

04.09.2025

13:40 – 14:10

NIS-2 Impulsvortrag

Gefördert durch:



Mittelstand-
Digital 

CYBERSicher

KMU.kompetent.sicher.
NIS2 Test- und
Trainingsplattform

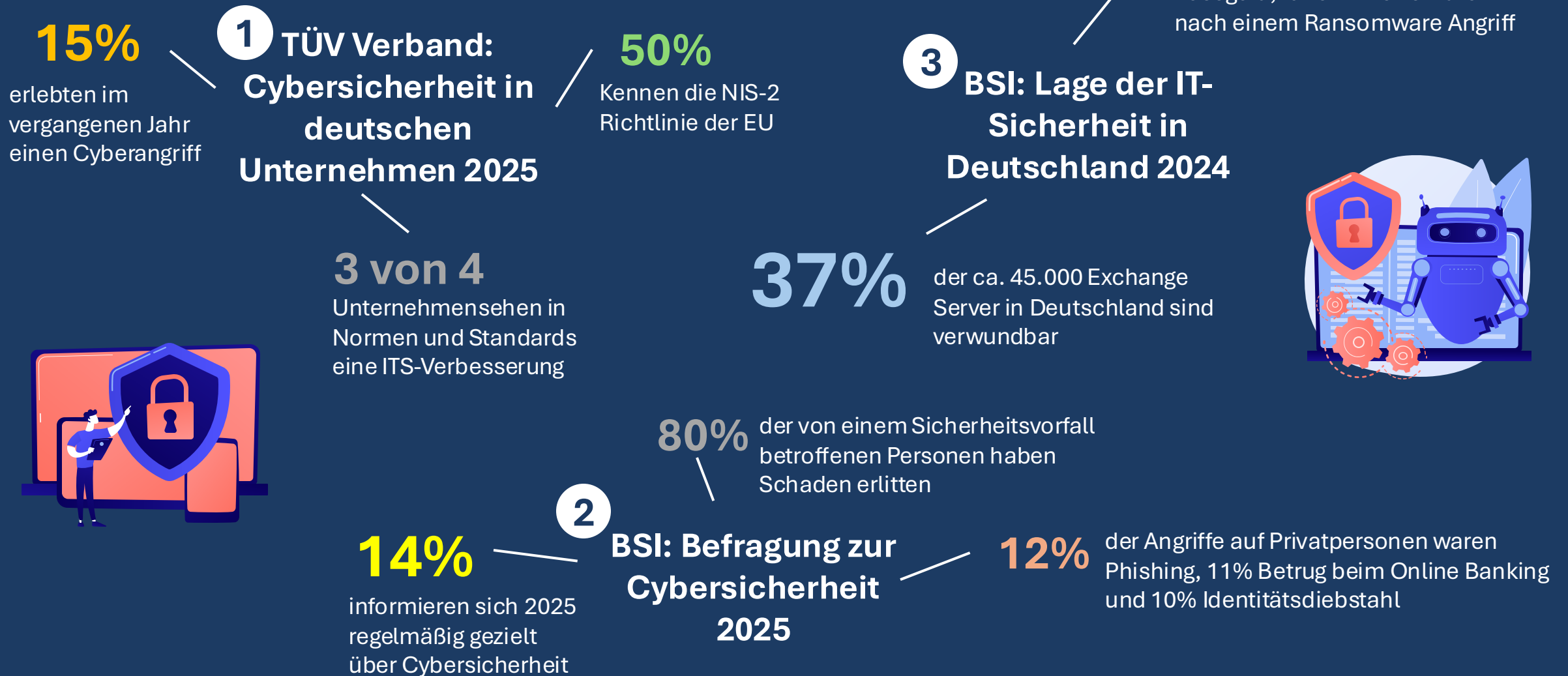
 **IT-Sicherheit**
IN DER WIRTSCHAFT

aufgrund eines Beschlusses
des Deutschen Bundestages

Motivation

Warum ist IT-Sicherheit heute so wichtig?

Die Lage der IT-Sicherheit in Deutschland



Der Weg zur NIS-2 Richtlinie

EU Cyber-Security Act

NIS-2 Richtlinie EU2022/2555

CER/CRE-Richtlinie

Cyber Resilience Act (CRA)

12.2022 NIS-2 (EU)

06.2025 Referentenentwurf

07.2025 Regierungsentwurf

Anfang.2026 Gesetzesbeschluss



Gesetzentwurf der Bundesregierung

Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung

Bearbeitungsstand: 25.07.2025 12:08

Entscheidungsbaum

Fällt mein Unternehmen unter die NIS-2 Richtlinie?

Wer fällt unter NIS-2?

<https://betroffenheitspruefung-nis-2.bsi.de/>



Kategorie	Unternehmensgröße	Sektoren mit hoher Kritikalität
Besonders wichtige Einrichtung (§ 28,1)	Großunternehmen: Unternehmen ab 250 Mitarbeiter oder ≥ 50 Mio. Umsatz + ≥ 43 Mio. Jahresbilanz	Energie, Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheit, Trinkwasser, Abwasser, ITK-Dienste, Weltraum
	Mittlere Unternehmen: Unternehmen ab 50 Mitarbeiter oder ≥ 10 Mio. Umsatz + ≥ 10 Mio. Jahresbilanz	Anbieter öffentlicher TK-Netze und TK-Dienste
	unerheblich	Qualifizierte Vertrauensdienste, TLD-Registries, DNS-Dienste
		Betreiber kritischer Anlagen (KRITIS-Betreiber), Digitale Energiedienste
		Bundesverwaltung
Wichtige Einrichtung (§ 28,2)	Mittlere Unternehmen: Unternehmen ab 50 Mitarbeiter oder ≥ 10 Mio. Umsatz + ≥ 10 Mio. Jahresbilanz	Transport und Verkehr, Finanz- und Versicherungswesen, Gesundheit, Trinkwasser, Abwasser, ITK-Dienste, Weltraum, Transport/Verkehr (Post und Kurier), Chemie, Forschung, Verarbeitendes Gewerbe, Digitale Dienste, Lebensmittel, Entsorgung
	unerheblich	Vertrauensdienste

Besonders wichtige Sektoren

Energie  Elektrizität	 Gas	 Öl	 H	 Klima	Transport  Luft	 Wasser	 Schiene	 Auto	Gesundheit  Medizin	 Pharma	Weltraum  Raumfahrt
---	--	---	--	--	---	---	--	---	---	---	---

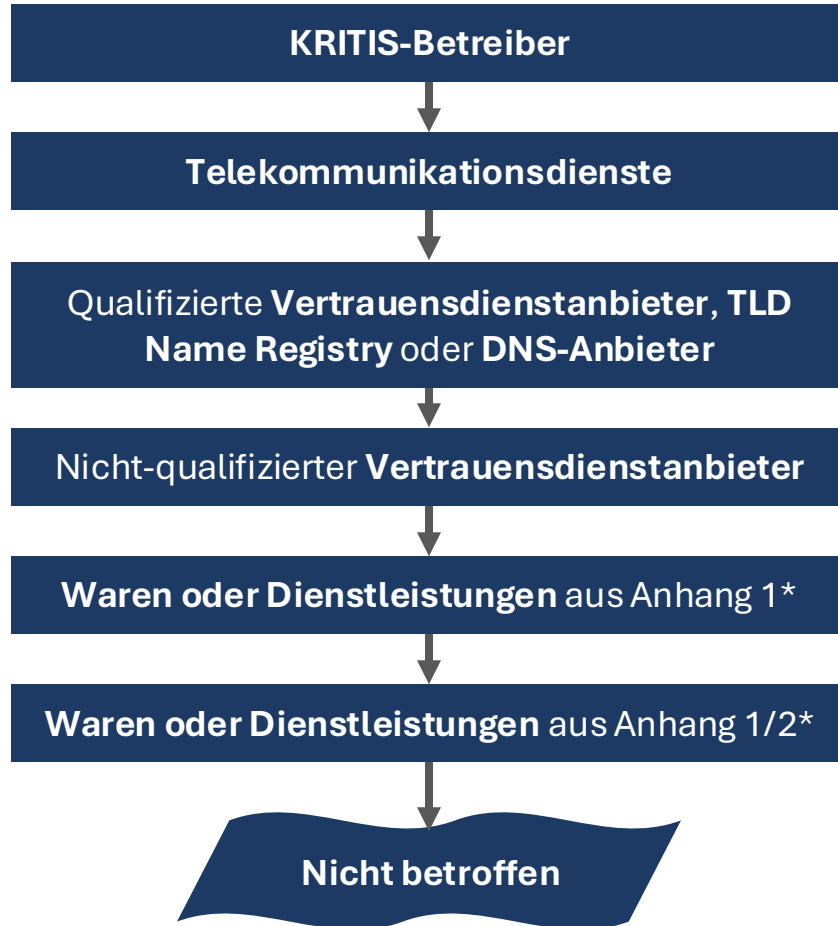
 Trinkwasser	 Abwasser	 Öffentlicher Dienst	 Digitale Infrastruktur	 Banken	 Finanzinfrastruktur	 IKT-Services
--	---	--	---	---	--	---

Wichtige Sektoren

Post 	Abfall 	Digitale Services Anbieter  Online Marktplätze	 Online Suchmaschinen	 Soziale Netze	Chemie 	Lebensmittel 	Forschung 
--	--	--	---	--	--	--	---

 Medizingeräte	 Elektrotechnik	 Elektrisches Equipment	 Maschinenbau	 Motor- und Fahrzeugbau	 Anderer Tansportbau
--	---	--	---	---	--

Entscheidungsbaum



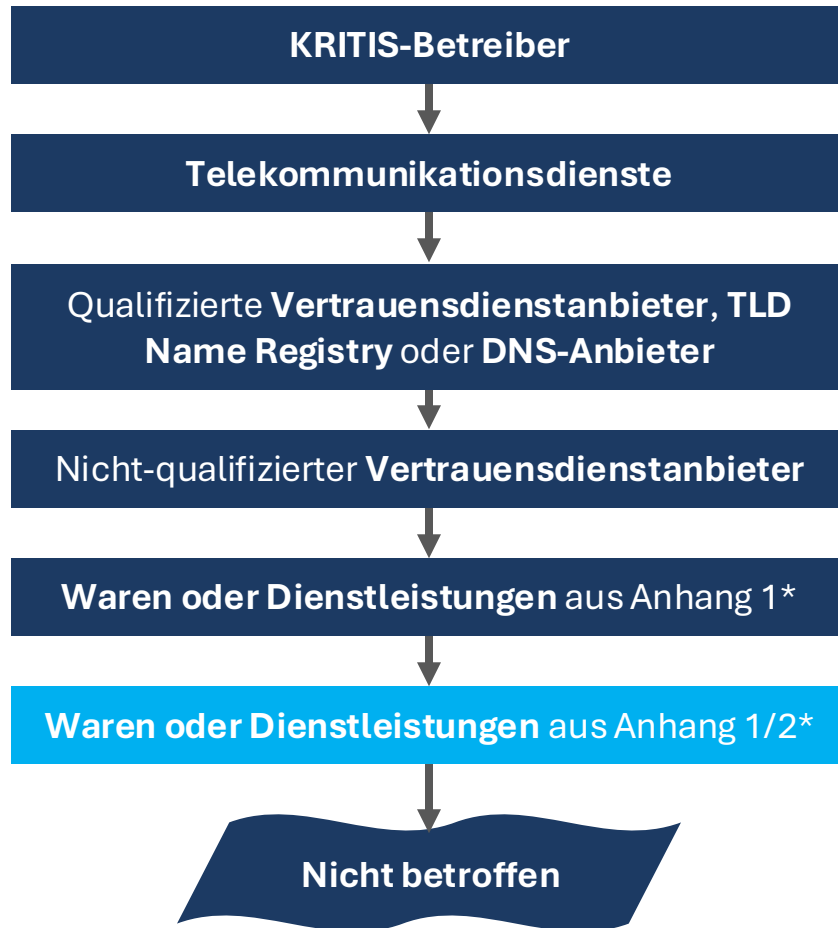
Entscheidungsbaum



Sektor	Art der Einrichtung
Energie	Versorgungsunternehmen, Verteilnetzbetreiber, Betreiber von Ladepunkten, Fernwärme/-kälte Betreiber,
Verkehr	Luftfahrtunternehmen (300/2008/EG), Passagier und Frachtbeförderung (2004/725/EG), Verkehrsmanagement
Bankwesen	Kreditinstitute (575/2013/EU)
Finanz	Betreiber von Handelsplätzen (2014/65/EU)
Gesundheit	Gesundheitsdienstleister (2011/24/EU), Arzneimittelforscher (2001/83/EG)
Trinkwasser	Lieferanten von Wasser für den menschlichen Gebrauch (2020/2184/EU)
Digitale Infrastruktur	Betreiber von Internet Knoten, DNS-Diensteanbieter, Anbieter von Cloud Computing Diensten, Vertrauensdiensteanbieter
IKT-Dienste	Anbieter verwalteter Dienste/Sicherheitsdienste
Öffentliche	Einrichtungen der öffentlichen Verwaltung
Weltraum	Bodeninfrastruktur, Anbieter weltraumgestützter Dienste

Sektoren mit hoher Kritikalität (Anhang 1)

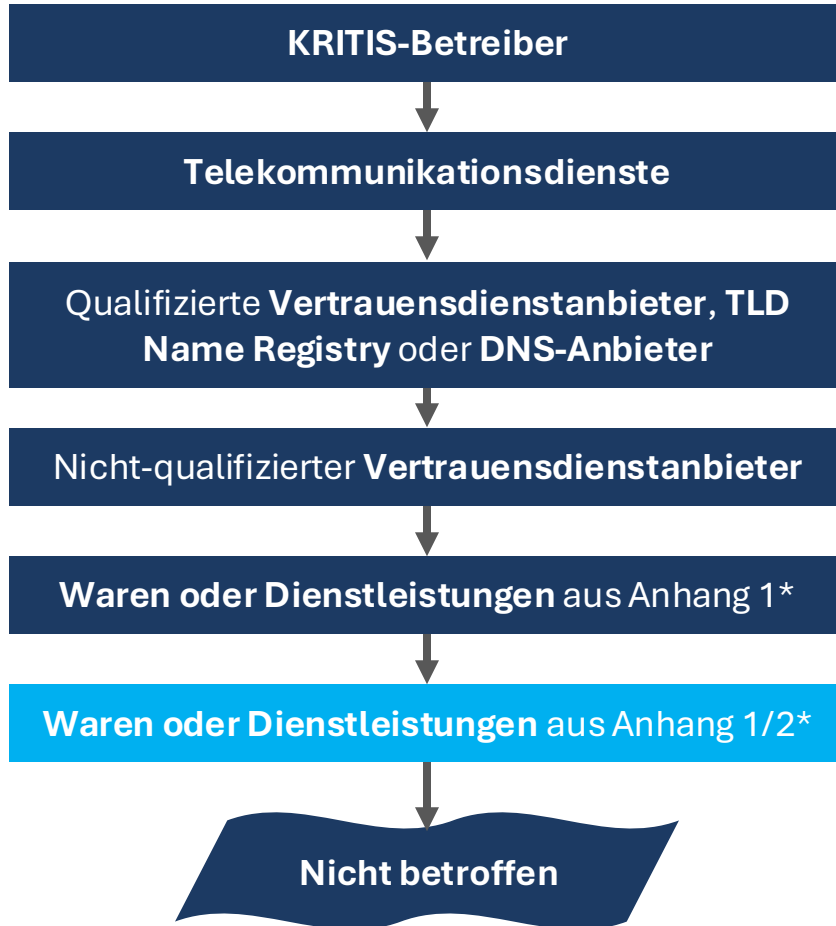
Entscheidungsbaum



Sektor	Art der Einrichtung
Post und Kurierdienste	gemäß 97/67/EG
Abfall-Bewirtschaftung	gemäß 98/2008/EG
Lebensmittel	gemäß 178/2002/EG
Verarbeitendes Gewerbe	Medizinprodukte, Datenverarbeitungsgeräte, Maschinenbau, Herstellung von Kraftwagen und Kraftwagenteilen, sonstiger Fahrzeugbau
Anbieter Digitaler Dienste	Anbieter Online Marktplätze/Online Suchmaschinen/Plattformen für Soziale Netzwerke
Forschung	Forschungseinrichtungen

Sonstige kritische Sektoren (Anhang 2)

Entscheidungsbaum



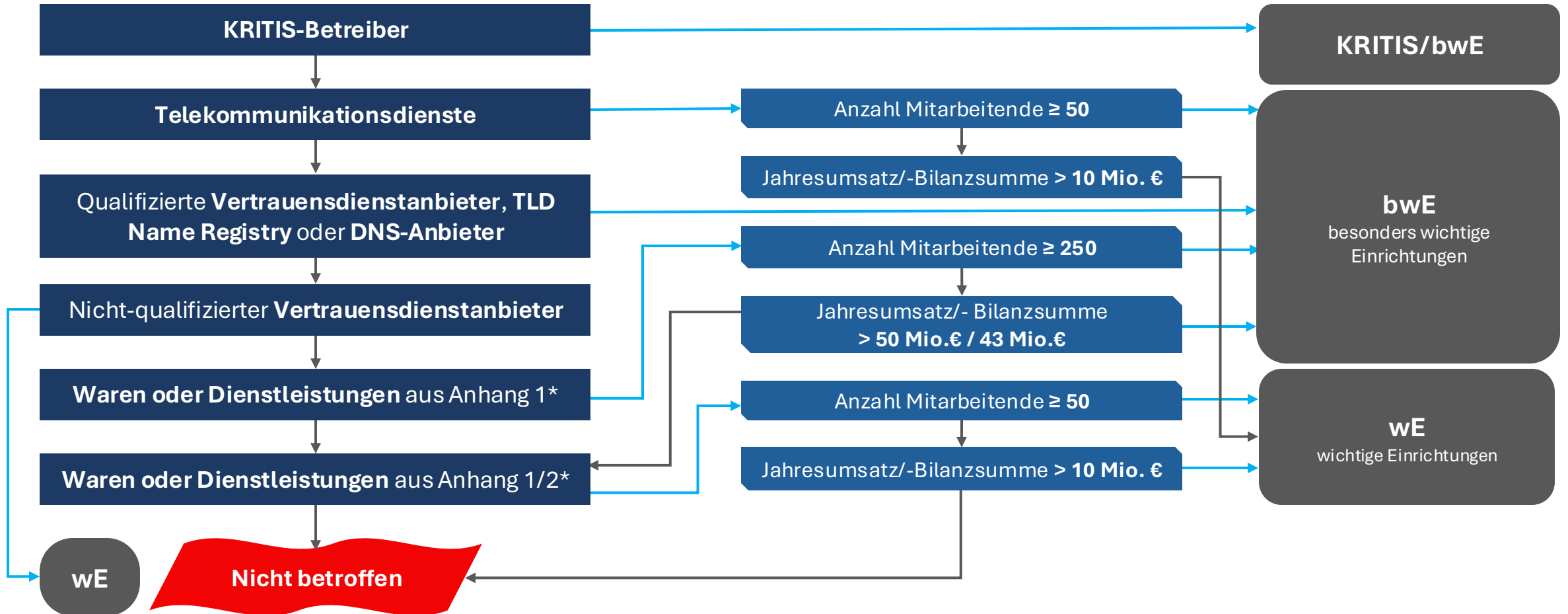
Sonstige kritische Sektoren (Anhang 2)

Sektor	Art der Einrichtung
Verarbeitendes Gewerbe	Medizinprodukte, Datenverarbeitungsgeräte, Maschinenbau, Herstellung von Kraftwagen und Kraftwagenteilen, sonstiger Fahrzeugbau

Unternehmen, die eine der Wirtschaftstätigkeiten im Sinne des Abschnitts C Abteilung 27, 28, 29, 30 der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft ausüben.

Sektor	Art der Einrichtung
Elektrotechnik	Elektromotoren, Generatoren, Batterien, Haushaltgeräte, Lampen und Leuchten, Kabel und Glasfaserkabel, u.v.m.
Maschinenbau	Verbrennungsmotoren, Pumpen und Kompressoren, Öfen und Brenner, Landmaschinen, Lager/Getriebe/Zahnräder, u.v.m.
Kraftwagen	Kraftwagenteile/Motoren, Karosserien, Anhänger, etc.
sonst. Fahrzeuge	Schiff- und Bootsbau, Schienenfahrzeuge, Lufts und Raumfahrzeugbau, militärische Kampffahrzeuge, u.v.m.

Entscheidungsbaum



Legende Service Anbieter/Betreiber: Mitarbeiter/Umsatz Kriterium: (besonders) wichtige Einrichtung: Ja: ➔ Nein: ➔

Verantwortung

Risikomanagement, Schulungen, Sanktionen, Haftung, Sicherheit in der Lieferkette

Auf einen Blick



§30 (1): Risikomanagement

Eine zentrale Forderung von NIS-2: Einrichtungen müssen ihr Risiko managen



Stand der Technik

Einrichtungen müssen verhältnismäßige, wirksame technische und organisatorische Maßnahmen ergreifen, die sich am Stand der Technik orientieren



Sicherheitsziele

Störungen der Verfügbarkeit, Integrität und Vertraulichkeit müssen vermieden werden



Verhältnismäßigkeit

Maßgeblich sind: Ausmaß der Risikoexposition, Größe der Einrichtung, Umsetzungskosten, Eintrittswahrscheinlichkeit, Schwere von Sicherheitsvorfällen, gesellschaftliche und wirtschaftlichen Auswirkungen



Implementierung

Backupmanagement, kryptographische Verfahren, Multifaktor-Authentifizierung, sichere Kommunikation,

§30 (2): Risikomanagement



Schulungen im Bereich Sicherheit in der Informationstechnik



§30 (2.7) Grundlegende Schulungen und Sensibilisierungsmaßnahmen

38 (3) Die Geschäftsleitung muss regelmäßig an Schulungen teilnehmen, um Kenntnisse zur Erkennung, Bewertung und Folgenabschätzung von Risiken und Risikomanagementpraktiken zu erlangen

Aus dem Anhang zum Gesetzestext (siehe §38 und Vorgabe 4.2.4)

1

Geschäftsführer aller adressierten Einrichtungen und die übrigen Mitarbeitenden sollen **regelmäßig** an Cybersicherheitsschulungen teilnehmen.

2

Eine **konkrete Periodizität und Dauer der Schulungen wird nicht vorgegeben**. Es wird angenommen, dass es sich um eine **halbtägige Schulung** handelt (4 Stunden).

3

Das Umsetzungsgesetz fordert nur **allgemeine Schulungen**, um Risiken im Bereich der Cybersicherheit zu erkennen und zu bewerten

4

Es ist **unklar, wer im Unternehmen konkret zu den Geschäftsleitern zählt**. Es wird angenommen, dass **einmal im Jahr zehn leitende Beschäftigte** je Unternehmen eine Schulung absolvieren müssen. An anderer Stelle wird regelmäßig bzgl. Geschäftsleitern mit „**mindestens alle 3 Jahre**“ angegeben.

Sanktionen



§65 (5)-(7) Bußgeldvorschriften und Tatbestände, geltend für alle Einrichtungsgruppen

Höhe	Verstöße (Beispiele)
10 Mio. EUR, wenn Umsatz > 500 Mio: 2% vom weltweiten Umsatz	<ul style="list-style-type: none">• <i>Besonders wichtige Einrichtungen:</i> Vorkehrungen zur Cybersicherheit nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig getroffen (§30,1)
7. Mio EUR, wenn Umsatz > 500 Mio: 1,4% vom weltweiten Umsatz	<ul style="list-style-type: none">• <i>Wichtige Einrichtungen:</i> Mitteilungen (an Kunden oder Öffentlichkeit) werden nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig gemacht (§35,2)
2 Mio. EUR	<ul style="list-style-type: none">• <i>TK-Anbieter:</i> durch BSI angewiesene Maßnahmen zur Abwehr konkreter erheblicher Gefahren werden nicht getroffen (§16, 1)
1 Mio. EUR	<ul style="list-style-type: none">• <i>Betreiber kritischer Anlagen:</i> Nachweis über Erfüllung der Anforderungen wird nicht richtig oder nicht vollständig erbracht (§39,1)
500.000 EUR	<ul style="list-style-type: none">• <i>Besonders wichtige und wichtige Einrichtungen:</i> Zuwiderhandlung gegen Anordnung des BSI zur Vorlage von Nachweisen über die Erfüllung von Verpflichtungen (§61,3)
100.000 EUR	<ul style="list-style-type: none">• Kontaktstelle nicht erreichbar (§33,2)• <i>Besonders wichtige Einrichtungen:</i> Betreten eines Raums nicht gestattet (§61,5)

Haftung



§38 (1) Geschäftsleitungen von bwe und we sind verpflichtet, die von diesen Einrichtungen nach § 30 zu ergreifenden **Risikomanagementmaßnahmen umzusetzen und ihre Umsetzung zu überwachen.**

§38 (2) Geschäftsleitungen, die ihre Pflichten nach Absatz 1 verletzen, **haften** ihrer Einrichtung **für einen schuldhaft verursachten Schaden** nach den auf die Rechtsform der Einrichtung anwendbaren Regeln des Gesellschaftsrechts. Nach diesem Gesetz haften sie nur, wenn die für die Einrichtung maßgeblichen gesellschaftsrechtlichen Bestimmungen keine Haftungsregelung nach Satz 1 enthalten.

1

Geschäftsleitung haftet mit ihrem **Privatvermögen** verschuldungsabhängig, in Verbindung mit der jeweiligen haftungsnorm. Wenn die Gesellschaftsrechtliche Norm keine Haftung vorsieht, haftet die Geschäftsleitung unter Umständen **direkt**.

2

Diese Haftung sollen die Organe der Geschäftsleitung **nicht vertraglich ausschließen** können: Entsprechende Verzichts- und Vergleichsvereinbarungen werden unwirksam sein. Vorübergehend kann auch die **Wahrnehmung der Leitungsaufgaben untersagt** werden.

3

§ 38 Abs. bezieht Cybersicherheit ausdrücklich in die Pflichten der Geschäftsleitung ein. Diese ist **nicht delegierbar**.

Sicherheit in der Lieferkette



§30 (2.4) Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der **Beziehungen zu unmittelbaren** Anbietern oder Diensteanbietern

Aus dem Anhang zum Gesetzestext (siehe Anhang § 30, zu Absatz 2)

Betrachten von **Beziehung zu Lieferanten**, nicht zwischen den Lieferanten

Ihr Unternehmen

Rohstoffe

Verarbeitung

Kunden

Security by **Design**/
Security by **Default**

Vertragliche Vereinbarungen zu Risiko-
managementmaßnahmen, Bewältigung von
Cybersicherheitsvorfällen, Patchmanagement

Empfehlungen des Bundesamtes in Bezug
auf zugelieferte Produkte und Dienstleistungen

Was bedeutet Stand der Technik?

Unbestimmter Rechtsbegriff, häufig im Zusammenhang mit Gesetzen betreffend der **Informationssicherheit**

i

Info

Der „Stand der Technik“ **verschiebt den Maßstab des Gebotenen an die Front der technischen Entwicklung**. Wenn dieser gefordert wird, muss **fortlaufend neu investiert** und die Maßnahme beschafft werden, die die Erreichung eines **hohen Schutzniveaus für die IT-Sicherheit voraussichtlich als gesichert erscheinen lässt**.

(Grundlegend dazu schon Bundesverfassungsgericht, Beschl. v. 8.8.1978 – 2 BvL 8/77)

Es handelt sich also um einen **dynamischen Begriff**, der sich an die technischen Entwicklungen anpasst

Praxisnah

Bundesverband IT-Sicherheit e.V. 

IT-Sicherheitsgesetz und Datenschutz-Grundverordnung:
Handreichung zum "Stand der Technik"
Technische und organisatorische Maßnahmen

 **TECHNICAL IMPLEMENTATION GUIDANCE V1.0**

 **VDI**
bitkom


TECHNISCHE REGEL [AKTUELL]
DIN SPEC 27076:2023-05


NIS-2 Konformität

 Bundesamt für Sicherheit in der Informationstechnik

BSI-IT-Grundschutz
BSI-Standard 200-1, 200-2, 200-3 und
IT-Grundschutzkompendium

Audit

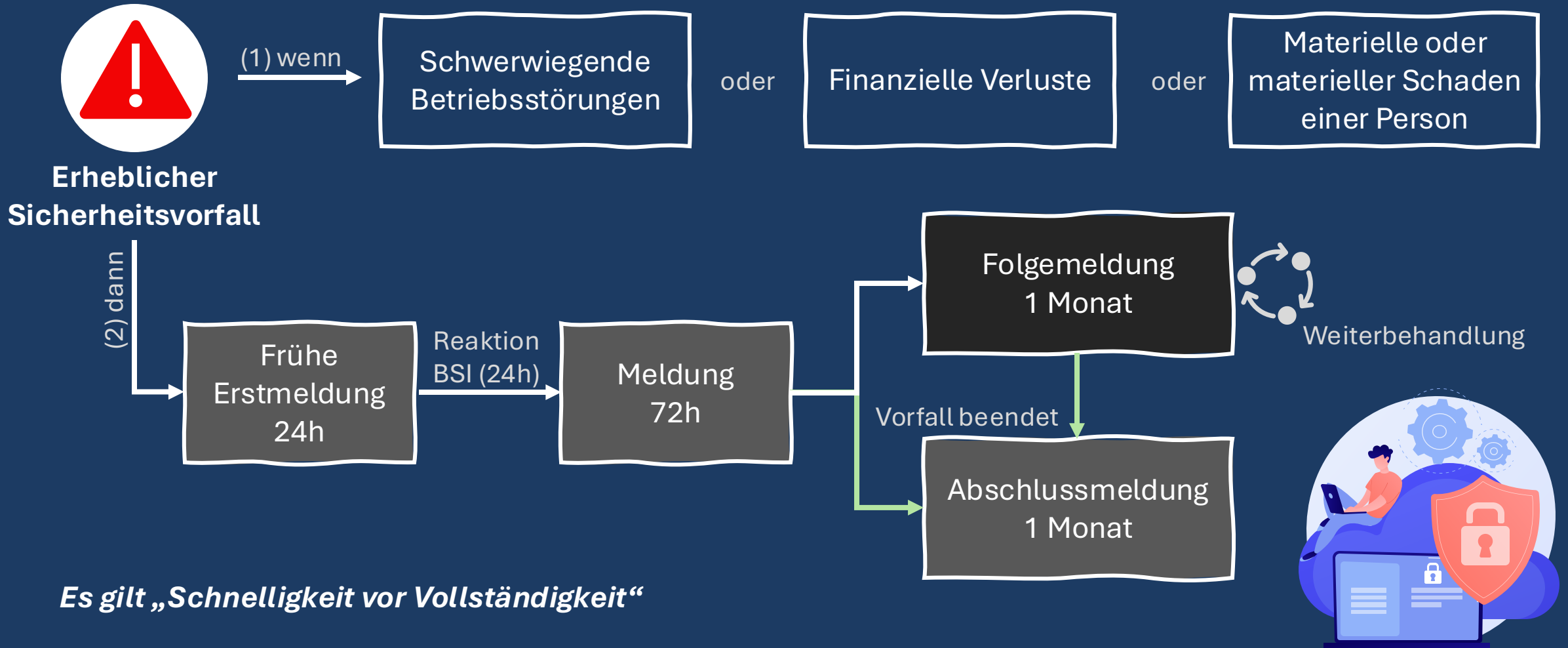
 **ISO/IEC 27001**
Informationssicherheit, Cybersicherheit und Datenschutz – Informationssicherheitsmanagementsysteme - Anforderungen

 **ISO/IEC 27002**
IT-Sicherheitsverfahren – Leitfaden für das Informationssicherheits-Management





Meldepflichten

Erstmeldung, Vorfallmeldung, Rückmeldung BSI, Abschlussmeldung

Die Meldekette



Meldungstypen

 Frühe Erstmeldung	 Meldung	 (Folgemeldung)	 Abschlussmeldung
<ul style="list-style-type: none"> • Charakter einer Frühwarnung • Verdacht, ob Vorfall auf rechtswidrige oder böswillige Handlungen zurückzuführen ist • Verdacht, ob grenzüberschreitende Auswirkungen möglich sind 	<ul style="list-style-type: none"> • Aktualisierung der Informationen der frühen Erstmeldung • Bewertung des erheblichen Sicherheitsvorfalls • Schweregrad des Vorfalls • Auswirkungen des Vorfalls • ggf. Kompromittierungsindikatoren (IOCs) 	<ul style="list-style-type: none"> • Aktualisierung der Informationen früherer Meldungen 	<ul style="list-style-type: none"> • Abschlussmeldung, wenn Vorfall beendet ist • Ausführliche Beschreibung des Sicherheitsvorfalls, dessen Schweregrads und seiner Auswirkungen, zur Art der Bedrohung bzw. zugrundeliegenden Ursache • Getroffene und laufende Abhilfemaßnahmen • Grenzüberschreitende Auswirkungen des Sicherheitsvorfalls

KMU.kompetent.sicher

Die NIS-2 Test und Trainingsplattform

<https://kmu-kompetent-sicher.de/>

CYBERSicher

KMU.kompetent.sicher.
NIS2 Test- und
Trainingsplattform

[Blog](#) [Das Projekt](#) [Veranstaltungen](#) [Kontakt](#)



🚩 Das Projekt ist gestartet.

KMU.kompetent.sicher.

NIS-2 Test- und Trainingsplattform

Loslegen

Informationen Erhalten

*Hier geht es zu den
Schulungen.*



KMU.kompetent.sicher

Fokus auf KMU

- Lerninhalte richten sich speziell auf die Bedürfnisse von KMU
- Unterstützung beim Aufbau von IT-Sicherheitskompetenz

- Netzwerk-Events, Erfahrungsaustausch
- Wissenstransfer in die Wirtschaft

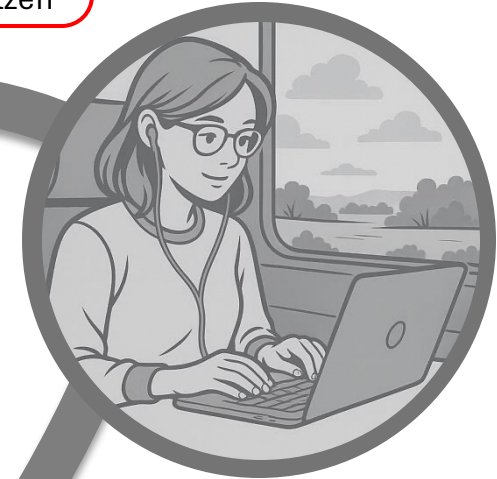
- Permanente Erhebung von Unternehmensbedürfnissen durch Fragebögen/Umfragen
- Vortragsreihen und Aufklärungsarbeit



Kompetenztests

- Individuelle Bedarfsermittlung, um ITS-Kompetenzniveaus zu ermitteln
- Risiken erkennen und einschätzen

- Unterschiedliche themenspezifische Lernformate
- Text, Video, Audio, KI-Generativ



Learning Nuggets

- Diskrete Lerneinheiten, thematischer Fokus auf einzelne Themenpunkte
- Sinnvolle Integration in Arbeitszeit

NIS-2 Erfüllung

- Schulungsverpflichtung für Mitarbeiter und Geschäftsführung
- Orientierung an Maßnahmen aus NIS-2 Richtlinie (EU2022/2555 und NIS2UmsuCG)



KMU.kompetent.sicher Lernplattform

Legen Sie noch heute los ...

Anmelden bei unserer kostenlosen **NIS2-Trainingsplattform**

7 kostenlose IT-Sicherheits-Zertifikate

Aktuell bleiben: Folgen Sie uns hier:

- **LinkedIn**: #kmukompetentsicher
- **Blog** (Neuigkeiten rund um NIS2)
- treffen Sie uns in **Veranstaltungen** und auf **Messen**
kostenlos

Machen Sie mit Ihrem Unternehmen MIT:

Ihr Unternehmen für **Erfa-Runden** zum Thema NIS2
kostenlos



ab 2026:

- **Learning-Nuggets**
- **Regelkreis und Cockpit**

... mit mehr IT-Sicherheit in Ihrem Unternehmen!

Referenzen

- https://www.tuev-verband.de/fileadmin/user_upload/Content_local/Studien_local/2025_TUEV-Verband_Cybersecurity-Studie_Studienbericht.pdf
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Digitalbarometer/CyMon-ProPK-BSI_2025_Kurzbericht.pdf?__blob=publicationFile&v=2
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2024.pdf?__blob=publicationFile&v=5
- <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html>
- <https://www.datacore.com/blog/nis2-directive/>
- https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Meldepflicht/NIS-2-Meldepflicht_node.html
- https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/Downloads/kabinettsfassung/CI1/nis2-regierungsentwurf_2025.pdf?__blob=publicationFile&v=4
- https://web-assets.eset.com/fileadmin/ESET/DACH/Docs/Stand_der_Technik/ESET_Whitepaper_Stand_der_Technik_2.pdf
- <https://www.dinmedia.de/de/technische-regel/din-spec-27076/365252629>
- <https://www.datenschutzexperte.de/blog/geschaeftsfuehrerhaftung-nis2>
- <https://www.security-insider.de/nis2-umsetzungsgesetz-update-auswirkungen-unternehmen-a-c7282a16efff52830dc053969abf45ca/>
- <https://www.openkritis.de/betreiber/bussgelder-kritis-bsig.html>
- https://www.kritisschutz.de/geschaeftsfuehrerhaftung_nis2/
- <https://www.csoonline.com/article/4022498/nis2-umsetzungsgesetz-geschäftsleitung-haftet-mit-privatvermogen.html>
- <https://ecs-org.eu/ecso-uploads/2025/01/ECISO-NIS2-White-Paper.pdf>

Bilder und Grafiken

- https://www.freepik.com/free-vector/general-data-security-personal-information-protection-database-access-control-cyber-privacy-synchronized-gadgets-cross-platform-devices-regulation_11669630.htm#fromView=search&page=1&position=1&uuid=73ec13c8-1f67-4561-a021-af178b948e55&query=cybersecurity
- https://www.freepik.com/free-vector/industrial-cybersecurity-abstract-concept-illustration_11668653.htm#fromView=search&page=1&position=3&uuid=40136b46-6e7d-4978-a0a0-c619745d2aba&query=cybersecurity