CYBER INTELLIGENCE
.Institute

NIS 2 kommt: Neue Anforderungen an das Cybersecurity Risikomanagement

Prof. Dr. jur. Dennis-Kenji Kipker

Wer ist quantitativ durch NIS 2 betroffen?

Mittlere Unternehmen gem. Empfehlung 2003/361/EG: Beschäftigung von min. 50 Personen oder Jahresumsatz und Jahresbilanz übersteigt jeweils 10 Mio. EUR

Unternehmen, die die Schwellenwerte für mittlere Unternehmen nach EU-Recht überschreiten (min. 250 Beschäftigte oder Jahresumsatz von mehr als 50 Mio. EUR und Jahresbilanz von mehr als 43 Mio. EUR)

Von Unternehmensgröße unabhängig, soweit qualifizierende Faktoren erfüllt sind, z.B. wegen kritischer Tätigkeit, Auswirkungen auf öff. Ordnung, Systemrisiken, grenzüberschreitenden Auswirkungen

Wer ist qualitativ durch NIS 2 betroffen?

Sektoren nach Anhang I	Sektoren nach Anhang II
Energie	Post- und Kurierdienste
Verkehr	Abfallbewirtschaftung
Bankwesen	Produktion, Herstellung und Handel mit chem. Stoffen
Finanzmarktinfrastrukturen	Produktion, Verarbeitung und Vertrieb von Lebensmitteln
Gesundheitswesen	**Verarbeitendes Gewerbe/Herstellung von Waren, u.a. Datenverarbeitungsgeräte, elektronische und optische Erzeugnisse und Ausrüstungen, Maschinenbau, Kraftwagen, Kraftwagenteile, Fahrzeugbau**
Trinkwasser	Anbieter digitaler Dienste
Abwasser	Forschungseinrichtungen
Digitale Infrastruktur	
Verwaltung von IKT-Diensten	
Öffentliche Verwaltung	
Weltraum	

Risikomanagement zur Cybersicherheit

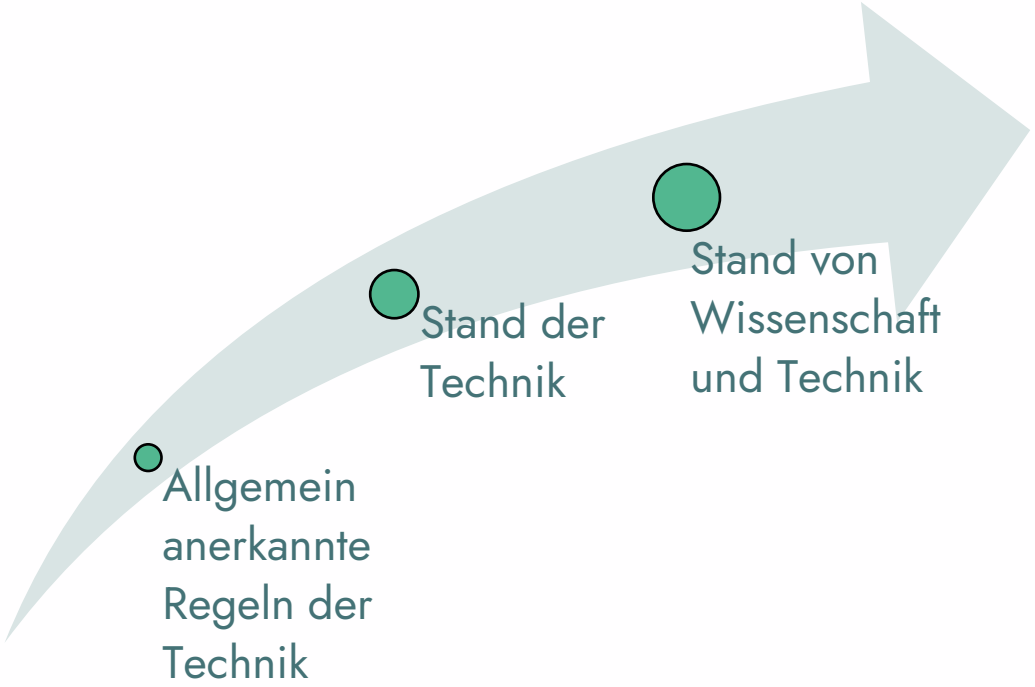
§ 30

Risikomanagementmaßnahmen besonders wichtiger Einrichtungen und wichtiger Einrichtungen

(1) Besonders wichtige Einrichtungen und wichtige Einrichtungen sind verpflichtet, geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen, die nach Absatz 2 konkretisiert werden, zu ergreifen, um Störungen der Verfügbarkeit, Integrität und Vertraulichkeit der informationstechnischen Systeme, Komponenten und Prozesse, die sie für die Erbringung ihrer Dienste nutzen, zu vermeiden und Auswirkungen von Sicherheitsvorfällen möglichst gering zu halten. Bei der Bewertung der Verhältnismäßigkeit der Maßnahmen nach Satz 1 sind das Ausmaß der Risikoexposition, die Größe der Einrichtung, die Umsetzungskosten und die Eintrittswahrscheinlichkeit und Schwere von Sicherheitsvorfällen sowie ihre gesellschaftlichen und wirtschaftlichen Auswirkungen zu berücksichtigen. Die Einhaltung der Verpflichtung nach Satz 1 ist durch die Einrichtungen zu dokumentieren.

(2) Maßnahmen nach Absatz 1 sollen den Stand der Technik einhalten, die einschlägigen europäischen und internationalen Normen berücksichtigen und müssen auf einem gefahrenübergreifenden Ansatz beruhen. Die Maßnahmen müssen zumindest Folgendes umfassen:

1. Konzepte in Bezug auf die Risikoanalyse und auf die Sicherheit in der Informationstechnik,
2. Bewältigung von Sicherheitsvorfällen,
3. Aufrechterhaltung des Betriebs, wie Backup-Management und Wiederherstellung nach einem Notfall, und Krisenmanagement,



Risikomanagement zur Cybersicherheit

Anforderung	Umsetzung
Kohärenz zwischen physischer Sicherheit und Cybersicherheit	Berücksichtigung von Cybersicherheit und nicht cyberbezogenen Risiken
Einsatz von Künstlicher Intelligenz	Verwendung von KI-Tools zur ressourcenwirksameren Abwehr von Cyberangriffen, insb. auch vor dem Kontext von KMU
Aktiver Cyberschutz	SzA, Verschlüsselung, Netzwerksegmentierung, Zugriffsregelung, Schwachstellenmanagement
Cyberhygiene	Zero-Trust, Update-Policy, Awareness, Netzwerkkartografie
Wirtschaftsspionage/Geschäftsgeheimnisschutz	Risikomanagement in der Beziehung mit Externen im weiter gefassten Ökosystem jenseits reiner Cybersicherheit
Governance auf Unternehmensleitungsebene	Leitungspersonen mit eigenem Know-how/Verantwortlichkeit
Dokumentation	Nachweis von Cybersicherheit als Prozessmanagement
Lieferkettenschutz	Untersuchung der Beziehungen zu externen IT-Lieferanten
Einbeziehung nichttechnischer Risikofaktoren	Rechtliche, politische und geostrategische Auswirkungen

Keine Cybersicherheit “um jeden Preis”

Welche Kritikalität besitzt eine Einrichtung? Ist sie in der Öffentlichkeit besonders exponiert?

Inwieweit ist eine Einrichtung in ihrer Funktion von vernetzten IT-Systemen abhängig?

Ist das Funktionieren der Einrichtung abhängig vom Funktionieren digitaler Lieferketten?

Hat es bereits Vorfälle in der Vergangenheit gegeben bzw. ist anzunehmen, dass sich Angriffe in Zukunft häufen werden?

Was könnten potenzielle Angreifer infolge einer erfolgreichen Kompromittierung der Einrichtung erlangen?

NIS 2: Es geht um Prozesse, Menschen und Technologie!

Vielen Dank!

Prof. Dr. Dennis-Kenji Kipker

cyberintelligence.institute
Research Director

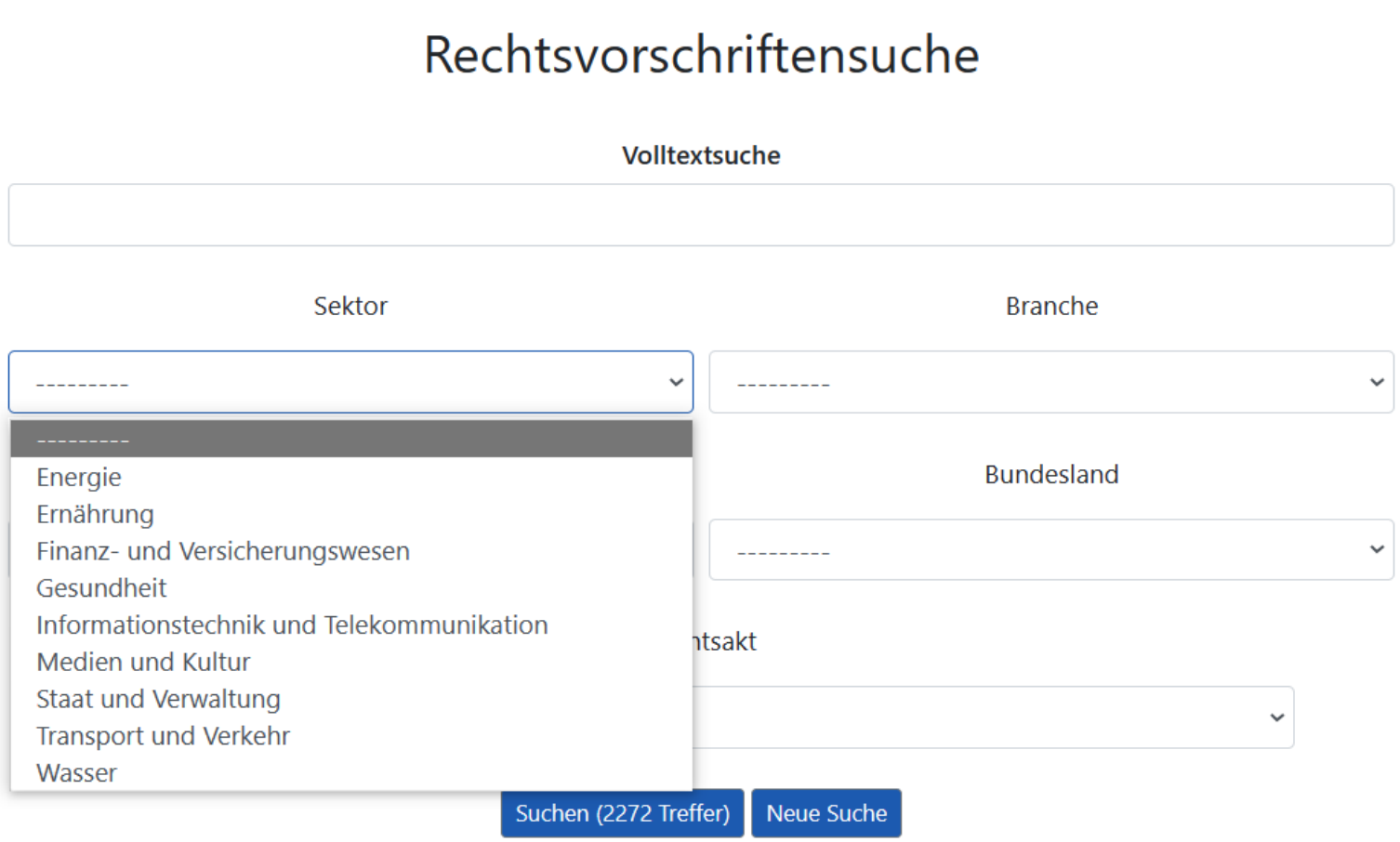
MesseTurm
Friedrich-Ebert-Anlage 49
60308 Frankfurt a.M.
GERMANY

dennis.kipker@cyberintelligence.institute

Cybersecurity Navigator

CYBERSECURITY
NAVIGATOR

https://cybersecurity-navigator.de



Weiterführende Literatur