CYTAKTICS 5

Strategien und operative Cybersicherheit

Jahrestagung Zentrum für Digitale Transformation

2026/11/05

CYBERSECURITY IN BRANDENBURG

ZUR PERSON

Kurz & Knapp

Senior Manager Cyber und Information Security

- Spezialisierung auf die Sektoren Industrie und Government
- Gründung x-net training & solutions im Jahre 2003 (Projektbegleitungen und Audits in den Themengebieten der Informationssicherheit)
- Seit 2014 Auditorin und Referentin für die TÜV NORD Gruppe
- 2021 bis Anfang 2025 Leiterin CERT Land Brandenburg
- 2025 Gründung des neuen Unternehmens „CYTAKTICS 5“



CYTAKTICS 5
Strategien und operative Cybersicherheit

CYTAKTICS 5

Strategien und operative Cybersicherheit

Agenda:

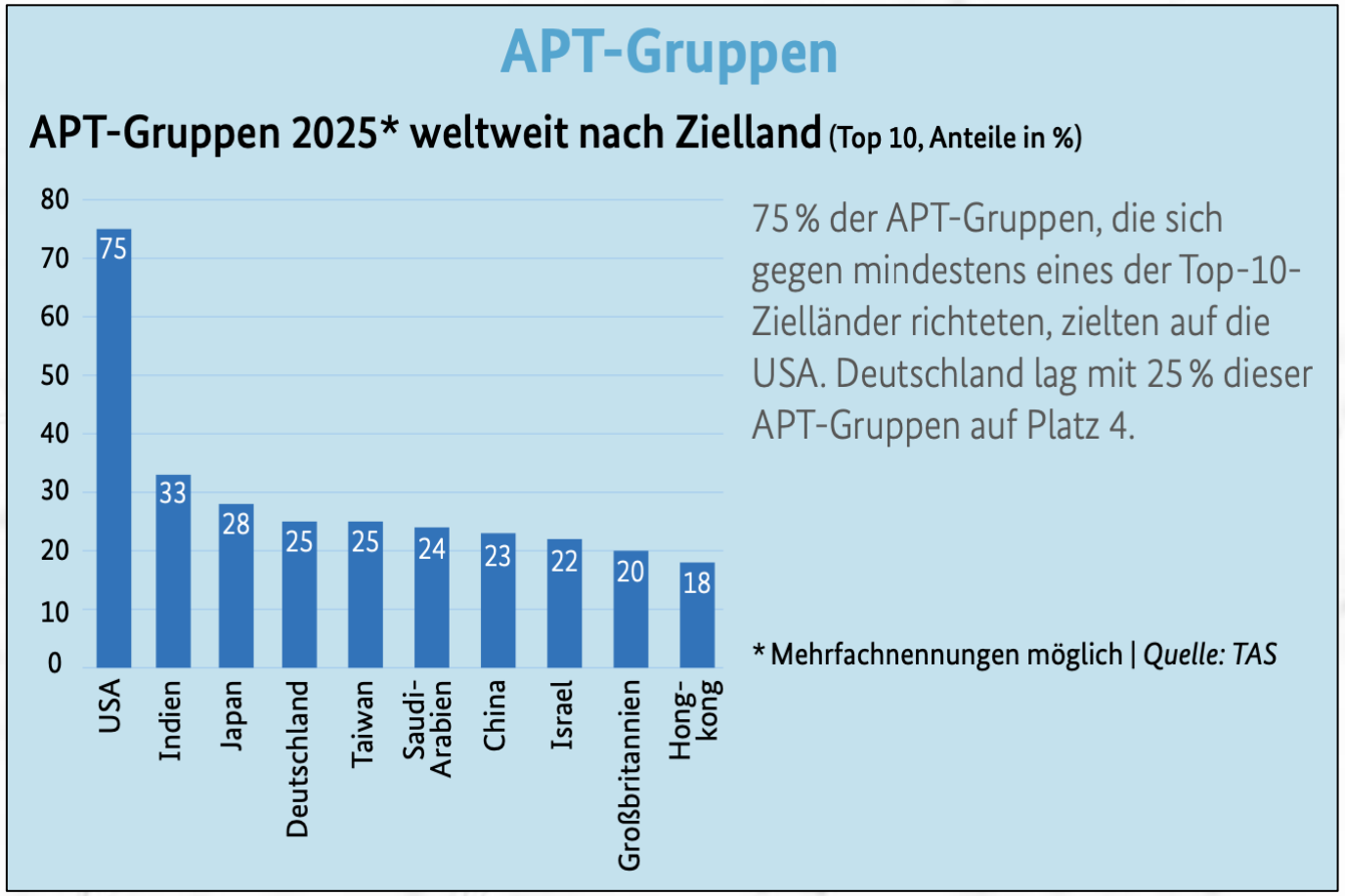
- Bedrohungslage
- rechtlicher Kontext
- Cyberstrategie Brandenburg
- Maßnahmen BSI Gesetz (NIS-2)

CYBERSECURITY IN BRANDENBURG

Einführung

BEDROHUNGSLAGE

BEDROHUNGSLAGE



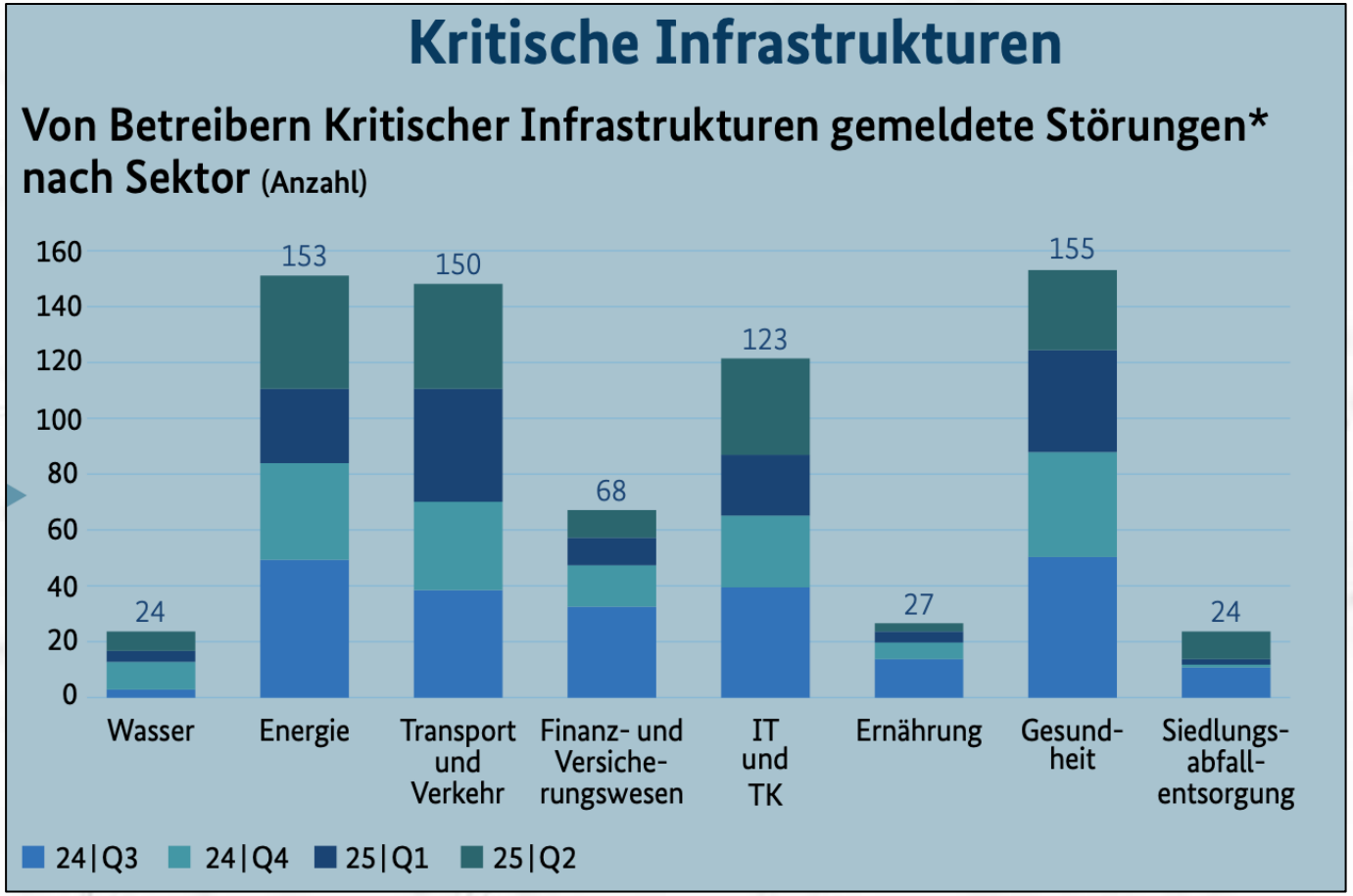
DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2025 (BSI)

Deutschland liegt auf **Platz 4** im internationalen Ranking bei **gezielten**, komplexen **Cyberangriffen** durch hochgradig spezialisierte Tätergruppen. Diese werden durch Sponsoren finanziert und verfolgen meist politische Ziele.

APT= Advanced Persistent Thread

Quellenverweis: [01]

BEDROHUNGSLAGE



DIE LAGE DER IT-SICHERHEIT IN DEUTSCHLAND 2025 (BSI)

In fast allen Sektoren verzeichnet das BSI im Berichtszeitraum **mehr** gemeldete **Störungen** als im vorherigen Berichtszeitraum.

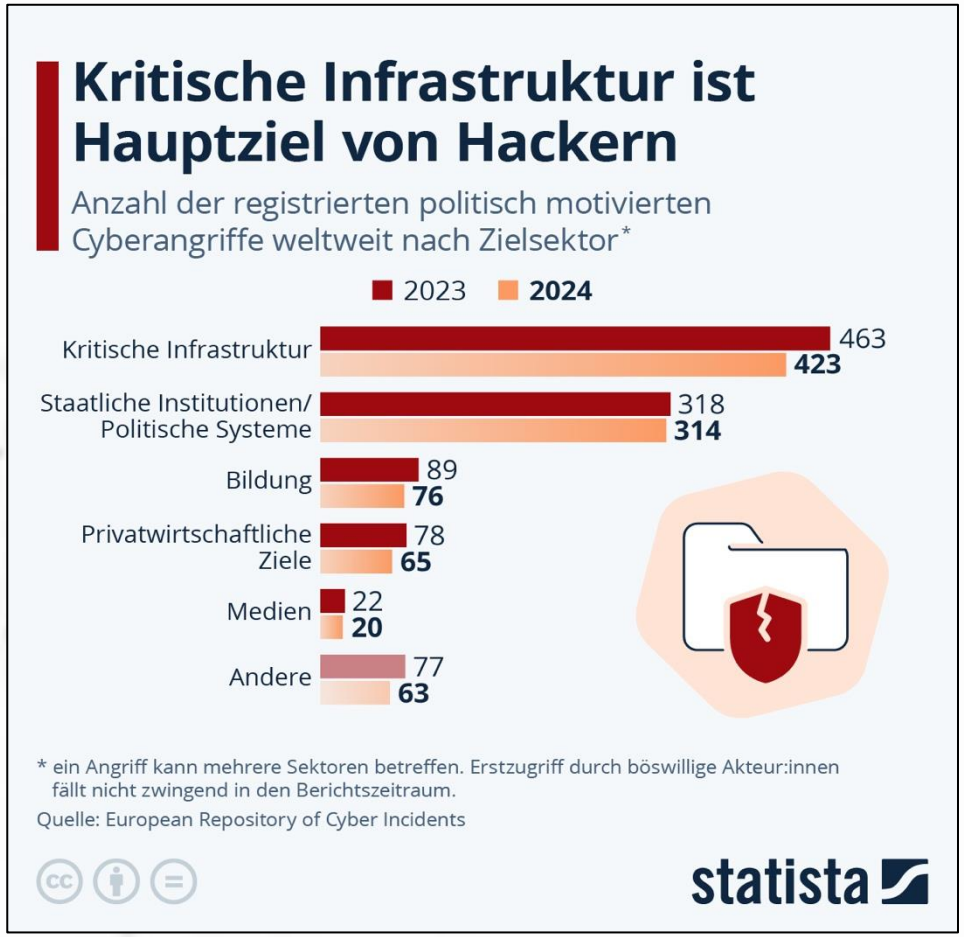
Quellenverweis: [01]

BEDROHUNGSLAGE

Hoch dynamische + geopolitische Lage

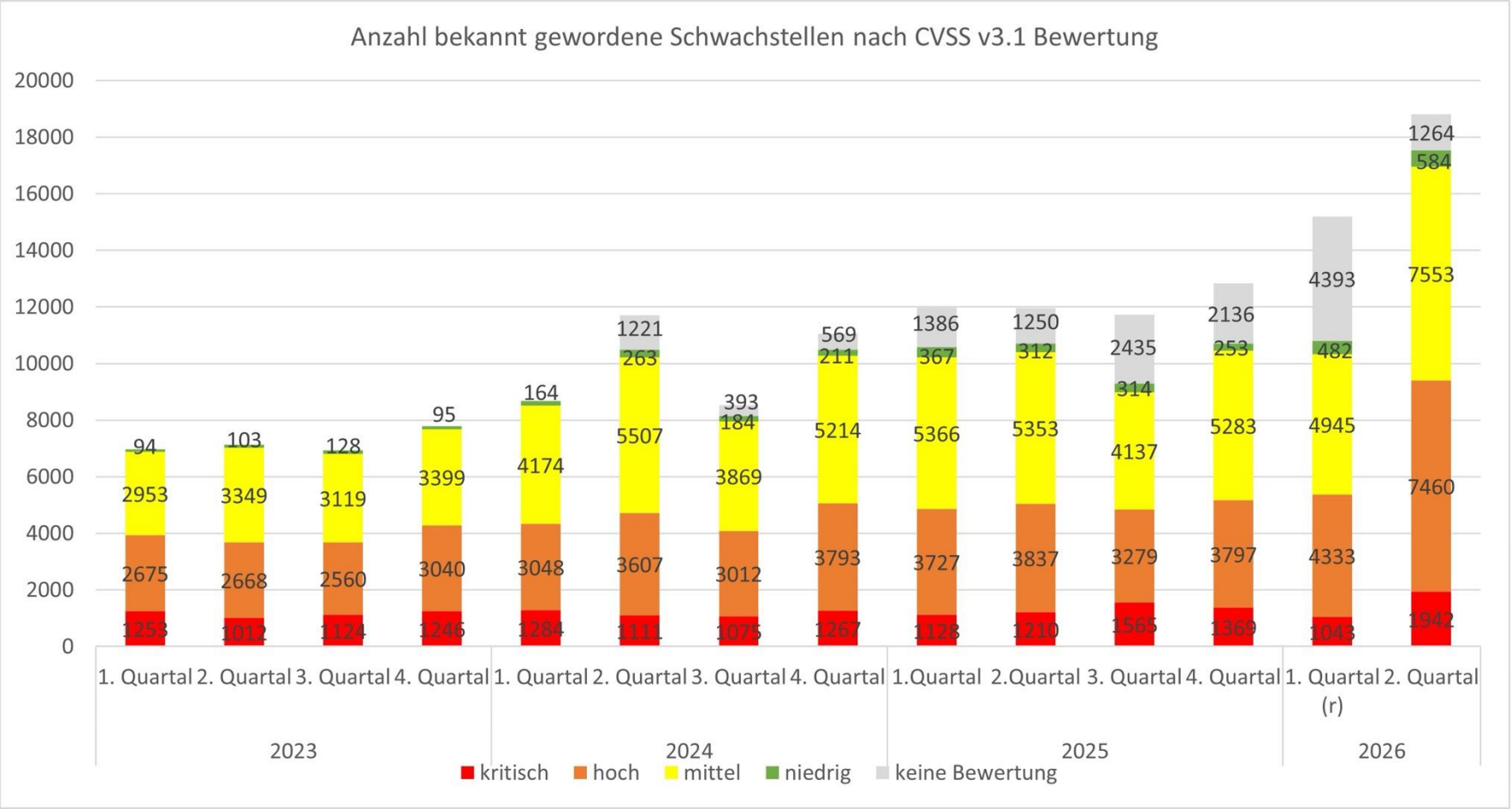
„Häufigstes Ziel der Hacker sind **Behörden**, Sicherheitsunternehmen, Medien oder andere **Kritische Infrastrukturen**. In den Jahren 2023 und 2024 wurden jeweils mehr als 400 Vorfälle in Branchen wie Energie, Telekommunikation, Verkehr oder Bildung in die Datenbank aufgenommen, gefolgt von Angriffen auf staatliche Institutionen oder politische Systeme (jeweils mehr als 300 Vorfälle).

Insgesamt verzeichnete das EuRepoC für 2024 insgesamt 740 Cybervorfälle mit politischer Dimension, wobei viele dieser Attacken mehr als einen Bereich ins Visier genommen haben.“



Quellenverweis: [02]

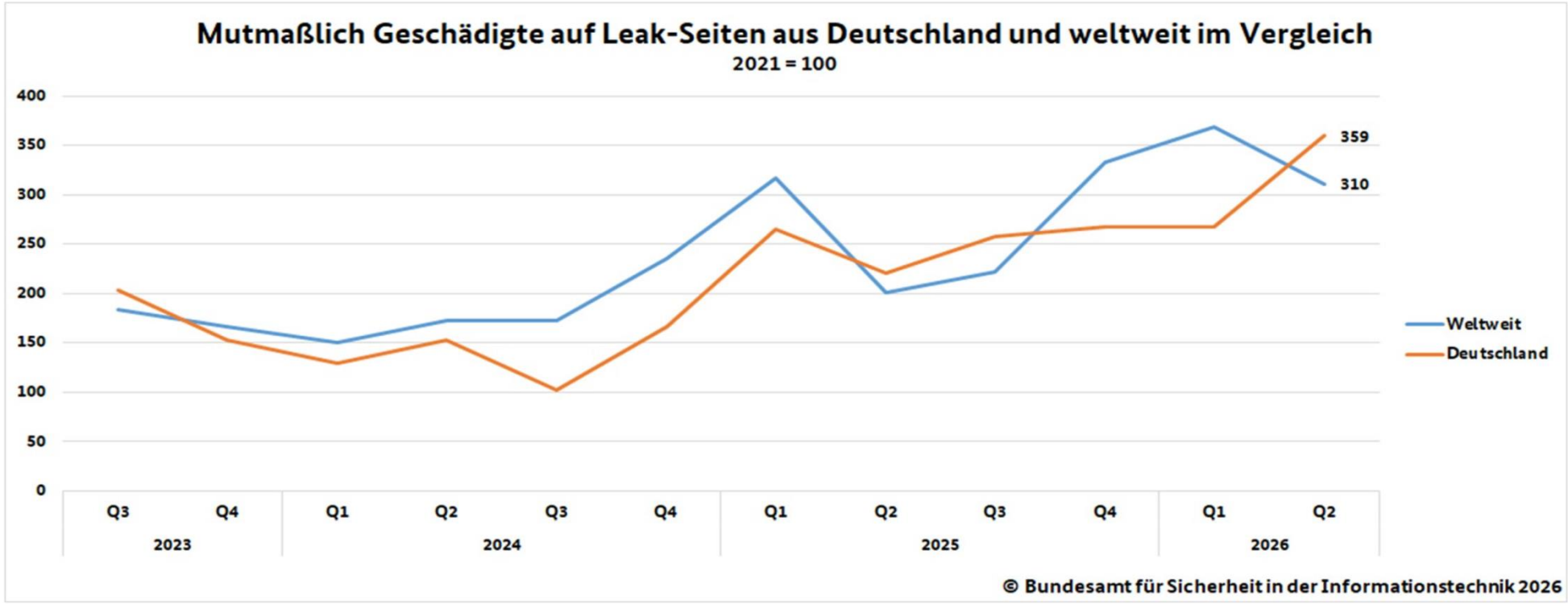
WACHSTUM DER GEMELDETEN SCHWACHSTELLEN



Quellenverweis: [03]

GESCHÄDIGTE AUS LEAK-SEITEN PRO QUARTAL

Mutmaßlich Geschädigte auf Leak-Seiten aus Deutschland und weltweit im Vergleich pro Quartal



Mutmaßlich Geschädigte auf Leak-Seiten aus Deutschland und weltweit im Vergleich pro Quartal
Quelle: BSI

Quellenverweis: [03]

BEDROHUNGSLAGE

Sicherheitsvorfälle von großer Tragweite

2026 Erheblicher Sicherheitsvorfall Land Berlin bei zwei Senatsverwaltungen

- Eine kriminelle Angreifergruppe hat sich Zugriff auf das digitale Netzwerk der Berliner Verwaltung verschafft, Datenbestände kopiert und diese am 4. September 2026 im Darknet veröffentlicht.

2025 Cyberangriff trifft europäische Flughäfen

- Ein IT-Dienstleister für die Check-In Abfertigung war am 19.09.2025 zur Zielscheibe eines Cyberangriffs geworden, wie er der Deutschen Presse-Agentur bestätigte. Die Hintergründe des Cyberangriffs sind weiterhin unklar.

2023 mehrere Angriffe auf E-Mail-Accounts im politischen Kontext

Im Januar 2023 verschafften sich unbekannte Hacker Zugriff auf eine einstellige Zahl an E-Mail-Postfächern des SPD-Parteivorstands. Die Täter nutzten dabei eine zu diesem Zeitpunkt noch unbekannte Schwachstelle in einer Microsoft-Software.

BEDROHUNGSLAGE

Sicherheitsvorfälle von großer Tragweite

2022 Angriff auf Satelliteninfrastruktur

- aufgrund eines Cyberangriffs fällt im europäischen Raum ein Satellitendienst aus, über welchen u. a. Prozesse zur Entstörung von Windenergieanlagen in der Strombranche mittels Satellitenkommunikationslösungen unterhalten werden. Infolge des Angriffs konnten rund 5.800 Windenergieanlagen nicht mehr mittels Fernwartung gewartet werden.

2021 Schwachstelle Log4shell

- Die kritische Schwachstelle (Log4Shell) in der weit verbreiteten Java-Bibliothek führt zu einer extrem kritischen Bedrohungslage. BSI erhöht die Cybersicherheitswarnung auf Warnstufe Rot.

2021 1. digitaler Katastrophenfall in Deutschland

- Eine Landkreisverwaltung in Sachsen-Anhalt im 5. Juli 2021 zum Ziel eines Ransomware-Angriffs. Sämtliche IT-Systeme aller Standorte der Kreisverwaltung sind beeinträchtigt. In der Folge des Angriffs konnten keine Dienste für Bürgerinnen und Bürger erbracht werden. Am 9. Juli 2021 stellte der Landkreis den örtlichen Katastrophenfall fest.

BEDROHUNGSLAGE UNIVERSITÄTEN

Universität / Einrichtung	Zeitpunkt	Ausmaß / Folgen
LMU München	September 2026	Datenleck betrifft rund 600.000 Datensätze von aktuellen und ehemaligen Studierenden aus den letzten 50 Jahren.
Universität Kopenhagen	Oktober 2026	Angriff auf eine Testumgebung; Abfluss von Daten von etwa 525.000 Personen.
MLU Halle-Wittenberg	Oktober 2026	Potenziellem Datenabfluss von rund 51.000 Studienbewerbern; Systeme wurden tagelang offline genommen.
Universität Leipzig	Oktober 2026	Komplette Abschaltung aller internetverbundenen Server zur Schadensabwehr; Ausfall des Mailverkehrs.
Hochschulservicezentrum BW (HSZ)	Oktober 2026	Lahmlegung der zentralen Verwaltungssysteme (z.B. Noten- und Campusportale) für zahlreiche Kunst-, Musik- und angewandte Hochschulen in Baden-Württemberg.

BEDROHUNGSLAGE

Zunahme von Sabotage und Terrorismus

- Anschläge auf die Infrastruktur der Stromversorgung
- vermehrtes Drohnenaufkommen mit politisch motivierten Zielen
- Anschläge auf den Schienenverkehr
- Desinformation durch u.a. Deep Fakes
- Manipulation der OT (z. B. Kühlschränke)

BEDROHUNGSLAGE

Schäden und deren Auswirkungen

- Laut bitkom Studie zum Wirtschaftsschutz 2026[04] steigt der **Schaden** im Zusammenhang mit Diebstahl, Industriespionage oder Sabotage in 2025 erneut auf nunmehr **289,2 Milliarden Euro**
  - Vergleich 2024: 266,6 Milliarden Euro
  - Vergleich 2023: 205,9 Milliarden Euro
- Spitzenreiter der Schadensauswirkungen betrifft **Ausfall, Diebstahl oder Schädigung** von Informations- und Produktionssystemen oder Betriebsabläufen
- Kosten für Ermittlungen und Ersatzmaßnahmen betrugen 37 Mrd. Euro

ALLGEMEINER RECHTLICHER KONTEXT

WORUM GEHT ES?

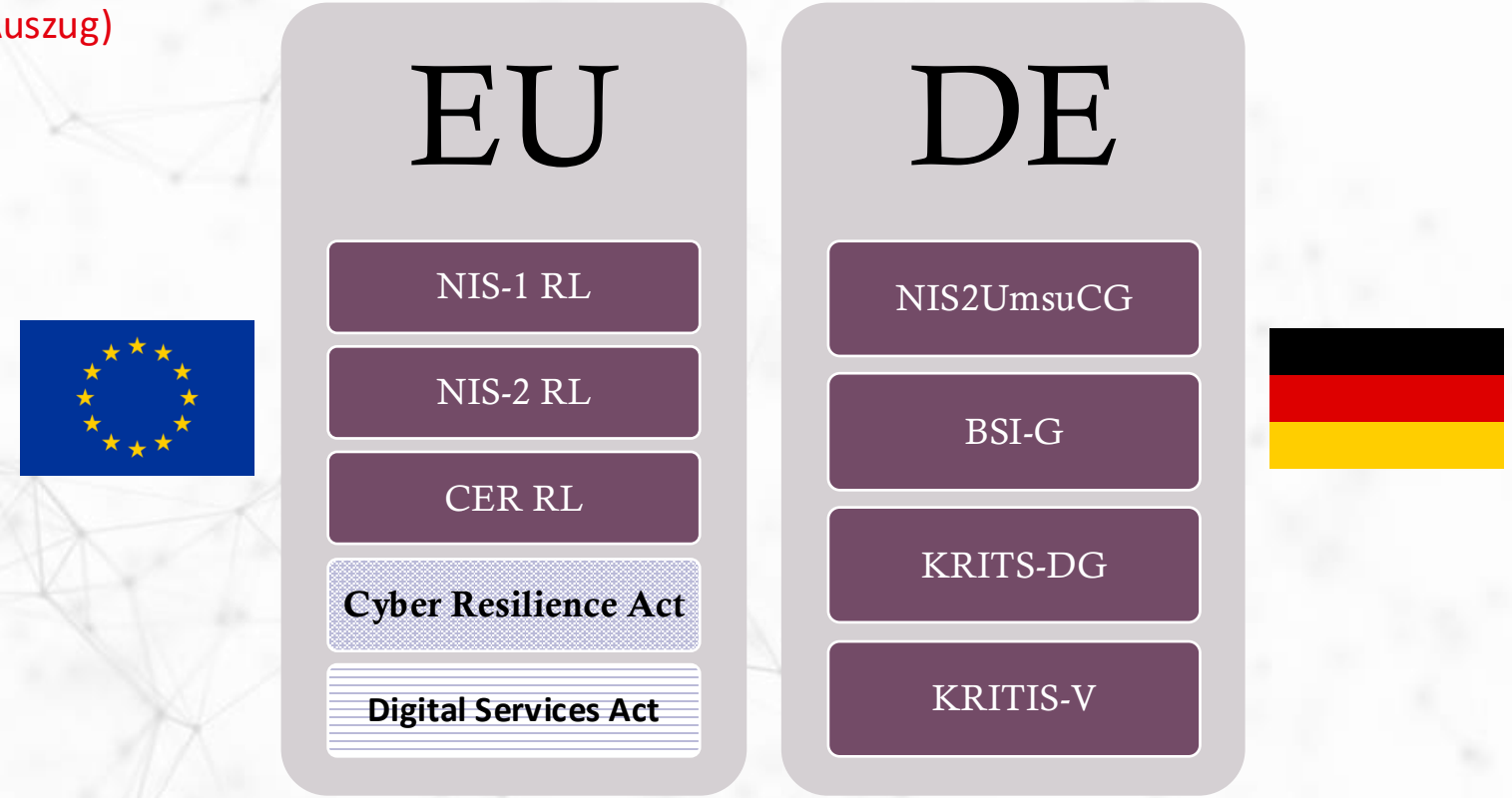
Verstärkter Schutz der Bürgerinnen und Bürger in der EU

- **Stärkung der Cybersicherheit** zur Sicherung des **Gemeinwohls**
- **Ganzheitliche** Konzepte zur **Gefahrenabwehr**
- **Maßnahmen** zur Stärkung der Cybersicherheit für Behörden und Unternehmen
- **Stärkung** des Bundesamtes für Sicherheit in der Informationstechnik (**BSI**)

„Verlässlichkeit und Sicherheit sind entscheidend für wirtschaftliche und gesellschaftliche Tätigkeiten und das Funktionieren des Binnenmarkts.“

RECHTLICHER KONTEXT

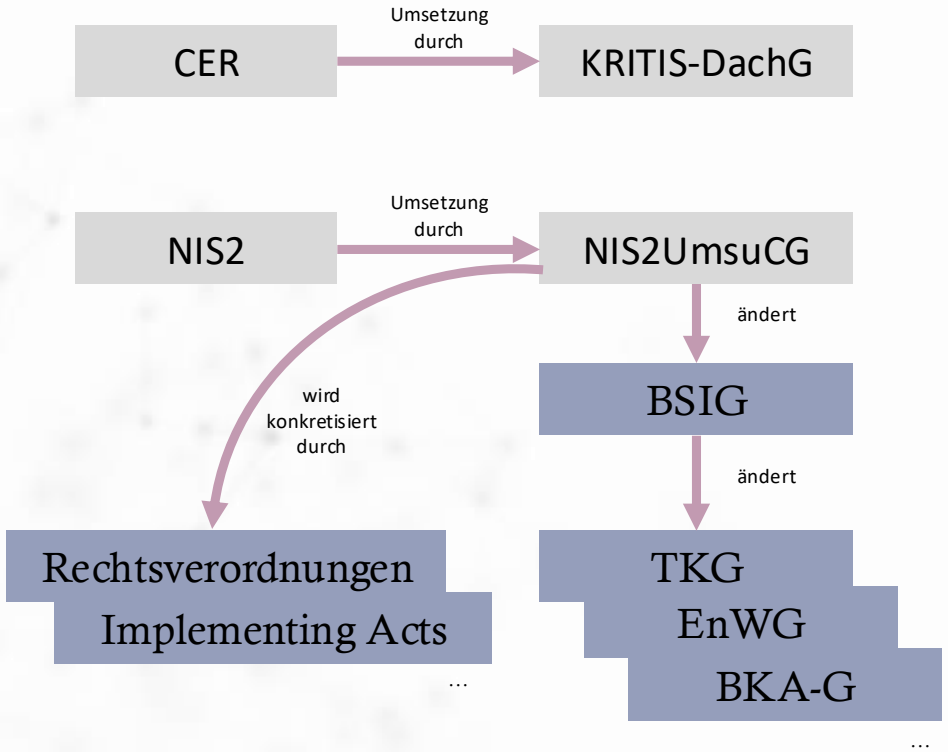
Überblick rechtlicher Anforderungen im Kontext der Informations- und IT-Sicherheit (Auszug)



RECHTLICHER KONTEXT

Kontext der rechtlichen Rahmenbedingungen

- NIS2 und CER bringen neue Anforderungen an den Schutz kritischer Infrastrukturen
- NIS2-Umsetzungsgesetz und KRITIS-Dachgesetz sind verabschiedet
- Branchenspezifisch: z.B. DORA für den Finanzsektor, TKG, EnWG usw.
- Implementing Acts fordern z.B. Cybersicherheitszertifizierungen



RECHTLICHER KONTEXT

Änderung der vorherigen deutschen KRITIS-Regulierung

- Das NIS-2-Umsetzungsgesetz ändert die vorherige deutsche KRITIS-Regulierung deutlich – neben den Betreibern kritischer (KRITIS) Anlagen werden nun auch die **besonders wichtigen** und **wichtige Einrichtungen** betrachtet.

Betroffene:	**Sektoren**:	**Cybersecurity**:
Betroffen sind Betreiber kritischer Anlagen (KRITIS) und Einrichtungen nach Unternehmensgröße sowie Bundeseinrichtungen und einige Sonderfälle.	Die KRITIS-Sektoren der kritischen Anlagen bleiben bestehen, die Einrichtungen umfassen wie in der EU in NIS-2 neben Infrastruktur nun große Teile der Wirtschaft.	Umfassende Sicherheitsmaßnahmen und großer Geltungsbereich im ganzen Unternehmen: Risikomanagement, Vorfallsmeldungen, technische Maßnahmen, Governance.

RECHTLICHER KONTEXT

Auszug EU-Vorgaben

Regelwerk	Betroffene in Deutschland	Zielsetzung	Gültigkeitsbeginn	Aufsicht	Deutsche Umsetzung durch
NIS2	Betreiber kritischer Anlagen, besonders wichtige und wichtige Einrichtungen, einzelne Bundesbehörden	**Cybersicherheits-standards**, Meldepflichten	Umsetzung bis Ende 2025/ Anfang 2026	Nationale Behörden	NIS2-Umsetzungs-gesetz, BSI-Gesetz (Neu)
CER	Betreiber kritischer Infrastrukturen	Schutz **physischer** Infrastruktur	Umsetzung bis Ende 2025/ Anfang 2026	Nationale Behörden	KRITIS-Dachgesetz
DORA	Finanzunternehmen, relevante IKT-Dienstleister	**Betriebsresilienz**, IKT-Risikomanagement	Anwendung ab 17.01.2025	EU/ nationale Aufsicht	Gilt unmittelbar, flankierende Auslegung durch BaFin etc.
CRA	Hersteller, Importeure, Händler digitaler Produkte (Hard- und Software) branchenübergreifend	Mindestanforderungen, **Security by Design**	Anwendungspflicht ab 11.12.2027, Meldepflicht ab 11.09.2026	Markt-aufsicht EU/ national	Gilt unmittelbar, Anpassung u. a. im ProdSG/CE-Prüfung

RECHTLICHER KONTEXT IN BRANDENBURG

NIS-2, BSI-G UND KRITIS-DG

Der Sektor **Forschung** zählt zu NIS-2 und muss die Anforderungen erfüllen:

Wer?

Forschungseinrichtungen mit dem primären Ziel, angewandte Forschung oder experimentelle Entwicklung im Hinblick auf die Nutzung der Ergebnisse dieser Forschung für **kommerzielle Zwecke** durchzuführen

Wer nicht?

Bildungseinrichtungen zählen nicht hierzu und sind aktuell **nicht** in den Gesetzen reguliert

NIS-2, BSI-G UND KRITIS-DG

- durch massive Zunahme der Angriffe auf Universitäten sollten sich die Bildungseinrichtungen an den Vorgaben nach §30 BSI-G als **Leitfaden** orientieren

- die Gesetze werden regelmäßig **evaluiert** und neue Sektoren aufgenommen (zuletzt der Sektor Raumfahrt)

- Es kann **nicht ausgeschlossen** werden, dass der Sektor Bildung zu einem späteren Zeitpunkt aufgenommen wird (aktuell nicht im Diskurs)

ANFORDERUNGEN BSI-G IM ÜBERBLICK

Maßnahmen auf Grundlage eines Risikomanagements

Bei der Bewertung der Verhältnismäßigkeit von Maßnahmen […] sind

- die **Risikoexposition**,
- die **Größe der Einrichtung**, die Umsetzungskosten und
- die **Eintrittswahrscheinlichkeit** und Schwere von **Sicherheitsvorfällen** sowie
- ihre gesellschaftlichen und wirtschaftlichen **Auswirkungen**

zu berücksichtigen.

ANFORDERUNGEN BSI-G IM ÜBERBLICK

Maßnahmen auf Grundlage eines Risikomanagements

Die Maßnahmen

- sollen den **Stand der Technik** einhalten,
- die einschlägigen europäischen und internationalen **Normen** berücksichtigen und
- müssen auf einem **gefahrenübergreifenden Ansatz** beruhen.

ANFORDERUNGEN BSI-G IM ÜBERBLICK

Maßnahmen nach §30

- **Risikoanalyse** und Sicherheit für Informationssysteme
- Bewältigung von **Sicherheitsvorfällen**
- **Aufrechterhaltung** und Wiederherstellung, Backup-Management, **Krisenmanagement**
- Sicherheit der **Lieferkette**, Sicherheit zwischen Einrichtungen, Dienstleister-Sicherheit
- Sicherheit in der Entwicklung, **Beschaffung** und Wartung
- Management von **Schwachstellen**
- Bewertung der **Effektivität** von Cybersicherheit und Risikomanagement
- Schulungen Cybersicherheit und **Cyberhygiene**
- **Kryptografie** und Verschlüsselung
- **Personalsicherheit**, Zugriffskontrolle und Anlagen-Management
- **Multi-Faktor-Authentisierung** und kontinuierliche Authentisierung
- **Sichere Kommunikation** (Sprach-, Video- und Text-)
- Sichere **Notfallkommunikation**

ANFORDERUNGEN BSI-G IM ÜBERBLICK

Meldewesen

Erheblicher Sicherheitsvorfall

Interne Meldestelle des Meldenden

< 24 Std.

- Verdacht rechtswidrige Handlungen
- Grenzüberschreitende Auswirkungen
- Art der betroffenen Anlage, kDL, Auswirkungen auf kDL
- Anzahl und Anteil betroffene Nutzer
- Bisherige und voraussichtliche Dauer
- Geografisches Gebiet
- Informationen Beurteilung Art, Ursache, Folgen
- Bestätigung/Aktualisierung Erstmeldung

72 Std.

- Erste Bewertung mit Schweregrad, Auswirkungen, Kompromittierungsindikatoren

Zwischen-meldungen

- Auf Ersuchen des BSI
- Relevante Statusaktualisierungen

1 Monat

- Ausführliche Beschreibung mit Schweregrad, Auswirkungen
- Art der Bedrohung / Ursache
- Abhilfemaßnahmen
- Ggf. grenzüberschreitende Auswirkungen
- „ausführlicher Bericht“

Meldestelle von BBK und BSI

RECHTLICHER KONTEXT IN BRANDENBURG

CYBERSICHERHEIT IN BRANDENBURG

- E-Government-Gesetz
- Verordnung zur Umsetzung der NIS-2-Richtlinie
- Cybersicherheitsstrategie

E-GOVERNMENT-GESETZ

§16 CERT

Unterstützung und Beratung der an das Landesverwaltungsnetz Brandenburg (LVNBB) angeschlossenen Behörden.

Das CERT sammelt und bewertet Daten zur Abwehr von Gefahren

Die an das LVNBB angeschlossenen Behörden melden dem CERT sicherheitsrelevante Vorfälle (MUSS-Anforderung)

Das CERT spricht Warnungen und Empfehlungen gegenüber den Behörden des Landes und der Kommunen aus

Das CERT informiert die für Informationssicherheit zuständigen Stellen des Bundes und der Länder über ihm bekannt gewordene sicherheitsrelevante Vorfälle

Organisatorische Angliederung beim Brandenburgischen IT-Dienstleister

VERORDNUNG ZUR UMSETZUNG DER NIS-2-RICHTLINIE

- Verweis auf CERT bzw. CSIRT
- Risikomanagement & Bericht- und Informationspflichten
- Verweis auf BSI-Gesetz (NIS-2)
- Umsetzungs-, Überwachungs- und Schulungspflichten

VERORDNUNG ZUR UMSETZUNG DER NIS-2-RICHTLINIE

- Verweis auf CERT bzw. CSIRT
- Risikomanagement & Bericht- und Informationspflichten
- Verweis auf BSI-Gesetz (NIS-2)
- Umsetzungs-, Überwachungs- und Schulungspflichten

...

CYBERSICHERHEITSSTRATEGIE

- Aufbau der zentralen Stelle für Cyber- und Informationssicherheit im Land Brandenburg
- Prüfung landesgesetzlicher Cyber- und Informationssicherheitsregelungen
- regelmäßige Überprüfung der Wirksamkeit der Cybersicherheitsarchitektur
- stärkere Einbindung der Kommunen
- Weiterentwicklung und Umsetzung von Risikomanagementmaßnahmen für die Verwaltung
- Etablierung eines landesweiten operativen Lagebildes „Cybersicherheit“
- Ausweitung der Meldepflichten
- Etablierung von Cybersicherheitsübungen für die Verwaltungen Brandenburgs
- Berücksichtigung von Cyber- und Informationssicherheit in allen Landesvorhaben der Digitalisierung
- Rahmenbedingungen für die Entwicklung von Schulungskonzepten und Ausbau bestehender Schulungsangebote

QUELLENANGABEN UND VERWEISE

[01] BSI Jahreslagebericht zur IT-Sicherheit in Deutschland

https://medien.bsi.bund.de/lagebericht/

[02] Statistik der Statista bezgl. Angriffsziele

https://de.statista.com/infografik/34055/anzahl-der-registrierten-politisch-motivierten-cyberangriffe-weltweit-nach-zielsektor/

[03]BSI Quartalsberichte 2026

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Cyber-Sicherheitslage/Lageberichte/Monatsbericht_LageCybernation/Monatsberichte_Lage_node.html

[04]bitkom Studie Wirtschaftsschutz 2024

https://www.bitkom.org/sites/main/files/2024-08/240828-bitkom-charts-wirtschaftsschutz-cybercrime.pdf

ENDE & DANKE

Zeit für Austausch



CYTAKTICS 5
David-Gilly-Straße 1
14469 Potsdam
Telefon: 0331 – 23 22 00 60
Mail: brozat@cytaktics5.de