CYBERsicher | FitNIS2-Navigator Prüfen. Verstehen. Handeln.

IT-Sicherheit IN DER WIRTSCHAFT

Fit für NIS2

EU Netz- und Informationssicherheitsrichtlinie verstehen

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

UNIVERSITÄT PADERBORN | SICP

CYBER|INTELLIGENCE .Institute

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

Warum NIS-2?

Ziel: Harmonisierung hinsichtlich eines EU-weiten Mindeststandards an IT-Sicherheit für den Schutz von Wirtschaft und Gesellschaft

„Gefangenen-Dilemma“

„Negative Externalitäten“

DIHK
Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

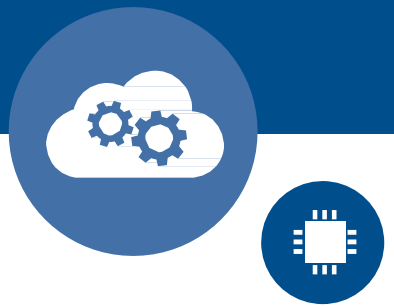
NIS-2-Richtlinie auf einen Blick

- NIS = Network Information Security
- Nachfolgerin NIS-1-Richtlinie, in Kraft seit 16.01.23
- Richtlinien müssen national umgesetzt werden
- Umsetzung durch Änderung des BSI-Gesetzes im NIS2UmsuCG
- Ursprüngliche Umsetzungsfrist: 17. Oktober 2024

- **NEU:** Ausweitung des Anwendungsbereichs (size cap-rule)
- **NEU:** detailliertere Pflichten: Registrierung, Risikomanagementmaßnahmen und Meldungen
- **NEU:** neue Maßnahmen der Aufsicht, Haftung und Sanktionen

DIHK Deutsche Industrie- und Handelskammer
DsiN Deutschland sicher im Netz

Zentrale NIS-2 Inhalte



Feststellung Betroffenheit und Registrierung

Risikomanagement und Sicherheitsmaßnahmen

Meldung von Sicherheitsvorfällen

Awareness und Verantwortung Geschäftsleitungen

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

Betroffenheit: Ablauf

1 Selbst-identifizierung

- Unternehmen müssen Ihre Betroffenheit **selber feststellen**

2 Betroffenheits-prüfung

1. Qualitatives Kriterium
(Nach Branchen und Sektoren)

- NIS2 Anhang I
  (hohe Kritikalität)
- NIS2 Anhang II
  (sonstige kritische Sektoren)

2. Quantitatives Kriterium
(knüpft an Unternehmensgröße an)

3 Registrierung

- **Nach Inkrafttreten** des NIS2UmsuCG
- BSI plant digitalisierte **Online-Portallösung zur Registrierung**
- **Frist < 3 Monate**

*BSI: NIS2-Betroffenheitsprüfung

Grundsätzlich:

Auch wenn Unternehmen nicht den Verpflichtungen unterliegen, bieten die aufgeführten Maßnahmen zum Risikomanagement eine gute Orientierung für mehr Cybersecurity

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

Quantitatives Kriterium: Schwellenwerte

Mitarbeitende		Jahresumsatz		Jahresbilanzsumme	
≥ 50	oder	**> 10 Mio.€**	und	**> 10 Mio.€**	→ **wichtige** Einrichtung (ca. 25000 Unternehmen)
≥ 250	oder	**> 50 Mio.€**	und	**> 43 Mio.€**	→ **besonders wichtige** Einrichtungen (ca. 5000–10000 Unternehmen)

oder unabhängig von Unternehmensgröße

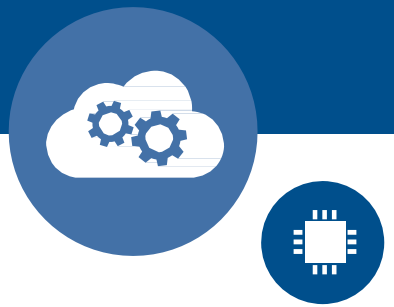
z.B. wenn

- bestimmte Dienste erbracht werden (z. B. DNS-Registrierungsdienste) oder
- bestimmte Auswirkungen im Falle einer Störung drohen

