IT-SICHERHEIT

Die rechtlichen Herausforderung für ihr Unternehmen

GoldbergUllrich
Rechtsanwälte

GoldbergUllrich
Rechtsanwälte

Michael Ullrich, LL.M.
Rechtsanwalt, Partner

Fachanwalt für gewerblichen Rechtsschutz
Fachanwalt für Informationstechnologierecht

ZIELE DES VORTRAGS

1. **Grundwissen**: NIS-Richtlinien, IT-Sicherheitsgesetze, NIS2UmsuCG
2. **Erfassen** der wesentlichen Regelungsinhalte
3. **Herausarbeitung** der Anforderungen an Unternehmen und Unternehmensführung:
4. **Aktuelle Pflichten**: Was gilt im Moment?
5. **Zukünftige Pflichten**: Was gilt morgen?
6. **Einordnung** auf der zeitlichen Achse (= Wie schnell muss was umgesetzt werden?)

AUFBAU

GoldbergUllrich
Rechtsanwälte

WAS IST NIS?

= (en.) ***„European Network and Information Security Directive“***

= (dt.) ***„EU-Richtlinie zur Netzwerk- und Informationssicherheit“***

- Es gibt zwei NIS-Richtlinien:
  - **NIS-1** Richtlinie (EU) **2016***/1148
  - **NIS-2** Richtlinie (EU) **2022**/2555

  *(Jahresdatum des Beschlusses. **Nicht**: Datum des Inkrafttretens).

- **NIS-2 hat NIS-1 ersetzt:**

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**

GoldbergUllrich
Rechtsanwälte

WAS SIND EU-RICHTLINIEN UND WIE WIRKEN SIE?

- EU-Richtlinien werden zunächst als EU-Sekundärrecht von den Organen der EU (Parlament, Rat etc.) auf Grundlage der EU-Verträge angenommen.

- Richtlinien entfalten durch Erlass nicht unmittelbar Wirksamkeit, § 288 Abs. 3 AEUV:

„Die Richtlinie ist für jeden Mitgliedstaat, an den sie gerichtet wird, hinsichtlich des zu erreichenden Ziels verbindlich, überlässt jedoch den innerstaatlichen Stellen die Wahl der Form und der Mittel.“

- Müssen in Mitgliedsstaaten noch mit nationalen Gesetz umgesetzt werden, um Wirkung zu entfalten. Allerdings gibt es Ausnahmen (*Vorwirkung*, *Richtlinienkonforme Auslegung*).
- Nationale Gesetze können strenger sein, als die europäische Vorlage!
- Umsetzungsfrist wird in Richtlinien bestimmt und normiert – i.d.R. 2 Jahre.
  NIS-2: abweichende Umsetzungsfrist, Art. 41 Abs. 1 S. 1.

GoldbergUllrich
Rechtsanwälte

AKTUELLE PFLICHTEN: WAS GILT AKTUELL?

(Einige Beispiele)

- Einsatz von **Systemen zur Angriffserkennung** (spätestens bis zum **01.05.2023** – IT-SiG 2.0)
  (IDS = Intrusion Detection Systems; SIEM-Tools = Security Information Event Management; SAP-ETD = System Applications & Products [für Datenverarbeitung] - Enterprise Threat Detection)
- Pflicht zur **„unverzüglichen" Meldung** von Störungen und Angriffen (Art. 14, 16 NIS-1, § 8c BSIG, § 11 EnWG)
- Systeme müssen auf **„neuestem Stand der Technik"** sein, § 8a I BSIG (z. B. ISO 27001)
- **Reaktionspläne** und **Präventionsmaßnahmen**
  („*Business Continuity Planning*", „*Desaster Recovery Planning*")
- Durchführung von ***Audits*** (*dt. eig.* Bücherprüfung, Rechnungsprüfung) alle 2 Jahre; Meint: Sicherheitsuntersuchung durch geschulte Auditoren
- **Registrierungspflichten** bei BSI

GoldbergUllrich
Rechtsanwälte

AKTUELLE PFLICHTEN: WAS GILT AKTUELL?

- **Maßnahmen zur physischen Sicherheit von Datenzentren** (Geosicherheit etc.) – Hier nur am Rande erwähnt, da Schwerpunkt hier auf Sicherheit bei Software
- Ggfs. Pflicht zur Bestandsdatenauskunft bei Telekommunikationsanbietern (aktuell § 5c BSIG)
- Bei Verstößen drohen (abgestuft) Bußgelder.

BIS WANN MUSS NIS-2 IN NATIONALES RECHT UMGESETZT WERDEN?

- **Inkrafttreten von NIS-1** am 08.08.2016.
- **Umsetzung in Deutschland** erfolgte mit „**Gesetz zur Umsetzung der europäischen Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit**“, verkündet am 29.06.2017 (≈ 11 Monate).

- **Inkrafttreten von NIS-2** am 16.01.2023
- **Umsetzung** in deutsches Recht noch nicht vorgenommen!
- **Umsetzungsfrist für NIS-2** beträgt 21 Monate = spätestens 17.10.2024.
- Bei Ansetzen des Vergleichswerts von NIS-1 könnte mit Verkündung des Umsetzungsgesetzes im **Dezember 2023** zu rechnen sein.

  → Bisheriges Gerücht: NIS-2 könnte mit dem IT-Sicherheitsgesetz 3.0 umgesetzt werden. Aber…

GoldbergUllrich
Rechtsanwälte

WAS IST DAS IT-SICHERHEITSGESETZ (IT-SIG)?

- Bislang gilt:

IT-SiG ≠ NIS

…denn bisher hat das IT-SiG völlig getrennt von der NIS-Richtlinie bestanden.

Die bisherigen IT-Sicherheitsgesetze erweiterten „nur“ den Schutz eines bestehenden (vorherigen) Gesetzes zur Umsetzung von NIS.

Tatsächlich gab es bisher schon zwei IT-Sicherheitsgesetze. Diese haben aber andere Regelungen betroffen bzw. getroffen.

⟶ Wie kann und soll das IT-SiG also nun Regelungen aus NIS-2 umsetzen?

WAS IST DAS IT-SIG? (TEIL 2)

- Alle IT-SiG waren bisher sog. **Mantel-** oder **Artikelgesetze**.

= Zusammenfassung mehrerer Regelungen und/oder Änderungen an anderen Gesetzen unter dem „Mantel“ einer bestimmten Thematik.

Die unterschiedlichen Regelungen und Änderungen an den einzelnen Gesetzen werden typischerweise in verschiedene Artikel unterteilt und so übersichtlich geordnet.

- Vorschriften aus NIS-2 können also mit untergebracht werden oder sogar allein den Inhalt von IT-SiG 3.0 ausmachen.

GoldbergUllrich
Rechtsanwälte

KLEINE ENTSTEHUNGSGESCHICHTE DES IT-SIG

- **Erstmaliges Inkrafttreten** am 25.07.2015
- **Anlass**:
  Sicherheitspolitische Bedenken & Beobachtungen

  Häufung von Angriffen auf kritische Infrastruktur, Terroranschläge, militärische Überlegungen zum „Multi-Domaine-Battlefield“ der Zukunft (Land, Wasser, Luft, Weltraum, Cyber, Menschlich/Psychologisch).
- **Ursprüngliches Ziel**:
  Schutz von kritischer Infrastruktur, digitalen Systemen und Daten durch die Definierung von (Mindest-)Standards für die Sicherheit in diesem besonders schützenswerten Bereich (z. B. Anforderungen zur Angriffserkennung).
- **Verantwortliche Prüf- und Meldestelle**:
  Bundesamt für Sicherheit in der Informationstechnik (BSI)

ENTWICKLUNG DES IT-SIG

- IT-SiG wird fortlaufend erweitert und überarbeitet. 2023 könnte eine neue Änderung anstehen.
- Bezeichnung wie bei Versionen von Programmen („IT-Sicherheitsgesetz 2.0“ etc.).

Versionen:

- **IT-Sicherheitsgesetz 1.0** – In Kraft getreten am 25.07.2015
- **IT-Sicherheitsgesetz 2.0 –** In Kraft getreten am 28.05.2021

  U. a. Verstärkte Berücksichtigung von Schutz von Verbrauchern
- **IT-Sicherheitsgesetz 3.0** – Ende 2023?

  Neuer Entwurf wird seit Ende 2022 diskutiert. Innenministerium wollte „bis zur Sommerpause 2023 einen Gesetzesentwurf vorlegen“. Aktuell kein Entwurf vorgelegt. Ob er noch kommt – Ungewiss.

Ziel eines neues IT-SIG 3.0 könnte sein: Einheitlichere Regelungen zur physischen und softwaretechnischen Sicherheit der Infrastruktur in der EU

WAS REGELT DAS IT-SIG BISLANG?

- Erweiterung der Zuständigkeiten und Befugnisse des BSI.
- Bislang primär Regelungen zum Schutz von:

1. Kritischen Infrastrukturen (**KRITIS**)
2. Unternehmen im besonderen öffentlichen Interesse (**UBIs**).

- Allgemein änderte das IT-SiG bisher z. B. Paragraphen des **BSI-Gesetzes**, des **Atomgesetzes**, des **Energiewirtschaftsgesetzes**, des **Telemediengesetzes**, des **Telekommunikationsgesetzes**, und des **Bundeskriminalamtgesetzes**.

KRITIS (AKTUELL)

[1]gemäß BSIG
[2]gemäß Bund-Länder-Arbeitsgruppe

*Grafik: Bundesamt für Bev.schutz u. Katastrophenh. (BBK)

GoldbergUllrich
Rechtsanwälte

WAS SIND UBIS?

- Die Kategorie der „UBIs“ ist ein Auffangtatbestand.
- UBIs sind Unternehmen, die keine KRITIS darstellen, aber trotzdem schutzzwecktechnisch auf einer Stufe mit diesen stehen sollen.
- Der Begriff ist in **§ 2 Abs. 14 BSIG** legaldefiniert.
- Bislang drei Kategorien von UBIs:

KATEGORIEN VON UBIS

- § 2 Abs. 14 **Nr. 1** BSIG: Hersteller/Entwickler von Gütern i.S.v. § 60 Außenwirtschaftsverordnung (AWV).
  Z. B. Hersteller von Waffen- und Verteidigungssystemen.
- § 2 Abs. 14 **Nr. 2** BSIG: Unternehmen mit größten Anteilen an inländischer Wertschöpfung in Deutschland (BIP) und ihre Zulieferer.
  Z. B. große Autohersteller oder Zulieferer für Industrietechnik.
- § 2 Abs. 14 **Nr. 3** BSIG: Betreiber eines Betriebsbereichs der obersten Klasse der Störfall-Verordnung, oder diesen gem. § 1 Abs. 2 gleichgestellte Betriebe.
  Z. B. Betriebe, die mit gefährlichen Stoffen handeln (Chem. Industrie).

WARUM GIBT ES NUN MIT NIS-2 ÄNDERUNGEN?

1. Überprüfung der NIS-1-Richtlinie hat „***inhärente Mängel*** *ergeben, die ein wirksames Vorgehen gegen aktuelle und neue Herausforderungen im Bereich Cybersicherheit verhindern*“.
2. Ausweitung der **Cyberbedrohungslage**:
   „*Anzahl, Tragweite, Komplexität, Häufigkeit und Auswirkungen von Vorfällen nehmen zu*“.
3. Dadurch Bedrohung und Schäden für **Wirtschaft** und **Gesellschaft** im EU-Binnenmarkt.
   (Finanzielle Verluste, Wirtschaftsspionage, Datenverluste, Ransomware-Erpressungen)
4. **Zu unterschiedliche Umsetzung von NIS-1 in den einzelnen Mitgliedsstaaten (MS)**.
   - Keine einheitlichen Anforderungen bei Cybersicherheit (Detail, Art der Aufsicht).
   - Zu großer Ermessensspielraum bei Verpflichtung zu Meldungen von Sicherheitsvorfällen.
   - Abweichende Einstufungen von vergleichbaren Unternehmen in den MS

GoldbergUllrich
Rechtsanwälte

WARUM GIBT ES NUN MIT NIS-2 ÄNDERUNGEN?

6. Deswegen:
   Zusätzliche Kosten,
   Schwierigkeiten für Einrichtungen, die Waren und Dienste grenzüberschreitend anbieten.
7. Anwendungsbereich von NIS-1 zu klein. Mehr Sektoren werden erfasst.

   Schätzungen gehen bei NIS-2 von **„29.000 - 30.000“ zusätzlich erfassten Unternehmen** aus**!***
6. „Aktuelle geopolitische Entwicklungen (Zeitenwende)“ = Bedrohungslage u.a. Ukraine-Krieg (Beschlussdatum für NIS-2 war am 14.12.2022)
7. Ziel von NIS-2: „*Unterschiede zwischen den Mitgliedsstaaten* […] *beseitigen*“.
8. (Keine Einbeziehung von Vertrauensdienstanbietern in NIS-1.)
9. (Keine Einbeziehung von DNS-Diensten (*domain name system*) in NIS-1.)

* Nur im Vergleich: Bei NIS-1 wurde noch von 500-1500 zusätzlich erfassten Unternehmen ausgegangen!

GoldbergUllrich
Rechtsanwälte

ÜBERBLICK: WAS FÜR ÄNDERUNGEN GIBT ES IN NIS2?

1. Ausweitung des Anwendungsbereichs von NIS-2

   Ziel: Umfassende Abdeckung aller grundlegenden gesellschaftlichen und wirtschaftlichen Tätigkeiten.

   = Mehr Unternehmen werden nach NIS-2 unter „**KRITIS**“ fallen! Dazu gleich mehr…
2. Unterscheidung zwischen „**wesentlichen**“ und „**wichtigen**“ Einrichtungen bezüglich notwendiger Risikomanagementmaßnahmen und Meldepflichten.
3. Vereinheitlichung der Kriterien für Einstufung als Betreiber wesentlicher Dienste. (Bisher waren die Mitgliedsstaaten für Einstufung nach Kriterien verantwortlich.)
4. Einbeziehung von „**Vertrauensdienstanbietern**“. Hierzu…

GoldbergUllrich
Rechtsanwälte

VERTRAUENSDIENSTANBIETER

- Definition gem. **Art. 3 Nr. 19, Nr. 16 Verordnung (EU) 910/2014**:

  [19] „Vertrauensdiensteanbieter“ ist eine natürliche oder juristische Person, die einen oder mehrere Vertrauensdienste als

  qualifizierter oder nichtqualifizierter Vertrauensdiensteanbieter erbringt.

  [16] „Vertrauensdienst“ ist ein elektronischer Dienst, der in der Regel gegen Entgelt erbracht wird und aus Folgendem besteht:

  a) Erstellung, Überprüfung und Validierung von elektronischen Signaturen, elektronischen Siegeln oder elektronischen Zeitstempeln, und Diensten für die Zustellung elektronischer Einschreiben sowie von diese Dienste betreffenden Zertifikaten oder

  b) Erstellung, Überprüfung und Validierung von Zertifikaten für die Website-Authentifizierung oder

  c) Bewahrung von diese Dienste betreffenden elektronischen Signaturen, Siegeln oder Zertifikaten.

- = Personenidentifizierungsdienste, elektronische Zahlungen usw.

ÜBERBLICK: WAS FÜR ÄNDERUNGEN GIBT ES IN NIS2?

1. Ausweitung des Anwendungsbereichs von NIS-2

   Ziel: Umfassende Abdeckung aller grundlegenden gesellschaftlichen und wirtschaftlichen Tätigkeiten. Nach Stat. Bundesamt 5-mal mehr Unternehmen erfasst.

   = Mehr Unternehmen werden nach NIS-2 unter „**KRITIS**“ fallen! Dazu gleich mehr…
2. Unterscheidung zwischen „wesentlichen“ und „wichtigen“ Einrichtungen bezüglich notwendiger Risikomanagementmaßnahmen und Meldepflichten.
3. Vereinheitlichung der Kriterien für Einstufung als Betreiber wesentlicher Dienste. (Bisher waren die Mitgliedsstaaten für Einstufung nach Kriterien verantwortlich.)
4. Einbeziehung von „**Vertrauensdienstanbietern**“.

ÜBERBLICK: WAS FÜR ÄNDERUNGEN GIBT ES IN NIS2?

5. Einrichtung eines Zentralregisters bei der European Union Agency for Cybersecurity (**ENISA**), in dem alle wesentlichen und wichtigen Einrichtungen sowie Domänennnamen-Registrierungsdienste aufgeführt werden.
6. **Ausnahme**: Für Finanzunternehmen soll stattdessen die Verordnung (EU) 2022/2554 gelten („Verordnung über […] digitale operationale Resilienz im Finanzsektor). Informationsaustausch soll aber weiter gefördert werden.
7. **„CSIRTs“** sollen im Bezug auf personenbezogene Daten in der Lage sein, auf Ersuchen der Einrichtungen, proaktive Sicherheitsüberprüfungen vorzunehmen. (Hierzu…)

WAS IST EIN „CSIRT“?

= Ein Team von IT-Sicherheitsexperten bzw. -sachverständigen, deren Hauptaufgabe darin besteht, auf Computersicherheitsverletzungen zu reagieren. Dieses Team bietet die zu ihrer Behandlung notwendigen Dienstleistungen und unterstützt seine Klientel bei der Wiederherstellung nach derartigen Sicherheitsverletzungen.

Der Begriff **CSIRT** wird vorwiegend in Europa für den geschützten Begriff **CERT** verwendet, der in den USA vom CERT Coordination Center (CERT/CC) eingetragen ist.

Es gibt mehrere Akronyme, die für derartige Teams verwendet werden: .....

- **CSIRT** (**C**omputer **S**ecurity **I**ncident **R**esponse **T**eam)
- **CERT** oder **CERT/CC** (**C**omputer **E**mergency **R**esponse **T**eam/**C**oordination **Ce**
- **CIRT** (**C**omputer **I**ncident **R**esponse **T**eam)
- **MIRT** (**M**obile **I**ncident **R**esponse **T**eam)
- **IRT** (**I**ncident **R**esponse **T**eam)
- **SERT** (**S**ecurity **E**mergency **R**esponse **T**eam)

GoldbergUllrich
Rechtsanwälte

ÜBERBLICK: WAS FÜR ÄNDERUNGEN GIBT ES IN NIS2?

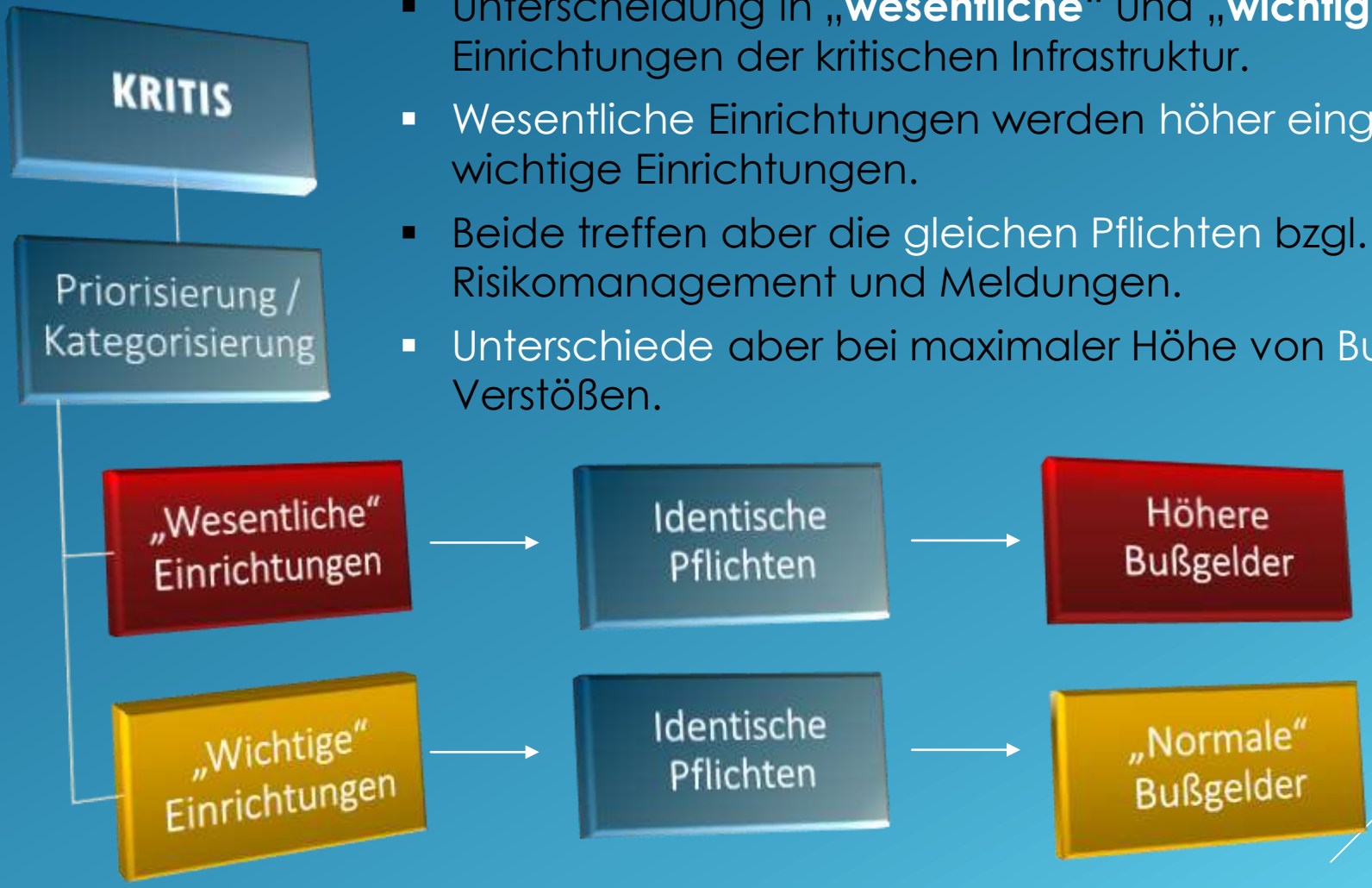
5. Einrichtung eines Zentralregisters bei der European Union Agency for Cybersecurity (**ENISA**), in dem alle wesentlichen und wichtigen Einrichtungen sowie Domänennamen-Registrierungsdienste aufgelistet werden.
6. **Ausnahme**: Für Finanzunternehmen soll stattdessen die Verordnung (EU) 2022/2554 gelten („Verordnung über […] digitale operationale Resilienz im Finanzsektor). Informationsaustausch soll aber weiter gefördert werden.
7. **CSIRTs** sollen im Bezug auf personenbezogene Daten in der Lage sein, auf Ersuchen der Einrichtungen, proaktive Sicherheitsüberprüfungen vorzunehmen.
8. Schaffung eines europäischen **CSIRT-Netzwerks** („CERT-Bund").
9. **Förderung** von **Open-Source-Cybersicherheitswerkzeugen und –Anwendungen**.
10. „*Governance*": **(Geschäfts-)Leitungsorgane** sollen für Verstöße von Einrichtungen **verantwortlich** gemacht werden können, Art. 20 Abs. 1 NIS-2 **!**

GoldbergUllrich
Rechtsanwälte

ÜBERBLICK: WAS FÜR ÄNDERUNGEN GIBT ES IN NIS2?

11. Pflicht (?) zur Einführung von Verfahren zur Entgegennahme von Tipps von Dritten zu Sicherheitsschwachstellen bei Herstellern und Anbietern von IKT-Produkten. (Gründe Nr. 58; ISO/IEC 30111, ISO/IEC 29147)
12. Errichtung einer europäischen **Schwachstellen-Datenbank** durch die ENISA. (Kooperation mit **CVE-Programm** (Common Vulnerabilities and Exposures) soll geprüft werden.)
13. Bestimmte CSIRTs sollen als **Koordinatoren** benannt werden und als Schnittstelle zwischen Schwachstellenmeldern und IKT-Betreibern fungieren.
14. Dreistufiges Meldesystem – u. a. Frühwarnpflicht (24h) und allgemeine Meldepflicht (bis 72h) bei „erheblichen Sicherheitsvorfällen“.
15. Möglichkeit zur öffentlichen „Anprangerung“ von Unternehmen, durch Verpflichtung zur Veröffentlichung von Verstößen gg. NIS-2 durch diese selbst, Umsetzung von Art. 32 Abs. 4 lit. e, h NIS-2 – In Deutschland durch das BSI.

