Technische Hochschule Brandenburg
University of Applied Sciences

Security-Strategie als Unternehmensauftrag im Kontext NIS2

18. Security Forum

Johann Loran

15.01.2026

Bedrohungslage und EU NIS 2-Richtlinie

Cyber-Angriffe auf KRITIS Unternehmen richten nicht nur wirtschaftlichen Schäden an, sondern erschüttern das Vertrauen in staatliche Stabilität und Sicherheit!

Die EU stellt eine Vielzahl an EU-Digitalvorschriften auf, die die Cyber-Widerstandsfähigkeit steigern sollen!

Bedrohungslage

- IT-Sicherheitslage in Deutschland blieb angespannt und hoch gefährdet
- Anhaltende Zahl von Cybercrime-Fällen
- Ransomware-Attacken
- DDoS-Kampagnen
- politisch motivierte Angriffe aus dem Ausland

Hauptakteure

- Kriminelle Netzwerke & Ransomware (-aaS)
- Staatlich unterstützte bzw. staatliche Akteure (APT's)
- Hacktivisten & geopolitische Motive
- ➔ **verstärkte hybride Bedrohung**

Konkrete Angriffstrends 2025

- Phishing & Social Engineering
- Ransomware-Dominanz
- DDoS & hybride Angriffe
- KI-gestützte Angriffe

Gefahreneinschätzung

- Deutschland bleibt eines der Top-Ziele-Länder für Cyber-Angriffe in Europa
- Kritische Infrastruktur hat hohe Angriffsoberfläche, da oft nicht „state of the art"
- Kombination aus professionellen Gruppen, staatlich gesteuerten Akteuren und hybriden Motivationen (finanziell und/oder politisch)

Quellen: BSI "Die Lage der IT-Sicherheit in Deutschland 2025"; BKA „Bundeslagebild Cybercrime 2024/2025"; AG KRITIS Referentenentwurf „NIS 2-Umsetzung in Deutschland"

EU Cyber Security Regulierungen

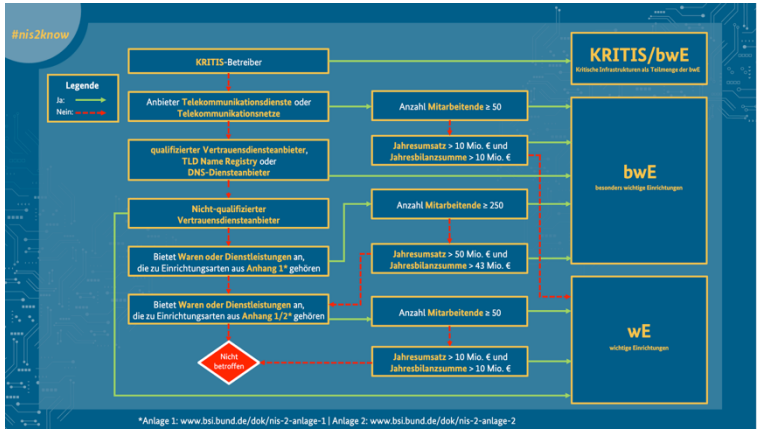
- **NIS2 Directive**
- Resilience of Critical Entities Directive (CER)
- Cyber Resilience Act (CRA)
- Digital Operational Resilience Act (DORA)
- Cyber Security Act (CSA)
- Cyber Solidarity Act (CSA)
- … weitere Regulierungen und Vereinfachungen (Digital Omnibus)

NIS2-Richtlinie

- „Mit der NIS2-Richtlinie wird ein einheitlicher Rechtsrahmen für die Aufrechterhaltung der **Cybersicherheit in 18 kritischen Sektoren** in der gesamten EU geschaffen."
- "Die Richtlinie schreibt vor, dass jeder Mitgliedstaat eine **nationale Cybersicherheitsstrategie** verabschiedet, die Strategien für die **Sicherheit der Lieferkette**, das **Schwachstellenmanagement** sowie die **Aufklärung und Sensibilisierung** im Bereich der Cybersicherheit umfasst."
- Security Fokusthemen:
  - Dokumentiertes Risikomanagement und Governance
  - Lieferkettensicherheit
  - Business Continuity
  - Schwachstellen-Management
  - Vorfallsberichtwesen
  - **Haftung der Geschäftsführung**

