# Die Weiterentwicklung des IT-Sicherheitsgesetzes

## Kommentar zum IT-Sicherheitsgesetz 2.0

Herausgegeben von

Steve Ritter,
Königswinter

Bearbeitet von dem Herausgeber und

Prof. Dr. Anne Paschke,
Technische Universität Braunschweig

Dr. Laura Schulte,
Rechtsanwältin, Bielefeld

Dr. Lutz Keppeler,
Rechtsanwalt, Köln

Fachmedien Recht und Wirtschaft I dfv Mediengruppe I Frankfurt am Main

**Bibliografische Information der Deutschen Nationalbibliothek**

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.de abrufbar.

ISBN 978-3-8005-1777-0

dfv Mediengruppe




www.ruw.de



Druck: WIRmachenDRUCK GmbH, Backnang

Printed in Germany

# Teil 1
# Die bisherige Entwicklung

Das IT-SiG 2.0 steht in einer inzwischen längeren Tradition. Wie sich schon aus der oft verwendeten Versionierung „2.0" erkennen lässt, gab es bereits zuvor ein IT-Sicherheitsgesetz. Doch dies ist nicht der einzige Vorgänger des IT-SiG 2.0, auch das NIS-RL-Umsetzungsgesetz von 2017 gehört dazu. Nachfolgend sollen die durch diese beiden Änderungsgesetze eingeführten Regelungen nachgezeichnet werden, um ein besseres Hintergrundverständnis der Gesetzeslage zu vermitteln, auf der das IT-SiG 2.0 mit seinen Änderungen aufsetzt. **1**

## A. Das IT-Sicherheitsgesetz 1.0

Eigentlich war das „Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes" von 2009[1] bereits das erste IT-Sicherheitsgesetz und hatte – zumindest in der Anfangsphase der Erstellung – auch den Arbeitstitel IT-Sicherheitsgesetz. Offiziell trug diesen Titel dann jedoch erst das „Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz)" von 2015.[2] Dieses erste offizielle IT-Sicherheitsgesetz (IT-SiG 1.0) geht bis auf das Jahr 2012 zurück. Der damalige Bundesinnenminister *Friedrich* verfolgte das Ziel, den Schutz Kritischer Infrastrukturen und der übrigen Nutzer im Bereich der IT-Sicherheit zu erhöhen.[3] Da sich nicht alle Unternehmen freiwillig um die Erhöhung der IT-Sicherheit kümmerten, wurde das Ziel – wie zuvor bereits öffentlich angekündigt[4] – mit gesetzgeberischen Maßnahmen weiterverfolgt.[5] Der vorgelegte Referentenentwurf vom 5.3.2013[6] konnte zwar noch öffentlich diskutiert, aber aufgrund des **2**

1 Gesetz zur Stärkung der Sicherheit in der Informationstechnik des Bundes vom 14.8.2009, BGBl. 2009 I S. 2821.

2 Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme (IT-Sicherheitsgesetz) vom 17.7.2015, BGBl. 2015 I S. 1324.

3 Vgl. https://www.wiwo.de/technologie/digitale-welt/innenminister-hans-peter-friedrich-angriffe-auf-alle-netze/6563892.html (Stand: 27.7.2021).

4 Vgl. https://www.wiwo.de/technologie/digitale-welt/innenminister-hans-peter-friedrich-angriffe-auf-alle-netze/6563892.html (Stand: 27.07.2021).

5 Pressemeldung des BMI vom 12.3.2013, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2013/03/eco_mmr_itsicherheitsgesetz.html (Stand: 27.7.2021).

6 Referentenentwurf eines Gesetzes zur Erhöhung der Sicherheit informationstechnischer Systeme, https://www.bmi.bund.de/SharedDocs/downloads/DE/gesetzestexte/gesetzesentwuerfe/Entwurf_it-sicherheitsgesetz.pdf (Stand: 27.7.2021).

nahenden Endes der Legislaturperiode nicht mehr von der Bundesregierung in den Bundestag eingebracht werden.[7]

**3** 2014 wurden die Arbeiten am IT-SiG 1.0 jedoch vom neuen Innenminister Seehofer wieder aufgenommen. Es wurden ein erster Referentenentwurf vom 18.8.2014[8] sowie ein zweiter Referentenentwurf vom 6.11.2014[9] öffentlich, die auf dem Entwurf aus dem Jahr 2013 beruhten. Bereits am 17.12.2014 verabschiedete die Bundesregierung den RegE des IT-SiG 1.0[10] und brachte diesen in den Bundestag ein. Dort erfuhr das Gesetz noch einige Änderungen durch den Innenausschuss,[11] bevor es am 17.7.2015 verabschiedet wurde.[12] Am 25.7.2015 trat das IT-SiG 1.0 in Kraft.

