Rechtliche Anforderungen der Richtlinie für ein hohes gemeinsames Cybersicherheitsniveau der Union NIS 2 RL

Sabine Proßnegg

Sabine.prossnegg@fh-joanneum.at

Disclaimer: Dieser Vortrag ersetzt keine rechtsfreundliche Beratung und basiert auf der Richtlinie der EU. Die gesetzliche Umwandlung ist in Österreich noch nicht erfolgt, Überlegungen zum Gesetzesentwurf sind nicht berücksichtigt.

FH JOANNEUM

FH | JOANNEUM
University of Applied Sciences

STUDIUM JOANNEUM ACADEMY FORSCHUNG NEWS ÜBER UNS

FH JOANNEUM

APPLIED COMPUTER SCIENCES

BUILDING, ENERGY & SOCIETY

ENGINEERING

HEALTH STUDIES

MANAGEMENT

MEDIA & DESIGN

FH JOANNEUM

Hochschule für Angewandte Wissenschaften

Assoziierte Professorin (FH)

Telefon
+43 316 5453 - 6364

E-Mail
sabine.prossnegg@fh-joanneum.at

Adresse
FH JOANNEUM
Software Design und Security
Werk-VI-Straße 46
Raum WS46a.01.115
8605 Kapfenberg
Österreich

Portrait

Ausbildung: Diplom- und Doktoratsstudium der Rechtswissenschaften an der KFU Graz (1 Jahr Erasmusstudium in Frankreich, 1 Monat ELSA Praktikum in der Türkei, 1. Abschnitt Europa, Sprachen, Wirtschaft); Postgraduate Study Master in Commercial Law at the Universities Glasgow & Strathclyde (joint degree).; Projektcoach (next level); Mediatorin (ARGE Bildungsmanagement Wien), seit 2006 eingetragene Mediatorin (BMJ);

Berufliche Stationen: Gerichtsjahr im Sprengel Graz; Placement at James R. Knowles (Glasgow); Rechtsanwaltskanzlei Wolf, Theiss und Partner (Wien); Steirische Wirtschaftsförderung GmbH (Graz); seit 2017 an der FH JOANNEUM GmbH (Kapfenberg);

Schwerpunkte:

IT-Recht, Datenschutzrecht, Vertragsrecht (SLA), Urheberrecht, Wirtschaftsmediation und Konfliktmanagement

Projekte (nur Leitung): Accelerator (EU Projekt), KAIT-Kapfenberg Accelerator für IT (SFG), Datensicherheit für KMU (DaSi) (FFG);

Lehrveranstaltungen

IT-Recht & Management (Master, BB)

FH JOANNEUM

KAIT

KAIT-Kapfenberg Accelerator & Incubator für IT

conicode

Conicode ist ein junges, agiles Unternehmen das individuelle Softwarelösungen im Bereich Green-Energy und Energiesimulationen umsetzt.

Vorstellungsvideo » read more »

New Horizons

New Horizons unterstützt Firmen bei der reibungslosen Ansiedlung (Relocation) von hochqualifizierten ausländischen Arbeitskräften. Diese sind besonders für manche Berufsfelder am österreichischen Arbeitsmarkt sehr gefragt.

read more »

FITAPP

Mit über 8 Millionen Downloads zählt FITAPP zu einer der erfolgreichsten App aus Österreich. FITAPP ermöglicht es verschiedene Sprachen über GPS aufzuzeichnen und diese in einem Feed zu teilen

read more »

KAIT stands for….

Green KAIT

Kapfenberger Accelerator & Incubator for Green IT

Melanie Dunst

Inpro Analytics

… People with ideas and with real enthusiasm

KAIT-KAPFENBERG Accelerator & Incubator for IT-products and IT-services / for Green IT-products & -services

