GRUNDRISS NIS-2-RICHTLINIE

„Netz- und Informationssystem-Sicherheit“

© Adam 121 Fotolia #151193550

Foto: © Darko Todorovic

KANZLEI FÜR IT- & WIRTSCHAFTSRECHT

DR. CHRISTINE KNECHT-KLEBER LL.M.

- IT- UND SOFTWARE-VERTRÄGE
- WIRTSCHAFTSRECHT (VERTRAGSPRÜFUNG / GESTALTUNG)
- DATENSCHUTZRECHT
- E-COMMERCE RECHT / WEBSHOP / AGB
- URHEBER- UND MARKENRECHT
- ONLINE MARKETING / SOCIAL MEDIA RECHT
- INNOVATIONS- UND KNOW-HOW-SCHUTZ

INHALT

1) Grundlagen NIS-Richtlinie / NIS-Gesetz
2) Neuerungen durch NIS-2-Richtlinie
3) Überblick To Do‘s für Unternehmen
4) Zusammenfassung / Ausblick

© 2024 Christine Knecht-Kleber

AUSGANGLAGE
NIS-RL / NIS-GESETZ

© Tomasz Zajda fotolia #149823674

AUSGANGSLAGE
WAS IST DIE NIS-RICHTLINIE?

- **NIS = S**icherheit von **N**etz- und **I**nformationssystemen ➔ Teil der europäischen Cybersecurity-Strategie
- **Ziel: Stärkung der Cyberresilienz von <u>kritischen</u> Infrastrukturen** wie Energie, Verkehr, Gesundheit und Finanzen
- Steigende Anzahl an Cyber-Attacken und Sicherheitsvorfällen
- **2016** EU-Gesetzgeber erlässt NIS-Richtlinie (RL (EU) 2016/1148)

© 2024 Christine Knecht-Kleber

AUSGANGSLAGE
NIS-RICHTLINIE - BISHER

- Vorschriften für **Betreiber wesentlicher Dienste in kritischen Sektoren** und **Anbieter digitaler Dienste**
- Umsetzung der NIS-RL in Österreich
  - 2018 NIS-Gesetz
  - 2019 NIS-Verordnung
    https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20010722

© 2024 Christine Knecht-Kleber

AUSGANGSLAGE

NIS-GESETZ – BETREIBER WESENTLICHER DIENSTE

- Energie
- Verkehr
- Bankwesen
- Finanzmarktinfrastrukturen
- Gesundheitswesen
- Trinkwasserversorgung
- Digitale Infrastrukturen

Kritische Infrastrukturen

© 2024 Christine Knecht-Kleber

AUSGANGSLAGE
NIS-GESETZ – ANBIETER DIGITALER DIENSTE

- Alle Unternehmen, die
  - Online-Marktplätze
  - Online-Suchmaschinen
  - Cloud-Computing-Dienste

  anbieten

© 2024 Christine Knecht-Kleber

AUSGANGSLAGE
NIS-GESETZ – PFLICHTEN

- Implementierung von **IT-Sicherheitsmaßnahmen** (§§ 17 und 21 NIS-G)
  - geeignete, verhältnismäßige, technische und organisatorische Sicherheitsmaßnahmen
  - risikoadäquat, Stand der Technik
- **Meldepflichten** (unverzüglich!) an Computer-Notfall-Team (§§ 19 und 21 NIS-G)
  www.nis.gv.at; www.cert.at; www.energy-cert.at

© 2024 Christine Knecht-Kleber

AUSGANGSLAGE
NIS-RL DEFIZITE

- Unterschiedlich starke Resilienz in den Mitgliedstaaten und Sektoren
- Unzureichende Cyber-Resilienz von Unternehmen
- Ineffektive Aufsicht und begrenzte Durchsetzung
- Mangelnde gemeinsame Cyber-Krisenreaktion

© 2024 Christine Knecht-Kleber

NEUERUNGEN DURCH NIS-2-RL

© Tomasz Zajda fotolia #149823674

NIS-2-RICHTLINIE
ÜBERBLICK

- Richtlinie (RL (EU) 2022/2555 vom 14. Dezember 2022
  über Maßnahmen für ein gemeinsames Cybersicherheitsniveau in der EU (NIS-2-RL)
- **Umsetzung in Österreich bis 17. Oktober 2024**
- Aktuell: Gesetzesentwurf NIS-2 Gesetz in Begutachtung bis 01. Mai 2024
  - https://www.parlament.gv.at/gegenstand/XXVII/ME/326
- DISCLAIMER: innerstaatliche Umsetzung noch offen

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
HAUPTZIELE

- Größerer Anwendungsbereich in Wirtschaft (mehr Sektoren)
- Systematische Konzentration auf größere, mittlere und kritische Akteure
- Angleichung der Sicherheitsanforderungen
- Angleichung der Aufsicht und Durchsetzung
- Straffung der Berichtspflichten

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
WAS ÄNDERT SICH?

- Aufhebung der Unterscheidung „Betreiber wesentlicher Dienste“ und „Anbieter Digitaler Dienste“
- Klassifizierung der erfassten Einheiten als **„wesentlich“** oder **„wichtig“**
- Ausdehnung des Anwendungsbereichs

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
ANWENDUNGSBEREICH (ART. 2)

- gilt für **öffentliche** oder **private** Einrichtungen
- in den in **Anhang I** oder **II** genannten **Sektoren** (…), die
- als **mittlere** oder **große Unternehmen** gelten (…), und
- ihre Dienste in der **EU** erbringen oder ihre Tätigkeiten dort ausüben

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
KLASSIFIZIERUNG

Anhang I – Wesentlich („*essential*“)

- **Energie** (Strom, Fernwärme, Öl, Gas, Wärme, Wasserstoff)
- **Gesundheit** (Versorger, Labore, F&E, Pharma)
- Transport (Luft, Schiene, Wasser, Straße)
- Banken und Finanzmärkte
- Wasser und Abwasser
- **Digitale Infrastrukturen** (Anbieter von Internet Exchange Points (IXP), DNS-Dienstanbieter, TLD-Namensregistrierungen, Anbieter von Rechenzentrumsdiensten, Anbieter von Cloud-Computing-Diensten, Anbieter von Inhaltsbereitstellungsnetzwerken, Anbieter von Vertrauensdiensten)
- Verwaltung von IKT-Diensten (B2B), Raumfahrt, öffentliche Verwaltung

Anhang II – Wichtig („*important*“)

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Chemie (Herstellung und Handel)
- Ernährung (Produktion, Verarbeitung, Vertrieb)
- Verarbeitendes/Herstellendes Gewerbe (Medizinprodukte; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
- **Anbieter digitaler Dienste**
- Forschung

Kupfer = neu gegenüber NIS 1
Schwarz fett = Ergänzungen im Sektor
Schwarz = NIS 1

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
PRÜFSCHEMA

1) Tätigkeit des Unternehmens in der EU ?
2) Entspricht Unternehmen einer genannten „Art“ in Spalte 3 von Anhang I oder Anhang II ?
3) Wenn ja, ist Unternehmen größer als Kleinunternehmen?

   ABER: Ausnahmen und Sonderregeln für Kleinunternehmen im Sektor „Digitale Infrastruktur“ und wenn als kritisch eingestuft
4) Ist Unternehmen wesentliche oder wichtige Einrichtung ?

