



Checkliste nach NIS-2-Kriterien

Hinweise für Unternehmen zur Umsetzung der NIS-2-Richtlinie

DOKUMENTINFORMATIONEN

Erstellt am:	12.12.2025		
Version	1.2		
Seitenanzahl	11	© 2025 Landesamt für Sicherheit in der Informationstechnik	TLP: CLEAR

INHALT

Einleitung.....	3
NIS-2 FAQ.....	3
NIS-2-Checkliste	5
Sanktionen	8
Weitere Empfehlungen und Hilfestellungen.....	9
Weiterführende Hinweise (Links).....	10
Glossar	10

Einleitung

Aufgrund der zunehmenden Digitalisierung und der gleichzeitig veränderten geopolitischen Gesamtlage sowie weiterer Herausforderungen hat der europäische Gesetzgeber weitreichende Anforderungen an die Informationssicherheit in der EU-NIS-2-Richtlinie formuliert. Dementsprechend mussten in Deutschland bestehende gesetzliche Regulierungen angepasst werden. Dies kann auch Auswirkungen auf Ihr Unternehmen beziehungsweise Ihre Organisation haben.

Die vorliegende Checkliste richtet sich an öffentliche und private Betreiber kritischer Infrastrukturen und an privatwirtschaftliche Unternehmen. Dieses Dokument unterstützt Sie dabei festzustellen, ob die gesetzlichen Änderungen auch für Ihr Unternehmen relevant sind, worin diese bestehen und dient einem erleichterten Einstieg in die sich aus der NIS-2-Richtlinie ergebenden Anforderungen. Es erhebt keinen Anspruch auf Vollständigkeit und stellt keine Rechtsberatung dar.

Die vorherige Version dieser Checkliste bezog sich auf den Regierungsentwurf (Stand 25.7.2025). Die aktuelle Version dieser Checkliste (1.2) bezieht sich nun auf das am 5. Dezember 2025 veröffentlichte Gesetz.

NIS-2 FAQ

Was ist NIS-2 und ist mein Unternehmen betroffen?

- Die NIS-2-Richtlinie der EU stellt eine Weiterentwicklung der ersten NIS-Richtlinie aus dem Jahr 2016 dar und regelt die Anforderungen an die Informationssicherheit betroffener Unternehmen und Organisationen.
- Sie sind verpflichtet selbstständig zu prüfen, ob Ihr Unternehmen betroffen ist, und falls ja, in welche Kategorie (wichtige Einrichtung, besonders wichtige Einrichtung, Betreiber kritischer Anlagen) Ihr Unternehmen fällt.
- Hinweis für Kommunen: Obwohl die NIS-2-Richtlinie auf die Kommunalverwaltung als solche nicht angewendet wird, ist unbedingt zu prüfen, ob kommunale Betriebe, insbesondere kritische Infrastrukturen wie beispielsweise Wasserversorgung oder Kläranlagen betroffen sind.
- Unter dem folgenden Link können Sie unverbindlich prüfen, ob Sie unter die NIS-2-Richtlinie fallen: <https://betroffenheitspruefung-nis-2.bsi.de/>

Was ist der Unterschied zwischen der europäischen Richtlinie und der deutschen Regelung?

- Die NIS-2-Richtlinie der EU ist am 16.01.2023 in Kraft getreten und musste von Bund und Ländern in deutsches Recht überführt werden.
- Die Umsetzung der NIS-2-Richtlinie in das Recht des Bundes ist mit Inkrafttreten des Gesetzes am 6. Dezember 2025 abgeschlossen. Mit Inkrafttreten des Gesetzes besteht für betroffene Unternehmen ein unmittelbarer Handlungsbedarf.
- Das Gesetz unterscheidet zwischen den folgenden Kategorien:
 - wichtige Einrichtungen
 - besonders wichtige Einrichtungen
 - Betreiber kritischer Anlagen, die den besonders wichtigen Einrichtungen zugerechnet werden aber weitergehenden bundesrechtlichen Vorschriften unterliegen.

Welche Anforderungen ergeben sich aus dem Gesetz zur Umsetzung der NIS-2 Richtlinie für mein Unternehmen?

