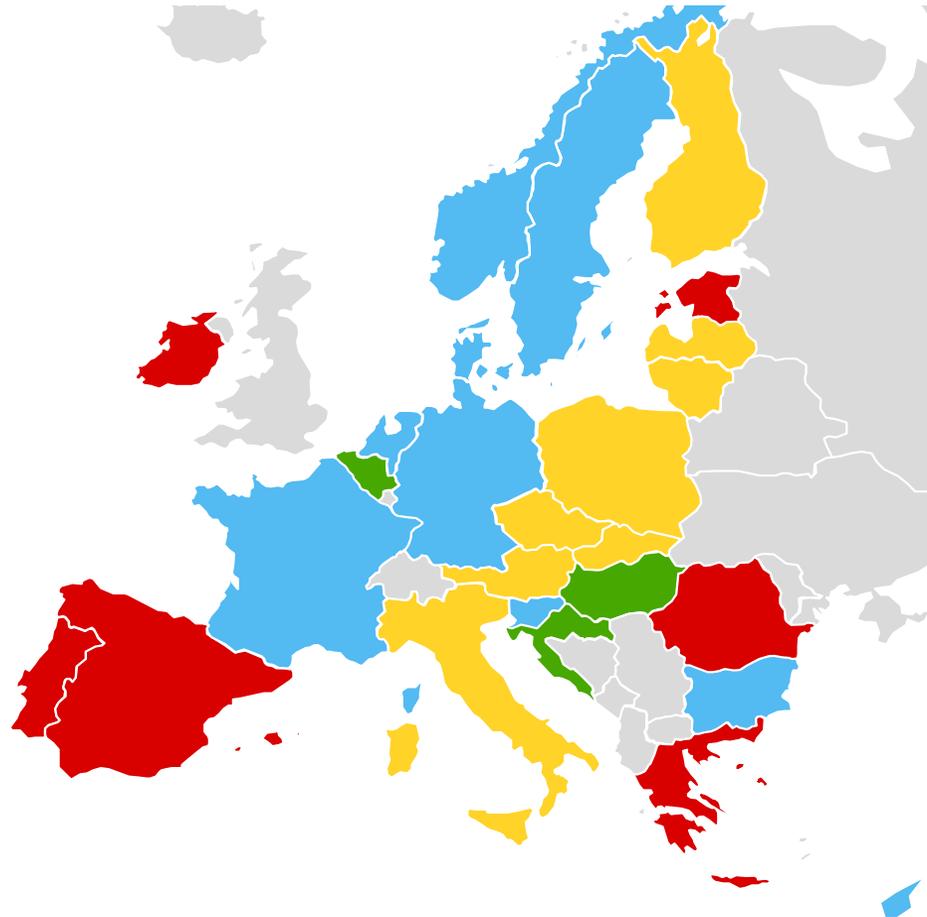


Das NIS2UmsuCG ist die Nachfolgeregelung des ITSiG2.0 und stellt die nationale Umsetzung der EU-Regelung dar. Die Registrierung der Gesellschaften, die unter NIS2 fallen, muss bis spätestens 3 Monate nach Inkrafttreten erfolgen.

Umsetzungsstand in der EU

Inkraftsetzung

Die EU-NIS2 muss in den Mitgliedsstaaten umgesetzt werden bis zum 17.10.2024.



Die EU-NIS2 haben bisher folgende Länder in nationales Recht umgesetzt:

