bayern innovativ
Innovation leben

NIS2, CRA, AI Act

aktuelle EU-Regulation und wie damit umgehen?

Dr.-Ing. Robert Couronné
Projektmanager Bayern Innovativ

Überblick

Kommende EU-Regularien die helfen (können)

1

NIS 2 Richtlinie (EU) 2022/2555 – Sicherheit der Informationsnetzte in kritischen Infrastrukturen

2

Cyber Resilience Act - Security by law für alle

3

AI Act (EU) – verantwortliche Nutzung von AI

4

EDIH DIBI: Wir unterstützen - nicht nur bei Regularien

Schadensfallbeispiel

Hacker-Attacke auf US Pipeline zur Treibstoffversorgung in 2021

➔ Treibstoffengpässe an amerikanischer Ostküste über mehrere Tage

- Hackergruppe „DarkSide“ attackierte Colonial Pipeline mit einem Ransomware-as-a-Service Angriff
- IT-Systeme der Verwaltung betroffen – Auswirkungen auf die Versorgung
- 100 GB Daten abgegriffen
- Lösegeldzahlung von 4,4 Mio. US-Dollar
- Bitcoin-Zahlungen konnten vom FBI teilweise wieder zurückgeholt werden

Nach Hackerangriff

Colonial Pipeline zahlte Lösegeld

Stand: 20.05.2021 09:31 Uhr

Schaden steigt auf 266,6 Milliarden Euro

Welche Schäden sind Ihrem Unternehmen im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage entstanden?

Schaden durch...	Schadenssummen in Mrd. Euro (2024)	Schadenssummen in Mrd. Euro (2023)	Schadenssummen in Mrd. Euro (2022)
Ausfall, Diebstahl oder Schädigung von Informations- und Produktionssystemen oder Betriebsabläufen	54,5	35,0	41,5
Kosten für Rechtsstreitigkeiten	53,1	29,8	16,2
Umsatzeinbußen durch nachgemachte Produkte bzw. Plagiate	39,2	15,3	21,1
Kosten für Ermittlungen und Ersatzmaßnahmen	32,2	25,2	10,1
Datenschutzrechtliche Maßnahmen, z.B. durch Behörden	27,2	12,4	18,3
Imageschaden bei Kunden oder Lieferanten, Negative Medienberichterstattung	20,2	35,3	23,6
Patentrechtsverletzungen, auch vor Anmeldung	14,8	10,4	18,8
Erpressung mit gestohlenen Daten	13,4	16,1	10,7
Umsatzeinbußen durch Verlust von Wettbewerbsvorteilen	11,2	21,5	41,5
Geldabfluss durch Betrugsversuche	0,8	3,9	-
Sonstige Schäden	0	1,1	0,9
Gesamtschaden pro Jahr	**266,6**	**205,9**	**202,7**

Basis: Alle Unternehmen (n=1.003) | Mehrfachnennungen möglich | rundungsbedingt kann die Summe der Einzelschäden vom Gesamtschaden abweichen. | Quelle: Bitkom Research 2024

bitkom

NIS 2

Motivation und Ziel

Motivation:

- Digitale Infrastruktur erfasst immer mehr Bereiche der Daseinsvorsorge.
- Gravierende Störungen (bis Totalausfall) lebenswichtiger Versorgungsstrukturen möglich

➔ **Ziel: Hohes Cybersicherheitsniveau in EU durch verschärfte Anforderungen an die Cybersicherheit für Unternehmen und Organisationen**

https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

NIS 2

Ziele

1. EU-weiter Aufbau von Cybersicherheitskapazitäten
2. Eindämmung von Bedrohungen für Netz- und Informationssysteme, die zur Erbringung wesentlicher Dienste in Schlüsselsektoren verwendet werden
3. Sicherstellung der Kontinuität solcher Dienste bei Vorfällen

Quelle: https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32022L2555&from=EN#d1e40-80-1

https://pixabay.com/de/images/search/ziele/

NIS 2

Produkte und Dienstleistungen für welche Sektoren?

https://de.freepik.com/fotos-vektoren-kostenlos/sicherheitsbranche

- Sektoren mit hoher Kritikalität
  - Kritische Infrastruktur

Neu:

- kritische Sektoren
- Mitgliedsstaaten der EU können Richtlinie auch auf Kommunen und Bildungseinrichtungen anwenden

NIS 2 – Sektoren

mit hoher Kritikalität

Hohe Kritikalität:

- Energie
- Verkehr
- Bankwesen
- Finanzmarkt-infrastrukturen
- Gesundheitswesen
- Trinkwasser
- Abwasser
- Digitale Infrastruktur
- Verwaltung von IKT-Diensten (Business-to-Business)
- Öffentliche Verwaltung
- Weltraum

Kritische Sektoren:

- Post- und Kurierdienste
- Abfallbewirtschaftung
- Produktion, Herstellung, Handel mit chemischen Stoffen
- Produktion, Verarbeitung und Vertrieb von Lebensmitteln
- Verarbeitendes Gewerbe / Herstellung von Waren

➔ **80% der betroffenen Unternehmen und Organisationen wussten es Ende 2023 noch nicht.**

Foto: https://www.istockphoto.com/de/fotos/branchen

NIS 2

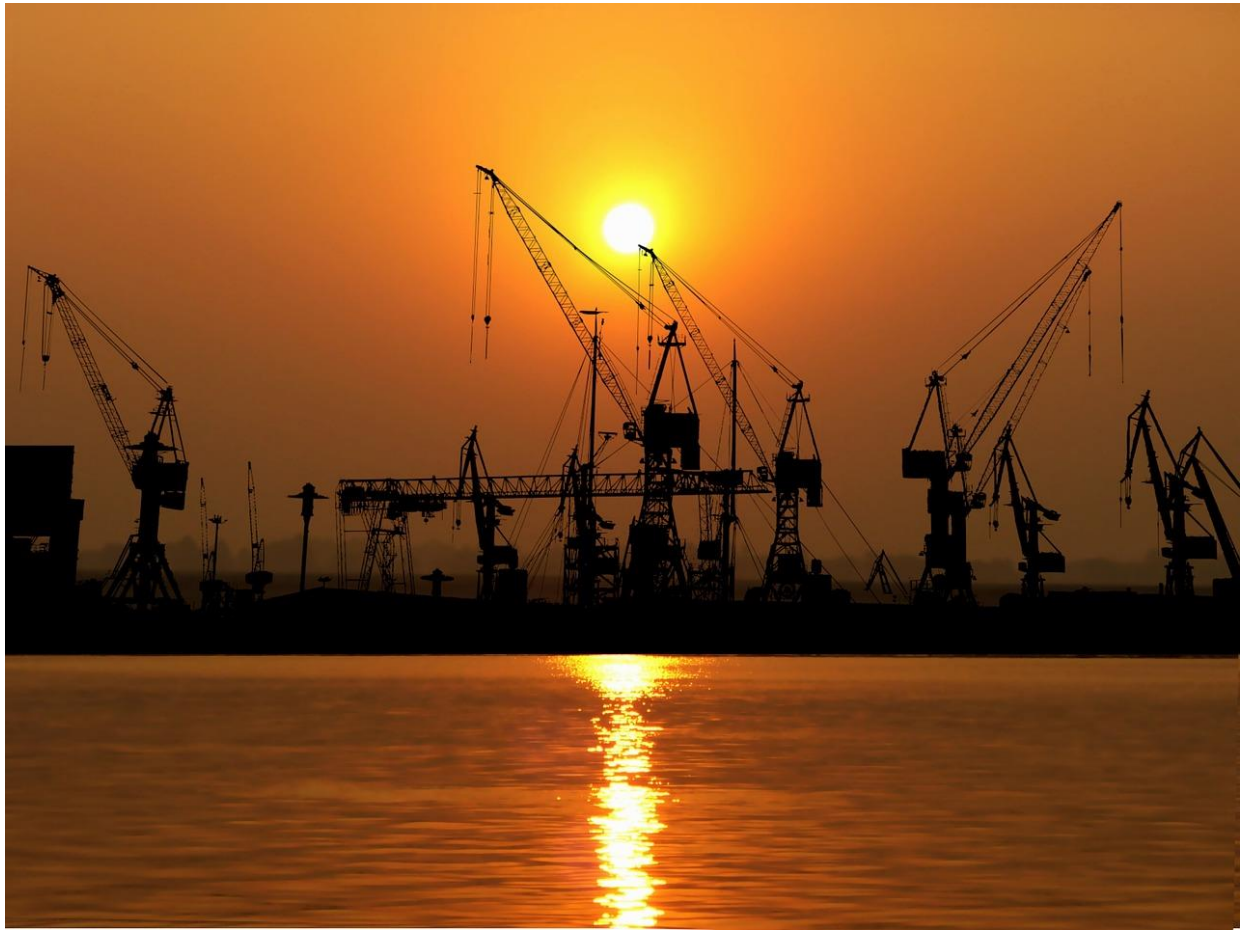
Relevante Unternehmensgrößen

NIS-2 gilt

ab mittlerer Unternehmensgröße
> 50 Personen, Jahresumsatz bzw. Jahresbilanz
> 10 Millionen Euro

NIS-2 gilt unabhängig von der Größe **auch für kleinere Firmen**

- in besonders kritischen Bereichen (IT-Kommunikationsnetze, Domainverwaltung, Vertrauensdienste, …)
- als einziger Anbieter agieren



https://pixabay.com/de/photos/sonnenuntergang-port-kr%C3%A4ne-branchen-4055837/

NIS 2

Neue Haftungsregeln

ESET Whitepaper_NIS2_CISO_NIS-Loesungen.pdf

- Höhere Bußgelder
- Erweiterte Haftungsregeln bei grob fahrlässiger Missachtung der Vorgaben ➔ persönliche Haftung der Geschäftsführung

Was ist zu tun?

Security mit System (ISMS)

Cyber Security Maturity Assessment (CSMA)

Netzwerk-segmentierung (NG-Firewall)

Anomalieerkennung

Security Operations Center (SOC)

Backup-Konzept

Netzwerkanalyse einer Produktionslinie

Security Awareness Kampagne und Training

Schwachstellen-scan & Penetrationstest

Notfallmanagement & Business Continuity Prozesse

Information Security Management System (ISMS)

Quelle: Syskron, 2021 inhaltlich basierend auf https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

SYSKRON

NIS2

Versuch einer Checkliste

Für die Organisation:

- ✓ ISMS, Notfallplan, Vorfallsmanagement mit Aufrechterhaltung des Betriebs (Business Continuity)
- ✓ Secure Operations – Anomalieerkennung im Betrieb
- ✓ Sicherheit der Lieferkette (Supply Chain Security)
- ✓ Awarenessmaßnahmen und Tests für Mitarbeitende
- ✓ Risikomanagement von Anlagen (Asset Management)

Für Produkte und Dienstleistungen

- ✓ CS von Produkten und Services produktlebenslang gewährleisten
- ✓ Schwachstellenmanagement, SW Bill of Materials
- ✓ Security by Design, regelmäßiges PEN-Testing Secure Product Development by Governance (IEC)
- ✓ Secure Remote Services - MFA

NIS 2 – Was ist zu tun?

Schritt 1

Ist mein Unternehmen betroffen?

Schritt 2

In welchem Umfang?

Schritt 3

CS-Ziele, Strategie und Maßnahmen entwickeln und umsetzen

https://iiot-world.com/ics-security/cybersecurity/four-most-hard-to-solve-iiot-security-issues/

NIS 2 tritt (voraussichtlich) im Oktober 2024 in Kraft!

Cybersicherheit ist Organisationsverantwortung

➔Verschärfte CS-Regularien mit erhöhter Haftung.