- Prüfen Sie, ob Ihr Unternehmen betroffen ist. (Siehe dazu FAQ „[Was ist NIS-2 und ist mein Unternehmen betroffen?](#)“ oben.)
- Gehen Sie die vorliegende Checkliste durch. Diese gibt einen Überblick über die wesentlichen gesetzlichen Neuerungen.
- Prüfen Sie, welche Maßnahmen Sie bereits ergriffen haben und welche zusätzlich noch erforderlich sind.

Ab wann muss ein betroffenes Unternehmen die Maßnahmen umgesetzt haben?

- Die Verpflichtung zur Umsetzung der geforderten Maßnahmen ([siehe unten](#)) gilt ab dem Inkrafttreten des Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung, also zum 6. Dezember 2025.
- Die Registrierung ([siehe unten](#)) muss innerhalb von drei Monaten nach dem Inkrafttreten des Gesetzes bzw. nachdem ein Unternehmen oder eine Organisation erstmalig in eine der oben aufgeführten Kategorien fällt, erfolgt sein.
- Für weitere Details empfehlen wir, das BSI-Gesetz und die BSI-Kritisverordnung (BSI-KritisV) heranzuziehen. Falls Sie darüber hinaus weitere Fragen haben, hilft Ihnen das LSI weiter.

NIS-2-Checkliste

Im Folgenden werden zentrale Anforderungen der NIS-2-Richtlinie für besonders wichtige und wichtige Einrichtungen sowie Betreiber kritischer Anlagen, die den besonders wichtigen Einrichtungen zuzurechnen sind, aufgeführt.

Registrierungspflicht

- Betroffene Unternehmen und Organisationen sind verpflichtet, sich spätestens nach drei Monaten zu registrieren. Derzeit ist ein zweistufiger Registrierungsprozess vorgesehen: Im ersten Schritt muss eine Registrierung beim digitalen Dienst „Mein Unternehmenskonto“ (MUK) erfolgen. Als zweiter Schritt hat die Registrierung bei einer gemeinsam vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichteten Registrierungsmöglichkeit zu erfolgen. Diese Plattform („BSI-Portal“) wird voraussichtlich ab Anfang Januar 2026 zur Verfügung stehen.

Pflichten der Geschäftsleitung

- Die Geschäftsleitung ist verpflichtet, die [erforderlichen Risikomanagementmaßnahmen](#) umzusetzen und ihre Umsetzung zu überwachen.
- Die Geschäftsleitung muss regelmäßig an Schulungen teilnehmen, um ausreichende Kenntnisse und Fähigkeiten zur Erkennung und Bewertung von Risiken und von Risikomanagementpraktiken im Bereich der Sicherheit in der Informationstechnik zu erlangen.

Risikomanagement

- Betroffene Unternehmen und Organisationen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen, um Störungen der informationstechnischen Systeme, Komponenten und Prozesse zu vermeiden. Die Auswirkungen von Sicherheitsvorfällen sollen möglichst gering gehalten werden.
- Die Verhältnismäßigkeit der Maßnahmen muss durch jedes betroffene Unternehmen bzw. jede betroffene Organisation individuell unter Einhaltung des Stands der Technik bestimmt werden. Die Gesamtverantwortung dafür liegt bei der Geschäftsführung.
- Es muss eine angemessene Dokumentation für den Nachweis der Umsetzung der Maßnahmen erstellt und verfügbar gehalten werden.

Mindestens sind folgende Punkte unter Berücksichtigung des aktuellen Stands der Technik umzusetzen:

- Konzepte zur Risikoanalyse und zur Sicherheit der Informationstechnik
 - Bewältigung von Sicherheitsvorfällen
 - Aufrechterhaltung des Betriebs, Backup-Management ([siehe Glossar](#)), Wiederherstellung nach einem Notfall, Krisenmanagement
 - Sicherheit der Lieferkette
 - Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen
 - angemessener Umgang mit Schwachstellen (unter anderem Patch-Management, [siehe Glossar](#))
 - Systematische Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Informationssicherheit
 - zielgruppenspezifische Schulungen und Sensibilisierungsmaßnahmen zur Informationssicherheit, z.B. für Geschäftsführungen mit dem Schwerpunkt Risikomanagement, IT-Sicherheit für Systemadministratoren und allgemeine Schulungen zur Informationssicherheit für alle Mitarbeiter
 - systematischer Einsatz von kryptographischen Verfahren ([siehe Glossar](#))
 - Konzepte für die Sicherheit des Personals
 - Konzepte für die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen
 - Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung (beide Begriffe [siehe Glossar](#))
 - gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung
- Die EU hat sich vorbehalten, dedizierte Rechtsakte zu Umsetzungsvorgaben zu erlassen.