**4** Anders als der Name zunächst vermuten ließe, regelte das IT-SiG 1.0 nicht das gesamte Recht der IT-Sicherheit, sondern änderte als Artikelgesetz nur eine Reihe bereits bestehender Gesetze.[13] Dazu gehörten das BSI-Gesetz (BSIG), das Atomgesetz (AtG), das Energiewirtschaftsgesetz (EnWG), das Telemediengesetz, das Telekommunikationsgesetz (TKG), das Bundeskriminalamtgesetz (BKAG), das Bundesbesoldungsgesetz (BBesG) sowie das Gesetz zur Strukturreform des Gebührenrechts des Bundes. Die Änderungen lassen sich grob in drei Kategorien einordnen: 1. Erhöhung der IT-Sicherheit Kritischer Infrastrukturen, 2. Stärkung der IT-Sicherheit in der Bundesverwaltung und 3. Erhöhung der IT-Sicherheit für die Allgemeinheit. Anhand dieser drei Kategorien sollen die wesentlichen Regelungen des IT-SiG 1.0 nachfolgend beleuchtet werden.

## I. Stärkung der IT-Sicherheit Kritischer Infrastrukturen

**5** Die für die Versorgung der Bevölkerung notwendigen Infrastrukturen können sich der Digitalisierung nicht entziehen. Insbesondere durch die damit einhergehende Vernetzung der Anlagen werden sie jedoch auch gegenüber Cyberangriffen anfällig. Welchen Einfluss Cyberangriffe auf den Betrieb von industriellen Anlagen haben können, hatte die Schadsoftware *Stuxnet* bereits 2010 gezeigt. Mit dieser Schadsoftware wurden die Zentrifugen

7 Vgl. *Roos*, K&R 2013, 769.

8 Der Entwurf ist auf den Webseiten des BMI nicht mehr zu finden, aber unter https://www.rainer-gerling.de/PDF/Entwurf_IT-Sicherheitsgesetz_2014_08_18.pdf noch abrufbar (Stand: 27.7.2021).

9 Vgl. https://netzpolitik.org/wp-upload/141104-Anlage-Referentenentwurf-IT-Sicherheitsgesetz-final.pdf (Stand: 27.7.2021).

10 Pressemeldung des BMI vom 17.12.2014, https://www.bmi.bund.de/SharedDocs/kurzmeldungen/DE/2014/12/bundeskabinett-beschlie%C3%9Ft-it-sicherheitsgesetz.html (Stand: 27.7.2021).

11 BT-Drs. 18/5121.

12 BT-PlPr 18/110, 10582B.

13 Vgl. Gabel/Heinrich/Kiefner/*Wimmer/Mechler*, Kap. 5 Rn. 4.

der Urananreicherungsanlagen im iranischen Natanz sabotiert, so dass sie ihre Funktion nicht mehr erfüllen konnten. Der Angriff erfolgte durch die Ausnutzung von Sicherheitslücken in einer Software für industrielle Steuersysteme, die auch im Bereich Kritischer Infrastrukturen genutzt wird. Der breiten Öffentlichkeit wurde das daraus folgende Potenzial für Angriffe auf Kritische Infrastrukturen durch den Roman „Black Out" bekannt, der die Möglichkeiten für IT-Angriffe auf Infrastrukturen der Elektrizitätsversorgung anschaulich beschrieb. Vor diesem Hintergrund war eines der Hauptziele des IT-SiG 1.0, die IT der Kritischen Infrastrukturen vor den Gefahren durch Cyberangriffe besser zu schützen, um die Versorgung der Bevölkerung sicherstellen zu können.[14]

### 1. Was sind Kritische Infrastrukturen?

Um dieses Ziel zu erreichen, wurde erstmals eine gesetzliche Definition für „Kritische Infrastrukturen" in § 2 Abs. 10 BSIG eingeführt. Diese orientiert sich an einer bereits länger bestehenden Definition, auf die sich die Bundesministerien bereits 2003 geeinigt hatten.[15] Die gesetzliche Definition stellt dabei auf einen dreigliedrigen Begriff Kritischer Infrastrukturen ab.[16] **6**

In einem ersten Teil des Begriffs wird festgelegt, dass es sich bei KRITIS um „*Einrichtungen, Anlagen oder Teile davon*" (im Nachfolgenden der Einfachheit halber als Anlagen bezeichnet) handeln muss. KRITIS sind also nicht die Unternehmen als Rechtspersönlichkeiten, die eine Versorgungsleistung erbringen, sondern die tatsächlichen Betriebsanlagen, mit denen die Versorgungsleistungen erbracht werden. **7**

Nach dem zweiten Begriffsteil müssen die Anlagen den *„Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswirtschaft"* angehören. **8**

Als drittes Merkmal wird benannt, dass die Anlagen aus diesen Sektoren auch *„von hoher Bedeutung für das Funktionieren des Gemeinwesens sind, weil durch ihren Ausfall oder ihre Beeinträchtigung erhebliche Versorgungs-* **9**

---

14 BT-Drs. 18/4096, 2.

15 Diese lautete: „Kritische Infrastrukturen (KRITIS) sind Organisationen oder Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden", vgl. https://www.bbk.bund.de/DE/AufgabenundAusstattung/KritischeInfrastrukturen/kritischeinfrastrukturen_node.html (Stand: 27.7.2021).

16 *Voigt*, Rn. 353, stellt auf Ebene des Gesetzes nur auf zwei Voraussetzungen ab, indem er den Teil zu den Anlagen weglässt. Auf Ebene der Rechtsverordnung greift er jedoch auch den Anlagen-Aspekt auf, vgl. *Voigt*, Rn. 355.

*engpässe oder Gefährdungen für die öffentliche Sicherheit eintreten würden."* Die nähere Bestimmung, wann das jeweils der Fall ist, wurde durch § 2 Abs. 10 S. 2 BSIG auf die BSI-KritisV verlagert, die das Bundesministerium des Innern (BMI) nach § 10 Abs. 1 BSIG erlässt. Die erste Fassung der BSI-KritisV vom 22.4.2016[17] legte die Regelungen für die Sektoren Energie, Wasser, Ernährung sowie Informationstechnik und Telekommunikation fest.[18] Mit der Änderungsverordnung vom 21.6.2017[19] wurden die Regelungen für die Sektoren Gesundheit, Finanz- und Versicherungswesen sowie Transport und Verkehr ergänzt. In der BSI-KritisV werden für jeden Sektor bestimmte kritische Dienstleistungen festgelegt und diesen Anlagen(-typen) und konkrete anlagenbezogene Schwellenwerte zugeordnet (z. B. 420 MW installierte Netto-Nennleistung bei Energieerzeugungsanlagen im Sektor Energie gem. Anhang 1 BSI-KritisV – Stand 2016). Überschreitet eine aufgeführte Anlage diesen Schwellenwert, ist sie KRITIS. Bei der Bestimmung der Schwellenwerte wurde darauf abgestellt, welche „Mengen" jeweils notwendig sind, um ca. 500.000[20] Menschen zu versorgen.[21] An diesem rein quantitativen Ansatz wird durchaus Kritik geübt und eine Vereinbarkeit mit den Vorgaben der NIS-RL bezweifelt. Denn nach deren Art. 4 Nr. 4 i. V. m. Art. 5 Abs 2 i. V. m. Annex II sollen für die Bestimmung der „Betreiber wesentlicher Dienste" (= KRITIS) sowohl qualitative als auch quantitative Kriterien herangezogen werden.[22] Nach Ansicht der Kritiker müssten auch mögliche Domino-Effekte als qualitative Kriterien herangezogen werden, die sich daraus ergeben, dass bestimmte KRITIS von den Vorleistungen anderer Anlagen abhängig sind, die möglicherweise die genannten fixen Schwellenwerte nicht erreichen. Ein Ausfall dieser unterschwelligen Anlagen hätte dann trotzdem den Ausfall der von ihr abhängigen KRITIS zur Folge. Dieser Gedanke ist nicht ohne weiteres von der Hand zu weisen. Allerdings verkennt er im Bereich der Stromversorgung auch, dass der Strom i. d. R. nicht unmittelbar von einer Energieerzeugungsanlage zur versorgten KRITIS fließt, deren Stromversorgung also unmittelbar von dieser (kleinen) Anlage abhängt. Vielmehr wird der Strom ins Netz eingespeist und dann an alle möglichen Verbraucher weiterverteilt. Fällt eine Energieerzeugungsanlage aus, so wird dies schon zur Stabilisierung des Netzes dadurch aus-

17 BSI-Kritisverordnung vom 22.4.2016 (BGBl. I S. 958).

18 Vgl. *Gehrmann/Klett*, K&R 2017, 372, 373.

19 Erste Verordnung zur Änderung der BSI-Kritisverordnung vom 21.6.2017 (BGBl. I S. 1903).

20 Für Krankenhäuser wurde auf die Versorgung von 30.000 Menschen abgestellt, da die Versorgungsleistung deutlich verteilter und durch kleinere Einheiten erbracht wird. Ein Abstellen auf 500.000 Menschen hätte hier vermutlich dazu geführt, dass es keine KRITIS gibt.

21 *Voigt*, Rn. 359.

22 Vgl. dazu *Voigt*, Rn. 360; *Gehrmann/Klett*, K&R 2017, 372, 374.

geglichen, dass andere Anlagen mehr Strom einspeisen. Aus gesamtgesellschaftlicher Sicht macht es daher auch unter qualitativen Gesichtspunkten durchaus Sinn, nur die Energieerzeugungsanlagen als KRITIS zu definieren, die eine gewisse Größe haben und deren Ausfall sich nicht völlig einfach kompensieren lässt.

### 2. Staatliche Maßnahmen zum Schutz Kritischer Infrastrukturen

**10** Zum Schutz der KRITIS hat der Gesetzgeber mit dem IT-SiG eine Reihe von Maßnahmen vorgesehen. So kann das BSI die Betreiber von solchen KRITIS nach § 3 Abs. 3 BSIG auf deren Ersuchen hin bei der Absicherung ihrer IT beraten und unterstützen oder auf qualifizierte Sicherheitsdienstleister verweisen. Eine entsprechende Liste qualifizierter Dienstleister veröffentlicht das BSI auf seiner Webseite.[23] Zudem hat der Gesetzgeber dem BSI in § 8b Abs. 1 BSIG die Aufgabe als zentrale Meldestelle für Betreiber Kritischer Infrastrukturen zugewiesen. Als solche hat das BSI die Aufgabe, sämtliche für die IT-Sicherheit Kritischer Infrastrukturen relevanten Informationen nach § 8b Abs. 2 BSIG zu sammeln und diese den Betreibern und den zuständigen Aufsichtsbehörden zur Verfügung zu stellen. Das BSI kann gem. § 8 Abs. 6 BSIG auch die Hersteller von informationstechnischen Produkten und Systemen zur Mitwirkung an der Beseitigung oder Vermeidung von Störungen bei der Informationstechnik von KRITIS verpflichten. Voraussetzung ist, dass dies erforderlich ist, also kein milderes, gleich wirksames Mittel zur Verfügung steht. Dies wird regelmäßig dann der Fall sein, wenn die Störung ihre Ursache im jeweiligen IT-Produkt hat oder haben kann – etwa bei Programmierfehlern. Diese werden in der Regel nur durch den Hersteller des jeweiligen Produktes beseitigt werden können, da nur der Hersteller das Produkt in Gänze kennt und etwa wichtige Sicherheitsupdates für alle Nutzer schnell entwickeln kann.[24]

### 3. Verpflichtungen für Betreiber Kritischer Infrastrukturen

**11** Doch der Schutz von KRITIS erfolgt nicht nur über staatliche Maßnahmen. Vielmehr werden auch den KRITIS-Betreibern verschiedene Absicherungs-, Nachweis- und Meldepflichten auferlegt. Wie der mit dem IT-SiG 1.0 eingeführte § 8c BSIG klarstellt, fungieren die §§ 8a und 8b BSIG als Auffangregelungen für alle KRITIS-Betreiber, für die nicht bereits entsprechende Verpflichtungen nach anderen gesetzlichen Regelungen bestehen.[25]

---

23 Vgl. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Qualifizierte-Dienstleister/qualifizierte-dienstleister_node.html (Stand: 27.7.2021).