Überblick

Kommende EU-Regularien die helfen (können)

1
NIS2 Richtlinie (EU) 2022/2555 – Sicherheit der Informationsnetzte in kritischen Infrastrukturen

2
Cyber Resilience Act - Security by law für alle

3
AI Act (EU) – verantwortliche Nutzung von AI

4
EDIH DIBI: Wir unterstützen
- nicht nur bei Regularien

https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act

EU Cyber Resilience Act

Ziel

- Schutz der **Verbraucher, Unternehmen und Organisationen**
- V**erbindlicher CS-Anforderungen für Hersteller und Händler** mit Kommunikationsschnittstelle zum Internet
- **Schutzpflicht über Produktlebenszyklus von 5 Jahren**
- Beispiele:
  - Kommunikationselektronik
  - vernetzte Produkte im Smart Home
  - Steuerungen in vernetzte Maschinen und Anlagen (Update der Maschinenrichtlinie)

https://de.freepik.com/vektoren-kostenlos/isometrische-mobilfunknetz-konzept_4327449.htm#fromView=search&page=1&position=5&uuid=baed95d2-33f9-45d4-b807-7372e685749e

bayern innovativ
Innovation leben

Umsetzung Cyber Resilience Act

- Unklarheiten in der Umsetzung:
  - Security by Design
  - SW Bill of Materials (SW-Stückliste)
  - Schwachstellenmanagement
  - Regelmäßiges Pen-Testing
  - Überwachungsaufgaben
  - IoT-Devices (Geräte) im Feld sichern

➔ Cybersecurity-Regulation trifft auf Wirklichkeit
– noch viele Herausforderungen in praktischer Umsetzung
Inkrafttreten vermutlich 2027

https://de.freepik.com/vektoren-kostenlos/kommunikationsikonen-schwarzsatz_1529652.htm#fromView=search&page=1&position=4&uuid=baed95d2-33f9-45d4-b807-7372e685749e

Die Rechtswirksamkeit des CRA wird erwartet für 2027

Cybersicherheit ist Organisationsverantwortung

➔ Heute beginnen.

Überblick

Kommende EU-Regularien die helfen (können)

1
NIS2 Richtlinie (EU) 2022/2555 – Sicherheit der Informationsnetzte in kritischen Infrastrukturen

2
Cyber Resilience Act - Security by law für alle

3
AI Act (EU) – verantwortliche Nutzung von AI

4
EDIH DIBI: Wir unterstützen
- nicht nur bei Regularien

EU AI Act

Warum?

KI gewinnt an Bedeutung

Birgt neue Risiken oder negative Folgen

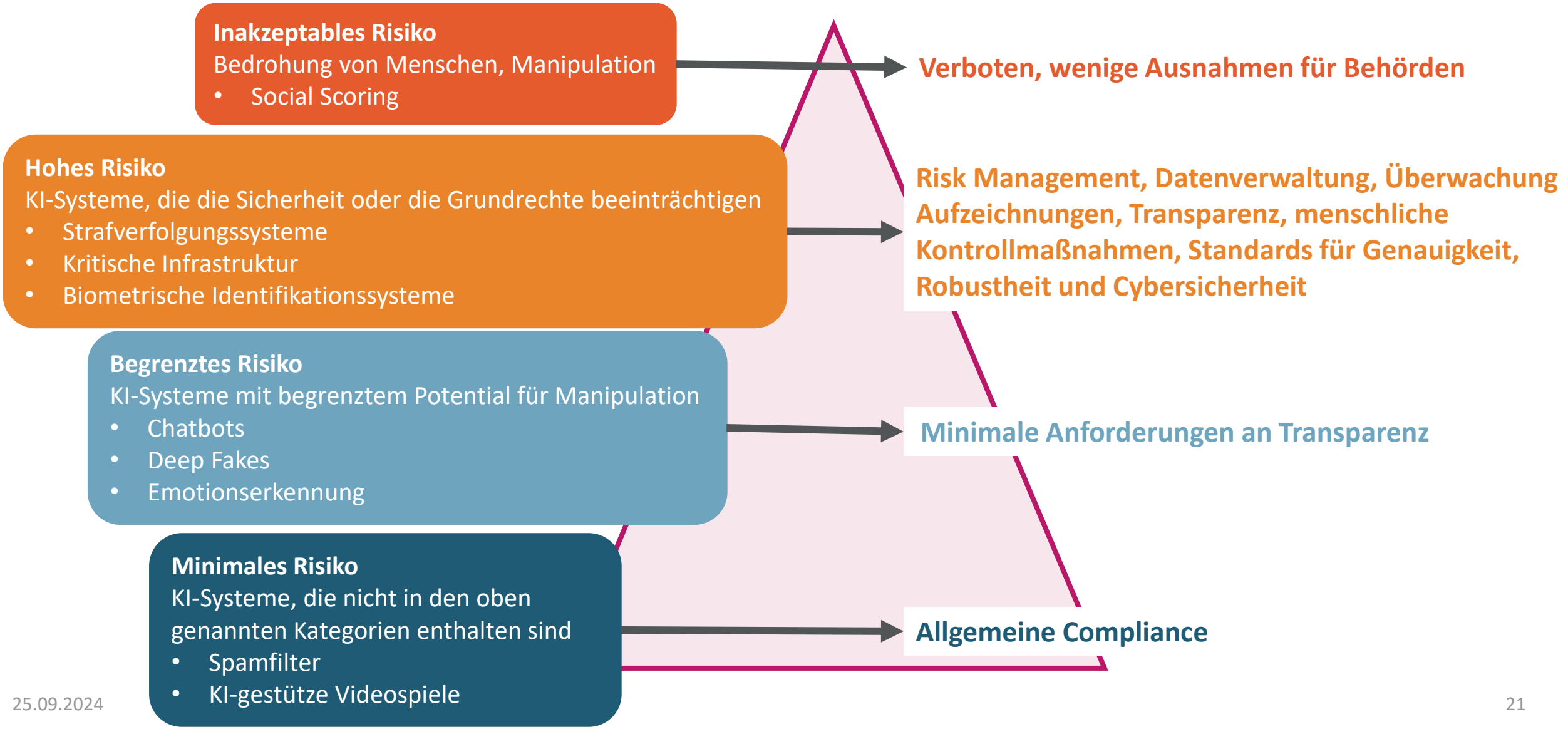
Rechtsvorschriften zur Förderung sicherer künstlicher Intelligenz unter Wahrung der Grundrechte

Harmonisierte Regeln für die Entwicklung und den Einsatz von KI in der EU

Definition von KI wichtig:
"Software, die in der Lage ist, Aufgaben auszuführen, für die normalerweise menschliche Intelligenz erforderlich wäre, wie das Verstehen natürlicher Sprache, das Erkennen von Bildern oder das Treffen von Entscheidungen".

