CYBERsicher | EASY.CRA Tool zur Umsetzung des Cyber Resilience Act

IT-Sicherheit IN DER WIRTSCHAFT

NIS 2 im Fokusprojekt EASY.CRA

23.04.2026

ibi research | OTH Regensburg

Gefördert durch:

Bundesministerium für Wirtschaft und Energie

Mittelstand-Digital

aufgrund eines Beschlusses des Deutschen Bundestages

CYBERsicher | EASY.CRA Tool zur Umsetzung des Cyber Resilience Act

IT-Sicherheit IN DER WIRTSCHAFT

Übersicht über die Veranstaltung

- Was ist NIS 2?
- Wie „kritisch“ ist meine Organisation?
- Wozu verpflichtet das Gesetz, das NIS2 umsetzt?
- Wovon bin ich betroffen? Sektor? Kenngrößen?
- Ist die Lieferkette ein Problem?
- Was sind Meldepflichten? Und wo muss ich melden?
- Schulungen, Trainings und Maßnahmen?
- Einzelschritte, wie geht man diese?

Ihr Referent

Dr. Matthias Kampmann

ibi research an der Universität Regensburg GmbH

Kontakt

matthias.kampmann@ibi.de

Galgenbergstraße 25

93053 Regensburg

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

Mittelstand-Digital

NIS 2-Richtlinie EU 2022/2555 vom 14.12.2022

Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der EU

- Überprüfung des Vorläufers (EU) 2016/1148 hat Mängel ergeben.
- Neue Lagen, neue Bedrohungen.
- Bedeutung der Cybersicherheit im Zuge der Digitalisierung steigt stetig.
- Steigerung des Sicherheitsniveaus in der EU.
- Die Richtlinie muss umgesetzt werden (Unterschied zum „Act“ der direkt aus der EU wirkt): 6. Dezember 2025 integriert ins neue BSI-Gesetz.
- BSI nun zuständig für 29.500 neue „besonders wichtige“ (bwE) und wichtige (wE) Einrichtungen.

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

Zweck der NIS2-Richtlinie

Cyberattacken nehmen zu. NIS 2 soll EU-Sicherheitsniveau erhöhen

- 2025 Deutschland: 16. Stelle der meisten Cyberangriffe.
- 2024 betrafen über 80 % der 950 Ransomware-Angriffe KMU. Zahlungen nehmen ab!
- 48 Fälle (ransomware.live) in Dtl 2026.
- Tägl. 280.000 neue Schadsoftwarevarianten
- BSI: Handlungsbedarf bei Resilienz.*
- Cybercrime-Gruppen nehmen nach USA und UK Deutschland ins Visier.
- Software: 119 Schwachstellen tgl. (24 % mehr als im Berichtszeitraum zuvor).
- Zahlungen bei Datenleaks nehmen zu.
- Zunahme der Leakseiten.

* Quelle: https://medien.bsi.bund.de/lagebericht/de/index.html

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

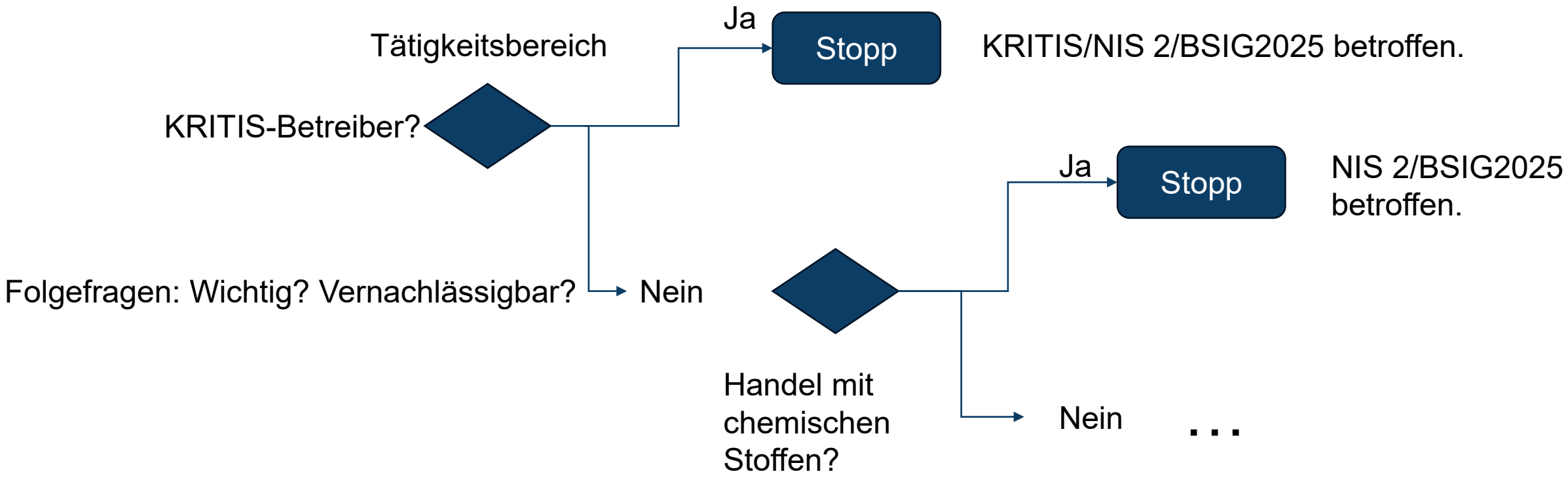
Bundesamt für Sicherheit in der Informationstechnik (BSI)

ist nun zuständig: Meldestelle.

- Erweiterung des Begriffs kritischer Infrastruktur.
- KRITIS wird Teilmenge.
- wE und bwE unterliegen besonderen Registrierungs- und Meldepflichten.
- Pflichten steigen mit Kritikalität.

- Herausforderung f. Unternehmen: Maßnahmen müssen umgesetzt werden.
- Unternehmen/Organisationen müssen ein angemessenes Risikomanagement und dazugehörige Maßnahmen umsetzen und dokumentieren.
- Verantwortung und Schulungspflicht bei Geschäftsführung.

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



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

Gesetzliche Pflichten aus NIS 2

Pflichten für Organisationen

Meldepflicht

Erweiterung der staatlichen Aufsicht durch Registrierungs-, Nachweis- und Meldepflichten sowie eines verbindlichen Informationsaustauschs.

Risikomanagement

Registrierungspflicht

Pflichten für die Geschäftsleitung

Umsetzung/ Überwachung

Haftung

Ausweitung der Sanktionsvorschriften mit neuen Bußgeldtatbeständen und erhöhten Bußgeldern.

Schulungspflicht

Dokumentationspflicht der Sicherheitsmaßnahmen, um die Umsetzung belegen zu können.

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

Wer hilft?

Auf dem Weg zur Compliance kann viel selbst unternommen werden.

Erste Hilfe:

BSI-Schnellcheck ist eine einfache Betroffenheitsprüfung.

https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Betroffenheitspruefung/nis-2-betroffenheitspruefung_node.html

Betroffenheitsprüfung eines Fokusprojekts der Transferstelle für Cybersicherheit.

Start - FitNIS2-Navigator

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

Betroffenheit: Die Sektoren

Besonders wichtig:

- Energie,
- Transport, Verkehr,
- Finanzen, Versicherungswesen, (Ausnahmen; Harmonisierung mit DORA)
- Gesundheitswesen,
- Trink-/Abwasser,
- Informationstechnik, Telko, Raumfahrt

Sonderfälle

- TLD, DNS, qTSP (qualified Trust Service Provider),
- TK-Anbieter.
- Kritische Anlagen,
- Zentralregierung.

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

Betroffenheit: Die Sektoren

Wichtig:

- Energie,
- Transport, Verkehr,
- Finanzen, Versicherungswesen,
- Chemie,
- Gesundheitswesen,
- Trink-/Abwasser,
- Verarbeitendes Gewerbe,
- Informationstechnik und Telko,
- digitale Dienste,
- Raumfahrt,
- Lebensmittel,
- Entsorgung,

Sonderfälle

- Vertrauensdienste

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

Betroffenheit und Kennzahlen

Empfehlung der EU-Kommission 2003/361/EG (KMU/KKU)

Wichtige Einrichtungen

- Mitarbeitende ≥ 50
- Jahresumsatz > 10 Mio. €
- Jahresbilanzsumme > 10 Mio. €

Besonders wichtige Einrichtungen

- Mitarbeitende ≥ 250
- Jahresumsatz > 50 Mio. €
- Jahresbilanzsumme > 43 Mio. €

Gilt für natürliche oder juristische Personen oder rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft.

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

Fragen und Antworten 1

Diese Fragen sind kein juristischer Rat/Beistand und können diesen in keiner Weise ersetzen. Daher sollten Sie für eine wirklich relevante Aussage qualifizierte Kanzleien oder Fachanwälte konsultieren. An dieser Stelle bekommen Sie lediglich eine Orientierungshilfe. Wir hoffen, dass diese Ihnen dennoch weiterhilft.

- **Frage:** Ein Konzern hat mehrere selbstständige Firmen:
  Firma 1: Die GmbH XYZ ist Händler und überschreitet hinsichtlich ihres Gesamtumsatzes die Schwellwerte der NIS2. Der überwiegende Umsatzanteil wird in mit einem Produkt realisiert. In einem kleinen, scheinbar unerheblichen Umfang handelt das Unternehmen im kritischen Sektor. Betrachtet man die Sektoren der NIS2, so macht die nur einen kleinen Teil des Gesamtumsatzes aus, der aufsummiert zudem kleiner 10 Mio. ist, den in Anlage 1 + 2 NIS2 Umsetzungsgesetz genannten Einrichtungsarten zugeordnet werden.
  Firma 2: Eins der Tochterunternehmen ist Betreiber eines Verkaufstellennetzes und liegt unterhalb der Schwellwerte von KRITIS. Nun betreibt das Unternehmen allerdings auch zwei KRITIS-relevante Einrichtungen, die in Anlage 1 und 2 der NIS2 aufgeführt sind. Hiermit werden im Jahr keine 10 Mio. Umsatz erzielt, und das Unternehmen beschäftigt auch < 50 Mitarbeiter.

Fragen und Antworten 2

***Frage:* Müssen nur die Umsätze/Mitarbeiterzahlen in den relevanten Bereichen gewertet werden, oder pauschal alle Umsätze des gesamten Unternehmens, auch die, die nicht im relevanten Bereich vorliegen?**

- **Antwort:** Es kommt auf den Gesamtumsatz des Unternehmens an, nicht, wieviel Umsatz in bestimmten Bereichen gemacht wird. Prüfungsfolge:
  - Unternehmen in der Anlage 1 oder 2 tätig? Und:
  - Schwellenwerte des § 28 Abs. 1 bzw. Abs. 2 BSIG überschritten (einzeln)?

  Falls nein: müssen die Zahlen eventuell nach Abs.4 zusammengezählt werden?
- Damit dürfte das Beispiel ein NIS-2-Unternehmen sein.

Fragen und Antworten 3

- **Frage:** Zur Grenze 50 Mitarbeiter (Folie 11): Werden alle "Köpfe" gezählt oder gibt es Personen, die nicht mitgerechnet werden müssen (z.B. Auszubildende, Minijobber, Mitarbeiter in Elternzeit etc.)?
- **Antwort:** Dazu verweisen NIS2 und BSIG auf die Empfehlung 2003/361/EG (https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32003H0361). S. hier Punkt 12: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-FAQ/NIS-2-FAQ-allgemein/FAQ-zu-NIS-2_node.html. §28 Abs. 4 BSIG: „Bei der Bestimmung von Mitarbeiteranzahl, Jahresumsatz und Jahresbilanzsumme nach den Absätzen 1 und 2 ist außer für rechtlich unselbstständige Organisationseinheiten einer Gebietskörperschaft die Empfehlung der Kommission (2003/361/EG) mit Ausnahme von Artikel 3 Absatz 4 des Anhangs anzuwenden. Die Daten von Partner- oder verbundenen Unternehmen im Sinne der Empfehlung der Kommission (2003/361/EG) sind nicht hinzuzurechnen, wenn das Unternehmen unter Berücksichtigung der rechtlichen, wirtschaftlichen und tatsächlichen Umstände mit Blick auf die Beschaffenheit und den Betrieb der informationstechnischen Systeme, Komponenten und Prozesse unabhängig von seinen Partner- oder verbundenen Unternehmen ist.“ (https://www.gesetze-im-internet.de/bsig_2025/__28.html)

NIS 2/BSIG* und die Lieferkette

Betroffenheit von wE und bwE

- Schutz vor Cyberangriffen!
- Vermeidung von Schadsoftware, kompromittierter Hardware,
- Datenschutz,
- Produkt-/Anbietervertrauen
- **Todos**: SLAs, Zulieferer auf Standards verpflichten; sicheres Beschaffungsmanagement.

Quelle: https://www.gesetze-im-internet.de/bsig_2025/

Quelle: BSI

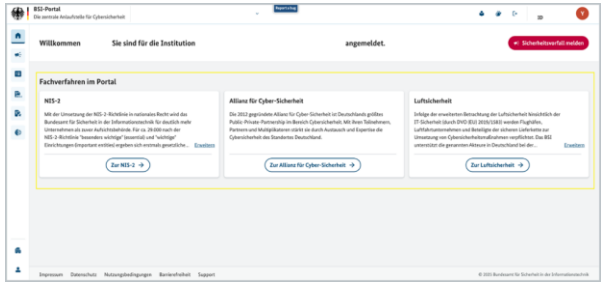
Gefördert durch: Bundesministerium für Wirtschaft und Energie aufgrund eines Beschlusses des Deutschen Bundestages
Mittelstand-Digital

Das Meldeportal des BSI

Wie funktionierts?

portal.bsi.bund.de:

Verwaltung, Registrierung und Meldung laufen über dieses Portal. Daten werden in ELSTER geändert, wenn fehlerhaft. Hier legen Sie Ihre Organisation



an und erstellen und bearbeiten Ihre Profile.

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

Meldepflicht bei Betroffenheit

Erstmeldung, Einstufung, Folgemeldung, Abschluss

- Sicherheitsvorfälle müssen unverzüglich nach Kenntniserlangung gemeldet werden.
- Die Erstmeldung eines Vorfalls muss innerhalb von *24 Stunden nach Kenntniserlangung* erfolgen. Zugang über die Hauptseite des BSI-Portals (rote Schaltfläche „Sicherheitsvorfall melden“). Einstufung: „erheblicher Sicherheitsvorfall“, „Sicherheitsvorfall“, „Beinahevorfall“ (?) unter Angabe des Meldegrunds.
- Folgemeldung: 72 Stunden nach Kenntniserlangung
- Abschlussmeldung: spätestens nach einem Monat nach Meldung.

BSI - Anleitung zur Meldung im BSI-Portal

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

Schulungspflichten (Kap. 2, §30, §38)

Verpflichtende Schulungen für die Geschäftsleitung (1x Jahr) und Mitarbeitende (1 x Jahr), Tech-Staff (fortlaufend, bei neuen Systemen)

- Die GF muss an Cybersicherheitsschulungen teilnehmen.
- GF muss Risiken der IT-Sicherheit kennen und bewerten können.
- GF muss Risikomanagement verstehen und praktizieren können.
- GF muss Aufsicht und Kontrollfunktionen wahrnehmen, das Sicherheitsniveau einschätzen und Entscheidungen über Maßnahmen fällen können.
- MA: Awareness (Phishing, Social Engineering etc.), rollenbasierte Schulungen (Admin, Entwickler (Sec by Design) oder Einkauf (Lieferkette); Meldung, Notfall