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

Betroffenheit feststellen



Quelle: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/NIS-2/nis-2-betroffenheit-entscheidungsbaum.pdf?__blob=publicationFile&v=15

Geldbußen bei Nichteinhalten

Dabei wird gem. § 65 BSIG zwischen zwei Kategorien unterschieden:

- Besonders wichtige Unternehmen:
  Hier können bei Verstößen Strafen von **bis zu 10 Mio. Euro oder 2 % des globalen Jahresumsatzes** verhängt werden.
- Wichtige Einrichtungen:
  Bei Nichteinhaltung drohen Bußgelder von **bis zu 7 Mio. Euro oder 1,4 % des Jahresumsatzes**.
- Anwendung von §30 (2) Satz 2 OWiG, wenn Umsatz größer 500 Mio. Euro.

Quelle: https://www.openkritis.de/betreiber/bussgelder-kritis-bsig.html

Most security strategies die as soon as they meet Q4, a cloud migration, or a Friday 4:59 pm incident!

Antipattern einer Strategie in der „Wildnis“

… wenn Ihre Strategie eine Abkürzungslegende benötigt, handelt es sich wahrscheinlich um einen Produktkatalog!

“strategy by shopping list” → Software/Hardware ≠ Auswahlmöglichkeit

“slideware strategy” → Hohe Ziele, sinnlose KPI’s und Maßnahmen, zahnlos in der Schublade

“buzzword soup” → Zero Trust + AI + XDR + SASE + [füge drei weitere hinzu]

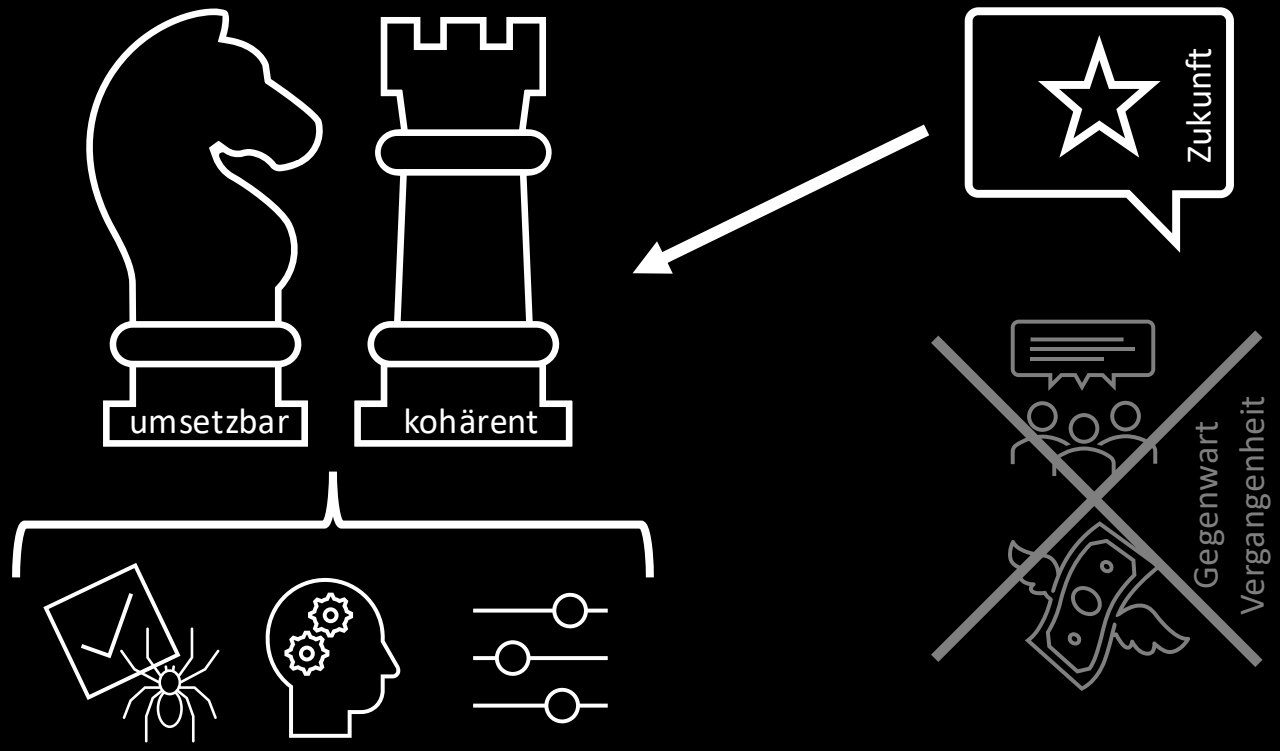
“everything is priority 1.” → Dies ist ein schlechter Plan das Fehlen einer Strategie zu verstecken

