TÜVIT

NIS-2-Richtlinie

Vor welchen Herausforderungen Unternehmen stehen und wie die optimale Vorbereitung aussieht

Inhalt

1. Die NIS-2-Richtlinie revolutioniert die Cybersicherheit

Mit der EU-Richtlinie NIS-2 („The Network and Information Security Directive“) kommt auf Unternehmen eine neue Herausforderung zu, die nicht zu unterschätzen ist. Denn die NIS-1-Nachfolgerin bringt strengere Anforderungen mit sich und verlangt von Unternehmen, dass diese ihre bisherigen Cybersicherheitsstrategien verstärken. Für viele Organisationen geht das mit einem erheblichen Mehraufwand einher, auf den es sich frühzeitig vorzubereiten gilt. Was Sie in Bezug auf die NIS-2-Richtlinie unbedingt beachten sollten und wie Sie sich bestmöglich auf die bevorstehenden Anforderungen vorbereiten, erfahren Sie in diesem Whitepaper.

Die fortschreitende Digitalisierung sowie die zunehmende Vernetzung stellen Unternehmen und Organisationen in Bezug auf die Sicherheit ihrer Netzwerke und Informationssysteme vor immer komplexere Herausforderungen. Zeitgleich nehmen Cyberbedrohungen stetig zu und können erhebliche Auswirkungen auf die kritischen Infrastrukturen und digitalen Dienste haben, die unser tägliches Leben unterstützen.

Um diesen Herausforderungen zu begegnen, hat die Europäische Union die NIS-2-Richtlinie entwickelt. Die Richtlinie baut auf dem Erfolg der vorherigen NIS-1-Richtlinie auf und zielt darauf ab, ein höheres Maß an Netzwerk- und Informationssicherheit innerhalb der EU zu gewährleisten.

Dabei stellt NIS-2 einen bedeutenden Schritt in Richtung einer umfassenden und kohärenten Cybersicherheitsstrategie dar, indem sie den **Anwendungsbereich der Richtlinie erweitert, die Sicherheitsanforderungen verschärft und detailliertere Meldepflichten festlegt**. Auf diese Weise zielt sie darauf ab, die Widerstandsfähigkeit von kritischen Infrastrukturen und digitalen Diensten sowie die Fähigkeit der Mitgliedstaaten zur Reaktion auf und Bewältigung von Cyberbedrohungen zu stärken. Damit ebnet die NIS-2-Richtlinie den Weg für eine sicherere und widerstandsfähigere digitale Zukunft für Unternehmen innerhalb der EU.

Mit diesem Whitepaper möchten wir Ihnen eine Hilfestellung an die Hand geben, die einerseits konkret darauf eingeht, welche Auswirkungen die Richtlinie letztendlich hat, und andererseits Lösungen aufzeigt, wie Sie Ihre Pflichten erfüllen können, um die Sicherheit Ihrer Netzwerke und Informationssysteme zu gewährleisten.

KEY-FACTS
Die NIS-2-Richtlinie ...

- ist für alle EU-Mitgliedstaaten verbindlich
- stellt für Deutschland eine Konsolidierung der bestehenden KRITIS- und BSI-Gesetze dar
- ist eine systematische und umfangreiche Erweiterung der bestehenden KRITIS-Anforderungen auf weitere Zielgruppen sowie Unternehmen
- repräsentiert das erste Gesetz, das sehr konkrete Vorgaben auch für den Mittelstand definiert
- geht mit einer massiven Erweiterung der BSI-Kompetenzen einher
- ist bereits seit 2023 auf EU-Ebene in Kraft
- ist als EU-Richtlinie nicht direkt anwendbar, sondern erst in nationales Recht umzusetzen (Stichtag: **17.10.2024**)
- ist das deutsche Gesetz zur Umsetzung der Richtlinie (Das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) ist noch nicht erlassen (nach aktuellem Stand im **März 2025**))

2. Ist mein Unternehmen von der NIS-2-Richtlinie betroffen?

„Ist mein Unternehmen betroffen?“ ist wohl die erste und wichtigste Frage, die sich die meisten Organisationen in Bezug auf die NIS-2-Richtlinie stellen. Um hierauf eine Antwort zu finden, haben wir nachfolgend vier Schritte aufgeführt, mithilfe derer Sie bestimmen können, ob auch Ihr Unternehmen unter die NIS-2-Richtlinie fällt.

2.1. Schritt 1: Unternehmenssektor

Im ersten Schritt muss zunächst geprüft werden, ob Ihr Unternehmen zu einem der 18 relevanten Sektoren gehört. Diesbezüglich differenziert die NIS-2-Richtlinie zwischen 11 Sektoren mit hoher Kritikalität („Essential“) sowie 7 weiteren „sonstigen“ kritischen Sektoren („Important“). Diese NIS-2-Sektoren ähneln denen der deutschen KRITIS-Einstufung.

SEKTOREN MIT HOHER KRITIKALITÄT – ESSENTIAL ENTITIES[1]

Energie

- Elektrizität, Fernwärme, Erdöl, Erdgas, Wasserstoff
- KRITIS-Sektor „Energie“

Transport

- Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr
- KRITIS-Sektor „Transport“

Bankwesen (Kreditinstitute)

- KRITIS-Sektor „Finanzwesen“

Finanzmarktinfrastruktur

- Handelsplätze, Zentrale Gegenpartien
- KRITIS-Sektor „Finanzwesen“

Gesundheit

- Gesundheitsdienstleister, EU-Labore, Medizinforschung, Pharmazeutik, Medizingeräte
- KRITIS-Sektor „Gesundheit“

Trinkwasser

- Wasserversorgung
- KRITIS-Sektor „Wasser“

Abwasser

- Abwasserentsorgung
- KRITIS-Sektor „Wasser“

Digitale Infrastruktur

- Internet-Knoten (IXP), DNS (ohne Root), TLD Registries, Cloud Provider, Rechenzentren, CDNs, Vertrauensdienste (TSP), Elektronische Kommunikation
- KRITIS-Sektor „IT“, teilweise TKG (Telekommunikationsgesetz)

IKT-Dienstleistungsmanagement

- B2B: Managed Service Providers, Managed Security Service Providers
- Keine KRITIS-Entsprechung

Öffentliche Verwaltungen

- Zentralregierung, Regionale Regierung
- Keine KRITIS-Entsprechung

Weltraum

- Bodeninfrastruktur
- Teilweise KRITIS-Sektor „Transport“

1 Vgl. Richtlinie (EU) 2022/2555, Anhang I

2. Ist mein Unternehmen von der NIS-2-Richtlinie betroffen?

SONSTIGE KRITISCHE SEKTOREN – IMPORTANT ENTITIES[2]
Post- und Kurierdienste
■ Postdienste ■ Teilweise KRITIS-Sektor „Transport“
Abfallwirtschaft
■ Abfallbewirtschaftung ■ KRITIS-Sektor „Entsorgung“
Produktion, Herstellung von Medizinprodukten, Maschinen, Fahrzeugen sowie elektrischen/elektronischen Geräten
■ KRITIS-Sektor „UBI“ (2)
Digitale Anbieter
■ Marktplätze, Suchmaschinen, Soziale Netzwerke ■ KRITIS-Sektor teilweise „TMG“ (Telemediengesetz)
Forschung
■ Forschungsinstitute ■ Keine KRITIS-Entsprechung

2.2. Schritt 2: Unternehmensgröße

In einem zweiten Schritt muss die Größe des Unternehmens herangezogen werden, um zu definieren, ob es sich um eine wesentliche („Essential“) oder eine wichtige („Important“) Einrichtung handelt.

WESENTLICHE EINRICHTUNGEN	WICHTIGE EINRICHTUNGEN
> 250 Beschäftigte	50-250 Beschäftigte
> 50 Mio. € Umsatz	10-50 Mio. € Umsatz
> 43 Mio. € Bilanz	< 43 Mio. € Bilanz

2.3. Schritt 3: Sonderfall – Ja oder Nein?

Unabhängig von der Größe und des Umsatzes sind nachfolgende Unternehmen ebenfalls von der NIS-2-Richtlinie betroffen. Diese Unternehmen können vom Anwendungsbereich der NIS-2-Richtlinie erfasst sein, auch wenn sie weniger als 50 Mitarbeitende haben oder ihr Jahresumsatz unter 10 Mio. Euro liegt[3]:

- 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-Mitgliedstaat gesehen werden, der kritisch für das öffentliche Leben ist
- Unternehmen, deren Störung einen wesentlichen Effekt auf die öffentliche Ordnung, Sicherheit oder Gesundheit hat
- Unternehmen, die bereits vor dem 16. Januar 2023 gemäß der Richtlinie (EU) 2016/1148 oder nach nationalem Recht als Betreiber wesentlicher Dienste eingestuft wurden[4]

Eine Ausnahme bilden Anbieter öffentlicher elektronischer Kommunikationsnetze. Hier sind nur Unternehmen von mindestens mittlerer Unternehmensgröße (siehe Schritt 2 „Wichtige Einrichtungen“) betroffen.

2 Vgl. Richtlinie (EU) 2022/2555, Anhang II

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

4 Vgl. Richtlinie (EU) 2022/2555, Artikel 3, Absatz 1

2.4. Schritt 4: Fällt mein Unternehmen vielleicht gar nicht unter die NIS-2-Richtlinie?

Ausnahmen bestehen nicht nur für Unternehmen und Institutionen, die über Schritt 1 und 2 hinaus unter die NIS-2-Richtlinie fallen, Unternehmen und Institutionen können auch grundsätzlich von der Richtlinie ausgenommen sein. So zum Beispiel Einrichtungen, die Tätigkeiten in Bereichen wie Verteidigung oder nationale Sicherheit, öffentliche Sicherheit und Strafverfolgung ausüben. Auch Justiz, Parlamente und Zentralbanken sind vom Anwendungsbereich ausgeschlossen.

