TÜV AUSTRIA GRUPPE

TÜV TRUST IT
TÜV AUSTRIA Group

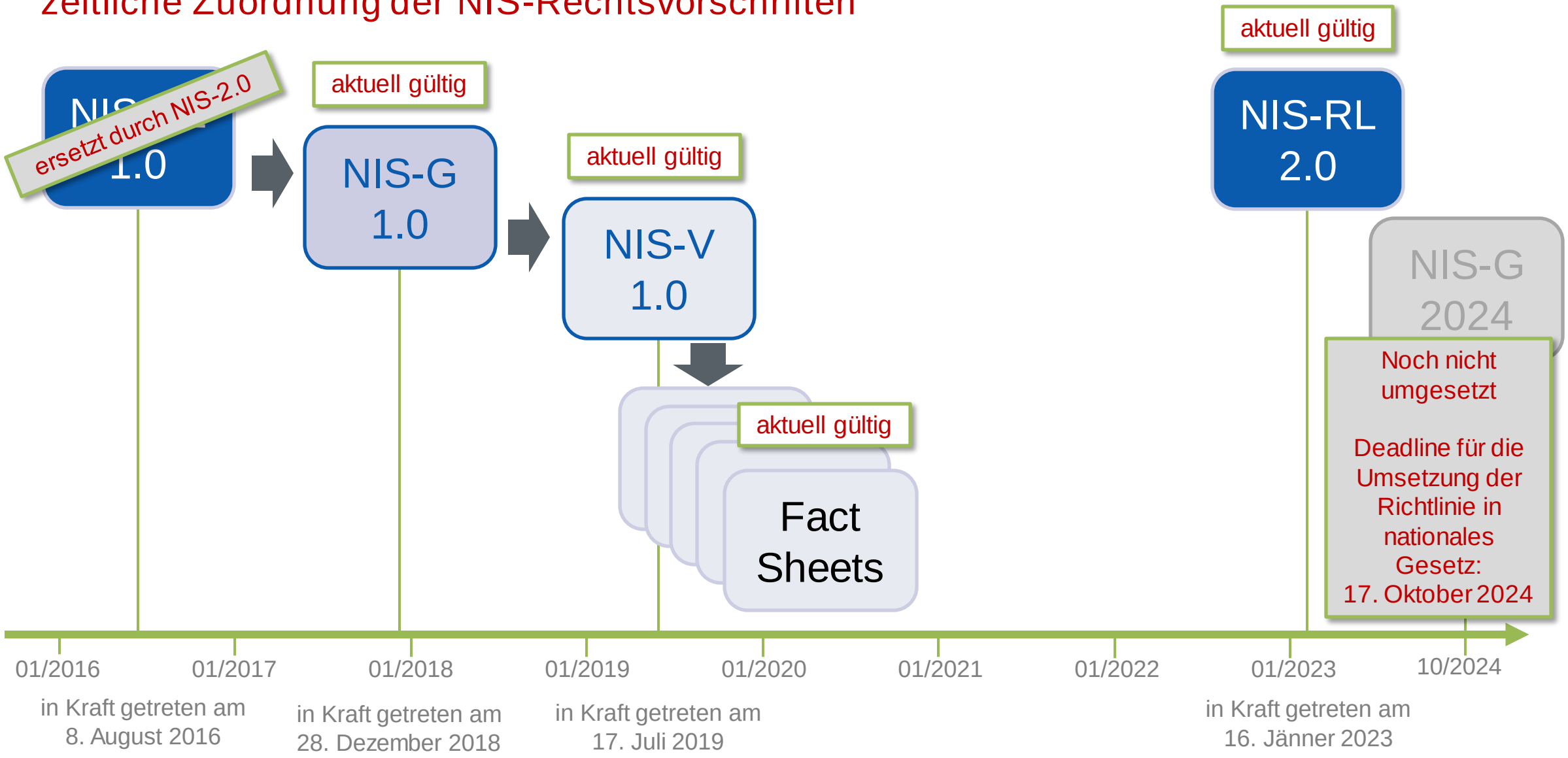
Anforderungen des Netz- und Informationssicherheitsgesetzes (NIS) für den Arbeiter-Samariter-Bund Österreichs (ASBÖ)

Markus Dörfler (H-I-P) / Alexander Zeppelzauer (TÜV AUSTRIA)

