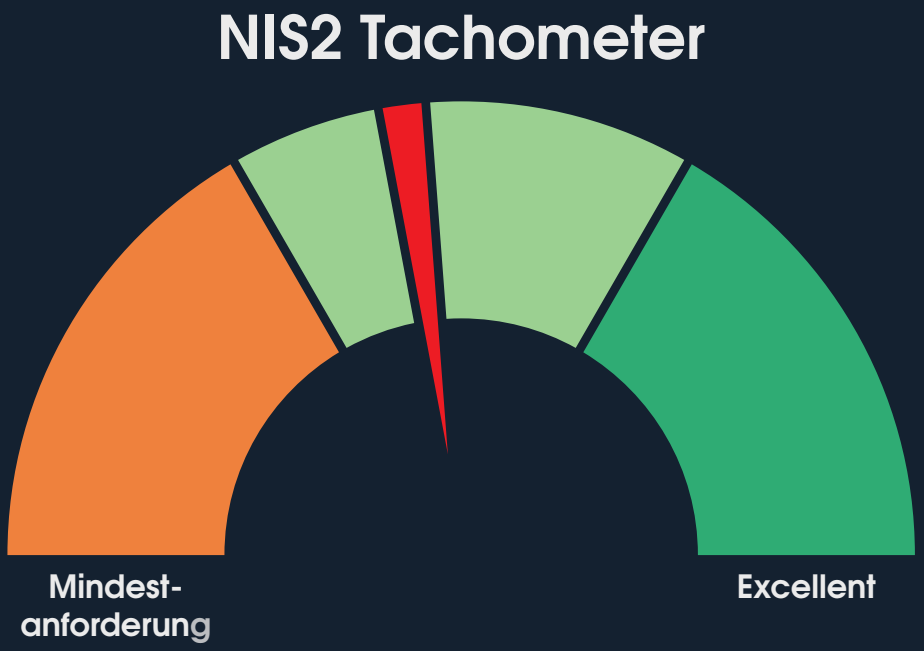
SpediHub

Damit der Maschinenbau auf Kurs bleibt.
Mit IT Sicherheit.



IT-Sicherheit im Anlagen- und Maschinenbau NIS2-Compliance bis 17.10.2024 umsetzen

Wir unterstützen Sie mit dem SpediHub NIS2-Check

MEHR INFOS
www.spedihub.de/nis2-check

NIS2 Richtlinie auf einen Blick

Die EU-Richtlinie zur Netz- und Informationssicherheit (NIS-Richtlinie) soll für 18 Wirtschaftssektoren ein hohes gemeinsames Niveau der Cyber-Sicherheit in der EU gewährleisten.

Der Maschinen und Anlagenbau wurde als wichtiger Wirtschaftssektor identifiziert. Wichtige Einrichtungen sind Unternehmen mit

> 50 Beschäftige **oder**
> 10 Mio. Jahresumsatz **und**
> 10 Mio. Jahresbilanzsumme

Die Bußgelder für Nichteinhaltung wurden im Vergleich zur Vorgänger-Directive drastisch verschärft.

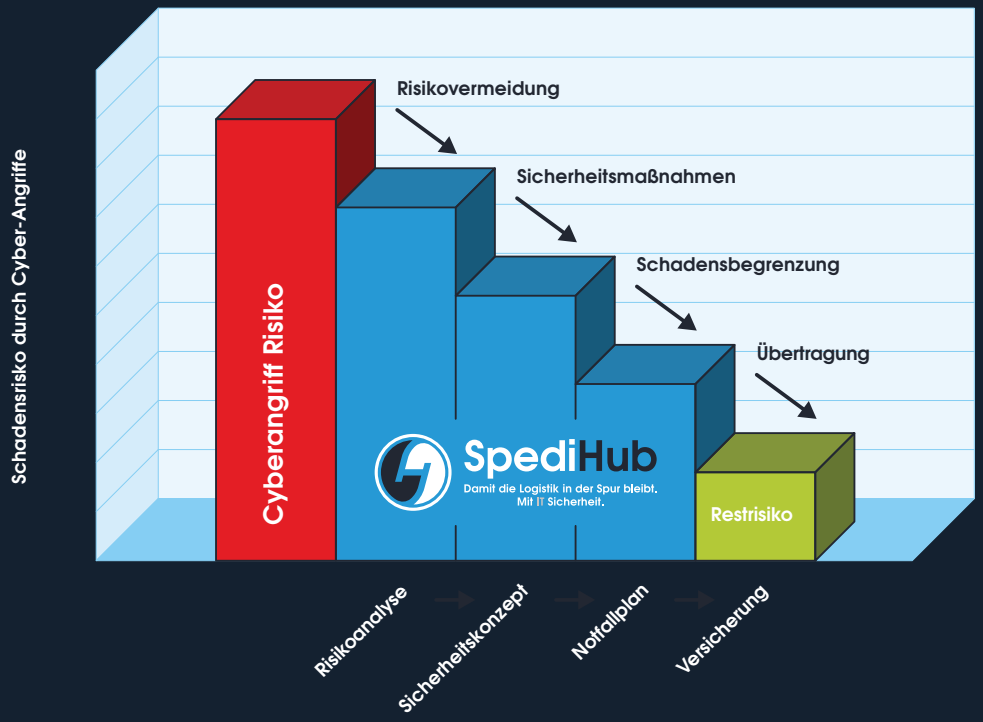
Wichtige Sektoren:

- Verarbeitendes Gewerbe
  Maschinenbau
  NACE Code 26 - 30
- Chemikalien
- Lebensmittel
- Digitale Dienste
- Medizinprodukte
- Forschungseinrichtungen

Ab dem 18.10.2024 gilt das IT-Sicherheitsgesetz 3.0. Bis zu diesem Termin müssen alle betroffenen Anlagen- und Maschinenbauunternehmen die NIS2-Richtlinie umgesetzt haben.

Am 17.10.2024 endet die Umsetzungsfrist für die neue NIS2-Richtlinie

Ziel der NIS2: Wichtige Unternehmen besser vor Cyberangriffen schützen



Jedes Unternehmen ist dem allgemeinen Risiko von Cyber-Angriffen ausgesetzt. Gerade die Industrie ist ein attraktives Ziel, da sie mit enormen Mengen an Datensätzen umgehen und stark mit den Geschäftspartnern vernetzt sind.

Anhand einer Risikoanalyse ist es möglich, ein durchdachtes IT-Sicherheitskonzept zu entwickeln und eine erste Absenkung des Risikoniveaus zu erreichen. Die eigentliche Risikominderung erfolgt jedoch erst durch die Umsetzung und das Zusammenwirken von technischen und organisatorischen Maßnahmen, die sich aus den Zielen des IT-Sicherheitskonzeptes ableiten.

Wenn diese drei Bausteine der IT-Sicherheit abgearbeitet sind – Risikoanalyse, IT-Sicherheitskonzept und Notfallplan – kann das Restrisiko auf eine Cyber-Versicherung übertragen werden.

Wichtigste Maßnahme gegen Cyberkriminalität ist die Investition in ein durchdachtes IT-Sicherheitskonzept inklusive Backup-Strategie und Notfallplan.

Umsetzung der NIS2-Richtlinie bis 17.10.2024

Anforderungen und Meldepflichten für den Anlagen- und Maschinenbau

Bis zum 17.10.2024 ist ein **IT-Sicherheitsbeauftragter** zu benennen und sicherzustellen, dass alle notwendigen Maßnahmen zur Umsetzung der NIS2-Richtlinie ergriffen wurden.

Alle betroffenen Unternehmen müssen gemäß der NIS2-Richtlinie **technische, betriebliche** und **organisatorische Maßnahmen** ergreifen, die zu einer Minimierung von IT-Sicherheitsvorfällen führen und Cyber-Angriffen vorbeugen.

Es ist sicherzustellen, dass die Cyber-Sicherheit durch ein **Risikomanagement** überwacht und eingehalten wird.

Unternehmen müssen bei **Geschäftspartnern**, die für einen reibungslosen Geschäftsablauf unerlässlich sind, Audits durchführen, um auszuschließen, dass keine IT-Sicherheitsschwachstellen vorliegen.

Meldepflichten

- 24h Frühwarnung
  Verdacht auf einen IT-Sicherheitsvorfall
- 72h Bewertung des IT-Sicherheitsvorfalles
  Schweregrad und Auswirkungen
- Zwischenbericht - falls von den Behörden angefordert
- Abschlussbericht nach einem Monat
  Detaillierte Beschreibung Bedrohung, Ursache, Abhilfemaßnahmen

Sicher in die digitale Zukunft: Erfüllen Sie die NIS2-Richtlinie bis 17.10.2024

Erforderliche Maßnahmen nach NIS-2:

Alle betroffenen Unternehmen müssen laut der NIS2-Richtlinie:

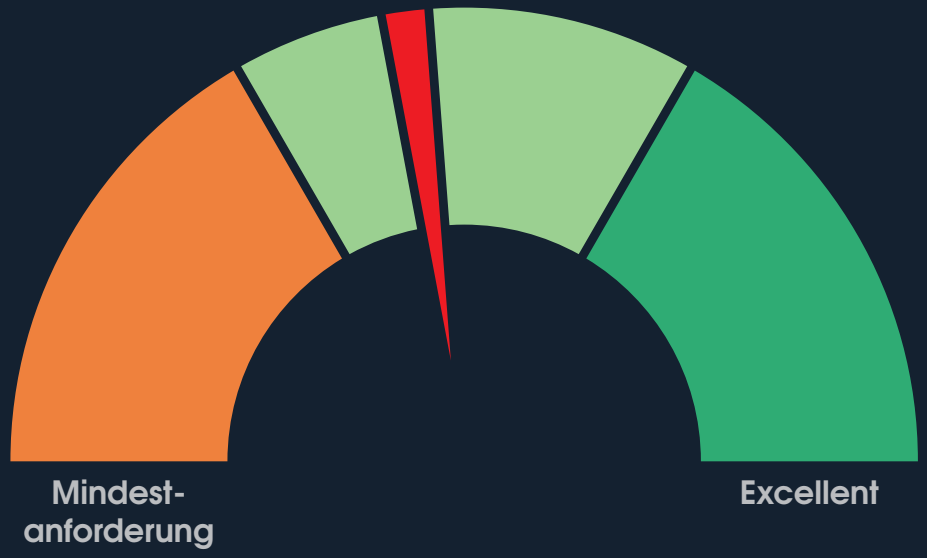
- Cyber-Sicherheitsstrategie (IT-Sicherheitskonzept) implementieren
- Cybersecurity-Risikomanagement aufbauen
- IT-Sicherheitsrisiken bewerten (Cyber Security Risk Assessment)
- IT-Sicherheitsbeauftragten ernennen
- Berichtspflichten erfüllen
- Aufrechterhaltung des Betriebs sichern durch
  - Backup-Management (inkl. Wiederherstellung)
  - Notfall- und Krisenmanagement
- Sicherheitsmaßnahmen bei Beschaffung, Entwicklung und IT-Systemen festlegen (inkl. Schwachstellen-Management)
- Risikomanagementmaßnahmen für Cyber-Sicherheit evaluieren
- Konzepte für Kryptografie und Verschlüsselung entwickeln
- Konzepte zur Zugriffskontrolle entwickeln
- Multi-Faktor-Authentifizierung anwenden
- Sicherheit der Lieferkette gewährleisten (Überwachung kritischer Geschäftspartner durch Audits)
- Professionellen Umgang mit IT-Sicherheitsvorfällen gewährleisten
- Meldepflichten nachkommen

Gewährleisten Sie Ihre Cyber-Sicherheit durch eine ganzheitliche IT-Sicherheits-Strategie: von der Cyber-Sicherheitsstrategie und Risikomanagement bis zur Überwachung kritischer Geschäftspartner

Ihr Weg zu Umsetzung der NIS2-Richtlinie

Unser IT-Security Check deckt Ihre Schwachstellen auf.
Übrigens lassen sich diese meist mit überschaubarem Aufwand überwinden.
Wir zeigen Ihnen, wie.

NIS2 Tachometer



Folgende Quick-Win Maßnahmen können sich aus einer IT-Sicherheitsbewertung ergeben:

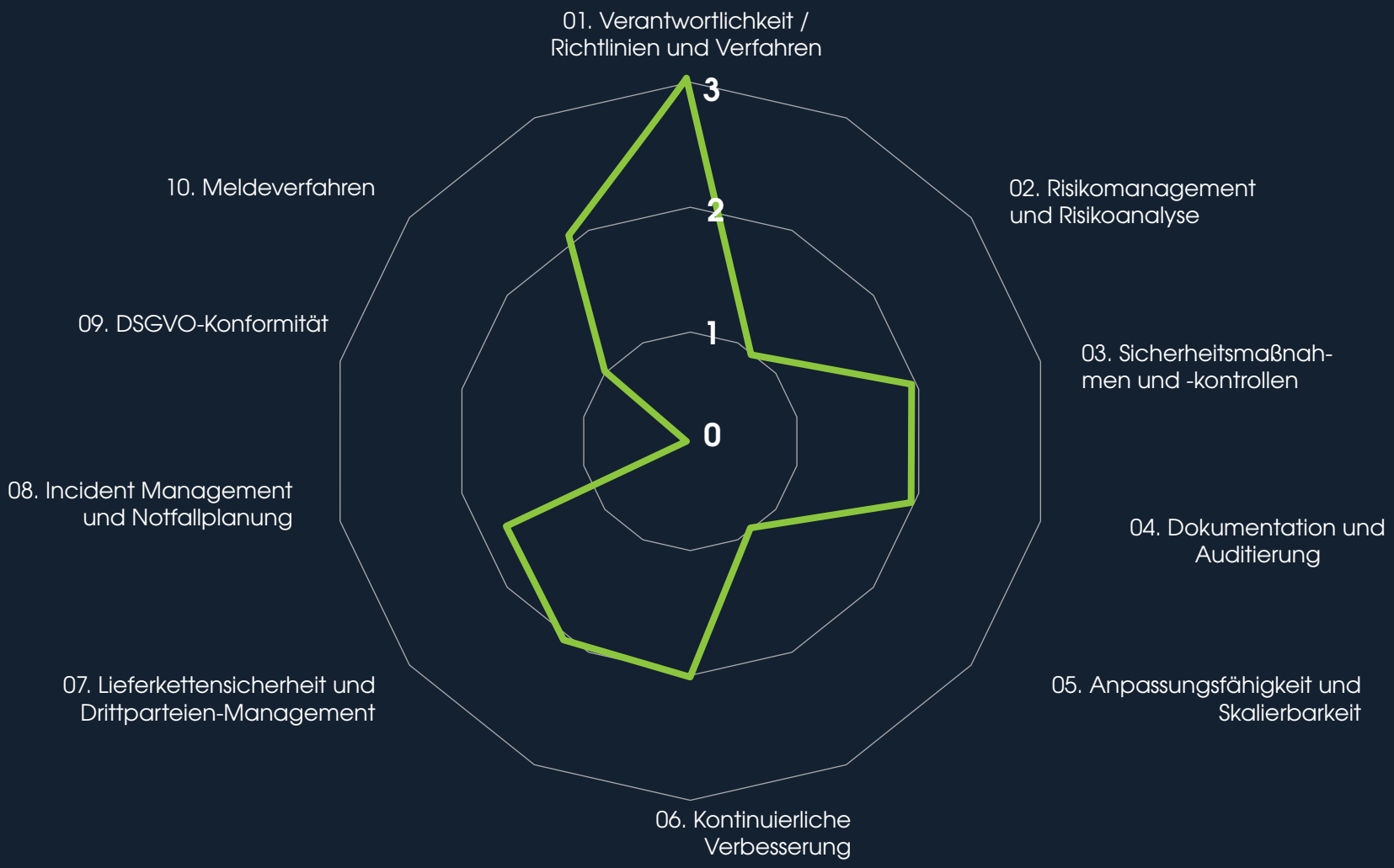
- ✓ Nachweis eines Security-Audits
- ✓ Richtlinien und Sicherheitskonzepte
- ✓ Backupstrategie
- ✓ Cyber-Risk-Analyse durch Netzwerkscan
- ✓ Regelmäßige Software- und Sicherheitsupdates
- ✓ Sicherheitsvorkehrungen im Home-Office
- ✓ Passwortmanagement
- ✓ Einführung Multi-Faktor-Authentifizierung (MFA)
- ✓ Schutzvorkehrungen im E-Mail-Verkehr
- ✓ Regelungen zu BYOD (Bring your own device)

1. NIS2-Security-Check durchführen –> 2. Gemeinsam Ihr IT-Sicherheitsniveau erhöhen

www.spedihub.de/nis2-check

NIS2 IT-Sicherheitsniveau

Reifegrad 0-3



Welche IT-Security-Maßnahmen müssen umgesetzt werden, um Kernprozesse und -daten zu schützen? Den Überblick darüber erhalten Sie mit dem SpediHub NIS2-Check.

NIS2 ready in 2 Schritten

1. NIS2 IST-Analyse
   Gemeinsam mit Ihnen und ggf. mit Ihrem IT-Dienstleister analysieren wir das aktuelle IT-Sicherheitsniveau, führen einen NIS2-Check durch und erarbeiten Handlungsempfehlungen.

2. NIS2 Umsetzungsunterstützung
   - Erarbeitung einer Cyber-Sicherheitsstrategie (IT-Sicherheitskonzept)
   - Unterstützung bei der Umsetzung der Handlungsempfehlungen
   - Aufbau eines Cybersecurity-Risikomanagements
   - Verbesserung des IT-Sicherheitsniveaus
   - Erfüllung der Anforderungen der NIS2-Richtlinie

Legen Sie die Umsetzung der NIS2-Richtline in die Hände eines IT-Security-Spezialisten und profitieren Sie von einer 70% Förderung für die Umsetzung!

ONLINE-TERMINVEREINBARUNG: WWW.SPEDIHUB.DE/MEETING
TEL: 05 665 / 96 80 69 0 | E-MAIL: tim.iglauer@spedihub.de | WEB: www.spedihub.de

MEHR INFOS
www.spedihub.de/nis2-check

NIS2-Audit - und dann?
Viele Wege führen nach Rom

Um die Einhaltung der grundlegenden IT-Sicherheitsstandards zu gewährleisten, wird die Einführung eines Informationssicherheits-Managementsystems (ISMS) empfohlen. Es bietet sich an, dieses stufenweise einzuführen, um das laufende Tagesgeschäft nicht zu beeinflussen.

In einem ersten Schritt wird das aktuelle Sicherheitsniveau mit dem SpediHub IT-Security Check analysiert.

Darauf aufbauend kann die Analyse des Sicherheitsniveaus mit ISA+ detailliert werden. Der Vorgang ist unkompliziert und zielt darauf ab, potenzielle Handlungsfelder zu benennen.

Die nächste Etappe ist die Zertifizierung als vollwertiges ISMS. Für KMU wird CISIS12 empfohlen. Obwohl sich CISIS12 durch einen schlanken Aufbau auszeichnet, handelt es sich um ein vollwertiges System zur Datensicherheit im Unternehmen. Sollte ein Kunde dennoch eine internationale Zertifizierung nach ISO 27001 oder TISAX fordern, lässt sich das CISIS12 Rahmenwerk entsprechend erweitern.

Die Kombination aus SpediHub IT-Security Check und ISA+ ist die optimale Voraussetzung, um ein vollwertiges ISMS nach Anforderungen Ihrer Kunden aufzubauen.

Warum Sie SpediHub als Partner wählen sollten

- ✓ Wir bieten über 20 Jahre Expertise im Bereich Datenschutz und Informationssicherheit.
- ✓ Wir sind hochqualifizierte IT-Security-Spezialisten und arbeiten entsprechend zielorientiert.
- ✓ Der Schutz Ihrer Daten hat für uns absolute Priorität.
- ✓ Sie bekommen von uns eine professionelle Analyse Ihres IT-Sicherheitsniveaus.
- ✓ Wir erarbeiten ein konkretes Konzept für den Schutz Ihrer IT-Systeme und Unternehmensdaten.
- ✓ Bei Bedarf unterstützen wir Sie bei der Umsetzung der Handlungsempfehlungen.
- ✓ Durch unsere Expertise entlasten Sie Ihre Mitarbeiter und schonen auch Ihre eigenen Nerven. Sie sparen Zeit und damit Kosten.

Erhalten Sie Zugriff auf unser zertifiziertes Expertenwissen und Know-how.

Sie wissen noch nicht, wie Sie Ihre IT-Sicherheit angehen sollen?
Gerne können wir uns unverbindlich darüber austauschen!

Tim Iglauer
Geschäftsführer SpediHub GmbH

ONLINE-TERMINVEREINBARUNG: WWW.SPEDIHUB.DE/MEETING
TEL: 05 665 / 96 80 69 0 | E-MAIL: tim.iglauer@spedihub.de | WEB: www.spedihub.de

MEHR INFOS
www.spedihub.de/nis2-check

SpediHub

Damit der Maschinenbau auf Kurs bleibt.
Mit IT Sicherheit.

SpediHub GmbH
Geschäftsführer: Tim Iglauer
Unter den Pappeln 7, 34327 Körle
E-Mail: tim.iglauer@spedihub.de
Tel.: 05665 / 96 80 69 0