Für öffentliche Verwaltungen wird NIS-2 dagegen auf zentraler und regionaler Ebene gelten.

Darüber hinaus können die Mitgliedstaaten beschließen, dass sie auch für derartige Einrichtungen auf lokaler Ebene gilt.

Prüfen Sie jetzt mit unserem NIS-2 Betroffenheits-Check in nur wenigen Klicks, ob Ihr Unternehmen unter die Richtlinie fällt!

3. Welche Pflichten habe ich als betroffenes Unternehmen?

Die für kritische Infrastrukturen bislang bestehenden Vorgaben werden mit dem NIS2UmsuCG nicht nur konkretisiert, sondern zugleich verschärft. Dies betrifft sowohl das Risikomanagement als auch die Melde-, Registrierungs-, Nachweis- sowie Unterrichtungspflichten.

3.1. Mindestmaßnahmen zur Risikoreduktion[5]

1. **Risikomanagement:** Überwachung von Maßnahmen zur Minimierung von Cyberrisiken
2. **Verantwortlichkeit des Managements**
3. **Policies:** Konzepte in Bezug auf die Risikoanalyse und Sicherheit für Informationssysteme
4. **Vorfallbewältigung:** Prävention, Detektion und Bewältigung von Sicherheitsvorfällen
5. **Business Continuity:** Aufrechterhaltung des Betriebs (wie Backup-Management und Wiederherstellung nach einem Notfall) und Krisenmanagement
6. **Supply Chain:** Ausfallsicherheit der Lieferkette
7. **Einkauf:** Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen
8. **Wirksamkeit:** Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen
9. **Schulungen:** Cyberhygiene und Schulungen im Bereich der Cybersicherheit
10. **Kryptografie:** Konzepte und Verfahren für den Einsatz von Kryptografie und gegebenenfalls Verschlüsselung
11. **Personal, Zugriff & Asset-Management:** Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Assets
12. **Authentifizierung & Kommunikation:** Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme

5 Vgl. Richtlinie (EU) 2022/2555, Artikel 21 Absatz 2

3. Welche Pflichten habe ich als betroffenes Unternehmen?

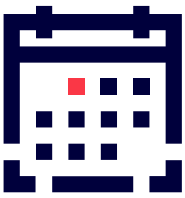
Bereiten Sie sich als Unternehmensleitung darauf vor, Verantwortung im Bereich Risikomanagement übernehmen zu können und informieren Sie sich über entsprechende Schulungsangebote.

3.2. Meldepflicht[6]

Signifikante Störungen, Vorfälle und Cyber-Bedrohungen sind von Unternehmen unverzüglich bei ihrer nationalen Cyber Security Authority zu melden. In Deutschland ist die zuständige Behörde das Bundesamt für Sicherheit in der Informationstechnik (BSI).

Vorgesehen ist dafür der folgende dreistufige Prozess:

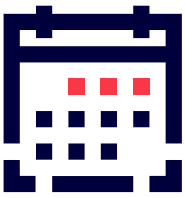
1.



Innerhalb von 24 Stunden ...

... nach Bekanntwerden eines Vorfalls muss ein **vorläufiger Bericht** übermittelt werden.

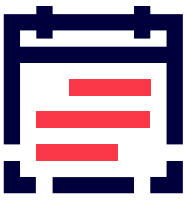
2.



Innerhalb von 72 Stunden ...

... muss ein **vollständiger Bericht** folgen, der auch eine erste **Bewertung des Vorfalls** enthält.

3.



Innerhalb eines Monats ...

... muss ein **Abschlussbericht** eingereicht werden, der detaillierte Beschreibungen des Vorfalls, der Art der Bedrohung und der grenzüberschreitenden Auswirkungen enthält.

6 Vgl. Richtlinie (EU) 2022/2555, Artikel 23

4. Welche Sanktionen könnten auf mein Unternehmen zukommen, wenn ich meinen Pflichten nicht nachkomme?

Gemäß der NIS-2-Richtlinie können Unternehmen Sanktionen auferlegt werden, wenn sie gegen die Sicherheitsanforderungen und Pflichten der Richtlinie verstoßen. Zu diesen zählen:

WESENTLICHE EINRICHTUNGEN[7]	WICHTIGE EINRICHTUNGEN[8]
▪ Vor-Ort-Kontrollen, Ad-hoc-Prüfungen	▪ Vor-Ort-Kontrollen, gezielte Sicherheitsprüfungen
▪ Verlangen von Nachweisen	▪ Verlangen von Nachweisen, Sicherheitsscans
▪ Warnungen	▪ Warnungen
▪ Verbindliche Anweisungen	▪ Verbindliche Anweisungen
▪ Umsetzung der Empfehlungen der Sicherheitsüberprüfung mit entsprechender Fristsetzung	▪ Umsetzung der Empfehlungen der Sicherheitsüberprüfung mit entsprechender Fristsetzung
▪ Benennung eines Überwachungsbeauftragten	
▪ Öffentliche Bekanntmachung der Verstöße	▪ Öffentliche Bekanntmachung der Verstöße
▪ Aussetzung von Zertifizierungen	
▪ Persönliche Haftung der Führungskräfte	▪ Persönliche Haftung der Führungskräfte
Geldbuße mit einem Höchstbetrag **von mind. € 10 Mio. oder mind. 2 % des weltweiten Konzernumsatzes** des Vorjahres (je nachdem, was höher ist)	**Geldbuße** mit einem Höchstbetrag **von mind. € 7 Mio. oder mind. 1,4 % des weltweiten Konzernumsatzes** des Vorjahres (je nachdem, was höher ist)

Darüber hinaus bleiben die Anforderungen der Datenschutzgrundverordnung (DSGVO) an die Verarbeitung personenbezogener Daten sowie die dort vorgesehenen Sanktionsmöglichkeiten von der NIS-2-Richtlinie unberührt.

Die für die NIS-2-Richtlinie zuständigen Behörden, in Deutschland das BSI, sind jedoch verpflichtet, eng mit den Datenschutzbehörden zusammenzuarbeiten. Somit wächst für Unternehmen das Risiko vermehrter Bußgelder, da neben den empfindlichen Geldstrafen, die bereits seit 2018 nach der DSGVO verhängt werden können, nun auch Bußgelder gemäß NIS-2-Richtlinie erlassen werden können.

Sie brauchen Hilfe zur Umsetzung der DSGVO und des BDSG und möchten sich auch hier vor den drohenden Bußgeldern schützen, die im Ernstfall bis zu **4 % des gesamten weltweit erzielten Jahresumsatzes**[9] betragen können?

Unsere Datenschutz-Expert:innen unterstützen Sie mit unterschiedlichsten Leistungen. Diese finden Sie unter **https://www.tuvit.de/de/leistungen/datenschutz/**

7 Vgl. Richtlinie (EU) 2022/2555, Artikel 32, Absatz 4 ff.

8 Vgl. Richtlinie (EU) 2022/2555, Artikel 32, Absatz 4

9 Vgl. Art. 83 Abs. 5 DSGVO

5. Wer kontrolliert die Umsetzung der NIS-2-Richtlinie?

Die Umsetzung der NIS-2-Richtlinie wird in den Mitgliedstaaten der Europäischen Union durch nationale Behörden kontrolliert. Jeder Mitgliedstaat ist verpflichtet, eine oder mehrere nationale zuständige Behörde(n) zu benennen, die für die Überwachung und Durchsetzung der Richtlinie verantwortlich ist bzw. sind. Diese Behörden haben die Aufgabe, sicherzustellen, dass die in der Richtlinie festgelegten Sicherheitsanforderungen von den betroffenen Unternehmen und Organisationen eingehalten werden.

Zusätzlich zu den nationalen Behörden gibt es auf EU-Ebene die Zusammenarbeit zwischen den nationalen Behörden im Rahmen des CSIRTs-Netzwerks (Computer Security Incident Response Teams) und der NIS-Kooperationsgruppe, die ebenfalls eine Rolle bei der Überwachung und Koordination der Umsetzung der Richtlinie spielen. Diese Gremien fördern den Austausch von Informationen sowie zu bewährten Verfahren zwischen den Mitgliedstaaten und unterstützen die harmonisierte Anwendung der Richtlinie in der gesamten EU.

Die spezifischen Behörden und ihre genauen Rollen können von Land zu Land variieren. Generell sind es jedoch die nationalen Behörden für Cybersicherheit oder ähnliche regulierende Institutionen, die für die Überwachung der Einhaltung der NIS-2-Richtlinie zuständig sind.

In Deutschland ist das **Bundesamt für Sicherheit in der Informationstechnik (BSI)** die zuständige Aufsichtsbehörde. Unternehmen, die zu den besonders wichtigen Einrichtungen oder KRITIS-Betreibern zählen, müssen dem BSI alle zwei Jahre nachweisen, dass sie die NIS-2-Maßnahmen umgesetzt haben. Den Zeitpunkt des ersten Audits legt das BSI nach der Registrierung des Unternehmens fest – spätestens jedoch vier Jahre nach Inkrafttreten des neuen Gesetzes. Ähnlich wie bisher die KRITIS-Audits werden die Audits von externen Auditor:innen durchgeführt. Stellen die Auditor:innen Mängel fest, haben die Unternehmen anschließend die Möglichkeit, diese innerhalb einer bestimmten Frist zu beheben.