Juni 2024

NIS – Grundlagen

zeitliche Zuordnung der NIS-Rechtsvorschriften



Das NIS-Gesetz (NIS-G 1.0)

Sicherheitsanforderungen an BwD (Art 14)

- Umsetzung geeigneter und verhältnismäßiger technischer und organisatorischer Maßnahmen, um unter Berücksichtigung des Stands der Technik ein risikoangemessenes Sicherheitsniveau der Netz- und Informationssysteme zu gewährleisten
  - Risiko: mit vernünftigem Aufwand feststellbare Umstände oder Ereignisse, die potenziell nachteilige Auswirkungen auf die Sicherheit von Netz- und Informationssystemen haben
- Geeignete Maßnahmen, um Auswirkungen von Sicherheitsvorfällen vorzubeugen bzw. zu minimieren, damit die Verfügbarkeit der Dienste gewährleistet ist

➔ **Treffen der Maßnahmen abhängig vom Risiko und den Kosten**

NIS-G 2024

Juristischer Rahmen

- Die NIS-2-Richtlinie legt fest:
  - Nationale Cybersicherheitsstrategien müssen verabschiedet werden
  - Nationale Behörden für das Cyberkrisenmanagement, zentrale Anlaufstellen für Cybersicherheit und Computer-Notfallteams müssen benannt bzw. eingerichtet werden
  - Pflichten in Bezug auf das Cybersicherheitsrisikomanagement sowie Berichtspflichten für betroffene Einrichtungen
  - Nationale Aufsichts- und Durchsetzungspflichten
- Aktueller Entwurf eines Netz- und Informationssystemsicherheitsgesetz 2024 – NISG 2024 (Auszug):
  - Meldepflicht bei erheblichen Cybersicherheitsvorfällen an das CSIRT (§ 34)
  - Aufsichtsmaßnahmen durch die Cybersicherheitsbehörde (§ 38)
  - Strafen bei Verstößen bis zu EUR 10Mio oder 2% des weltweiten Jahresumsatzes

NIS-G 2024

Sektoren

Blau – neu aufgenommen in NIS-RL 2.0

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

NIS-G 2024

Betroffene Einrichtungen

- Anwendungsbereich wird durch Größenschwellwert („size cap rule“) bestimmt:
  - Mittlere und große Unternehmen (Kleinunternehmer nur in bestimmten Ausnahmefällen)
  - Öffentliche oder private Einrichtungen
  - Wesentliche oder wichtige Einrichtungen
  - Dienste werden in der Union erbracht oder Tätigkeiten werden dort ausgeübt

- Unternehmensgröße (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 beschäftigt und das entweder einen Jahresumsatz von höchstens 50 Mio. EUR erzielt, oder deren Jahresbilanzsumme sich höchstens auf 43 Mio. EUR beläuft.
  - **Großunternehmen**: alle Unternehmen, sofern kein KMU

Sicherheitsanforderungen (1/2)

- ✓ 4 Teile – 11 Domänen – 29 Sicherheitsvorkehrungen

Part	Domäne	Sicherheitsvorkehrung
Part 1 - Governance und Ökosystem	Governance und Risikomanagement	Risikoanalyse
		Sicherheitsrichtlinie
		Überprüfungsplan der Netz- und Informationssysteme
		Ressourcenmanagement
		Informationssicherheitsmanagementsystemprüfung
		Personalwesen
	Umgang mit Lieferanten und Dritten	Beziehungen mit Lieferanten und Dritten
		Leistungsvereinbarungen mit Lieferanten
Part 2 - Schutz	Sicherheitsarchitektur	Konfigurationsdokumentation
		Vermögenswerte
		Netzwerksegmentierung
		Netzwerksicherheit
		Kryptographie und Datensicherheit
	System Administration	Administrative Zugangsrechte
		Administrative Systeme und Anwendungen
	Identitäts- und Zugriffsmanagement	Identifikation und Authentifikation
		Autorisierung
	Systemwartung und Betrieb	Systemwartung und Betrieb
		Fernzugriff
	Physische Sicherheit	Physische Sicherheit

Sicherheitsanforderungen (2/2)

✓ 4 Teile – 11 Domänen – 29 Sicherheitsvorkehrungen

Part	Domäne	Sicherheitsvorkehrung
Part 3 - Verteidigung	Erkennung von Vorfällen	Erkennung
		Protokollierung und Monitoring
		Korrelation und Analyse
	Bewältigung von Vorfällen	Vorfallsreaktion
		Vorfallsmeldung
		Vorfallsanalyse
Part 4 - Resilienz	Betriebskontinuitätsmanagement	Betriebskontinuitätsmanagement
		Notfallmanagement
	Krisenmanagement	Krisenmanagement

NIS-Richtlinie 2.0 - Risikomanagement

Fokus

- Leitungsorgane
- Sicherheitsrichtlinien
- Risikomanagement Richtlinie und –prozess
- Verwaltung von Vermögenswerten
- Personalwesen
- Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen
- Sicherheit von Lieferketten
- Zugangssteuerung
- Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung
- Kryptographie
- Umgang mit Cybersicherheitsvorfällen

Risikomanagementmaßnahmen Cybersicherheit

- ✓ **Entwurf NIS-G 2024 § 32. (1) Wesentliche und wichtige Einrichtungen haben** geeignete und verhältnismäßige technische, operative und organisatorische Risikomanagementmaßnahmen in den Bereichen der **Anlage 3 umzusetzen**,…

Anlage 3

Risikomanagementmaßnahmen-Bereiche	
1.	Leitungsorgane
a.	Rollen und Verantwortlichkeiten der Leitungsorgane
2.	Sicherheitsrichtlinien
a.	Sicherheitsrichtlinien
b.	Funktionen, Aufgaben und Verantwortlichkeiten
3.	Risikomanagement
a.	Risikomanagementrichtlinie und -prozess
b.	Beurteilung der Effektivität von Risikomanagementmaßnahmen
c.	Überwachung der Einhaltung von Vorgaben
d.	Unabhängige Überprüfungen
4.	Verwaltung von Vermögenswerten
a.	Inventarisierung von Vermögenswerten
b.	Klassifikation von Vermögenswerten
c.	Handhabung von Vermögenswerten
d.	Umgang mit Wechseldatenträger
e.	Rücknahme oder Löschung von Vermögenswerten
5.	Personalwesen
a.	Sicherheit im Personalwesen
b.	Hintergrundüberprüfung
c.	Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses
d.	Disziplinarmaßnahmen
6.	Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen
a.	Bewusstseinsschaffung und Cyberhygiene
b.	Cybersicherheitsschulungen
7.	Sicherheit von Lieferketten
a.	Richtlinie zur Sicherheit von Lieferketten
b.	Lieferantenverzeichnis
8.	Zugangssteuerung
a.	Zugangssteuerungsrichtlinie
b.	Verwaltung von Zugriffsberechtigungen
c.	Privilegierte und administrative Zugänge
d.	Systeme und Anwendungen zur Systemadministration
e.	Identifikation
f.	Authentifikation
g.	Multi-Faktor-Authentifikation
9.	Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung
a.	Konfigurationsmanagement
b.	Änderungsmanagement und Wartung
c.	Umgang mit Schwachstellen und deren Offenlegung
d.	Sicherheitstests
e.	Patchmanagement

Umsetzungsmöglichkeiten eines NIS-kompatiblen ISMS

Mapping auf anerkannte, zertifizierbare Normen/Industriestandards

NIS-RL

NIS-G

NIS-V

Fact Sheets

Notwendigkeit zum Aufbau und Betrieb eines ISMS

wesentlicher Dienst

Welche Systeme sind betroffen?

ISMS- Ausprägung wählen, z.B.

Enterprise IT
Büroumgebung, Rechenzentrum-Infrastruktur

nach ISO 27001

Industrial IT
kritische Industriekomponenten

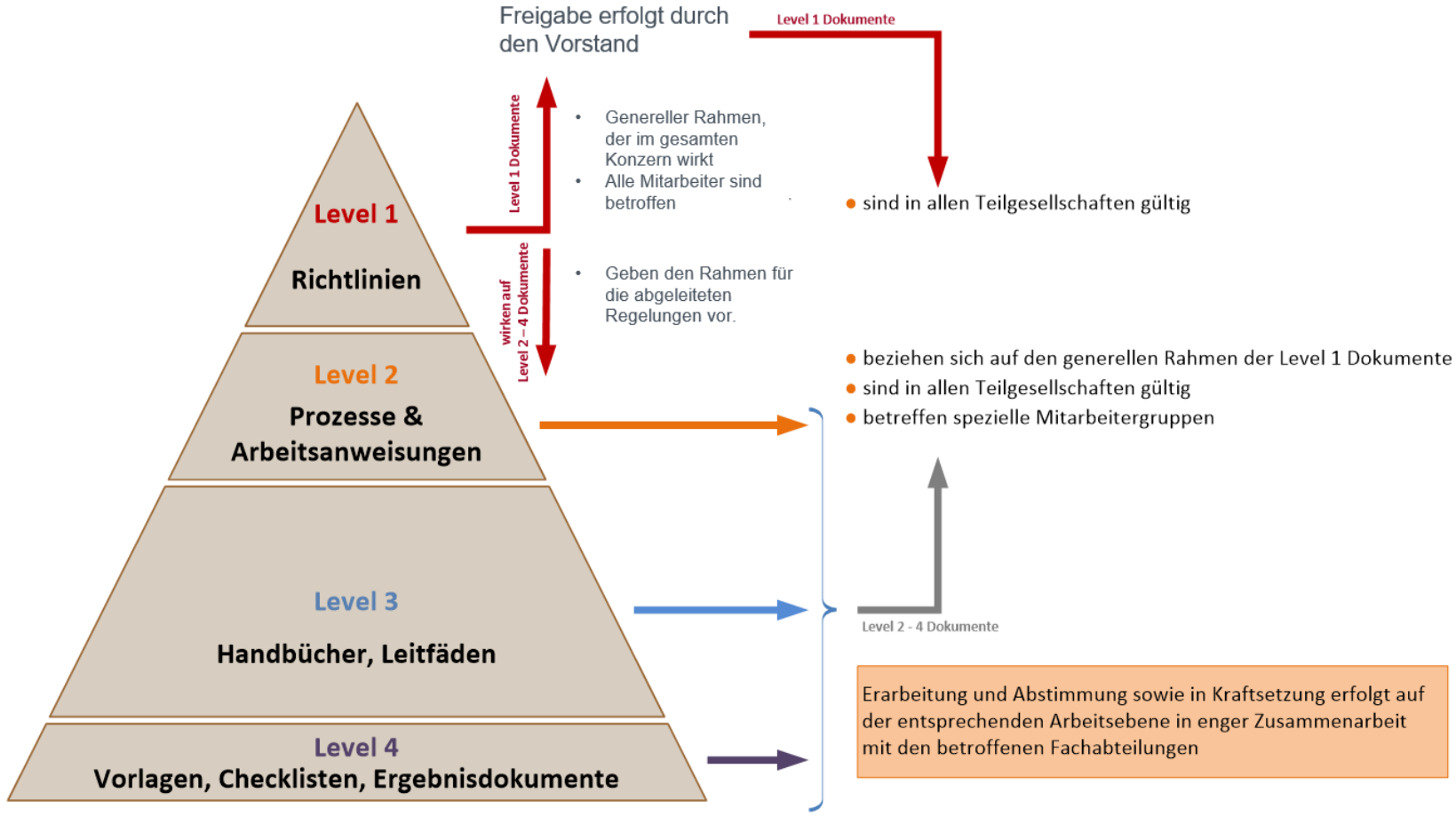
Risikommgt. ISO 27005

nach IEC 62443 Teil 2-1

Basisinfrastruktur
(Netze, Räumlichkeiten, Energie, etc.)

Richtlinien und Dokumente

✓ Beispiel: Umsetzung eines ISMS



Vielen Dank für Ihre Aufmerksamkeit!

Markus Dörfler
Rechtsanwalt Mag., LL.M., CIPP/E

Höhne, In der Maur & Partner Rechtsanwälte GmbH & Co KG

Mariahilfer Straße 20
1070 Wien
Tel.: +43 1 / 52175-41

markus.doerfler@h-i-p.at
www.h-i-p.at

Alexander Zeppelzauer
Vertriebsleiter

TÜV TRUST IT
TÜV AUSTRIA GmbH

TÜV AUSTRIA-Platz 1
2345 Brunn am Gebirge
Mobil: +43 664 60454 6276

alexander.zeppelzauer@tuv.at
www.it-tuv.com