KPMG

NIS2: Ein Reality Check

Zwischen Anspruch und Alltag.
Wenn Theorie auf gelebte Realität trifft

Linz, 5. November 2025

Cable Days 2025

10 JAHRE CYBER SECURITY STUDIE

Agenda

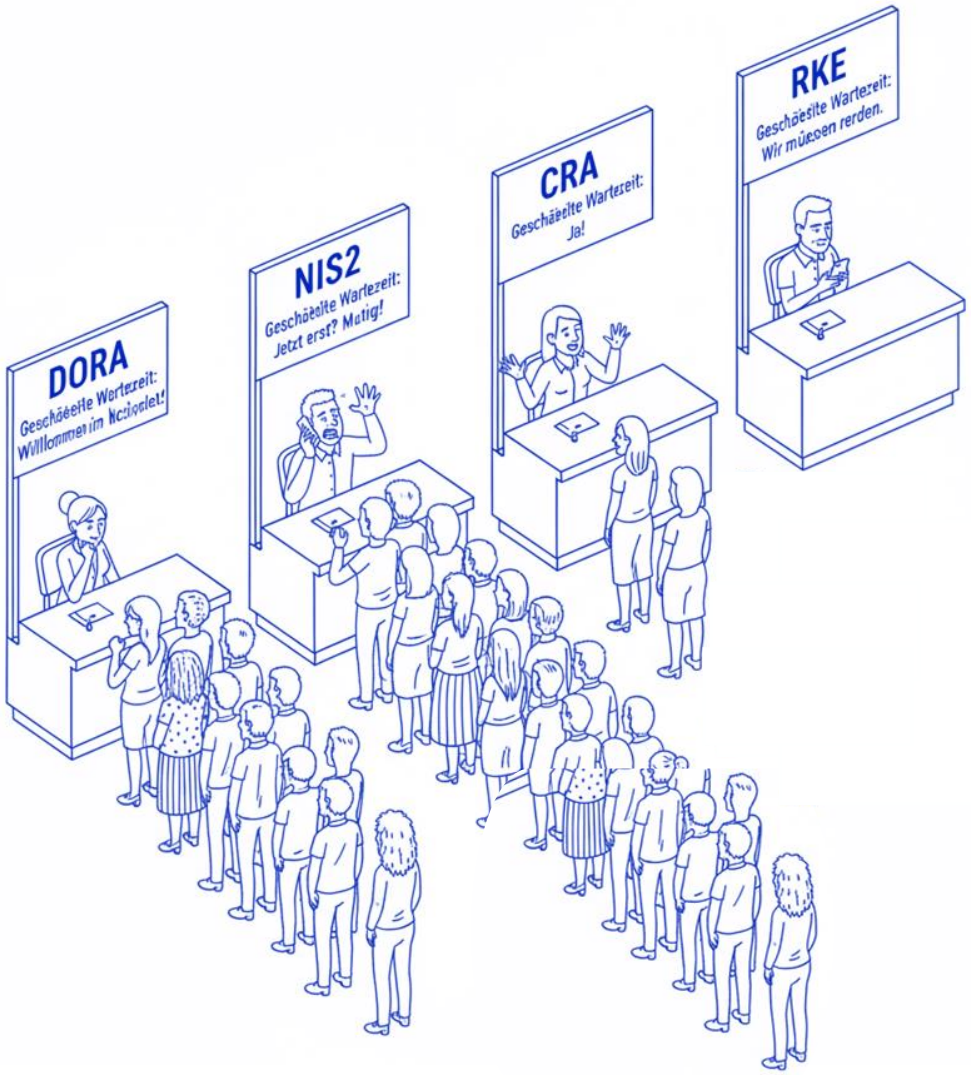
1 Einordnung: EU Cybersicherheitsarchitektur

2 NIS-2 auf einen Blick

3 RKEG: Resilienz Kritischer Einrichtungen

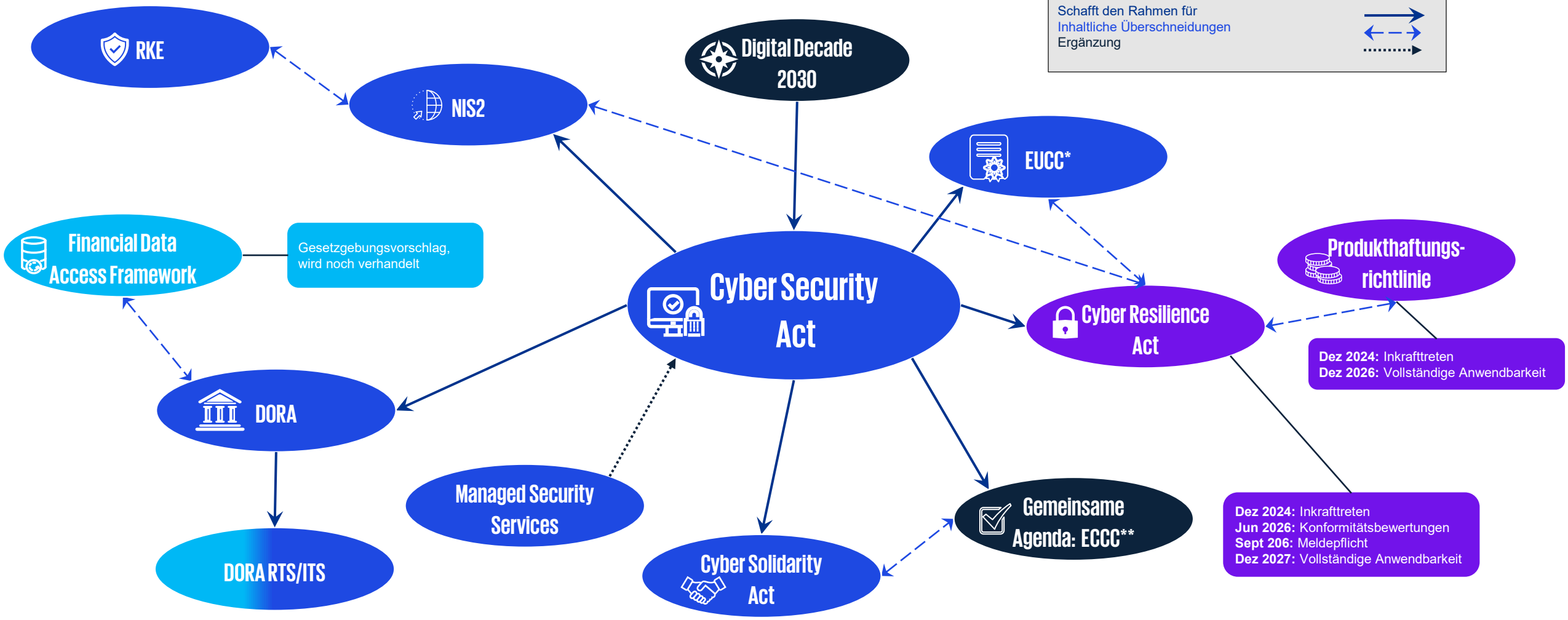
4 Aktuelle Herausforderungen in der Praxis

Unterschiedliche Wahrnehmung des regulatorischen Drucks[1]



1 KI generiertes Bild

EU Cybersecurity Architektur



*EUCC: European Cybersecurity Certification
**ECCC: European Cybersecurity Competence Centre

Source: https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

Agenda

1 Einordnung: EU Cybersicherheitsarchitektur

2 NIS-2 auf einen Blick

3 RKEG: Resilienz Kritischer Einrichtungen

4 Aktuelle Herausforderungen in der Praxis

Schaffung eines hohen gemeinsamen Niveaus der Cybersicherheit in der EU

Ziel Verbesserung **der Resilienz und Reaktion auf Sicherheitsvorfälle** des öffentlichen und des privaten Sektors in der EU.

Umsetzung Die NIS-2 Richtlinie muss bis **17.Oktober 2024** in nationales Recht umgesetzt werden.

Betroffene Sektoren

Unterscheidungg zwischen **„wesentlichen Einrichtungen“** (Ex-Ante Aufsicht: ohne Anlass) und **„wichtigen Einrichtungen“** (Ex-Post Aufsicht: nur mit Anlass).

Betroffene Unternehmen

Schwellwerten (size-cap-rule) für die Unternehmen.

Sektor des Unternehmens + Mitarbeiteranzahl, Umsatz, Bilanzsumme

Große Organisationen
- ab 250 Beschäftigte und
- mind. 50 Mio. EUR Umsatz oder Bilanz von mehr als 43 Mio. EUR

Mittlere Organisationen
- mehr als 50 Beschäftigte und
- zw. 10 und 50 Mio. EUR Umsatz oder Bilanz zw. 10 und 43 Mio. EUR

Einzelfallprüfung bei komplexeren Unternehmensstrukturen. Neben der Unternehmensgröße wird berücksichtigt, ob es sich um ein eigenständiges Unternehmen, Partnerunternehmen (Beteiligungen an anderen Unternehmen ab 25 % bis 50 %) oder verbundenes Unternehmen (Beteiligungen an anderen Unternehmen über 50 %) handelt.

Scope

Feststellung nicht mehr mittels eines Bescheides (NIS1: ca. 100 Unternehmen)

Verpflichtung gegen **sämtliche Gefahren („all hazards approach“) Vorkehrungen zu treffen**, welche die Sicherheit der Netz- und Informations-systeme **tatsächlich oder potentiell** bedrohen - unabhängig von deren Art oder Herkunft (NIS2 schätzungsweise mehrere Tausend Unternehmen in Österreich).

Notwendige Maßnahmen

(1) Sicherheitskonzept für NIS
(2) Konzept für Risikomngmt.
(3) Incident-Management
(4) BCM
(5) Sicherheit der Lieferkette
(6) Sicherheitsmaßnahmen bei Erwerb, Entwicklung und Wartung von NIS
(7) Verfahren zur Bewertung der Wirksamkeit von Riskmgmt-Maßnahmen
(8) Cyberhygiene u. Schulungen
(9) Kryptographie
(10) Sicherheit des Personals
(11) Zugriffskontrolle
(12) Asset-Management
(13) Physische Sicherheit)

Haftung und Sanktionen bei Nichteinhaltung

Persönliche Haftung der Geschäftsleitung, wenn die Maßnahmen nicht eingeführt wurden

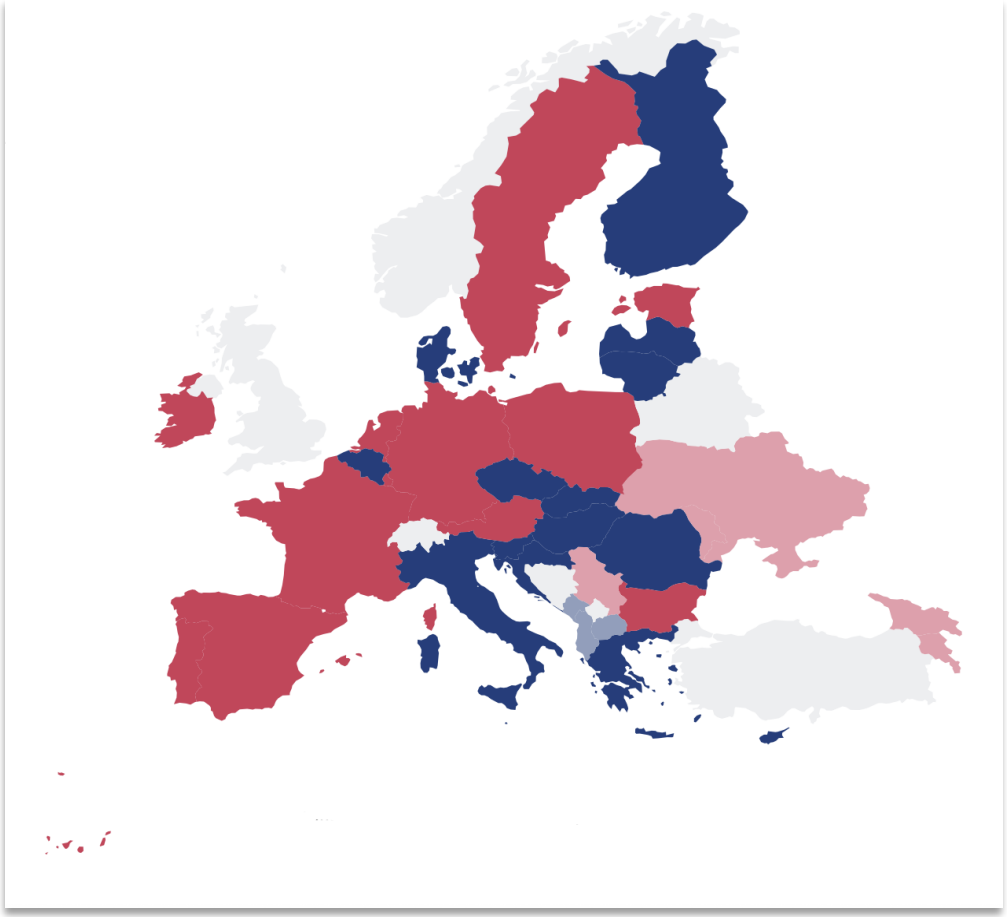
Strafrahmen **bei Verstößen/**Nichteinhaltung.

Wesentliche Einrichtungen: max. 10 Mio. € oder 2 % des weltweiten Umsatzes

Wichtige Einrichtungen: .max. 7 Mio. € oder 1,4 % des weltweiten Umsatzes

1 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 (NIS-2-Richtlinie)

Neues zu NIS-2 in Europa



Umgesetzt (EU-Mitgliedsstaat)
Gesetzesentwurf (EU-Mitgliedsstaat)
Umgesetzt (Nicht-EU-Mitgliedsstaat)
Gesetzesentwurf (Nicht-EU-Mitgliedsstaat)

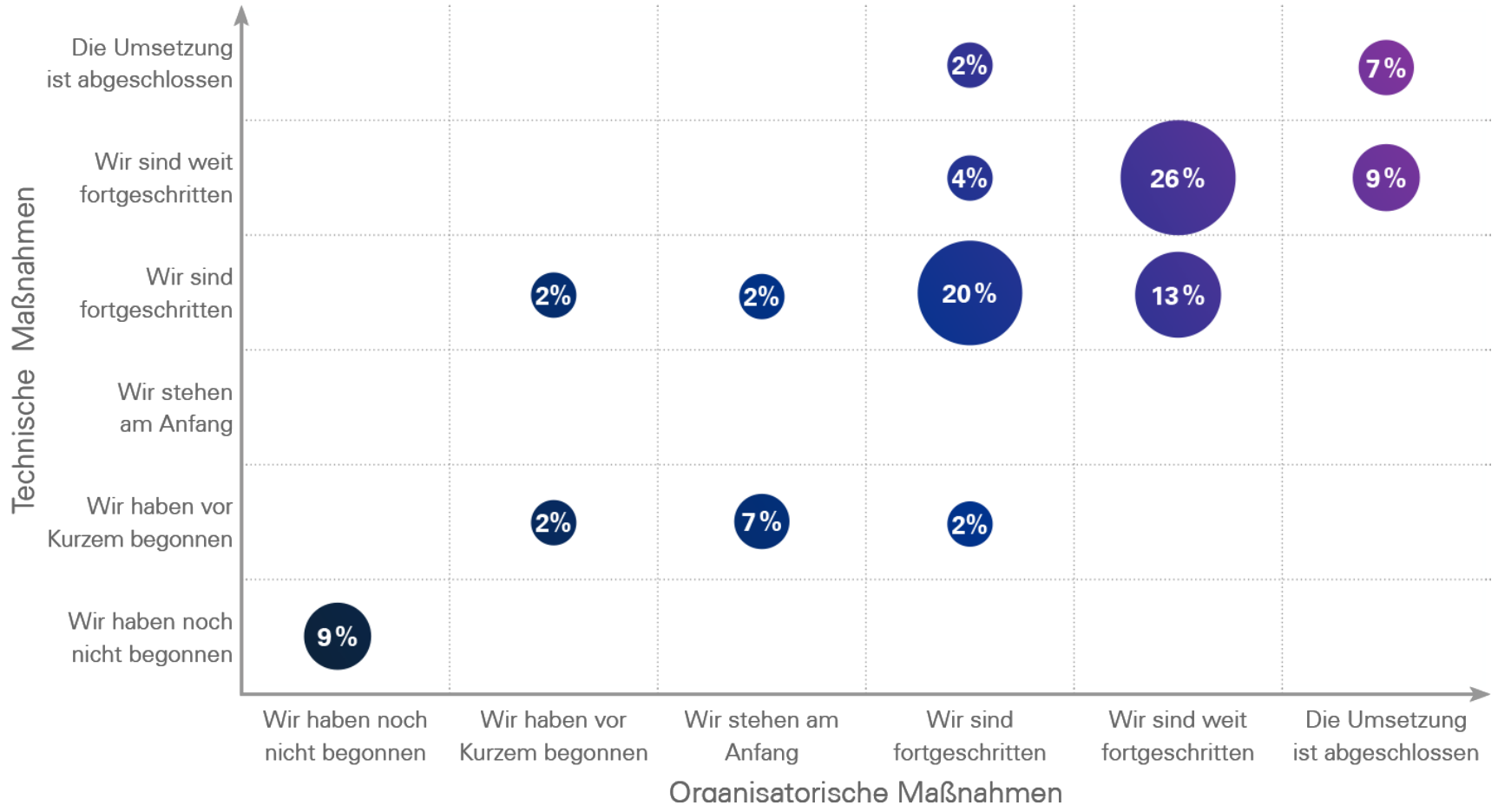
Source: https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

Stand 14.10.2025

Neueste Entwicklungen

- Kroatien, Italien, Belgien, Litauen, Griechenland, Rumänien, Ungarn, Slowakei, Finnland, Lettland, Tschechien sind die Länder, die NIS2 vollständig umgesetzt haben
- Registrierungsplattformen sind für Belgien, Finnland, Griechenland, Italien, Litauen, Luxemburg, Slowakei Tschechien und Ungarn vorhanden

NIS-2 Umsetzungsstand in Österreich



Source: https://kpmg.com/at/de/home/insights/2025/05/cybersecurity-studie-2025.html

Agenda

1 Einordnung: EU Cybersicherheitsarchitektur

2 NIS-2 auf einen Blick

3 RKEG: Resilienz Kritischer Einrichtungen

4 Aktuelle Herausforderungen in der Praxis

Begriffsdefinitionen

Resilienz kritischer Einrichtungen-Gesetz

§

Die **Resilienz bzw. physische Widerstandsfähigkeit kritischer Einrichtungen,** die für wichtige **gesellschaftliche** Funktionen oder **wirtschaftliche** Tätigkeiten im Binnenmarkt unerlässliche Dienste erbringen, zu stärken und ihre **Schwachstellen zu verringern**, indem ein harmonisiertes **Mindestmaß** an Verpflichtungen festgelegt wird und kohärente sowie gezielte Unterstützungs- und Aufsichtsmaßnahmen vorgesehen werden.

Konkret sollen kritische Einrichtungen ihre Fähigkeit verbessern, **Sicherheitsvorfälle zu verhindern**, sich davor zu **schützen**, darauf zu **reagieren**, die Folgen solcher Vorfälle zu **begrenzen**, Sicherheitsvorfälle zu **bewältigen** sowie sich von solchen Vorfällen zu **erholen**.

