EU – NIS 2 und EU - CRE

Verordnete IT- Sicherheit ! – Was jetzt zu tun ist

EU – NIS 2 und EU - CRE

Die neuen Gesetze im Überblick

EU-Richtlinien		Nationale Umsetzung (DE)
NIS 2 – Directive (EU 2022/2555)	→	NIS 2- Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)
EU – CRE (EU 2022/2557)	→	KRITIS- Dachgesetz (KRITIS-DachG)
Am 12.03.24 im EU- Parlament beschlossen EU - CRA - Directive	→	noch ausstehend

EU – NIS 2 und EU - CRE

Sektoren & Schwellenwerte EU- CRE

Anlagen KRITIS-Sektoren (EU-CRE)

Energie
u.a. Strom, Fernwärme und -kälte, Erdöl, Gas, Wasserstoff

Verkehr
u.a. Luftfahrt, Schienenverkehr, Schifffahrt, Straßenverkehr

Bankwesen
u.a. Kreditinstitute

Finanzmarktinfrastrukturen
u.a. Handelsplätze, CCP's

Digitale Infrastruktur
u.a. Internet-Knoten, DNS, TLD, Cloud-Computing, Rechenzentrumsdienste, Inhaltszustellnetze, Vertrauensdienste, elektr. Kommunikationsnetze

Produktion, Verarbeitung- und Vertrieb von Lebensmitteln

Gesundheit
u.a. Gesundheitsdienstleister, Referenzlaboratorien, Forschungs- und Entwicklung von Arzneimitteln, Herstellung von pharmazeutischen Erzeugnissen, Medizinprodukte- Herstellung, Großhändler

Öffentliche Verwaltung
u.a. Einrichtungen der Zentralregierungen

Trinkwasser Lieferanten

Abwasser Entsorger

Weltraum
u.a. Bodeninfrastrukturen

Schwellenwerte können derzeit aus der KritisV entnommen werden

- Anhang 2 (zu § 1 Nummer 4 und 5, § 3 Absatz 4 Nummer 1 und 2) Anlagenkategorien und Schwellenwerte im Sektor Wasser

BSI-KritisV - nichtamtliches Inhaltsverzeichnis (gesetze-im-internet.de)

EU – NIS 2 und EU - CRE

Sektoren & Schwellenwerte EU - NIS2

Sektoren der Anlage 1 (NIS-Richtlinie)

Energie
u.a. Stromversorgung, Fernwärme und -kälte- Versorgung & Gasversorgung

Finanz- und Versicherungswesen
u.a. Bankwesen & Finanzmarktinfrastruktur

Wasser und Abwasser
u.a. Trinkwasserversorgung & Abwasserversorgung

Informationstechnik und Telekomunikation
u.a. DNS-Anbieter, Anbieter von Rechenzentrumsdiensten

Transport und Verkehr
u.a. Luftverkehr, Schienenverkehr, Schifffahrt & Straßenverkehr

Gesundheit
u.a. Erbringer von Gesundheitsdienstleistungen, Unternehmen, die Forschungs- und Entwicklungstätigkeiten in Bezug auf Arzneimittel im Sinne des § 2 AMG ausüben

Weltraum
u.a. Betreiber von Bodeninfrastrukturen

EU – NIS 2 und EU - CRE

Sektoren & Schwellenwerte EU - NIS2

Sektoren der Anlage 2 (NIS-Richtlinie)

Transport und Verkehr
u.a. Post- und Kurierdienste

Produktion, Herstellung und Handel von chemischen Stoffen
u.a. Unternehmen im Sinne des Artikels 3 Nummern 9 und 14 der Verordnung (EG) Nr. 1907/2006

Anbieter digitaler Dienste
u.a. Online-Marktplätze, Suchmaschinen, Soziale Netzwerke

Forschung
u.a. Forschungseinrichtungen

Siedlungsabfallentsorgung
u.a. Unternehmen der Abfallbewirtschaftung im Sinne des § 3 Abs. 14 KrWG

