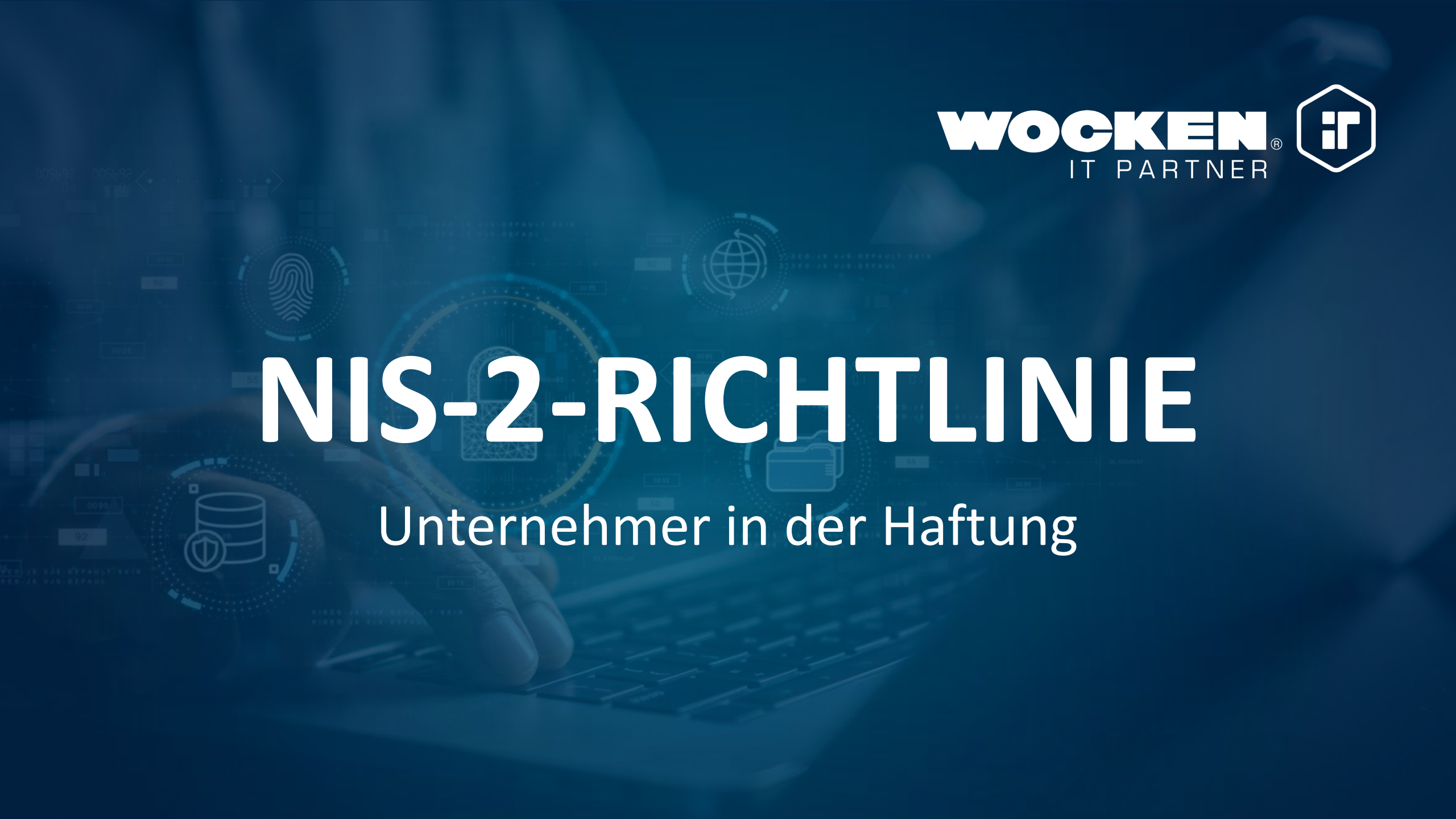

NIS-2-RICHTLINIE

Unternehmer in der Haftung

IT IN BESTFORM

WOCKEN IT PARTNER

2015
Gründung

>300
Kunden

60
Mitarbeiter

3
Standorte

NEUER NAME, NEUES LOGO

ABER UNSER VERSPRECHEN BLEIBT:

IT IN BESTFORM

Tobias Oortman

IT-Security-Beauftragter (TÜV)

venta IT GmbH

EU-RICHTLINIE NIS-2?

- **N**etwork and **I**nformation **S**ecurity
- **2**. Version
- Bereits in Kraft seit **16.01.2023**

UMSETZUNG IN DEUTSCHLAND?

- EU-Vorgabe: **17.10.2024 (!)**
- Durch sog. **NIS2UmsuCG**
- Voraussichtlich: **Q1/25**
- Aber **KEINE** Übergangsreglung vorgesehen

ZIEL DER NIS-2-RICHTLINIE?

*In dieser Richtlinie werden **Maßnahmen** festgelegt,*

*mit denen in der **gesamten Union***

*ein **hohes gemeinsames Cybersicherheitsniveau** sichergestellt werden soll,*

*um so das **Funktionieren des Binnenmarkts zu verbessern**.*

Kap. I, Art. 1, Abs. 1, Richtlinie (EU) 2022/2555 (NIS-2-Richtlinie)

WELCHE ORGANISATIONEN SIND BETROFFEN?

Unternehmen mit mehr als

- **50 Mitarbeiter**
- **10 Mio. Euro Umsatz** oder **Bilanz**
- Und Teil von **18 kritischen Sektoren** sind

  * Und alle bisherigen **KRITIS-Einrichtungen**

Also: **Sehr viele** (laut Bundesinnenministerium ca. 29.000)
und indirekt **noch viel, viel mehr** („Absicherung der Lieferketten“)

11 **SEKTOREN** MIT HOHER KRITIKALITÄT:

- Energie
- Transport
- Bankwesen
- Finanzmarkt-Infrastruktur
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- IKT-Dienstleister
- Öffentliche Verwaltung
- Weltraum

7 **SONSTIGE** KRITISCHE SEKTOREN:

- Post- & Kurierdienste
- Produktion & Vertrieb von Lebensmitteln
- Anbieter digitaler Dienste
- Abfall-wirtschaft
- Hersteller von Waren
- Forschung
- Produktion & Handel von chemischen Stoffen

DIESE ORGANISATIONEN MÜSSEN NUN NEUE

- **Registierungs-**
- **Nachweis-**
- Und **Meldepflichten** erfüllen

REGISTIERUNGSPFLICHTEN?

- **Selbstständige Betroffenheitsprüfung**
- Und bei der **zuständigen, nationalen Aufsichtsbehörde melden**
  - **Bundesamt für Sicherheit in der Informationstechnik (BSI)**

NACHWEISPFLICHTEN?

Über „Risikomanagementmaßnahmen für Cybersicherheit“
oder „Cybersicherheits-Risikomanagement“

= Informationssicherheits-Managementsystem (ISMS)

Dauerhaft

- **geeignete** und **verhältnismäßige**
- **technische** und **organisatorische Sicherheits-Maßnahmen**

planen, umsetzen **und dokumentieren!**

DAS BEDEUTET KONKRET?

Geeignet:

- „Stand der Technik“
- „nach int. Standards“

Verhältnismäßig:

- Eintrittswahrscheinlichkeit
- Organisationsgröße
- Möglicher Schaden

DAS BEDEUTET KONKRET? MINDESTENS:

- Risikoanalyse- & IT-Sicherheits-Konzepte
- Sicherheitsvorfall-Bewältigung
- Backup- & Krisen-Management
- Lieferkettensicherheit
- Sicherheit bei Erwerb, Entwicklung & Wartung von IT-Systemen
- Schwachstellen-Management
- Maßnahmenbewertung
- Cyberhygiene & Cybersicherheits-Schulungen
- Kryptografie/Verschlüsselung
- Personalsicherheit, Zugriffskontrolle & Asset-Management
- Multi-Faktor-Authentifizierung & sichere Kommunikation

MELDEPFLICHT!

Bei einem IT-Sicherheitsvorfall

24 h: erste Frühwarnung an die nationale Aufsichtsbehörde (= BSI)

72 h: detaillierte Bewertung

Und **nach einem Monat**:

vollständiger „**Fortschritts-**“ oder „**Abschlussbericht**“!

WER IST VERANTWORTLICH?

Die **Unternehmensleitung** muss…

- **Risikomanagementmaßnahmen** billigen
- ihre **Umsetzung** überwachen
- und ist für **Verstöße verantwortlich**
- an **Cybersicherheits-Schulungen** teilnehmen!
- (und **Mitarbeitern** regelmäßig entsprechende **Schulungen** anbieten)


SCHÜTZE
HAUS & DATEN
www.wocken-it.com/nis2
Download Whitepaper
Kostenloses Erstgespräch