FH JOANNEUM
University of Applied Sciences

Agenda

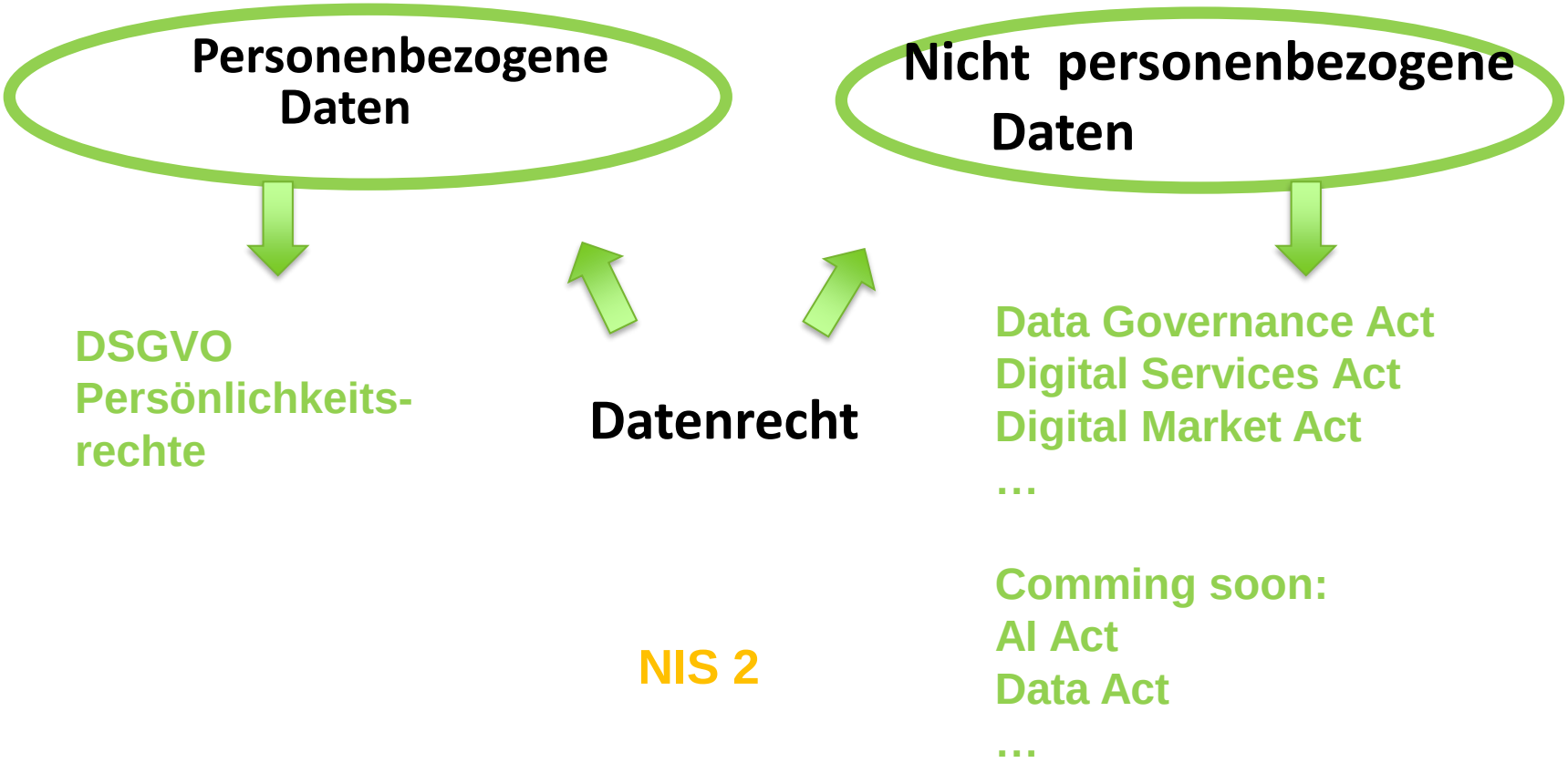
Einleitung

Bildnachweis: https://www.pexels.com/photo/postit-scrabble-to-do-todo-3299/

Der DIH SÜD bietet Qualifizierungen für Klein- und Mittelbetriebe im Bereich der Digitalisierung an. Der Besuch aller Weiterbildungen ist für Personen aus KMU kostenlos.

FH JOANNEUM
University of Applied Sciences

Digitalisierung



Medienneutralität des Rechts (allgemein)

FH JOANNEUM
University of Applied Sciences

Historie 10 Jahre NIS

NIS = Sicherheit von Netz- und Informationssystemen

Quelle: WKO, Vortrag Februar 2023.

FH JOANNEUM
University of Applied Sciences

Agenda

NIS (1)

Bildnachweis: https://www.pexels.com/photo/postit-scrabble-to-do-todo-3299/

NIS –> NIS Gesetz

- Die EU hat mit der NIS Richtlinie I von 2016/1148 und Österreich daraufhin mit der Umsetzung in nationales Recht in Form des NIS Gesetzes (NISG, StF: BGBl I Nr. 111/2018) einen wichtigen Grundstein für die Gewährleistung der Sicherheit der für die zunehmend digitalisierte Welt erforderlichen Strukturen geschaffen.

- Wichtige **Punkte:**

  - *Nationale Strategien* für die Cybersicherheit.
  - Schaffung einer *Kooperationsgruppe* für die strategische Zusammenarbeit und den Informationsaustausch zwischen den MS zu unterstützen.
  - Schaffung eines Netzwerks von *Computer-Notfallteams* (CSIRTs-Netzwerk).
  - Einführung von *Sicherheitsanforderungen und Meldepflichten*.
  - Nennung oder *Schaffung nationaler Behörden*, zentraler Anlaufstellen und CSIRTs.