- Belgien ab 17.10.2024
- Ungarn
- Kroatien

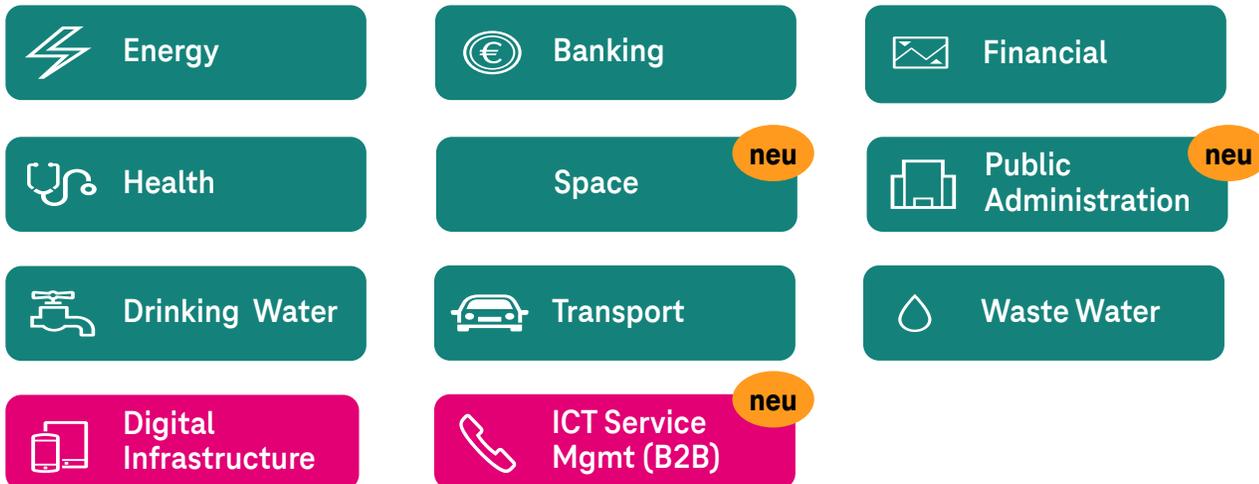
Status

- Umsetzung in nationales Gesetz erfolgt
- Veröffentlichung eines Gesetzesentwurfs
- Konsultationsphase
- Keine Entwicklung

Der Umsetzungsstand der NIS2 in nationales Recht in Europa ist sehr unterschiedlich.

Überblick der von NIS2 betroffenen Sektoren

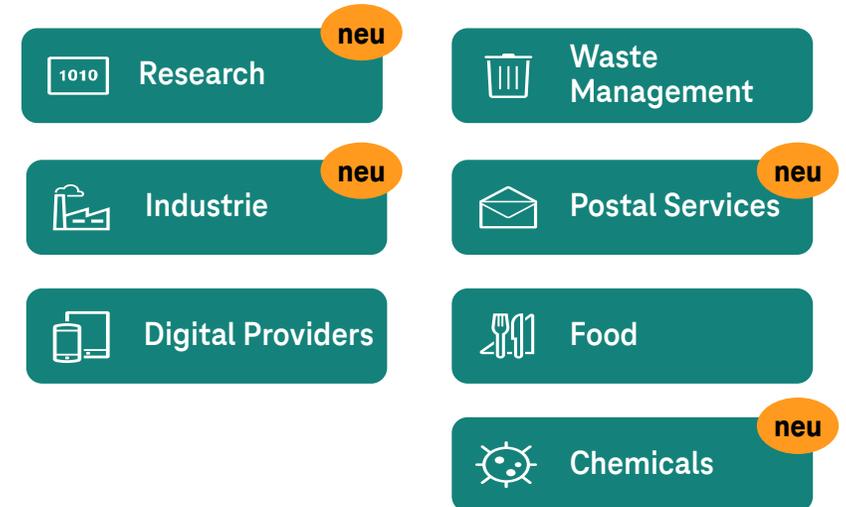
Annex I – Sektoren mit hoher Kritikalität



- Internet Exchange Point providers
- DNS service providers, excluding operators of root name servers
- TLD name registries
- Cloud computing service providers
- Data centre service providers
- Content delivery network providers
- Trust service providers
- Providers of public electronic communications networks
- Providers of publicly available electronic communications services

- Managed service providers (neu)
- Managed security service providers

Annex II – andere kritische Sektoren



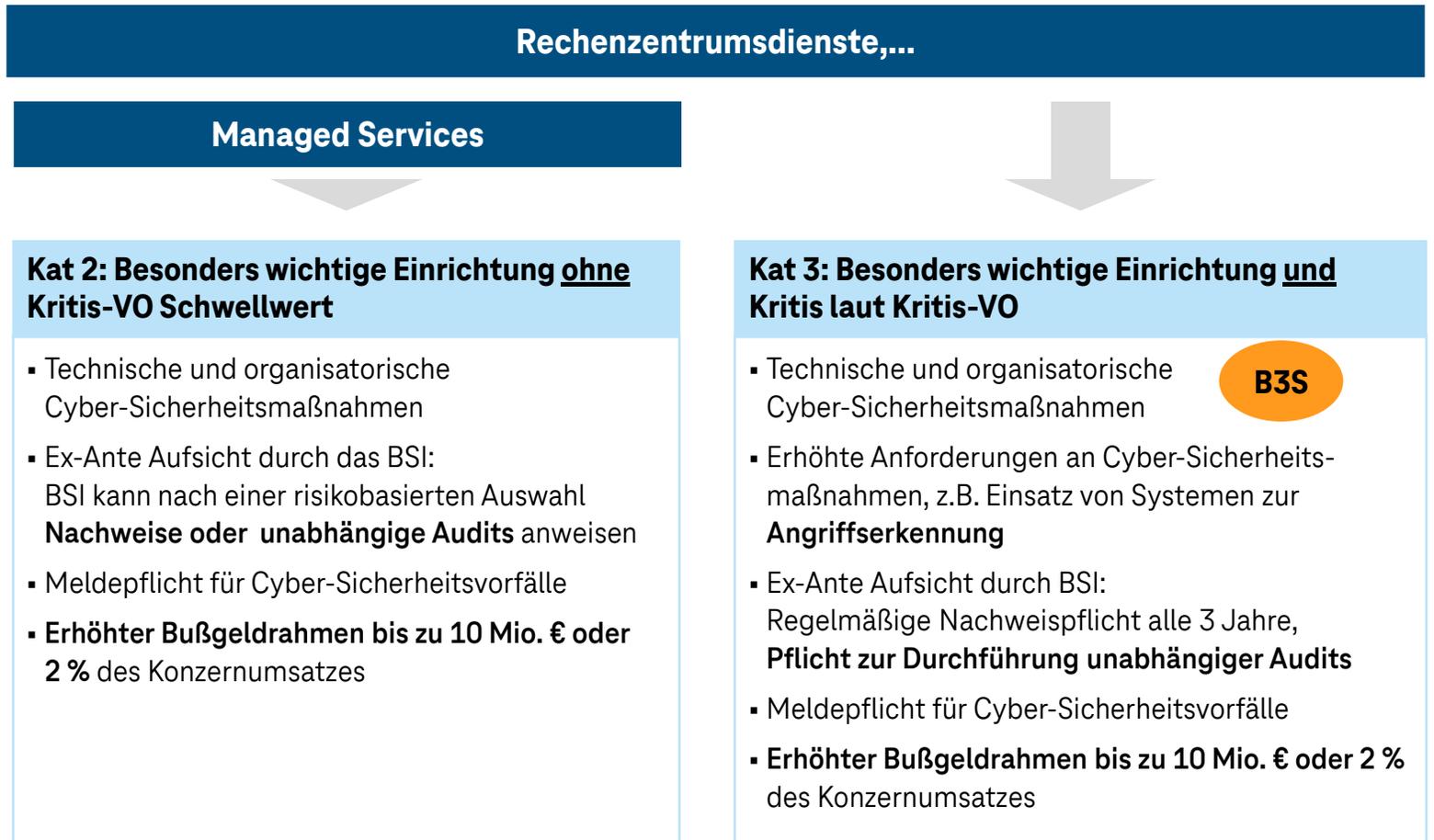
- Providers of online marketplaces
- Providers of online search engines
- Providers of social networking services platforms

Neue Sektoren bzw. Services fallen unter die EU NIS2 im Vergleich zur KRITIS-Verordnung Deutschland.

Bundesamt für Sicherheit in der Informationstechnik

Gesetzentwurf

Kritische Dienstleistungen, die unter die aktuelle Kritis-VO fallen, sind sog. besonders wichtige Einrichtungen mit zusätzlichen Anforderungen nach deutschem Recht und werden regelmäßig auditiert.



In der deutschen Ausgestaltung der NIS2 gibt es jetzt 3 Kategorien (wichtig, besonders wichtig, KRITIS), statt nur KRITIS.

DTAG relevante Services in der NIS2

Digitale Dienste: Identifizierung des europaweiten TS-Portfolios und zentrale Registrierung beim BSI in Deutschland

Cloud Computing Service

Ein digitaler Dienst, der eine On-Demand-Verwaltung und einen umfassenden Fernzugriff auf einen skalierbaren und elastischen Pool gemeinsam nutzbarer Rechenressourcen ermöglicht, auch wenn diese Ressourcen auf mehrere Standorte verteilt sind; zum Beispiel IaaS, PaaS, SaaS

Data Center Service

Eine Dienstleistung, die Strukturen oder Gruppen von Strukturen umfasst, die der zentralen Unterbringung, Vernetzung und dem Betrieb von IT- und Netzwerkgeräten gewidmet sind und Datenspeicher-, -verarbeitungs- und -transportdienste zusammen mit allen Einrichtungen und Infrastrukturen für die Energieverteilung und Umweltkontrolle erbringen, und wird mit Housing bzw. Hosting bezeichnet.

Managed Service Provider

Eine Stelle, die Dienstleistungen im Zusammenhang mit der Installation, dem Management, dem Betrieb oder der Wartung von IKT-Produkten, -Netzen, -Infrastrukturen, -Anwendungen oder anderen Netz- und Informationssystemen erbringt, und zwar durch Unterstützung oder aktive Verwaltung, die entweder in den Räumlichkeiten der Kunden oder aus der Ferne durchgeführt wird.

Managed Security Service Provider

Ein Managed Service Provider, der Tätigkeiten im Zusammenhang mit dem Cybersicherheitsrisikomanagement durchführt oder unterstützt

TK-Dienste: Registrierung im betroffenen Land

Public Electronic Communications Network

Internetzugangsdienste, interpersonelle Kommunikationsdienste

Electronic Communication Services

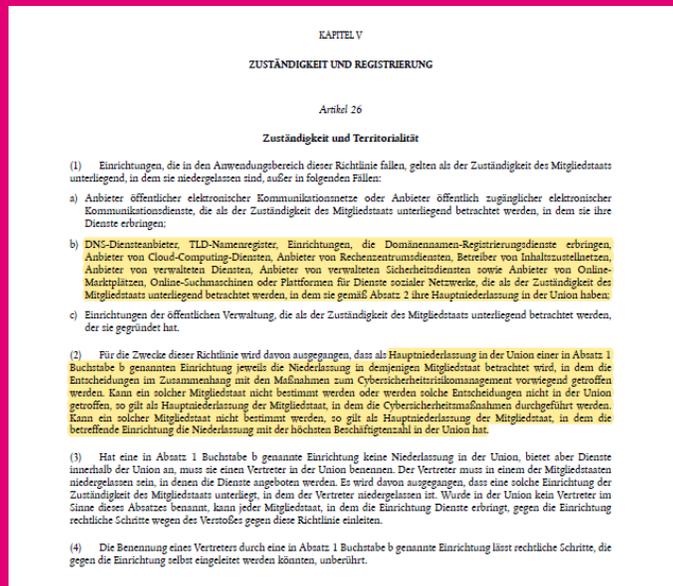
Internetzugangsdienste, interpersonelle Kommunikationsdienste und Dienste, die ganz oder überwiegend in der Übertragung von Signalen bestehen, wie z. B. Übertragungsdienste, die für die Erbringung von Maschine-Maschine-Diensten und für den Rundfunk verwendet werden; ein öffentliches elektronisches Kommunikationsnetz im Sinne von Art. 2, Nr. 8/Nr. 4 EU 2018/1972

Von den Sektoren und Services, die unter die NIS2 fallen sind vier Services insbesondere für den Konzern relevant.

Artikel 26 Abs. 1 NIS2 – Territorialität Digitale Dienste

Grundsatz

Zuständigkeit für die Umsetzung der Anforderungen liegen grundsätzlich in dem Mitgliedsstaat, in dem das Unternehmen niedergelassen ist.



Ausnahme

Ausnahme – IT -Services

Zuständigkeit in dem Mitgliedsstaat, in dem die **Hauptniederlassung ihren Sitz hat** für alle EU-Tochter (Art. 26II)

[...] DNS-Diensteanbieter, TLD-Namenregister, Einrichtungen, die Domännennamen-Registrierungsdienste erbringen, Anbieter von **Cloud-Computing-Diensten**, Anbieter von **Rechenzentrumsdiensten**, Betreiber von Inhaltzustellnetzen, **Anbieter von verwalteten Diensten**, **Anbieter von verwalteten Sicherheitsdiensten** [...] die als der Zuständigkeit des Mitgliedsstaats unterliegend betrachtet werden, in dem sie gemäß Absatz 2 ihre Hauptniederlassung in der Union haben; [...]

Identifikation + Zentrale Registrierung

Zentrale Steuerung durch Hauptniederlassung DE.

Artikel 26 Abs. 1 NIS2 (Territorialität)



**Hauptniederlassung
Deutschland**

Meldungen
zentrale
Registrierung

Zuständige Behörde in Deutschland: BSI



Das BSI ist zuständig in Deutschland für:

- EU-weit angebotene Cloud-Computing-Dienste,
- Anbieter von Rechenzentrumsdiensten,
- Anbieter von verwalteten Diensten,
- Anbieter von verwalteten Sicherheitsdiensten,

die konzernweit innerhalb der Telekom Gruppe in den Bereichen Europe, TDG, TSI angeboten werden.

Damit erfolgt eine zentrale Registrierung, Meldungen, Überwachung für o.g. Dienste.

EW 114 NIS2, Art. 26 I NIS2

Hauptniederlassung ist:

Der betrachtete Mitgliedstaat, in dem die Entscheidungen im Zusammenhang mit den Maßnahmen zum Cybersicherheits-Risikomanagement vorwiegend getroffen werden.

Falls nicht zu bestimmen:
der Mitgliedstaat, in dem die Cybersicherheitsmaßnahmen durchgeführt werden.

Falls nicht zu bestimmen:
der Mitgliedstaat, in dem die betreffende Einrichtung die Niederlassung mit der höchsten Beschäftigtenzahl in der Union hat.



Hauptniederlassung Deutschland



**Cloud / Rechenzentrumsdienste /
Managed Services /
Managed Security Services ...**



Rechenzentrum der Telekom Gruppe in der EU

02

NIS2 Anforderungen (neu)

NIS2 Risiko: Haftung der Geschäftsführung

Was ist zu überwachen?

Article 20

Governance

1. Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article.

The application of this paragraph shall be without prejudice to national law as regards the liability rules applicable to public institutions, as well as the liability of public servants and elected or appointed officials.

27.12.2022 EN Official Journal of the European Union L 333/127

2. Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.

Die Geschäftsführung besonders wichtiger und wichtiger Einrichtungen

- soll die Maßnahmen zum Risikomanagement im Bereich der Cybersicherheit genehmigen und
- kann haftbar gemacht werden.

Das Management (GF) hat

- an Schulungen teilzunehmen und
- ihren Mitarbeitern regelmäßig ähnliche Schulungen anzubieten.

Die Geschäftsführung haftet persönlich und trägt Umsetzungsverantwortung.

NIS2 Risiko: Umzusetzende 10 Handlungsfelder

Was ist zu implementieren und zu pflegen?

(2) Die in Absatz 1 genannten Maßnahmen müssen auf einem gefahrenübergreifenden Ansatz beruhen, der darauf abzielt, die Netz- und Informationssysteme und die physische Umwelt dieser Systeme vor Sicherheitsvorfällen zu schützen, und zumindest Folgendes umfassen:

- a) Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme;
- b) Bewältigung von Sicherheitsvorfällen;
- c) Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement;
- d) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern;
- e) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen;
- f) Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit;
- g) grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit;
- h) Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung;
- i) Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen;
- j) Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

1 Risikoanalyse
Policies

3 BCM; DRC..(ISO 22301)

5 Wartung und
Schwachstellenmanagement

7 Schulung der Geschäftsführung

9 HR Sicherheit
Sicherheitsüberprüfung Personal
Klassifizierung von Assets

2 Incident Handling

4 Sicherheit der Lieferkette

6 Wirksamkeitsprüfung

8 Kryptografie

10 Multi-Faktor-Authentifizierung

Für einige Themen besteht noch Handlungsbedarf.

NIS2 Risiko: Reporting Anforderungen

What to report?

- Incident**
3. An incident shall be considered to be significant if:
- (a) it has caused or is capable of causing severe operational disruption of the services or financial loss for the entity concerned;
 - (b) it has affected or is capable of affecting other natural or legal persons by causing considerable material or non-material damage.
4. Member States shall ensure that, for the purpose of notification under paragraph 1, the entities concerned submit to the CSIRT or, where applicable, the competent authority:
- (a) without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact;
 - (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise;
 - (c) upon the request of a CSIRT or, where applicable, the competent authority, an intermediate report on relevant status updates;
 - (d) a final report not later than one month after the submission of the incident notification under point (b), including the following:
 - (i) a detailed description of the incident, including its severity and impact;
 - (ii) the type of threat or root cause that is likely to have triggered the incident;
 - (iii) applied and ongoing mitigation measures;
 - (iv) where applicable, the cross-border impact of the incident;
 - (e) in the event of an ongoing incident at the time of the submission of the final report referred to in point (d), Member States shall ensure that entities concerned provide a progress report at that time and a final report within one month of their handling of the incident.
- Reporting**

<https://eur-lex.europa.eu/eli/dir/2022/2555>

**Unterbrechung der Dienstleistungen
oder
finanzieller Verlust**

**Zahl der betroffenen Personen
durch
materielle oder immaterielle Schäden**

 **24 h**

**Frühzeitige Warnung ohne
unangemessene Verzögerung**

 **72 h**

Aktualisierung des Incidents

 **1 Monat**

**Abschließender detaillierter Bericht
mit Infos zu:**

- Grenzüberschreitenden Auswirkungen
- Art der Bedrohung oder Ursache
- Angewandte und laufende Maßnahmen

Alle EU Incidents von relevanten IT-Diensten müssen an das BSI gemeldet werden.

03

NIS2 Betroffenheitsanalyse – nächste Schritte

Handlungsfelder NIS2 Umsetzung in Konzern

Nr.	Handlungsfeld	Beschreibung
1	Betroffenheitsanalyse	Identifikation aller verbundenen Unternehmen durch Information, Interview und dokumentierter Abfrage
2	NIS2 Governance	...durch Critical Infrastructure Compliance Rules
3	Registrierung aller Services an Behörden	a) in Deutschland (BSI) und b) die dem Territorialitätsprinzip unterliegen (BSI) c) sowie lokale Registrierung (EU)
4	NIS2 Assessment	... bezogen auf Readiness und den Anforderungen aus NIS2UmsuCG, nationalen Anforderungen durch Orientierungshilfen BSI, Implementing Acts, etc.
5	NIS2 Maßnahmen	...schließen von GAPs
6	Schulungen und Trainings	Geschäftsführung und Mitarbeiter:innen
7	Monitoring und Control, Verbesserung	...bezogen auf Nachweisverpflichtungen bzw. KRITIS Audits u.a.

Vorgehen NIS2 Betroffenheitsanalyse

1 Betroffenheitsanalyse

Identifikation aller verbundenen Unternehmen durch Information, Interview und dokumentierter Abfrage



Aufgaben in Abhängigkeit der Zuständigkeit nach NIS2.0, Artikel 26

HQ	Registrierung und Meldungen müssen im Land des Headquarters (HQ) erfolgen. Die Umsetzung erfolgt für alle Dienste zentral in Deutschland . → Landesgesellschaften sind verantwortlich, alle notwendigen Informationen zu liefern.
L	Registrierung und Meldungen müssen im EU Land mit Sitz der Legaleinheit (L = Local) bzw. in allen EU Ländern erfolgen, in denen der Dienst erbracht wird (S = Service).
S	→ Die Umsetzungsverantwortung obliegt der betroffenen Landesgesellschaft Hinweis: Für Deutschland werden diese Dienste zentral registriert.

Sektor Digitale Infrastruktur		Zuständigkeit
<input type="checkbox"/>	Betreiber von Internet-Knoten (Internet Exchange Points (IXP))	L
<input type="checkbox"/>	DNS-Diensteanbieter, ausgenommen Betreiber von Root-Namenservern	HQ
<input type="checkbox"/>	Top Level Domain (TLD) -Namenregister	
<input type="checkbox"/>	Anbieter von Cloud-Computing-Diensten	
<input type="checkbox"/>	Anbieter von Rechenzentrumsdiensten	L
<input type="checkbox"/>	Betreiber von Inhaltszustellnetzen (<i>Content Delivery Netzwerken (CDN)</i>)	
<input type="checkbox"/>	Vertrauensdiensteanbieter	S
<input type="checkbox"/>	Qualifizierter Vertrauensdiensteanbieter	
<input type="checkbox"/>	Anbieter öffentlicher elektronischer Kommunikationsnetze oder	
<input type="checkbox"/>	Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste	
Sektor Verwaltung von IKT-Diensten (Business-to-Business)		
<input type="checkbox"/>	Anbieter verwalteter Dienste (Managed Services)	HQ
<input type="checkbox"/>	Anbieter verwalteter Sicherheitsdienste (Managed Security Services)	
Sektor Digitale Anbieter		
<input type="checkbox"/>	Online Marktplätze	HQ
<input type="checkbox"/>	Suchmaschinen	
<input type="checkbox"/>	Soziale Netzwerke	

Start der Betroffenheitsanalyse

Ein großer Konzern ist komplex

ca. 620

Legaleinheiten

ca. 350

Legaleinheit mit Hauptsitz in der Europäischen Union

ca. 150

Legaleinheiten, die möglicherweise unter die Gesetzgebung fallen

ca. 60-100

Legaleinheiten, die registriert werden müssen



NIS2 Umsetzung 1/2

2 NIS2 Governance

...durch Critical Infrastructure
Compliance Rules



Inhaltsverzeichnis

Abbildungsverzeichnis	6
Tabellenverzeichnis	7
1 Einleitung	8
1.1 Geltungsbereich der Regelung	8
1.2 Gesetzliche Grundlagen	8
2 Betroffenheit, Kategorie & Zuständigkeit	9
2.1 Sektoren (Branchen) und zugeordnete Kategorien	9
2.2 Zuständigkeit "Territorialität" nach NIS2, Artikel 2e)	10
3 Anforderungen (Maßnahmen)	12
3.1 Übersicht	12
3.2 Organisatorische Anforderungen und Regelungen	12
3.3 Risikomanagementmaßnahmen im Bereich der Cybersicherheit	13
3.4 Weitergehende Anforderungen und Regelungen	14
4 Rollen & Aufgaben	15
4.1 Verantwortlichkeiten und Rollen	15
4.2 Geschäftsleitung (Legaleinheit/Unit)	15
4.3 Group Security/Deutsche Telekom Security (DT-Sec)	15
4.4 Security Officer	17
4.5 KRITIS-Manager (CRITIS-Manager)	17
4.6 KRITIS-Koordinator	18
Mitgeltende Unterlagen	19
Abkürzungsverzeichnis/Glossar	20

Diese Guideline soll abgeleitete Verantwortlichkeiten, Aufgaben und technisch/organisatorische **Cyber-Security** und **Resilience (BCM)** Maßnahmen innerhalb der DTAG beschreiben.

Regelwerk zur kritischen Infrastruktur befindet sich im Entwurf.

04

Q&A