6. Wie mache ich mein Unternehmen NIS-2 konform?

Damit auch Sie und Ihr Unternehmen auf der sicheren Seite sind, sollten Sie die Maßnahmen zur Risikoreduktion schnellstmöglich angehen.

Hierzu bieten wir Ihnen unterschiedliche Dienstleistungen an, um Sie NIS-2 konform aufzustellen und damit das Risiko von Bußgeldern zu minimieren.

6.1. NIS-2 Betroffenheits-Check und Erstberatung

Zunächst sollten Sie feststellen, ob Ihr Unternehmen unter die NIS-2 Richtlinie fällt.

Hierzu bieten wir zum einen online unseren **NIS-2 Betroffenheits-Check** als unverbindlichen Schnell-Check an. Zum anderen unterstützen wir Sie mit **Erstberatung** im Hinblick auf die NIS-2-Thematik für Ihr Unternehmen.

Mehr unter **https://www.tuvit-consulting.de/de/leistungen/informationssicherheit-cyber-security/nis-2-betroffenheits-check/**

6.2. Vor-Audits und Deltachecks von NIS-1 zu NIS-2

War Ihr Unternehmen bereits von NIS-1 betroffen und Sie haben sich nun auf NIS-2 vorbereitet bzw. sind mittendrin? Prüfen Sie mit uns, was auf der Habenseite steht und was es noch zu tun gibt. Wir bringen Licht ins Dunkel mit:

- Deltaprüfungen NIS-1 zu NIS-2
- Voraudits

Mehr unter: **https://www.tuvit-consulting.de/de/leistungen/informationssicherheit-cyber-security/nis-2-betroffenheits-check/**

6.3. Informationssicherheitsmanagementsystem

Die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) gemäß NIS-2, das Regeln und Prozesse für die Informationssicherheit umfasst, erfordert Zeit und Anstrengung. Wenn Ihr Unternehmen von der neuen Richtlinie betroffen ist, ist es wichtig, nicht nur ein Expertenteam zu haben, das die Einführung oder Erweiterung des ISMS überwacht, sondern auch sicherzustellen, dass die Belegschaft ein grundlegendes Verständnis dafür bekommt, wie wichtig NIS-2 – und damit das Thema Cybersicherheit – sowie die Einhaltung entsprechender Vorgaben sind. Bedingt durch Abstimmungsprozesse, Richtlinienerstellung und Schulungen kann dieser Prozess zeitaufwendig sein, was im Rahmen der Budgetplanung einbezogen werden sollte.

Für Unternehmen, die eine Zertifizierung gemäß DIN ISO/IEC 27001:2022 oder BSI IT-Grundschutz für ihr ISMS anstreben, ist es ratsam, je nach individuellem Reifegrad mit einer Einführungszeit von etwa ein bis zwei Jahren zu rechnen. Obwohl eine Zertifizierung nicht zwingend vorgeschrieben ist, kann sie im Hinblick auf zukünftige Compliance-Anforderungen sinnvoll sein. Zudem erleichtert sie den Nachweis über ein wirksames ISMS gegenüber Kunden, Lieferanten oder dem Bundesamt für Sicherheit in der Informationstechnik (BSI).

6.3.1. Implementierung, Prüfung & Zertifizierung eines ISMS nach ISO 27001

Die ISO 27001 ist ein weltweit anerkannter Standard für Informationssicherheitsmanagementsysteme (ISMS). Die Einführung eines ISMS gemäß ISO 27001 unterstützt Unternehmen dabei, Risiken systematisch zu managen, Sicherheitskontrollen zu etablieren und die Anforderungen von NIS-2 in Bezug auf Informationssicherheit sowie Berichterstattung über Sicherheitsvorfälle zu erfüllen. Eine Zertifizierung nach ISO 27001 ist zudem ein wirksames Mittel, um die Einhaltung der Sicherheits- und Berichterstattungsanforderungen zu belegen.

Unsere Leistungen

- Beratungsdienstleistungen zur Implementierung eines ISMS nach ISO 27001
  Mehr unter: **https://www.tuvit-consulting.de/de/leistungen/informationssicherheit-cyber-security/**
- GAP-Analysen, interne Audits, Prüf- und Zertifizierungsdienstleistungen
  Mehr unter: **https://www.tuvit.de/de/leistungen/informationssicherheitsmanagement/iso-27001/**

6.3.2. Implementierung, Prüfung & Zertifizierung eines ISMS nach ISO 27001 auf der Basis von IT-Grundschutz

Eine BSI IT-Grundschutz-Zertifizierung kann ebenfalls dazu beitragen, den Anforderungen von NIS-2 zu entsprechen. Das BSI IT-Grundschutz-Zertifikat belegt, dass Ihr Unternehmen die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) empfohlenen Maßnahmen zur Informationssicherheit implementiert hat. Obwohl sie keine explizite Anforderung gemäß der NIS-2-Richtlinie ist, kann die BSI IT-Grundschutz-Zertifizierung dennoch als Nachweis darüber dienen, dass angemessene Sicherheitsmaßnahmen entsprechend den anerkannten Standards umgesetzt wurden. Letztlich kann eine solche Zertifizierung das Vertrauen von Behörden und anderen Interessengruppen in die Sicherheitsmaßnahmen des Unternehmens stärken und somit zur Erfüllung der NIS-2-Anforderungen beitragen.

Unsere Leistungen

- Beratungsdienstleistungen zur Implementierung eines ISMS nach BSI IT-Grundschutz
  Mehr unter: **https://www.tuvit-consulting.de/de/leistungen/informationssicherheit-cyber-security/**

Prüf- und Zertifizierungsdienstleistungen:

- Standortbestimmung bezüglich der IT-Sicherheit in Ihrer Organisation
- Analyse & Bewertung des Managements der Informationssicherheit nach IT-Grundschutz
- Durchführung von GAP-Analysen zur Bestimmung von Abweichungen
- ISMS-Assessments durch lizenzierte & erfahrene ISMS-Auditor:innen
- Planung & Durchführung von IT-Grundschutz-Audits als Basis für Zertifizierungen nach ISO 27001
- Planung & Durchführung von Lieferantenaudits

Mehr unter: **https://www.tuvit.de/de/leistungen/informationssicherheitsmanagement/it-grundschutz/**

6.4. Business Continuity Management

Ein Business Continuity Management (BCM) kann Ihr Unternehmen dabei unterstützen, die Anforderungen von NIS-2 zu erfüllen. Durch die Implementierung eines BCM zeigt ein Unternehmen, dass es angemessene Maßnahmen ergriffen hat, um auf Sicherheitsvorfälle zu reagieren und die Kontinuität von geschäftskritischen Prozessen zu gewährleisten. Dies ist von Bedeutung, da NIS-2 die Sicherheit und die Widerstandsfähigkeit von Unternehmen und Organisationen in Bezug auf ihre digitalen Dienste und Prozesse betrifft.

Indem Ihr Unternehmen ein BCM implementiert, demonstriert es, dass es in der Lage ist, auf Sicherheitsvorfälle angemessen zu reagieren und die Auswirkungen auf geschäftskritische Aktivitäten weitestgehend zu minimieren. Damit trägt ein BCM dazu bei, die Erfüllung der NIS-2-Anforderungen zu unterstützen, da es einen wichtigen Aspekt der Resilienz und Sicherheit von Informationssystemen abdeckt. Letztlich kann ein BCM nach ISO 22301 damit einen Beitrag dazu leisten, die Widerstandsfähigkeit des Unternehmens gegenüber Cyberbedrohungen zu stärken und somit den Vorgaben von NIS-2 gerecht zu werden.

Unsere Leistungen:

- Aufbau eines Business Continuity Management Systems (BCMS)
  - Preparation
  - Entwicklung & Implementierung
  - (Vor-)Audits & Zertifizierungsvorbereitung

  Mehr unter: **https://www.tuvit-consulting.de/de/leistungen/informationssicherheit-cyber-security/bcm/**

- Prüfung und Zertifizierung eines BCMS nach ISO 22301
  - GAP-Analysen zum aktuellen Ist-Zustand der BCM-Umsetzung nach ISO 22301
  - Prüfung Ihres BCMs nach ISO 22301

  Mehr unter: **https://www.tuvit.de/de/leistungen/informationssicherheitsmanagement/iso-22301/**

6.5. § 8a Audits gemäß BSIG

Ein § 8a Audit gemäß des BSI-Getzes kann Ihnen dabei helfen, die Anforderungen von NIS-2 zu erfüllen. Das Audit überprüft die Implementierung angemessener Sicherheitsmaßnahmen zur Gewährleistung der Informationssicherheit. Ein erfolgreiches § 8a Audit kann das Vertrauen von Behörden und anderen Interessengruppen in die Sicherheitsmaßnahmen Ihres Unternehmens stärken, indem es belegt, dass die erforderlichen Maßnahmen zur Risikominderung und angemessenen Reaktion auf Sicherheitsvorfälle implementiert wurden. Letztlich trägt ein § 8a Audit gemäß BSIG dazu bei, die Erfüllung der NIS-2-Anforderungen zu unterstützen und die Sicherheit der betroffenen Informationssysteme zu gewährleisten.

Unsere Leistungen

- Prüfung nach § 8a BSIG
  - Planung und Vorbereitung der Prüfung
  - Optional: Stellung von Branchenexpert:innen
  - Durchführung der Prüfung
  - Erstellung aller Nachweisdokumente

- GAP-Analysen zur Reifegrad-Ermittlung Ihres ISMS
  - Sichtung der zur Verfügung gestellten Unterlagen und Pläne (im Vorfeld)
  - Auditierung vor Ort (Begehung der Räumlichkeiten, Durchführung von Interviews und Stichproben) sowie
  - nachgelagert die Erstellung eines Berichts mit Feststellungen und Schlussfolgerungen

- GAP-Analysen zu branchenspezifischem Sicherheitsstandard (B3S)
  - Sichtung der zur Verfügung gestellten Unterlagen und Pläne (im Vorfeld)
  - Auditierung vor Ort (Begehung der Räumlichkeiten, Durchführung von Interviews und Stichproben) sowie
  - nachgelagert die Erstellung eines Berichts mit Feststellungen und Schlussfolgerungen

Mehr unter: **https://www.tuvit.de/de/leistungen/informationssicherheitsmanagement/kritis/**

6.6. Sichere Lieferketten

Betreiber einer KRITIS-Infrastruktur sind nach NIS-2 verpflichtet, für die Ausfallsicherheit ihrer Lieferketten zu sorgen. Auf Lieferantenseite bedeutet das: IT-Systeme, Devices und Komponenten so zu entwickeln und zu fertigen, dass sie die hohen Anforderungen an IT-Sicherheit erfüllen – ganz besonders bei deren Einsatz in einer kritischen Infrastruktur. Wir erbringen den Nachweis für die in der NIS-2 geforderten Pflichten.

6.6.1. Beschleunigte Sicherheitszertifizierung (BSZ)

Auch die Beschleunigte Sicherheitszertifizierung (BSZ) ist, insbesondere im Hinblick auf Lieferketten, für die NIS-2-Richtlinie von Relevanz, da sie dazu beiträgt, die Sicherheit von Produkten und Dienstleistungen zu gewährleisten, die in kritischen Infrastrukturen eingesetzt werden. Im Kontext von Lieferketten ermöglicht die BSZ eine schnellere und dennoch gründliche Zertifizierung von Produkten und Dienstleistungen, die in verschiedenen Phasen der Lieferkette verwendet werden. Dies trägt dazu bei, sicherzustellen, dass die Sicherheitsanforderungen gemäß der NIS-2-Richtlinie eingehalten werden, ohne dabei die Effizienz der Lieferkette zu beeinträchtigen. Die BSZ kann somit einen Beitrag dazu leisten, die Sicherheit entlang der gesamten Lieferkette zu verbessern, indem sie sicherstellt, dass Produkte und Dienstleistungen den erforderlichen Sicherheitsstandards entsprechen, bevor sie in kritischen Infrastrukturen zum Einsatz kommen.

Unsere Leistungen:

- Durchführung eines Pre-Pentests
- Review der Sicherheitsvorgaben
- Evaluierung des IT-Produktes nach BSZ

Mehr unter: **https://www.tuvit.de/de/leistungen/cyber-security/bsz/**

6. Wie mache ich mein Unternehmen NIS-2 konform?

6.6.2. Audits nach IEC 62443-X

Im Zusammenhang mit der NIS-2-Richtlinie fördert die IEC 62443 die Sicherung von Lieferketten, indem sie klare Sicherheitsanforderungen für Hersteller, Lieferanten und Betreiber von industriellen Steuerungssystemen festlegt. Dies ermöglicht es den in die Lieferkette eingebundenen Unternehmen, Sicherheitsstandards zu implementieren sowie sicherzustellen, dass Produkte und Dienstleistungen den erforderlichen Sicherheitsanforderungen entsprechen. Durch die Anwendung der Normreihe IEC 62443 können Lieferketten widerstandsfähiger gegen Cyberbedrohungen werden und somit dazu beitragen, die Ziele der NIS-2-Richtlinie im Hinblick auf die Sicherheit von Lieferketten zu erfüllen.

Unsere Leistungen:

- Scope-Bestimmung
- Voraudits zur Feststellung der Zertifizierungsreife
- Lieferantenbewertungen mit Hilfe der Security Scorecard
- Zertifizierungsaudit (inkl. Zertifizierung durch TÜV NORD CERT)