ANWENDUNGSBEREICH: WAS GEHÖRT ZU DEN KRITIS ?



- Unterscheidung in „**wesentliche**“ und „**wichtige**“ Einrichtungen der kritischen Infrastruktur.
- Wesentliche Einrichtungen werden höher eingeordnet als wichtige Einrichtungen.
- Beide treffen aber die gleichen Pflichten bzgl. Risikomanagement und Meldungen.
- Unterschiede aber bei maximaler Höhe von Bußgeldern bei Verstößen.

GoldbergUllrich
Rechtsanwälte

WESENTLICHE EINRICHTUNGEN

Die wesentlichen Einrichtungen werden nach **zwei Kategorisierungen** bestimmt/definiert:

Größe & **Typ** des Unternehmens	Nur **Typ** des Unternehmens
➓Sog. „*Mittlere Unternehmen*“ ➓Nach Mitarbeiteranzahl ➓Nach Umsatz ➓Nach Art des Geschäftsfeldes	➓Explizite Nennung des Unternehmenstypus in Richtlinie (später: Gesetz) ➓Keine Berücksichtigung der Größe des Unternehmens

- Die Unternehmen, die davon nicht erfasst werden, sind grds. nicht von NIS-2 betroffen!

GoldbergUllrich
Rechtsanwälte

1. KATEGORIE: GRÖßE & TYP

- **Grundsatz**: „*Überschreiten des Schwellenwertes für **mittlere** Unternehmen*“
- Schwellenwert steht nicht ausdrücklich in Norm, aber…

*(2) Innerhalb der Kategorie der KMU wird ein **kleines** Unternehmen als ein Unternehmen definiert, das **weniger als 50 Personen** beschäftigt und dessen **Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt**.*
- (Anhang) Art. 2 I, II Empfehlung 2003/361/EG

- **…Umkehrschluss:**

WESENTLICHE EINRICHTUNGEN (BEI ÜBERSCHREITEN DES SCHWELLENWERTES)

1. **Energie** (Elektrizität, Fernwärme, Erdöl, Erdgas, Wasserstoff)
2. **Verkehr und Transport** (Luftverkehr, Schienenverkehr, Schifffahrt, Straßenverkehr)
3. **Bankwesen** (Kreditinstitute)
4. **Finanzmärkte** (Handelsplätze und sog. zentrale Gegenparteien)
5. **Gesundheitswesen** (Dienstleister, Laboratorien, Forschung, Pharmazeutik, Medizingeräte)
6. **Trinkwasser** (Wasserversorgung für menschlichen Gebrauch)
7. **Abwasser** (Abwasserentsorgung für Verbraucher & Industrie)
8. **Digitale Infrastruktur** (Internet-Knoten, DNS, TLD-Registrare, Cloud Provider, Rechenzentren, Inhaltszustelldienste („*Content Delivery Networks*“ / CDN), Vertrauensdienste, Anbieter für öff. zugängliche elektronische Kommunikationsnetze und Kommunikationsdienste)
9. **B2B: Verwaltung von IKT-Diensten** (Anbieter verwalteter Dienste („*Managed Service Providers*“) und Anbieter verw. Sicherheitsdienste („*Managed Security Providers*“))
10. **Öffentliche Verwaltung** (Zentrale und regionale Regierungseinrichtungen)
11. **Weltraum** (Betreiber von Bodeninfrastruktur f. Unterstützung weltraumgestützter Dienste)

GoldbergUllrich
Rechtsanwälte

2. KATEGORIE:
WESENTLICHE EINRICHTUNGEN NACH TYP (GRÖßE EGAL)

- **Qualifizierte Vertrauensdiensteanbieter**, Art. 3, Abs. 1 lit. b) NIS-2
- **Domänenregister der Domäne oberster Stufe**, Art. 3, Abs. 1 lit. b) NIS-2
- **(Alle) DNS-Dienstanbieter**, Art. 3, Abs. 1 lit. b) NIS-2
- **[!!!] Variable Einstufungen**, Art. 3, Abs. 1 lit. e) NIS-2

  = EU-Mitgliedsstaaten können bestimmte Einrichtungen als „wesentlich“ einstufen, wenn diese sonst nicht unter NIS-2 fallen würden, oder aber sonst nur als „wichtige“ Einrichtung eingestuft würden.

  Für die Kriterien gibt es aber einen **Katalog**, der den Anwendungsbereich etwas eingrenzt (Art. 2, Abs. 2 lit. b) – e) NIS-2).

VARIABLE EINSTUFUNGEN

4 Sondereinstufungsmöglichkeiten für die Mitgliedsstaaten:

1. Einrichtung ist **einziger Anbieter eines Dienstes in einem MS**, der für „*die Aufrechterhaltung kritischer gesellschaftlicher oder wirtschaftlicher Tätigkeiten unerlässlich ist*“.
2. Störung v. Dienst wirkt sich „wesentlich“ auf **öffentliche Ordnung**, **Sicherheit** oder **Gesundheitsversorgung** aus.
3. Störung v. Dienst führt zu einem „***wesentlichen Systemrisiko***“. Insbesondere bei grenzübergreifenden Auswirkungen relevant.
4. Einrichtung ist kritisch, da sie „**besondere Bedeutung**“ hat für den betroffenen Dienst oder Sektor direkt, oder für andere voneinander abhängigen Sektoren/Dienste.

2. KATEGORIE: WESENTLICHE EINRICHTUNGEN NACH TYP

- **Qualifizierte Vertrauensdiensteanbieter**, Art. 3, Abs. 1 lit. b) NIS-2
- **Domänenregister der Domäne oberster Stufe**, Art. 3, Abs. 1 lit. b) NIS-2 („*Top-Level-Domain*“, z. B. „.de“, „.org“ etc.)
- **(Alle) DNS-Dienstanbieter**, Art. 3, Abs. 1 lit. b) NIS-2
- **Variable Einstufungen**, Art. 3, Abs. 1 lit. e) NIS-2
- „**Kritische Einrichtungen**“ (KRITIS) nach „RCE“ bzw. „CER“ Richtlinie (EU) 2022/2557 („*EU RCE Directive*“) zur Regulierung von physischer Resilienz (= Ausfallsicherheit) der KRITIS in der EU. – Anwendungsbereich zu NIS-2 sehr ähnlich, aber es gibt Unterschiede, z. B. zählt Lebensmittelgroßhandel und –logistik mit zu KRITIS. Art. 3, Abs. 1 lit. f) NIS-2 i.V.m. Art. 5 CER i.V.m. Anhang CER.
- **Voreinstufungen**: Einrichtungen, die **vor dem 16.01.2023** schon aufgrund von **NIS-1** als wesentlich eingestuft wurden, Art. 3, Abs. 1 lit. g) NIS-2

WAS SIND „WICHTIGE“ EINRICHTUNGEN?

- = **Ausschlussprinzip** – All das was in den Anhängen I oder II zu NIS-2 genannt wird, aber nicht zu den „wesentlichen“ Einrichtungen gezählt wird:

Für die Zwecke dieser Richtlinie gelten Einrichtungen der in Anhang I oder II aufgeführten Art, die nicht als wesentliche Einrichtungen im Sinne von Absatz 1 des vorliegenden Artikels gelten, als wichtige Einrichtungen. Dies schließt Einrichtungen ein, die von den Mitgliedsstaaten gemäß Artikel 2 Absatz 2 Buchstaben b bis e als wichtige Einrichtungen eingestuft werden.

[Art. 3 Abs. 2 NIS-2]

- **Insbesondere**: Anhang II zu NIS-2 zu beachten!