Produktion, Verarbeitung und Vertrieb von Lebensmitteln
u.a. Lebensmittelunternehmen im Sinne des Artikels 3 Nummer 2 der Verordnung (EG) Nr. 178/2002

Verarbeitendes Gewerbe/Herstellung von Waren
u.a. Herstellung von Medizinprodukten und In-vitro-Diagnostika, Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, Maschinenbau, Herstellung von Kraftwagen und Kraftwagenteilen & sonstiger Fahrzeugbau

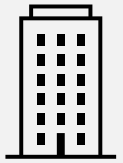
EU – NIS 2 und EU - CRE

Unternehmensgrößen NIS2

große Einrichtungen

Ab 250 Mitarbeiter
----- oder -----
Mehr als 50 Mio. EUR Jahresumsatz
Und
Mehr als 43 Mio. EUR Jahresbilanzsumme

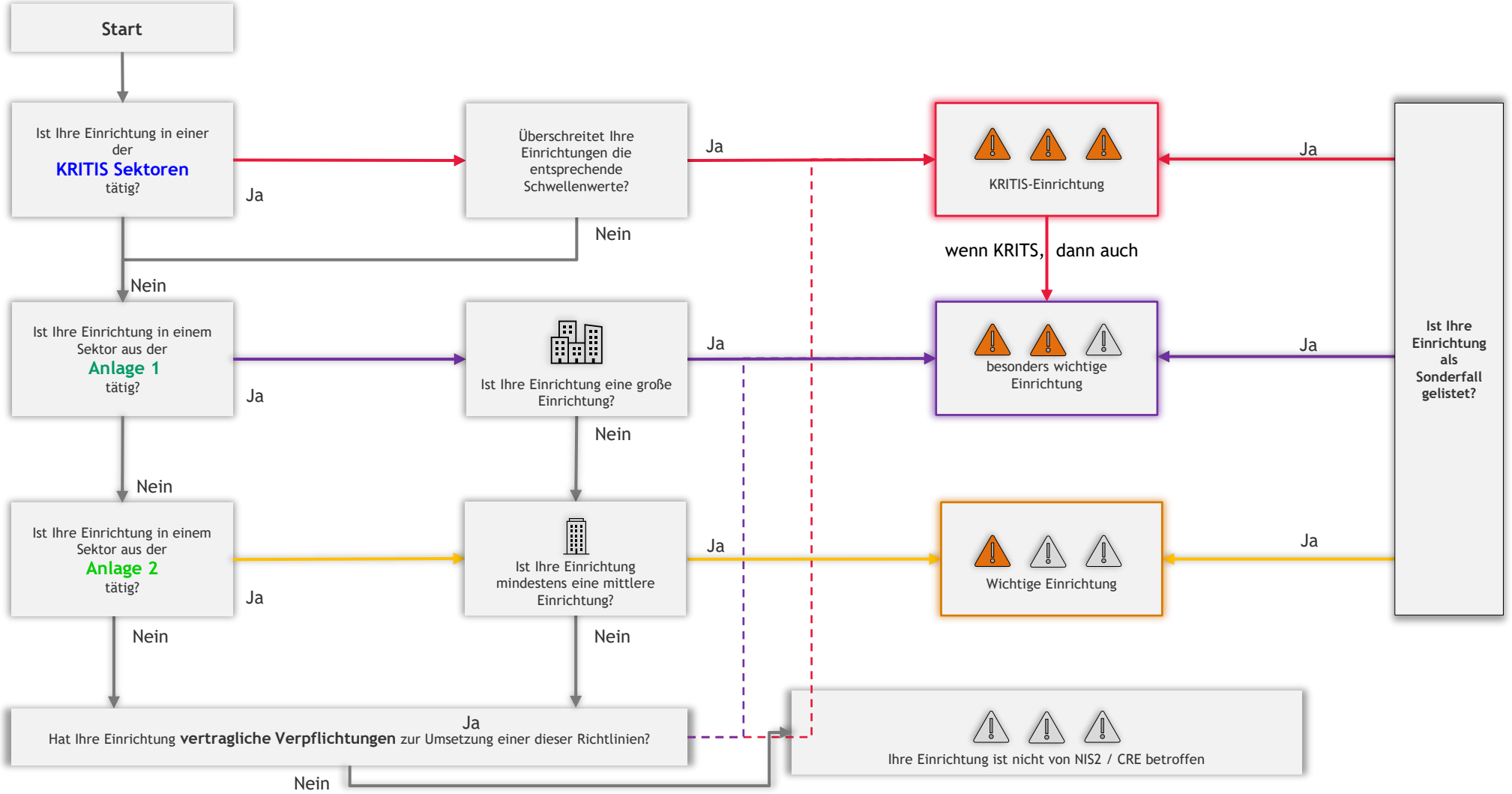
mittlere Einrichtungen



Ab 50 Mitarbeiter
----- oder -----
Mehr als 10 Mio. EUR Jahresumsatz
Und
Mehr als 10 Mio. EUR Jahresbilanzsumme

EU – NIS 2 und EU - CRE

Was trifft auf mich zu ?



EU – NIS 2 und EU - CRE

Sonderfälle

Importanzkategorie	Sonderfälle
KRITIS - Einrichtungen	• Für Einrichtungen aus den Sektoren **Banken, Finanzmarktinfrastruktur** und **digitale Infrastruktur** (Nummer 3,4 und 8 aus dem Gesetzesanhang) gelten die Artikel 11 und die Kapitel III, IV und VI der EU-CRE **nicht**. Die Inhalte der Artikel werden durch andere Richtlinien und Gesetze (z.B. DORA) abgedeckt und verschärft.

Besonders wichtige Einrichtungen	• Anbieter von **Telekommunikationsdiensten** oder **öffentlich zugänglichen Telekommunikationsnetzen**, die mindestens **der Größe einer mittleren Einrichtung** entsprechen, sind auch der Kategorie besonders wichtige Einrichtung zuzuordnen.
	• **Unabhängig der Größe** sind folgende Einrichtungen der Kategorie besonders wichtige Einrichtung zuzuordnen:
	  • Alle KRITIS - Einrichtungen sind auch automatisch besonders wichtige Einrichtungen nach NIS2
	  • Qualifizierte Vertrauensdienstanbieter
	  • Top Level Domain Registries
	  • DNS-Dienstleister
	  • Alle Einrichtungen die gemäß Anlage 3 dem Teilsektor **Zentralregierung** des Sektors **öffentliche Verwaltung** angehören.
	  (Diese Anlage ist aktuell noch nicht veröffentlicht)
	• **Finanzunternehmen** im Sinne des Artikels 2 Absatz 2 der Verordnung (EU) 2022/2554 sind dieser Kategorie **nicht** zuzuordnen.

Wichtige Einrichtungen	• Vertrauensdienstanbieter sind **unabhängig ihrer Größe mindestens** in die Kategorie der **wichtigen Einrichtungen** zuzuordnen.

EU – NIS 2 und EU - CRE

Umzusetzende Maßnahmen

Risikomanagementmaßnahmen	KRITIS-Einrichtung	Besonders wichtige Einrichtung	Wichtige Einrichtung
 Das Auftreten von Vorfällen verhindern ▶ Umsetzung erweiterter (physischer) Maßnahmen der Notfallvorsorge u.a ○ Maßnahmen zur Anpassung an den Klimawandel ○ Maßnahmen zur Bewältigung von Katastrophenfällen	✓		
 Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme umsetzen, z.B. mit Hilfe von ▶ ISMS auf Basis der ISO 27001 oder ▶ ISMS auf Basis der BSI 200-2 und BSI 200-3	✓	✓	✓
 Verwendung von Lösungen zur ▶ Multi-Faktor Authentifizierung oder kontinuierlichen Authentifizierung, ▶ gesicherte Sprach-, Video- und Textkommunikation sowie ▶ gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung	✓	✓	✓
 Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung etablieren, z.B.: ▶ Proprietäre Festplattenverschlüsselung und Verschlüsselung von Laufwerken, ▶ verschlüsselte Kommunikation (WLAN, Server, E-Mails, etc.)	✓	✓	✓

EU – NIS 2 und EU - CRE

Umzusetzende Maßnahmen

Risikomanagementmaßnahmen	KRITIS-Einrichtung	Besonders wichtige Einrichtung	Wichtige Einrichtung
 Sicherheitsmaßnahmen und Konzepte zu folgenden Zwecken etablieren ▶ Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und ▶ Offenlegung und Verwaltung von Schwachstellen	✓	✓	✓
 Reaktion, Abwehr und Begrenzung der negativen Auswirkungen eines Vorfalls durch: ▶ Risiko- und Krisenmanagementverfahren und -protokollen und ▶ vorgegebenen Abläufen im Alarmfall (z.B. durch ein BCM inkl. Notfallhandbuch)	✓		
 Bewältigung von Sicherheitsvorfällen z.B. durch ▶ Einführung von Business Continuity Management (BCM) und ▶ eines Notfallhandbuch mit Checklisten	✓	✓	✓
 Aufrechterhaltung und Wiederherstellung der kritischen Dienstleistungen nach Vorfällen gewährleisten z.B. durch ▶ technischen Maßnahmen, wie Notstromversorgung, ▶ organisatorische Maßnahmen wie alternative Lieferketten, … ▶ Regulatorische Maßnahmen, wie Business Continuity Management für alle kritischen Prozesse	✓		

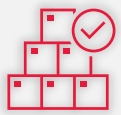
EU – NIS 2 und EU - CRE

Umzusetzende Maßnahmen

Risikomanagementmaßnahmen	KRITIS-Einrichtung	Besonders wichtige Einrichtung	Wichtige Einrichtung
 Aufrechterhaltung des Betriebs, durch Konzepte wie z.B. ▶ Backup-Management und ▶ Wiederherstellung nach einem Notfall und ▶ Krisenmanagement	✓	✓	✓
 Sicherheitsmanagement der Mitarbeiter, einschließlich des Personals externer Dienstleister ▶ die Festlegung • von Kategorien von Personal, das kritische Funktionen wahrnimmt, • von Zugangsrechten zu Liegenschaften, kritischen Anlagen und zu sensiblen Informationen sowie • von angemessenen Schulungsanforderungen und Qualifikationen ▶ Einführung von Verfahren für Zuverlässigkeitsüberprüfungen und die Benennung von Kategorien von Personal, die Zuverlässigkeitsüberprüfungen durchlaufen müssen	✓		
 Sicherheit des Personals durch Konzepte für die Zugriffskontrolle und das Management von Anlagen, u.a. ▶ Schließanlagen, Videoüberwachungen in speziellen Bereichen ▶ Zutrittsberechtigungen, Zugriffsdokumentation, Kontrollen	✓	✓	✓
 Besondere Maßnahmen für das Personal, das KRITIS-Maßnahmen umsetzt ▶ regelmäßige Schulung und Qualifikation ▶ Durchführung von Übungen	✓		

EU – NIS 2 und EU - CRE

Umzusetzende Maßnahmen

Risikomanagementmaßnahmen	KRITIS-Einrichtung	Besonders wichtige Einrichtung	Wichtige Einrichtung
 Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit z.B. ▶ Übungen ▶ Awareness-Schulungen	✓	✓	✓
 Angemessener physischer Schutz der Liegenschaften und kritischer Anlagen u.a. ▶ Maßnahmen des Objektschutzes, u.a. Zäune, Sperren, Überwachung, Detektionsgeräte und Zugangskontrolle	✓		
 Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit u.a. ▶ Notfallübung ▶ Penetrationstests ▶ KPIs	✓	✓	✓
 Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern u.a. ▶ Vertragsmanagement ▶ Richtlinien zum Einkauf und Wartung	✓	✓	✓

EU – NIS 2 und EU - CRE

Umzusetzende Maßnahmen

Risikomanagementmaßnahmen	KRITIS-Einrichtung	Besonders wichtige Einrichtung	Wichtige Einrichtung
 Es müssen Systeme zur Angriffserkennung (SzA) eingesetzt werden, die im laufenden Betrieb u.a. ▶ kontinuierlich und automatisch Parameter aufnehmen (Protokollierung), ▶ auswerten, um Bedrohungen zu identifizieren (Detektion) ▶ und auf Abweichungen reagieren (Reaktion) können	✓		

Ausnahmen:

- Die zuvor aufgeführten **NIS2-Risikomanagementmaßnahmen** gelten für folgenden Einrichtungen nicht, da diesen Vorgaben an anderer Stelle gemacht werden:
  - Die Gesellschaft für Telematik
  - Betreibern von:
    - Diensten für die Telematikinfrastruktur
    - öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdienste
    - Energieversorgungsnetzen oder Energieanlagen
- Für Betreiber kritischer Anlagen gelten für die informationstechnischen Systeme, Komponenten und Prozesse, die für die Funktionsfähigkeit der von ihnen betriebenen kritischen Anlagen maßgeblich sind, **auch aufwändigere Maßnahmen nach § 30 als verhältnismäßig**, wenn der dafür erforderliche Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der betroffenen kritischen Anlage steht (§ 31 Abs. 1 NIS2UmsuCG).

EU – NIS 2 und EU - CRE

Nachweise

Maßnahmen zum Nachweis der Umsetzung	KRITIS-Einrichtung	Besonders wichtige Einrichtung	Wichtige Einrichtung
▶ Verpflichtung der Einrichtung zu Audits, Prüfungen und/oder Zertifizierungen, auch durch Dritte ▶ Ergebnisübermittlung der Ergebnisse (Audits, Zertifizierungen, Mängelbeseitigungen, etc.) an das Bundesamt ▶ Einhaltung der Anforderungen nach dem Gesetz überprüfen, auch durch Dritte ▶ Anweisungen in Bezug auf Maßnahmen erlassen in Bezug auf die Verhütung oder Behebung eines Sicherheitsvorfalls ▶ Anweisungen in Bezug auf Umsetzung des Gesetzes erlassen ▶ Anweisung zu Unterrichtung der Öffentlichkeit oder Betroffener über den Sicherheitsvorfall ▶ Ernennung eines Überwachungsbeauftragten ▶ Bei Nichtumsetzung trotz Fristsetzung: • Aufforderung zum Entzug der Genehmigung der Tätigkeit • Untersagung der Leitungstätigkeiten ggü. natürlichen Personen, die als Geschäftsführung oder Leitung zuständig sind	✓	✓	bei Anlass

EU – NIS 2 und EU - CRE

Meldepflichten

Zeitpunkt der Kenntniserlangung eines erheblichen Sicherheitsvorfalls

Erstbericht

- Angabe, ob ein Verdacht auf rechtswidriges oder böswilliges Handeln besteht
- besteht die Gefahr auf grenzüberschreitende Auswirkungen

bis 24 Stunden nach Kenntniserlangung

Aktualisierung der Informationen des Erstberichtes

- bestätigen oder aktualisieren der Informationen aus dem Erstbericht
- Bewertung des Sicherheitsvorfalls:
  - Schweregrad
  - Auswirkungen
  - Kompromittierung-Indikator
  - evtl. Abhilfemaßnahmen

Zusätzlich für **KRITIS-Einrichtungen:**

- Art, Anzahl und Anteil der von der Störung betroffenen Anlage
- Auswirkungen auf betroffene kritische Dienstleistungen
- bisherige und voraussichtliche Dauer der Störung
- betroffene geografische Gebiet
- Angabe, ob das Gebiet geografisch isoliert ist

72 Stunden nach Kenntniserlangung

Auf Ersuchen des Bundesamtes ist diesem zu jedem Zeitpunkt eine Zwischenmeldung zu machen.

EU – NIS 2 und EU - CRE

Meldepflichten

72 Stunden nach Kenntniserlangung

Fortschrittsmeldung *(bei noch andauerndem Sicherheitsvorfall)*

- Aktualisierung der übermittelten Informationen

bis 1 Monat nach Kenntniserlangung

Abschlussmeldung

- Ausführliche Beschreibung des Sicherheitsvorfall inklusive Schweregrad und dessen Auswirkungen
- Ursache und Art der Bedrohung
- Getroffene und laufende Abhilfemaßnahmen
- Ggf. aufgetretene grenzüberschreitende Auswirkungen

KRITIS-Einrichtungen: Ausführlicher Bericht über den Vorfall

Rückkehr in den Normalbetrieb

Auf Ersuchen des Bundesamtes ist diesem zu jedem Zeitpunkt eine Zwischenmeldung zu machen.

EU – NIS 2 und EU - CRE

Registrierungspflicht

Alle Einrichtungen sind verpflichtet, **sich selbst** auf eine mögliche Zuordnung in eine der drei Importanzkategorien zu überprüfen.

Ist dabei die Zugehörigkeit zu mindestens einer der drei Importanzkategorien festgestellt, muss die Einrichtung sich bei einer gemeinsamen Meldestelle (BBK & BSI) registrieren.

Die Registrierung der Einrichtungen kann bei Nichterfüllung dieser Pflicht oder Fehleinschätzung auch von den Behörden vorgenommen werden. Allerdings muss in diesem Fall schon mit einem Bußgeld gerechnet werden, da es sich um eine Pflichtverletzung handelt. Die Bußgeldhöhe kann dabei bis zur Höchststrafe reichen.

Bei der Registrierung sind je nach Kategorie folgenden Angaben zu machen:

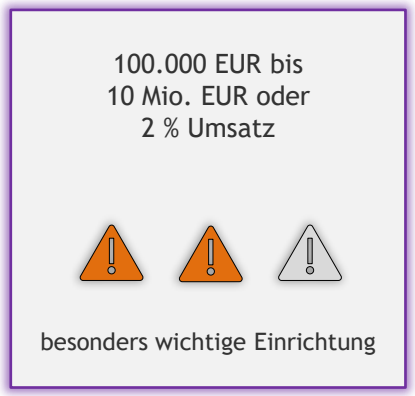
- Name der Einrichtung inklusive der Rechtsform
- Handelsregisternummer
- Anschrift
- Kontaktdaten, mindestens:
  - E-Mail
  - Telefonnummer
- IP-Adressbereich(e)
- Zutreffend(r) Sektor(en) & Teilsektor(en)
- Liste der EU-Mitgliedsstaaten in denen die Tätigkeit(en) erfolgen.

Zusätzliche Informationen, die **KRITIS-Einrichtungen** bei der Registrierung angeben müssen:

- IP-Adressbereiche von den von Ihnen betriebenen Anlagen
- Anlagenkategorie und Versorgungskennzahlen der betriebenen kritischen Anlagen

EU – NIS 2 und EU - CRE

Strafen



Haftung der Geschäftsführung und Leitungen

Zusätzlich werden durch das NIS2-Umsetzungsgesetz spezielle Pflichten und Haftungsmöglichkeiten der **Geschäftsleitung und deren Stellvertreter (Leitungsorgane)** eingeführt. Diese können bei Verletzung Ihrer Pflichten auch persönlich zur Rechenschaft gezogen werden. Die EU-NIS2 sieht dabei u.a. folgende Pflichten für Leitungsorgane vor:

- Die genannten NIS2-Risikomanagementmaßnahmen zu billigen und deren Umsetzung zu überwachen.
- Die regelmäßige Teilnahme an Schulungen als Nachweis für ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken, sowie Risikomanagementpraktiken im Bereich der Cybersicherheit und deren Auswirkungen auf die von der Einrichtung erbrachten Dienste zu erwerben.

