T SECURITY

# Die neue NIS-2-Richtlinie und die Auswirkungen auf KRITIS 3.0

Auf welche Unternehmen kommen neue Herausforderungen zu?

Erleben, was verbindet.

# Inhaltsverzeichnis


| | | |
|---|---|---|
| 1. | Die Zeit drängt | 3 |
| 2. | Welche Unternehmen sind von der neuen NIS-Richtlinie betroffen? | 5 |
| 3. | Welche Pflichten kommen auf Unternehmen zu? | 8 |
| 4. | Wie können die Behörden Unternehmen kontrollieren? | 10 |
| 5. | Zusammenfassung | 11 |
| 6. | Wir machen Sie NIS-2- und KRITIS-3.0-konform | 12 |

# Die Zeit drängt

Die NIS-2-Richtlinie (Network and Information Security) ist verabschiedet. Der enge Umsetzungszeitplan, die hohen Anforderungen und die strengen Aufsichts- und Sanktionierungsmaßnahmen setzen Unternehmen unter Druck.

**Die zweite Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU muss in den Mitgliedsländern bis zum 17.10.2024 in nationales Recht umgesetzt werden. Besonders für Unternehmen, die bisher nicht von der NIS-Richtlinie betroffen waren, bedeutet das eine große Herausforderung. Dieses Whitepaper fasst zusammen, was Sie über die NIS-2-Richtlinie wissen müssen: Welche Unternehmen und Einrichtungen werden als kritische Infrastruktur definiert und welche Neuerungen gibt es hier? Was kommt auf die Betreiber kritischer Infrastrukturen zu? Worauf kommt es bei der Umsetzung von Risikomanagement-maßnahmen an?**

Seit Beginn des Angriffskriegs auf die Ukraine hat sich die Sicherheitslage in Europa drastisch zugespitzt. Dies betrifft auch die Cyberbedrohungslage. Die Verwundbarkeit von Organisationen im Cyberraum und die leichte Zugänglichkeit des Internets stellen insbesondere kritische Infrastrukturen vor die Herausforderung, sich vor weltweiten Angriffen schützen zu müssen

Als Reaktion auf die sich entwickelnde Bedrohungslandschaft für Cybersicherheit haben das europäische Parlament und der Rat der EU die NIS-2-Richtlinie verabschiedet. Gemeinsam mit der NIS-2-Richtlinie wurde auch die Richtlinie über die Resilienz kritischer Einrichtungen verabschiedet, die ergänzend zur NIS 2 zu sehen ist. Ziel ist die Sicherstellung kritischer Infrastruktur, ohne die eine Gesellschaft nicht funktionieren kann und die das Überleben von Millionen Menschen in der Europäischen Union sichert.

*Kritische Infrastrukturen (KRITIS) sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.*

*– KRITIS-Definition des Bundesamtes für Sicherheit in der Informationstechnik*

*Der Cyberraum ist der neue Kriegsschauplatz. Angesichts der vor uns liegenden Herausforderungen und Bedrohungen brauchen wir moderne und interoperable europäische Streitkräfte, die über die neuesten Cyberabwehrfähigkeiten verfügen. Im Rahmen der neuen EU-Cyberabwehrpolitik wird die Zusammenarbeit zwischen den EU-Akteuren im Bereich der Cyberabwehr gestärkt. Außerdem sollen Mechanismen für den Einsatz von Fähigkeiten auf EU-Ebene entwickelt werden, auch für Missionen und Operationen im Rahmen der gemeinsamen Sicherheits- und Verteidigungspolitik. So werden wir besser in der Lage sein, Cyberangriffe zu erkennen, zu vereiteln und davon abzuschrecken, wie dies im Strategischen Kompass gefordert wird.“*

– *Josep Borrell,*
*Hoher Vertreter der EU für Außen- und Sicherheitspolitik*

Seit dem 16. Januar 2023 ist die NIS-2-Richtlinie in Kraft getreten: Das bedeutet, dass die Mitgliedsländer der Europäischen Union bis zum 17. Oktober 2024 Zeit haben, sie in nationales Gesetz zu gießen. Dabei müssen die Länder sich an die Vorlagen des Richtlinientextes halten, wobei die vorliegende Fassung den Mindeststandard darstellt. Den Ländern ist es vorbehalten, von den Unternehmen und Organisationen, die in ihrem Staatsgebiet angesiedelt sind, auch höhere Standards zu fordern.

Durch die NIS-2-Richtlinie sollen Unterschiede in den Sicherheitsbestrebungen zwischen den Mitgliedstaaten verringert werden und ein einheitliches Sicherheitsniveau hergestellt werden. Die neue Bestimmung fordert mehr Schutzmaßnahmen und ermöglicht eine strengere Überwachung und Sanktionierung der Umsetzung dieser Maßnahmen. Außerdem werden mehr Bereiche als kritische Infrastrukturen definiert.

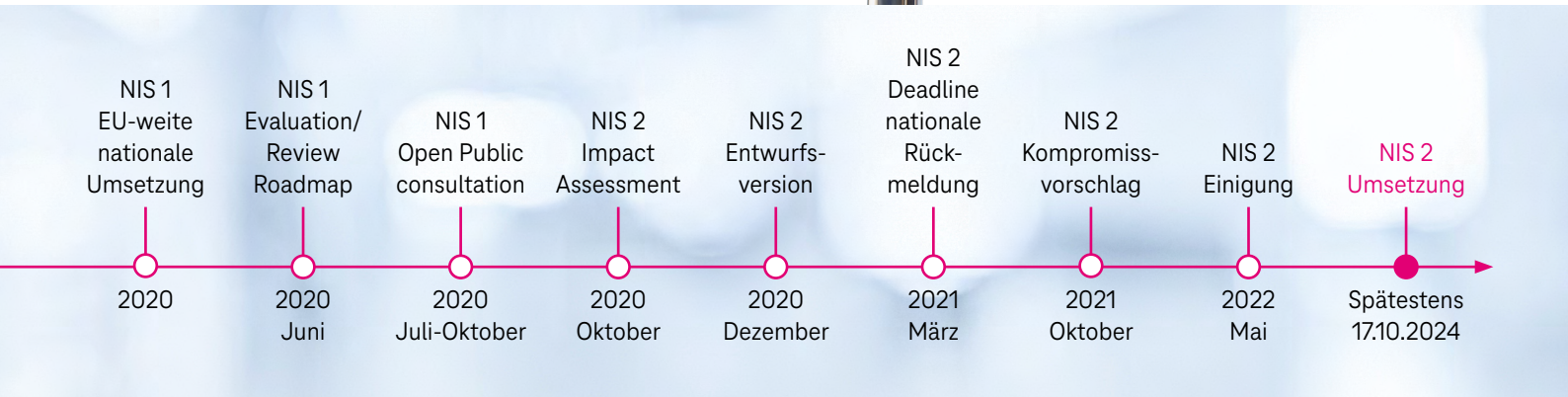



Abbildung 1: Zeitstrahl zur Umsetzung der NIS-2-Richtlinie

# Welche Unternehmen sind von der neuen NIS-Richtlinie betroffen?

Ob Unternehmen von der NIS-2-Richtlinie betroffen sind, hängt vom Tätigkeitsbereich sowie von der Unternehmensgröße ab. Dabei ist es wichtig zu wissen, dass die NIS-2-Richtlinie für deutlich mehr Bereiche relevant ist als die erste NIS-Richtlinie. Unterschieden wird zwischen Sektoren mit hoher Kritikalität und sonstigen kritischen Sektoren. Zusätzlich zu dieser Unterscheidung gibt es die Kategorien wesentliche Einrichtungen und wichtige Einrichtungen. Letztere Unterteilung spielt hauptsächlich in Bezug auf die staatlichen Aufsichts- und Sanktionsmöglichkeiten eine Rolle. Die bisherigen Schwellenwerte in Deutschland, die in der KRITIS-Verordnung festgelegt wurden, werden so in einem zukünftigen Sicherheitsgesetz 3.0 nicht mehr zu finden sein. Die NIS-2-Richtlinie definiert hier bereits im Voraus Schwellenwerte in Abhängigkeit von der Betriebsgröße.

Zuerst steht die Unterscheidung der zwei Sektoren. Einerseits werden Sektoren mit hoher Kritikalität definiert und andererseits jene mit sonstiger Kritikalität. Die Sektoren mit hoher Kritikalität decken sich großteils mit jenen, die bereits in Deutschland unter KRITIS fallen. Unklar ist zu diesem Zeitpunkt noch, welchen Regelungen der KRITIS-Sektor Medien und Kultur unterliegt, der in der NIS 2 nicht berücksichtigt wird, aber in Deutschland kritische Infrastruktur ist. Ebenso muss abgewartet werden, wie der Gesetzgeber Unternehmen im besonderen öffentlichen Interesse (UBI) einstufen wird. Vorstellbar ist, dass die Kategorien 1 und 3 der UBI in den zweiten kritischen Sektor fallen könnten. Bei der Kategorie 2 muss noch abgewartet werden.

## Sektoren mit hoher Kritikalität[1]

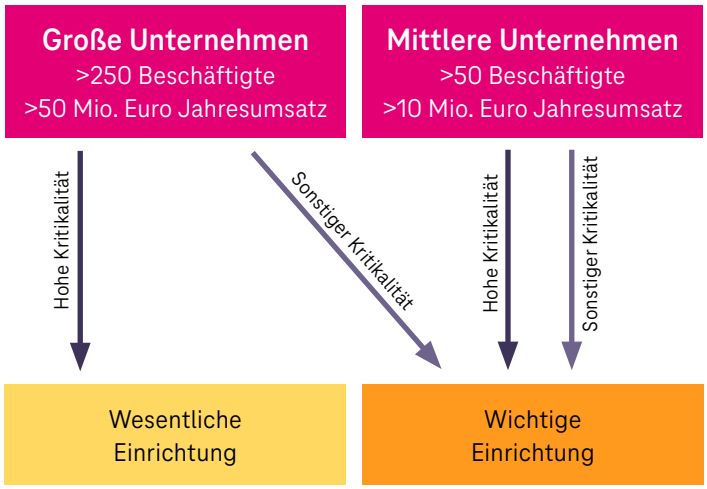
- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten
- Öffentliche Verwaltung
- Weltraum

## Sonstige kritische Sektoren[2]

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung und Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe / Herstellung von Waren
  - Herstellung von Medizinprodukten
  - Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen
  - Herstellung von elektrischen Ausrüstungen
  - Maschinenbau
  - Herstellung von Kraftwagen und Kraftwagenteilen
  - Sonstiger Fahrzeugbau
- Anbieter digitaler Dienste
- Forschung

[1] Vgl. Richtlinie (EU) 2022/2555, Anhang I
[2] Vgl. Richtlinie (EU) 2022/2555, Anhang II

In einem zweiten Schritt muss die Größe des Unternehmens herangezogen werden, um zu definieren, ob es sich um eine wesentliche oder eine wichtige Einrichtung handelt. Unternehmen, die weniger als 50 Beschäftigte haben und weniger als 10 Millionen Euro Jahresumsatz aufweisen, fallen nicht unter die NIS-2-Richtlinie.




## Sonderfälle

Folgende Unternehmen sind unabhängig von ihrer Größe von NIS 2 betroffen.[3] Eine Ausnahme bilden Anbieter öffentlicher elektronischer Kommunikationsnetze – hier sind nur Unternehmen von mindestens mittlerer Unternehmensgröße* betroffen.