Verabscjoedet im Bundesrat am 9.10.2025 (981. Sitzung)

Resilienz kritischer Einrichtungen-Gesetz – RKEG; Tilgungsgesetz, Änderung (186 d.B.)

Bundesgesetz, mit dem das Bundesgesetz zur Sicherstellung eines hohen Resilienzniveaus von kritischen Einrichtungen (Resilienz kritischer Einrichtungen-Gesetz – RKEG) erlassen und das Tilgungsgesetz 1972 geändert wird

Begriffsbestimmungen §3

Kritische Einrichtung	Eine **öffentliche oder private Einrichtung**, die gemäß § 11 vom BMI als solche **eingestuft** wird.
Resilienz	Fähigkeit einer kritischen Einrichtung, Sicherheitsvorfälle zu verhindern, abzuwehren, ihre Auswirkungen zu begrenzen und sich davon zu erholen
Wesentlicher Dienst	Dienst, der durch **EU- oder nationale Verordnung festgelegt** wird und für die Aufrechterhaltung zentraler gesellschaftlicher, wirtschaftlicher, gesundheitlicher, sicherheitsrelevanter oder umweltbezogener Funktionen **von erheblicher Bedeutung** ist.
Sicherheitsvorfall	Ereignis, das die Erbringung wesentlicher Dienste oder die Funktionsfähigkeit verfassungsmäßiger Einrichtungen **erheblich stört oder gefährdet** (wird **per Verordnung bestimmt**, was genau ein Sicherheitsvorfall laut RKE ist)
Beinahe-Sicherheitsvorfall	Ereignis, das einen **Sicherheitsvorfall** auslösen könnte, aber **rechtzeitig verhindert oder nicht eingetreten** ist.
Kritische Infrastruktur	Objekte, Anlagen, Ausrüstungen, Netze, Systeme oder Teile eines Objekts, einer Anlage, einer Ausrüstung, **eines Netzes oder eines Systems, die für die Erbringung eines wesentlichen Dienstes** erforderlich sind.
Wesentlicher Dienst	[…] Dienste, die für die Aufrec**hterhaltung wichtiger gesellschaftlicher Funktionen, wichtiger wirtschaftlicher Tätigkeiten, der öffentlichen Gesundheit und Sicherheit oder die Erhaltung der Umwelt** von erheblicher Bedeutung sind und von einer Einrichtung der im Anhang der RKE-RL angeführten Kategorien in den gelisteten Sektoren und Teilsektoren erbracht werden;
Resilienzplan	Ein Dokument, in dem die **geeigneten und verhältnismäßigen technischen, sicherheitsbezogenen und organisatorischen Maßnahmen** zur Gewährleistung der Resilienz nachvollziehbar dargelegt werden;

Source: https://www.parlament.gv.at/gegenstand/XXVIII/I/186

Anwendungsbereich für betroffene Unternehmen

Vier kumulative Voraussetzungen müssen Vorliegen:

1. Unternehmen ist im **Inland** tätig
2. Die **kritische Infrastruktur** des Unternehmens befindet sich im **Inland**
3. Es wird zumindest **ein wesentlicher Dienst** erbracht
4. Ein Sicherheitsvorfall könnte eine **erhebliche Störung bei diesem** wesentlichen Dienst oder bei **anderen wesentlichen Diensten**, die von der Einrichtung abhängig sind, **bewirken**

RKE gilt nicht für (§2):

- Gerichtsbarkeit
- Gesetzgebung
- Parlamentsdirektion
- Österreichische Nationalbank

- Besonderes Regime für den Sektor **öffentliche Verwaltung**
  - Jeweilige/r Minister/in muss sich trotzdem um Resilienz kümmern (insb. Landesverteidigung und Strafverfolgung)
- **Bescheidmäßige** Feststellung

Source: https://www.parlament.gv.at/gegenstand/XXVIII/I/186

Zusammenfassung der Pflichten für kritische Einrichtungen

Erhalt des Bescheids über die Einstufung durch das BMI

01 Kontaktstelle

Mitteilung and das BMI einer Kontaktstelle und mindestens einer Ansprechperson

4 Wochen nach Erhalt des Bescheids, diesbezügliche Änderungen sind innerhalb von **2 Wochen** zu kommunizieren

9 Monate nach Erhalt des Bescheids, danach alle **4 Jahre**

02 Risikoanalyse

Die Einrichtung muss eine eigene Risikoanalyse durchführen und deren Ergebnis dem BMI mitteilen

03 Zuverlässigkeits-prüfungen

Wenn durch Risikoanalyse erforderlich, muss für bestimmte Personen eine solche Prüfung durchgeführt werden

Im Zuge der Risikoanalyse, danach **alle 3 Jahre**

10 Monate nach Erhalt des Bescheids

04 Maßnahmen

Implementierung geeigneter Maßnahmen und deren Dokumentation im Resilienzplan

05 Meldepflicht

Einrichtungen sind verpflichtet Sicherheitsvorfälle an das BMI zu melden

Ab **10 Monate** nach Erhalt des Bescheids

Auf Anfrage des BMIs

06 Nachweise & Audits

Einrichtungen müssen Nachweise über die getroffenen Maßnahmen erbringen und bei Bedarf Audits durchführen

Source: https://www.parlament.gv.at/gegenstand/XXVIII/I/186

Agenda

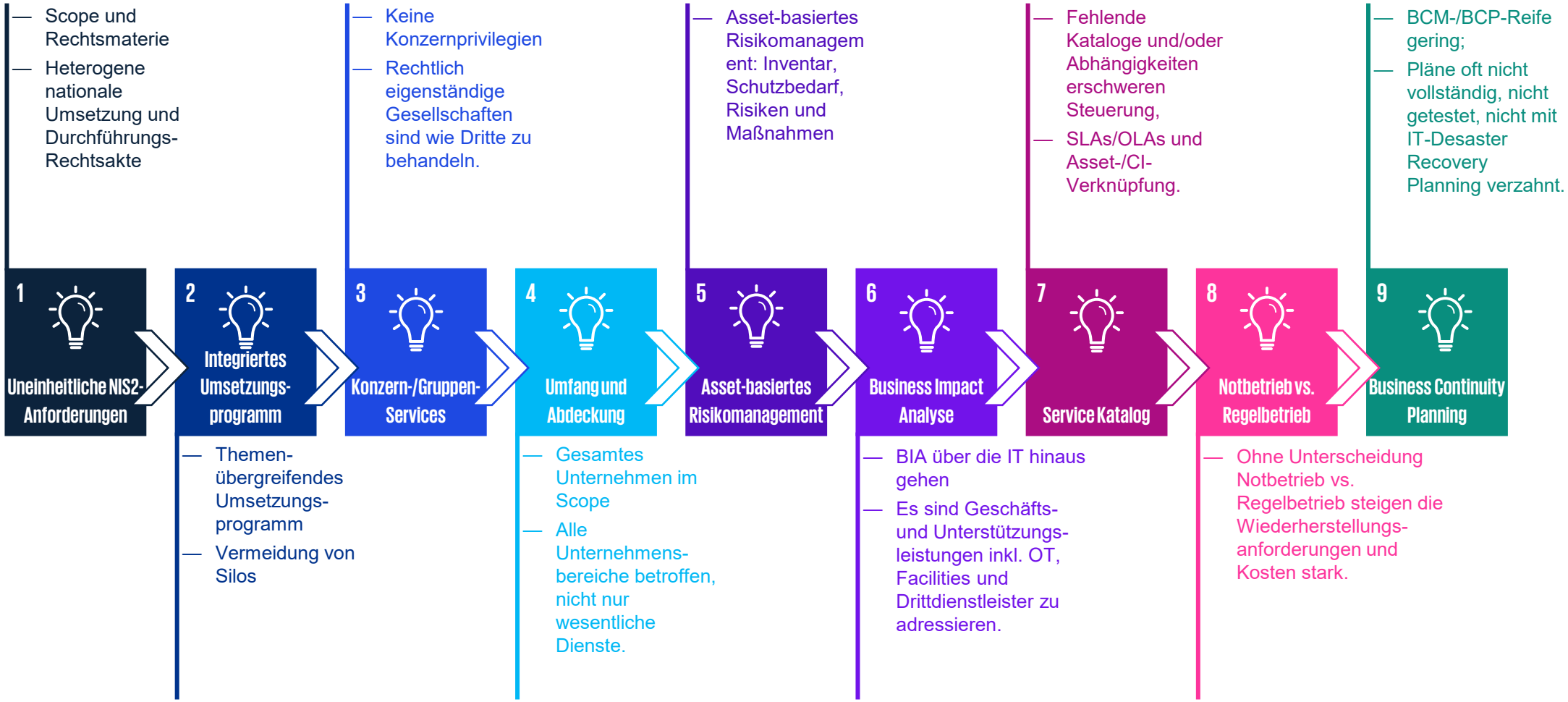
1 Einordnung: EU Cybersicherheitsarchitektur

2 NIS-2 auf einen Blick

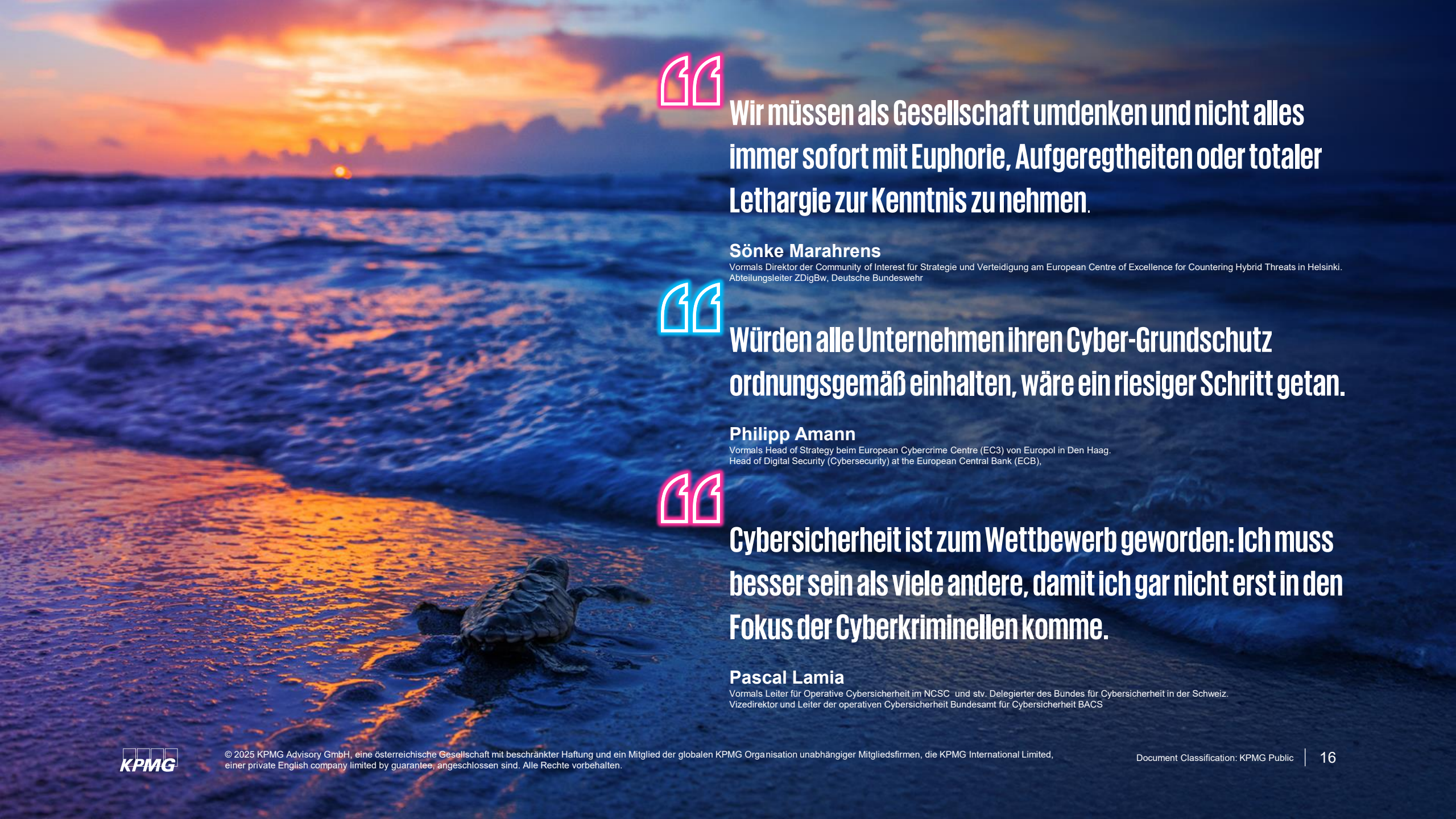
3 RKEG: Resilienz Kritischer Einrichtungen

4 Aktuelle Herausforderungen in der Praxis

Aktuelle Herausforderungen in der Praxis




„Risiken,
die andere für mich eingehen,
sind auch meine Risiken.“



> Wir müssen als Gesellschaft umdenken und nicht alles immer sofort mit Euphorie, Aufgeregtheiten oder totaler Lethargie zur Kenntnis zu nehmen.

Sönke Marahrens
Vormals Direktor der Community of Interest für Strategie und Verteidigung am European Centre of Excellence for Countering Hybrid Threats in Helsinki.
Abteilungsleiter ZDigBw, Deutsche Bundeswehr

> Würden alle Unternehmen ihren Cyber-Grundschutz ordnungsgemäß einhalten, wäre ein riesiger Schritt getan.

Philipp Amann
Vormals Head of Strategy beim European Cybercrime Centre (EC3) von Europol in Den Haag.
Head of Digital Security (Cybersecurity) at the European Central Bank (ECB),

> Cybersicherheit ist zum Wettbewerb geworden: Ich muss besser sein als viele andere, damit ich gar nicht erst in den Fokus der Cyberkriminellen komme.

Pascal Lamia
Vormals Leiter für Operative Cybersicherheit im NCSC und stv. Delegierter des Bundes für Cybersicherheit in der Schweiz.
Vizedirektor und Leiter der operativen Cybersicherheit Bundesamt für Cybersicherheit BACS

Mehr zur NIS in unserem KPMG IMPULSE-Podcast oder in unserer KPMG/KSÖ Studie „Cybersecurity in Österreich 2025“

https://open.spotify.com/episode/31d4SAPaadH2tlYLFvqo5m?si=06aNIBEGRQGIBOBaXgNbOg

https://open.spotify.com/episode/09XaSwsXHztNz1vUza4oiZ?si=rgR4pSLiQoOSoJ0X1gUHfw

KPMG IMPULSE-Podcast Ausgben zur KPMG/KSÖ Studie „Cybersecurity in Österreich 2025“

#106 Sicherheit im digitalen Zeitalter: Österreichs Kampf gegen Cybercrime und Desinformation

In unserer neuesten Podcast-Folge spricht unser Partner und Cybersecurity-Experte Robert Lamprecht mit Andreas Holzer, Direktor des österreichischen Bundeskriminalamts, und Hermann Kaponig, Direktor der Direktion für IKT und Cyber im österreichischen Bundesheer. Gemeinsam besprechen sie die aktuellen Herausforderungen und Strategien zur Bekämpfung von Cyberkriminalität und hybriden Bedrohungen.

