Implementing NIS2 & CER
Where to start?

Martin „Krisenwolf“ Wölfel

Wer ist die AG KRITIS?

- 42 aktive Mitglieder
- unabhängig von Wirtschaft und Staat
- ausschließlich im Ehrenamt
- Alle beruflich im KRITIS-Umfeld unterwegs
- Gründung 2018 im Dunstkreis des Chaos Computer Club
- Seit August 2019 unabhängig vom CCC e.V.

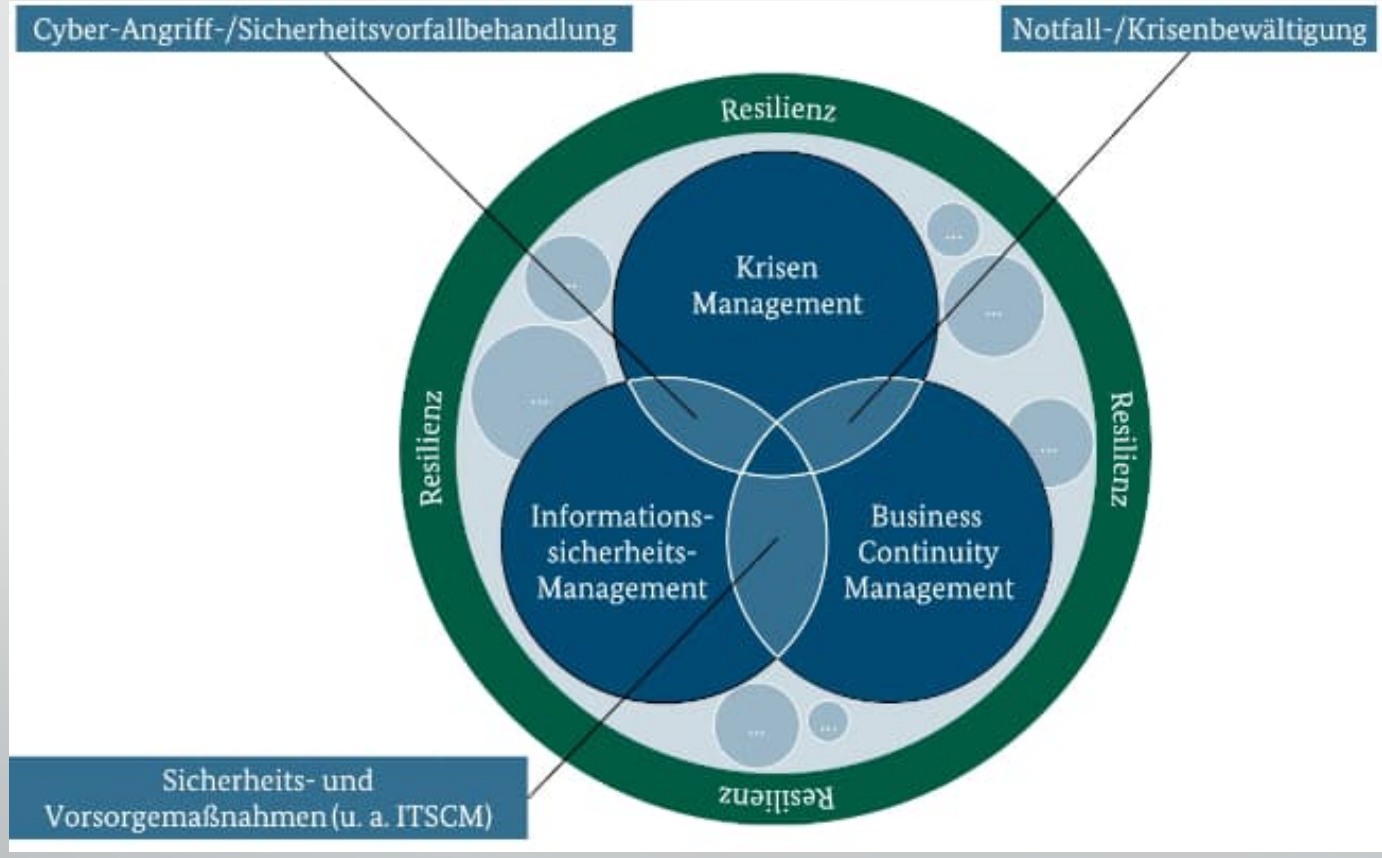
Selbstverständnis der AG KRITIS

“Wir vertreten das Interesse der BürgerInnen an Versorgungssicherheit sowie digitaler und physischer Resilienz Kritischer Infrastrukturen.”

