KEDi
Kompetenzzentrum
Energieeffizienz
durch Digitalisierung

25.11.2025

Herzlich willkommen zum KEDi Webinar

Augen auf: (Cyber)Sicher in die Zukunft - Die Umsetzung der EU-Richtlinie (NIS-2) zur Cybersicherheit in Unternehmen

Ein Projekt der
dena

Allgemeine Informationen

Webinar wird aufgezeichnet

Fragen gerne im Chat stellen

Mikrofone sind stumm geschaltet

Vortragsfolien erhalten Sie im Nachgang

Allgemeine Informationen

- **Fortbildungsanerkennung**: Als Energieeffizienz-Expert:in können Sie sich das Webinar als Fortbildung anerkennen lassen.
- Anfrage an info@kedi-dena.de: Wir senden Ihnen die Teilnahmebescheinigung nach dem Webinar zu.

Vorstellung KEDi

Seit **2023** ist das KEDi als bundesweite Anlaufstelle mit Sitz in **Halle (Saale)** aktiv. Es ist ein Projekt der **dena** (Deutsche Energie-Agentur) und unterstützt **Industrie-KMU** sowie die **Gebäudewirtschaft** dabei, **Energieeffizienzpotenziale durch Digitalisierung** besser zu erschließen.

Was erwartet Sie heute?

Ablauf des Webinars

- **Impulse**
  - **Umsetzung der Anforderungen der NIS-2-Richtlinie in Unternehmen**

    Volker Fett | Transferstelle Cybersicherheit im Mittelstand
  - **Vorstellung dena-Roadmap Cybersicherheit**

    Marius Dechand | dena
  - **Handlungsempfehlungen für den cybersicheren Umgang mit cloudbasierten Energiemanagementsystemen**

    Frank Borchardt | VDE
- Fragen aus dem Chat/Diskussion
- Ausblick und Verabschiedung

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

IT-Sicherheit IN DER WIRTSCHAFT

Augen auf: (Cyber)Sicher in die Zukunft

Volker Fett
Transferstelle Cybersicherheit im Mittelstand
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH

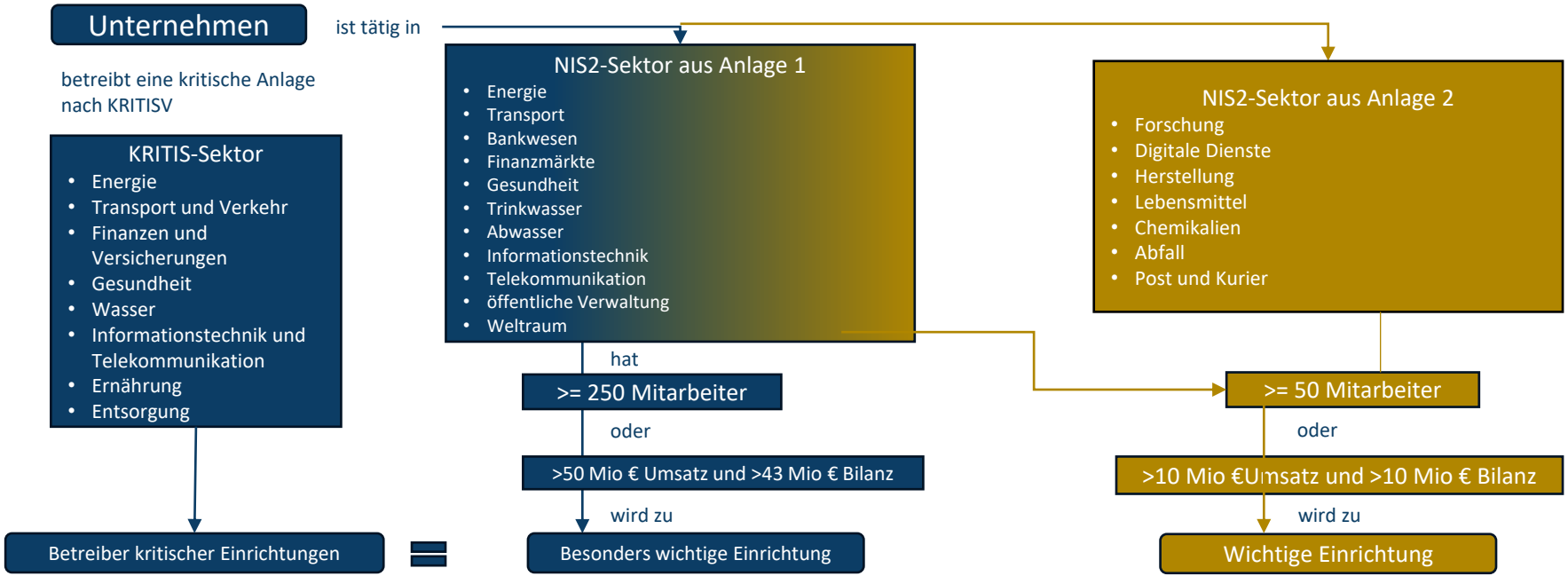
Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Regulierung in der Cybersicherheit – NIS2

Jun 2016		NIS1
Dez 2022		Entwurf NIS2- Umsetzungsgesetz
Jan 2023	Inkrafttreten	NIS-2 Richtlinie
17. Okt 2024		Fristablauf zur Umsetzung
11. Sep 2025		Bundesregierung legt Gesetzentwurf dem Bundestag vor
13./21. Nov. 2025		NIS2- Umsetzungsgesetz im Bundestag und Bundesrat
Dez 2025/ Anfang 2026		Inkrafttreten der NIS2- Umsetzung

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

Mittelstand-Digital



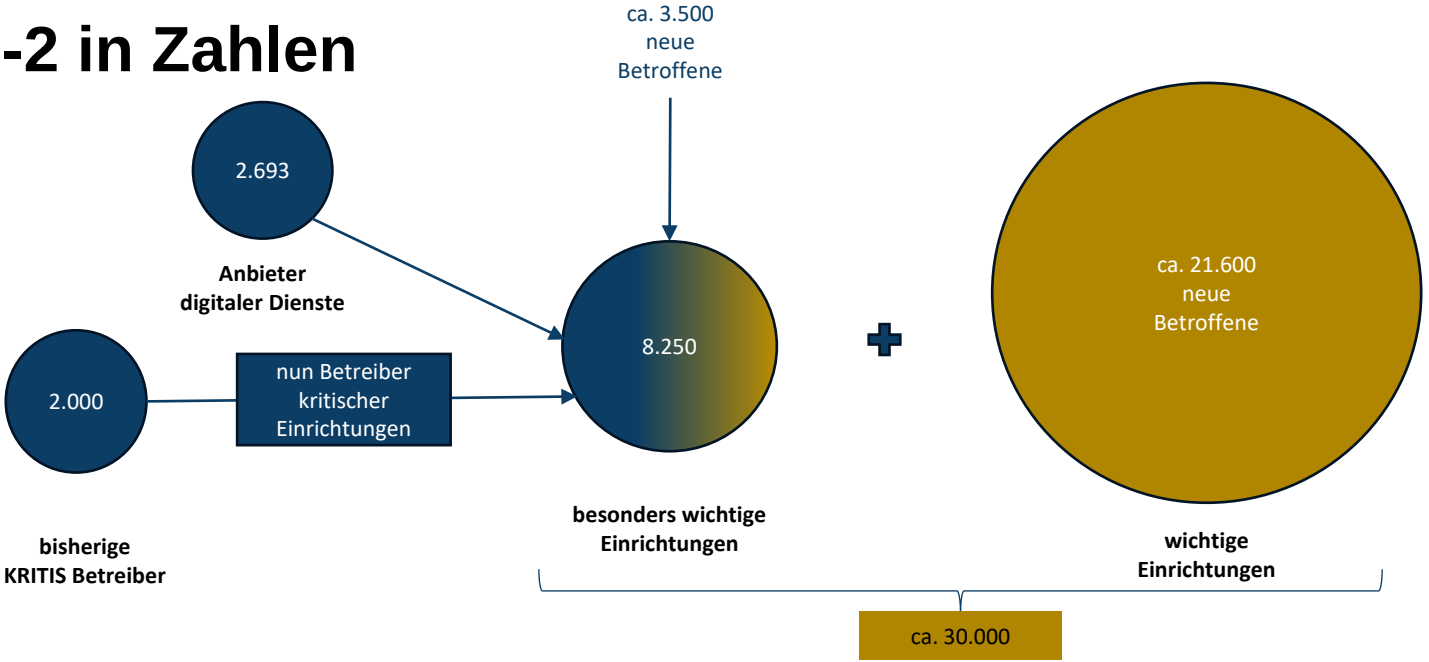
"Betreiber kritischer Anlagen" gelten auch "besonders wichtige Einrichtungen"

Übernahme von cybersicher.org

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

Mittelstand-Digital

NIS-2 in Zahlen



Übernahme von cybersicher.org

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

NIS-2-Betroffenheitsprüfung

Sind Sie unsicher, ob Ihr Unternehmen von der NIS-2-Richtlinie der EU betroffen ist?

Die NIS-2-Betroffenheitsprüfung des BSI bietet Ihnen in wenigen Schritten dafür eine erste Orientierung.

- BSI - NIS-2-Betroffenheitsprüfung (bund.de)

Einrichtungen der Bundes-, Landes- und Kommunalverwaltung werden in der NIS-2-Betroffenheitsprüfung nicht betrachtet.

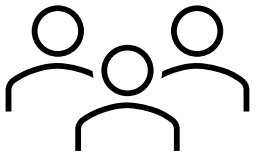
Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital

Auswirkungen auf die Lieferkette

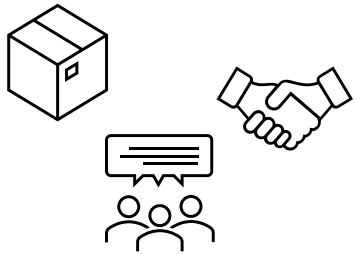
„Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu **unmittelbaren** Anbietern oder Diensteanbietern“,

Innenverhältnis: Prozesse und Organisation ← (un)mittelbare Verpflichtung nach der NIS2 Richtlinie → Außenverhältnis: Vertragliche Vereinbarungen



Beschäftigte

Unternehmen



Kunden, Zulieferer und Dienstleister

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

Pflichten für Unternehmen in NIS-2

§30 Risikomanagement

- Risikoanalysen, ISMS
- Notfallkommunikation
- Training

§32 Meldepflichten

- BSI: zentrale Meldestelle
- 24h/72h/30 Tage
- Zwischenmeldungen

§33 Registrierung

- eigenständige Identifikation
- Registrierungsfrist 3 Monate
- Registrierung auch durch BSI möglich

§39 Nachweispflichten

- Dokumentationspflichten
- Stichproben durch BSI
- mögliche Einsichtnahme durch BSI

§ 35 Unterrichtungspflichten

- BSI: Weisungsbefugnis für Unterrichtung für Kunden
- und für Veröffentlichung von Vorfall

§38 Governance

- GFs müssen Risikomanagement-maßnahmen umsetzen
- GFs haften für Schaden bei Pflichtverletzung
- GFs müssen an Schulungen teilnehmen

§31 KRITIS-Anforderungen

- Angriffserkennung verpflichtend
- Besondere Sorgfalt bei der Auswahl der Maßnahmen
- kontinuierlicher Einsatz im Betrieb

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

Meldewesen mit NIS-2

Erheblicher Sicherheitsvorfall

Interne Meldestelle

<24 h
- Verdacht rechtswidriger Handlungen
- grenzüberschreitende Auswirkungen

72 h
- Bestätigung/ Aktualisierung Erstmeldung
- erste Bewertung mit Schweregrad, Auswirkungen

Zwischen-meldungen
- Auf Ersuchen des BSI
- relevante Statusaktualisierungen

1 Monat
- Ausführliche Beschreibung mit Schweregrad
- Art der Bedrohung
- Abhilfemaßnahmen

BSI -Meldestelle

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

GFs müssen an Schulungen teilnehmen

initiale Veröffentlichung vom 30.09.2025

- Umsetzungs-, Überwachungs- und Schulungspflicht für Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen
- …Die Geschäftsleitungen besonders wichtiger Einrichtungen und wichtiger Einrichtungen müssen 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 sowie um die Auswirkungen von Risiken sowie Risikomanagementpraktiken auf die von der Einrichtung erbrachten Dienste beurteilen zu können.

- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-geschaeftsleitungsschulung.pdf?__blob=publicationFile&v=3

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

NIS-2

Maßnahmenkatalog für ein Unternehmen

Quelle: https://de.fotolia.com/p/204251986

- Umsetzung nach „Allgefahrenansatz“ (all hazards approach)
- keine isolierte Betrachtung, sondern das Komplettpaket u.a. mit
  - Informations- und Sicherheits-Management-System (ISMS)
  - Business Continuity Management (BCM)
  - Supply Chain Management
  - Training in Bezug auf „Cyber- Security Hygiene“ („grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik“)
  - Kryptographie und Authentifizierung
  - physische Gefahren

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

NIS-2

„grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik“ im Überblick (alt Cyber-Securitiy-Hygiene)

- Schärfung des Bewusstseins für Cyberbedrohungen Phishing oder Social-Engineering
- Passwortänderungen und die Verwendung sicherer Passwörter
- Zero-Trust Grundsätze
- Einschränkungen der Zugriffe auf Administratorebene
- Soft- und Hardware-Updates
- Verwaltung neuer Installationen
- Netzwerk-segmentierung
- Datensicherung

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

Sanktionen im NIS2UmsuCG

Allgemeine Tatbestände	Wichtige Einrichtungen	Besonders wichtige Einrichtungen
• 100.000,- € bis 2.000.000 €	• 100.000,- € bis 7.000.000 € oder 1,4% vom globalen Umsatz	• 100.000,- € bis 10.000.000 € oder 2,0% vom globalen Umsatz

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

NIS-2

Vorbereitende Schritte

Sicherheitsleitlinie vorhanden?

- Bekennen der Unternehmensleitung zur Informationssicherheit

Übersichten vorhanden?

- Infrastruktur
- Rechner
- Geschäftsprozesse
- Berechtigungen
- Zugang

Ergriffene Maßnahmen

- Firewall?
- Awareness Schulungen

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

Mittelstand-Digital

Referent

Volker Fett
LinkedIn: Volker Fett
volker.fett@transferstelle-cybersicherheit.de

- tti Technologietransfer und Innovationsförderung Magdeburg GmbH
  - Projektleiter Transferstelle Cybersicherheit im Mittelstand
    - zertifizierter ISO und BCM-Praktiker (TÜV Nord)
- cubeoffice GmbH & Co. KG
- Leitspruch:
  - Immer mal den Blickwinkel wechseln -

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

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

IT-Sicherheit IN DER WIRTSCHAFT

VIELEN DANK

für Ihre Aufmerksamkeit!

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

aufgrund eines Beschlusses des Deutschen Bundestages

Mittelstand-Digital

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

IT-Sicherheit IN DER WIRTSCHAFT

Was bieten wir darüber hinaus an?

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

Mehr Cybersicherheit im Mittelstand

Unsere Mission

Die **Transferstelle Cybersicherheit im Mittelstand** unterstützt als zentrale Plattform und Anlaufstelle kleine und mittlere Unternehmen, Start-Ups und Handwerksbetriebe.

Wir sind Netzwerkknotenpunkt.

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

Projektpartner

- Der Mittelstand., BVMW e.V.
- FZI Forschungszentrum Informatik, Karlsruhe
- Institut für Berufspädagogik und Erwachsenenbildung der Universität Hannover
- tti Technologietransfer und Innovationsförderung Magdeburg GmbH

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

CYBERsicher, aber wie?