Der vertragliche Verzicht einer Einrichtung auf Ersatzansprüche ist unzulässig, dies bedeutet, dass **Geschäftsführer für das Unterlassen und Verhindern von Maßnahmen haftbar gemacht werden müssen.**
Den natürlichen Personen, die als Geschäftsführung oder gesetzliche Vertreter für Leitungsaufgaben in besonders wichtigen Einrichtungen zuständig sind, kann die Wahrnehmung der Leitungsaufgaben vorübergehend untersagt werden, sofern deren Einrichtungen den Anordnungen des Bundesamtes trotz Fristsetzung nicht nachkommen.

EU – NIS 2 und EU - CRE

Was sollten Sie nun tun?

- **Selbsteinschätzung der Zugehörigkeit**
  Evaluation der Zugehörigkeit zu einer Importanzkategorie und Auflistung der umzusetzenden Maßnahmenkataloge je nach Sektoren.
  *Preis 450€**

- **EU-NIS2 / EU-CRE / EU-CRA – GAP Analyse**, ein IST-SOLL-Abgleich der Maßnahmen um Nachbesserungsbedarf zu ermitteln und konkrete Verbesserungsvorschläge zu erhalten.
  - Ablauf einer entsprechenden GAP-Analyse durch BDO Cyber Security GmbH
    - Dokumentensichtung und Interview
    - VOR-ORT- Termin zur Analyse und Konkretisierung
    - Ergebnisbericht mit Lagebild und Maßnahmenvorschlägen

  *Preise ab 3.900€**

- **Umsetzungsstrategie entwickeln - Umsetzungsteams für Maßnahmen festlegen**
  *Preise ab 300€**

- **Maßnahmen umsetzen und Dokumentation ergänzen**
  *Preise ab 300€**

- **EU-NIS2 / EU-CRE / EU-CRA – Compliance Audit durchführen lassen**
  - Ablauf eines Compliance- Audit durch BDO Cyber Security GmbH
    - Auditplanung
    - Dokumentensichtung und Fragebogenanalyse
    - VOR-ORT- Termin zur Beobachtung, Interviews und Konkretisierung
    - Ergebnisbericht mit Lagebild und Maßnahmenvorschlägen
    - Compliance- Audit- Bericht

  *Preise ab 5.500€**

Wir helfen Ihnen gerne.
Termin unkompliziert online anfragen unter:

https://forms.office.com/e/ZgHtwWhqui

continuity@bdo.de

Unsere Preise orientieren sich an der Größe und Komplexität ihres Unternehmens. Dadurch variiert die benötigte Zeit für eine gründliche Evaluation.
Wir sind Premium - dies bedeutet für uns jeden Kunden individuell, ausführlich und zielorientiert zu beraten.

* Nettopreise zzgl. MwSt und NK

BCM & ITSCM

Kontaktieren Sie uns persönlich oder unter continuity@bdo.de

Manuel Ressel

Manager
BCM & ITSCM
Phone: +49 2111371

manuel.ressel@
bdosecurity.de

Stefan Zimmermann

Senior Consultant
BCM & ITSCM
Phone: +49 35186691172

stefan.zimmermann@
bdosecurity.de

Liane Kiesewalter

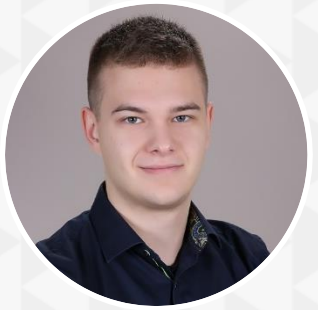
Senior Consultant
BCM & ITSCM
Phone: +49 35186691171

liane.kiesewalter@
bdosecurity.de

Frank Langer

Senior Consultant
CIRCC / BCM & ITSCM
Phone: +49 35186691175

frank.langer@
bdosecurity.de



Janek Schwarz

Consultant
BCM & ITSCM
Phone: +49 30 885 722-200

janek.schwarz@
bdosecurity.de

Vielen Dank für Ihre Aufmerksamkeit