NIS

- Zielgruppe: Unternehmen, die entweder kritische Infrastrukturen betreiben oder digitale Dienste bereitstellen; in geringerem Grade auch deren Partner (Zulieferer).
- Rollen und Aufgaben der zuständigen Behörden der NIS RL bzw im NISG gut umrissen, Auswirkungen auf Unternehmen war unklar und uneinheitlich.

Betroffene Sektoren im NIS (7)

NIS

- **Pflichten und Definitionen:**

- EU-weiter Aufbau nationaler Kapazitäten für Cyber-Sicherheit,
- enge Zusammenarbeit der Mitgliedstaaten (NIS Strategien)
- die Einhaltung von Mindestanforderungen an Sicherheitsvorkehrungen
- Meldepflichten für Betreiber wesentlicher Dienste (BwD, Operator of Essential Services OES) und
- Anbieter digitaler Dienste (AdD, Digital Service Providers DSP), sowie
- Sanktionen, die wirksam, angemessen und abschreckend sind.

CERT.at: nationales Computer Emergency Response Team, Ansprechpartner für IT-Sicherheit im nationalen Umfeld.

Bescheidzustellung.

CERT.at

FH JOANNEUM
University of Applied Sciences

Meldungen in NIS

- Sicherheitsvorfälle sind unverzüglich an CERT zu melden
- Standardisiertes elektronisches Format
  - Sicherheitsvorfall → Störung der Verfügbarkeit, Integrität, Authentizität oder Vertraulichkeit von Netz- & Informationssystemen zur Einschränkung oder zu Ausfall von erheblicher Auswirkung z.B. Cyberangriff, Stromausfall, Mitarbeiterversagen etc.
  - Erhebliche Auswirkung:
    - mehr als 5.000.000 Nutzerstunden nicht verfügbar
    - mehr als 100.000 Nutzer in der Union betroffen
    - Sachschaden in Höhe von mehr als 1 Mio € / Verstoß gegen die Vorgaben des NISG (Meldepflicht, Sicherheitsvorkehrungen, Mitwirkungspflichten)
- Strafen bis zu € 50.000, im Wiederholungsfall bis zu € 100.000

NIS

- *CERT.at:* nationales Computer Emergency Response Team, Ansprechpartner für IT-Sicherheit im nationalen Umfeld.
- *CSIRT: N*ationaler Rahmen für die Sicherheit von Netz- und Informationssystemen umfasst gemäß Art 9 der NIS I RL weiters sogenannte Computer-Notfallteams (Computer Security Incident Response Teams - CSIRTs), wobei die Richtlinie unter dem Begriff CSIRT auch CERTs versteht.
- *Cyberkrise:* Sicherheitsvorfall, der eine gegenwärtige und unmittelbare Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen darstellt und schwerwiegende Auswirkungen auf die Gesundheit, Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen nach sich ziehen kann.
- *Cyberkrisenmanagement*: Koordinierungsverfahren zur Bewältigung von Cyberkrisen.

NIS

- *Netz- und Informationssystem*: ein elektronisches Kommunikationsnetz im Sinne des § 3 Z 11 Telekommunikationsgesetz 2003.

- *Netz- und Informationssystemsicherheit (NIS)*: die Fähigkeit, Sicherheitsvorfällen vorzubeugen, zu erkennen, abzuwehren und zu beseitigen.

- Bescheidzustellung an die durch NIS I betroffenen Unternehmen erfolgte durch Behörde: binnen 2 Woche Bekanntgabe einer Kontaktstelle
- Nachweis der Anforderung mind alle 3 Jahre an BMI

NIS

- *§ 17 (1) Zur Gewährleistung der NIS haben BwD in Hinblick auf die Netz- und Informationssysteme, die sie für die Bereitstellung des wD nutzen, geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen zu treffen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.*

NIS Gesetz § 20

- Kritische Infrastrukuren und Zulieferer zu kritischen Infrastrukturen müssen ein dem (mit vernünftigem Aufwand feststellbaren) Risiko angemessenen Standard technischer und organisatorischer Sicherheitsvorkehrungen (TOMs) aufweisen. Geeignet und verhältnismäßig, dh idR einen höheren Standard als andere Unternehmen.
- TOMs zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer Netz- und Informationssysteme.
- Rahmen, um angemessen reagieren zu können: Meldungen, Kontakt mit CERTs und CSIRTs

NIS Gesetz Meldungen

- Inhalte der Pflichtmeldung:
  - Angaben zum Sicherheitsvorfall
  - Angaben zu den technischen Rahmenbedingungen, insbesondere vermutete Ursache, betroffene Informationstechnik usw.
  - Alles, was zum Zeitpunkt der Meldungen bekannt ist
  - Angaben über später bekanntgewordene Umstände sind nachzureichen
  - Verwendung festgelegter Kommunikationskanäle (Meldeformular etc.)

FH | JOANNEUM
University of Applied Sciences

NIS Gesetz Pflichten der Unternehmen

- Unternehmen haben präventive Sicherheitsvorkehrungen für Ihre Netz- und Informationssysteme zu treffen:
  - Sicherheit der Systeme & Anlagen
  - Bewältigung von Sicherheitsvorfällen.
  - Betriebskontinuitätsmanagement
  - Überwachung, Überprüfung & Erprobung
  - Einhaltung der internationalen Normen
  - Dokumentation

NIS Gesetz Pflichten

- Unternehmen haben präventive Sicherheitsvorkehrungen für Ihre Netz- und Informationssysteme zu treffen, Verpflichtung ist dem jeweiligen Sektor anzupassen
- Sicherheit der Systeme & Anlagen, Stand der Technik oder Stand der Wissenschaft und Forschung, Einhaltung der internationalen Normen
- Überwachung, Überprüfung & Erprobung
- 2 Wochen nach Zustellung des Bescheids muss Kontaktstelle für die NIS-Kommunikation bekanntgegeben werden
- Nachweis der Anforderungserfüllung alle drei Jahre an BMI
- Wichtigste Pflicht der Unternehmen ist, Meldungen von Sicherheitsvorfällen zu erstatten, dh Personen/Stellen dafür und Kontakt für CERTs und CSIRTs
- Bewältigung von Sicherheitsvorfällen, Betriebskontinuitätsmanagement

FH JOANNEUM
University of Applied Sciences

NIS Gesetz Rollen

Bundeskanzler (strategisch)

- Koordination der Erstellung einer Strategie
- Erstellung jährlichen Berichte
- Vertretung von Österreich
- Koordniation von PPP
- Betrieb des GovCERT
- Unterrichtung der Öffentlichkeit
- Ermittlung von BwD / Liste von BwD und Computer-Notfallteams

BMI (operativ)

- Betrieb einer zentralen Anlaufstelle (SPOC)
- Leitung von IKDOK und OpKoord
- Entgegennahme und Analyse von Meldungen
- Informationen zur Vorbeugung von Sicherheitsvorfällen
- Überprüfung der Sicherheitsvorkehrungen, Meldepflichten und qualifizierte Stellen

IKDOK

- Erörterung und Aktualisierung des Lagebildes
- Erörterung der Erkenntnisse
- Unterstützung des Koordinationsausschusses
- Austausch klassifizierter Informationen

OpKoord

- Erörterung eines gesamtheitlichen Lagebildes (inkl. freiwillige Meldungen)
- Verarbeitung personenbezogenen Daten erlaubt

NIS Gesetz Rollen

Zentrale Anlaufstelle

- operative Verbindungsstelle
- Gewährleistung der grenzüberschreitenden Zusammenarbeit
- Meldungen weiterleiten
- informiert internationale Anlaufstellen

Computer-Notfallteams

- Entgegennahme von Meldungen
- Weiterleitung von Meldungen an BMI
- Ausgabe von Frühwarnungen, Alarmmeldungen und Handlungsempfehlungen
- technische Unterstützung
- Lagebeurteilung
- Teilnahme an den Koordinierungsstrukturen

BwD und AdD

- Einhaltung von Sicherheitsvorkehrungen
- Erfüllung der Sich.Anforderungen nachweisen
- Meldepflicht für schwerwiegende Sicherheitsvorfälle
- Freiwillige Meldungen

Qualifizierte Stellen

- Zertifizierung und Überprüfung von BwD und AdD
- Kontrolle der Einhaltung der Erfordernisse für qualifizierte Stellen

NIS Fragestellungen

- Aus Sicht der Infrastrukturbetreiber müssen sich diese unter anderem mit folgenden Fragen kritisch auseinandersetzen:
  - Was passiert, wenn Daten gestohlen oder unerlaubt weitergegeben werden?
  - Was passiert, wenn das System ausfällt, außer Kontrolle gerät oder geändert wird?
  - Wie kann ich Fehlverhalten, Modifikationen oder Löschungen erkennen?
  - Wie erlange ich die Kontrolle über ein System zurück, das sich in einem unkontrollierbaren Zustand befindet?

NIS

- Dokumentation
- Weitere Einrichtungen (nicht BwD und AdD) können auf freiwilliger Basis Sicherheitsvorfälle melden, die erhebliche Auswirkungen auf die Verfügbarkeit der von ihnen angebotenen Dienste haben.
- Wichtig sind also Personen/Stellen, die die Meldepflicht erfüllen und die als Kontakt für die CERTs und CSIRTs zur Verfügung stehen, um den nationalen Lageplan und Maßnahmen rasch umsetzen / Umsetzung einleiten zu können.

FH JOANNEUM
University of Applied Sciences

Agenda

NIS 2

Bildnachweis: https://www.pexels.com/photo/postit-scrabble-to-do-todo-3299/

Warum NIS 2

- Das 5-Jahre Monitoring ergab Lücken in NIS bzw. der nationalen Umsetzungen
- Unzureichende Cyber-Resilienz von Unternehmen
  - Einige kritische Sektoren fehlten
  - Keine einheitlichen Anwendungsbereiche in den MS
  - Keine einheitlichen Sicherheitsanforderungen
  - Keine einheitlichen Meldepflichten
  - tw ineffektive Aufsicht / Durchsetzung
  - Resilienz, gemeinsame Lageerfassung und Krisenreaktion zu schwach

FH JOANNEUM
University of Applied Sciences

NIS 2 Richtlinie 2022/2555 und deren Ziele

Größeren Teil der Wirtschaft und Gesellschaft abdecken (**mehr Sektoren**)	Systematische Konzentration auf **größere, mittlere und kritische Akteure**	**Angleichung der Sicherheitsanforderungen**
Straffung der Berichtspflichten	Angleichung der **Aufsicht und Durchsetzung**	**Mehr operative Zusammenarbeit,** inkl. EU-Cyber-Krisenmanagement

Die NIS2 soll die Cybersicherheit in der EU vereinheitlichen. Hierzu **erhöht** sie **Sicherheitsanforderungen** an Unternehmen, weitet die Anzahl der betroffenen Unternehmen aus und adressiert die Absicherung von **Lieferketten** (Supply Chain Security), **erweitert Berichtspflichten** und gibt den zuständigen Behörden umfassendere **Aufsichts- und Durchsetzungsmechanismen** an die Hand (Strafrahmen!).

Quelle: WKO, Vortrag Februar 2023, Art 1 und 2 NIS II RL.

NIS 2 Betroffene Sektoren (Fact Sheet der EU, January 2023)

FH JOANNEUM University of Applied Sciences

Anhang I (= Sektoren mit hoher Kritikalität)	Anhang II (= sonstige kritische Sektoren)
Energie (Elektrizität, Fernwärme/Kälte, Öl, Gas und Wasserstoff)	Post- und Kurierdienste
Verkehr (Luft, Schiene, Schifffahrt, Straße)	Abfallbewirtschaftung
Bankwesen	Chemie (Herstellung und Handel)
Finanzmarktinfrastrukturen	Lebensmittel (Produktion, Verarbeitung, Vertrieb)
Gesundheitswesen (Gesundheitsdienstleister, EU-Referenzlaboratorien, Forschung und Herstellung von pharmazeutischen und medizinischen Produken und Geräte)	Verarbeitendes / Herstellendes Gewerbe (Medizinprodukten; Datenverarbeitungs-, elektronische und optische Geräte und elektronische Ausrüstungen; Maschinenbau; Kraftwagen und Kraftwagenteile und sonstiger Fahrzeugbau)
Trinkwasser	Anbieter digitaler Dienste (Suchmaschinen, Online-Marktplätze und soziale Netzwerke)
Abwasser	Forschung
Digitale Infrastruktur (IXP, DNS, TLD, Cloud-Computing, Rechenzentren, CDN, TSP und Anbieter öffentlicher elektronischer Kommunikationsnetze- und dienste)	
Verwaltung von IKT-Diensten (B2B)	
Öffentliche Verwaltung	
Weltraum	

Große und mittlere UN kritischer Sektoren sind wichtig.

Rot = Neuerungen gegenüber NIS1

Anbieter wesentliche Sektoren unabhängig von Ihrer Größe (Operators of Essental Services, OES): Große UN sind wesentlich, mittlere UN sind wichtig.

Ausnahme digitale Dienste, hier können auch KMU umfasst sein.

FH JOANNEUM
University of Applied Sciences

NIS 2 Pflichten für Unternehmen

Statt Bescheid

- > Selbstverantwortliche Meldung bei der Behörde

Kernpflichten sind

- Berichtspflichten
- Risikomanagementmaßnahmen
- Verantwortlichkeit des Top-Managements
- Pflichten je nach wesentlich oder wichtig Einrichtungen
- Umfassende Sicherheitsmaßnahmen (TOMs)

wko.at Online-Ratgeber - Cybersicherheitsrichtlinie - NIS2

FH JOANNEUM
University of Applied Sciences

NIS 2 Anwendungsbereich

Anwendungsbereich wird durch Größenschwellenwert bestimmt („size cap rule“):

- Große und Mittlere Unternehmen sind erfasst
- Kleinunternehmen sind in bestimmten Ausnahmefällen erfasst
- „Level Playing Field“
- Öffentliche oder private Einrichtungen

Prüfschema

- Diensteerbringung oder Tätigkeit in der EU (Art 2 Abs 1 NIS 2 RL)?
- Entspricht das Unternehmen einer in Spalte 3 von Anh I und Anh II genannten Art?
- Großes / Mittleres Unternehmen? Kleinunternehmen insb im Sektor digitale Infrastrukture erfasst, wenn sie als kritisch eingestuft werden (Art 2 Abs 2 NIS 2 RL
- wesentliche oder wichtige Einrichtung?

Quelle: WKO, Vortrag Februar 2023.

FH | JOANNEUM

KMU

- Empfehlung 2003/361/EG der EU-Kommission
  - **Kleines Unternehmen**: ein Unternehmen, das weniger als 50 Personen beschäftigt und dessen Jahresumsatz bzw. Jahresbilanz 10 Mio. EUR nicht übersteigt.
  - **Mittleres Unternehmen**: ein Unternehmen, das weniger als 250 Personen beschäftigen und die entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielen oder deren Jahresbilanzsumme sich auf höchstens 43 Mio. EUR beläuft.
  - **Großunternehmen**: Alle Unternehmen, sofern kein KMU.
- Benutzerleitfaden der EU-Kommission zur Definition von KMU

Wesentliche oder Wichtige Einrichtung?

- **Wesentliche Einrichtungen**
  - Alle im Anhang I angeführten Arten von Unternehmen, die groß sind.
- **Wichtige Einrichtungen**
  - Alle anderen Einrichtungen.
- **Sonderregeln:**
  - Sektor Digitale Infrastruktur

Quelle: WKO, Vortrag Februar 2023.

NIS 2

Für Unternehmen besonders relevant

Die 3 Säulen von NIS2

Fähigkeiten der Mitgliedstaaten	Kooperation und Informationsaustausch	Risikomanagement
Nationale Behörden	NIS-Kooperationsgruppe Peer-Review	Verantwortlichkeit des Top-Managements
Computer-Notfallteams (CERTs/CSIRTs)	CSIRTs-Netzwerk	Schulungen für Top-Management
Cyber-Krisenmanagement	EU-Cyberkrisennetzwerk (CyCLONe)	Unterscheidung wesentliche und wichtige Einrichtungen
Nationale Strategien	ENISA Cybersecurity Reports	Sicherheitsmaßnahmen
Rahmen für CVD (Coordinated Vulnerability Disclosure)	Europäisches Schwachstellenregister	Berichtspflichten

Rot = Neuerungen gegenüber NIS1

Quelle: WKO, Vortrag Februar 2023.

NIS 2

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 / öffentliche Verwaltung	wesentlich	wichtig	

- Große Unternehmen: Wesentlich
- Mittlere Unternehmen: Wichtig
- Kleinunternehmen: Nicht im Anwendungsbereich

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 / Chemie	wichtig	wichtig	

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

Quelle: WKO, Vortrag Februar 2023.

NIS 2 Sonderregeln im Sektor Digitale Infrastruktur

<table>
<tr><th>Sektor</th><th>Art der Einrichtung</th><th>groß</th><th>mittel</th><th>klein</th></tr>
<tr><td rowspan="7">Digitale Infrastruktur</td><td>TLD-Namenregister
qualifizierte Vertrauensdiensteanbieter</td><td colspan="3" rowspan="2">wesentlich</td></tr>
<tr><td>DNS Diensteanbieter (ausgenommen Betreiber von Root-Nameserver)</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: WKO, Vortrag Oktober 2023.

Zusammengefasst die wesentlichen Einrichtungen im NIS 2

Großunternehmen in den Bereichen:

- Energie, Verkehr, Wasserversorgung, Gesundheitswesen, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, ICT-service Management B2B, Chemie oder Weltraum
- Qualifizierte Vertrauensdienstanbieter, Domänennamenregister der Domäne oberster Stufe sowie DNS-Diensteanbieter
- Anbieter öffentlicher elektronischer Kommunikationsnetze oder öffentlich zugänglicher elektronischer Kommunikationsdienste
- Öffentlicher Verwaltung

- **-> können ohne Anlass geprüft werden** (ex ante)

Zusammengefasst die wichtigen Einrichtungen im NIS 2

- Alle unter den wesentlichen Einrichtungen genannten, die Mittlere Unternehmen sind;
- Post- & Kurierdienste
- Abfallbewirtschaftung
- Chemie (Herstellung und Handel)
- Lebensmittel (Produktion, Verarbeitung, Vertrieb)
- Hersteller bestimmter Waren (z.B. Medizinprodukte, Datenverarbeitungsgeräte, Maschinenbau…)
- Anbieter digitaler Dienste (Plattformen für Dienste sozialer Netzwerke)
- Forschungseinrichtungen

- **Achtung Digitale Infastruktur:**
- Großunternehmen **und** KMU
- Wesentlich oder wichtig

FH JOANNEUM
University of Applied Sciences

Zusammengefasst die wesentlichen Einrichtungen im NIS 2

wesentliche Einrichtung

ex-ante Aufsicht und ex-post-Aufsicht

- regelmäßige und gezielte Sicherheitsprüfungen
- Vor-Ort-Kontrollen und externe Aufsichtsmaßnahmen, Stichprobenkontrollen
- Bußgeldrahmen EUR 10 Mio oder 2 Prozent des weltweiten Umsatzes (je nachdem, welcher Betrag höher ist)

wichtige Einrichtung

ex-post-Aufsicht:

- nur bei begründetem Verdacht
- Vor-Ort-Kontrollen und externe nachträgliche Aufsichtsmaßnahmen
- EUR 7 Mio oder bei 1,4 Prozent des weltweiten Umsatzes

Unterscheidungsmerkmal: wesentlich vs. wichtig

Wesentliche Einrichtungen

große Einrichtungen laut Anhang I

Wichtige Einrichtungen

mittlere Einrichtungen Anhang I
große und mittlere Einrichtungen Anhang II

Digitale Infrastruktur

NIS 2, Risikomanagement für Unternehmen

- All-Gefahren-Ansatz
- NIS 2 Verordnung sieht umfangreiche Maßnahmen besonders im Risikomanagement vor (Governance Art 20f NIS 2 RL)
  -> Erstellung von Risikoanalyse- & Informationssicherheitskonzepten
- Maßnahmen zur Bewältigung von Sicherheitsvorfällen
  -> Notfallspläne
- Maßnahmen zur Aufrechterhaltung des Betriebs (wie Back-up-Management & Wiederherstellung)
- Konzepte für Zugriffskontrollen & Sicherheit des Personals
- Lieferkettensicherheit
- Verwendung von Lösungen zur Multi-Faktor-Authentifizierung, gesicherte Kommunikation etc.

NIS 2, Risikomanagement für Unternehmen

- Zero-Trust-Prinzip
- Software-Updates
- Gerätekonfiguration
- Netzwerksegmentierung
- Identitäts- und Zugriffsmanagement
- Sensibilisierung der Nutzer & Schulungen für Mitarbeiter
- Bewertung der eigenen Cybersicherheitskapazitäten
- …

Governance, Pläne und Schulung der Leitungsorgane gem Art 20 NIS 2 RL
Compliance gem Art 21 NIS 2 RL

NIS 2 Meldepflicht für Unternehmen

Cybersicherheitsvorfällen an Behörde **24 Stunden** grobe Infos (CERT/CSIRT)

Binnen **72 Stunden** ausführliche Einschätzung an Behörde

(inkl. Schweregrad, Auswirkungen & Kompromittierungsindikatoren)

1 Monat nach Meldung Ausführliche Beschreibung, Angaben zur Art der Bedrohung, Ursachen & Abhilfemaßnahmen

NIS 2

NIS2 wird unser Unternehmen betreffen. Entweder direkt oder als Lieferant.

CYBERRISK RATING by KSV1870

Stellen Sie sich vor, Ihr Geschäftspartner wird gehackt.

Was wollen Sie wissen?

1. Betrifft mich das? Kann mein Partner noch liefern? Wurden Daten von mir verloren?
2. Wer kann mir diese Fragen beantworten? Wo kann ich anrufen?
   ...und etwas später:
3. Wurde eigentlich im Vorfeld alles unternommen, um den Schaden zu verhindern?
   Was unternimmt er, um so etwas in Zukunft zu verhindern?

...und jetzt wissen Sie genau, was eigentlich von uns allen erwartet wird:

- Sie müssen wissen, für welche Daten ihr Unternehmen verantwortlich ist und was damit geschieht.
- Sie müssen alle bei Ihnen eingesetzten Geräte, Programme und Daten absichern. Ohne Ausnahme.
- Sie müssen auf Hackingangriffe vorbereitet sein und IT-Sicherheit mit Ihren Geschäftspartner proaktiv diskutieren - im Ernstfall genauso wie davor.

WKO bietet auf Webseite einen Check an: wko.at/NIS

KSÖ biete Cyber Rating Risk Beratung / Rating.

NIS 2 in der EU

Tochtergesellschaften, Konzerne und verbunden Unternehmen

- Immer das Land mit der strengsten NIS2 Auslegung für Bewertungen heranziehen
- Einzelfallprüfung (Konzerne) der Struktur → eigenständiges Unternehmen, Partnerunternehmen oder verbundenes Unternehmen
- Gesamthafte Betrachtung des Konzerns: NIS2-Anwendungsbereich gilt, wenn ein Teilbereich davon betroffen ist
- Konzerngesellschaften sind oft verbundene Unternehmen mit Beteiligungen über 50%
- Vermeidung von Aufspaltungen großer Unternehmen zur Umgehung von NIS2
- Heranziehung der Zahlen des gesamten Konzerns (Mitarbeiter:innen, Jahresumsatz, Jahresbilanzsumme)
- Beurteilung jeder Tochtergesellschaft mit losgelösten Zahlen nicht möglich

Vorbereitung auf NIS2:

- Anpassungen an Cybersicherheitspraktiken aufgrund erweiterter Compliance-Anforderungen
- Grenzüberschreitende Koordination für effektive Kommunikation und Einhaltung von Compliance-Standards
- Analyse der Lieferkettensicherheit, inklusive Lieferantenprüfung

NIS 2

Identifikation betroffener Unternehmen?

vorbehaltlich Gesetzesentwurf!!!

- **Unternehmen muss sich selbst als wesentlich oder wichtige Einrichtung einstufen**
- Bescheid (wie unter NIS-Gesetz derzeit) nur mehr in Ausnahmefällen
- Übermittlung von:
  - Namen, Anschrift
  - Kontaktdaten, inkl. E-Mail-Adressen, IP-Adressbereiche und Telefonnummern
  - Sektor und Teilsektor gemäß Anhang I
  - ggf. Mitgliedstaaten, in denen sie Die

10 Risikomanagementmaßnahmen

- Konzept **Risikoanalyse** und Sicherheit für Informati systeme
- **Bewältigung** von Sicherheitsvorfällen
- **Business Continuity** und Krise
- Lieferkettensicherh
- Sicherheits artung von IKT
- Konzepte u er Wirksamkeit von Risikomanagementmaßnahmen
- Cyberhygien zur Cybersicherheit
- **Kryptografie** u Verschlüsselung
- Sicherheit des **Personals**, Konzepte für die **Zugriffskontrolle**
- **Multi-Faktor-Authentifizierung**

- Stand der Technik
- Normen
- dem Risiko angemessen
- Kosten

WKO INFORMATION · CONSULTING

NIS Literatur & Links

- WKO Webinar zu NIS 2 → PowerPoint-Präsentation (wko.at) / Cybersicherheits-Richtlinie NIS 2 tritt in Kraft - WKO.at
- NIS2 Richtlinie der EU → L_2022333DE.01008001.xml (europa.eu)
- NIS1 Richtlinie der EU → L_2016194DE.01000101.xml (europa.eu)
- wko.at Online-Ratgeber - Cybersicherheitsrichtlinie - NIS2
- KMPG Präsentation NIS2 (10 Maßnahmen) → Wide screen template (wko.at)
- Cyberrisk Rating by KSV1870 → PowerPoint-Präsentation (wko.at)
- IT-Sicherheitshandbuch für KMU (wko.at) / Onlinesicherheit / Rechtliches und Dokumente (nis.gv.at) /
- Cybersicherheit in der EU: Was bedeutet die NIS2-Richtlinie für UN?
- NIS2 Europaweit → Cybersecurity-Revolution und viele Fragen: Die NIS2-Richtlinie bringt neue Herausforderungen und Chancen - PwC Legal Blog / NIS2 Europaweit → NIS-2: Alles Wissenswerte zur neuen Richtlinie – PwC
- www.it-safe.at = Initiative der WKO
- Cert.at

-> WKO.at bietet einen NIS II Check an

->KSÖ biete Cyber Rating Risk Beratung / Rating.

FH JOANNEUM
University of Applied Sciences

Datentransfer in Drittstaaten

Nachweis Sicherheit der Lieferkette nach NIS-Gesetz (derzeit)

Empfehlung NIS-Behörde für Betreiber wesentlicher Dienste:

- ÖISHB: Zusammenarbeit mit Externen, Evaluierung von Zertifizierungen, Lieferantenbeziehungen
- **ISO/IEC 27001: Information security in supplier relationships**
- IEC 62443 2-1: Supply chain security
- CIS CSC v8.0: Service Provider Management
- **KSÖ Cyber Risk Rating: Anforderungen für A bzw. B Rating**

Quelle: NIS Factsheet 9/2022

Links:
Good practises for supply chain security - ENISA
Threat Landscape for Supply Chain Attacks — ENISA (europa.eu)

FH | JOANNEUM
University of Applied Sciences

https://www.pexels.com/ pixabay

"Technology is a useful servant, but a dangerous master."

[Christian Lous Lange]

Für Wünsche und Anregungen:

Sabine.prossnegg@fh-joanneum.at

0316/5453 6364

DIHSÜD
Digital Innovation Hub