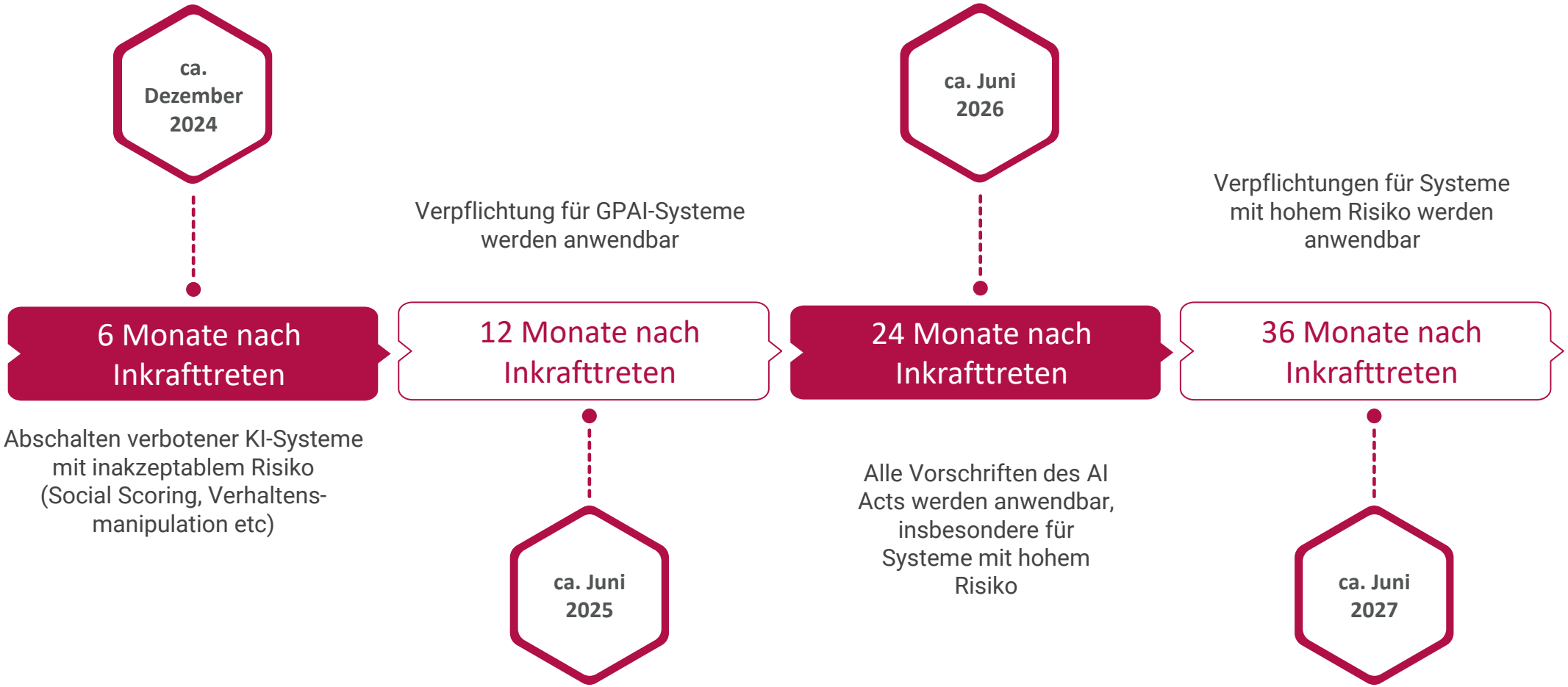
EU AI Act

Risikobasierter Ansatz



EU AI Act

Wo stehen wir bei der Umsetzung des Gesetzes?



Der AI Act tritt im Oktober 2024 in Kraft

Compliance & Risikomanagementpflichten im Vordergrund

➔ Leitfaden und Best Practice Beispiele wichtig!

Überblick

Kommende EU-Regularien die helfen (können)

1

NIS2 Richtlinie (EU) 2022/2555 – Sicherheit der Informationsnetzte in kritischen Infrastrukturen

2

Cyber Resilience Act - Security by law für alle

3

AI Act (EU) – verantwortliche Nutzung von AI

4

EDIH DIBI: Wir unterstützen - nicht nur bei Regularien

EDIH Digitale Innovationen für die bayerische Industrie

Support für KMU

Aufgaben EDIH-DIBI:

- Förderung von Wissens-/Erfahrungstransfer, Kompetenzentwicklung, Finanzierung und Vernetzung
- Ausschöpfung der Synergien **regionaler** Zentren mit **paneuropäischem Netzwerk**

Partner

edih dibi digital innovations for bavarian industry

EDIH European Digital Innovation Hubs Network

NIS2, CRA, AI Act:

➔ EDIH DIBI unterstützt Sie bei Fragen der Relevanz, Umsetzung und Nutzung

➔ mit Cybersicherheits-Check gemäß **DIN Spec 27076 für KMU (BSI approved)**

Sie finden uns am Stand.

edih dibi
digital innovations for bavarian industry

Dr. Robert Couronné
robert.couronne@bayern-innovativ.de
Tel.: +49 911 20671-230
Matthias Hafner
matthias.hafner@bayern-innovativ.de
Marius Elgershäuser
marius.elgershaeuser@bayern-innovativ.de

info@bayern-innovativ.de
www.bayern-innovativ.de

Regularien und kein Ende?.