NIS-2

MYRA

FACT SHEET

NIS-2: Plötzlich KRITIS und was nun?

NIS-2: Betroffenheit prüfen, IT-Sicherheitsvorgaben ableiten, Umsetzung anstoßen

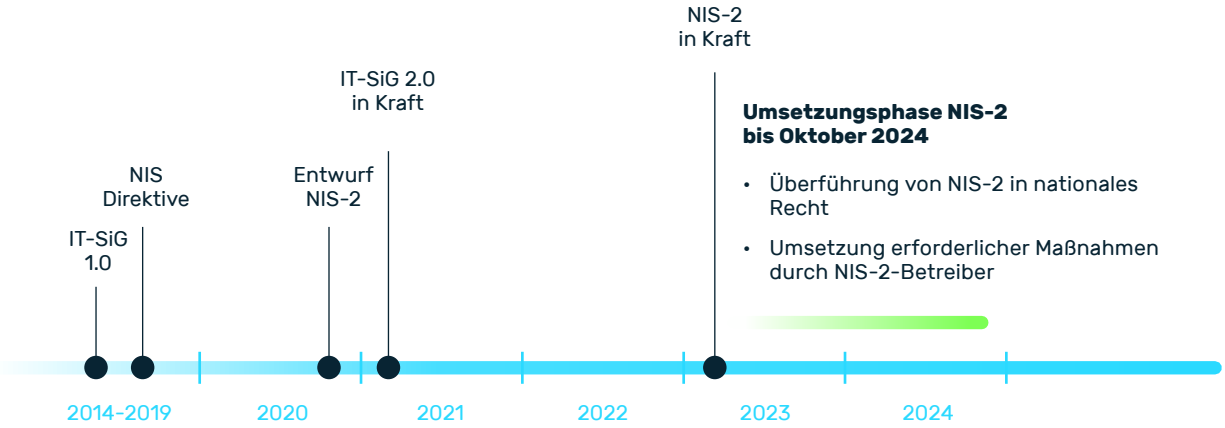
Betreiber kritischer Infrastrukturen sind in Deutschland bereits jetzt bei Erreichung gewisser Schwellenwerte durch das IT-Sicherheitsgesetz 2.0 verpflichtet, strenge Maßnahmen zur Etablierung und Aufrechterhaltung der Informationssicherheit umzusetzen.

Durch die NIS-2-Richtlinie (EU 2022/2555) zählen nun deutlich mehr Unternehmen zu den kritischen Infrastrukturen (KRITIS). Allein in Deutschland ist von einer Verzehnfachung der KRITIS-Betreiber auszugehen. Europaweit kommen schätzungsweise 100.000 Firmen hinzu.

Gleichzeitig verschärft NIS-2 die regulatorischen Vorgaben für IT-Sicherheit erheblich und führt striktere Sanktionsmaßnahmen ein, die bei gravierenden Verstößen auch eine persönliche Haftung für das verantwortliche Management einschließt. Außerdem müssen KRITIS-Unternehmen neuerdings die Cybersicherheit entlang Ihrer Lieferketten sicherstellen. Dadurch rücken auch angeschlossene Partner und Dienstleister in den Fokus der Regulierungsbehörden.

Das vorliegende Fact Sheet verschafft Ihnen einen schnellen Überblick zu den wichtigsten Inhalten aus der NIS-2-Richtlinie und erlaubt Ihnen eine Schnelleinschätzung, inwieweit Ihr Unternehmen davon betroffen ist. Außerdem erhalten Sie auf den folgenden Seiten Informationen zu den daraus resultierenden regulatorischen Vorgaben sowie Tipps zur Umsetzung.

NIS-Timeline



Welche Unternehmen und Branchen betrifft NIS-2?