“busywork plan” → 1.000 Tickets ohne Zielverknüpfung

“comply harder” → Audit bestehen ≠ Angriffsresilienz

Eine gute Strategie macht die nächste taktische Entscheidung offensichtlich

… alles andere ist nur Rauschen, das Sie nicht kontrollieren können!



Erste Entscheidung zur NIS 2-Richtlinie

Im Management Team einfach Losrennen?

oder

Im Management Team nachdenken was zielführend ist?

Security-Strategie in vier Schritten aufsetzen

	Grundlagenarbeit	Mission, Vision und Zweck	Leitbild und -prinzipien	Strategische Zielvorgabe
Inputs	+ Geschäftsstrategie & weitere + Security Richtlinien + Regulatorische Auflagen	+ Kontext Dokumente	+ Mission, Vision, Zweck Statement	+ Mission, Vision, Zweck Statement + Leitprinzipien
Tools & Methoden	# SWOT, TOWS, PESTEL, etc. # Risikoappetit # Interviews und Dokumente	# Workshops # Abgleichsprüfungen # Strategielandkarte	# Kritische Erfolgsfaktoren # Wertstromanalyse # Einbettung in Governance Framework	# Workshops zur Zielsetzung und Priorisierung # GAP-Analysen # Szenarioplanung
Outputs	> Geschäftskontext > Security-Kontext	> Im Kontext nachvollziehbare Statements	> Leitprinzipien im Rahmen des Leitbilds	> Strategische Zielvorgaben (engl. objectives)

… und nun in die Umsetzung bringen

	Strategische Initiativen, Ziele, Metriken	Finanz- und Ressourcenplanung, Genehmigung	Kommunikation, kontinuierliche Überwachung
Inputs	+ Strategische Zielvorgaben + Liste laufender Initiativen, Programme, Projekte	+ Initiativen + Zielen und Metriken	> Genehmigte und zusammenhängende Strategie- und Planungs-Dokumente > Performance-Daten
Tools & Methoden	# PM/Pg Methoden # KPI und Dashboards # Trendanalysen	# Forecasting, Kosten-Nutzen-Analysen # Risikoszenarioplanung # Entscheidungsframeworks	# PM- und CM-Frameworks # Szenarioplanung zur Bedrohungslage # Audit und Compliance Checks
Outputs	> Plan mit strategischen Initiativen > Landkarte mit strategischen Zielen und Metriken	> Finanzprojektion > Ressourcenplan > Top Management-Genehmigung	> Kommunikationsplan > KVP-Plan

#Call to Action

Wende bewährte Methoden, Tools und Taktiken an!

Betrachte erste eine, dann inkludiere weitere betreffende Vorgaben!

Erstelle eine Security Strategie, die…

praktisch,
bedrohungs- & risikoinformiert,
und **geschäftsorientiert** ist

… sowie an einem Montag anwendbar ist!

Technische Hochschule Brandenburg
University of Applied Sciences

Vielen Dank für Ihre Aufmerksamkeit

Johann Loran
Senior Cyber Security Architect

LinkedIn: