Die Verrechtlichung der IT

CIS-Compliance-Summit 2026

CERHA HEMPEL

Boris Treml, 8.9.2026

CERHA HEMPEL

Ing. Mag. Boris Treml, LL.M.
Senior Associate

+43 1 514 35 0
boris.treml@cerhahempel.com

Zugelassen als

- Rechtsanwalt, Österreich (2023)

Ausbildung

- Universität Wien (Mag. iur. 2013)

Tätigkeitsschwerpunkte

IT & Datenschutz
IT-Sicherheitsrecht

Sprachen

- Deutsch
- Englisch

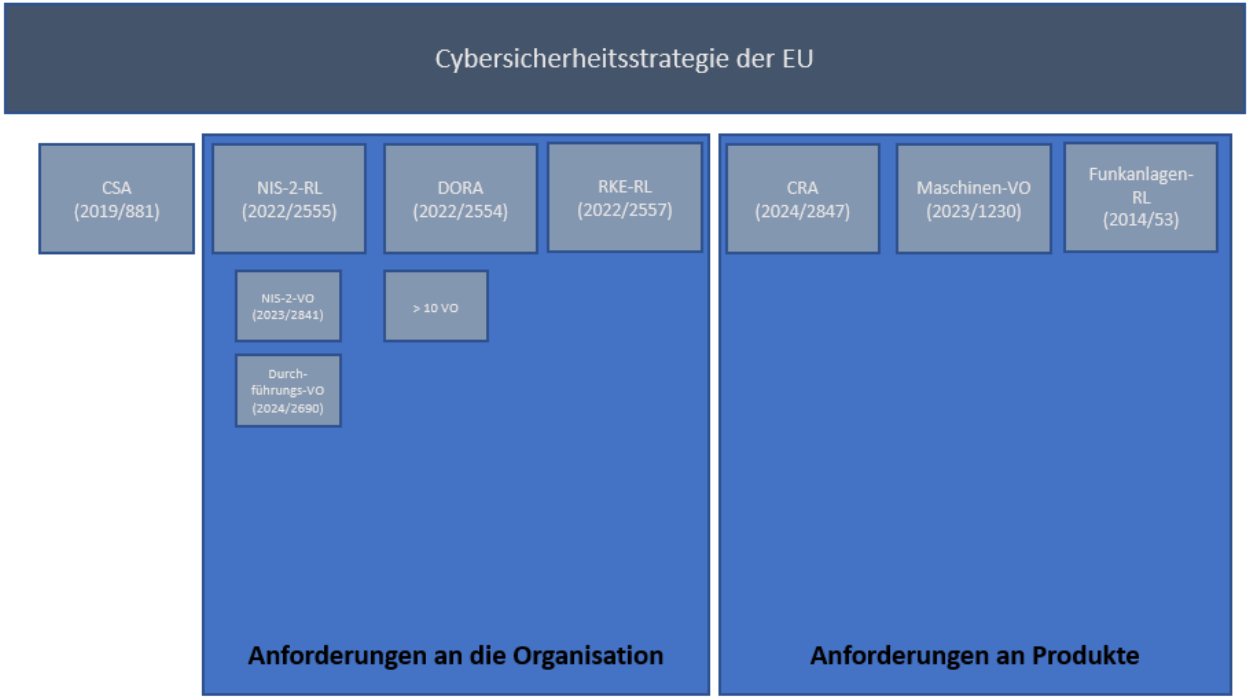
1. Die Verrechtlichung der IT
2. Von der „klassischen“ Informationssicherheit zur „regulierten“ Informationssicherheit
3. Fazit

Daten & Datenschutz	Cybersicherheit	Produktsicherheit	E-Commerce & Verbraucherschutz
ePrivacy RL RL (EG) 2002/58	**Europäischer Kodex für die elektronische Kommunikation (EECC)** RL (EU) 2018/1972	**Produkthaftungs-RL** RL (EWG) 1985/374	**AGB-RL** RL (EWG) 1993/13
EU-Statistikverordnung VO (EG) 2009/223	**Cybersecurity Act** VO (EU) 2019/881	**Spielzeugrichtlinie** RL (EG) 2009/48	**Preisangaben-RL** RL (EG) 1998/6
Datenschutz-Grundverordnung (DSGVO) VO (EU) 2016/679	**Verordnung zur Errichtung des Europäisches Kompetenzzentrum für Cybersicherheit** VO (EU) 2021/887	**Normungsverordnung** VO (EU) 2012/1025	**E-Commerce-RL** RL (EG) 2000/31
EU-Datenschutz-VO VO (EU) 2018/1725	**NIS-2-RL** RL (EU) 2022/2555	**Funkanlagen-RL (RED)** RL (EU) 2014/53	**Richtlinie über unlautere Geschäftspraktiken** RL (EG) 2005/29
Free-Flow-of-Data-VO VO (EU) 2018/1807	**EU-Cybersicherheits-VO** VO (EU) 2023/2841	**eIDAS Verordnung** VO (EU) 2014/910	**Verbraucherrechterichtlinie** RL (EU) 2011/83
Open-Data-Richtlinie VO (EU) 2019/1024	**EU-Informationssicherheits-VO** 2022/0084(COD)	**Single Digital Gateway-Verordnung** VO (EU) 2018/1724	**Richtlinie über die elektronische Rechnungsstellung bei öffentlichen Aufträgen** RL (EU) 2014/55
Data Governance Act (DGA) VO (EU) 2022/868	**Cyber Resilience Act** VO (EU) 2024/2847	**EU-Produktsicherheits-VO (GPSR)** VO (EU) 2023/988	**Verordnung über die Zusammenarbeit zwischen den für die Durchsetzung der Verbraucherschutzgesetze zuständigen nationalen Behörden** VO (EU) 2017/2394
Data Act VO (EU) 2023/2854	**Cyber Solidarity Act** VO (EU) 2025/38	**MaschinenVO** VO (EU) 2023/1230	**Geoblocking-VO** VO (EU) 2018/302
Verordnung für ein interoperables Europa VO (EU) 2024/903		**Verordnung über künstliche Intelligenz** VO (EU) 2024/1689	**Digitale-Inhalte-Richtlinie** RL (EU) 2019/770
Verordnung zur Kurzzeitvermietung VO (EU) 2024/1028		**Ökodesign-Verordnung** VO (EU) 2024/1781	**Warenkauf-Richtlinie** RL (EU) 2019/771
Verordnung über den Europäischen Gesundheitsdatenraum VO (EU) 2025/327		**KI-Haftungs-RL** 2022/0303(COD)	**Digital Services Act** VO (EU) 2022/2065
Verordnung zur Festlegung zusätzlicher Verfahrensregeln für die Durchsetzung der DSGVO VO (EU) 2025/2518			**Verordnung über die Transparenz und das Targeting politischer Werbung** VO (EU) 2024/900
Zugriff auf Fahrzeugdaten, Funktionen und Ressourcen			**Richtlinie über gemeinsame Vorschriften zur Förderung der Reparatur von Waren** RL (EU) 2024/1799
GreenData4all-Programm			**Überarbeitung der Verordnung über die Zusammenarbeit im Verbraucherschutz**

Daten & Datenschutz	Cybersicherheit	Produktsicherheit	E-Commerce & Verbraucherschutz
Europäische Exekutivagentur für Gesundheit und Digitales (HaDEA) (EU) 2021/173	**CERT-EU** (EU, EURATOM) 2023/2841	**KI-Büro der Europäischen Kommission** 2021/0106 (COD)	**European Commission (DG JUST): Unit B.3** Consumer Enforcement and Redress
Europäischer Datenschutzausschuss (EDSA) (EU) 2016/679	**Europäisches Kompetenzzentrum für Cybersicherheit** (EU) 2021/887	**Gateway-Koordinierungsgruppe** (EU) 2018/1724	**Europäisches Gremium für digitale Dienste** (EU) 2022/2065
Europäischer Datenschutzbeauftragter (EDSB) (EU) 2018/1725	**Europäische Verteidigungsagentur** (CFSP) 2015/1835	**Europäischer Ausschuss für künstliche Intelligenz** 2021/0106(COD)	**Netzwerk für Verbraucherschutz (CPC)** (EU) 2017/2394
Ausschuss für das Europäische Statistische System (EC) 2009/223	**Agentur der Europäischen Union für Cybersicherheit (ENISA)** (EU) 2019/881	**Europäisches Komitee für elektrotechnische Normung (CENELEC)** (EU) 2012/1025	**European Consumer Centres Network** (EU) 2021/690
Europäisches Dateninnovationsgremium (EU) 2022/868, (EU) 2023/2854	**Europäischer Cyber-Schild** 2023/0109(COD)	**Europäisches Komitee für Normung (CEN)** (EU) 2012/1025	**Consumer Safety Network** (EU) 2023/988
Gremium für ein interoperables Europa (EU) 2024/903	**Europäische Cybersicherheits-Zertifizierungsgruppe** (EU) 2019/881	**Europäisches Institut für Telekommunikationsnormen (ETSI)** (EU) 2012/1025	
Gremium für den Europäischen Gesundheitsdatenraum 2022/0140(COD)	**Interinstitutional Cybersecurity Board (IICB)** (EU, Euratom) 2023/2841		
	Kooperationsgruppe gemäß NIS-2 (EU) 2022/2555		
	Interinstitutional Information Security Coordination group 2022/0084(COD)		
	Netz nationaler Koordinierungszentren (EU) 2021/887		
	CSIRTs-Netzwerk (EU) 2022/2555		
	EU-CyCLONe (EU) 2022/2555		

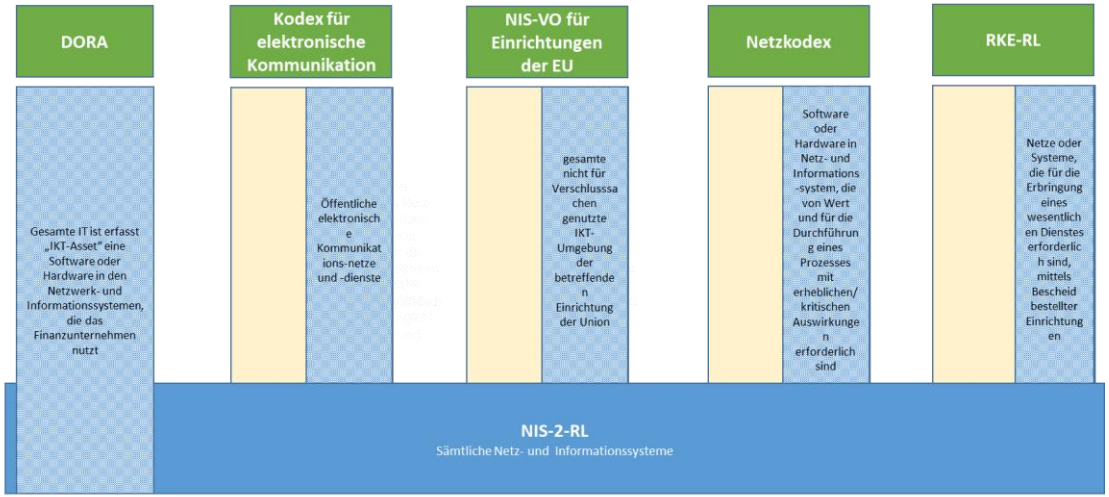
Cybersicherheitsrecht

Strukturierung



Cybersicherheitsrecht

Das Recht der Organisation



Von der sektorspezifischen Regulierung erfasste IT-Systeme

Sonstige IT-Systeme, die nicht von der sektorspezifischen Regulierung erfasst sind

Die Konsequenz

LVwG
LANDESVERWALTUNGSGERICHT NIEDERÖSTERREICH

3109 St. Pölten / Rennbahnstraße 29
Telefon: +43 2742 90590 / Fax: +43 2742 90590 15540
E-Mail: post@lvwg.noel.gv.at / www.lvwg.noel.gv.at
Datenschutz: www.lvwg.noel.gv.at/datenschutz

Geschäftszahl:
LVwG-S-331/001-2025

St. Pölten, am 27. März 2025

IM NAMEN DER REPUBLIK

Das Landesverwaltungsgericht Niederösterreich erkennt durch den Richter Mag. Schnabl über die Beschwerde des Herrn A, ***, ***, vertreten durch B, Rechtsanwalt in ***, ***, gegen das Straferkenntnis des Bürgermeisters der Stadt *** vom 17.01.2025, GZ. ***, betreffend Bestrafungen nach dem Netz- und Informationssystemsicherheitsgesetz (NISG),

zu Recht:

1. Der Beschwerde wird gemäß § 50 Verwaltungsgerichtsverfahrensgesetz (VwGVG) Folge gegeben, das angefochtene Straferkenntnis aufgehoben und das Verwaltungsstrafverfahren gemäß § 45 Abs. 1 Z. 1 Verwaltungsstrafgesetz 1991 (VStG) eingestellt.

2. Gegen dieses Erkenntnis ist gemäß § 25a Verwaltungsgerichtshofgesetz 1985 (VwGG) eine ordentliche Revision an den Verwaltungsgerichtshof nach Art. 133 Abs. 4 Bundes-Verfassungsgesetz (B-VG) nicht zulässig.

Entscheidungsgründe:

1. Zum verwaltungsbehördlichen Verfahren:

Mit dem Straferkenntnis des Bürgermeisters der Stadt *** vom 17.01.2025, GZ. ***, wurde dem Beschwerdeführer Folgendes zur Last gelegt:

Tatbeschreibung:

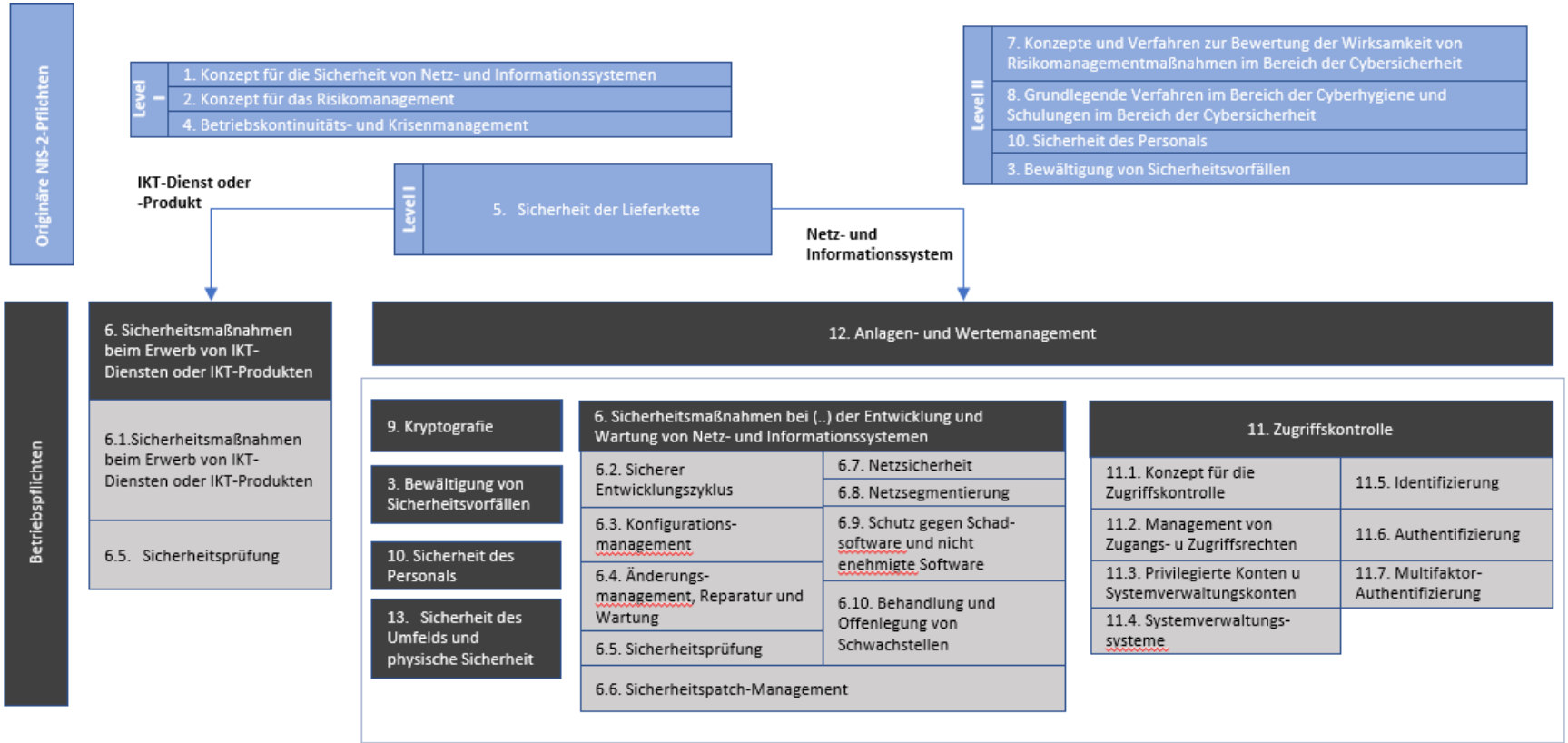
1. Als Geschäftsführer der C GmbH (FN ***) haben Sie es zu verantworten, dass nicht fristgerecht eine Dokumentation oder Vorgaben für erlaubte Kommunikation und Schnittstellen zwischen den Netzwerksegmenten unterschiedlicher Schutzklassen umgesetzt und es keine dokumentierte Verfahren die Zugriff auf Netzwerke, die Überwachung derselben oder auch Datenaustausch über entsprechende Netzwerksegmente hinweg definieren, erstellt wurden und wurde dies gegenüber dem Bundesminister für Inneres nicht nach § 17 Abs. 1 u. 3 NISG fristgerecht nachgewiesen.

2. Als Geschäftsführer der C GmbH (FN ***) haben Sie es zu verantworten, dass der Netzwerkverkehr innerhalb des Netzwerks weitgehend ungefiltert ist, da der Verkehr zwischen Netzwerksegmenten nicht über Firewalls funktioniert und daher wurde eine Filterung des Verkehrs auch zwischen Netzwerksegmenten, dem Stand der Technik angemessen, nicht fristgerecht umgesetzt.

3. Als Geschäftsführer der C GmbH (FN ***) haben Sie es zu verantworten, dass kein implementiertes System, das auf Basis von Protokolldaten in der Lage ist, sicherheitsrelevante Vorfälle zu erkennen und kein Prozess oder Informationssystem, dass es ermöglichen würde Protokolldaten zu korrelieren, analysieren und in Folge auch Vorfallsbearbeitung damit abzuhandeln, existiert.

NIS-2-Regime

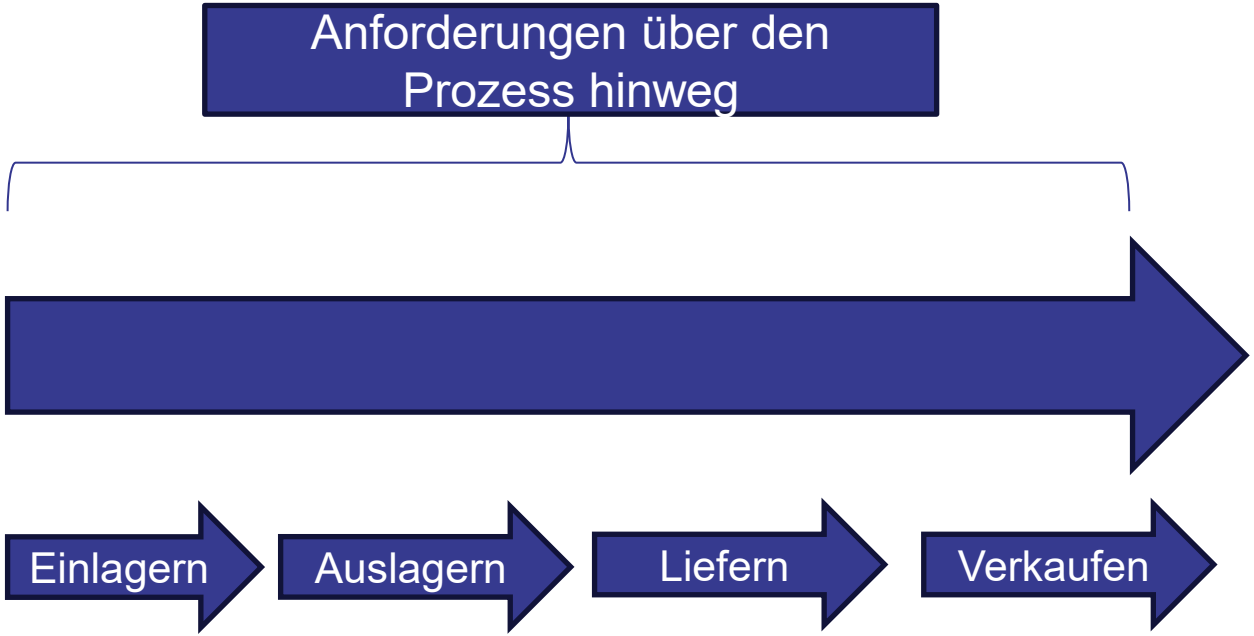
VO 2024/2690



1. Die Verrechtlichung der IT
2. Von der „klassischen“ Informationssicherheit zur „regulierten“ Informationssicherheit
3. Fazit

„Klassische“ Informationssicherheit (I/II)

Verkauf von Waren



„Klassische“ Informationssicherheit (II/II)

Zertifizierung im Multi-Site-Verfahren

- Multi-Site-Organisation ist eine Organisation, die von einem einzigen Managementsystem erfasst wird und aus einer festgelegten zentralen Funktion sowie einer Anzahl von Standorten besteht, an denen die Prozesse und Tätigkeiten ganz oder teilweise ausgeführt werden (IAF MD 1:2023, Abschnitt 2).
- Standort ist jeder physische oder virtuelle Ort, an dem die Organisation arbeitet oder eine Leistung erbringt. Ob dieser Ort eine eigene juristische Person ist, spielt keine Rolle.
- Zentrale Funktion ist die Funktion, die für das Managementsystem verantwortlich ist und dieses zentral steuert, nicht der eingetragene Sitz und auch nicht zwingend die Konzernmutter.

„Regulierte“ Informationssicherheit

5. Sicherheit der Lieferkette

- **Die NIS-2-RL kennt kein Konzernprivileg**
- Werden von einer Konzerngesellschaft (IT-Gesellschaft) Leistungen für eine weitere Konzerngesellschaft erbracht, erfolgt dies ausschließlich auf der Grundlage von Verträgen.
- Für die Leistungserbringerin gelten **grundsätzlich*** dieselben Voraussetzungen wie für externe Lieferanten.
- Aus Sicht IT-Gesellschaft sind die Cybersicherheitsanforderungen Teil des Vertrages Auditgegenstand sind die vertraglichen Regelungen und die Nachweise

* 5.1.4, - soweit angemessen – Art 2 Abs 2 VO 2024/2690

1. Die Verrechtlichung der IT
2. Von der „klassischen“ Informationssicherheit zur „regulierten“ Informationssicherheit
3. Fazit

FAZIT

Folgen für den CISO

- **Der Prüfmaßstab ist nicht mehr allein die Norm.** Neben ISO 27001 tritt der Rechtsakt.
  Beide verlangen Nachweise, nur einer davon ist sanktionsbewehrt.
- **Strafen machen Commitment „spürbar“.**
  Bis zu 10 Millionen Euro oder 2 Prozent des weltweiten Umsatzes bei wesentlichen Einrichtungen,
  7 Millionen oder 1,4 Prozent bei wichtigen.
- **Die Leitung fragt häufig nach Haftung, nicht nach Technik.**
  GmbH Geschäftsführer haften nach § 25 GmbHG und
  Vorstände nach § 84 AktG
- **Der CISO liefert die Grundlage der Entlastung.**
  Wer Risiken dokumentiert, verlagert die Entscheidung dorthin, wo sie hingehört. Wer schweigt, trägt sie selbst.

Das Budget folgt nicht immer der Bedrohung, sondern zeitweise auch der Sanktion.