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

AUSZUG ANHANG I

ANHANG I

SEKTOREN MIT HOHER KRITIKALITÄT

Sektor	Teilsektor	Art der Einrichtung
1. Energie	a)Elektrizität	— Elektrizitätsunternehmen im Sinne des Artikels 2 Nummer 57 der Richtlinie (EU) 2019/944 des Europäischen Parlaments und des Rates ([1]), die die Funktion „Versorgung“ im Sinne des Artikels 2 Nummer 12 jener Richtlinie wahrnehmen
		— Verteilernetzbetreiber im Sinne von Artikel 2 Nummer 29 der Richtlinie (EU) 2019/944
		— Übertragungsnetzbetreiber im Sinne des Artikels 2 Nummer 35 der Richtlinie (EU) 2019/944
		— Erzeuger im Sinne des Artikels 2 Nummer 38 der Richtlinie (EU) 2019/944
		— nominierte Strommarktbetreiber im Sinne des Artikels 2 Nummer 8 der Verordnung (EU) 2019/943 des Europäischen Parlaments und des Rates ([2])
		— Marktteilnehmer im Sinne des Artikels 2 Nummer 25 der Verordnung (EU) 2019/943, die Aggregierungs-, Laststeuerungs- oder Energiespeicherungsdienste im Sinne des Artikels 2 Nummern 18, 20 und 59 der Richtlinie (EU) 2019/944 anbieten
		— Betreiber von Ladepunkten, die für die Verwaltung und den Betrieb eines Ladepunkts zuständig sind und Endnutzern einen Aufladedienst erbringen, auch im Namen und Auftrag eines Mobilitätsdienstleisters
	b)Fernwärme und -kälte	— Betreiber von Fernwärme oder Fernkälte im Sinne des Artikels 2 Nummer 19 der Richtlinie (EU) 2018/2001 des Europäischen Parlaments und des Rates ([3])
	c)Erdöl	— Betreiber von Erdöl-Fernleitungen
		— Betreiber von Anlagen zur Produktion, Raffination und Aufbereitung von Erdöl sowie Betreiber von Erdöllagern und Erdöl-Fernleitungen
		— zentrale Bevorratungsstellen im Sinne des Artikels 2 Buchstabe f der Richtlinie 2009/119/EG des Rates ([4])
	d)Erdgas	— Versorgungsunternehmen im Sinne des Artikels 2 Nummer 8 der Richtlinie 2009/73/EG des Europäischen Parlaments und des Rates ([5])
		— Verteilernetzbetreiber im Sinne des Artikels 2 Nummer 6 der Richtlinie 2009/73/EG

Anhang I: 53 Arten
Anhang II: 14 Arten

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
SCHWELLENWERTE KMU

SCHWELLENWERTE *(Artikel 2)*

Kategorie des Unternehmens	Mitarbeiterzahl: Jahresarbeits-einheit (JAE)	Jahresumsatz	oder	Jahresbilanz-summe
Mittelgroß	< 250	≤ 50 Mio. EUR	oder	≤ 43 Mio. EUR
Klein	< 50	≤ 10 Mio. EUR	oder	≤ 10 Mio. EUR
Kleinst	< 10	≤ 2 Mio. EUR	oder	≤ 2 Mio. EUR

Quelle: Benutzerleitfaden zur Definition von KMU der EU-Kommission (Empfehlung 2003/361/EG)

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

GRUNDREGEL ANWENDUNGSBEREICH – ANHANG I

Sektoren	Große Unternehmen	Mittlere Unternehmen	Klein-unternehmen
Anhang I			
Energie / Verkehr / Bankwesen / Finanzmarktinfrastrukturen / Gesundheitswesen / Trinkwasser / Abwasser / Verwaltung von IKT-Diensten / Weltraum	wesentlich	wichtig	

Quelle: Mag. Vinzenz Heußler Bundeskanzleramt, Abt. I/8 Cyber Security

- Große Unternehmen: wesentlich
- Mittlere Unternehmen: wichtig
- Kleinunternehmen: Nicht im Anwendungsbereich

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

GRUNDREGEL ANWENDUNGSBEREICH – ANHANG II

Sektoren	Große Unternehmen	Mittlere Unternehmen	Klein-unternehmen
Anhang II			
Post- und Kurierdienste / Abfallbewirtschaftung / Lebensmittel / Verarbeitendes Gewerbes bzw. Herstellung von Waren / Anbieter digitaler Dienste / Forschung	wichtig	wichtig	