- Grundvoraussetzung: ab 50 Mitarbeiter/10 Mio. EUR Umsatz
- Betreiber aus 18 Sektoren (Art. 3), unterteilt in „Sektoren mit hoher Kritikalität“ (Anhang I) und „Sonstige kritische Sektoren“ (Anhang II)

Sektoren mit hoher Kritikalität (Anhang I)

Energie
(Elektrizität, Fernwärme und -kälte, Erdöl, Erdgas, Wasserstoff)

Verkehr
(Straßenverkehr, Luftverkehr, Schienenverkehr, Schifffahrt einschließlich Reedereien und Hafenanlagen)

Bankwesen
(Kreditinstitute)

Finanzmarktinfrastrukturen

Gesundheitswesen
(Gesundheitsdienstleister, Forschungslabors, Pharmazeutika, Herstellung medizinischer Geräte)

Trinkwasser
(Trinkwasserversorger)

Abwasser
(Abwasserentsorger)

Digitale Infrastruktur (Betreiber von Internet-Knoten, DNS-Diensteanbieter (ohne Root), TLD-Namenregister, Anbieter von Cloud-Computing-Diensten, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Vertrauensdiensteanbieter, Anbieter öffentlicher elektronischer Kommunikationsnetze oder Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste)

Verwaltung von IKT-Diensten (B2B)

Öffentliche Verwaltung

Weltraum
(Betreiber von Bodeninfrastrukturen)

Sonstige kritische Sektoren (Anhang II)

Post- und Kurierdienste

Abfallbewirtschaftung

Produktion, Herstellung und Handel mit chemischen Stoffen

Produktion, Verarbeitung und Vertrieb von Lebensmitteln

Forschung

Verarbeitendes Gewerbe
(Herstellung von Medizinprodukten und In-vitro-Diagnostika, Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen, elektrischen Ausrüstungen, Maschinenbau, Kraftwagen und Kraftwagenteilen, sonstiger Fahrzeugbau)

Anbieter digitaler Dienste
(Anbieter von Online-Marktplätzen, Online-Suchmaschinen, Plattformen für Dienste sozialer Netzwerke)

Wesentliche und wichtige Einrichtungen

Die regulatorischen Anforderungen richten sich bei NIS-2 aber nicht nur an den Branchen aus. Die Richtlinie unterteilt die betroffenen Unternehmen zudem in wesentliche und wichtige Einrichtungen auf, wobei die Größe des Unternehmens mitgewichtet wird.

Wesentliche Einrichtungen:

- Große Betreiber aus Anhang I (Sektoren mit hoher Kritikalität) mit mehr als 250 Beschäftigten, mehr als 50 Mio. Euro Jahresumsatz oder einer Jahresbilanzsumme von mehr als 43 Mio. EUR.
- Ausnahmen*

Wichtige Einrichtungen:

- Mittlere Betreiber aus Anhang I oder II mit 50-250 Beschäftigten, 10-50 Mio EUR Jahresumsatz oder weniger als 43 Mio. EUR Jahresbilanzsumme.
- Große Betreiber aus Anhang II mit mehr als 250 Mitarbeiter, mehr als 50 Mio. Euro Jahresumsatz oder Jahresbilanzsumme mehr als 43 Mio. EUR.
- Ausnahmen*

Welche Konsequenz ergibt sich daraus für die betroffenen Unternehmen?
Die Art der Einrichtung bestimmt den Umfang der staatlichen Aufsichts- und Sanktionsmöglichkeiten. Weitere Informationen hierzu finden Sie unter dem Abschnitt “Welche Strafen drohen bei Verstößen?” auf Seite 5.

* siehe Seite 7

Cybersicherheit: Was ist zu tun?

Betreiber in der EU müssen geeignete und verhältnismäßige technische, operative und organisatorische Maßnahmen ergreifen, um die IT und Netzwerke ihrer kritischen Dienstleistungen zu schützen (Art. 21). Im Detail sind folgende IT-Sicherheitsmaßnahmen gemäß NIS-2 erforderlich:

- Policies: Risikoanalyse und Sicherheit für Informationssysteme
- Incident Management: Prävention, Detektion und Mitigation von Cyberattacken
- Business Continuity Management: Backup Management, Disaster Recovery, Krisenmanagement
- Sicherheit in der Lieferkette: Sicherheit bei Dienstleistern und Zulieferern
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT und Netzwerksystemen
- Effektivitätsbewertung des IT-Risikomanagement
- Awareness-Schulungen für Personal: Cyberhygiene und Cybersicherheit
- Vorgaben für Kryptographie und Verschlüsselung
- Sicherheit des Personals
- Zugriffskontrolle
- Anlagenmanagement
- Authentifizierung: Multi Factor Authentisierung (MFA) oder kontinuierliche Authentifizierung
- Sichere Sprach-, Video- und Textkommunikation
- Sichere Notfallkommunikationssysteme

Meldepflichten & Fristen

Alle erheblichen Sicherheitsvorfälle müssen den zuständigen Behörden gemeldet werden (z.B. dem Bundesamt für Sicherheit in der Informationstechnik (BSI) in Deutschland). Als erheblich gelten schwere Betriebsstörungen und Vorfälle, die finanzielle Verluste oder Schäden für die Einrichtung oder andere Personen bedeuten (Art. 23).

- Frühwarnung muss spätestens 24 Stunden nach Kenntnisnahme erfolgen
- Meldung inklusive Analyse muss spätestens nach 72 Stunden erfolgen
- Abschlussbericht des Vorfalls inklusive Auswirkungen und Abhilfemaßnahmen ist innerhalb eines Monats vorzulegen

Welche Strafen drohen bei Verstößen?

Das Ausmaß möglicher Sanktionen und Bußgelder orientiert sich in NIS-2 primär an der Einordnung des jeweiligen Unternehmens zu den wesentlichen oder wichtigen Einrichtungen. Während wichtige Einrichtungen nur einer reaktiven Aufsichtsregelung unterliegen, werden wesentliche Einrichtungen proaktiv von den Aufsichtsbehörden überwacht, was auch Ad-hoc-Prüfungen vor Ort miteinschließt.

Wesentliche Einrichtungen: Bei Verstößen gegen Artikeln 21 und 23 NIS-2 drohen je nach nationaler Umsetzung Geldbußen mit einem Höchstbetrag von mindestens 10.000.000 EUR oder mit einem Höchstbetrag von mindestens 2 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens – je nachdem, welcher Betrag höher ist (Art.34).

Wichtige Einrichtungen: Bei Verstößen gegen Artikeln 21 und 23 NIS-2 drohen je nach nationaler Umsetzung Geldbußen mit einem Höchstbetrag von mindestens 7.000.000 EUR oder mit einem Höchstbetrag von mindestens 1,4 % des gesamten weltweiten im vorangegangenen Geschäftsjahr getätigten Umsatzes des Unternehmens – je nachdem, welcher Betrag höher ist (Art.34).

Aufsicht und Durchsetzung: Um die Einhaltung der NIS-2-Vorgaben zu prüfen und durchzusetzen sieht die Richtlinie weitreichende Befugnisse für die zuständigen Behörden vor. So müssen den Behörden auf Anordnung mitunter Daten, Akten und weitere Informationen als Nachweis ausgehändigt werden. Auch Prüfungen und Audits durch die Behörden und unabhängige Dritte sind in NIS-2 vorgesehen (Art. 32).

Bei Verstößen gegen die Vorgaben können die zuständigen Behörden unter anderem Anweisungen an den betroffenen Betreiber ausgeben, öffentliche Warnungen aussprechen oder sogar die Betriebserlaubnis oder die Gültigkeit von Zertifizierungen aussetzen. Darüber hinaus besteht Organhaftung, d.h. das Management kann persönlich für Verstöße haftbar gemacht werden (Art. 20).

Was müssen Unternehmen jetzt tun?

Die NIS-2-Richtline ist zwar EU-weit seit 16.01.2023 in Kraft, wurde bislang aber noch nicht in nationales Recht überführt. Dies muss bis spätestens Oktober 2024 erfolgen, in Deutschland wahrscheinlich in Form des NIS2UmsuCG (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz). Details hierzu finden Sie auf Seite 7.

