Technische Hochschule Würzburg-Schweinfurt

FAKULTÄT INFORMATIK UND WIRTSCHAFTSINFORMATIK

VORLESUNGSSKRIPT

Informationssicherheitsrecht – KRITIS, NIS2 & Strafrecht

Rechtsquellen, Resilienz kritischer Einrichtungen, Cybersicherheitspflichten und Cyberstrafrecht

MODUL
Governance, Risk, Compliance & Ethics – Teil 2

SEMESTER
WS 26/27

VERSION
1.0

Prof. Dr. Markus Oermann
Dozent
markus.oermann@thws.de
Technische Hochschule Würzburg-Schweinfurt

Stand: 23.07.2026

Inhalt

In der vorangegangenen Einheit haben Sie gesehen, wie das Datenschutzrecht über Art. 32 DSGVO ein „angemessenes Schutzniveau" für personenbezogene Daten verlangt. Das heißt technische und organisatorische Maßnahmen, die Vertraulichkeit, Integrität und Verfügbarkeit sichern. Diese Pflicht ist zugleich der Brückenkopf in ein eigenständiges Rechtsgebiet: das **Informationssicherheitsrecht**. Wo der Datenschutz auf die einzelne Person blickt, fragt das Informationssicherheitsrecht nach der Funktionsfähigkeit ganzer Systeme und Versorgungsstrukturen. Ein Stromausfall, ein lahmgelegtes Krankenhaus, ein kompromittiertes Wasserwerk, das sind keine Datenschutzvorfälle, sondern Bedrohungen der **Resilienz** der Gesellschaft. Diese Einheit ordnet das junge, in den Jahren 2025/2026 grundlegend umgebaute Rechtsgebiet und zeigt seine drei Säulen: die physische Resilienz kritischer Einrichtungen, die Cybersicherheit in der Fläche und das flankierende Strafrecht.

01

KAPITEL

Die Rechtsquellen des Informationssicherheitsrechts

1.1 Eine kurze Geschichte: vom BSI-Errichtungsgesetz zur NIS2-Umsetzung

Das deutsche Informationssicherheitsrecht ist um eine zentrale Behörde herum gewachsen: das **Bundesamt für Sicherheit in der Informationstechnik (BSI)**. Mit dem BSI-Errichtungsgesetz vom 1.1.1991 entstand eine dem Bundesinnenministerium nachgeordnete Bundesoberbehörde. Lange blieb ihr Mandat beschränkt; erst 2009 wurden die Aufgaben des BSI erheblich erweitert und um eigene Befugnisse ergänzt. Den eigentlichen Wendepunkt markiert das **erste IT-Sicherheitsgesetz von 2015**: Es schrieb im BSI-Gesetz erstmals Vorgaben zur IT-Sicherheit Kritischer Infrastrukturen fest, flankiert durch sektorspezifische Regeln im Energiewirtschaftsgesetz, Atomgesetz, Telemediengesetz und Telekommunikationsgesetz. Parallel begann auf europäischer Ebene 2016 mit der ersten NIS-Richtlinie (EU) 2016/1148 die unionsweite Harmonisierung von Cybersicherheitsvorgaben. Das **IT-Sicherheitsgesetz 2.0 (2021)** verschärfte die Pflichten weiter. Die heutige Architektur entsteht jedoch erst mit der zweiten Generation der EU-Rechtsakte, die das nationale Recht seit 2025 tiefgreifend umbaut.

DEFINITION

Was ist das BSI?

Das Bundesamt für Sicherheit in der Informationstechnik ist die 1991 errichtete, dem BMI nachgeordnete Bundesoberbehörde für Cybersicherheit. Heute ist es die zentrale Aufsichts-, Melde- und Registrierungsstelle im BSIG.

1.2 Die EU-Ebene: ein Bündel paralleler Rechtsakte

Anders als das frühere, fragmentierte Recht verteilt sich das Informationssicherheitsrecht heute auf einen ganzen Strauß europäischer Instrumente, die jeweils einen Ausschnitt abdecken. - Die **CER-Richtlinie** (Critical Entities Resilience, Richtlinie (EU) 2022/2557) zielt auf die **physische** Resilienz kritischer Einrichtungen. - Die **NIS2-Richtlinie** (Richtlinie (EU) 2022/2555) regelt parallel die **Cybersicherheit** dieser und vieler weiterer Einrichtungen. - Für den Finanzsektor gilt mit **DORA** (Digital Operational Resilience Act, Verordnung (EU) 2022/2554) ein vorrangiger, unmittelbar geltender Sektorrechtsakt. - Hinzu treten die **KI-Verordnung** (Gegenstand der nächsten Einheit) und der **Cyber Resilience Act** (Cyber-Resilienz-Verordnung), der Sicherheitsanforderungen an Produkte mit digitalen Elementen stellt.

Wichtig ist die Rechtsnatur: CER und NIS2 sind **Richtlinien** und müssen erst in nationales Recht umgesetzt werden, während DORA, KI-VO und CRA als **Verordnungen** unmittelbar gelten.

1.3 Die Bundesebene und juristische Nebenaspekte

Auf der Bundesebene setzen zwei Gesetze die beiden Richtlinien um: Das **KRITIS-Dachgesetz (KRITIS-DachG)** setzt die CER-Richtlinie um, das novellierte **BSI-Gesetz (BSIG)** die NIS2-Richtlinie. Beide greifen ineinander – wer Betreiber einer kritischen Anlage nach KRITIS-DachG ist, unterliegt zugleich den schärfsten BSIG-Pflichten.

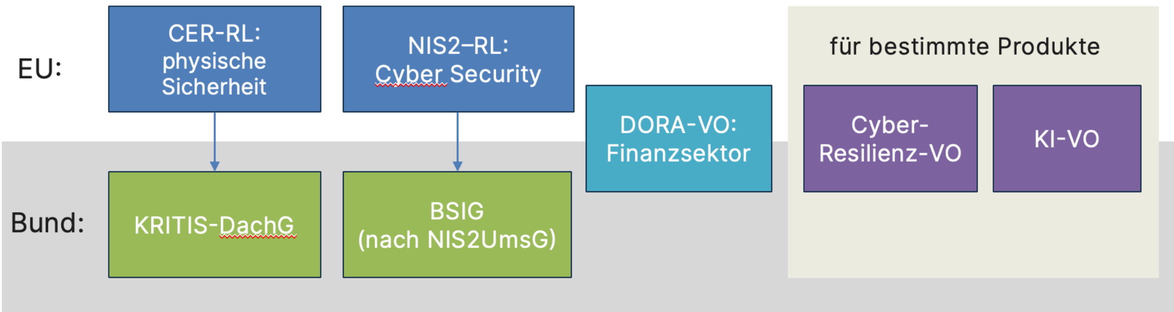

Abbildung 1: Überblick über das Zusammenspiel von EU-Richtlinien und deutschen Umsetzungsgesetzen im Informationssicherheitsrecht: CER-Richtlinie und NIS2-Richtlinie werden durch KRITIS-DachG und BSIG umgesetzt, DORA-VO gilt unmittelbar für den Finanzsektor, Cyber-Resilienz-VO und KI-VO für bestimmte Produkte (eigene Darstellung).

Daneben enthält die Rechtsordnung weitere, oft übersehene Anreize zur IT-Sicherheit: § 91 Abs. 2 AktG (für die GmbH § 43 Abs. 1 GmbHG) verpflichtet die Geschäftsleitung im Rahmen der Corporate Governance zur Einrichtung eines Überwachungssystems zur Früherkennung bestandsgefährdender Entwicklungen. Das **Geschäftsgeheimnisgesetz (GeschGehG)** schützt Geschäftsgeheimnisse nur, wenn „angemessene Geheimhaltungsmaßnahmen" getroffen wurden – also faktisch nur bei hinreichender IT-Sicherheit. Hinzu treten handels- und steuerrechtliche Dokumentationspflichten (§§ 238, 257 HGB; §§ 145–147 AO). Und schließlich setzt das allgemeine zivilrechtliche Haftungsrecht des BGB einen starken Anreiz: Wer Sorgfaltspflichten verletzt, haftet auf Schadensersatz.

ÜBUNG · BEGRIFFE

Ordnen Sie zu: Die **CER-Richtlinie** zielt auf physische Resilienz, die **NIS2-Richtlinie** auf Cybersicherheit, und **DORA** ist der vorrangige Sektorrechtsakt für den Finanzsektor.

QUICK-CHECK

Welche Aussage trifft zu?

- CER-Richtlinie und NIS2-Richtlinie sind unmittelbar geltende Verordnungen
- **CER-Richtlinie und NIS2-Richtlinie sind Richtlinien und werden durch KRITIS-DachG bzw. BSIG umgesetzt**
- Das KRITIS-Dachgesetz setzt die NIS2-Richtlinie um
- DORA ist auf alle Sektoren gleichermaßen anwendbar

02

KAPITEL

Resilienz kritischer Einrichtungen: CER-Richtlinie und KRITIS-Dachgesetz

2.1 Ziel und der All-Gefahren-Ansatz

Die CER-Richtlinie und ihr deutsches Umsetzungsgesetz verfolgen ein anderes Ziel als die Cybersicherheitsregeln: Es geht um die **Ausfallsicherheit kritischer Einrichtungen durch physischen, „analogen" Schutz**, um die Verfügbarkeit kritischer Dienstleistungen abzusichern. Leitidee ist der **All-Gefahren-Ansatz**: Geschützt wird nicht nur gegen Cyberangriffe, sondern gegen sämtliche Gefahren: Naturkatastrophen, Sabotage, terroristische Anschläge, Klimafolgen oder menschliches Versagen. Erfasst werden **elf Sektoren** essenzieller Dienstleistungen (Annex CER-RL, § 4 Abs. 1 KRITIS-DachG): Energie, Transport, Banken, Finanzmärkte, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, Raumfahrt und Ernährung. Die genaue Abgrenzung der Sektoren weicht in Deutschland leicht von der Richtlinie ab.

Das KRITIS-Dachgesetz ist Anfang 2026 in Kraft getreten. Die Registrierung der Betreiber ist **ab dem 17.7.2026** verpflichtend. Das ist der für die Praxis entscheidende Stichtag.

2.2 Registrierung, Risikoanalyse und Resilienzplan

Der Pflichtenkreis baut sich in Stufen auf. Zunächst müssen alle Unternehmen identifiziert und **registriert** werden, die in einem der Sektoren eine essenzielle Dienstleistung erbringen, ihren Geschäftsbetrieb und ihre kritische Infrastruktur in Deutschland haben und deren Ausfall signifikante disruptive Effekte hätte (Art. 6 CER-RL; §§ 2, 8 KRITIS-DachG). Der maßgebliche

Schwellenwert liegt bei der Versorgung von in der Regel **mehr als 500.000 Personen** (§ 5 Abs. 2 KRITIS-DachG). Das Nähere definiert eine ergänzende KRITIS-Verordnung. Die Unternehmen sollen sich grundsätzlich **selbst registrieren** (§ 8 Abs. 1 KRITIS-DachG).

Nach der Registrierung folgen die inhaltlichen Pflichten. Betreiber müssen innerhalb von neun Monaten eine **Risikoanalyse** durchführen, um ihre Ausfallrisiken zu beurteilen; diese ist mindestens **alle vier Jahre** zu wiederholen (Art. 12 CER-RL; § 12 Abs. 1 KRITIS-DachG). Auf dieser Grundlage sind verhältnismäßige TOMs nach dem Stand der Technik zu treffen (§ 13 KRITIS-DachG), die in einem dokumentierten **Resilienzplan** zusammengefasst werden (§ 13 Abs. 4 KRITIS-DachG). Branchenverbände können branchenspezifische Resilienzstandards vorschlagen, deren Eignung das **Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK)** – ggf. im Einvernehmen mit dem BSI – auf Antrag feststellt (§ 14 KRITIS-DachG). Schließlich besteht eine **Meldepflicht**: Betreiber müssen ihre Behörden unverzüglich, spätestens in 24 Stunden, über signifikante Störungen unterrichten (Art. 15 CER-RL; § 18 KRITIS-DachG).

Maßnahmenfeld	Beispielhafte Anforderung
Notfallvorsorge	Prävention gegen Vorfälle und Klimafolgen
Physische Sicherheit	Absicherung der Liegenschaften, Überwachung, Zutrittskontrolle
Krisenreaktion	Krisenmanagement mit definierten Prozeduren und Alarmierung
Wiederherstellung	Business Continuity Management, alternative Lieferketten
Personal	Sicherheitsüberprüfung, auch externes Personal und Dienstleister
Schulungen	regelmäßige Übungen für das Personal

2.3 Durchsetzung und Geschäftsleiterhaftung

Damit die Pflichten nicht folgenlos bleiben, ordnet § 20 KRITIS-DachG eine **direkte Verpflichtung und Haftung der Geschäftsleitung** an. Die Aufsichtsbehörden erhalten Befugnisse zu Inspektionen, Audits und anschließenden Anweisungen; bei Verstößen sollen angemessene Sanktionen verhängt werden können (Art. 21, 22 CER-RL; §§ 16, 24 KRITIS-DachG). Betreiber von **besonderer europäischer Relevanz**, die mindestens sechs EU-Mitgliedstaaten mit essenziellen Dienstleistungen versorgen, werden identifiziert, der EU-Kommission gemeldet und besonders überwacht (Art. 17, 18 CER-RL; § 9 KRITIS-DachG).

03
KAPITEL

Cybersicherheit: NIS2-Richtlinie und BSI-Gesetz

3.1 Regelungsziel und das Verhältnis zu CER

Während CER und KRITIS-DachG die physische Resilienz adressieren, regelt die NIS2-Richtlinie die **Cybersicherheit** und zwar mit deutlich größerem Adressatenkreis. Ihr Ziel ist die Gewährleistung von Cybersicherheit in der Fläche, auf einem vergleichbar hohen Niveau in der gesamten EU. Die Umsetzung im BSIG trat **am 6. Dezember 2025** in Kraft. Vorrangig bleiben sektorspezifische Regelungen: für Telekommunikationsanbieter das Telekommunikationsgesetz, für Energieversorger das Energiewirtschaftsgesetz, für Finanzdienstleister die **DORA**-Verordnung. Erfasst werden zunächst alle Betreiber kritischer Anlagen nach KRITIS-DachG. Die BSIG-Pflichten treffen jedoch zusätzlich **viele weitere Unternehmen**.

3.2 Anwendungsbereich: zwei Klassen von Einrichtungen

Hier liegt die zentrale Verschiebung gegenüber dem alten Recht: Statt eines engen KRITIS-Begriffs unterscheidet das BSIG nun **zwei Größenklassen** in einer breiten Liste von Sektoren (Anlage 1 und 2 BSIG: u. a. Energie, Transport/Verkehr, Finanz-/Versicherungswesen, Gesundheit, Wasser/Abwasser, IT/Telekommunikation, Weltraum, Lebensmittel, Post- und Kurierdienste, Abfallbewirtschaftung, chemische Stoffe, Warenproduktion, digitale Dienste, Forschung). Die Zuordnung folgt einer Schwellenwertlogik.

Klasse	Schwellenwert (i. d. R.)	Rechtsgrundlage
Besonders wichtige Einrichtung	> 250 Beschäftigte **ODER** (> 50 Mio. € Umsatz **UND** > 43 Mio. € Bilanzsumme)	§ 28 Abs. 1 BSIG
Wichtige Einrichtung	> 50 Beschäftigte **UND** (> 10 Mio. € Umsatz **UND** > 10 Mio. € Bilanzsumme)	§ 28 Abs. 2 BSIG
Betreiber kritischer Anlagen	unabhängig von der Größe	stets besonders wichtige Einrichtung

Achten Sie auf die Verknüpfungen: Für die *besonders wichtige* Einrichtung genügt **eines** der beiden Kriterien (Beschäftigtenzahl ODER der Umsatz-und-Bilanz-Block), während die *wichtige* Einrichtung **beide** Schwellen kumulativ erfüllen muss. Und beachten Sie: NIS2/BSIG knüpft, anders als das KRITIS-DachG mit seiner Schwelle von 500.000 versorgten Personen, an die **Unternehmensgröße** (Beschäftigte, Umsatz, Bilanz) an, nicht an die Zahl der versorgten Personen.

Betreiber kritischer Anlagen nach KRITIS-DachG sind also **stets** besonders wichtige Einrichtungen. Weil die Selbsteinordnung in der Praxis schwierig ist, hat das BSI eine **NIS2-Betroffenheitsprüfung** online gestellt: https://betroffenheitspruefung-nis-2.bsi.de/

Verantwortlich im Unternehmen sind die **Geschäftsführer**: Sie haften bei Verstößen und müssen regelmäßig an Schulungen teilnehmen (§ 38 BSIG).

Prüfen Sie im folgenden Widget selbst, welcher Klasse eine Einrichtung mit speziellen Eigenheiten zuzuordnen ist und welche Kernpflichten daraus folgen:

3.3 Pflichten: Registrierung, Risikomanagement, Meldung

Die Pflichten nach dem BSIG sind gestuft. **Alle** erfassten Einrichtungen müssen sich beim BSI registrieren (§§ 33, 34 BSIG), Risikomanagementmaßnahmen nach dem Stand der Technik treffen (§ 30 BSIG) und Sicherheitsvorfälle melden (§ 32 BSIG). Die Meldekette ist dreistufig: **Erstmeldung innerhalb von 24 Stunden**, Detailmeldung innerhalb von 72 Stunden, Abschlussmeldung innerhalb eines Monats. Bei erheblichen Vorfällen kommt die Unterrichtung von Kunden und Öffentlichkeit hinzu (§§ 35, 36 BSIG).

Besonders wichtige Einrichtungen müssen zusätzlich proaktiv den Nachweis ihrer Risikomanagementmaßnahmen erbringen (§ 39 BSIG). Kritisch anzumerken ist hierbei, dass die Bundesverwaltung selbst keine entsprechenden Risikomanagementmaßnahmen vorsehen muss (§ 29 Abs. 2 BSIG).

Der **Mindestumfang** der Risikomanagementmaßnahmen ist in § 30 Abs. 2 BSIG katalogisiert: Konzepte zur Risikoanalyse und zur Bewältigung von Sicherheitsvorfällen, Aufrechterhaltung des Betriebs (Backup-Management, Wiederherstellung, Krisenmanagement), Sicherheit der Lieferkette, Sicherheit bei Erwerb, Entwicklung und Wartung von IT, Verfahren zur Wirksamkeitsbewertung, Cyberhygiene und Schulungen, Kryptografie und Verschlüsselung, Personalsicherheit und Zugriffskontrolle sowie Multi-Faktor-Authentifizierung und gesicherte Kommunikation zählen dazu.

3.4 Aufsicht und Sanktionen

Die Aufsichtsintensität staffelt sich nebenfalls nach der Einrichtungsklasse: Bei besonders wichtigen Einrichtungen hat das BSI **anlasslose**, weitgehende Aufsichts- und Durchsetzungsbefugnisse (§ 61 BSIG), bei wichtigen Einrichtungen greift es nur bei Hinweisen auf Verstöße ein (§ 62 BSIG).

Geldbußen sind bei Verstößen bis zu **10 Mio. Euro oder zwei Prozent** des weltweiten Jahresumsatzes möglich (§ 65 BSIG) – ein bewusst an die DSGVO angelehntes, abschreckendes Sanktionsniveau.

FALLSTUDIE

Das mittelständische Maschinenbauunternehmen

Ein Maschinenbauunternehmen (Sektor Warenproduktion) beschäftigt 180 Personen, erwirtschaftet 35 Mio. € Umsatz bei 20 Mio. € Bilanzsumme. Die Geschäftsführung geht davon aus, mangels „kritischer Infrastruktur" von NIS2 nicht betroffen zu sein, und investiert nicht in ein Risikomanagementsystem. Trifft diese Einschätzung zu?
Lösung. Nein. Das Unternehmen ist in einem erfassten Sektor (Anlage 1/2 BSIG) tätig. Es überschreitet die Schwelle der **wichtigen Einrichtung** (§ 28 Abs. 2 BSIG): mehr als 50

Beschäftigte und mehr als 10 Mio. € Umsatz und Bilanzsumme. Eine besonders wichtige Einrichtung ist es nicht, weil es weder über 250 Beschäftigte hat noch die Umsatz-/Bilanzschwelle von 50/43 Mio. € erreicht.
Als wichtige Einrichtung treffen es gleichwohl Registrierung (§§ 33, 34 BSIG), Risikomanagement (§ 30 BSIG) und die dreistufige Meldepflicht (§ 32 BSIG). Bleibt die Geschäftsführung untätig, haftet sie persönlich (§ 38 BSIG), und es drohen Bußgelder. Der verbreitete Irrtum, NIS2 betreffe nur „die großen KRITIS-Betreiber", ist daher gefährlich.

04

KAPITEL

Relevante Straftatbestände des Cyberstrafrechts

4.1 Der Kernbestand: §§ 202a–c und 303a/b StGB

Das Informationssicherheitsrecht wird strafrechtlich flankiert. Den Kern bildet eine Gruppe von „Computerdelikten" im StGB.

§ 202a (Ausspähen von Daten) stellt unter Strafe, wer sich unbefugt unter Überwindung einer Zugangssicherung Zugang zu besonders gesicherten, nicht für ihn bestimmten Daten verschafft (Freiheitsstrafe bis drei Jahre oder Geldstrafe).

§ 202b (Abfangen von Daten) erfasst das unbefugte Abfangen nicht-öffentlicher Datenübermittlungen oder elektromagnetischer Abstrahlung mit technischen Mitteln. Auf der Schädigungsseite stehen

§ 303a (Datenveränderung) – das rechtswidrige Löschen, Unterdrücken, Unbrauchbarmachen oder Verändern von Daten – und **§ 303b (Computersabotage)**, der Störungen von Datenverarbeitungen erfasst, die für einen anderen von wesentlicher Bedeutung sind. Vermögensbezogen ergänzt

§ 263a (Computerbetrug) den klassischen Betrug um die Manipulation von Datenverarbeitungsvorgängen. Hinzu treten § 268 (Fälschung technischer Aufzeichnungen) und § 274 (Urkundenunterdrückung).

DEEP DIVE **Wortlaut § 202a Abs. 1 StGB**

„Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.” Absatz 2 stellt klar, dass Daten nur solche sind, die elektronisch, magnetisch oder sonst nicht unmittelbar wahrnehmbar gespeichert sind oder übermittelt werden.

4.2 Der Hackerparagraf § 202c und das Dual-Use-Problem

Besondere Aufmerksamkeit verdient **§ 202c StGB**, der sogenannte „Hackerparagraf”. Er verlagert die Strafbarkeit ins **Vorbereitungsstadium**: Strafbar macht sich bereits, wer eine Tat nach § 202a oder § 202b vorbereitet, indem er Passwörter, Sicherungscodes oder Computerprogramme, deren Zweck die Begehung einer solchen Tat ist, herstellt, sich verschafft, verkauft, überlässt, verbreitet oder sonst zugänglich macht (Freiheitsstrafe bis zwei Jahre oder Geldstrafe). Das Problem liegt in der **Dual-Use-Natur** vieler Sicherheitswerkzeuge: Portscanner, Exploit-Frameworks oder Passwort-Cracker werden sowohl von Angreifern als auch von legitimen Penetrationstesterinnen eingesetzt. Heikel ist insbesondere das **Ethical Hacking / Penetration Testing ohne Auftrag** des Betroffenen – etwa wenn Sicherheitsforscher Schwachstellen öffentlicher Stellen aufdecken. Eine Reform der §§ 202a ff. StGB, die legitime Sicherheitsforschung rechtssicher stellen soll, befindet sich schon seit längerem in Abstimmung.

DEEP DIVE Verfassungskonforme Einschränkung durch das BVerfG (2009)

Das Bundesverfassungsgericht hat die Schärfe des § 202c StGB bereits 2009 abgemildert (Beschluss vom 18.5.2009 – 2 BvR 2233/07 u. a.): Strafbar macht sich nur, wer das Werkzeug **mit dem Vorsatz einer rechtswidrigen Tat** nach § 202a oder § 202b herstellt, sich verschafft oder verbreitet. Der bloße Besitz oder der Einsatz von Dual-Use-Software zu legitimen Zwecken – etwa beim beauftragten Penetrationstest – erfüllt den Tatbestand nicht. Das entschärft das Dual-Use-Problem dogmatisch, beseitigt aber die Rechtsunsicherheit im unbeauftragten Graubereich nicht vollständig.

QUICK-CHECK

Warum ist § 202c StGB für Sicherheitsforscherinnen problematisch?

- Weil er nur vollendete Angriffe erfasst
- **Weil er bereits die Vorbereitung mit Dual-Use-Werkzeugen unter Strafe stellt und Penetrationstests ohne Auftrag erfasst**
- Weil er ausschließlich auf öffentliche Stellen anwendbar ist
- Weil er Geldbußen bis 10 Mio. Euro vorsieht

05

KAPITEL

Ausblick

Sie haben damit die drei tragenden Säulen des Informationssicherheitsrechts kennengelernt: die physische Resilienz kritischer Einrichtungen (CER-RL/KRITIS-DachG), die flächendeckende Cybersicherheit (NIS2-RL/BSIG) und das flankierende Cyberstrafrecht. Gemeinsam ist den beiden erstgenannten eine Verschiebung vom punktuellen Schadensausgleich hin zu **vorausschauenden, lebenszyklusbezogenen Pflichten** mit persönlicher Verantwortung der Geschäftsleitung. Genau dieses Muster, risikobasierte Pflichten über den gesamten Lebenszyklus eines Systems, kehrt in der nächsten Einheit wieder, wenn wir mit der **KI-Verordnung** den wohl ehrgeizigsten Baustein der digitalen Rechtsordnung untersuchen.

06

KAPITEL

Quellen

6.1 Normen & Standards

- Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über die Resilienz kritischer Einrichtungen (CER-Richtlinie). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2557
- Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS2-Richtlinie). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022L2555
- Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz – BSIG). https://www.gesetze-im-internet.de/bsig_2025/
- KRITIS-Dachgesetz (KRITIS-DachG), in Kraft seit Anfang 2026. https://www.gesetze-im-internet.de/kritisdachg/
- Strafgesetzbuch (StGB), §§ 202a–202c, 263a, 268, 274, 303a, 303b. https://www.gesetze-im-internet.de/stgb/
- Verordnung (EU) 2022/2554 (DORA – Digital Operational Resilience Act). https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32022R2554