Quelle: Mag. Vinzenz Heußler Bundeskanzleramt, Abt. I/8 Cyber Security

- Große Unternehmen: wichtig
- Mittlere Unternehmen: wichtig
- Kleinunternehmen: Nicht im Anwendungsbereich

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

SONDERREGELN IM SEKTOR DIGITALE INFRASTRUKTUR

<table>
<tr><th>Sektor</th><th>Art der Einrichtung</th><th>Große Unternehmen</th><th>Mittlere Unternehmen</th><th>Klein-unternehmen</th></tr>
<tr><td rowspan="10">Digitale Infrastruktur</td><td>TLD-Namenregister</td><td colspan="3" rowspan="3">Wesentlich</td></tr>
<tr><td>DNS Diensteanbieter (ausgenommen Betreiber von Root-Nameserver)</td></tr>
<tr><td>Qualifizierte Vertrauensdiensteanbieter</td></tr>
<tr><td>Anbieter öffentlicher elektronischer Kommunikationsnetze oder elektronischer Kommunikationsdienste</td><td colspan="2">Wesentlich</td><td>Wichtig</td></tr>
<tr><td>Vertrauensdiensteanbieter</td><td>Wesentlich</td><td colspan="2">Wichtig</td></tr>
<tr><td>Betreiber von Internet-Knoten</td><td rowspan="4">Wesentlich</td><td rowspan="4">Wichtig</td><td rowspan="4"></td></tr>
<tr><td>Anbieter von Cloud-Computing-Diensten</td></tr>
<tr><td>Anbieter von Rechenzentrumsdiensten</td></tr>
<tr><td>Betreiber von Content Delivery Networks (CDN)</td></tr>
</table>

Quelle: Mag. Vinzenz Heußler Bundeskanzleramt, Abt. I/8 Cyber Security

© 2024 Christine Knecht-Kleber

PFLICHTEN FÜR UNTERNEHMEN

© Tomasz Zajda fotolia #149823674

© Jan Vasek Pixabay

NIS-2-RICHTLINIE

TO DO‘S FÜR UNTERNEHMEN

- Registrierungspflicht binnen 3 Monaten ab Inkrafttreten des NIS-G 2024
- Governance und Implementierung von Risikomanagementmaßnahmen
- Berichtspflichten und Meldepflichten
- Sicherstellung der Wirksamkeit der Risikomanagementmaßnahmen

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

GOVERNANCE (ART. 20)

- Verantwortung des **Top-Managements!**
- Pflicht zur regelmäßigen Teilnahme an Schulungen für Top-Management
- Einheitliche und umfangreichere Maßnahmen insbesondere iZm Risikomanagement
- risikobasiertes Vorgehen ist zu etablieren
    - verhältnismäßig, Stand der Technik, wirksam, angemessen

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

10 MINDESTMASSNAHMEN RISIKOMANAGEMENT (ART. 21)

- Konzepte in Bezug auf Risikoanalyse und Informationssicherheit
- Maßnahmen zur Bewältigung von Sicherheitsvorfällen
- Maßnahmen zur Aufrechterhaltung des Betriebs (Back-Up- und Krisenmanagement)
- **Sicherheit der Lieferkette** (ErwGr 85, 90) insb in Bezug auf Datenspeicherungs- und Verarbeitungsdienste, Softwarehersteller
- Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von Netz- und Informationssystemen – Offenlegung von Schwachstellen

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

10 MINDESTMASSNAHMEN RISIKOMANAGEMENT (ART. 21)

- Prozesse zur Bewertung der Wirksamkeit von Risikomanagementverfahren
  iZm Cybersicherheit
- Verfahren und Schulungen im Bereich der Cyberhygiene und Cybersicherheit
- Konzepte und Verfahren für den Einsatz von Kryptographie und ggf. Verschlüsselung
- Sicherheit des Personals, Konzept für die Zugriffskontrolle und Management von Anlagen
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung, gesicherter Kommunikation