Obwohl die konkreten regulatorischen Vorgaben noch nicht bekannt sind, können und sollten Unternehmen bereits jetzt auf Basis der bestehenden Verordnung die notwendigen Vorbereitungen zur Umsetzung treffen.

Vorbereitung für NIS-2-Compliance

Cybersicherheit spielt durch NIS-2 eine zentrale Rolle in der Compliance-Strategie betroffener Betreiber und sollte daher als fester Bestandteil in allen relevanten Geschäftsprozessen integriert sein.

- Bestandsaufnahme zur Betroffenheitsprüfung und Einordnung der geltenden Richtlinien
- Identifizierung möglicher Lücken in Cybersicherheit und Cyberabwehr (organisatorisch, technisch und prozessual) unter Beachtung etablierter Best-Practice-Verfahren wie den BSI-Standards (z.B. 200-1 bis 200-4) und/oder ISO/IEC 27001
- Supply Chain: Überprüfung und mögliche Neuevaluierung von Dienstleistern und Zulieferern. Geeignete Anbieter verfügen über erforderliche Sicherheitsexpertise und weisen diese mittels Zertifizierungen und Testaten aus (z.B. ISO 27001 (auf Basis von IT-Grundschutz) oder BSI C5).
- Umsetzung der erforderlichen Maßnahmen
- Etablierung geeigneter Überwachungs- und Monitoring-Mechanismen, um die Wirksamkeit der getroffenen Maßnahmen und deren Compliance regelmäßig zu überprüfen und bei Bedarf nachzubessern.

Deutsche Umsetzung geht über NIS-2-Vorgaben hinaus: erweiterter Geltungsbereich, höhere Bußgelder

Die NIS-2-Richtline ist zwar EU-weit seit 16.01.2023 in Kraft, wurde bislang aber noch nicht in nationales Recht überführt. Dies muss bis spätestens Oktober 2024 erfolgen, in Deutschland in Form des NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes (NIS2UmsuCG). Ein Referentenentwurf des Gesetzes mit Stand April 2023 von intrapol.org zeigt, wie in Deutschland die Umsetzung von NIS-2 konkret aussehen könnte. Da Deutschland nicht nur die Vorgaben von NIS-2 über das neue Artikelgesetz umsetzt, sondern zudem die Cybersicherheit insgesamt verbessern will, gehen die konkreten Maßnahmen aus dem Referentenentwurf in einigen Stellen weit über NIS-2 hinaus.

Neben den regulatorischen Vorgaben für das Risikomanagement schärft das NIS2UmsuCG auch beim Bußgeld nach. Mit Summen zwischen 100.000 Euro bis 20. Mio Euro liegt das NIS2UmsuCG deutlich über den Vorgaben aus NIS-2. Hinsichtlich der Haftung sind Geschäftsführer mitunter persönlich für die Umsetzung der Sicherheitsmaßnahmen in ihren Einrichtungen verantwortlich. Die staatliche Aufsicht wird im Zuge des NIS2UmsuCG um Registrierungs-Nachweis- und Meldepflichten ergänzt. Außerdem gilt ein verpflichtender Informationsaustausch.

Geltungsbereich

Im Gegensatz zu NIS-2 sieht das NIS2UmsuCG drei Betreibergruppen vor, die über das Gesetz reguliert werden. Die bisherigen Kritischen Infrastrukturen (KRITIS) aus dem BSIG bleiben als Kritische Anlagen mit den darin definierten Sektoren und Schwellenwerten in der Gesetzgebung bestehen. Darüber hinaus werden die besonders wichtigen und wichtigen Einrichtungen aus NIS-2 eingeführt, deren Eingliederung nach Mitarbeiterzahl und Umsatz erfolgt. Ebenso sind die in NIS-2 definierten Sektoren im NIS2UmsuCG enthalten. Ergänzend schließt die Regulierung öffentliche Einrichtungen des Bundes sowie verschiedene Ausnahmen ein – Landes- und Kommunalbehörden werden nicht adressiert. Die aus dem IT-Sicherheitsgesetz hergeleiteten Unternehmen im besonderen öffentlichen Interesse (UBI) werden in den besonders wichtigen bzw. wichtigen Einrichtungen mit aufgenommen. Die regulatorischen Vorgaben und Verpflichtungen an die jeweils betroffenen Unternehmen richten sich nach Betreibergruppen-Zugehörigkeit und etwaigen Ausnahmeregelungen. Alle vorgegebenen Maßnahmen sind dem Risiko angemessen und nach dem Stand der Technik umzusetzen.

NIS2UmsuCG: Sektoren und Pflichten

Sektoren	Kritische Anlagen	Besonders wichtige Einrichtungen	Wichtige Einrichtungen
	KRITIS - Kritische Infrastrukturen (gemäß BSI-KritisV, IT-SiG 2.0): Energie, Wasser, Ernährung, Gesundheit, Transport und Verkehr, Informationstechnik und Telekommunikation, Finanz- und Versicherungswesen, Entsorgung	**Großunternehmen** (gemäß NIS-2 Anhang I): Energie, Verkehr und Transport, Trinkwasser, Abwasser, Gesundheitsweisen, Bankwesen, Finanzmärkte, Digitale Infrastruktur, IKT-Dienste, Weltraum **Mittlere Unternehmen:** Anbieter öffentlicher TK-Netze und TK-Dienste **Unabhängig der Größe:** Qualifizierte Vertrauensdienste, TLD-Registries, DNS-Dienste, KRITIS-Betreiber, Bundesministerien und Bundeskanzleramt	**Großunternehmen und Mittlere Unternehmen** (gemäß NIS-2 Anhang II): Logistik, Siedlungsabfallentsorgung, Produktion, Chemie, Ernährung, verarbeitendes Gewerbe, digitale Dienste, Forschung **Mittlere Unternehmen** (gemäß NIS-2 Anhang I): Energie, Verkehr und Transport, Trinkwasser, Abwasser, Gesundheitsweisen, Bankwesen, Finanzmärkte, Digitale Infrastruktur, IKT-Dienste, Weltraum **Unabhängig der Größe:** Vertrauensdienste, Hersteller Rüstungsgüter und VS-IT (UBI 1), Betreiber Betriebsbereich obere Klasse (UBI 3)

Pflichten	Kritische Anlagen	Besonders wichtige Einrichtungen	Wichtige Einrichtungen
§ 30 Risikomanagement-maßnahmen (verhältnismäßige TOM nach dem Stand der Technik)	●	●	●
§ 30 (3) erhöhte Anforderungen für Sicherheitsniveau	●		
§ 31 Meldepflichten (mehrstufig: 24h / 72h / Zwischenmeldung auf Anfrage / Abschlussmeldung nach 1 Monat)	●	●	●
§ 32 Registrierungspflicht	●	●	●
§ 33 Besondere Registrierungs-pflicht für Anbieter digitaler Dienste	●	●	●
§ 34 Nachweispflichten für besonders wichtige Einrichtungen	●	●	
§ 35 Unterrichtungspflichten	●	●	●
§ 36 Rückmeldungen des Bundesamts gegenüber meldenden Einrichtungen; Information der Öffentlichkeit	●	●	●
§ 37 Ausnahmebescheid	●	●	●
§ 38 Billigungs- und Überwachungspflicht für Leitungsorgane von Wesentlichen Einrichtungen und Wichtigen Einrichtungen; Schulungen	●	●	●
§ 39 Zusätzliche Anforderungen an Kritische Einrichtungen (Einsatz von Systemen zur Angriffserkennung)	●		

Risikomanagementmaßnahmen nach § 30

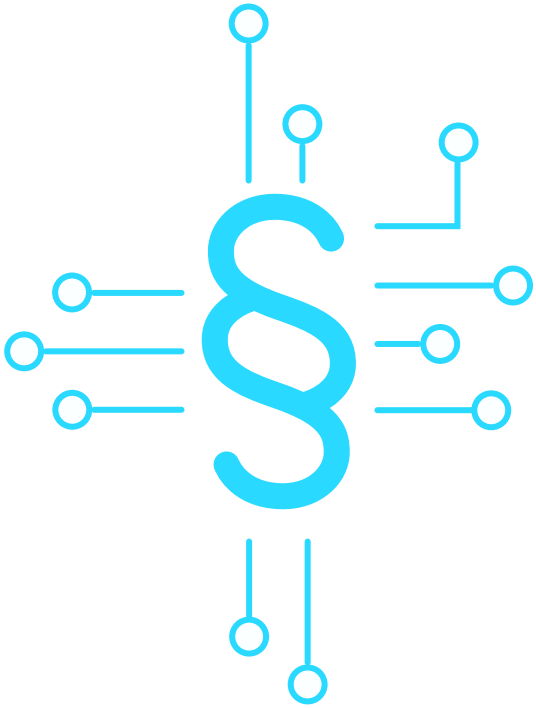
Gemäß § 30 müssen Betreiber kritischer Anlagen sowie besonders wichtiger und wichtiger Einrichtungen technisch-organisatorische Maßnahmen (TOMs) zur Absicherung von IT und Prozessen umsetzen, um dadurch Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit sicherzustellen. Dabei ist ein risikoorientierter Ansatz zu verfolgen, der eine angemessene Absicherung nach dem Stand der Technik vorsieht. Mindestens sind dabei folgende Themen umzusetzen:

1. **Risikoanalyse:** Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme.
2. **Sicherheitsvorfälle:** Bewältigung von Sicherheitsvorfällen.
3. **Aufrechterhaltung:** Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, sowie Krisenmanagement.
4. **Sicherheit der Lieferkette:** Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern.
5. **Sicherheit in der Entwicklung und Beschaffung:** Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen.
6. **Bewertung und Wirksamkeit:** Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit.
7. **Schulung und Cyberhygiene:** Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit.
8. **Kryptografie:** Konzepte und Verfahren für den Einsatz von Kryptografie und Verschlüsselung.
9. **Personal, Zugriffe, Anlagen:** Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen.
10. **Authentifizierung und (Notfall-)Kommunikation:** Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

NIS2UmsuCG: Ersteinschätzung aus Politik und Wirtschaft

Aus Gesprächen mit dem BMI, Parlamentariern, Anwälten und dem Branchenverband Bitkom geht hervor, dass vor allem der kurze Umsetzungszeitraum für viele betroffene Betreiberfirmen eine große Herausforderung darstellen wird – insbesondere, wenn das jeweilige Unternehmen bislang wenig in das Thema Cybersicherheit investiert hat und quasi bei null beginnt.

Nimmt man den IT-Grundschutz des BSI als Orientierung für die Umsetzung der drängendsten NIS-2-Themen sollten Firmen mindestens sechs Monate Umsetzungszeit veranschlagen; Tendenz länger, da externe Abhängigkeiten zu Beratern und Prüfern bestehen. Vor dem Hintergrund, dass durch NIS-2 mehrere Tausend Firmen vor denselben Herausforderungen stehen und damit die verfügbaren Ressourcen nochmals knapper werden dürften, empfiehlt es sich, die Umsetzung frühestmöglich anzustoßen.



Anhang

NIS-2 reguliert bestimmte Betreiber und Branchen unabhängig ihrer Größe als wesentliche oder wichtige Einrichtungen. Diese Ausnahmen finden Sie nachfolgend aufgeführt.

Wesentliche Einrichtungen:

- **Digitale Infrastruktur** (Qualified Trust Service Provider, TLD Registries, Domain-Registrare, Anbieter elektronischer Kommunikation (ab mittlerer Unternehmensgröße)
- **Öffentliche Verwaltung** (Verwaltungsorgane aus der Zentralregierung oder kritische Verwaltungsorgane regionaler Ebene)
- **Sonderfälle, die von den Mitgliedsstaaten als wesentlich definiert sind:**
  - Einzige Anbieter des Dienstes (sole provider) mit gesellschaftlich oder wirtschaftlich kritischer Rolle
  - Betreiber, deren Ausfall die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit gefährden könnte.
  - Betreiber, deren Ausfall ein wesentliches Systemrisiko darstellt, insbesondere hinsichtlich grenzübergreifender Auswirkungen.
  - Betreiber mit besonderer nationaler, regionaler oder sektoraler Bedeutung
- **Kritische Einrichtungen** (eingestuft nach EU RCE bzw. CER-Richtlinie (EU 2022/2557))
- **Bisherige KRITIS-Betreiber:** Unternehmen, die bereits vor dem 16. Januar 2023 gemäß der Richtlinie (EU) 2016/1148 oder nach nationalem Recht (z.B. IT-Sicherheitsgesetz) als Betreiber wesentlicher Dienste eingestuft wurden.

Wichtige Einrichtungen:

- **Sonderfälle, die von den Mitgliedsstaaten als wichtig definiert sind:**
  - Einzige Anbieter des Dienstes (sole provider) mit gesellschaftlich oder wirtschaftlich kritischer Rolle
  - Betreiber, deren Ausfall die öffentliche Ordnung, die öffentliche Sicherheit oder die öffentliche Gesundheit gefährden könnte.
  - Betreiber, deren Ausfall ein wesentliches Systemrisiko darstellt, insbesondere hinsichtlich grenzübergreifender Auswirkungen.
  - Betreiber mit besonderer nationaler, regionaler oder sektoraler Bedeutung

Profitieren Sie von zertifizierter KRITIS-Kompetenz

- **BSI-KRITIS-qualifiziert:** Myra erfüllt als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister
- **Hochzertifizierte Qualität:** ISO 27001 auf Basis von IT-Grundschutz, PCI-DSS-zertifiziert, IDW PS 951 Typ 2 (ISAE 3402) geprüft, BSI-KRITIS-qualifiziert, BSI-C5-Testat Typ 2, DIN-EN-50600-zertifizierte Rechenzentren, Trusted Cloud
- **KRITIS-Cluster:** DSGVO- und IT-SiG-konforme, mehrfach georedundante Server-Infrastruktur in Deutschland
- **Made in Germany:** Volle technische Kontrolle, permanente Weiterentwicklung, 24/7-Full-Service- Betreuung durch unsere IT-Experten im Security Operations Center
- **Green IT:** Zertifizierte Umwelt- und Energiemanagementsysteme der Rechenzentren nach ISO 14001 und ISO 50001

BSI-geprüfte IT-Sicherheit

Die Myra-Technologie ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Standard ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Zudem erfüllen wir als einer der führenden Anbieter weltweit alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | EU-DSGVO konform | BSI C5 Testat Typ 2 | Trusted Cloud | ISAE 3402 IDW PS 951 Type 2 | DIN EN 50600 zertifiziert Betriebssicheres Rechenzentrum

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard | KRITIS-qualifiziert nach §3 BSI-Gesetz | Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600

Myra ist Ihr Compliance-Garant für NIS-2

Die Myra-Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic bevor virtuelle Angriffe einen realen Schaden anrichten. Unsere zertifizierte Security-as-a-Service-Plattform schützt Ihre digitalen Geschäftsprozesse vor vielfältigen Risiken wie DDoS-Angriffen, Bot-Netzwerken und Angriffen auf Datenbanken.

Bundesministerium für Gesundheit | ITSG | msc Munich Security Conference | Barmenia Einfach. Menschlich. | Finanzportal | BZgA Bundeszentrale für gesundheitliche Aufklärung | BIOSCIENTIA Medizin. Labor. Service. | Liechtensteinische Landesbank 1861

Made in Germany

Myra Security ist der neue Maßstab für globale IT-Sicherheit.

Sie wollen mehr darüber erfahren, wie Sie mit unseren Lösungen Ihren Umsatz steigern, Ihre Kosten minimieren und Ihre Anwendungen vor bösartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihr Unternehmen. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

Kostenlose Schutzberatung anfordern →

Myra Security GmbH

+49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com