Mittelstand-Digital
Zentrum
Chemnitz

NACHGELESEN

NIS-2-Richtlinie – was Unternehmen wissen müssen

MIKE WÄSCHE

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages

Die neue NIS-2-Richtlinie der EU, kurz für Netzwerk- und Informationssicherheit, bringt bedeutende Veränderungen für Unternehmen in Europa mit sich. Diese Richtlinie zielt darauf ab, ein hohes Maß an Cybersicherheit in kritischen Infrastrukturen zu gewährleisten, indem sie Standards und Zusammenarbeit innerhalb der EU-Mitgliedsstaaten fördert. In diesem Nachgelesen erfahren Sie

- was NIS-2 konkret bedeutet,
- welche Unternehmen von der NIS-2-Richtlinie betroffen sind,
- mit welchen Themen sich Unternehmen auseinandersetzen müssen und
- was Unternehmen tun können, um der Richtlinie zu entsprechen.

Impressum

HERAUSGEBER
Mittelstand-Digital Zentrum Chemnitz
c/o TU Chemnitz
Erfenschlager Str. 73, 09125 Chemnitz
Tel: 0371 531 19935 Fax: 0371 531 819935
info@digitalzentrum-chemnitz.de
www.digitalzentrum-chemnitz.de

REDAKTION Anikó Lessi

GESTALTUNG
PUNKT191 – Marketing und Design
www.punkt191.de

BILDNACHWEIS TITEL
titima037 - Freepik.com

VERÖFFENTLICHUNG April 2024

© Sarayut - Freepik.com

Was ist NIS-2?

NIS ist die Abkürzung für Netzwerk- und Informationssicherheit. Unter NIS-2 wird die neue Richtlinie für die Cybersicherheit von kritischen Infrastrukturen in der Europäischen Union (EU) zusammengefasst (The Network and Information Security (NIS) Directive)[1]. Diese beinhaltet Maßnahmen zur Schaffung eines hohen gemeinsamen Cybersicherheitsniveaus mit dem Ziel, dass innerhalb der EU alle Mitgliedsstaaten enger zusammenarbeiten und die gleichen Standards der Cybersicherheit abbilden. Unternehmen und Organisationen festgelegter Wirtschaftssektoren bzw. Größenklassen sind dadurch aufgefordert, sich mit Themen wie Cyber-Risikomanagement sowie Kontrolle und Überwachung bzw. den Umgang mit Zwischenfällen bei gleichzeitiger Sicherstellung des Geschäftsbetriebs zu befassen. Durch die Richtlinie sollen die dazu notwendigen Maßnahmen initiiert und der gleiche Standard in der Cybersicherheit angewendet werden, die Mitgliedstaaten der EU sollen enger zusammenarbeiten. So soll u.a. ein einheitliches Meldesystem und -verfahren für Sicherheitsvorfälle etabliert werden, um damit schneller zu reagieren und einheitlich bei der Behebung zu agieren.

Bisher gab es noch keine einheitliche EU-Richtlinie bzw. die bisherigen Richtlinien wurden sehr unterschiedlich umgesetzt. Dadurch ist das Cybersicherheitsniveau in den Mitgliedstaaten sehr unterschiedlich. Die neue Richtlinie betrifft ca. 15-mal so viele Unternehmen wie bisher und somit ca. 30.000 allein in Deutschland.[2] Bisher lag der Fokus vor allem auf der Reaktion bei Sicherheitsvorfällen. Zukünftig steht die Sensibilisierung der Mitarbeitenden in den Unternehmen im Mittelpunkt, um eventuelle Vorfälle schneller zu erkennen.

Im deutschen Recht findet die Umsetzung über das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) statt. Mit Wirkung zum 18. Oktober 2024 wird das Gesetz offiziell in Krafttreten. Aktuell liegt der vierte Referentenentwurf zur weiteren Abstimmung vor. Aufgrund des Widerstandes verschiedener Sektoren könnte es aber zu Verzögerungen kommen.

Welche Unternehmen sind von der neuen Richtlinie betroffen?

Die Kriterien, welche Unternehmen von der NIS-2-Richtlinie betroffen sind, beziehen sich sowohl auf die Unternehmensgröße als auch den Sektor, in dem das Unternehmen wirtschaftlich tätig ist. Demnach wird die Richtlinie im Wesentlichen für Unternehmen mit mindestens 50 Mitarbeitenden und einem Jahresumsatz von über 10 Mio. Euro angewendet, wenn diese auch einem wesentlichen bzw. wichtigen Sektor zugeordnet sind. Hierzu zählen insbesondere die in Abbildung 1 dargestellten besonders wichtigen Bereiche.

Abbildung 1: besonders wichtige Einrichtungen entsprechend der NIS-2-Richtlinie

Hierbei wird deutlich, dass insbesondere elementare Versorgungsbereiche (Schlüsselbereiche) wie z. B. die Energie- und Wasserversorgung, der Transportsektor, das Finanz- und Bankwesen, die Gesundheitswirtschaft bzw. die öffentliche Verwaltung eingeordnet sind und somit ein hohes Maß an hoher Kritikalität darstellen.

Daneben sind einige darüber hinaus gehende wichtige Bereiche definiert. Die Zuordnung erfolgt nach der Unterscheidung in wesentliche sowie wichtige Sektoren für das öffentliche Leben und sind in Abbildung 2 dargestellt.

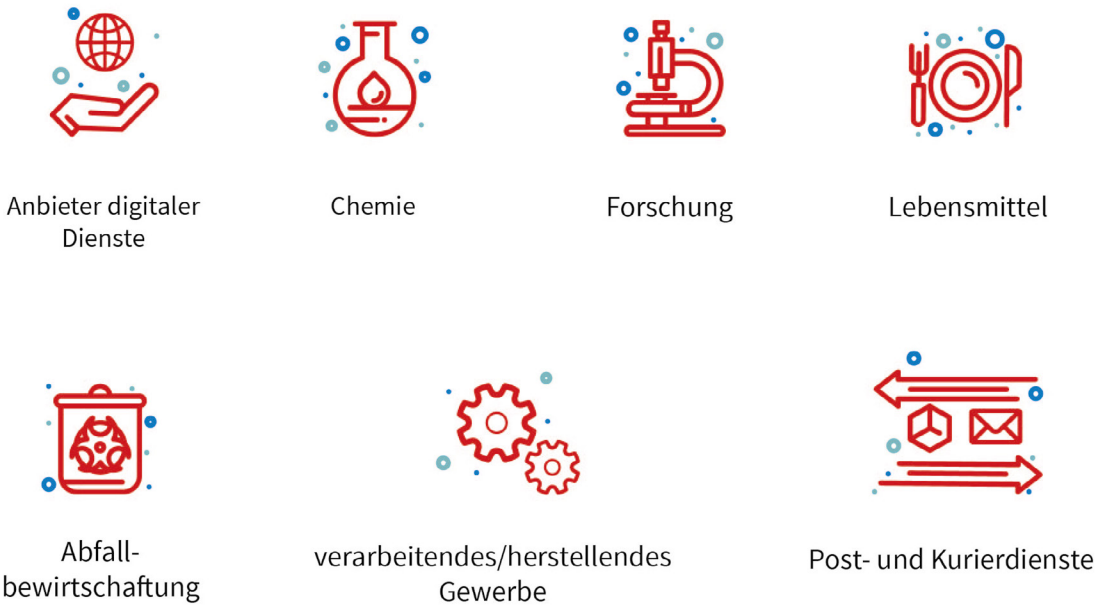

Abbildung 2: wichtige Einrichtungen entsprechend der NIS-2-Richtlinie

Dieser Bereich umfasst sonstige kritische Einrichtungen wie z. B. Hersteller von Waren, das verarbeitende Gewerbe, Kurierdienste oder Anbieter von digitalen Diensten. Die Einordnung in die einzelnen Bereiche basiert auf der Statistischen Systematik der Wirtschaftszweige in der Europäischen Gemeinschaft.[3]

Neben dieser sektorspezifischen Eingrenzung existieren Ausnahmen, in denen z. B. aktuell keine Größenbeschränkungen gelten. Davon betroffen sind die digitalen Infrastrukturen (z. B. Rechenzentren, Online-Suchmaschinen, Marktplätze) und die öffentliche Verwaltung. Durch die Erbringung von Dienstleistungen für Unternehmen der wichtigen Einrichtungen entsprechend der NIS-2-Richtlinie, fallen auch die Dienstleister in den Anwendungsbereich.

Mit welchen Themen müssen sich Unternehmen beschäftigen?

Der Gesetzgeber sieht vor, dass die Unternehmen selbstständig zu prüfen haben, ob sie durch die Richtlinie aktiv werden und sich ggf. melden müssen. Neben einer Kontrolle der in der Richtlinie aufgeführten Sektoren bieten sich auch Selbstchecks zur Anwendbarkeit im Unternehmen an.[4] Unternehmen, die direkt von der NIS-2-Richtlinie betroffen sind, sollten sich anschließend über die geltenden Anforderungen und ggf. über mögliche Strafen informieren. Dazu existieren zahlreiche Angebote z. B. durch die Mittelstand-Digital Zentren (https://www.mittelstand-digital.de), von der Transferstelle Cybersicherheit im Mittelstand (https://transferstelle-cybersicherheit.de) sowie spezialisierten Beratungseinrichtungen. Hierdurch stehen zunächst u. a. Checklisten zur Ermittlung der Anwendbarkeit im Unternehmen, allgemeine Informationen zum Thema NIS-2 und begleitende Schulungen für unterschiedliche Zielgruppen wie z. B. Management, Administratoren oder Mitarbeitende zur Verfügung. Eine gute Orientierung bieten auch aktuelle IT-Sicherheitsstandards wie

- ISO27.00X[5],
- BSI-Standard 200-1 bis 200-4 (IT-Grundschutz)[6] sowie
- weitere Branchenstandards[7].

Neben diesem Grundverständnis sind Unternehmen aufgefordert, sich mit weiteren Themen rund um die IT-Sicherheit zu beschäftigen. Diese beinhalten verschiedene Schwerpunkte nach dem Allgefahrenansatz (all hazards approach) und umfassen die Punkte

- Vorfallmanagement (Incident Management),
- Business Continuity Management,
- Lieferkettenmanagement (Supply Chain Management),
- Training in Bezug auf „Cyber Security Hygiene“,
- Kryptographie und Authentifizierung sowie
- physische Gefahren.

Unter einem **Vorfallmanagement** wird die Bereitstellung von Prozessen, Werkzeugen und das Konzept für eine schnelle Störungsbehebung verstanden. Ziel ist hierbei die Beschreibung und Gestaltung von Handlungsanweisungen bei einem Vorfall. Zur Sicherstellung der Fortführung kritischer Geschäftsprozesse existiert darüber hinaus das Business Continuity Management. Ausgehend von der Fragestellung „Es gab einen Vorfall – wie geht es nun weiter?“ fokussieren die hierbei beschriebenen Maßnahmen auf die schnelle Wiederaufnahme des Tagesgeschäfts.

Beim Thema **Supply Chain Management** werden IT-Sicherheitsgesichtspunkte vom Zulieferer bis zum Kunden ganzheitlich betrachtet. Dies beinhaltet Datenaustauschmechanismen, ebenso Zertifizierungen sowie organisatorische Aspekte der IT-Sicherheit bei Dritten. Ziel ist es, entsprechende Lieferketten stabil aufrecht zu erhalten und gegenüber Vorfällen in dieser Kette gewappnet zu sein.

Im Bereich **Cyber Security Hygiene** werden organisatorische Maßnahmen zur Steigerung der IT-Sicherheit zusammengefasst. So stehen hier u. a. Themen zur Schärfung des Bewusstseins für Cyberbedrohungen, Phishing oder Social-Engineering im Mittelpunkt. Ziel ist die Sensibilisierung von Mitarbeitenden, um potenzielle Gefahren zu erkennen. Weiterhin beinhaltet dieser Bereich das Management von Passwörtern, Zugriffen, Updates und Netzwerken sowie das Thema der Datensicherung.

Der Schwerpunkt **Kryptographie** und Authentifizierung sieht den Einsatz von Verschlüsselung beim Versand von sensiblen Daten vor. Entsprechende Möglichkeiten sollten im Unternehmen bekannt sein und angewendet werden. Darüber hinaus ist die Anwendung von starken Passwörtern durch den Einsatz von Multi-Faktor-Authentifizierung zu unterstützen. Hierfür bieten sich neben SMS , separater E-Mail oder biometrischen Daten auch hardwarebasierte Lösungen (bspw. Chipkarten, Smartcards oder YubiKey) an.

Als letzter Teil des Allgefahrenansatzes ist der Schutz vor **physischen Gefahren** wie z. B. Feuer, Wasser, Sturm usw. zusammengefasst. Entsprechende Risiken sind zu erfassen und der Umgang zu regeln.

Ein weiteres Thema, mit dem sich Unternehmen auseinandersetzen sollten, ist die Pflicht, erhebliche Sicherheitsvorfälle zu melden. Diese betreffen schwerwiegende Betriebsstörungen der Dienste oder verursachte bzw. zu erwartende finanzielle Verluste. Folgenden Regelungen sind in der Richtlinie festgelegt:

- innerhalb von 24 Stunden – Meldung einer Frühwarnung bei einem Verdacht inklusive einer kurzen Darstellung der Art des Verdachtsfalls und möglicher Auswirkungen auf das Unternehmen
- innerhalb von 72 Stunden – Meldung der Bestätigung der Frühwarnung mit aktualisierter Darstellung und einer ersten Bewertung des Schweregrades
- innerhalb von 1 Monat – umfassende Beschreibung des Vorfalls, des Schweregrades und der Art der Bedrohung sowie Darstellung der möglichen Ursache und der ergriffenen Maßnahmen

Welche Maßnahmen sollten Unternehmen ergreifen?

Ist das Unternehmen mit der NIS-2-Richtlinie direkt konfrontiert, sind zwei wesentliche Punkte zu realisieren. Zunächst gilt es, die **Erarbeitung einer Sicherheitsleitlinie im Unternehmen voranzubringen**. Dazu ist es wichtig, dass sich die Geschäftsführung zur Umsetzung der Informationssicherheit verpflichtet. Sie sorgt dafür, dass wesentliche Prozesse und die vorhandene Infrastruktur zunächst dokumentiert werden. Dies umfasst v. a. Übersichten des vorhandenen Netzwerks und der Rechner, zu den IT-unterstützten Geschäftsprozessen sowie den gewährten Zugangsberechtigungen. Dadurch sollen wesentliche Geschäftsprozesse sowie Informationen mit Bezug zur IT-Sicherheit erfasst werden. Auch die Definition von Zuständigkeiten gehört an dieser Stelle dazu.

Ziel ist es, mit dem Fokus einer kontinuierlichen Verbesserung durch die Sicherheitsleitlinie einzelne Prozesse zu lenken und zu überwachen. Aus diesen vorbereitenden Schritten lassen sich die Informationssicherheitsziele realistisch, praxisorientiert, überzeugend und verständlich festlegen. Diese Ziele lassen sich in

- strategische Leitaussagen,
- Erarbeitung konzeptioneller Vorgaben und
- Schaffung organisatorischer Rahmenbedingungen für ordnungsgemäßen und sicheren Umgang mit Informationen in den Geschäftsprozessen

zusammenfassen. Im Ergebnis steht die Sicherheitsleitlinie als zentrales Dokument zur Verfügung, das den Stellenwert der Informationssicherheit im Unternehmen verdeutlicht. Durch laufende prozessspezifische oder infrastrukturelle Anpassungen unterliegt diese Leitlinie ständigen Aktualisierungen. Abbildung 3 stellt wesentliche Schritte zur Erstellung einer Sicherheitsleitlinie als Kreislauf dar.

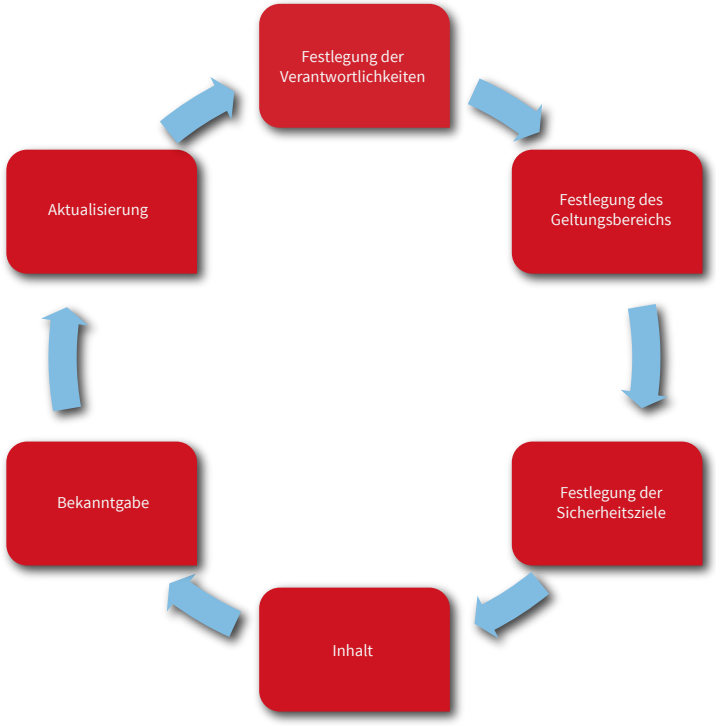

Abbildung 3: Schritte zur Erstellung einer Sicherheitsrichtlinie als Kreislauf

Der zweite wesentliche Punkt geeigneter Maßnahmen für Unternehmen im Rahmen der NIS-2-Richtlinie ist die **Feststellung des Schutzbedarfs**. Hierfür ist die vollständige Infrastruktur, das eingebundene Personal und die eingesetzte Technik für die Erfüllung des Geschäftsprozesses zu berücksichtigen. Dies beinhaltet auch die Darstellung der Definition von Schnittstellen sowie deren Abhängigkeiten. Voraussetzung ist deshalb die komplette Abbildung im festgelegten Geltungsbereich, so wie sie in den Schritten zur Erstellung der Sicherheitsleitlinie beschrieben sind.

Für die Feststellung des Schutzbedarfs sind die Aspekte Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität entsprechend des VIVA-Prinzips zu berücksichtigen. Aufbauend auf diesen Rahmenbedingungen lassen sich folgende wesentliche Schritte zusammenfassen:

1. Ermittlung und Analyse von Gefahren in Bezug auf Informationssicherheit
2. Identifizierung von Schäden (Vertraulichkeit, Integrität und Verfügbarkeit)
3. Analyse und Bewertung möglicher Auswirkungen auf Geschäftstätigkeiten z. B. durch Sicherheitsvorfälle und -risiken

Die Ergebnisse sind entsprechend zu dokumentieren. Hier eignen sich v. a. Matrixdarstellungen wie in Tabelle 1, die unterschiedliche Schutzkategorien und die jeweilige Bewertung gegenüberstellt.

Man unterscheidet die Risikokategorien gering, mittel, hoch und sehr hoch. Bei geringer Risikokategorie ist das Sicherheitskonzept umgesetzt. Dabei erfolgt eine laufende Beobachtung der Risiken und des damit einhergehenden Gefährdungspotenzials. In der mittleren Risikokategorie werden die im Konzept vorgesehenen Sicherheitsmaßnahmen als nicht ausreichend eingeschätzt. Bei der hohen bzw. sehr hohen Risikokategorie existiert kein ausreichender Schutz vor Gefährdungen.

Tabelle 1: Risikodarstellung in Matrixform

Auswirkungen / Schadenshöhe					
	Existenzbedrohend	mittel	hoch	sehr hoch	sehr hoch
	beträchtlich	mittel	mittel	hoch	sehr hoch
	begrenzt	gering	gering	mittel	hoch
	vernachlässigbar	gering	gering	gering	gering
		selten	**mittel**	**häufig**	**sehr häufig**
		Eintrittswahrscheinlichkeit			

Aufbauend auf der Einschätzung der Risiken ist das weitere Vorgehen als Risikobehandlungsstrategie unternehmensindividuell festzulegen und entsprechend den geltenden Anforderungen der NIS-2-Richtlinie auszurichten[8].

Fazit

Die NIS-2-Richtlinie beinhaltet Maßnahmen zur Schaffung eines hohen gemeinsamen Cybersicherheitsniveaus mit dem Ziel, dass innerhalb der EU alle Mitgliedsstaaten enger zusammenarbeiten und die gleichen Standards der Cybersicherheit abbilden. Die darin enthaltenen Regelungen betreffen insbesondere elementare Versorgungsbereiche (Schlüsselbereiche) wie z. B. die Energie- und Wasserversorgung, der Transportsektor, das Finanz- und Bankwesen, die Gesundheitswirtschaft bzw. die öffentliche Verwaltung, die insgesamt ein hohes Maß an hoher Kritikalität darstellen. Daneben sind weitere wichtige Bereiche definiert, die in wesentliche sowie wichtige Sektoren für das öffentliche Leben unterschieden werden können.

Unternehmen dieser Bereiche sind aufgefordert, sich mit den einzelnen Bestandteilen der NIS-2-Richtline zu beschäftigen. Dies umfasst die Prüfung zur Anwendbarkeit der Richtlinie im Unternehmen inklusive möglicher Auswirkungen, der Erhöhung des Grundverständnisses zu Schwerpunkten nach dem Allgefahrenansatz sowie der Festlegung von Zuständigkeiten zur Meldung von erheblichen Sicherheitsvorfällen bei den beauftragten Einrichtungen. Als wesentliche Schritte zur Berücksichtigung der Anforderungen der NIS-2-Richtlinie sind für die Unternehmen die Erarbeitung einer Sicherheitsleitlinie sowie die Feststellung des Schutzbedarfs relevant.

Quellen und weiterführende Literatur

1 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates. (2022). Amtsblatt der Europäischen Union. https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555

2 IT-Sicherheitsgesetz und KRITIS-Regulierung – OpenKRITIS. (o. D.). Copyright 2021-2024 Paul Weissmann, Bonn. Abgerufen am 3. April 2024, von https://www.openkritis.de/it-sicherheitsgesetz/index.html

3 NACE Rev. 2 Statistische Systematik der Wirtschaftszweige in der europäischen Gemeinschaft. (2008). https://ec.europa.eu/eurostat/documents/3859598/5902453/KS-RA-07-015-DE.PDF

4 NIS2 Quick-Check. (o. D.). Abgerufen am 3. April 2024, von https://nis2-check.de/

5 Deutsches Institut für Normung: DIN EN ISO/IEC 27001 Informationssicherheit, Cybersicherheit und Datenschutz - Informationssicherheitsmanagementsysteme - Anforderungen (ISO/IEC 27001:2022); Deutsche Fassung EN ISO/IEC 27001:2023. (2023). https://www.din.de/de/mitwirken/normenausschuesse/nia/veroeffentlichungen/wdc-beuth:din21:370680635

6 BSI-Standards. (o. D.). Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/BSI-Standards/bsi-standards_node.html

7 Zertifizierung nach TISAX – Was ist das? (o. D.). DGQ Blog. https://blog.dgq.de/zertifizierung-nach-tisax-was-ist-das

8 BSI-Standard 200-3. (2017). In Risikoanalyse Auf der Basis von IT-Grundschutz. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_3.pdf?__blob=publicationFile&v=2

Autor

MIKE WÄSCHE ist Projektmanager bei der tti Technologietransfer und Innovationsförderung Magdeburg GmbH. Im Mittelstand-Digital Zentrum Chemnitz ist er im Bereich IT-Sicherheit tätig..
mike.waesche@digitalzentrum-chemnitz.de

Weitere Informationen

Das Mittelstand-Digital Zentrum Chemnitz gehört zu Mittelstand-Digital. Mit dem Mittelstand-Digital Netzwerk unterstützt das Bundesministerium für Wirtschaft und Klimaschutz die Digitalisierung in kleinen und mittleren Unternehmen und dem Handwerk.

WAS IST MITTELSTAND-DIGITAL?
Das Mittelstand-Digital Netzwerk bietet mit den Mittelstand-Digital Zentren, der Initiative IT-Sicherheit in der Wirtschaft und Digital Jetzt umfassende Unterstützung bei der Digitalisierung. Kleine und mittlere Unternehmen profitieren von konkreten Praxisbeispielen und passgenauen, anbieterneutralen Angeboten zur Qualifikation und IT-Sicherheit. Das Bundesministerium für Wirtschaft und Klimaschutz ermöglicht die kostenfreie Nutzung und stellt finanzielle Zuschüsse bereit. Weitere Informationen finden Sie unter www.mittelstand-digital.de.

Mittelstand-Digital
Zentrum
Chemnitz

Mittelstand-
Digital

Gefördert durch:

Bundesministerium
für Wirtschaft
und Klimaschutz

aufgrund eines Beschlusses
des Deutschen Bundestages