- Vertrauensdiensteanbieter
- Domänennamenregister der Domäne oberster Stufe
- DNS-Diensteanbieter
- Anbieter öffentlicher elektronischer Kommunikationsnetze mit mittlerer Unternehmensgröße
- Öffentliche Verwaltung
- Unternehmen, die als einziger Anbieter eines Dienstes in einem EU-Mitgliedsstaat gesehen werden, der kritisch ist für das öffentliche Leben ist
- Unternehmen, deren Störung einen wesentlichen Effekt auf die öffentliche Ordnung, Sicherheit oder Gesundheit haben
- Unternehmen, die laut der Resilienz-Richtlinie der EU als kritisch einzustufen werden
- Unternehmen, die vor dem 16. Januar 2023 schon als kritisch eingestuft wurden[4]

* Hierunter werden Organisationen verstanden, die zwischen 50 und 250 Beschäftigte haben und entweder einen Jahresumsatz zwischen 10 und 50 Millionen Euro oder eine Jahresbilanz von mindestens 43 Millionen Euro aufweisen.

[3] Vgl. Richtlinie (EU) 2022/2555, Artikel 3, Absatz 1, Ziffer a
[4] Vgl. Richtlinie (EU) 2022/2555, Artikel 3, Absatz 1

## Beispiele

| | | | |
|---|---|---|---|
| **Krankenhaus** | 500 Beschäftigte<br>500 Mio. Jahresumsatz | → | Wesentliche Einrichtung |
| **Produktion von optischen Geräten** | 500 Beschäftigte<br>1 Mio. Jahresumsatz | → | Wichtige Einrichtung |
| **Wasserwerk** | 25 Beschäftigte<br>30 Mio. Jahresumsatz | → | Wichtige Einrichtung |
| **Produktion von Autoteilen** | 20 Beschäftigte<br>400 Mio. Jahresumsatz | → | Wichtige Einrichtung |

## Vergleich KRITIS und NIS 2

# Welche Pflichten kommen auf Unternehmen zu?

Was müssen Firmen unternehmen, um NIS-2-konform zu werden? Prinzipiell gibt die EU Unternehmen zwei große Pflichten auf. Erstens wird verlangt, dass **Risikomanagement-maßnahmen** getroffen werden, um die kritische Dienstleistung zu schützen. Zweitens wird verlangt, dass **Sicherheitsvorfälle** an die zuständigen staatlichen Einrichtungen gemeldet werden.

Im Gegensatz noch zur ersten NIS-Richtlinie werden jetzt schon auf EU-Ebene konkretere Maßnahmen gefordert. Für die EU ist es hier vor allem wichtig, dass wesentliche und wichtige Organisationen technische, operative und organisatorische Maßnahmen ergreifen. Dabei steht der Grundsatz der Verhältnismäßigkeit im Fokus. Es wird nicht verlangt, dass sich ein Unternehmen wegen der Maßnahmen in den Ruin treibt. Dabei sollen Maßnahmen getroffen werden, die dem Stand der Technik entsprechen und eventuell auch Gegenstand von europäischen Normen sind. Die Kosten der Umsetzung sollen ein Sicherheitsniveau gewährleisten, das dem bestehenden Risiko angemessen ist. Die Richtlinie gibt hierbei auch schon relativ genau vor, was für die EU Verhältnismäßigkeit bedeutet.

## Folgende Faktoren müssen in die Evaluierung einfließen:

- Ausmaß der Risikoexposition der Organisation
- Größe der Organisation
- Wahrscheinlichkeit des Eintretens des Risikos
- Auswirkung und Schwere des Risikos (inklusive der Auswirkung auf die Gesellschaft und Wirtschaft des Landes)

Erkennbar ist, dass der risikobasierte Ansatz, der schon in der ersten NIS-Richtlinie enthalten war, weiter ausgebaut wurde und einen noch größeren Stellenwert als bisher einnimmt.[5] Hinzu kommt nun auch ein gefahrenübergreifender Ansatz. Das bedeutet, dass Netz- und Informationssysteme nicht nur gegen Angriffe aus dem Cyberraum, sondern auch gegen Angriffe aus dem physischen Umfeld gewappnet sein müssen. Auch die Sicherheit der Lieferkette gerät dabei erstmals in den Blick und muss gewährleistet werden.[6] Des Weiteren werden in der Richtlinie die Mindestmaßnahmen zur Reduzierung eines Risikos vorgestellt.