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

Zentrale NIS-2 Inhalte



Feststellung Betroffenheit und Registrierung

Risikomanagement und Sicherheitsmaßnahmen

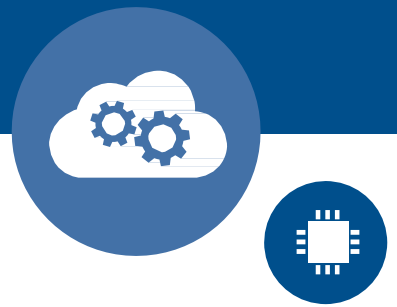
Meldung von Sicherheitsvorfällen

Awareness und Verantwortung Geschäftsleitungen

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

Risikomanagement-Maßnahmen



Maßnahmen:

- geeignete, verhältnismäßige und wirksame **technische und organisatorische Maßnahmen**
- um **Störungen** der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme zu **vermeiden**
- und **Auswirkungen von Sicherheitsvorfällen möglichst gering** zu halten

Stand der Technik, Normen

Berücksichtigung der Verhaltnismäßigkeit

Dokumentation!!!

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

Risikomanagement: ISMS

Anforderung	Umsetzung
Konzepte in Bezug auf Risikoanalyse	potenzielle **Bedrohungen identifizieren**, bewerten und **Maßnahmen** zur Minimierung der Risiken **implementieren** (technische Systeme und organisatorische Prozesse)
Bewertung der Wirksamkeit von Cybersicherheit und Risiko-Management	kontinuierliche **Bewertung der Wirksamkeit** der implementierten Sicherheitsmaßnahmen, um Schwachstellen zu identifizieren und Strategien kontinuierlich zu verbessern
Personalsicherheit, Zugriffskontrolle und Anlagen-Management	**Sicherheit des Personals** prüfen, effektive **Zugriffskontrollen** verhindern unbefugten Zugriff auf sensible Informationen, das Management von Anlagen umfasst die Identifizierung, Bewertung und Überwachung aller **IT-Ressourcen**, einschließlich Hardware, Software und IoT-Geräten, um diese vor verschiedenen Sicherheitsbedrohungen zu schützen
Sicherheit der Lieferkette	beispielsweise **vertragliche Vereinbarungen** mit Zulieferern und Dienstleistern zu Risikomanagementmaßnahmen, Bewältigung von Cybersicherheitsvorfällen, Patchmanagement, Berücksichtigung von Empfehlungen des BSI in Bezug auf deren Produkten und Dienstleistungen, Durchführung von External Attack Surface (EAS) Scans

Risikomanagement: Business Continuity & Krisenmanagement

Anforderung	Umsetzung
Bewältigung von Sicherheitsvorfällen	**klar definierter Prozess** für schnelle Erkennung, Reaktion und Aufklärung von Vorfällen sowie die Implementierung von Maßnahmen zur Vermeidung zukünftiger Vorfälle
Aufrechterhaltung des Betriebs	effektives **Backup-Management** und **Krisenmanagementstrategien** stellen sicher, dass Daten und Systeme nach einem Notfall schnell wiederhergestellt werden können

Risikomanagement: Life Cycle Management

Anforderung	Umsetzung
Sicherheit in der Entwicklung, Beschaffung und Wartung	sichere **Entwicklungspraktiken**, sorgfältige **Beschaffung** und regelmäßige Wartung der Systeme (**Sicherheits-Updates**), um Sicherheitslücken zu schließen, Management und Offenlegung von **Schwachstellen**

Risikomanagement: weitere Anforderungen

Anforderung	Umsetzung
Schulungen	**Bewusstsein der Mitarbeitenden** für Cyberbedrohungen, Social Engineering, Phishing etc. schärfen
Kryptographie und Verschlüsselung	systematischer Einsatz zum **Schutz vertraulicher Daten** bei Übertragung und Speicherung
sichere Authentifizierung und gesicherte Kommunikation	Verwendung von Lösungen zur **Multi-Faktor-Authentifizierung**, **sichere Sprach-, Video- und Textkommunikation** und sichere **Notfallkommunikationssysteme**

Bewertung der Verhältnismäßigkeit von Risikomanagementmaßnahmen

Fragen der Geschäftsleitung zum Aufbau eines Risikomanagements nach NIS-2

Risikoausmaß

Welche spezifischen Cyber-Risiken drohen unserem Unternehmen? Welche Geschäftsprozesse sind besonders gefährdet?

Unternehmensgröße

Sind aktuelle Sicherheitsmaßnahmen im Verhältnis zur Unternehmensgröße und Komplexität angemessen?

Umsetzungskosten

Welche finanziellen und personellen Ressourcen sind erforderlich, um die geplanten Maßnahmen umzusetzen?

Eintrittswahrscheinlichkeit

Wie wahrscheinlich sind Cyber-Bedrohungen für unser Unternehmen, basierend auf aktuellen Bedrohungs-analysen und historischen Daten?

Schwere von Sicherheitsvorfällen

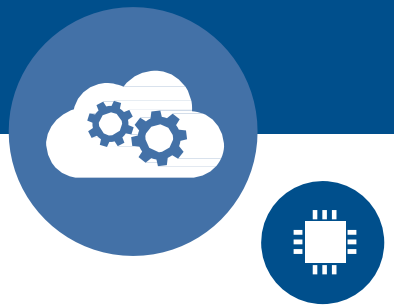
Welcher Schaden (z. B. finanziell, rufschädigend) könnte beim Sicherheitsvorfall entstehen?

Gesellschaftliche & wirtschaftliche Auswirkungen

Welche Auswirkungen hätte ein schwerwiegender Cyber-Vorfall auf Kund:innen, Partner:innen und die Gesellschaft?

DIHK Deutsche Industrie- und Handelskammer
DsiN Deutschland sicher im Netz

Zentrale NIS-2 Inhalte



Feststellung Betroffenheit und Registrierung

Risikomanagement und Sicherheitsmaßnahmen

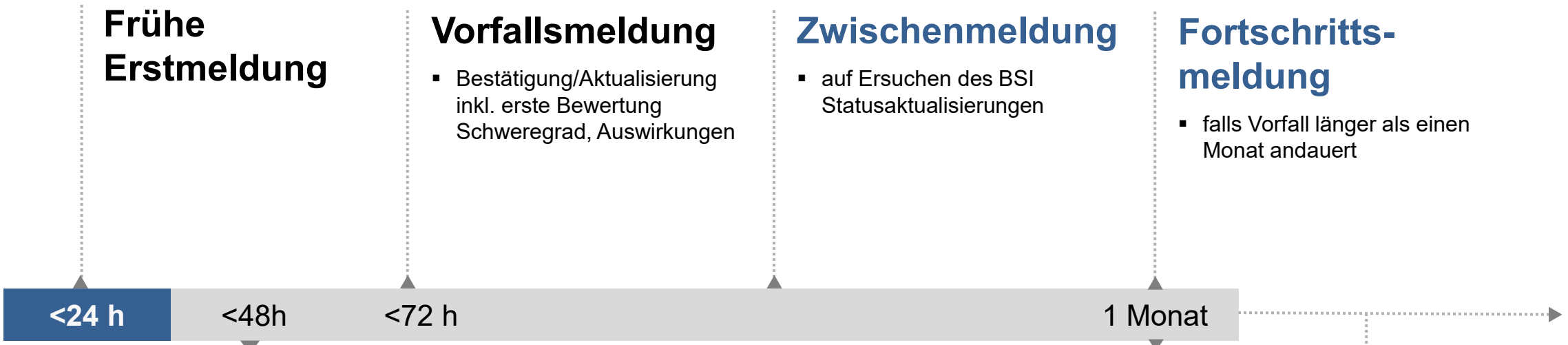
Meldung von Sicherheitsvorfällen

Awareness und Verantwortung Geschäftsleitungen

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

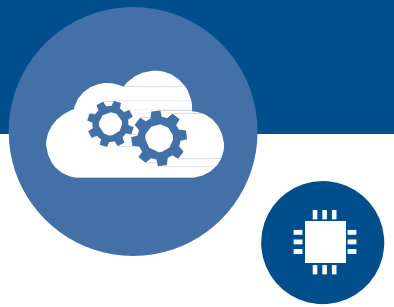
Meldepflichten: Erheblicher Sicherheitsvorfall



DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

Zentrale NIS-2 Inhalte



Feststellung Betroffenheit und Registrierung

Risikomanagement und Sicherheitsmaßnahmen

Meldung von Sicherheitsvorfällen

Awareness und Verantwortung Geschäftsleitungen

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

Billigungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen

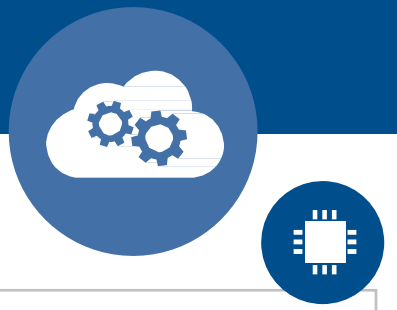
Monitoring

- Geschäftsleitungen sind verpflichtet, die **Risikomanagementmaßnahmen** im Bereich Cybersicherheit **zu billigen** und ihre Umsetzung **zu überwachen**

Schulungen

- Geschäftsleitungen müssen **regelmäßig** an **Schulungen** teilnehmen, um ausreichende Kenntnisse und Fähigkeiten
  - ✓ zur **Erkennung und Bewertung von Risiken** sowie **Risikomanagement-praktiken** im Bereich der Sicherheit in der **Informationstechnik** und
  - ✓ zu **Auswirkungen** von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten **Dienste** zu erwerben

Wie vorbereiten?



Verantwortliche benennen
(Koordination, Vernetzung)

Verantwortung übernehmen
(persönliche Verantwortung Geschäftsführende)

Bestandsaufnahme und Gap-Analyse

Cybersicherheit verbessern
(Maßnahmen umsetzen)

Auf Pflichten vorbereiten
(Registrierung, Meldungen, Empfang von Warnungen, Ansprechpersonen)

Fortlaufende Evaluierung und Anpassung

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

FitNIS2 Projekt

CYBERsicher FitNIS2-Navigator Prüfen. Verstehen. Handeln.

IT-Sicherheit IN DER WIRTSCHAFT

Akteur:innen

- **Projektpartner**: Deutschland sicher im Netz e.V. & SICP Uni Paderborn
- **Förderung:** Bundesministerium für Wirtschaft & Energie
- **Projektträger**: Deutsches Zentrum für Luft- und Raumfahrt (DLR)
- **Begleitforschung:** wissenschaftliches Institut für Infrastruktur & Kommunikationsdienste (WIK)

Projektrahmen

- **Zeitraum**: 01.09.2024 bis 31.08.2026
- **Angebote**: Wissensformate, Workshops, Road-Shows & Informationsmaterialien
- **Produkt**: Online Tool, dass Unternehmen unterstützt, den neuen Anforderungen der NIS2 Richtlinie gerecht zu werden

DsiN Deutschland sicher im Netz

UNIVERSITÄT PADERBORN | SICP

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Hilfestellung FitNIS2 Navigator

CYBERsicher FitNIS2-Navigator Prüfen. Verstehen. Handeln.

FitNIS2 NAVIGATOR

IT-Sicherheit IN DER WIRTSCHAFT

Der FitNIS2 Navigator ist ein **kostenfreies** Online Tool zur NIS2 Compliance!

Unterstützt in 3 Schritten:

1. Prüfen
   Bin ich betroffen?

2. Einordnen
   Was ist meine Ausgangslage?

3. Handeln
   Was muss ich tun?

Besondere KMU-Eignung:

- Leitet mit zusätzlichen Erklärungen durch den Betroffenheitstest
- Enthält spezifische Informationen angepasst auf Branche und Unternehmensgröße
- Verlinkt zu bedarfsorientiert auf kostenfreie Angebote

Mehr Infos auf www.FitNIS2.de

DsiN Deutschland sicher im Netz

UNIVERSITÄT PADERBORN | SICP

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

CYBERsicher | FitNIS2-Navigator Prüfen. Verstehen. Handeln.

IT-Sicherheit IN DER WIRTSCHAFT

VIELEN DANK!

Deutschland sicher im Netz e.V.
Tel. +49 (0) 30 767581-571
info@sicher-im-netz.de
www.dsin.de

Prof. Dr. Simon Trang
Universität Paderborn

Mit freundlicher Unterstützung durch:

CySec – Institut für Cybersicherheit und Compliance
kristin.masuch@cysec-institut.de

cyberintelligence.institute
dennis.kipker@cyberintelligence.institute

DIHK Deutsche Industrie- und Handelskammer

DsiN Deutschland sicher im Netz

Universität Paderborn SICP

CySec - Institut für Cybersicherheit & Compliance

CYBER|INTELLIGENCE .Institute

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital