F. NIS2/BSI-Gesetz/KRITIS-DachG

I. Rechtsentwicklung und Rechtsquellen

Vergleichbar mit den Entwicklungen des Datenschutzrechts findet auch im IT-Sicherheitsrecht eine **zunehmende Regulierung auf nationaler und EU-Ebene** statt. 260

1. Nationale Gesetzgebung: BSI-Gesetz und IT-Sicherheitsgesetz (2.0)

Bereits vor der weitverbreiteten Internetnutzung in Unternehmen unternahm der deutsche Gesetzgeber 1991 mit der **Errichtung des BSI** erste Schritte hin zur Schaffung gesetzlicher IT-Sicherheitsvorgaben.[1] Nachfolgend wurden über die Verabschiedung und Änderung des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) ab 2009 dem BSI Befugnisse eingeräumt, um als **zentrale Meldestelle für IT-Sicherheit** Informationen zu Sicherheitslücken und neuen Angriffsmustern zu sammeln, auszuwerten und daraufhin entsprechende Informationen und Warnungen an die betroffenen Unternehmen und die Öffentlichkeit auszugeben.[2] Auf diese Weise schuf der deutsche Gesetzgeber bereits frühzeitig eine zentrale Stelle zur Gewährleistung der IT-Sicherheit im Bundesgebiet. 261

Im Jahr 2015 wurde der Gesetzgeber im Bereich der IT-Sicherheit mit der Verabschiedung des Artikelgesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG)[3] tätig. Das IT-SiG führte insbesondere zu Änderungen am BSIG und erfasste **Unternehmen** in Geschäftsfeldern, für deren Funktionsfähigkeit eine sichere IT-Infrastruktur unerlässlich ist, **hauptsächlich im Bereich der Versorgungsdienstleistungen** (sog. Betreiber „Kritischer Infrastrukturen", **KRITIS**). Diese wurden über das IT-SiG **zu einem Mindeststandard an IT-Sicherheit verpflichtet**. 262

Das am 18.5.2021 beschlossene **Zweite Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-SiG 2.0)**[4] führt als Artikelgesetz zu einigen weiteren Änderungen im BSiG und in anderen bereichsspezifischen Gesetzen mit Bezug zur IT-Sicherheit, wie dem EnWG. Wesentliche Änderungen durch das IT-Sicherheitsgesetz 2.0 waren[5]: 263

- Erweiterungen von Prüf- und Kontrollbefugnissen des BSI zum Schutz der IT der Bundesverwaltung u.a. durch Festlegung von Mindeststandards;

1 Gesetzlich normiert im Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik vom 17.12.1990, BGBl. I 1990, S. 2834, gültig vom 1.1.1991 bis 19.8.2009.

2 Begr. RegE, BT-Drs. 16/11967, S. 1.

3 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 17.7.2015, BGBl. I 2015, S. 1324.

4 Zweites Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme vom 18.5.2021, BGBl. I 2021, S. 1122 und 4304.

5 Begr. RegE, BT-Drs. 19/26106, S. 2, 102.

- Schaffung von Befugnissen zur Detektion von Schadprogrammen zum Schutz der Regierungsnetze;
- Befugnis zur Abfrage von Bestandsdaten bei Anbietern von Telekommunikationsdiensten, um Betroffene über Sicherheitslücken und Angriffe zu informieren;
- Einführung einer Rechtsgrundlage für das BSI, Sicherheitslücken an den Schnittstellen informationstechnischer Systeme zu öffentlichen TK-Netzen festzustellen sowie zum Einsatz von Systemen und Verfahren zur Analyse von Schadprogrammen und Angriffsmethoden;
- Schaffung einer Anordnungsbefugnis des BSI gegenüber Telekommunikations- und Telemedienanbietern zur Abwehr spezifischer Gefahren für die Informationssicherheit;
- Ausweitung der Pflichten für Betreiber Kritischer Infrastrukturen und weiterer Unternehmen im besonderen öffentlichen Interesse;
- Schaffung von Eingriffsbefugnissen für den Einsatz und Betrieb kritischer IT-Komponenten;
- Schaffung der Voraussetzungen für ein einheitliches IT-Sicherheitskennzeichen.

2. Europäische Gesetzgebung: NIS-, NIS2- und CER-Richtlinie

264 Auch die EU erkannte die erheblichen Auswirkungen von IT-Sicherheitsvorfällen auf den europäischen Binnenmarkt. Bereits 2013 wurde deshalb der erste Entwurf für die Richtlinie über Maßnahmen zur Gewährleistung einer hohen gemeinsamen Netz- und Informationssicherheit in der Union (kurz: **NIS-Richtlinie**) vorgelegt.[1] Eine Einigung ließ sich erst zwei Jahre später erzielen, so dass die NIS-Richtlinie[2] im August 2016 – also ein Jahr nach dem deutschen IT-SiG – in Kraft trat. Die NIS-Richtlinie verpflichtete Unternehmen aus dem **KRITIS-Bereich** sowie bestimmte **Anbieter digitaler Dienste** zur Einhaltung von Mindest-IT-Sicherheitsstandards, um Sicherheitsvorfällen entgegenzuwirken. Die Vorgaben zum Schutzniveau, den erfassten Unternehmen und der Durchsetzung waren in der NIS-Richtlinie allerdings nur sehr rudimentär, weshalb keine umfassende Harmonisierung gelungen ist. Aus diesem Grund hat die Europäische Kommission 2021 eine überarbeitete Richtlinie vorgeschlagen, die Anfang 2023 als NIS2-Richtlinie in Kraft getreten ist.[3] Die Umsetzungsfrist bis zum 17.10.2024 hielt die Mehrheit der EU-Mitgliedstaaten nicht

1 *Voigt/Gehrmann*, ZD 2016, 355, 355.
2 Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union, ABl. EU L 194/1.
3 Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14.12.2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union […] (NIS2-Richtlinie), ABl. EU L 333/80.

ein.[1] Das Gesetzgebungsverfahren für die deutsche Umsetzung im NIS2UmsuCG[2] zog sich über mehrere Jahre, ehe das Gesetz in seiner finalen Fassung am 6.12.2025 in Kraft trat.

Die **NIS2-Richtlinie** enthält deutlich klarere Regelungen etwa zum Anwendungsbereich, zu den notwendigen technischen und organisatorischen Maßnahmen, Meldepflichten und Bußgeldern. Den nationalen Gesetzgebern bleibt daher nur noch wenig Spielraum für die Umsetzung. Infolgedessen sind auch die Vorgaben des erneuerten BSIG sehr nah an der NIS2-Richtlinie orientiert. 265

Gemeinsam mit der NIS2-Richtlinie hat die EU auch die **CER-Richtlinie**[3] verabschiedet, die komplementäre Regelungen **zur physischen Resilienz kritischer Anlagen** beinhaltet. Beide Richtlinien sollen möglichst kohärent sein, was sich auch darin zeigt, dass viele Regelungen bezüglich der Cybersicherheit und physischen Resilienz von kritischen Anlagen parallel ausgestaltet sind und dass bspw. das Meldewesen über eine gemeinsame Meldestelle erfolgen soll. Auch die CER-Richtlinie sollte bis zum 17.10.2024 in nationales Recht umgesetzt werden und auch diese Frist haben die meisten EU-Mitgliedstaaten versäumt. Der Verzug des deutschen Gesetzgebers ist dabei bei der CER-Richtlinie noch etwas größer als bei der NIS2-Richtlinie. Denn während das NIS2UmsuCG Ende 2025 verkündet worden ist, wurde der Regierungsentwurf zum **KRITIS-Dachgesetz** (KRITIS-DachG) bis Ende 2025 lediglich in 1. Lesung im Bundestag behandelt und dürfte mit etwas zeitlichem Abstand in der ersten Hälfte des Jahres 2026 verabschiedet werden. 266

Auch die künftige Entwicklung des Cybersicherheitsrechts auf Ebene der EU kündigt sich bereits an, denn die Europäische Kommission hat im Januar 2026 ein neues Cybersicherheitspaket veröffentlicht. Der Entwurf besteht einerseits aus dem Entwurf für einen umfassend reformierten „**Cybersecurity Act 2**“[4] (s. dazu Rz. 667) und andererseits aus einem (im Vergleich zum CSA2-E deutlich weniger umfassenden) Entwurf zur „gezielten Anpassung der NIS2-Richtlinie“[5]. Dieser Entwurf zur Anpassung

1 Europäische Kommission, Kommission leitet Schritte zur Gewährleistung der vollständigen und fristgerechten Umsetzung von EU-Richtlinien ein, 28.11.2024, abrufbar unter https://ec.europa.eu/commission/presscorner/api/files/document/print/de/inf_24_5988/INF_24_5988_DE.pdf, zuletzt aufgerufen am 4.12.2025.

2 Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung vom 2.12.2025, BGBl. 2025 I Nr. 301.

3 Richtlinie (EU) 2022/2557 des Europäischen Parlaments und des Rates vom 14.12.2022 über die Resilienz kritischer Einrichtungen […], ABl. EU L 333/164. Die verbreitete Bezeichnung als CER-Richtlinie orientiert sich an der englischen Bezeichnung der Richtlinie als „Critical Entities Resilience Directive“.

4 COM(2026) 11 final, Proposal for a Regulation of the European Parliament and of the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security […] (The Cybersecurity Act 2), abrufbar unter https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-eu-cybersecurity-act, zuletzt aufgerufen am 21.1.2026.

5 COM(2026) 13 final, Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and alignment

der NIS2-Richtlinie ergänzt vor allem Bezüge zu den Zertifizierungsschemata nach dem CSA2-E, um betroffenen Einrichtungen künftig den Nachweis der Einhaltung von NIS2-Vorgaben zu erleichtern.

II. Regelungssystematik des BSI-Gesetzes

267 Zusätzlich zu den allgemeinen IT-Sicherheitspflichten eines jeden Unternehmens (s. Rz. 34 ff.) schafft das durch das NIS2UmsuCG angepasste BSIG **verstärkte IT-Sicherheitspflichten für eine hohe Zahl an Unternehmen ganz verschiedener Branchen**. Für betroffene Unternehmen wird nicht bloß eine umfassende Erhöhung des IT-Sicherheitsniveaus erforderlich, sondern es treffen sie überdies u.a. Meldepflichten gegenüber dem BSI, die dabei helfen sollen, bspw. flächendeckende Cyber-Angriffe früh erkennen und möglichst abwenden zu können.[1] Das Ziel der Regelungen ist es, Unternehmen in gesellschaftskritischen Sektoren zu einer präventiven Sicherung ihrer IT-Systeme zu verpflichten und somit die Verfügbarkeit, Integrität und Vertraulichkeit dieser Systeme zu sichern.[2]

268 Neben dem bzw. statt des BSIG können **im Einzelfall IT-Sicherheitsvorschriften aus Spezialgesetzen zur Anwendung gelangen** (s. hierzu Teil G, Rz. 440 ff.). Grundsätzlich **tritt** das **BSIG** als *lex generalis* **gegenüber Spezialgesetzen für bestimmte Branchen zurück**.[3] Entsprechende Spezialgesetze sind etwa TKG (s. Rz. 462 ff.), EnWG (s. Rz. 506 ff.), AtG (s. Rz. 521 ff.), und DORA (s. Rz. 556 ff.). Das Zusammenspiel dieser Vorschriften bereitet in der Praxis allerdings teilweise Schwierigkeiten.[4] Aus diesem Grund hat die Europäische Kommission Leitlinien veröffentlicht, die das Verhältnis der NIS2-Richtlinie zu sektorspezifischen Vorgaben klären sollen, wobei nur DORA aus europäischer Sicht als ein Spezialgesetz im Verhältnis zur NIS2-Richtlinie angesehen wird. Deutsche Gesetze können dann *lex specialis* gegenüber dem BSIG sein, wenn sie selbst die Vorgaben der NIS2-Richtlinie umsetzen. Daraus ergibt sich folgende vereinfachte Anwendungsreihenfolge:

(1) Sektorielle Rechtsakte der EU, die der NIS2-Richtlinie vorgehen (DORA);

(2) nationale Spezialgesetze, soweit sie die Vorgaben der NIS2-Richtlinie umsetzen (z.B. EnWG und TKG);

(3) BSIG;

(4) sonstige IT-Sicherheitsvorgaben.

---

with the [Proposal for the Cybersecurity Act 2], abrufbar unter https://digital-strategy.ec.europa.eu/en/library/proposal-directive-regards-simplification-measures-and-alignment-cybersecurity-act, zuletzt aufgerufen am 21.1.2026.

1 Begr. RegE, BT-Drs. 18/4096, S. 1; Begr. RegE, BT-Drs. 19/26106, S. 31, 82, 102.

2 *Schmidt*, RDi 2024, 550, 553.

3 Vgl. etwa Begr. RegE, BT-Drs. 18/11242, S. 1; Art. 4 NIS2-Richtlinie.

4 Vgl. *von dem Bussche/Schelinski* in Leupold/Wiebe/Glossner, IT-Recht, Teil 7.1 Rz. 16, 49, 51 ff.

Die IT-Sicherheitsvorgaben des BSIG einschließlich ihres jeweiligen Anwendungsbereichs und der jeweiligen Verletzungsfolgen werden nachfolgend dargestellt. Durch die Vorgaben des BSIG können **mittelbar auch Hersteller und Zulieferer von IT-Produkten und -Systemen** erhöhten IT-Sicherheitspflichten unterliegen (s. Rz. 394 ff.). 269

III. IT-Sicherheitspflichten nach dem BSI-Gesetz

Das BSIG adressiert mit seinen allgemeinen Pflichten **wichtige und besonders wichtige Einrichtungen**. Die im BSIG a.F. maßgeblichen **Betreiber kritischer Anlagen** sind ausdrücklich in die Gruppe der besonders wichtigen Einrichtungen einbezogen worden, die früher separat geregelten **Unternehmen im besonderen öffentlichen Interesse** implizit in den beiden neuen Gruppe der wichtigen und besonders wichtigen Einrichtungen aufgegangen.[1] 270

Die materiell-rechtlichen **Anforderungen** sind für wichtige und besonders wichtige Einrichtungen **weitgehend identisch**. Unterschiede gibt es bei den Untersuchungsbefugnissen des BSI (s. Rz. 381 ff.) sowie der Höhe der angedrohten Bußgelder (s. Rz. 413 ff.). **Erhöhte Anforderungen** an den IT-Sicherheitsstandard und die Nachweispflichten knüpfen nicht an die Unterscheidung von wichtigen und besonders wichtigen Einrichtungen an, sondern richten sich speziell **an KRITIS-Betreiber** (s. Rz. 358 ff.) **und Anbieter bestimmter digitaler Dienste** (s. Rz. 366 ff.). 271

1. Adressaten

Der **Adressatenkreis** wurde im Zuge der Umsetzung der NIS2-Richtlinie **deutlich erweitert** und umfasst nun neben den Betreibern kritischer Anlagen auch die sog. **wichtigen und besonders wichtigen Einrichtungen**. Voraussetzung ist, dass sich die kritische Anlage in Deutschland befindet oder die Einrichtung in Deutschland niedergelassen ist, § 59 Nr. 1 und 2 BSIG. Das BSI geht davon aus, dass fast 30.000 Einrichtungen vom BSIG n.F. adressiert werden, während vom BSIG a.F. nur rund 2.000 kritische Anlagen betroffen waren.[2] Die zuvor im BSIG adressierten „Unternehmen im besonderen öffentlichen Interesse" werden seit der NIS2-Umsetzung im BSIG nicht mehr erwähnt.[3] Stattdessen werden Unternehmen nun in die Kategorien der wichtigen und besonders wichtigen Einrichtungen aufgeteilt. Maßgeblich für die Einstufung sind die Vorgaben in § 28 BSIG. Das BSIG legt seinen **räumlichen Anwendungsbereich** nicht ausdrücklich fest, dürfte sich aber schon aus Gründen der Regelungskompetenz nur an solche Einrichtungen richten, die die nach § 28 BSIG maßgeblichen Handlungen – Betrieb einer kritischen Anlage (s. Rz. 276 ff.) oder Anbieten von Waren oder Dienstleistungen (s. Rz. 290 ff.) – in Deutschland vornehmen.[4] 272

1 Vgl. Begr. RegE, BT-Drs. 21/1501, S. 136.
2 *Schmidt*, RDi 2024, 550, 550 f.
3 *Kipker/Dittrich*, MMR 2023, 481, 481.
4 Vgl. *Nink*, Das neue IT-Sicherheitsrecht, § 2 Rz. 4 sowie § 5 Rz. 10 ff.

Für digitale Dienste ergibt sich die Anwendbarkeit des BSIG aus der Zuständigkeit des BSI, s. Rz. 367 f.

273 Für den Anwendungsbereich nennt das BSIG immer wieder „**natürliche und juristische Personen**". Der Begriff der natürlichen Person entspricht hier dem allgemeinen Verständnis des Zivilrechts und bezeichnet Menschen. Der Begriff der juristischen Person stimmt hingegen nicht mit dem deutschen Zivilrecht überein, sondern ist unionsrechtskonform auszulegen. Aus Art. 54 Abs. 2 AEUV ergibt sich, dass auch Gesellschaften des bürgerlichen Rechts und des Handelsrechts als juristische Personen im Sinne des Unionsrechts gelten, so dass auch Personengesellschaften vom Begriff der juristischen Person im BSIG erfasst sind.[1]

274 Folgende Unternehmen gelten gem. § 28 Abs. 1 BSIG als **besonders wichtige Einrichtung**:

- **KRITIS-Betreiber** (s. Rz. 276 ff.),
- Anbieter bestimmter **digitaler Dienste** (s. Rz. 286 ff.),
- **Telekommunikationsunternehmen**, die keine Kleinst- oder Kleinunternehmen sind (s. Rz. 290), und
- Betreiber bestimmter **Einrichtungsarten nach Anlage 1 BSIG**, wenn sie größer als mittelgroße Unternehmen sind (s. Rz. 301).

Die Kategorie der besonders wichtigen Einrichtungen im BSIG entspricht den **wesentlichen Einrichtungen in der NIS2-Richtlinie**. Dass diese Begrifflichkeit aus der NIS2-Richtlinie abgeändert wurde, kann insbesondere in internationalen Unternehmen, die in verschiedenen EU-Mitgliedstaaten tätig sind, zu Missverständnissen führen.[2] Mit der abweichenden Bezeichnung wollte der Umsetzungsgesetzgeber mutmaßlich Verwechslungen zwischen wesentlichen und wichtigen Einrichtungen vermeiden.[3]

275 Als **wichtige Einrichtungen** gelten gem. § 28 Abs. 2 BSIG:

- **Vertrauensdiensteanbieter** (ohne Qualifizierung nach eIDAS-VO, s. Rz. 286),
- **Telekommunikationsunternehmen**, die Kleinst- oder Kleinunternehmen sind (s. Rz. 290),
- Betreiber bestimmter **Einrichtungsarten nach Anlage 1 BSIG**, wenn sie mittelgroße Unternehmen sind (s. Rz. 302 f.), sowie
- Betreiber bestimmter **Einrichtungsarten nach Anlage 2 BSIG**, wenn sie mindestens mittelgroße Unternehmen sind (s. Rz. 302 f.).

