CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

IT-Sicherheit IN DER WIRTSCHAFT

NIS-2 – Übersicht zur neuen Richtlinie in der Cybersicherheit

Sophie Haack
Transferstelle Cybersicherheit im Mittelstand
c/o tti Technologietransfer und Innovationsförderung Magdeburg GmbH

Mittelstand-Digital

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

Projektpartner

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

Regionale Partner & Netzwerkpartner

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

CYBERsicher, aber wie?

Unternehmen präventiv schützen

Angriffe einfach erkennen

Auf Angriffe schnell reagieren

Unsere Leistungen

Informieren

Wir erhöhen Wissen.

- WebImpulse
- CYBERDialoge
- CYBERsicher Check

Qualifizieren

Wir bieten Schulungen.

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

Vernetzen

Mehrwert durch Vernetzung.

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

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

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

IT-Sicherheit IN DER WIRTSCHAFT

Was ist bisher bekannt über NIS-2?

Mittelstand-Digital

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

NIS-2

Was ist das überhaupt?

Quelle: https://de.fotolia.com/p/202289213

- NIS = Netzwerk und Informationssicherheit
  - europäischer Rahmen für Betreiber kritischer Infrastrukturen in Bezug auf Cybersicherheit
  - Offizieller Titel: RICHTLINIE (EU) 2022/2555 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie)
  - Umsetzung in nationales Recht: NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz – NIS2UmsuCG
- viele Veränderungen für die Regierungen

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

NIS-2

Was ist der Unterschied zur bisherigen Richtlinie?

- einheitlicher Rahmen innerhalb der EU
- mehr betroffene Unternehmen
  - ca. 30.000 in Deutschland (15-fache zu NIS-1) (Quelle: https://www.openkritis.de/it-sicherheitsgesetz/index.html)
- größerer Fokus auf Prävention und Detektion
  - Cyber Security Hygiene
  - Allgefahrenansatz

Pflicht	Betreiber kritischer Anlagen	Besonders wichtige Einrichtung	Wichtige Einrichtung
Geltungsbereich	Anlage(n)	Unternehmen	Unternehmen
Maßnahmen Risikomanagement §30	*	✓	✓
Höhere Maßstäbe für KRITIS §31 (1)	✓		
Besondere Maßnahmen SzA §31 (2)	✓		
Meldepflichten §32	*	✓	✓
Registrierung §33 §34	✓	✓	✓
Unterrichtungspflichten (Kunden) §35	*	✓	✓
Leitungsorgane §38	*	✓	✓
Nachweise §39	✓	tw. (§64)	tw. (§65)

Quelle: https://www.openkritis.de/it-sicherheitsgesetz/nis2-umsetzung-gesetz-cybersicherheit.html

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

NIS-2

Welche Unternehmen sind von der neuen Regelung betroffen?

Besonders wichtige Einrichtungen	wichtige Einrichtungen
• Energie • Verkehr • Bankwesen • Finanzmarktinfrastrukturen • Gesundheitswesen • Trinkwasser • Abwasser • Digitale Infrastruktur • Verwaltung von IKT-Diensten (B2B) • Öffentliche Verwaltung • Weltraum • *Anbieter öffentlicher TK-Netze und TK-Dienste*	• Post- und Kurierdienste • Abfallbewirtschaftung • Produktion, Herstellung und Handel mit chemischen Stoffen • Produktion, Verarbeitung und Vertrieb von Lebensmitteln • Verarbeitendes Gewerbe/Herstellung von Waren • Anbieter digitaler Dienste • Forschung • *Mittlere Unternehmen aus Besonders wichtige Einrichtung*

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

NIS-2: §28 (Besonders) wichtige Einrichtungen

Beispiel: Informationstechnik und Telekommunikation

Definition

(2) Als wichtige Einrichtungen gelten

1. Vertrauensdiensteanbieter
2. Anbieter öffentlich zugänglicher Telekommunikationsdienste oder Betreiber öffentlicher Telekommunikationsnetze, die
   a) weniger als 50 Beschäftigte haben und
   b) einen Jahresumsatz und eine Jahresbilanzsumme von jeweils 10 Millionen Euro oder weniger aufweisen.

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

Arten der Betreiber

- Betreiber von Internet Exchange Points
- DNS-Diensteanbieter (ausgenommen Root-Nameserver)
- TLD-Registry
- Anbieter Cloud-Computing, Rechenzentrumsdiensten, öffentlicher elektronischer Kommunikationsnetze & öffentlich zugänglicher elektronsicher Kommunikationsdienste
- Betreiber CDN
- Vertrauensdienste
- Managed Service Provider & Security Services Provider

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

NIS-2: § 16

Beispiel: Telekommunikation

(1) Zur Abwehr konkreter erheblicher Gefahren für die in Absatz 2 genannten Schutzgüter kann das Bundesamt anordnen, dass ein Anbieter von öffentlich zugänglichen Telekommunikationsdiensten im Sinne des Telekommunikationsgesetzes (Anbieter von öffentlich zugänglichen Telekommunikationsdiensten) mit mehr als 100 000 Kunden

1. die in § 169 Absatz 6 und 7 des Telekommunikationsgesetzes bezeichneten Maßnahmen trifft oder

2. technische Befehle zur Bereinigung von einem konkret benannten Schadprogramm an betroffene informationstechnische Systeme verteilt,

sofern und soweit der Anbieter von öffentlich zugänglichen Telekommunikationsdiensten dazu technisch in der Lage und es ihm wirtschaftlich zumutbar ist. Vor der Anordnung der Maßnahmen nach Satz 1 Nummer 1 oder 2 durch das Bundesamt ist Einvernehmen mit der Bundesnetzagentur herzustellen. Vor der Anordnung der Maßnahme nach Satz 1 Nummer 2 durch das Bundesamt ist zusätzlich Einvernehmen mit der oder dem Bundesbeauftragten für den Datenschutz und die Informationsfreiheit herzustellen. Die Daten, auf die mit der Maßnahme nach Satz 1 Nummer 2 zugegriffen werden soll, sind in der Anordnung zu benennen. § 8 Absatz 8 Satz 2 bis 8 gilt entsprechend. Widerspruch und Anfechtungsklage gegen die Anordnungen nach Satz 1 haben keine aufschiebende Wirkung.

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

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

NIS-2

Welche Unternehmen sind von der neuen Regelung betroffen?

- Unterscheidung in kleine, mittlere und große Unternehmen
- bestimmte Sektoren besitzen keine Größenbeschränkung

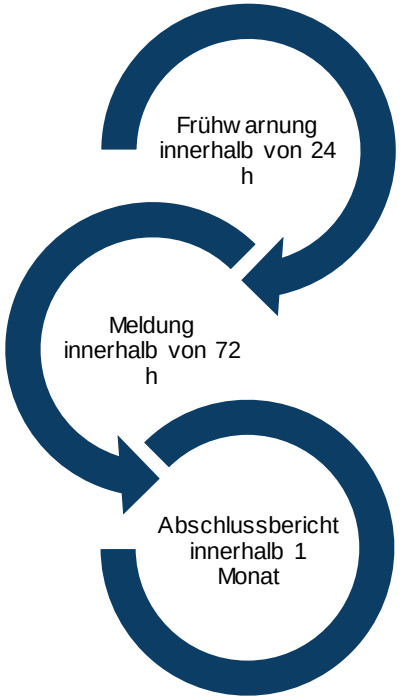
Kriterien	kleine Unternehmen	mittlere Unternehmen	große Unternehmen
Anzahl der Mitarbeiter	unter 49	50 bis 249	über 250
Umsatz	unter 10 Mio. EUR	10 bis 50 Mio. EUR	Über 50 Mio. EUR
Bilanz	unter 10 Mio. EUR	10 bis 43 Mio. EUR	Über 43 Mio. EUR
Zuordnung	nicht berücksichtigt	wichtige	Besonders wichtige

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

NIS-2

Was muss ich als Unternehmen tun?

- Überprüfung auf Betroffenheit nach NIS2UmsuCG und selbstständige Meldung
  - Beispiel: https://nis2-check.de/
- Orientierung an den aktuellen Standards
  - ISO2700X
  - BSI-Standards 200-1 bis 200-4
  - weitere Standards oder Alternativen je nach Branche möglich
- Einhaltung der Meldepflicht für erhebliche Sicherheitsvorfälle



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

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
  - Incident Management
  - Business Continuity Management
  - Supply Chain Management
  - Training in Bezug auf „Cyber Security Hygiene“
  - Kryptographie und Authentifizierung
  - Physische Gefahren

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

NIS-2

„Cyber Security Hygiene“ im Überblick

Schärfung des Bewusstseins für Cyberbedrohungen, Phishing oder Social-Engineering

Passwortänderungen und die Verwendung sicherer Passwörter

Zero-Trust-Grundsätze

Einschränkungen der Zugriffe auf Administratorebene

Software- und Hardware-Updates

Verwaltung neuer Installationen

Netzwerksegmentierung

Datensicherung

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

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

IT-Sicherheit IN DER WIRTSCHAFT

Wie können Sie sich als Unternehmen vorbereiten?

Mittelstand-Digital

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

NIS-2

Vorbereitende Schritte

Sicherheitsleitlinie vorhanden?

- Bekennen der Unternehmens-leitung zur Informations-sicherheit

Übersichten vorhanden?

- Infrastruktur
- Rechner
- Geschäftsprozesse
- Berechtigungen
- Zugang

Ergriffene Maßnahmen

- Firewall?
- Awareness Schulungen

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

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

IT-Sicherheit IN DER WIRTSCHAFT

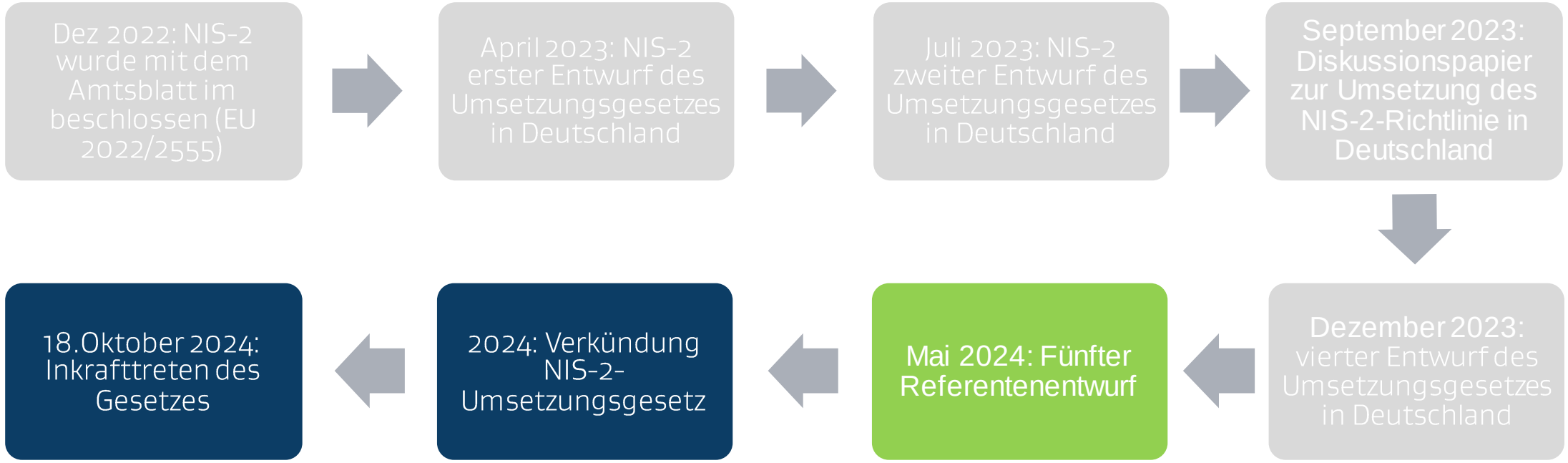
Wo stehen wir aktuell in der Beschließung des Gesetzes?

Mittelstand-Digital

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

NIS-2

Ausblick



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

Fragen?

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

Ihre Ansprechpartner

Sophie Haack

Sophie.haack@transferstelle-cybersicherheit.de

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

CYBERsicher Transferstelle. Cybersicherheit. Mittelstand.

IT-Sicherheit IN DER WIRTSCHAFT

VIELEN DANK

für Ihre Aufmerksamkeit!

Mittelstand-Digital

Gefördert durch:

Bundesministerium für Wirtschaft und Klimaschutz

aufgrund eines Beschlusses des Deutschen Bundestages