Erfahren Sie mehr über die Rolle des Bundeskriminalamts und des Bundesheers im Kampf gegen Cybercrime, die Bedeutung internationaler Zusammenarbeit und die Bedrohung durch Deepfakes und Desinformationskampagnen.

https://open.spotify.com/episode/0XBB5MnOczAuYWtuojsRMs?si=296bc99d31b44b1c

#112: Cyberresilienz im Finanzsektor: Einblicke und Strategien mit Anna Muri (FMA)

In dieser Cybersecurity-Podcast-Folge begrüßt KPMG Cybersecurity-Partner Robert Lamprecht Anna Muri, Leiterin des IT-Risiko-Teams bei der Finanzmarktaufsicht (FMA).

Anna Muri teilt ihre wertvollen Einblicke in die Herausforderungen und Schwerpunkte ihres Teams, die Bedeutung der IT-Governance und die Zusammenarbeit mit verschiedenen Institutionen.

Erfahren Sie mehr über die Umsetzung der DORA-Verordnung, die Rolle der IKT-Dienstleister und wie die Digitalisierung die Finanzbranche verändert. Außerdem gibt Anna Muri persönliche Einblicke in ihre außergewöhnliche Reise von der Indologie zur IT-Risiko-Managerin.

Ein Muss für alle, die sich für Cybersecurity und IT-Risiken im Finanzsektor interessieren!

https://open.spotify.com/episode/4XGPCj2QogYf0g32gBM99V?si=bcae0af4173a407e

#115 Multinationale Zusammenarbeit: Resilienz stärken mit Jean Nicolas GAUTHIER (Siemens AG)

Unser Cybersecurity-Partner Robert Lamprecht begrüßt den Regional Security Officer bei Siemens AG, Jean Nicolas GAUTHIER. Jean Nicolas GAUTHIER teilt wertvolle Einblicke in die Krisenbewältigung und die Stärkung der Widerstandsfähigkeit durch internationale Zusammenarbeit.

Die Episode beleuchtet die Anwendung militärischer Prinzipien des Krisenmanagements in Unternehmen wie klare Befehlsstrukturen und situative Bewertungen. Gauthier hebt die Bedeutung von Risikobewertungen und Sicherheitsbewusstsein hervor, um Unternehmen auf zukünftige Bedrohungen vorzubereiten. Zudem diskutiert er die Rolle von KI in der Ausbildung von Sicherheitsexpert:innen und im Kampf gegen Desinformationsbedrohungen.

https://open.spotify.com/episode/5LcoSx5vUbLLYtzJFFXzYT?si=kT7n_qoGQ4auKxgdkGppTw

#124: Neue Technologien und globale Sicherheit mit Elisabeth Hoffberger-Pippan (PRIF Peace Research Institute Frankfurt)

In der aktuellen Folge spricht KPMG Cybersecurity-Partner Robert Lamprecht mit Elisabeth Hoffberger-Pippan, Senior Researcher am Peace Research Institute Frankfurt, über die Bedeutung ethischer Standards und den Aufbau digitaler Kompetenzen, um sich auf zukünftige Herausforderungen vorzubereiten. Hoffberger-Pippan forscht zu Abrüstung, biologischen und chemischen Waffen sowie zur Rolle neuer Technologien wie KI. Sie erklärt, warum diese Themen auch für Unternehmen zentral sind.

Die beiden Expert:innen beleuchten:

- Chancen und Risiken neuer Technologien – und was das konkret für Unternehmen bedeutet
- Warum es wichtig ist, die eigene Komfortzone zu verlassen und KI aktiv mitzugestalten
- Wie wir verhindern, dass Geschwindigkeit in KI-Prozessen zu voreiligen oder fehlerhaften Entscheidungen führt
- Welche Maßnahmen vor Angriffen wie Data Poisoning schützen können

https://open.spotify.com/episode/3AJU4k2jkCBpLg5YjfBhar?si=9be1358635e740b3

Vortragender

Robert Lamprecht

Partner, Advisory
Cybersecurity & Crisis Management

T +43 1 31332 3409
M +43 664 8161232
rlamprecht@kpmg.at

Document Classification: KPMG Public

KPMG

NIS2: Ein Reality Check

Zwischen Anspruch und Alltag.
Wenn Theorie auf gelebte Realität trifft

Linz, 5. November 2025

Cable Days 2025

10 JAHRE CYBER SECURITY STUDIE