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

BEISPIELE MASSNAHMEN CYBERHYGIENE

- Zero-Trust Prinzip
- Software Updates
- Gerätekonfiguration
- Netzwerksegmentierung
- Identitäts- und Zugriffsmanagement
- Sensibilisierung / Schulung der Mitarbeiter:Innen und Nutzer:Innen
- Bewertung der eigenen Cybersicherheitskapazitäten

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

MELDUNG SICHERHEITSVERLETZUNGEN (ART. 23)

- Wesentliche und wichtige Einrichtungen
- CSIRT „Computer Security Incident Response Team“
  - erste Benachrichtigung innerhalb **24 Stunden** (Frühwarnung)
  - zweite Benachrichtigung mit einer Analyse des Vorfalls innerhalb von **72 Stunden**
  - Abschlussbericht **nach einem Monat**
  - nachdem ein **schwerwiegender Vorfall** bekannt geworden ist

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE

MELDUNG SICHERHEITSVERLETZUNGEN (ART. 23)

- **Schwerwiegender Sicherheitsvorfall** liegt vor, wenn er
  - schwerwiegende Betriebsstörung der Dienste oder finanzielle Verluste für die betreffende Einrichtung verursacht hat oder verursachen kann
  - andere natürliche oder juristische Personen durch erhebliche materielle oder immaterielle Schäden beeinträchtigt hat oder kann
  - Siehe auch Definition „Sicherheitsvorfall“(Art. 6 Ziffer 6 NIS-2-RL)

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
GELDBUSSEN (ART. 34)

- Geldbußen: in jedem Einzelfall wirksam, verhältnismäßig und abschreckend
- Verstöße gegen Risikomanagementmaßnahmen (Art. 21) oder Meldepflichten (Art. 23)
- **Wesentliche Einrichtung:**
  mind. **EUR 10 Mio** oder **2 %** des weltweiten Umsatz des Vorjahres
- **Wichtige Einrichtung:**
  mind. **EUR 7 Mio** oder **1,4 %** des weltweiten Umsatz des Vorjahres

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
ZUSAMMENFASSUNG TO DO‘S

- Betroffenheit klären
- Ressourcen einplanen (personell und finanziell)
- Verantwortlichkeiten im Unternehmen klären/bestimmen
- Durchführung einer Risikoanalyse zur Identifizierung von Lücken
- Maßnahmen ermitteln und setzen – Geschäftskontinuität sicherstellen

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
AUSBLICK ÖSTERREICH

- Ministerialentwurf für NIS-G liegt zur Begutachtung vor
- Starke Orientierung an Wortlaut NIS-2-RL
- Nationale Verordnungen zur Spezifikation erwartet
- 17. Oktober 2024

© 2024 Christine Knecht-Kleber

NIS-2-RICHTLINIE
TIPPS & HILFESTELLUNG

Wie unterstützt die WKO Unternehmen?

- Informationen zu NIS2 - https://wko.at/nis2
- Online-Ratgeber NIS2 – https://ratgeber.wko.at/nis2
- Informationen zu Cybersicherheit – https://it-safe.at
  - ✓Checklisten
  - ✓Förderungen KMU DIGITAL
  - ✓Betrugswarnungen
  - ✓Suche nach IT-Security-Expert:innen

© Verena Becker/Bundessparte Information und Consulting /WKÖ

DISKUSSION / FRAGEN

VIELEN DANK!

Dr. Christine Knecht-Kleber LL.M.
Rechtsanwältin & CIPP/E

Campus V
Hintere Achmühlerstraße 1
6850 Dornbirn

kanzlei@dckk.at
www.dckk.at

© 2024 Christine Knecht-Kleber

© Karin Nussbaumer