Hier setzen wir Schwerpunkte:

- Unternehmen präventiv **schützen**
- Angriffe einfach **erkennen**
- Auf Angriffe schnell **reagieren**

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

Mittelstand-Digital

Unsere Leistungen

Informieren

Wir erhöhen Wissen.

- WebImpulse
- CYBERDialoge
- Selbst-Check CYBERsicher

Qualifizieren

Wir bieten Schulungen.

- Workshops
- Train-the-Trainer
- mIT Sicherheit ausbilden

Vernetzen

Mehrwert durch Vernetzung.

- Vermittlung an IT-Expert:innen
- Partnernetzwerk
- Fachkongress

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

Mittelstand-Digital

Unsere Angebote für den Mittelstand

Cybersicherheitsniveau im Betrieb erhöhen

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

Unsere Angebote für die Cybersicherheitscommunity

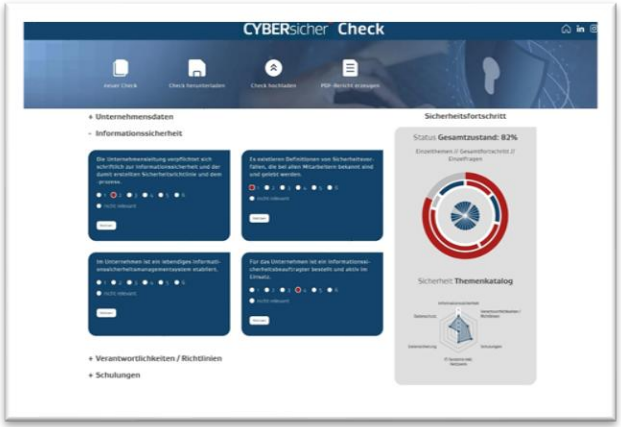
Gemeinsam für mehr Cybersicherheit im Mittelstand

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

Informieren: CYBERsicher Check

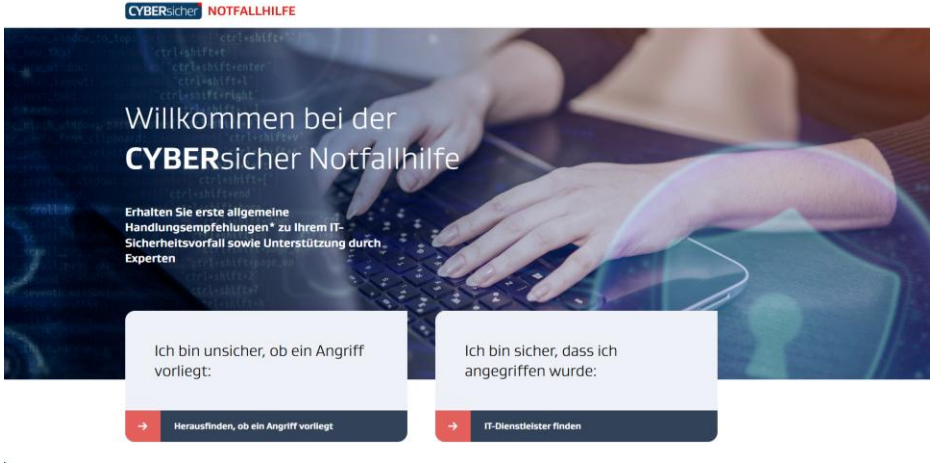
- Selbstanalyse des IT-Sicherheitsniveaus im Unternehmen
- Empfehlungen geeigneter Maßnahmen zur Steigerung des IT-Sicherheitsniveaus
- NEU: seit April 2024
  - Freie Nutzung des Tools, konkrete Handlungsempfehlungen (kuratierte Liste)
  - Einweisung der Partner für Einführungsgespräche durch Train-The Trainer Maßnahme

CYBERsicher-Check.de



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

CYBER-sicher Notfallhilfe



www.notfallhilfe.transferstelle-cybersicherheit.de/

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

Hilfe zur Selbsthilfe

www.fitnis2.de/

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

Mittelstand-Digital

Weitere Informationen zur Transferstelle Cybersicherheit im Mittelstand

www.transferstelle-cybersicherheit.de

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

Mittelstand-Digital

Future Energy Lab

NIS2 Roadmap

Ein Projekt der

dena

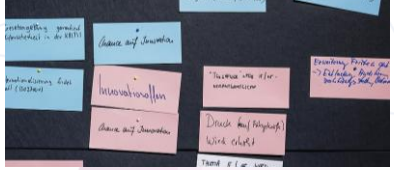
BRANCHENPLATTFORM CYBERSICHERHEIT

Ziel:

- Nachhaltige Wissensbasis
- Vertrauensvoller Raum für Austausch
- Antizipation von neu entstehenden Problemen
- Bewusstsein stärken

Umsetzungsphase:

- Partnerkreis aufbauen
- Austausche anregen: 3x Forum, 4 Workshops, 9 Partnerkreissitzungen
- Ergebnisse generieren: Themenroadmap, Cyberfit, gemeinsam Lernen, Cybersicherheits-Zertifizierungen, NIS2 Roadmap



NIS2 ROADMAP

Wesentliche Inhalte:

- Entwicklung einer **praxisorientierten Umsetzungs-Roadmap für die NIS-2-Richtlinie**, zugeschnitten auf KMUs und Start-ups der Stromwirtschaft.
- Erprobung der Maßnahmen durch ein **Mentoring-Programm.** Unterstützung von 7 KMU & Start-ups über 2 Monate.
- **Priorisierung** der umzusetzenden Maßnahmen sowie Entwicklung **praxisnaher Tipps**, die KMU bei der Umsetzung in ihrem Betrieb berücksichtigen sollten.

Ziele:

- Ein **besseres Verständnis** für die Anforderungen und Herausforderungen der NIS-2-Richtlinie zu schaffen
- Unterstützung von KMU, die indirekt durch die **Lieferketten-Abhängigkeiten** von NIS-2 betroffen sind.
- Vermittlung praxisnaher **Handlungsempfehlungen**.

Future Energy Lab

dena NIS2-Roadmap für Energie-Start-ups

In 6 Etappen durch die wichtigsten NIS2-Anforderungen. Von der Theorie zur Praxis mit konkreten Beispielen, Übungen und Meilensteinen.

Über die Roadmap >

Dies ist ein interaktives PDF. Sie können zwischen den Etappen springen.

Ein Projekt der dena

int[cube]

CYBER POLICY HAUS

GESELLSCHAFT FÜR INFORMATIK

Etappe

Risiko-management

Relevanz: Stringentes Risikomanagement im Kontext der Informationssicherheit schafft Vertrauen für alle Seiten.

Ein strukturiertes Risikomanagement sorgt dafür, dass technische und organisatorische Maßnahmen verhältnismäßig zu den identifizierten Risiken sind. Verfolgen Sie einen „Allgefahrenansatz“, indem Sie Gefahren systematisch identifizieren, bewerten (Vertraulichkeit, Integrität, Verfügbarkeit) und priorisieren. So können Sie gegenüber Ihren Kunden und Investoren und Aufsichtsbehörden nachweisen, dass Sie Risiken konsequent steuern und die Versorgungssicherheit entlang der gesamten Wertschöpfungskette unterstützen.

Etappen FAQ

Zur Roadmap

Etappenabschnitt

Identifikation von Risiken

Ordnen Sie Ihre Geschäftsprozesse nach Kritikalität und bewerten Sie die zugehörigen Gefährdungen hinsichtlich ihrer Auswirkungen.

- Info: Relevante Dokumente und Standards
- Übung: Einstufung schutzwürdiger Geschäftsprozesse
- Übung: Elementare Gefährdungen einstufen

Etappenabschnitt

Umgang mit Risiken

Implementieren Sie passende technische und organisatorische Maßnahmen, um identifizierte Risiken effektiv zu steuern und zu minimieren.

- Übung: Dimensionen der Risikoeinschätzung
- Methode: Risiko bewerten
- Info: Strategien zur Risikobehandlung

Zentrale Empfehlungen

- BSI-Betroffenheitsprüfung
- Registrierung und Meldungen priorisieren, Kapazitäten nach und nach aufbauen
- Austauschen, vernetzen und voneinander lernen

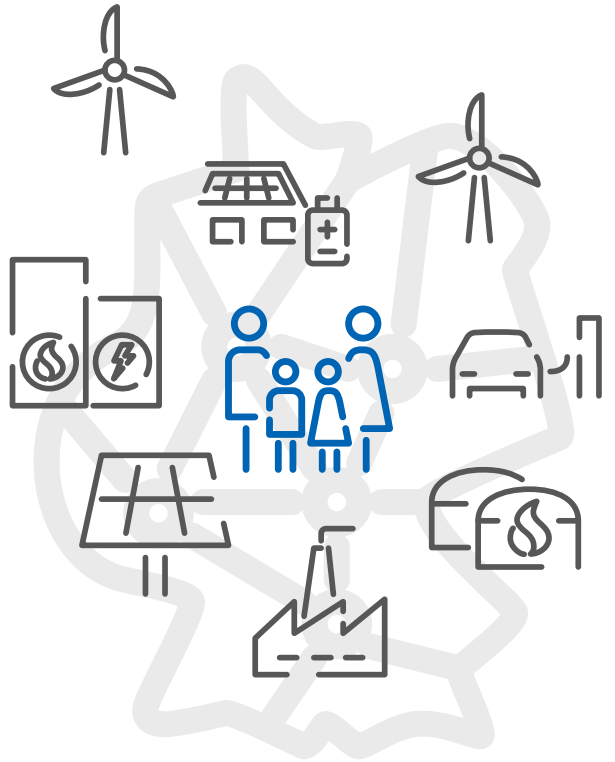
Future Energy Lab

Vielen Dank

Marius Dechand, Seniorexperte Cybersicherheit, dena

Ein Projekt der dena

Handlungsempfehlungen für den cybersicheren Umgang mit cloudbasierten Energiemanagementsystemen



Frank Borchardt
VDE FNN

KEDi Webinar, 25. November 2025

VDE FNN

VDE FNN – die Netzexperten im VDE

Gegründet
2008

511 Mitglieder aus
12 Nationen
Unternehmen, Behörden und Wissenschaft

Ca. 500
ehrenamtliche Experten
arbeiten in 60 Gremien

38
Anwendungsregeln

170
Lastenhefte & Hinweise

VDE FNN Anwendungsregeln
definieren die Regeln der Technik (§49 EnWG)

www.vde.com/de/fnn

Unser Stromnetz – mit Solidarität und Sicherheit

Von der Algarve bis in den Donbass

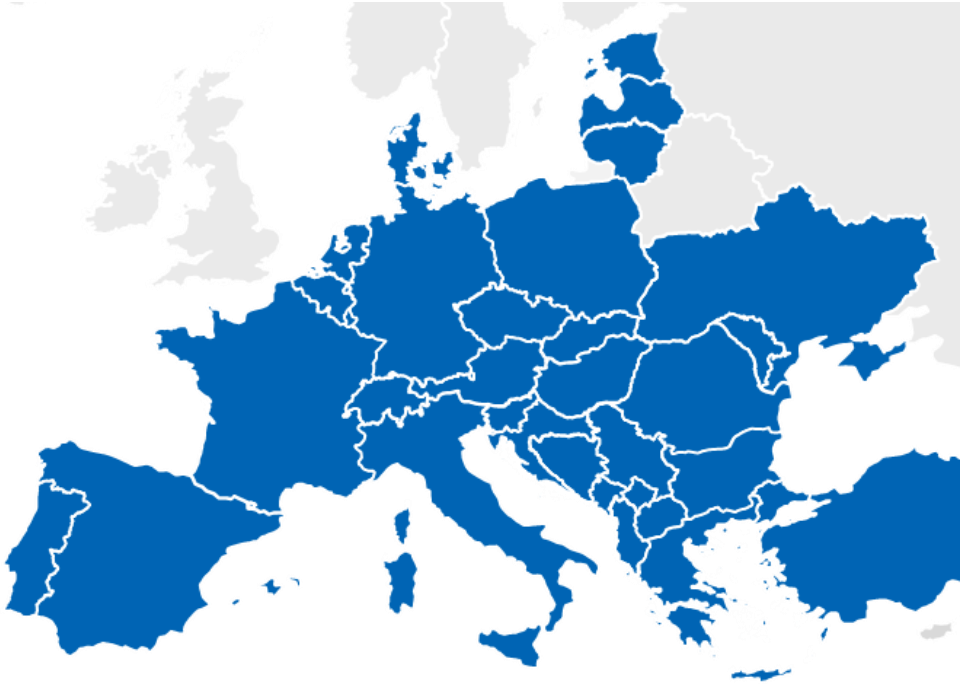
Das kontinentaleuropäische Verbundnetz

31
verbundene Staaten
seit 17.03.2022 inkl. Moldawien und Ukraine
seit 09.02.2025 inkl. Baltische Staaten

35
Übertragungs-
netzbetreiber

>440.000 km*
Übertragungsnetz
(Stromkreislänge ≥110 kV)

500 Millionen
versorgte Menschen

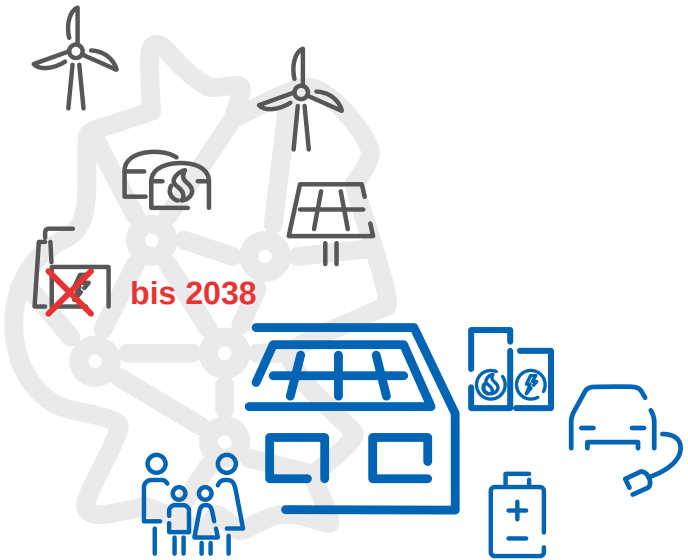


* davon Deutschland ca. 36.000 km

Quellen: ENTSO-E, Statista

Warum ist das wichtig?

Durch die Transformation zum „Prosumer“ werden Privathaushalte systemrelevant



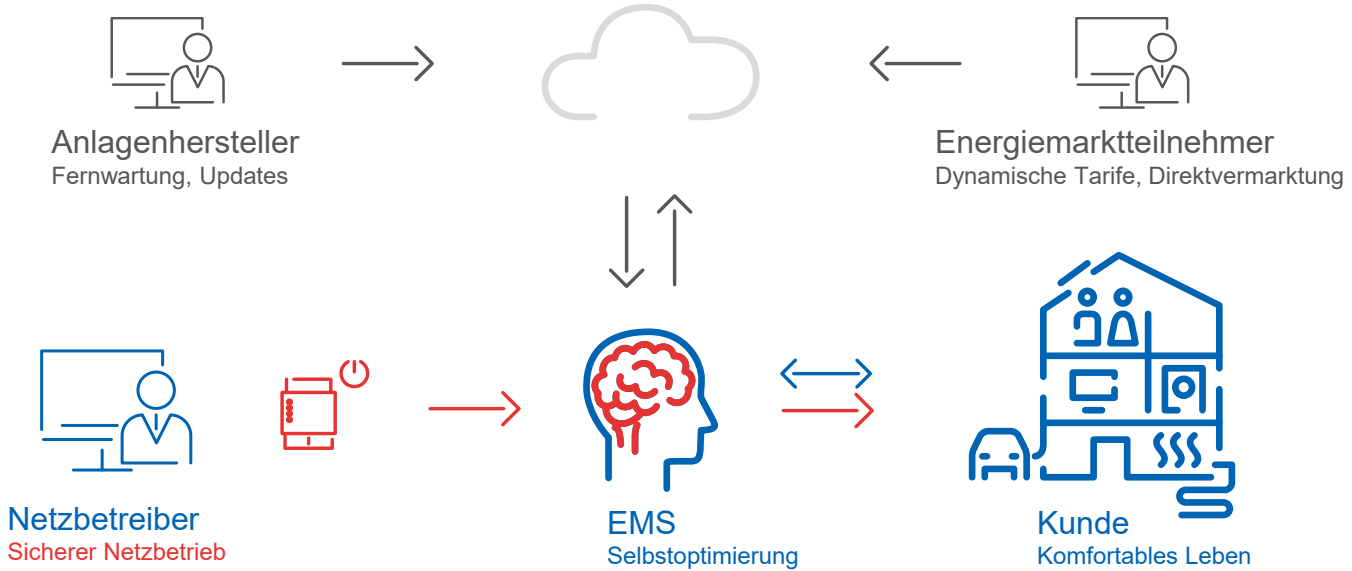
Haushalt in Zukunft

Wärmepumpe	3 - 16 kW
Wallbox	11 - 22 kW
	10 - 14 kW
PV-Anlage	**+25 kW**

Summe der steuerbaren Leistung ergibt ein attraktives Ziel für Cyberangriffe

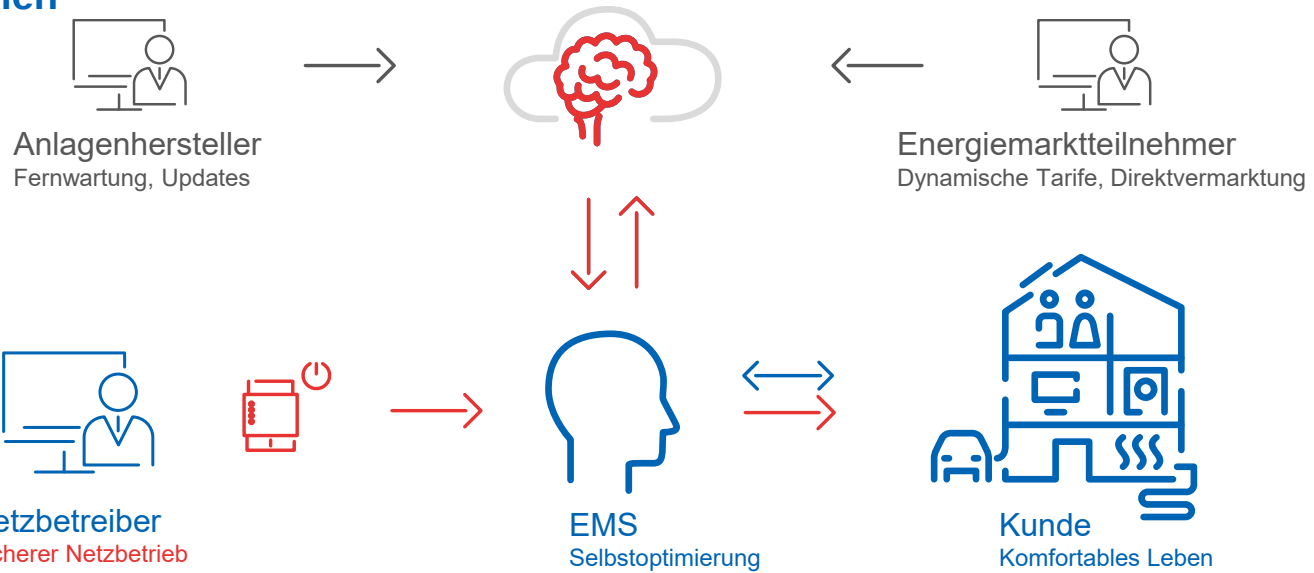
Das Energiemanagementsystem im Alltag

Das Energiemanagementsystem des Kunden „dient mehreren Herren“



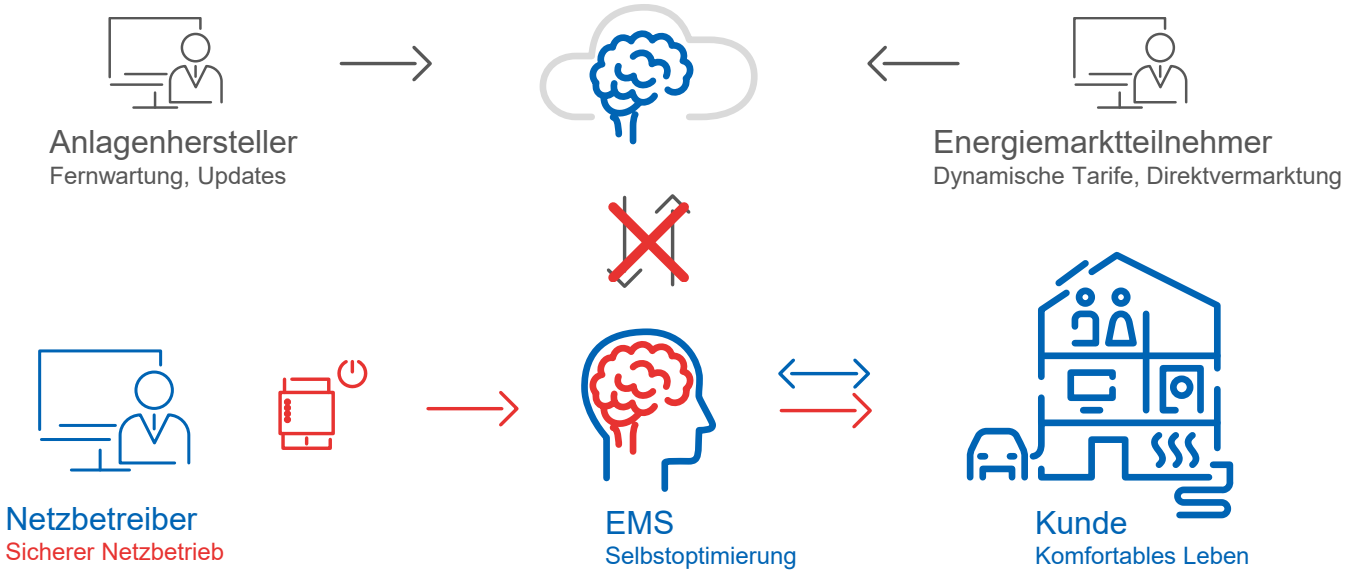
Das Energiemanagementsystem im Alltag

Die Auslagerung von Funktionen in die Cloud soll den (Normal-)Betrieb vereinfachen

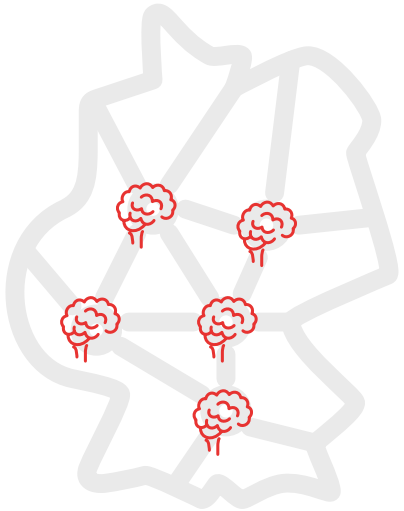


Das Energiemanagementsystem im Alltag

Die Notfallfunktion für den Netzbetreiber muss auf jeden Fall lokal erhalten bleiben



Zum Mitnehmen



Im Normalbetrieb können Energiemarktteilnehmer und Andere ungestört mit den Anlagen des Kunden kommunizieren. Im Fall einer Gefahrensituation greifen die Regeln des § 14a EnWG.

Die Auswahl des EMS und damit die Ausprägung als lokale oder cloudbasierte Lösung ist die alleinige Entscheidung des Kunden – solange die gesetzlichen Anforderungen erfüllt sind.

Im Ernstfall darf eine uneingeschränkte Verfügbarkeit von Clouddiensten nicht vorausgesetzt werden. Zur Erfüllung der gesetzlichen Vorgaben ist eine lokale Funktionalität notwendig.

Zum Nachlesen

VDE FNN

Steuerung über intelligente Messsysteme

Lastenhefte und Anwendungshinweise rund um das intelligente Messsystem

Technische Ausgestaltung zur Regulierung der Bundesnetzagentur

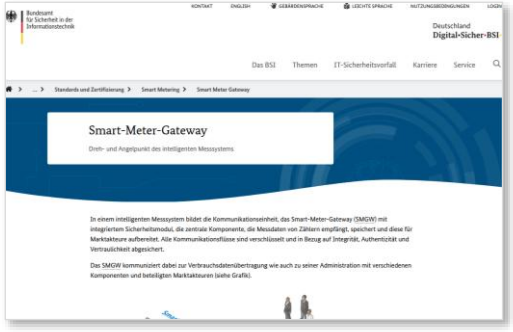
BNetzA

Regulierung zu § 14a EnWG, BK6-22-300

Technische Mindestanforderungen an die Schnittstelle vom Netz zum Kunden

Definition der netzorientierten Steuerung von Kundenanlagen

BSI



Technische Richtlinien zum intelligenten Messsystem

Cyber-Security-Anforderungen an Smart Meter Gateway und Steuerungseinrichtungen

Vielen Dank für Ihr Interesse!

VDE FNN – Gemeinsam zu einem digitalen, flexiblen und zuverlässigen Klimaschutznetz

Ihr Ansprechpartner

Frank Borchardt
Metering und Digitalisierung

Tel. +49 170 5763781
frank.borchardt@vde.com

Forum Netztechnik / Netzbetrieb im VDE (FNN)
Bismarckstraße 33 | D-10625 Berlin | Germany

Mitglied werden:
https://www.vde.com/de/fnn/vde-fnn-im-fokus/mitglied-werden

VDE FNN

Kompetenzzentrum
Energieeffizienz
durch Digitalisierung

Vielen Dank und bleiben Sie mit uns in Kontakt!

KEDi Newsletter

Weitere Informationen finden Sie unter **www.kedi-dena.de**

Mail:
katharina.staffa@dena.de
joerg.erdsack@dena.de

Ein Projekt der dena