Übersicht der Aktivitäten der letzten Jahre

- KRITIS im Sektor Staat und Verwaltung
- Umsetzung der europäischen Richtlinie NIS2 in Deutschland
- Regulierung zur physischen Sicherheit von KRITIS (KritisDachG)
- Funksysteme der Behörden und Organisationen mit Sicherheitsaufgaben
- Landesgesetze zum Katastrophenschutz
- Cyberhilfswerk-Konzept (Weiter-) Entwicklung

Rückblick Lehrveranstaltung ”IKT-Infrastruktursicherheit”, SoSe 2025



Q.: BSI 200-4

NIS2-Richtlinie

NIS2-Richtlinie der EU, 2022/2555

Ziel: *hohes, einheitliches Cybersicherheitsniveau in der EU zu erreichen, indem sie für wesentliche und wichtige Einrichtungen verbindliche Anforderungen an Risikomanagement und Lieferkettensicherheit festlegt sowie Regulierung EU-weit harmonisiert.*

- *„Network and Information Systems Directive 2“*
- Umsetzung in Deutschland über das NIS2UmsuCG, also die Überarbeitung des BSI-Gesetzes und weiterer

NIS2: Betroffenheit von der Richtlinie

Wann ist ein Unternehmen oder Einrichtung von NIS2 betroffen?

Die Betroffenheit nach NIS2 setzt sich zusammen aus der Tätigkeit in einem bestimmten Sektor und konkreten Schwellwerten.

Einrichtungsarten

- essential: „besonders wichtige“ Einrichtungen (bwE) [„wesentlich“]
- Important: „wichtige“ Einrichtungen (wE)

Sektorbezug

- Annex-I-Sektoren: in der Regel „essential“
- Annex-II-Sektoren: in der Regel „important“

Unternehmensgröße / Schwellwerte

- mittelgroße Unternehmen: ≥ 50 MA oder ≥ 10 Mio € Umsatz bzw. ≥ 13 Mio € Bilanzsumme
- große Unternehmen: ≥ 250 MA oder ≥ 50 Mio € Umsatz bzw. ≥ 43 Mio € Bilanzsumme

Managed Service Provider / Managed Security Service Provider

- typischerweise direkt erfasst (unabhängig davon, ob konzernintern oder extern)

NIS2: Sektoren der Richtlinien

Annex I: Sektoren hoher Kritikalität, „wesentliche“ Einrichtungen

- Energie (u. a. Elektrizität, Fernwärme/-kälte, Öl, Gas, Wasserstoff)
- Verkehr (Luft, Schiene, Wasser, Straße)
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur (z. B. IXP, DNS/TLD, Rechenzentren, Cloud, CDN, öffentliche elektronische Kommunikationsnetze/-dienste, Vertrauensdienste)
- Öffentliche Verwaltung
- Weltraum (bodenbasierte Infrastruktur)
- ICT-Service-Management (B2B), inkl. Managed Service Provider/Managed Security Service Provider

Annex II: weitere kritische Sektoren, typischerweise „wichtige“ Einrichtungen

- Post- und Kurierdienste
- Abfallwirtschaft
- Chemikalien (Herstellung und Handel/Vertrieb)
- Lebensmittel (Produktion, Verarbeitung, Verteilung)
- Verarbeitendes Gewerbe/Herstellung ausgewählter Branchen (u. a. Medizinprodukte, Computer/Elektronik, elektrische Ausrüstung, Maschinen, Kfz, sonstige Transportmittel)
- Digitale Anbieter (Online-Marktplätze, Suchmaschinen, soziale Netzwerke)
- Forschung

NIS2: Governance und Meldepflichten

NIS2 Governance

- Verpflichtung, „geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen [...] zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse [...] möglichst gering zu halten“. §30 (1) BSIG neu.

- Management genehmigt und überwacht das Sicherheits-Rahmenwerk
- Pflicht zu Schulung/Verantwortungsübernahme der obersten Leitung
- Registrierung: Erfassung bei der zuständigen Behörde
- Aufsicht strenger bei „besonders wichtigen“ Einrichtungen

NIS2 Meldungen bei Vorfällen (Art. 23)

- 24 h „Early Warning“
- 72 h „Incident Notification“
- ≤ 1 Monat Abschlussbericht (ggf. Zwischenberichte).
- Inhalte: was passiert ist, Auswirkungen, Maßnahmen, Indikatoren, ggf. grenzüberschreitender Bezug.

NIS2: zu ergreifende Maßnahmen betroffener Unternehmen

Maßnahmen gem. NIS2-Umsetzungsgesetz: §30 (2) – wortgleich nach Art. 21

„Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zu unmittelbaren Anbietern oder Diensteanbietern,
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von informationstechnischen Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen,
6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
7. grundlegende Schulungen und Sensibilisierungsmaßnahmen im Bereich der Sicherheit in der Informationstechnik,
8. Konzepte und Prozesse für den Einsatz von kryptographischen Verfahren,
9. Erstellung von Konzepten für die Sicherheit des Personals, die Zugriffskontrolle und für die Verwaltung von IKT-Systemen, -Produkten und -Prozessen,
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie gegebenenfalls gesicherte Notfallkommunikationssysteme innerhalb der Einrichtung.

CER-Richtline

CER-Richtlinie der EU, 2022/2557

Ziel: *Widerstandsfähigkeit kritischer Einrichtungen in der EU gegenüber allen relevanten Gefahren (All-Hazards-Ansatz) stärken, damit essenzielle Dienstleistungen auch bei Störungen, Naturereignissen, Sabotage oder Terrorbedrohungen verlässlich verfügbar bleiben.*

- „*Critical Entities Resilience*“
- Umsetzung in Deutschland über das KRITIS-Dachgesetz

CER: Sektoren und Betroffenheit von der Richtlinie

CER (EU-Richtlinie 2022/2557):

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheit
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Öffentliche Verwaltung
- Weltraum
- Lebensmittel (Produktion, Verarbeitung, Verteilung)

Faktoren für eine Betroffenheit

- **Sektorzugehörigkeit** – siehe links
- **Wesentliche Dienstleistungen**: Auswirkungen auf Sicherheit, Ordnung, Gesundheit,…
- **Nationale Benennung**: auf Basis einer nationalen Risikoanalyse
- **Europäische Bedeutung**: Aktivitäten in mehreren EU-Mitgliedsstaaten
- **Lieferkette**: nicht direkte Betroffenheit, aber Anforderungen werden über Lieferantenverträge an Schlüsselzulieferer und IT-Dienstleister durchgereicht.

CER: Pflichten betroffener Unternehmen

CER Kernpflichten

- Risikobewertung (nach Identifizierung): natürliche/menschengemachte Bedrohungen, Abhängigkeiten (auch sektorübergreifend).
- Resilienzmaßnahmen: Zutritt/Perimeter, baulich-technische Schutzmaßnahmen, Notstrom/Klima, Sabotage- und Brand-Schutz, Krisenmanagement und Übungen.
- Personal-/Lieferanten-Regeln: Zuverlässigkeit, Zugriff, Ersatz/Vertretung, vertragsgestützte Vorgaben.

CER Melde- und Kooperationspflichten

- Meldung erheblicher Störungen ohne schuldhaftes Zögern, in der Praxis innerhalb 24 h Erstmeldung; ≤ 1 Monat Abschlussbericht.
- SPOC/Koordination: Nationale Behörden koordinieren; Betreiber halten Kontaktwege vor, nehmen an Kooperation/Übungen teil.

Zusammenfassung

- CER adressiert Betreiber kritischer Einrichtungen.
- Lieferanten, wie auch MSP sind nur dann direkt betroffen, wenn sie selbst als Betreiber einer kritischen Anlage identifiziert wurden, darüber hinaus gelten Verpflichtungen als Lieferant.

CER: Pflichten für Lieferanten kritischer Einrichtungen

Risikotransparenz
- Risiken und Abhängigkeiten (Standorte, Energie, TK, Logistik, Subunternehmer) offenlegen und regelmäßig aktualisieren.

Business Continuity
- Funktionsfähiges BCM mit definierten RTO/RPO, Notbetriebs- und Wiederanlaufverfahren; regelmäßige Übungen und Nachweise.

Incident-Kommunikation
- 24/7 Erreichbarkeit, schnelle Meldung relevanter Vorfälle/Beeinträchtigungen, strukturierte Lage-Updates zur Unterstützung der Meldepflichten der kritischen Einrichtung.

Physische Sicherheit
- Zutritts- und Objektschutz, Schutz von Anlagen/Transporten, Insider- und Sabotageprävention, gesicherte Lagerung/Verteilung.

Betriebsstabilität
- Redundanzen, Ersatzteil-/Kapazitätsreserven, Mehrwegestrukturen (z. B. alternative Routen/Standorte), belastbare Wartungs- und Störungsprozesse.

Lieferkettensteuerung
- Verpflichtende Durchreichung gleichwertiger Anforderungen an Subunternehmer; Transparenz über eingesetzte Unterauftragnehmer und wesentliche Änderungen.

Teilnahme an Übungen
- Mitwirkung an gemeinsamen Notfall-/Krisenübungen und Tests mit der kritischen Einrichtung.

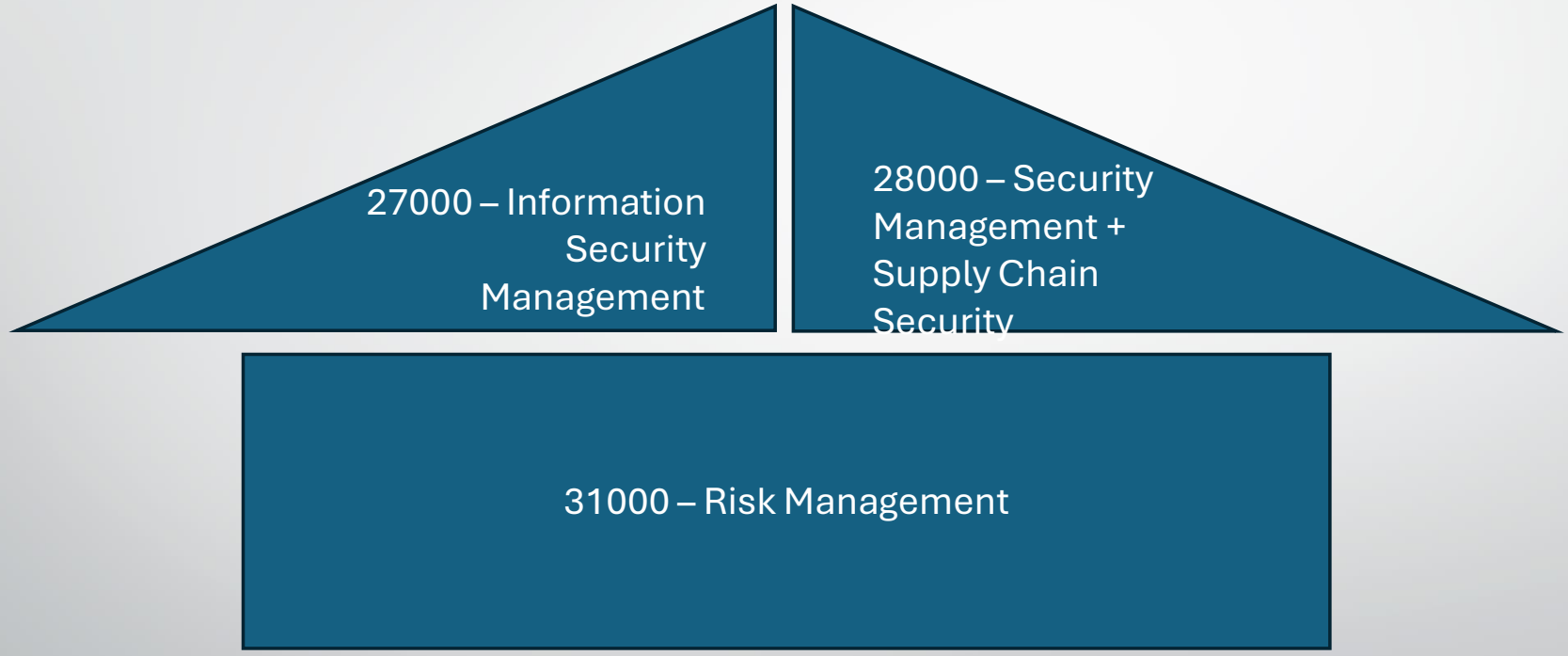
Nachweise & Audits
- Dokumentation zu Risiken, Maßnahmen, Tests, KPIs; Audit- und Inspektionsrechte der kritischen Einrichtung akzeptieren.

Compliance mit Standards
- Ausrichtung an anerkannten Normen (bei BCM, physischer Sicherheit, Supply-Chain-Sicherheit; bei IT-nahen Leistungen Ergänzung um NIS2-relevante Cyberstandards).

Eskalations- und Entscheidungswege
- Klar definierte Verantwortungen, Stellvertretungen und verbindliche Reaktionszeiten (SLA/OLA).

Standort- und Sektorbesonderheiten
- Berücksichtigung nationaler Vorgaben und spezieller Schutzbedarfe (z. B. KRITIS-Anlagen, Transport gefährlicher Güter).

Where to start?
Haus der Normen-Familien für eine NIS2- & CER-Umsetzung



Vorteil ISO-Normenfamilie: ein Management-System für viele inhaltliche Ausprägungen

Umsetzung von NIS2 und CER als Unternehmen
Welche Normen/Standards sind hierfür relevant?

Governance und Managementsysteme (NIS2, beide)
- ISO 27001 + 27002: ISMS mit konkreten Sicherheitsmaßnahmen
- ISO 27014: Governance der Informationssicherheit (Leitplanken, Rollen)

Risiko- und BIA-Methodik (beide, NIS2 mit Cyber-Fokus)
- ISO 31000 + 31010: Risikomanagement und -methoden
- ISO 27005: Informationssicherheits-Risikomanagement
- ISO 22317: Business Impact Analysis (BIA)

Business Continuity, Notfall- und Resilienzmanagement (beide, CER-Schwerpunkt)
- ISO 22301: Managementsystem für BCM
- ISO 22320: Notfall-/Incident-Management in Organisationen
- ISO 22398: Übungen und Tests (Planspiele, Drills)
- ISO 22316: Organisational Resilience
- ISO 27031: ICT-Readiness for Business Continuity

Incident- und Schwachstellen-Handling (NIS2)
- ISO 27035: Incident Management (Erkennung, Meldung, Behandlung)
- ISO 30111: Vulnerability Handling Prozesse
- ISO 29147: Vulnerability Disclosure (Koordinierte Meldung)

Asset- und Betriebsführung (Unterstützend für CER/NIS2)
- ISO 55001: Asset-Management (Lebenszyklus, Kritikalität, Instandhaltung)

Lieferkette und Cloud (beide, NIS2-Schwerpunkt)
- ISO 27036: Sicherheitsanforderungen in Lieferantenbeziehungen
- ISO 27017: Sicherheitskontrollen für Cloud-Dienste
- ISO 27018: Schutz personenbezogener Daten in Public Clouds
- ISO 28000: Sicherheitsmanagement-System & Supply-Chain-Security

Technische/OT-Sicherheit (beide; für Betreiber mit industriellen Anlagen besonders relevant)
- ISO 27033: Netzwerksicherheits-Architektur
- ISO 27034: Anwendungssicherheit
- IEC 62443 (Serie): Industrial/OT-Cybersecurity (Steuerungs- und Automatisierungssysteme)

Physische Sicherheit und Objektschutz (CER-Schwerpunkt)
- ISO 27002 (Kapitel Physische/Umgebungssicherheit): Zutritt, Standort, Versorgung
- ISO 22341: Crime Prevention Through Environmental Design (CPTED) – baulich-organisatorischer Schutz

Audit, Nachweis, KPIs (beide)
- ISO 19011: Leitfaden für Audits von Managementsystemen
- ISO 27004: Messung und KPIs im ISMS

Vielen Dank!

- Fragen? Dann jetzt!
- Danke für die Aufmerksamkeit
  - Mastodon: **@AG_KRITIS@chaos.social**
  - LinkedIn: **linkedin.com**/company/**ag-kritis**
  - Website: **ag.kritis.info**

  - Martin Wölfel: **linkedin.com**/in/**martinwoelfel**