Hinweis

Die von NIS-2 geforderten Maßnahmen sind grundsätzlich nicht neu, sondern seit langem etablierte „Best Practices“ der Informationssicherheit. Software enthält Schwachstellen, die durch das Einspielen von Patches geschlossen werden. Diese Patches werden von Herstellern bereitgestellt. „Best Practice“ ist es, sich über vom Hersteller bereitgestellte Updates zu informieren und Patches zeitnah einzuspielen. Das von der Richtlinie geforderte Patch-Management sollte also bei den meisten Unternehmen schon aus eigenem Interesse etabliert sein, um keine gravierenden Schwachstellen zu haben.

Die Betreiber kritischer Anlagen sind nach BSIG zu weiterführenden konkreten Maßnahmen verpflichtet, wie z.B. Systeme zur Angriffserkennung einzusetzen. Darüber hinaus müssen im Bereich der kritischen Anlagen höhere Sicherheitsanforderungen umgesetzt werden.

□ Meldepflicht

Betroffene Unternehmen und Organisationen sind verpflichtet

- Innerhalb von 24 Stunden nach Kenntniserlangung von einem erheblichen Sicherheitsvorfall eine Erstmeldung dazu abzugeben. Dabei gelten als Sicherheitsvorfälle auch solche Situationen, die zu einem erheblichen Schaden führen können, dieser jedoch nicht oder noch nicht eingetreten ist.
- Nach 72 Stunden eine ausführliche Meldung mit allen benötigten Informationen abzugeben.
- Nach einem Monat eine Abschlussmeldung einzureichen. Sollte der Vorfall noch andauern, ist eine Fortschrittmeldung und eine Abschlussmeldung nach dem Vorfall abzugeben.

Die Meldungen haben an eine vom Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe eingerichtete gemeinsame Meldestelle zu erfolgen. Bis das Meldeportal verfügbar ist, sind die bisherigen Meldewege zu nutzen. Für Unternehmen und Organisationen, die derzeit noch nicht registriert sind, steht ein [Online-Formular](#) bereit.

□ Nachweispflicht

- Betroffene Unternehmen und Organisationen sind verpflichtet, Nachweise zum Risikomanagement und die umgesetzten Maßnahmen zur Informationssicherheit vorzuhalten ([siehe oben](#)).
- Betreiber kritischer Anlagen haben die Umsetzung der Maßnahmen

zu einem festgelegten Zeitpunkt (frühestens drei Jahre nachdem sie erstmals oder spätestens drei Jahre nachdem sie erneut als ein Betreiber einer kritischen Anlage gelten, und anschließend alle drei Jahre) durch Sicherheitsaudits, Prüfungen oder Zertifizierungen nachzuweisen.

- Des Weiteren können auch wichtige und besonders wichtige Einrichtungen, ähnlich der Betreiber kritischer Anlagen, dazu verpflichtet werden, Sicherheitsaudits, Prüfungen oder Zertifizierung nachzuweisen.

Sanktionen

Haftung

Durch die Umsetzung der NIS-2-Richtlinie wird die Haftung von Geschäftsleitungen bei schuldhaftem Handeln erweitert.

Bußgelder

Abhängig von der Art und Ausprägung des Verstoßes und abhängig von der Kategorie können Bußgelder in unterschiedlicher Höhe anfallen:

- Bei besonders wichtigen Einrichtungen einschließlich der Betreiber kritischer Anlagen bis zu
 - 10 Millionen € oder
 - 2 % des Jahresumsatzes für Unternehmen, die mehr als 500 Millionen € Jahresumsatz erzielen.
- Bei wichtigen Einrichtungen bis zu
 - 7 Millionen € oder
 - 1,4 % des Jahresumsatzes, falls mehr als 500 Millionen € Jahresumsatz erzielt werden.