[5] Vgl. Richtlinie (EU) 2022/2555, Artikel 21, Absatz 1
[6] Vgl. Richtlinie (EU) 2022/2555, Artikel 21, Absatz 2

## Mindestmaßnahmen zur Reduzierung eines Risikos:

- Risikoanalyse und Sicherheit für Informationssysteme
- Bewältigung von Sicherheitsvorfällen
- Business Continuity Management (BCM)
- Sicherheit der Lieferkette
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen, einschließlich Management und Offenlegung von Schwachstellen
- Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
- Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptografie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzepte für die Zugriffskontrolle und das Management von Anlagen
- Multi-Faktor-Authentifizierung oder kontinuierliche Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggf. gesicherte interne Notfallkommunikationssysteme[7]

## Berichtspflichten

Wesentliche und wichtige Einrichtungen haben laut der NIS-2-Richtlinie die Verpflichtung, jeden Sicherheitsvorfall, der erhebliche Auswirkungen auf die kritische Dienstleistung hat, den Behörden und den Empfängern der Dienstleistung zu melden. Dabei muss auch gemeldet werden, welche Sofortmaßnahmen die Empfänger als Reaktion auf diese Bedrohung treffen können.[8]

Sollte sich ein erheblicher Sicherheitsvorfall ereignen, muss die Organisation innerhalb von 24 Stunden nach Kenntnisnahme eine Frühwarnung abgeben. Spätestens nach 72 Stunden muss eine erste Bewertung des Sicherheitsvorfalles geschehen sein. Höchstens nach einem Monat muss der nationalen Behörde ein Abschlussbericht inklusive der getroffenen Maßnahmen übermittelt werden.[9]

## Erhebliche Sicherheitsvorfälle laut NIS 2:

- **Schwerwiegende Betriebsstörungen,** die den kritischen Dienst ausfallen lassen oder auch ausfallen lassen könnten. Dabei wird auch die Komponente des finanziellen Verlustes berücksichtigt, so dass auch der Konkurs eines Unternehmens einen erheblichen Sicherheitsvorfall darstellen kann.

- Ein erheblicher Sicherheitsvorfall liegt vor, wenn dieser Menschen oder andere Firmen durch **erhebliche oder immaterielle Schäden** beeinträchtigt hat oder beeinträchtigen kann.[10]

[7] Vgl. Richtlinie (EU) 2022/2555, Artikel 21, Absatz 2
[8] Vgl. Richtlinie (EU) 2022/2555, Artikel 23, Absatz 1f.
[9] Vgl. Richtlinie (EU) 2022/2555, Artikel 23, Absatz 4
[10] Vgl. Richtlinie (EU) 2022/2555, Artikel 23, Absatz 3

# Wie können die Behörden Unternehmen kontrollieren?

Wurden keine oder nicht ausreichende Risikomanagementmaßnahmen getroffen, drohen mit der NIS-2-Richtlinie teils drastische Sanktionen. Die Sanktionen sollen laut der Richtlinie wirksam, verhältnismäßig und abschreckend sein.

## Sanktionsmaßnahmen für wesentliche Einrichtungen[11]

- Warnungen
- Verbindliche Anweisungen
- Umsetzung der Empfehlungen der Sicherheitsüberprüfung
- Benennung eines Überwachungsbeauftragten
- Veröffentlichung von Verstößen gegen die Richtlinie
- **Geldbuße mit einem Höchstbetrag von mind. € 10 Mio. oder mind. 2 % des weltweiten Konzernumsatzes des Vorjahres (je nachdem, was höher ist)**

Sollten diese Maßnahmen nicht ausreichen, können zudem die Zertifizierung oder Genehmigung für den Geschäftsbereich entzogen werden. Außerdem kann Geschäftsführer*innen und Vorstandsmitgliedern vorübergehend untersagt werden, weiterhin leitende Tätigkeiten in der Organisation auszuüben.