24 Vgl. BT-Drs. 18/5121, 16.

25 Vgl. Gabel/Heinrich/Kiefner/*Wimmer/Mechler*, Kap. 5 Rn. 30.

Für den Bereich der Telekommunikation, der Energieversorgung und des Atomgesetzes führte das IT-SiG 1.0 entsprechende Verpflichtungen neu ein. Sie waren durch den § 8c BSIG von den entsprechenden Verpflichtungen der §§ 8a und 8b BSIG befreit. Ebenfalls von den Pflichten der §§ 8a und 8b BSIG ausgenommen wurden Kleinstunternehmen, also Unternehmen, die weniger als 10 Personen beschäftigen und deren Jahresumsatz bzw. -bilanz den Betrag von 2 Mio. Euro nicht überschreitet.

*a) Absicherungs- und Nachweispflichten des § 8a BSIG*

**12** Mit § 8a Abs. 1 wurden die Betreiber Kritischer Infrastrukturen erstmals verpflichtet, angemessene organisatorische und technische Vorkehrungen zur Vermeidung von Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der IT-Systeme zu treffen, die sie zur Erbringung ihrer kritischen Versorgungsdienstleistungen benötigen. Dabei soll der Stand der Technik eingehalten werden. Da die Regelung als Soll-Vorschrift ausgestaltet ist, dürfen die Betreiber jedoch in begründeten Fällen davon abweichen.[26] Es sind die zielführenden Maßnahmen erforderlich, deren Aufwand nicht außer Verhältnis zu den Folgen eines Ausfalls oder einer Beeinträchtigung der Kritischen Infrastruktur steht. Aufgrund der besonderen Bedeutung der Versorgungssicherheit werden daher finanzielle Erwägungen („zu teuer") allein in aller Regel keine Abstriche bei der Absicherung begründen können.[27] Vielmehr muss sichergestellt sein, dass die Versorgung trotz Verzicht auf bestimmte Maßnahmen gesichert ist (z. B. durch Entnetzung o. ä.).

**13** Da der Stand der Technik im Bereich der IT-Sicherheit schwer zu bestimmen sein kann,[28] sieht § 8a Abs. 2 vor, dass die Betreiber und ihre Branchenverbände branchenspezifische Sicherheitsstandards (B3S) vorschlagen können. Unter Einbeziehung des Bundesamts für Bevölkerungsschutz und Katastrophenhilfe sowie der zuständigen Aufsichtsbehörden entscheidet das BSI auf Antrag, ob die B3S geeignet sind, die Einhaltung der Absicherungsanforderungen aus Abs. 1 zu gewährleisten.[29]

**14** Zudem hatten die Betreiber die Erfüllung der Sicherheitsanforderungen gem. § 8a Abs. 3 BSIG mindestens alle zwei Jahre auf geeignete Weise nachzuweisen. Hierfür sieht das Gesetz Sicherheitsaudits, Prüfungen und Zertifizierungen vor, ohne jedoch näher auszugestalten, wie diese auszusehen haben. Dem BSI war im § 8a Abs. 4 BSIG die Befugnis eingeräumt worden, Anforderungen an das Nachweisverfahren, die Anforderungen an die prü-

---

26 *Gitter/Meißner/Spauschus*, DuD 2016, 7, 8; Gabel/Heinrich/Kiefner/*Wimmer/Mechler*, Kap. 5 Rn. 16; Schenke/Graulich/Ruthig/*Buchberger,* § 8a BSIG Rn. 2.

27 *Voigt*, Rn. 364.

28 Vgl. Schwartmann/Jaspers/Thüsing/Kugelmann/*Ritter*, Art. 32 DSGVO Rn. 84.

29 *Rath/Kuss/Bach*, KuR 2015, 437, 439; *Roßnagel*, DVBL 2015, 1206, 1209.

fende Stelle und die auszustellenden Nachweise festzulegen. Davon hat das BSI jedoch keinen Gebrauch gemacht. Dadurch sollte den Unternehmen die Freiheit gelassen werden, auf bereits existierende Nachweissysteme aufzusetzen, sofern diese geeignet sind.[30] In der Fassung nach dem IT-SiG 1.0 sah die Regelung vor, dass die Betreiber dem BSI nur eine Aufstellung (!) der durchgeführten Audits, Prüfungen und Zertifizierungen nebst dabei aufgedeckter Sicherheitsmängel übermitteln müssen. Eine eigeninitiative Übermittlung der entsprechenden Nachweisunterlagen oder -ergebnisse selbst war nicht vorgesehen. Nur sofern dem BSI Sicherheitsmängel bekannt werden, durfte es diese anfordern. Beim Vorliegen von Sicherheitsmängeln sollte das BSI im **Einvernehmen mit der zuständigen Aufsichtsbehörde des Bundes** oder im **Einvernehmen mit sonstigen Aufsichtsbehörden** die Beseitigung der Sicherheitsmängel verlangen dürfen. Bei Nichtbeseitigung dieser Mängel konnte das BSI das höchste im BSIG vorgesehene Bußgeld i. H.v 100.000 Euro verhängen. Eine eigene Untersuchungs- und Kontrollbefugnis des BSI zur Feststellung von Sicherheitsmängeln war jedoch nicht vorgesehen.

*b) Meldepflichten des § 8b BSIG*

Die KRITIS-Betreiber wurden durch § 8b Abs. 3 BSIG erstmals verpflichtet, dem BSI binnen 6 Monaten nach Inkrafttreten der BSI-KritisV eine Kontaktstelle zu benennen, über die sie jederzeit Meldungen des BSI entgegennehmen können. Faktisch mussten sie also 24h pro Tag und 7 Tage die Woche eine Erreichbarkeit sicherstellen.[31] Dahinter steht die Idee, dass das BSI die Betreiber über diese Kontaktstelle jederzeit und schnell über Gefahren für die IT-Sicherheit der KRITIS-relevanten IT und entsprechende Schutzmöglichkeiten informieren kann.[32] Um den Aufwand der Informationsbewertung gerade für kleine Betreiber zu reduzieren, erlaubte § 8b Abs. 5 BSIG den Betreibern, zusätzlich eine gemeinsame übergeordnete Ansprechstelle aus dem gleichen KRITIS-Sektor zu benennen, die dann als Kommunikationskanal genutzt werden kann. **15**

Nicht zuletzt, um die o. g. Warnungen an die Betreiber auf eine breite Informationsbasis zu stellen, verpflichtete der neue § 8b Abs. 4 BSIG die KRITIS-Betreiber dazu, das BSI über erhebliche Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer IT zu informieren.[33] Diese Verpflichtung bezieht sich jedoch nur auf solche Störungen, die entweder zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der KRI- **16**

30 Vgl. BT-Drs. 18/4096, 26.
31 *Rath/Kuss/Bach*, K&R 2015, 437, 438.
32 BT-Drs. 18/4096, 27.
33 BT-Drs. 18/4096, 28.

TIS führen können oder geführt haben. Wenn ein Einfluss der Störung auf die Erbringung der kritischen Dienstleistung ausgeschlossen ist, besteht keine Meldepflicht.[34] Die Betreiber trifft insoweit eine Pflicht, die möglichen Folgen einer Störung zu analysieren und eine entsprechende Prognoseentscheidung zu treffen.[35]

**17** Wann eine Störung erheblich i. S. d. § 8b Abs. 4 S. 1 BSIG war, hat das Gesetz nicht im Detail geregelt.[36] Die Gesetzesbegründung umschrieb jedoch Kriterien, an denen sich die Betreiber orientieren können. So sollen Störungen erheblich sein, wenn sich nicht automatisiert und mit wenig Aufwand abgewehrt werden können. Insbesondere neuartige Angriffstechniken und ein erhöhter Ressourcenaufwand für die Bewältigung der Störungen können daher ein Indikator für erhebliche Störungen sein.[37]