WICHTIGE EINRICHTUNGEN NACH ANHANG II ZU NIS-2

1. **Post- und Kurierdienste**
2. **Abfallbewirtschaftung**
3. **Chemikalien** (Produktion, Herstellung und Handel)
4. **Lebensmittel** (Produktion, Verarbeitung und Vertrieb)
5. **Verarbeitendes Gewerbe/Herstellung von Waren…**

- **Herstellung von Medizinprodukten und In-vitro-Diagnostika**
- **Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen**
- **Herstellung von elektrischen Ausrüstungen**
- **Maschinenbau**
- **Herstellung von Kraftwagen und Kraftwagenteilen**
- **Sonstiger Fahrzeugbau**

WICHTIGE EINRICHTUNGEN NACH ANHANG II ZU NIS-2

1. **Post- und Kurierdienste**
2. **Abfallbewirtschaftung**
3. **Chemikalien** (Produktion, Herstellung und Handel)
4. **Lebensmittel** (Produktion, Verarbeitung und Vertrieb)
5. **Verarbeitendes Gewerbe/Herstellung von Waren…**

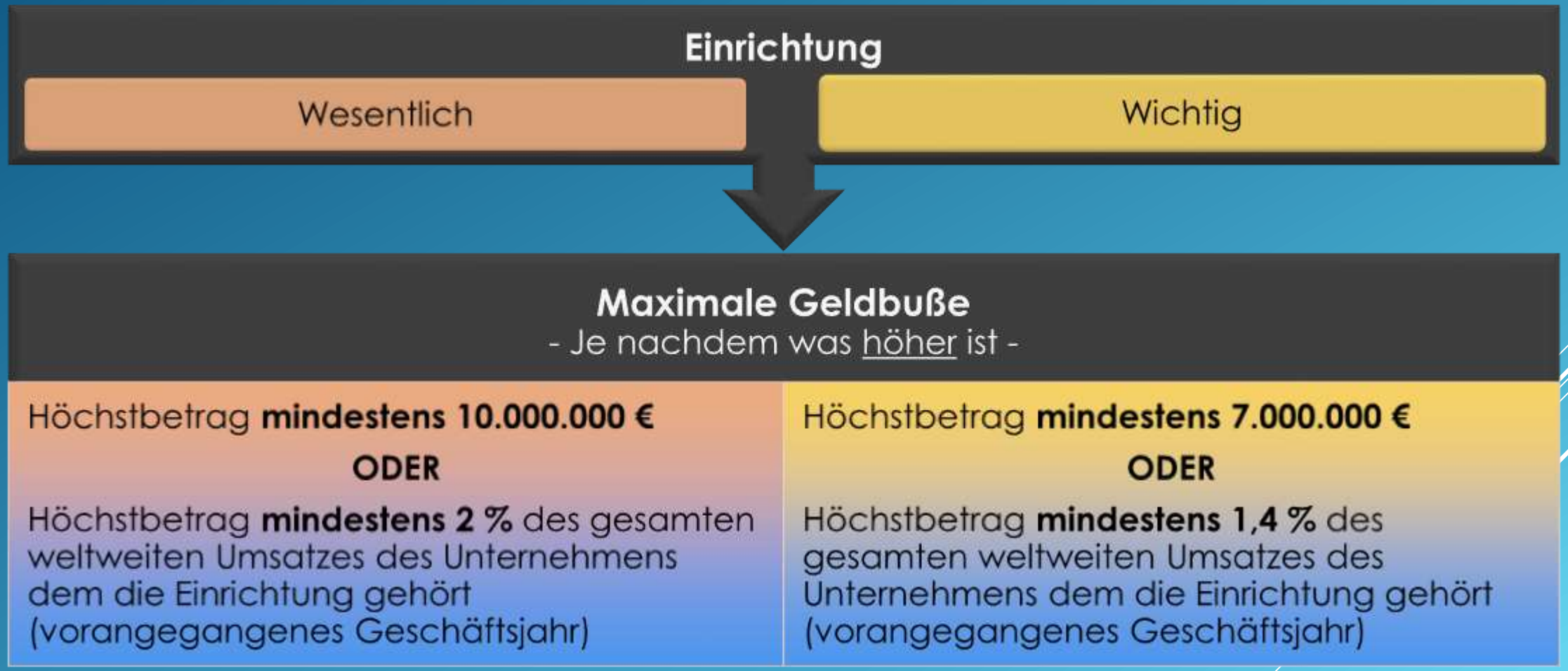
- **Herstellung von Medizinprodukten und In-vitro-Diagnostika**
- **Herstellung von Datenverarbeitungsgeräten, elektronischen und optischen Erzeugnissen**
- **Herstellung von elektrischen Ausrüstungen**
- **Maschinenbau**
- **Herstellung von Kraftwagen und Kraftwagenteilen**
- **Sonstiger Fahrzeugbau**

WICHTIGE EINRICHTUNGEN NACH ANHANG II ZU NIS-2

1. **Post- und Kurierdienste**
2. **Abfallbewirtschaftung**
3. **Chemikalien**
   (Produktion, Herstellung und Handel)
4. **Lebensmittel**
   (Produktion, Verarbeitung und Vertrieb)
5. **Verarbeitendes Gewerbe/Herstellung von Waren**
   (Medizinprodukte und In-vitro-Diagnostika, Computer, Elektronik, Optik, elektrische Ausrüstung, Maschinenbau, Kraftwagen und Teile, Fahrzeugbau)
6. **Digitale Dienste**
   (Marktplätze, Suchmaschinen, Soziale Netzwerke)
7. **Forschungseinrichtungen**

GoldbergUllrich
Rechtsanwälte

GELDBUßEN (NIS-2)



GoldbergUllrich
Rechtsanwälte

WELCHE PFLICHTEN ERGEBEN SICH BISLANG AUS NIS-2?

- **Identifikation** der eigenen Unternehmenseinstufung als wesentliches oder wichtiges Unternehmen (oftmals wohl durch Rechtsberatung).
- **Übermittlung** bestimmter Unternehmensdaten an zuständige Behörden in Mitgliedsstaaten (Deutschland: BSI), Art. 3 Abs. 4, 3 NIS-2.
- **Einrichtung** von Sicherheitsvorkehrungen für Unternehmen, die bisher nicht erfasst wurden.
- **Erweiterung** von Sicherheitsvorkehrungen.
- **Einplanen** von regelmäßigen proaktiven Sicherheitsüberprüfungstests.
- **Abweichende Meldepflichten** („dreistufiges Melderegime“ statt einstufigem System)

ABER

AKTUELLE ENTWICKLUNGEN

- Seit **03.04.2023** liegt Referentenentwurf eines „Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - **NIS2UmsuCG**)“ des Bundesministeriums des Inneren und für Heimat (BMI) vor.
- = NIS2UmsuCG wird wahrscheinlich Umsetzungsgesetz werden.
- NIS2UmsuCG wird aber ebenfalls Mantel- bzw. Artikelgesetz sein.
- **NIS2-UmsuCG ≠ IT-Sicherheitsgesetz 3.0** !!!
  (…könnte aber später so umbenannt werden)
- Gesetz sieht **Abweichungen** von NIS-2 vor!

ABWEICHUNGEN:

- **Abweichende Kategorien** für Einrichtungen
  (≈ „mehr Verhältnismäßigkeit bei Anforderungen“)
  Vor allem: „wesentliche“ Unternehmen werden vor allem Großunternehmen sein.
  Mittlere Unternehmen sollen etwas anders eingeordnet werden.
- **UBIs fallen weg**, bzw. werden in anderer Kategorie eingeordnet.
- **Evtl. höhere maximale Geldbußen**
- Einbeziehung sowohl von immateriellen Schäden bei Betrachtung der Erheblichkeit von Sicherheitsvorfällen
- **Extensiveres fünfstufiges Meldesystem**
- Konkrete(re) **Haftungs- und Verhaltensvorgaben** für **Geschäftsleitungen**

EINRICHTUNGEN IN NIS2UmsuCG

GoldbergUllrich
Rechtsanwälte

Kritische Anlagen

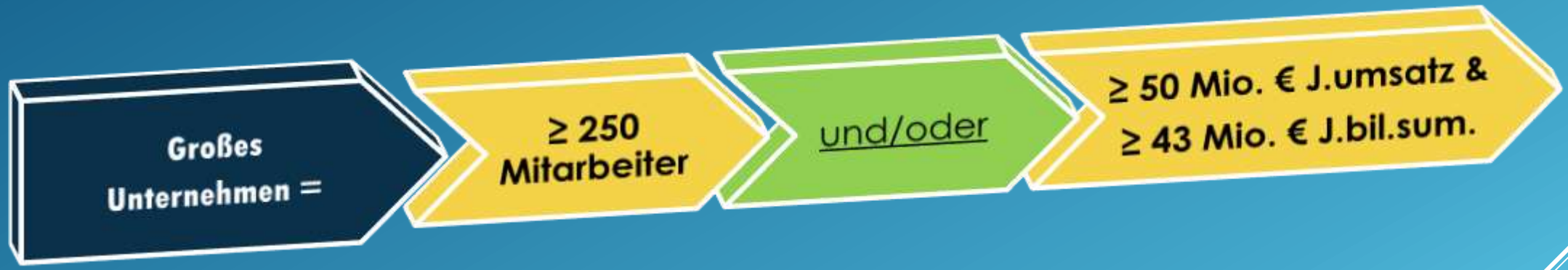
- Entspricht größtenteils den wesentlichen Einrichtungen in NIS-2, umfasst aber noch mehr.
- § 28 Abs. 2a NSI2UmsuCG:

Eine kritische Anlage ist eine Anlage, [die] den Sektoren Energie, Verkehr und Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, Ernährung, Digitale Infrastruktur, sowie Siedlungsabfallentsorgung angehört und die von hoher Bedeutung für das Funktionieren des Gemeinwesens ist, da durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungsengpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden; welche Anlagen im Einzelnen kritische Anlagen sind, bestimmt sich nach der Rechtsverordnung nach § 53 Absatz 1.

- Ernährung und Siedlungsabfallentsorgung sind im Gegensatz zu NIS-2 mit umfasst.
- Rechtsverordnung zu KRITIS-Dachgesetz soll später diese Anlagen spez. regeln.

Besonders wichtige Einrichtungen

- Kritische Anlagen, § 28 Abs. 3 Nr. 4 NSI2UmsuCG – Werden also trotz eigener Def. dazu „addiert“
- **<u>Groß</u>unternehmen gem. § 2 Abs. 1 Nr. 12** NSI2UmsuCG

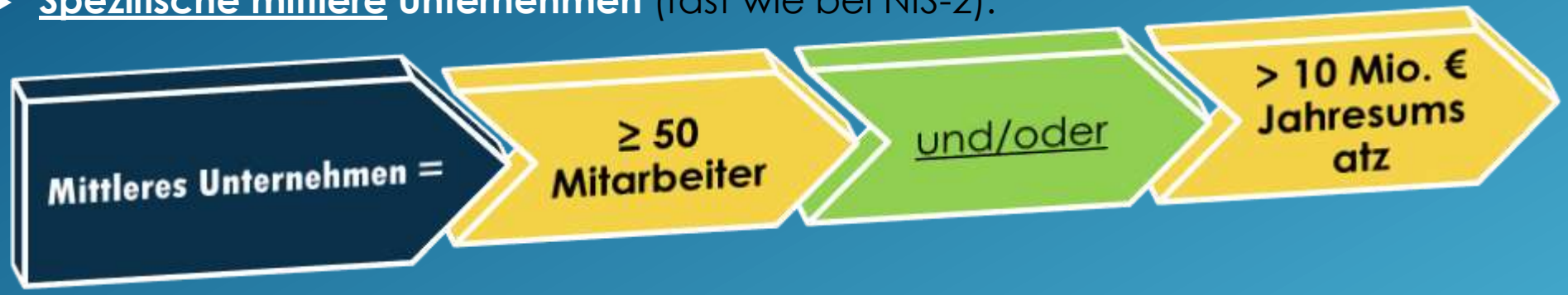


+ Sektor (wie bei „wesentlichen“ Einrichtungen bei NIS-2, also nichts neues…)
Energie, Verkehr und Transport, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasser, Abwasser, digitale Infrastruktur, Verwaltung von IKT-Diensten (B2B) oder Weltraum

…

Besonders wichtige Einrichtungen

- **<u>Spezifische mittlere</u> Unternehmen** (fast wie bei NIS-2):



+ spezifischer Sektor:

* gem. § 3 Nr. 44 TKG

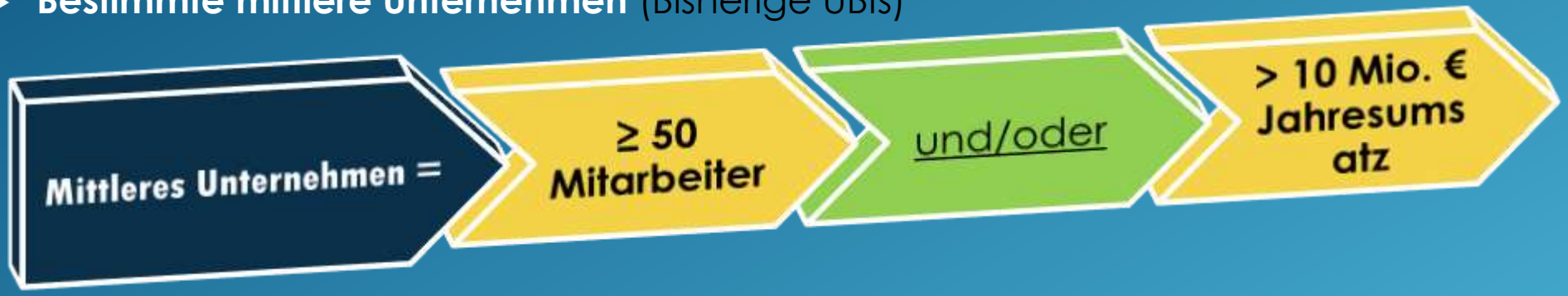
GoldbergUllrich
Rechtsanwälte

Besonders wichtige Einrichtungen

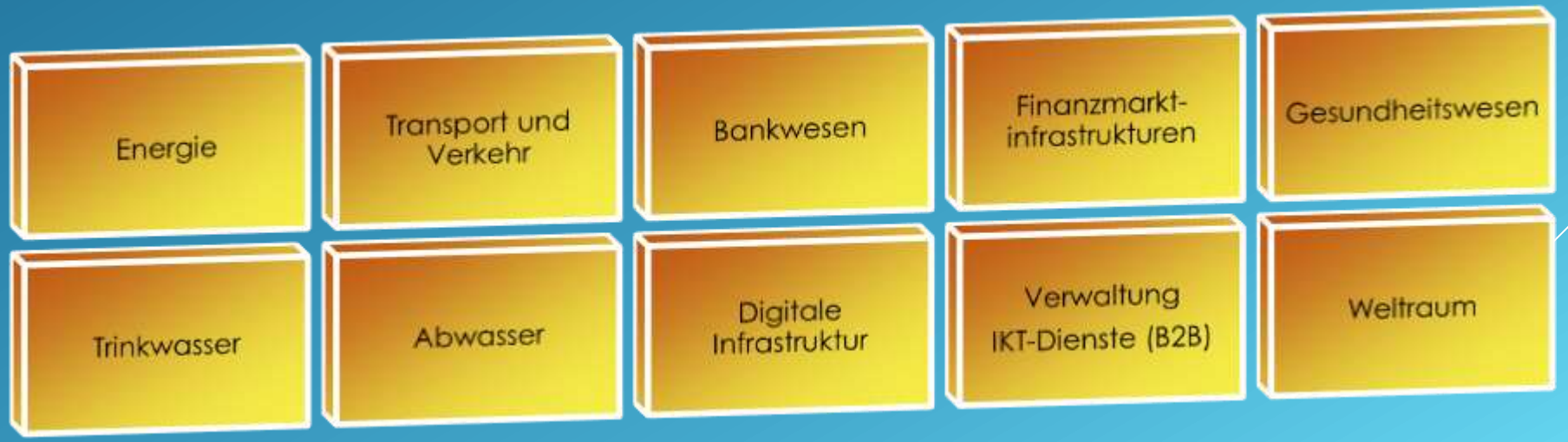
- **Einrichtungen** die gem. Rechtsverordnung nach § 53 Absatz 1 dem **Teilsektor Zentralregierung** des Sektors **öffentliche Verwaltung** angehören. (Diese Rechtsverordnung ist noch nicht erlassen worden)