## Sanktionsmaßnahmen für wichtige Einrichtungen[12]

- Warnungen
- Verbindliche Anweisungen
- Umsetzung der Empfehlungen der Sicherheitsüberprüfung
- Veröffentlichung von Verstößen gegen die Richtlinie
- **Geldbuße mit einem Höchstbetrag von mind. € 7 Mio. oder mind. 1,4 % des weltweiten Konzernumsatzes des Vorjahres (je nachdem, was höher ist)**

[11] Vgl. Richtlinie (EU) 2022/2555, Artikel 32, Absatz 4f.
[12] Vgl. Richtlinie (EU) 2022/2555, Artikel 33, Absatz 4

# Zusammenfassung

Wesentliche und wichtige Einrichtungen werden zunehmend in die Pflicht genommen, ihre Netz- und Informationssicherheit auszubauen und konstant auf dem aktuellen Stand der Technik zu halten. Mithilfe der NIS-2-Richtlinie versucht die Europäische Union, ein einheitliches Sicherheitsniveau für wesentliche und wichtige Einrichtungen im privaten und öffentlichen Bereich zu setzen. Hintergrund ist die aktuelle Sicherheitslage in Europa: Cyberangriffe auf kritische Infrastrukturen werden auch in den kommenden Monaten und Jahren mit hoher Wahrscheinlichkeit zunehmen.

## Wichtige Punkte auf einen Blick

**Mehr Unternehmen sind betroffen:** Der Kreis der potentiellen Unternehmen, die als kritische Infrastrukturen definiert werden, erhöht sich durch die NIS-2-Richtlinie deutlich. Neue Sektoren, die in Deutschland zum Beispiel bisher im Nebenbereich UBI (Unternehmen von besonderem öffentlichem Interesse) angesiedelt waren, kommen jetzt in den vollen Scope der NIS-Regulierung.

**Mehr Mindestmaßnahmen erforderlich:** Der Umfang der Risikomanagementmaßnahmen für kritische Infrastrukturen, die von der EU gefordert werden, nimmt zu. Welche genauen Maßnahmen gefordert werden, bleibt den Staaten überlassen. Vorstellbar ist, dass in Deutschland der Begriff "Stand der Technik" Bestandteil des Gesetztestextes bleibt. Besonderes Augenmerk wird dabei auf einen risikobasierten und gefahrenübergreifenden Ansatz gelegt. Supply Chain, Kryptographie und verbesserte Authentifizierungsmaßnahmen sind nur einige Beispiele von Maßnahmen, die verpflichtend werden.

**Strengere Überwachung:** Die Aufgaben und Rechte der nationalen Überwachungsbehörden werden ausgeweitet. Unternehmen müssen Informationen zur Verfügung stellen und Vor-Ort-Kontrollen und Sicherheitsaudits zulassen. Außerdem müssen den Behörden Nachweise und Auditberichte vorgelegt werden.

**Empfindliche Sanktionen:** Den nationalen Aufsichtsbehörden werden Instrumente an die Hand gegeben, mit denen sie die Unternehmen zur Umsetzung von Risikomanagementmaßnahmen zwingen können. Dies kann durch die Entsendung von Inspektoren in die Unternehmen geschehen, aber auch durch die Verhängung empfindlicher Geldstrafen. Die Sanktionen können bis zum Entzug von Zertifizierungen und Genehmigungen für das Geschäftsfeld und zum Arbeitsverbot für leitende Personen in den Unternehmen reichen.

**Um den gesetzlichen Anforderungen gerecht zu werden, ist es ratsam, sich frühzeitig mit den geänderten Anforderungen auseinander zu setzen. Dabei können wir, die Telekom Security, Ihnen helfen.**

# Wir machen Sie NIS-2- und KRITIS-3.0-konform

Ihr Unternehmen zählt zur kritischen Infrastruktur – was nun? Wir empfehlen, langfristig zu denken, auch wenn der sehr enge Umsetzungszeitplan zur Eile drängt. Eine einmalige Bewertung der Risikolandschaft und der Maßnahmen kann Ihre Geschäftsprozesse und Assets nicht nachhaltig schützen – und wird auch die Prüfenden nicht überzeugen. Nur mit einem funktionierenden Managementsystem können Sie den Anforderungen von NIS / KRITIS sinnvoll begegnen.