**18** § 8b Abs. 4 S. 2 BSIG machte auch konkrete Vorgaben zum Inhalt der Meldung. Diese sollte nicht nur Angaben zur Störung selbst enthalten, sondern auch zu den technischen Rahmenbedingungen, (vermuteten) Störungsursachen und der betroffenen Informationstechnik. Diese Angaben sollen dem BSI ein präzises Bild der Störung vermitteln, damit es sowohl den betroffenen Betreibern schneller helfen als auch anderen Betreibern zielgerichtet Informationen zur deren möglicher Gefährdung erstellen kann. Dafür ist es hilfreich zu wissen, welche Störungsursachen Betreiber vermuten oder gar sicher kennen. Die Angaben zur betroffenen IT lassen Schlüsse darüber zu, ob ggf. bisher unbekannte Schwachstellen bestimmter IT-Systeme ausgenutzt werden, und ermöglichen erst die zielgerichtete Warnung anderer Betreiber und die Erarbeitung spezifischer Abwehrmaßnahmen. Die Meldung muss nicht den Namen des meldenden Betreibers beinhalten, soweit die Störung noch nicht zu einem Ausfall oder einer Beeinträchtigung der Funktionsfähigkeit der KRITIS geführt hat. Damit wurde den Interessen der Betreiber Rechnung getragen, für die das Bekanntwerden von Störungen auch wirtschaftliche Auswirkungen haben kann.[38] Die Betreiber können die Meldung daher in diesen Fällen pseudonymisiert abgeben.[39] Durch die Abgabe einer pseudonymisierten, aber eben nicht anonymen Meldung wird sowohl den Betreiberinteressen Rechnung getragen als auch der Notwendigkeit, dass das BSI u. U. Rückfragen zum Vorgang stellen können muss.[40]

---

34 BT-Drs. 18/4096, 28.
35 *Voigt*, Rn. 372.
36 Dazu kritisch *Roßnagel*, DVBl 2015, 1206, 1210.
37 BT-Drs. 18/4096, 28.
38 *de Wyl/Weise/Bartsch*, N&R 2015, 21, 25.
39 *de Wyl/Weise/Bartsch*, N&R 2015, 21, 25, nehmen unzutreffend eine anonymisierte Meldung an, die jedoch von der Gesetzesbegründung gerade nicht gedeckt ist.
40 BT-Drs. 18/4096, 28.

Die Meldung an das BSI ist unverzüglich abzugeben, also ohne schuldhaftes Zögern. Ein solches schuldhaftes Zögern wird i. d. R. dann nicht vorliegen, solange die Meldepflichtigen selbst noch rudimentäre Informationen zur Beeinträchtigung zusammentragen. Im Hinblick auf die Funktion der Vorfallsmeldung im Frühwarnsystem des § 8b BSIG wird man einen Vorrang der Schnelligkeit vor der Vollständigkeit annehmen können.[41] Da sich die Informationslage bei Vorfällen dynamisch gestaltet, müssen Betreiber also bei ausreichender Erkenntnislage sofort melden und später hinzutretende neue Informationen ggf. sukzessiv nachmelden. Nur so ist eine zeitnahe Warnung anderer Betroffener über laufende Angriffswellen und -kampagnen gewährleistet. **19**

*c) Bußgeldbefugnis – § 14 BSIG*

Um die KRITIS-Betreiber zur Einhaltung ihrer neuen Verpflichtungen aus den §§ 8a und 8b BSIG anhalten zu können, wurden dem BSIG mit dem IT-SiG 1.0 erstmals Bußgeldregelungen hinzugefügt. Es wurde jedoch noch nicht jede Pflichtverletzung sanktioniert, sondern nur eine Auswahl. Dazu gehörten die Verletzung der Absicherungspflicht aus § 8a Abs. 1 S. 1 BSIG, die Nichtbefolgung einer vollziehbaren Anordnung zur Übermittlung der Audit-/Prüfergebnisse nach § 8a Abs. 3 S. 4 Nr. 1 oder zur Beseitigung von Sicherheitsmängeln nach § 8a Abs. 3 S. 4 Nr. 2 BSIG, die nicht oder zu spät erfolgte Benennung einer Kontaktstelle nach § 8b Abs. 3 BSIG sowie die nicht, nicht richtig, nicht vollständig oder nicht rechtzeitige Abgabe der Meldung über eine erhebliche IT-Störung, die zum Ausfall oder der Beeinträchtigung von KRITIS geführt hat nach § 8b Abs. 4 S. 1 Nr. 2 BSIG. Nicht erfasst waren z. B. die Verletzung der übrigen Meldepflicht nach § 8b Abs. 4 S. 1 Nr. 2 BSIG oder die Verletzung der Nachweispflicht aus § 8a Abs. 3 S. 1 BSIG. **20**

*d) Absicherungspflichten des § 109 TKG*

Im Telekommunikationsgesetz gab es im § 109 TKG bereits vor dem IT-SiG 1.0 Pflichten für die Telekommunikationsdiensteanbieter zur Absicherung ihrer Informationstechnik. Um einen gewissen Gleichlauf mit den Regelungen des § 8a BSIG zu erreichen, wurde durch das IT-SiG 1.0 in § 109 Abs. 2 S. 2 TKG die Maßgabe ergänzt, dass bei der Umsetzung dieser Absicherungsmaßnahmen der Stand der Technik berücksichtigt werden muss.[42] Eine entsprechende Formulierung war auch im Rahmen des § 8a Abs. 1 S. 2 BSIG noch im RegE des IT-SiG 1.0 vorgesehen.[43] Der Gesetz- **21**

41 Vgl. *Voigt*, Rn. 375.
42 Vgl. Gabel/Heinrich/Kiefner/*Wimmer/Mechler*, Kap. 5 Rn. 35 f.
43 BT-Drs. 18/4096, 10.

geber hat diese Formulierung in § 8a Abs. 1 S. 2 auf die Beschlussempfehlung des Innenausschusses hin jedoch verschärft („Dabei soll der Stand der Technik eingehalten werden").[44] In § 109 Abs. 1 S. 2 TKG blieb die bloße Pflicht zur Berücksichtigung jedoch erhalten. Daher genügt es, wenn die TK-Diensteanbieter sich bei ihren Planungen mit dem Stand der Technik beschäftigen. Abweichungen vom Stand der Technik müssen – anders als bei § 8a BSIG – nicht besonders begründet werden. Allerdings müssen die ergriffenen Maßnahmen geeignet sein, die Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu sichern, die Auswirkungen von Sicherheitsverletzungen für die Nutzer und andere Netze gering zu halten sowie den ordnungsgemäßen Netzbetrieb sicherzustellen. Dies wird bei Maßnahmen, die nicht dem Stand der Technik entsprechen, regelmäßig schwerfallen.

**22** Die von § 8a Abs. 1 S. 2 BSIG abweichende Regelung in § 109 Abs. 2 S. 2 TKG ist auch insoweit unproblematisch, als die von den TK-Diensteanbietern zu ergreifenden Maßnahmen in einem Katalog von Sicherheitsanforderungen durch die BNetzA nach § 109 Abs. 6 TKG konkretisiert werden können. Vor dem IT-SiG 1.0 tat sie dies im Benehmen mit dem BSI und dem oder der BfDI. Durch das IT-SiG 1.0 wurde aus dem Benehmenserfordernis ein Einvernehmenserfordernis. Dadurch sollte der gesteigerten Bedeutung von IT-Sicherheitsbelangen Rechnung getragen werden,[45] die aus der zunehmenden Umstellung klassischer leitungsvermittelter Kommunikation zu paketvermittelter Kommunikation resultiert. IT-Sicherheits- und Datenschutzbedenken sollten bei der Erstellung des Kataloges nicht einfach durch die BNetzA übergangen werden können.

**23** Um die ordnungsgemäße Absicherung kontrollieren zu können, wurde mit dem IT-SiG 1.0 erstmals die Pflicht der BNetzA eingeführt, die Umsetzung der Sicherheitskonzepte regelmäßig zu überprüfen. Zuvor war dies für die BNetzA als „Kann"-Aufgabe ausgestaltet. Diese Überprüfungen „soll" die BNetzA mindestens alle 2 Jahre durchführen. Da der Zeitraum als „Soll"-Vorschrift ausgestaltet ist, kann die BNetzA mit Begründung (z. B. Ressourcenmangel) davon abweichen.

**24** Nach dem durch das IT-SiG 1.0 eingeführten § 109 Abs. 8 TKG sollte die BNetzA das BSI darüber informieren, wenn sie Mängel bei der IT-Absicherung entdeckt und welche Abhilfemaßnahmen sie daraufhin vom TK-Anbieter gefordert hat.

---

44 Vgl. BT-Drs. 18/5121, 7.
45 BT-Drs. 18/4096, 36.