Wichtige Einrichtungen

- **Bestimmte mittlere Unternehmen** (Bisherige UBIs)



+ aus bestimmten Sektoren (sollen in Rechtsverordnung noch ganz genau bestimmt werden)



GoldbergUllrich
Rechtsanwälte

Wichtige Einrichtungen

- **Mittlere <u>und</u> große Unternehmen bestimmter Sektoren**

= entspricht größtenteils der Einordnung von wichtigen Einrichtungen nach Anhang II von NIS-2

- **Genauere Definition nach später zu erlassender Rechtsverordnung**

Wichtige Einrichtungen

- **(unqualifizierte) Vertrauensdienstanbieter**
- **Besondere Sicherheitsdienste – Hersteller und Entwickler von…**

Gütern des Teils B der Kriegswaffenliste

vom Bundesamt zugelassenen Produkten mit IT-Sicherheitsfunktionen zur Verarbeitung staatlicher Verschlusssachen oder für die IT-Sicherheitsfunktion

wesentlichen Komponenten für IT-Sicherheitsfunktionen von Produkten zur Verarbeitung von Verschlusssachen

ZUKÜNFTIGE PFLICHTEN: WAS GILT MORGEN?

- Einsatz von **Systemen zur Angriffserkennung**
- **Überarbeitete Meldepflichten für „erhebliche Sicherheitsfälle“** gem. § 31 NIS2UmsuCG i.V.m. Art. 23 IV 1 NIS-2…

GoldbergUllrich
Rechtsanwälte

ERHEBLICHER SICHERHEITSVORFALL

- § 2 Abs. 1 Nr. 37 NSI2UmsuCG

„Sicherheitsvorfall“ [ist] ein Ereignis, das die Verfügbarkeit, Authentizität, Integrität oder Vertraulichkeit gespeicherter, übermittelter oder verarbeiteter Daten oder der Dienste, die über informationstechnische Umsetzung Systeme, Komponenten und Prozesse angeboten werden oder zugänglich sind, beeinträchtigt;

- § 2 Abs. 1 Nr. 10 NSI2UmsuCG

[Erheblich ist ein] Sicherheitsvorfall, der schwerwiegende Betriebsstörungen der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann; oder andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder beeinträchtigen kann,

ERWEITERTE MELDEPFLICHTEN

- Bislang: „Unverzügliche“ Meldung = Ohne schuldhaftes Zögern § 121 Abs. 1 BGB
- **Neu** (§ 31 Abs. 1 Nr. 1-4 NSI2UmsuCG):

1. **Erstmeldung**: **Spätestens 24 Stunden** nach Kenntnis von einem erheblichen Sicherheitsvorfall. (+ Info ob Verdacht auf rechtswidrige und/oder böswillige Handlungen zurückzuführen ist o. grenzüberschreitende Auswirkungen hat
2. **Zweitmeldung**: **Spätestens 72 Stunden** nach Kenntnis von erh. Sicherheitsvorfall – Bestätigung/Aktualisierung Infos aus Erstmeldung, erste Bewertung (Schweregrad, Auswirkungen, Kompromittierungsindikatoren)
3. Ggfs. **Zwischenmeldung**: Auf Ersuchen des BSI muss ggfs. Statusaktualisierung erfolgen
4. Ggfs. **Fortschrittsmeldung**: **Spätestens 1 Monat nach Zweitmeldung** (Übermittlung) muss eine Fortschrittsmeldung erfolgen, wenn Sicherheitsvorfall noch andauert.
5. **Abschlussmeldung**: **Spätestens 1 Monat nach Zweitmeldung** (Übermittlung) **ODER nach Abschluss d. Bearbeitung d. Sicherheitsvorfalls (nach Fortschrittsmeldung)**; Ausführliche Beschreibung d. Vorfalls, Schweregrad, Auswirkungen, Bedrohungsart, Ursache, Abhilfemaßnahmen, grenzüberschreitende Auswirkungen

GoldbergUllrich
Rechtsanwälte

ZUKÜNFTIGE PFLICHTEN: WAS GILT MORGEN?

- Einsatz von **Systemen zur Angriffserkennung**
- **Überarbeitete Meldepflichten für erhebliche Sicherheitsfälle** gem. § 31 NIS2UmsuCG i.V.m. Art. 23 IV 1 NIS-2
- Reaktionspläne und präventive Maßnahmen
- „Verhältnismäßige technische und organisatorische Maßnahmen müssen ergriffen werden, um Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse […] zu vermeiden und Auswirkungen von Sicherheitsvorfällen auf ihre oder andere Dienste zu vermeiden oder möglichst gering zu halten.“ - § 30 I NIS2UmsuCG
- …dabei Einhaltung des „Stands der Technik“…

ZUKÜNFTIGE PFLICHTEN: WAS GILT MORGEN?

- … § 30 II NIS2UmsuCG, Maßnahmen sollen unter Berücksichtigung der ggfs. einschlägigen europäischen und internationalen Normen, sowie der Umsetzungskosten […] + sonstige Faktoren (Risikoexposition, Einrichtungsgröße, Betreibergröße, Eintrittswahrscheinlichkeit, Schwere von Sicherheitsvorfällen, Auswirkungen) angemessen sein.
- … Bei KRITIS-Betreibern höhere Anforderungen
- … das umfasst folgende Maßnahmen nach § 30 IV NIS2UmsuCG:

GoldbergUllrich
Rechtsanwälte

MAßNAHMEN NACH § 30 IV NIS2MSUCG (teilweise neu)

1. Konzepte in Bezug auf die Risikoanalyse und Sicherheit für IT-Systeme
2. Bewältigung von Sicherheitsvorfällen (Umsetzung von Art. 6 Nr. 8 NIS-2)
3. **Aufrechterhaltung des Betriebs**, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement
4. Sicherheit der Lieferkette einschließlich sicherheitsbezogener Aspekte der Beziehungen zwischen den einzelnen Einrichtungen und ihren unmittelbaren Anbietern oder Diensteanbietern
5. Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von IT-Systemen, Komponenten und Prozessen, einschließlich Management und Offenlegung von Schwachstellen

MAßNAHMEN NACH § 30 IV NIS2UMSUCG (teilweise neu)

6. Konzepte und Verfahren zur Bewertung der Wirksamkeit von Risikomanagementmaßnahmen im Bereich der Cybersicherheit
7. Grundlegende Verfahren im Bereich der Cyberhygiene und Schulungen im Bereich der Cybersicherheit
8. Konzepte und Verfahren für den Einsatz von Kryptographie und Verschlüsselung
9. Sicherheit des Personals, Konzepte für die Zugriffskontrolle und Management von Anlagen
10. Verwendung von Lösungen zur Multi-Faktor-Authentifizierung oder kontinuierlichen Authentifizierung, gesicherte Sprach-, Video- und Textkommunikation sowie ggfs. gesicherte Notfallkommunikationsysteme innerhalb der Einrichtung

MAßNAHMEN NACH § 30 IV NIS2UMSUCG (teilweise neu)

- **Ausgenommen** von diesen Vorgaben sind gem. § 30 V NIS2UmsuCG i.V.m. Art. 21 V NIS-2:
- DNS-Diensteanbieter, TLD-Namensregister, Cloud-Computing-Dienstleister, Anbieter von Rechenzentrumsdiensten, Betreiber von Inhaltszustellnetzen, Anbieter von verwalteten Diensten, Anbieter von verwalteten Sicherheitsdiensten, Anbieter von Online-Marktplätzen, Online-Suchmaschinen und Plattformen für Dienste sozialer Netzwerke und Vertrauensdienstanbieter
- …diese bekommen bis zum 17.10.2024 einen speziellen Rechtsakt der Europäischen Kommission, der technische und methodische Anforderungen festlegt

MAßNAHMEN NACH § 30 IV NIS2UMSUCG (teilweise neu)

- **Besonders wichtige Einrichtungen** müssen die vorgenommenen **Maßnahmen dokumentieren und** zu einem vom BSI bei Registrierung festgelegten Zeitpunkt anschließend **alle 2 Jahre dem BSI nachweisen**, § 34 I NSI2UmsuCG **!**
- Ab wann?
  Frühestens zwei Jahre, spätestens drei Jahre nach Inkrafttreten des NSI2UmsuCG = 2025/2026?

GoldbergUllrich
Rechtsanwälte

ZUKÜNFTIGE PFLICHTEN: WAS GILT MORGEN?

- Pflicht zur Verwendung von IKT-Produkten/Diensten/Prozessen mit **Cybersicherheitszertifizierung** nach Art. 49 Verordnung (EU) 2019/881 gem. § 30 IX NSI2UmsuCG
- Besonders wichtige Einrichtungen sind 1 Jahr nach Inkrafttreten des NIS2UmsuCG verpflichtet, am Informationsaustausch gem. § 6 NSI2UmsuCG zu Schwachstellen etc. teilzunehmen, § 30 X NSI2UmsuCG – Das geht über Art. 29 NIS-2 hinaus!
- Wenn nicht schon vorher registriert als KRITIS: **Registrierungspflicht bei BSI**, § 32 NSI2UmsuCG, **spätestens 3 Monate**, nachdem man als registrierungspflichtig gilt! – BSI kann Registrierung auch selbst vornehmen, § 32 II NSI2UmsuCG !
- Bei **neuen KRITIS**: Registrierungspflicht **spätestens einen einzigen Werktag** nach Einstufung als KRITIS!

GoldbergUllrich
Rechtsanwälte

ZUKÜNFTIGE PFLICHTEN: WAS GILT MORGEN?

- Pflicht zur **Sicherstellung der jederzeitigen Erreichbarkeit** bei **KRITIS-Betreibern** (durch angegebene Kontaktmöglichkeiten bei BSI), § 32 IV NSI2UmsuCG
- **Besondere Registrierungspflichten** bei bestimmten Einrichtungen, § 33 NSI2UmsuCG
- Nur besonders wichtige Einrichtungen: **Unterrichtungspflicht** = BSI kann Einrichtung anweisen, alle Dienstempfänger über erheblichen Sicherheitsvorfall zu informieren, § 35 I NSI2UmsuCG ! – Auch durch Veröffentlichung im Internet (…)
- **Teilweise* Unterrichtungspflicht / Mitteilungspflicht** über alle Abwehr- und Abhilfemaßnahmen, die die potenziell betroffenen Dienstempfänger gg. Cyberbedrohung ergreifen können, § 35 II NSI2UmsuCG

* Sektoren: Bankwesen, Digitale Infrastruktur, Verwaltung von IKT-Diensten, Digitale Dienste

GoldbergUllrich Rechtsanwälte

ZUKÜNFTIGE PFLICHTEN: WAS GILT MORGEN?

- **Pflicht** zum **Führen** von **Datenbanken** für **Domain-Name-Registrierungsdaten**, § 51 NSI2UmsuCG
- Pflichten für **Geschäftsleitungen**…

GoldbergUllrich
Rechtsanwälte

PFLICHTEN GESCHÄFTSLEITUNG, § 38 NSI2UMSUCG (neu)

- Legaldefinition in § 2 Abs. 1 Nr. 11 NSI2UmsuCG vorgesehen:

„Geschäftsleiter“ [sind] diejenigen natürlichen Personen, die nach Gesetz, Satzung oder Gesellschaftsvertrag zur Führung der Geschäfte und zur Vertretung einer Einrichtung berufen sind.

- Pflicht zur **Billigung & Überwachung** der Maßnahmen gem. § 30 NSI2UmsuCG
  Aufgabe / Kompetenz kann nicht (mehr) an Dritte delegiert werden!
  Bei Nichtbeachtung & Schäden haftet die Geschäftsleitung der Einrichtung persönlich!
  Vergleiche und/oder Verzichte auf diese Ansprüche durch die Einrichtung sind unwirksam, § 38 III NSI2UmsuCG ! (Strenger als NIS-2!)
- **Geschäftsführung muss selbst die Fähigkeiten und Kenntnisse** für die Erreichung des digitalen Schutzniveaus durch Teilnahme an Schulungen **erwerben!**
- Sanktionen sind speziell für Geschäftsleitungen vorgesehen.

GoldbergUllrich
Rechtsanwälte

SANKTIONEN GESCHÄFTSLEITUNG, § 64 NSI2UMSUCG (neu)

- Bei **besonders wichtigen Einrichtungen** können
- **Sicherheitszertifizierungen ausgesetzt** werden, § 64 VI Nr. 1 NSI2UmsuCG (neu) (> Signifikant, weil Geschäftspartner Lieferkettensicherheit beachten müssen…)
- Den natürlichen Personen, die die **Geschäftsführung** oder **gesetzliche Vertretung** ausüben, kann im Fall von Verstößen und Fristversäumnissen zur Behebung die **Wahrnehmung der Leitungsaufgaben (vorübergehend) untersagt werden**, § 64 VI Nr. 2 NSI2UmsuCG
- Mögliche Konsequenzen:
  Übernimmt BSI vorübergehend die Geschäftsführung?
  …oder werden Leitungsaufgaben nur anderweitig delegiert?

GoldbergUllrich
Rechtsanwälte

BLEIBT DAS SO?

- **Kann sich noch ändern.** Bislang nur Entwurf.
- Durchaus schon jetzt (öffentlich) **kritische Meinungen**:

„[Mit den Regelungen zu Geschäftsleitungen] schießt das BMI aber deutlich über das Ziel hinaus. Die Motivation zur Übernahme der Geschäftsleitung dürfte so kaum gefördert werden. Führungspersonal mit geeigneter IT-Erfahrung, oder dem Willen sich diese anzueignen, ist ohnehin spärlich gesät. Die Regelung sollte gestrichen werden."

- Eren Basar, Wessing & Partner, Artikel „Cybersicherheit als Pflicht" vom 23.05.2023 im HANDELSBLATT
(…vertritt aber eher die Unternehmensseite…)

- …weshalb der Gesetzgeber sich in der Effektivität seiner Regelungen (Abschreckung) bestätigt fühlen und gerade deswegen diese Regelung genau so umsetzen könnte.
- **Es bleibt also spannend…**

GoldbergUllrich
Rechtsanwälte

STRAFEN, § 59 NSI2UMSUCG (neu)

- **Stufensystem** von Bußgeldern, je nach Tat
- **Abstufungen** im Einzelnen noch **unklar**. Begründung des Entwurfes enthält Plan für bis zu **20.000.000 €** Bußgeld (unabhängig von Einrichtungstyp). Dieser Wert findet sich aber noch nicht im Text des entworfenen Gesetzes wieder.
- **Sonst wie in NIS-2 vorgesehen:**
- **Einzelpersonen grds. bis 2.000.000 €**
- **Wichtige Einrichtungen: bis 7.000.000 € oder 1,4% des gesamten weltweiten Geschäftsjahresumsatzes (Vorjahr)**
- **Besonders wichtige Einrichtungen/KRITIS: bis 10.000.000 € oder 2% des gesamten weltweiten Geschäftsjahresumsatzes (Vorjahr)**

GoldbergUllrich
Rechtsanwälte

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

Homepage

Büro Wuppertal

• **Friedrichstr. 51,**
42105 Wuppertal

Telefon:
+49(0)202 / 9422900

Büro Solingen

• **Melanchthonstr. 9,**
42653 Solingen

Telefon:
+49(0)212 / 3827720

Büro Gelsenkirchen

• **Torgauer Str. 11,**
45886 Gelsenkirchen

Telefon:
+49(0)209 / 94703318

GoldbergUllrich
Rechtsanwälte

GoldbergUllrich

Rechtsanwälte