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

Fragen und Antworten

- **Frage**: Wenn aus einem Förderprojekt eine Orientierungsveranstaltung (kostenfrei, weil gefördert) angeboten wird, kann das als Schulung für GF gewertet werden? Oder muss ein zertifizierter Träger diese Schulungen ausrichten und ein Zertifikat ausstellen?
- **Antwort:** Die Teilnahme an Webinaren kann als Wissenszuwachs betrachtet und somit im Kontext von NIS2 dokumentiert werden. Ob damit die Verhältnismäßigkeit der Maßnahmen zur Adressierung der NIS2-Pflichten gegeben ist, wird in Frage gestellt. Die Pflichten hängen nämlich von Ihrem je individuell zu betrachtenden Unternehmen ab. Selbst wenn die Geschäftsführung durch wiederholte Teilnahme an Infoveranstaltungen belegen kann, dass sie sich regelmäßig informiert, um auf dem aktuellen Stand zu bleiben, kann bezweifelt werden, dass das im Kontext von NIS2 ausreicht. Es ist unternehmensindividuell zu bewerten, wahrscheinlich aber zu bezweifeln, dass unsere Veranstaltungen ausreichen. Zur Beantwortung der Frage empfiehlt es sich, qualifizierten juristischen Rat einzuholen.

Sofortmaßnahmen und weiteres Vorgehen

Was kann umgehend in die Wege geleitet werden, wenn das Unternehmen betroffen ist (oder nicht)?

- Je nach Anzahl MA Aufstellung eines Sicherheitsteams. Achtung: potenzielle Interessenkonflikte berücksichtigen (z. B. von DSB und ISB).
- Ermittlung des Ist-Zustands der Informationssicherheit mittels Assessment (DIN-SPEC 27076, „CyberRisikoCheck“; BSI - CyberRisikoCheck nach DIN SPEC 27076).
- Ergebniskontrolle: Identifikation und Klassifikation der Mängel. Beseitigung. Neue Prüfung.
- Wichtige Maßnahmen: Risikomanagement, Assetmanagement: Was ist mein „Tafelsilber“? Was kostet mich der Ausfall?
- Vorbereitung für den Ausbau Richtung Informationssicherheitsmanagement (ISO-27000-Familie, BSI-GS 200 nach ISO, CISIS12).

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

Tag für Tag

Unabhängig, ob das Unternehmen betroffen ist, sollte die IT-Sicherheit immer auf der Tagesordnung stehen

- Habe ich Backups? Mindestens 3-2-1-0 (drei Kopien, zwei Medien an zwei Orten, eine offline, null Fehlertoleranz). Check: Regelmäßige Übungen zum Wiedereinspielen der Daten einplanen.
- Habe ich eine Passwortrichtlinie? Einführung von Passwortmanagern.
- Zugänge: Absicherung mit zweitem Faktor.
- Tools: Firewall, Virenschutz, ggf. Endpoint Detection and Response
- Datensparsamkeit: Nicht alles speichern, was man speichern kann.
- Habe ich ein Verschlüsselungskonzept (Zertifikatsmanagement!)?
- Patchen und Software aktuell halten.
- Sicheres Netzwerken: VPN, keine offenen Netzzugänge (WLAN oder freie LAN-Ports) anbieten.
- Regelmäßige Schulungen und Awarenesstrainings.

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

Vorbereitungen zusammengefasst

Auf dem Weg zur Optimierung der Organisation in drei Schritten

Leitlinie vorhanden?

- Was ist für die Organisation gewollt?
- Sind Geschäftsführung und wichtige Beteiligte (Personal-/Betriebsrat etc.) in Abstimmung miteinander und haben sich verpflichtet?
- Sind Mitarbeitende informiert, kennen die Leitlinie und wissen, wo sie diese finden?

Assetmanangement vorhanden?

- Was „besitzt“ die Organisation?
- Alle relevanten technischen Geräte und Softwaren sind erfasst.
- Wir wissen um die Risikogrößen, wenn wir auf die Ressourcen nicht zugreifen können.

Maßnahmen geplant?

- Welche Maßnahmen kommen auf uns zu?
- Wir schulen die Mitarbeitenden.
- Wir kontrollieren die Fortschritte.
- Wir kennen die Meldeverfahren.

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

CYBERsicher | EASY.CRA Tool zur Umsetzung des Cyber Resilience Act

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