1 Vgl. *Müller-Graff* in Streinz, EUV/AEUV, Art. 54 AEUV Rz. 4.
2 *Nink*, EuDIR 2025, 185, 188; *Schmidt*, RDI 2024, 550, 552.
3 *Kipker/Dittrich*, MMR 2023, 481, 481; *Schmidt*, RDI 2024, 550, 552.

a) KRITIS-Betreiber

Alle Betreiber kritischer Anlagen (KRITIS-Betreiber) sind als **besonders wichtige Einrichtungen** Adressaten des BSIG (§ 28 Abs. 1 Satz 1 Nr. 1 BSIG). Sie haben einige zusätzliche Pflichten unter dem BSIG (s. Rz. 358 ff.) und müssen zudem ihre physische Resilienz nach den Vorgaben des KRITIS-DachG sicherstellen (s. zum derzeitigen Entwurf Rz. 302 ff.). Vereinzelt werden die KRITIS-Betreiber wegen dieser Sonderregeln als eigene Kategorie neben wichtigen und besonders wichtigen Einrichtungen geführt.[1] Dies kann darauf zurückgeführt werden, dass die Kategorie der KRITIS-Betreiber bereits im BSIG a.F. mit Sicherheitspflichten adressiert wurde. Im Vergleich zur früheren Fassung wurde der Kreis der kritischen Anlagen erweitert. 276

Sobald ein Unternehmen auch nur eine kritische Anlage betreibt, müssen **alle IT-Systeme** des Unternehmens dem Sicherheitsstandard des BSIG entsprechen, also nicht nur solche, die für die Erbringung der kritischen Dienstleistung genutzt werden.[2] Für die IT-Systeme, -Komponenten und -Prozesse, die für die Funktionsfähigkeit der kritischen Anlage maßgeblich sind, greifen darüber hinaus zusätzliche IT-Sicherheitspflichten (s. Rz. 360 f.). 277

Die Vorschriften des BSIG zur Einstufung als KRITIS-Betreiber werden durch eine Rechtsverordnung des Bundesinnenministeriums nach § 56 Abs. 4 BSIG ergänzt, die sog. **BSI-Kritisverordnung** (BSI-KritisV). Die derzeit noch geltende BSI-KritisV wurde bereits unter der früheren Rechtslage verabschiedet und soll im Grundsatz beibehalten werden.[3] Das NIS2UmsuCG sieht zwar schon **Anpassungen der BSI-KritisV** bei den Definitionen, die teilweise in das BSIG verschoben wurden, sowie in den Sektoren Energie, Finanzwesen und Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende vor, aber der neue KRITIS-Sektor Weltraum ist dort noch nicht erfasst. Es ist daher zu erwarten, dass das Bundesinnenministerium gemeinsam mit den zuständigen anderen Bundesministerien die BSI-KritisV zeitnah entsprechend anpasst. Die Neufassung der BSI-KritisV soll zugleich auch der Einstufung kritischer Anlagen nach dem KRITIS-DachG dienen, weshalb künftig auch dessen Vorgaben zu beachten sind (s. dazu auch Rz. 415 ff.). 278

aa) Kritische Anlage

Als **Anlage** gelten gem. § 1 Abs. 1 Nr. 1 BSI-KritisV 279

- Betriebsstätten und sonstige **ortsfeste Einrichtungen**,
- Maschinen, Geräte und **sonstige ortsveränderliche Einrichtungen oder**
- **Software und IT-Dienste**,

die für die Erbringung einer kritischen Dienstleistung (s. Rz. 280) notwendig sind. Nach § 1 Abs. 1 BSI-KritisV sind **Anlagenteile und Verfahrensschritte**, die zum Betrieb notwendig sind, **sowie Nebeneinrichtungen**, die mit Anlagenteilen und Verfah-

1 Vgl. *Schmidt*, RDi 2024, 550, 551.
2 Begr. RegE, BT-Drs. 21/1501, S. 147.
3 Begr. RegE, BT-Drs. 21/1501, S. 168.