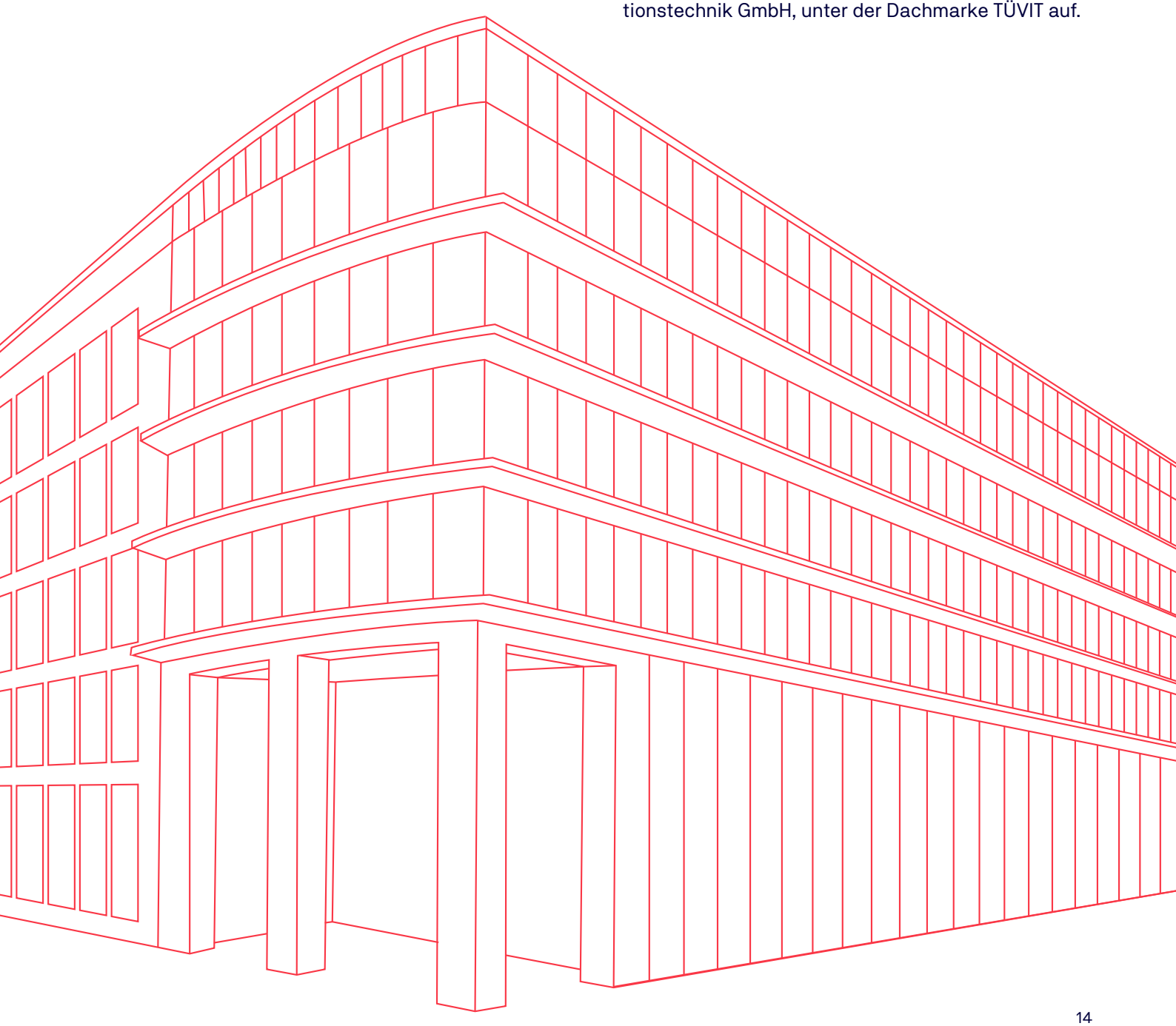
Mehr unter: **https://www.tuvit.de/de/themen/industrie-40/iec-62443/**

7. Über TÜV NORD IT Secure Communications

DIGITALISIERUNG. SICHER. GESTALTEN. Wir beraten Kunden in ihrem Bestreben, das Vertrauen in robuste, hoch verfügbare IT-Infrastrukturen und Organisationen zu stärken und begleiten Auftraggeber auf ihrem Weg der sicheren digitalen Transformation.

2018 in Berlin gegründet, ist TÜV NORD IT Secure Communications auf Consulting Services im Umfeld Informationstechnologien und Telekommunikation spezialisiert. Unsere Kernkompetenz ist die Beratung zu Sicherheitstechnologien im Rahmen der digitalen Transformation. Deren Mechanismen werden erst wirksam, wenn Resilienz, Cybersicherheit und Vertrauenswürdigkeit digitalisierter Infrastrukturen sowie deren Langlebigkeit und Robustheit gewährleistet sind.

Die TÜV NORD IT Secure Communications GmbH & Co. KG gehört zur Business Unit Digital & Semiconductor der TÜV NORD GROUP und tritt gemeinsam mit ihrem Schwesterunternehmen, der TÜV Informationstechnik GmbH, unter der Dachmarke TÜVIT auf.



TÜVIT

TÜV NORD IT Secure Communications GmbH & Co. KG
TÜV NORD GROUP
Hohenzollerndamm 184
10731 Berlin

tuvit-consulting.de

TÜV®

TÜVNORDGROUP