## Wir sind Managementsystem-Profis

Profitieren Sie von unserer langjährigen Erfahrung mit unterschiedlichsten Zertifizierungen und Prüfprozessen. Wir unterstützen Sie gerne: Gemeinsam finden wir heraus, wo Sie stehen, wohin Sie sich entwickeln wollen und wie wir den Weg dorthin gemeinsam gehen können. Die Vorgehensweise passen wir auf Ihre Bedürfnisse an. Ziel ist es, Ihr Sicherheitsniveau kontinuierlich zu erhöhen.

Aus dem breit aufgestellten Consulting-Bereich der Telekom Security, der nicht nur im DACH-Bereich, sondern auch europa- und weltweit vernetzt ist, stellen wir Ihnen die Expert*innen zur Seite, die Sie brauchen. So können wir Sie in allen Kategorien der neuen NIS-Richtlinie beraten.

Neben der Beratung im Bereich NIS/KRITIS führen wir auch damit zusammenhängende oder übergreifende Projekte mit Ihnen durch, z. B. wenn Sie parallel eine Zertifizierung nach internationalen Standards wie ISO 27001 oder ISO 22301 anstreben.

## So unterstützen wir Sie

Die Telekom Security bietet Unterstützung bei der Umsetzung der NIS-2-Konformität. Ihre Ausgangssituation entscheidet über die Fokusbereiche.

**Analyse und Dokumentation:** Grundlage für alle weiteren Schritte ist die Analyse und Dokumentation der Assets, um die zu schützende Infrastruktur genau abzugrenzen. Dazu gehört die Analyse der Systemlandschaft und der verschiedenen angeschlossenen Geräte. Anschließend erheben wir, welchen Bedrohungen Ihre Infrastruktur ausgesetzt ist und wie der aktuelle Stand und Reifegrad der bereits getroffenen Sicherheitsmaßnahmen ist.

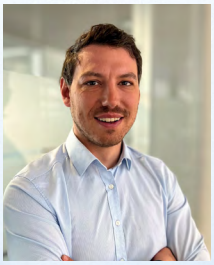
**Individueller Maßnahmenplan:** Basierend auf dem Ist-Stand identifizieren wir Abweichungen zu den NIS-Anforderungen und erstellen einen individuellen Maßnahmenplan.

**Umsetzung & Projektabschluss:** Auf Wunsch unterstützen wir Sie auch bei der Umsetzung der Maßnahmen. Nach erfolgreicher Umsetzung erfolgt der formale Projektabschluss mit einer gemeinsamen Retrospektive und der Identifizierung von Lessons Learned.

T SECURITY

## Felix Krainhöfner

Felix Krainhöfner unterstützt Betreiber von kritischen Infrastrukturen in der Analyse und Implementierung von Maßnahmen im Bereich des Security Risk Managements mit besonderem Augenmerk auf den nationalen Anforderungen der NIS-Richtlinie in Deutschland und Österreich. Dabei liegt sein Fokus im Bereich des Gesundheitswesens, in dem er seit langen Jahren tätig ist.



## Daniel Rösler

Herr Rösler berät KRITIS-Betreiber aller Sektoren, wobei sein Schwerpunkt im Bereich Operational Technologies liegt. Mithilfe seiner langjährigen Erfahrung unterstützt er Kunden bei der Entwicklung von Cyber Security Prozessen und der Steigerung der Resilienz. Er hilft bei der Vorbereitung und begleitet die KRITIS-/NIS-Umsetzung bis zur Prüfung. In seinen Projekten führt er Assessments durch, prüft Unternehmens-Security-Ziele und unterstützt bei individuellen Problemen.

T SECURITY

# Noch Fragen?

Wir beraten Sie gerne:
security@telekom.de

**Herausgeber**
Deutsche Telekom Security GmbH
Bonner Talweg 100
53113 Bonn

Erleben,
was verbindet.