Weitere Empfehlungen und Hilfestellungen

Auch Unternehmen, die nicht von der NIS-2-Richtlinie betroffen sind, empfiehlt das LSI dringend, sich mit IT-Sicherheit auseinanderzusetzen. Einen guten Einstieg bietet hierbei die Handlungsempfehlung „Informationssicherheit für kleine und mittelständische Unternehmen“ des LSI. Das zugehörige Vorgehensmodell empfiehlt eine zeitliche Reihenfolge bei der Umsetzung der „Best Practices“ der Handlungsempfehlung. Für einige Branchen (Krankenhäuser, Trinkwasserversorgung, Abwasserentsorgung, Siedlungsabfallentsorgung) bietet das LSI branchenspezifische Beratungsdokumente an.

Ein nächster Schritt kann die Einführung eines Informationssicherheitsmanagementsystems (ISMS) auf der Basis einer etablierten Norm, wie zum Beispiel der ISO/IEC 27001, sein.

Dieses Dokument in seiner aktuellen Fassung und weitere Dokumente zur Hilfestellung finden Sie im Downloadbereich des Landesamts für Sicherheit in der Informationstechnik:

<https://www.lsi.bayern.de/aktuelles/downloads/>

Bei weiteren Fragen stehen wir Ihnen gerne zur Verfügung.

Anschrift

Landesamt für Sicherheit in der Informationstechnik
Beratung öffentlicher KRITIS-Betreiber

Keßlerstraße 1
90489 Nürnberg

Telefon

0911 / 21549 - 525

E-Mail

beratung-kritis@lsi.bayern.de

Web

www.lsi.bayern.de

Weiterführende Hinweise (Links)

- Bundesgesetzblatt: Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung
- BSI: EU-Richtlinien zur Netzwerk- und Informationssicherheit
- BSI: NIS-2-Betroffenheitsprüfung
- BSI: Online-Formular für meldepflichtige Ereignisse
- Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV)
- LSI: Handlungsempfehlung für KMU
- LSI: Vorgehensmodell für KMU
- LSI: Infoblatt - Umgang mit Risiken
- LSI: Tabelle zur Behandlung von Risiken

Glossar

Backup-Management

Bei einer Datensicherung werden Sicherungskopien von Daten erstellt, um einem Datenverlust vorzubeugen. Backup-Management ist der Prozess der Erstellung, Verwaltung, Prüfung und Wiederherstellung von Sicherungskopien.

Kontinuierliche Authentifizierung

Die kontinuierliche Authentifizierung bezieht sich darauf, dass beispielsweise Nutzer von ihrem IT-System kontinuierlich, gegebenenfalls unter Einsatz von künstlicher Intelligenz, in Bezug auf ihre Identität geprüft werden. Diese Technologie ist derzeit eher im Hochsicherheitsbereich anzutreffen.

Kryptografie

Kryptografische Verfahren und Systeme dienen dem Ziel, die Vertraulichkeit und Integrität von gespeicherten und übertragenen Informationen sicherzustellen. Vertraulichkeit bedeutet, dass Informationen nur durch befugte Parteien gelesen werden können, Integrität bedeutet, dass Informationen vor Manipulation geschützt werden. Hierzu kommen unter anderem Verschlüsselungsverfahren zum Einsatz.

Multi-Faktor-Authentifizierung

Bei der Multi-Faktor-Authentifizierung (MFA) gibt es drei Gruppen von Faktoren, deren Verfahren für eine Authentifizierung verwendet werden können. Hierzu zählen die Faktoren: Wissen, Besitz und Biometrie. Bei einer MFA muss der Benutzer mindestens zwei Authentifizierungsmerkmale vorweisen können, die verschiedenen Faktoren angehören.

Patch-Management

Ein Patch ist ein Software-Update und dient dem Schließen von Sicherheitslücken oder der allgemeinen Verbesserung einer Software. Patch-Management umfasst Prozesse und Verfahren welche unterstützen, neue Patches zeitnah zu erhalten, verwalten und einzuspielen.